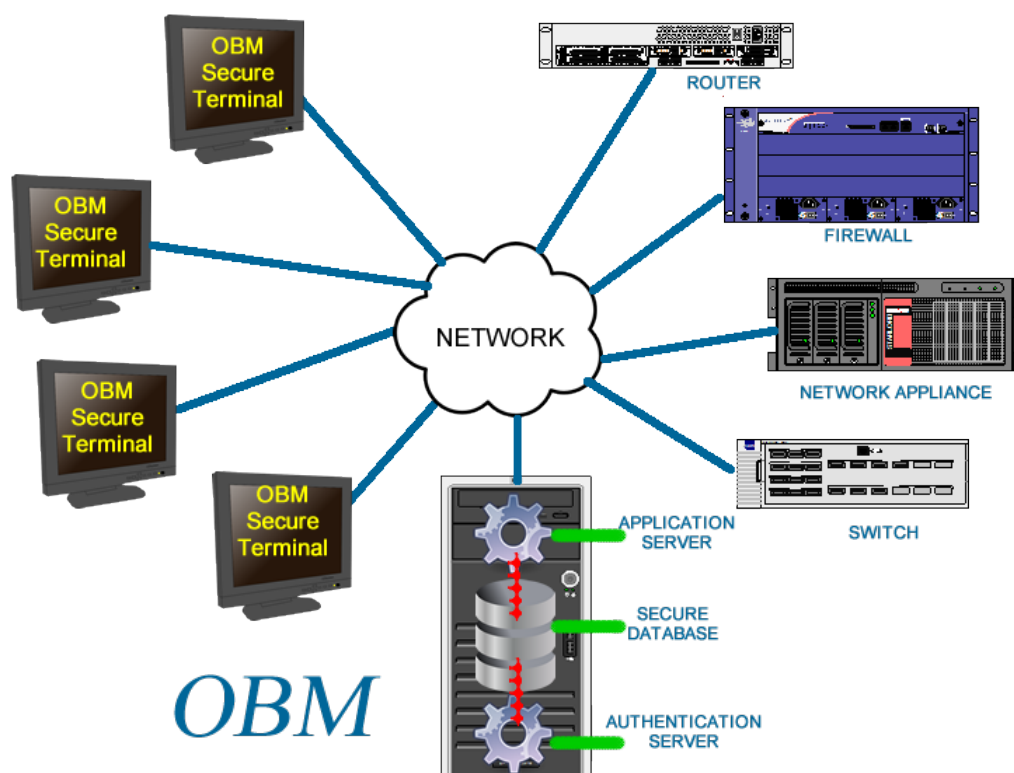


Version 6.04.00

OBM USER MANUAL



OUT OF BAND MANAGER



Communications Devices, Inc
The Global Leader in Network Security

Communication Devices Inc.

85 Fulton St.

Boonton, NJ 07005

USA

Phone: +1 973 334-1980/+1 800 359 8561

Internet: support@commdevices.com

<http://www.commdevices.com/support-center/>

OBM User Guide Release 6.04

Copyright © 1991, 2015 Communication Devices Inc. and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or de-compilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing. If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are “commercial computer software” or “commercial technical data” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007).

Communication Devices Inc. 85 Fulton Street Boonton, NJ 07005.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Communication Devices Inc. and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products, and services from third parties. Communication Devices Inc. and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Communication Devices Inc. and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1	GETTING STARTED	1-1
1.1	Installing the OBM	1-1
1.2	Starting the OBM Program.....	1-2
1.3	OBM Screen Description.....	1-4
1.4	Customizing the Appearance.....	1-5
1.5	Setup and Use Overview	1-6
2	CDI AND NETWORK SECURITY.....	2-1
2.1	CDI's Role in Network Security	2-1
2.2	Device Management	2-2
2.3	Database organization.....	2-3
3	MANAGING GROUPS.....	3-1
3.1	Group Template.....	3-1
3.1.1	Opening the Group Template.....	3-1
3.1.2	Device Info Tab	3-2
3.1.3	System Options tab	3-2
3.1.4	Internal Modem.....	3-3
3.1.5	Network Properties	3-3
3.1.6	Defined Ports	3-4
3.1.7	Polling.....	3-4
3.2	Group Management	3-5
3.2.1	Adding a Group.....	3-5
3.2.2	Deleting a Group.....	3-6
3.2.3	Renaming a Group	3-6
3.3	Remote Site Management.....	3-7
3.3.1	Adding a Remote Site	3-7
3.3.2	Removing a Remote Site	3-8
3.3.3	Renaming a Remote Site.....	3-8
4	WORKING WITH REMOTE DEVICES	4-1
4.1	Remote Devices.....	4-1
4.1.1	Adding a Remote device.....	4-1
4.1.2	Removing a Device.....	4-4
4.1.3	Modifying a Device's parameters	4-4
4.1.4	Adding a Non-CDI device	4-4
4.2	Device Info tab	4-5
4.3	Network Properties tab	4-8
4.4	Cellular Module Properties.....	4-11
4.5	System Options.....	4-12
4.6	Analog Internal Modem.....	4-14
4.6.1	Internal Modem Type:	4-15
4.6.2	Modem Inactivity timer (min):	4-15
4.6.3	Serial AT Commands:.....	4-15
4.6.4	Modem Port Bits/Parity:	4-15
4.6.5	Modem Port Baud Rate:.....	4-15

4.6.6	Defined Messages	4-15
4.6.7	Primary:.....	4-15
4.6.8	Secondary:.....	4-16
4.7	Cellular Internal Modem	4-16
4.8	Defined Ports	4-16
4.9	Client Devices.....	4-17
4.10	Ports View	4-18
4.11	Device Search.....	4-18
4.11.1	Displaying a list of all Devices	4-19
4.11.2	Displaying a list of Specific Devices	4-19
4.12	Adding Licenses	4-19
5	MANAGING CLIENT DEVICES.....	5-1
5.1	NOC Group.....	5-1
5.1.1	Viewing All Client Devices.....	5-1
5.1.2	Adding a site to the NOC Sites Group.....	5-2
5.1.3	Deleting a NOC Site	5-2
5.2	View the Client Devices of a Group.....	5-3
5.3	Attaching a Client Device to a Group	5-3
5.3.1	Attaching a Client Device from the Group Template.....	5-3
5.3.2	Attaching a Client Device from NOC Sites tab	5-4
5.4	Adding an SSE Device	5-4
5.5	Adding a UniGuard or Port Authority Client Device.....	5-7
6	USER MANAGEMENT	6-1
6.1	User Management tab features	6-1
6.1.1	Sorting the user list	6-1
6.2	Finding a User	6-2
6.3	Adding a User.....	6-2
6.4	Modifying a User.....	6-5
6.5	Deleting a User	6-5
6.6	RSA Add User Batch.....	6-6
6.7	Adding a System User	6-1
6.8	Managing Roles.....	6-1
6.8.1	Creating a Role	6-1
6.8.2	Modifying a Roles.....	6-2
6.9	Managing Access Calendars.....	6-3
6.9.1	Viewing Available Access Calendars.....	6-3
6.9.2	Adding an Access Calendar	6-4
6.9.3	Deleting an Access Calendar	6-4
6.9.4	Modifying an Access Calendar.....	6-4
7	PROGRAMMING	7-1
7.1	Programming Devices	7-1
7.2	Programming a Group	7-2
7.3	Programming a Single Device.....	7-3
7.4	Programming Multiple Devices.....	7-4
7.5	Programming all Devices of a Group	7-5
7.6	Telnet to a Device.....	7-5
7.7	Clear Device	7-6

7.8	View Alarms	7-6
7.9	Clear Alarms	7-7
8	CONNECTING TO REMOTE DEVICES	8-1
8.1	Overview	8-1
8.2	Terminal screen features	8-1
8.2.1	Connecting to a device	8-1
8.2.2	Terminal Options	8-3
8.3	Connecting to a Device	8-4
8.3.1	Modem:	8-5
8.3.2	Network:	8-5
8.3.3	Serial:	8-5
8.3.4	Cellular:	8-5
8.3.5	Modem Communications	8-6
8.3.6	Cellular Communications	8-7
8.3.7	Serial Communications	8-7
8.3.8	Network Communications	8-8
8.3.9	SSH Communications:	8-9
8.4	Sending and Receiving Files	8-9
9	SYSTEM SETTINGS.....	9-1
9.1	System Settings	9-1
9.2	Alarm Settings	9-3
9.3	Email Alerts	9-3
9.3.1	Email Settings	9-4
9.3.2	Adding a Group to receive alarms	9-4
9.3.3	Adding an individual user	9-5
9.3.4	Defining the Severity Level of an Event.....	9-5
9.4	Log Settings	9-6
9.4.1	Define OBM SNMP Events.....	9-6
9.4.2	OBM RealTime Log Setting	9-7
9.4.3	Custom Field Settings	9-7
9.4.4	Log Purge Settings	9-7
9.5	Common System Settings	9-7
9.6	Network Dialout Settings	9-7
9.7	Network Dialout Settings	9-8
9.8	Database Manager	9-8
10	REPORT MANAGEMENT	10-1
10.1	OBM Audit	10-1
10.2	Device Audit	10-1
10.3	Syslog	10-2
10.4	Custom Report	10-2
10.4.1	Adding a Filter	10-2
10.4.2	Deleting a Filter	10-3
10.5	Keystroke Log	10-3
10.6	Deleting a Report	10-3
10.7	Printing or Exporting a Report	10-3
10.7.1	Printing a Report	10-4
10.7.2	Exporting a Report	10-4

10.7.3	Emailing a Report.....	10-4
10.8	Report Filters Summary.....	10-5
11	POLLING SERVICE MANAGEMENT	11-1
11.1	About Polling Services	11-1
11.2	Setting up and Configuring the Polling Service	11-1
11.3	Scheduling Polling.....	11-2
11.4	Authentication Management.....	11-4
11.5	Network Discovery Tool	11-4

1 GETTING STARTED

This section describes how to get started using the OBM program to manage UniGuard and Port Authority devices.

- Access the OBM program
- Key Features of the OBM screen
- Lists steps to setup and use the OBM

1.1 Installing the OBM



There are four parts to the full OBM install

A common installation is placing all four components on a VMWARE server and using RDP or CITRIX to access.

1. SQL Express or SQL full server – the OBM uses an SQL compliant database. The database can run on SQL Express (provided with the install) or can run on SQL full, which will provide more enterprise functions for larger installs. THIS SHOULD BE INSTALLED FIRST IN A NEW INSTALL.
2. CDI Database – This is the framework for the CDI database. As CDI releases new version of the OBM, the CDI database may require updating. The screen shows the version that is installed and the version to be installed.
3. Application Server – The App serve is a piece of software that acts as an intermediary between the SQL database and the OBM client software. The APP server should reside on the same physical machine as the database.
4. Out of Band Manager – the OBM is a piece of software that can run on the server or on a client that can access the same network as the server.

1.2 Licenses associated with the software, Devices, Seat Licenses, EDL's, DL's, SSL's etc...

The CDI software is scaled by using several different license files to tailor the system for each type of application. These licenses include:

1.2.1 Enhanced Device License "EDL"

This is a software file that can be imported into the OBM allowing it to manage the device or devices in that file. An EDL is required for each device entered into the system.

1.2.2 Seat License "SL"

This is a software file that when imported into the OBM, will allow simultaneous access to the database by as many users in that file. It is recommended to have as many seat licenses as client devices in the system.

1.2.3 Device Information File ".DEV" *NEW*****

This file contains all the detailed information about each CDI device shipped. The file can be imported into the OBM via the "Unassigned Devices" tab at the top of the group tree. When imported, it will bring in all the devices in the file into the "unassigned devices" group. The devices can then be dragged and dropped into any existing group without having to re-create the device and all its properties.

The .DEV file also contains the EDL file for any device.

1.2.4 System Support License "SSL"

This is a software file that contains the serial number and all pertinent information about your copy of the OBM software. It needs to be updated once a year to keep your level of support up to date. When that date approaches, the system will pop up a window reminding you that it is time to update your SSL license.

1.3 Starting the OBM Program

To start the OBM application, click the *OBM* desktop shortcut or click the *Start* button and then select CDI OBM Manager from the program list.

NOTE: If this is the first time you are logging onto OBM a registration form is displayed. Complete the form and email or fax it to CDI. CDI's email address and fax number are included on the form. To be eligible for covered upgrades and support, you must return this form to CDI.

To avoid having the Registration form displayed each time you run OBM, make sure the "Show this window the next time" checkbox is not checked.

OBM Registration Form

Communication Devices Inc.
85 Fulton Street, Boonton, NJ 07005
Phone: +1 973 334 1980
Fax: +1 973 334 0545
email: sales@commdevices.com
Web: http://commdevices.com

This form must be completed and returned to CDI to be eligible for upgrades and support. Fill out registration form to either email to CDI or print and Fax form to +1 973 334 0545.

Name
Title
Company
Address1
Address2
City
State: AK Zip Code
Country: United States
Phone
Fax
Primary Email Address
Secondary Email Address
Tertiary Email Address

The OBM logon screen is displayed. Enter your username and password and click *Logon*. If you have successfully entered your username and password, the OBM screen is displayed.

Note: The initial default username and password is administrator. The default username and password can be changed.

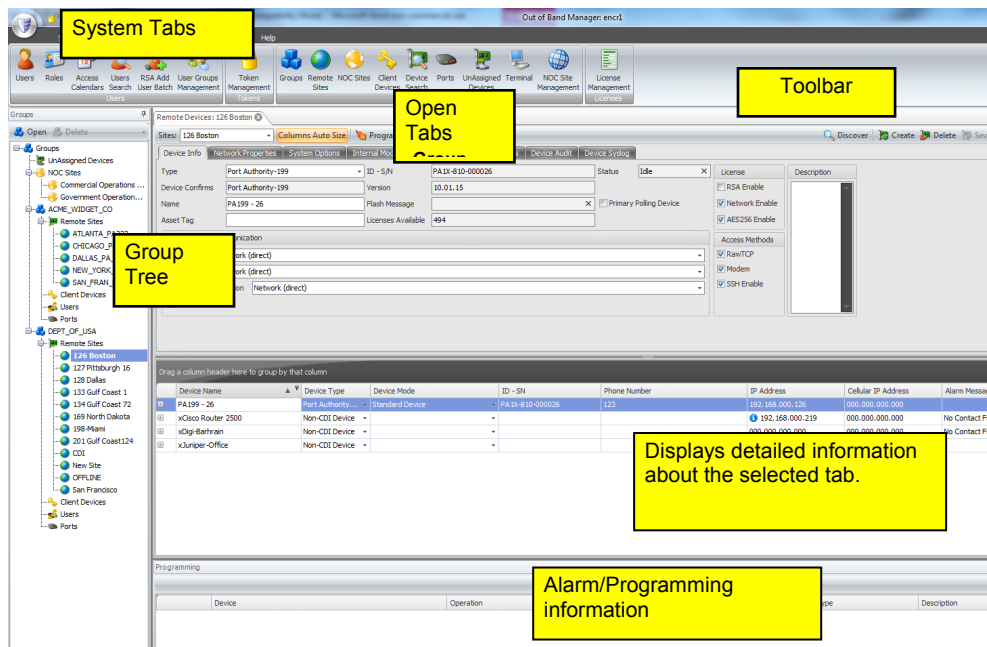


Figure 1-1 OBM screen

1.4 OBM Screen Description

The OBM screen makes it easy to perform all management tasks, from adding device, monitoring devices, managing users, and creating reports. Select the appropriate System Tab, and then clicking on the applicable tool perform the task.

System tabs: The system tabs enable you to switch among Security, Common, and Logs tasks. The toolbar icons displayed depend on the system tab selected. Note that selecting a different system tab does not close any tabs in the Open Tabs section.

Toolbar: The toolbar depends on the system tab selected.

Security: The tools in this toolbar enable you manage groups, system users, users, and devices.

Common: The tools in this toolbar allow you to specify system settings, display the registration form, manage polling and Radius service, and add licenses.

Logs: The tools in the toolbar enable you to view, create, and print audit reports, device batch logs, system logs, keystroke log, and create custom reports.

Group Tree: The Group Tree may be expanded to display all groups that have been retrieved from the OBM Databases in the SQL Server.

The NOC sites group defines the client devices in the system. Only in the NOC Sites can a client device be added to system, deleted from system and modified.

Each group may be compressed to display only the Group name or expanded to display the following information:

- **Unassigned Devices**

At the top of the group tree is a depository for any devices in the system that have not been assigned to any group or site. Each new device comes with a Device Information File or .DEV file. This file contains all the pertinent information for that device. To import this file open the “unassigned devices” group. There is a tab to import a device info file. Locate the device info file and import. Note this can be a batch file with multiple devices in it. The import process will create a device in the unassigned devices group based on the info in that file. This device can be edited and dragged into any existing group, or a new group can be created.

- **Remote Sites**

Each site is a remote edge point on a network. A typical site would contain a router, firewall, network switch, and a CDI Out of Band Device (PA100 or PA200 series). The OBM can provide access to all of these devices through its SSH functionality.

- **Client Devices**

Client devices are devices that are used to establish a secure connection from the NOC center to the remote site. The connections can be in band (network) or out of band (dial) . A typical client is a PA100 for FIPS 140-2 security, or a PA222 for commercial security.

- **Users**

Users are engineers or other personnel who can access the console port of a network element.

- **Ports**

Displays the individual ports on each CDI device and the device to which each port is connected. This is a convenient view if you are looking for a particular connected device rather than the CDI device that is managing it.

Open Tabs: This section displays all the tabs you have opened. To switch to a different tab, click the desired tab. To close a tab, click the “x:” by the tab name.

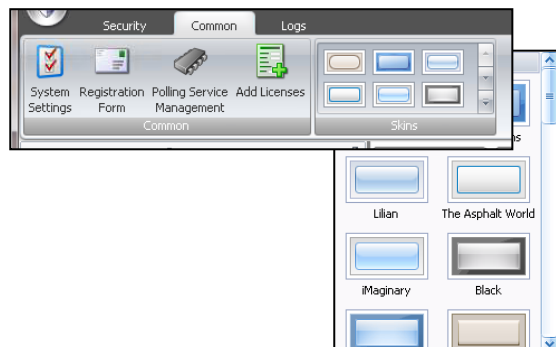
When you open a tab, more details may be displayed immediately below the tab. For example, when you select a Remote Site, a list of devices at the selected Remote Site is displayed.

Alarm/Programming: Depending on what is selected, the alarm/programming section displays alarms or programming status.

1.5 Customizing the Appearance

You can change color scheme of the OBM. Many color schemes are available.

To view the available color schemes, click **Common**, and then **Skins**. Select the skin that you want.



1.6 Setup and Use Overview

The steps to set up and use OBM are listed below.

1. Add **System Users** to establish who can access the OBM, what privileges they have, and when they can access the system. System Users, Roles, and Access Calendars allow you to do this.
2. Find your Device Info Files .DEV and import them into the system. This will streamline the setup process by grabbing all the details of each device from the device file instead of having to create them yourself. Do this by double clicking the “unassigned devices” group and importing via the tabs on the right.
3. Create your NOC site and add any **Client Devices**. **When you create your groups, these NOC devices can be assigned to each group individually.** Client Devices are your devices used in the NOC that will establish encrypted session with your remote devices via network or dial out connection.
4. Create a **Group**. The Group Template allows you to name and enter a description of the group, and establishes default parameters.
5. Check the number of **Device Licenses** available, and add licenses if necessary. Before you can add a device, a device license must be available.
6. Create **Remote Sites for that group** and add **Devices** to the site. CDI devices (PA100/PA200 series) or non-CDI device (routers, firewalls, switches) can be added to the site and managed/accessed via the OBM.
7. Add **Users**. These users can log on and authenticate to remote devices. They cannot access the OBM software itself like System users.
8. **Program** the devices. For first time use, select “Program-Reload” from the Programming dropdown list. This will “push” the config out to each CDI device selected for the program re-load.
9. Set up **Polling**. Polling is used for non-networked devices that require a dial out polling sequence to check on the remote devices. For networked devices, enable “OBM Heartbeat” and Syslog for real time reporting (including Telco line status) from the remote devices
10. **Connect to a device** to view and access devices attached to their host ports.
11. View **logs** and create **reports**.

2 CDI AND NETWORK SECURITY

A network is comprised of a plurality of connections to routers, firewalls, network switches, and other network elements. These elements are usually monitored and maintained by the Network Operations Center (NOC) Engineers. The engineers access the console port of the router or other network element to perform routine maintenance or to reset the device.

Access to the console port may be by in-band (direct SSH to the network interface) or out-of-band (through a CDI device to the serial console port) communications. Out of band access uses connections outside the bandwidth of the network thus security is critical to these access points.

To maintain network security, access to the console port is limited to authorized users, and the information being sent from the Engineer to the router or other element is protected.

2.1 CDI's Role in Network Security

CDI devices authenticate users and provide full encryption of data before allowing them access to the console port of a network element. Each CDI device maintains a database of authorized users and device credentials. Once an Engineer has successfully authenticated, he/she is permitted to access the network element. For example, to access a router, the Engineer first connects to a CDI device, such as a Port Authority 100 or 200 series, and authenticates. The device can also layer encryption on top of the connection.

Both in-band and out-of-band communication between the Engineer and the network element can be used by CDI devices, providing more security and enabling devices to be contacted even when there is a network problem. All information is encrypted.

CDI devices may provide both authentication and encryption functions or only authentication or encryption. PA100 series provided FIPS 140-2 encryption while PA200 series provide AES commercial encryption.

On the NOC side, a PA100 device can be set to encryption mode only and encrypt the information being sent by the Engineer.

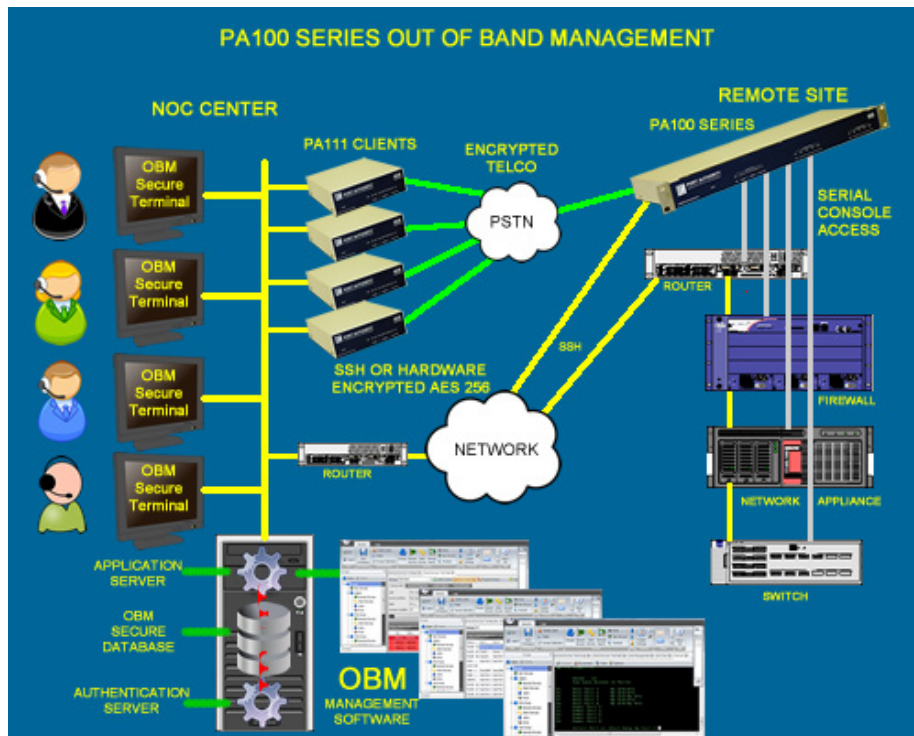


Figure 2-1 Example of Secure Out-of-Band Management for Routers

CDI has a full FIPS 140-2 validated product line, the PA100 series, or a PCI/FIPS compliant commercial line, the PA200 series. Both provide to factor authentication and encryption (optional on PA200).

The PA100 line has been submitted to the National Institute of Standards and Technology and is Validate for FIPS 140-2 for use on U.S. Government networks.

The PA200 line is built to the same standard but has not been submitted. It is PCI compliant.

Both product line provide basically the same functionality with the PA100 line being Validated as more secure.

2.2 Device Management

The CDI devices are managed remotely by the OBM (Out of Band Manager) application running on a Windows workstation. This can also be a VMWARE virtual machine. OBM provides centralized management and maintains a central database of users and devices enabling devices and users to be added, deleted, or modified from one location.

The OBM can be used for configuration only or can be used for configuration and access. If used for configuration only, once the devices are configured the software can sit idle.

Each Port Authority device has a local database updated from the OBM database. OBM communicates with remote devices over network, cell network,

or dial-up phone lines, serial ports, or IP connections. All communications are encrypted.

The OBM can also manage and access non CDI devices, such as Routers, Firewalls, and Network Switches. These devices can be access via SSH and periodically check for availability.

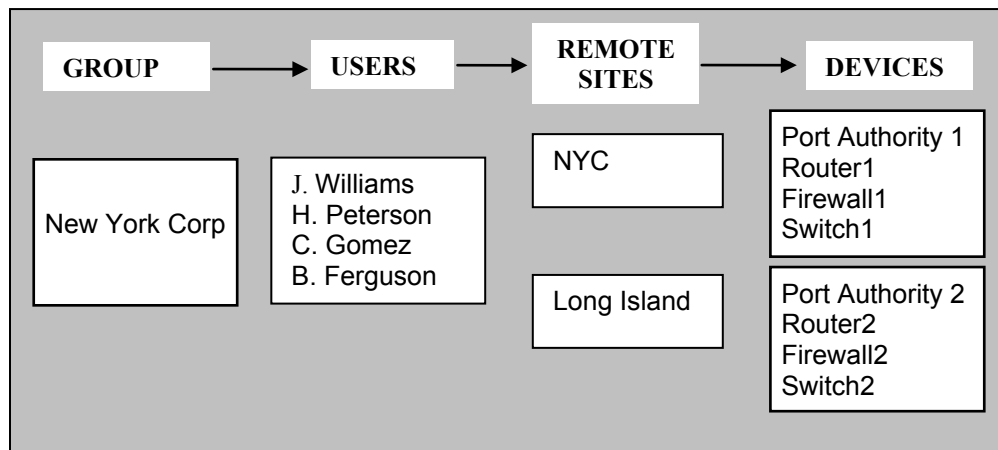
2.3 Database organization

The central database maintained by the OBM is organized into groups. A *group* is a collection of Sites which in turn are associated with devices that share a common user database. A group may be defined by region, company, or some other way. The key point to remember is that a group shares a common user database.

A group may be associated with remote devices and client devices. A *remote device* may be assigned to only one group and only to one remote site within the group. A *client device* may be added to the NOC and assigned to more than one group.

An individual *user* can be associated with multiple groups and to all Remote Sites within a group.

In the example below, four users are associated with the group New York Corp. The users have access to the two remote sites—NYC and Long Island. Each remote site has been assigned its own set of devices.



When a change is made to the database, it may be sent to one device, devices of one remote site, all devices of a group, or all devices, depending on what the change is and if auto programming is enabled.

For example, a user is changed (ex. "NocUser"). This user can be associated with multiple devices spanning several groups. All devices to which this user is associated would be set for update. If auto programming were enabled, all these devices associated with this user would be queued up for program updates.

The number of devices assigned to a site, the number of sites assigned to a group, as well as the total number of groups is virtually infinite, limited only by the storage capacity of the server running the SQL database program.

The maximum number of users associated with a device is 150.

3 MANAGING GROUPS

This section explains how to manage Groups and Remote Sites, use the Group Template to establish default settings for a device type, and modify all the devices of a particular type.

The following topics are included in this section:

- Description of the Group Template tabs
- Adding and deleting a Group
- Add and removing a Remote Site
-

3.1 Group Template

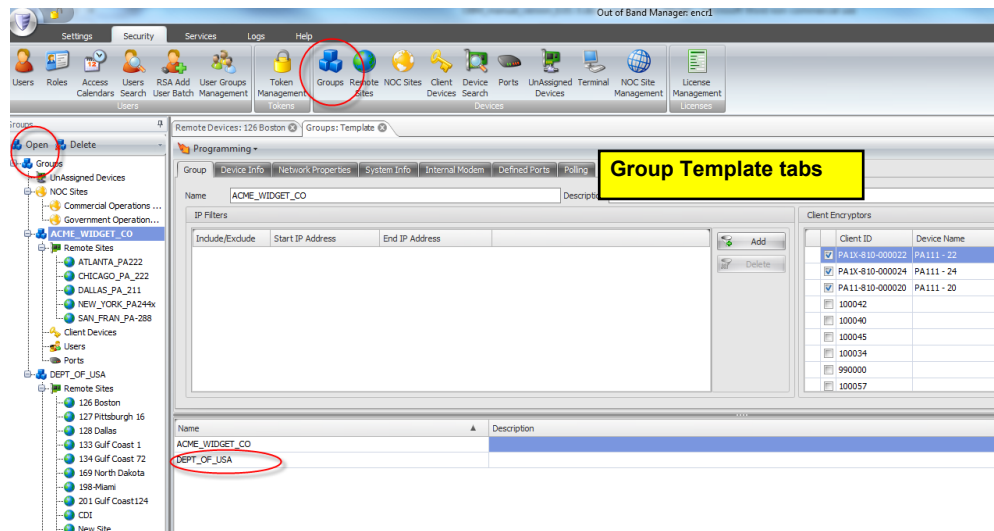
The Group Template establishes the default settings for the entire group. When a new device of the same type is added, the settings in the Group Template for that particular device type are used. You may modify all settings of a device type in the Device Info tab of the Group Template. To modify the settings of an individual device and for a detailed description of each parameter, please refer to the Working With Devices section.

3.1.1 Opening the Group Template

The Group Template for a Group can be opened by the following ways:

Select the Group from the Group List and click **Open**.

Click **Groups** in the toolbar and then click on the Group name from the list in open tab view.



From the Group view (Groups: Template tab) you will always see the following tabs:

- Group
- Device Info
- Network Properties
- System Info
- Internal Modem
- Defined Ports
- Polling

The tabs listed below depend on the type of device selected:

- Network Properties
- This tab is only displayed when the device type is set to a type that has an internal IP card.
- Defined Ports
- This tab is only displayed when the device type is set for a type with multiple host ports. Device types with only one host port (UniGuard, SAM-11, PA-111) will not have the Defined Ports tab.

3.1.2 Device Info Tab

The Device Info tab of the Group template enables to select a device type and define the communication paths by which OBM will access the device, and specify terminal communications. These settings will be used as the default settings when devices of the same type are added to the Group.

The screenshot shows the 'Device Info' tab of the 'Groups: Template' window. The window title is 'Remote Devices: 126 Boston'. The 'Sites' dropdown is set to '126 Boston'. The 'Columns Auto Size' button is visible. The 'Connect to' button is also present. The 'Device Info' tab is selected, showing the following fields:

Type	Port Authority-199	ID - S/N	PA1X-S10-000026	Status	Idle	X	License		Description
Device Confirms	Port Authority-199	Version	10.01.15				<input type="checkbox"/> RSA Enable		
Name	PA199 - 26	Flash Message		<input checked="" type="checkbox"/> Primary Polling Device			<input checked="" type="checkbox"/> Network Enable		
Asset Tag		Licenses Available	#94				<input checked="" type="checkbox"/> AES256 Enable		

Below the table, there are sections for 'Management Communication' and 'Terminal Communication'.

Management Communication:

Primary	Network (direct)
Secondary	Network (direct)

Terminal Communication:

Terminal Communication	Network (direct)
------------------------	------------------

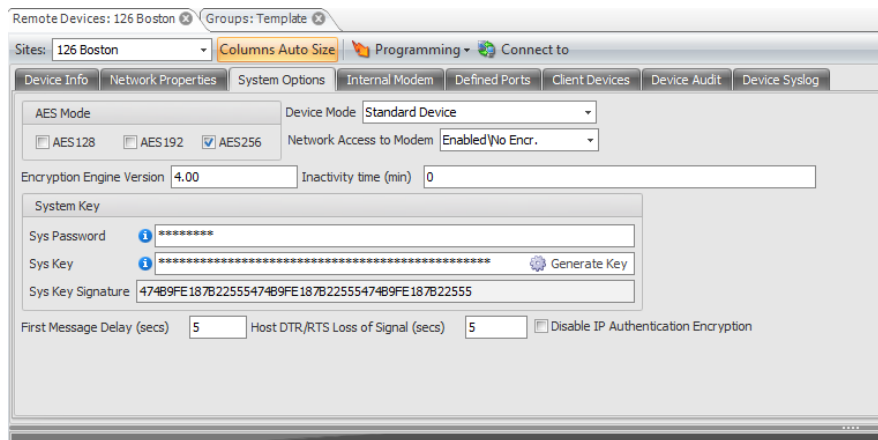
At the bottom left, there is a checkbox for 'SSH' which is checked.

On the right side, there is a section for 'Access Methods' with the following options:

- ☒ RawTCP
- ☒ Modem
- ☒ SSH Enable

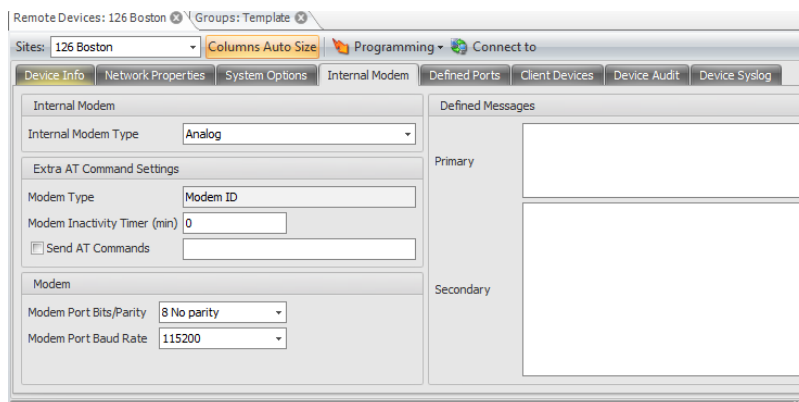
3.1.3 System Options tab

The parameters on this screen enable you to set user security levels, system password and key information, and first message delay time. The System Options screen may have different parameters depending on the device.



3.1.4 Internal Modem

The CDI device can have an internal modem or an internal Cellular Module. This can be selected in this tab. If a Cellular Module is selected the fields are all Network Based so the configuration for the Cellular Module is in the Network Properties tab. However the Cell Module must be select from the Modem tab. The fields of the Internal Modem tab enable you to define the modem port parameters, enable or disable AT commands sent to a remote device, and define the Primary, Secondary, and Host Connect messages for the device.



3.1.5 Network Properties

- This tab is only displayed when the device type is set to a type that has an internal IP card. The Networks Properties tab enables you to configure the include DNS, Syslog server, OBM Heartbeat, SNMP, and Radius Server attributes of a device.
- The network properties page is split into two sections.
 - Left: Ethernet network port on the device
 - Right: Cellular module IP address etc.

3.1.6 Defined Ports

This tab enables you to set communication parameters for the Host and Power ports of the Port Authority, Port Authority SAM, and MultiGuard devices. This tab is only displayed for multi-port devices; it is not available single-port devices like the UniGuard.

Remote Devices: 126 Boston Groups: Template

Sites: 126 Boston Columns Auto Size Programming Connect to

Device Info Network Properties System Options Internal Modem Defined Ports Client Devices Device Audit Device Syslog

Master/Slave Device: Master

Programmable ESC: ESC

Ports Power Ports

	Port Name	Baud Rate	Bits/Parity	Port Function	Port Direction	Authentication Type	Allow For Programming	Attach Modem	Host Port	Logica
1	cisco2900	9600	8 No parity	Host Port	In	Standard Device			1	
2	West Rack Switch	9600	8 No parity	Host Port	In	Standard Device			2	
3	East Rack Switch	9600	8 No parity	Host Port	In	Standard Device			3	
4	Juniper	9600	8 No parity	Host Port	In	Standard Device			4	
5	Firewall	9600	8 No parity	Host Port	In	Standard Device			5	

3.1.7 Polling

This tab enables you to set the parameters to poll non-CDI devices. You can specify how often the device contacted and the connection method.

Remote Devices: 126 Boston Groups: Template

Sites: 126 Boston Columns Auto Size Connect to

Device Info Network Properties Polling Device Audit Device Syslog

☒ Enable Polling

Interval: 4

Max No. of Missed Polls: 2

Connection: Ping

3.2 Group Management

Group management includes adding, removing, and renaming Groups and Remote Sites.

3.2.1 Adding a Group

To add a Group, click Groups button in the Security toolbar. The Group Template will open.

Click the **Create** button. A blank Group template will be displayed.

The screenshot shows the 'Groups: Template' dialog box. The 'Create' button in the top toolbar is highlighted with a red rectangle. The dialog has tabs for 'Group', 'Device Info', 'System Info', 'Internal Modem', and 'Non-CDI Heartbeat'. The 'Group' tab is active, showing fields for 'Name' and 'Description'. Below these are 'IP Filters' and 'Client Encryptors' sections.

Select existing users who will have access to this group

The screenshot shows the 'Select Items' dialog box. It contains a list of users with checkboxes next to their names. The users listed are: enc4, encr, encr1, encr2, encr3, encr4, encr5, encr6, encr7, encr8, encr9, hhhhhh, Jim_system, jimboo, John Galt, New User, and Newsom. The 'OK' and 'Cancel' buttons are at the bottom.

Enter a Group name and description.

If Client Encryptors (Devices) have already been defined, they will be listed in the Client Encryptor box. Click the checkbox of each client encryptor you would like to add to the group.

Set IP Filters, if necessary. The IP Filter address ranges can be set for inclusion mode and exclusion mode.

Example: The IP address range with the starting address of 192.1.142 to the ending address of 192.168.1.199 is set for exclusion mode. Another IP Address range with the starting address of 192.168.1.168 to the ending address of 192.168.1.170 is set for inclusion mode.

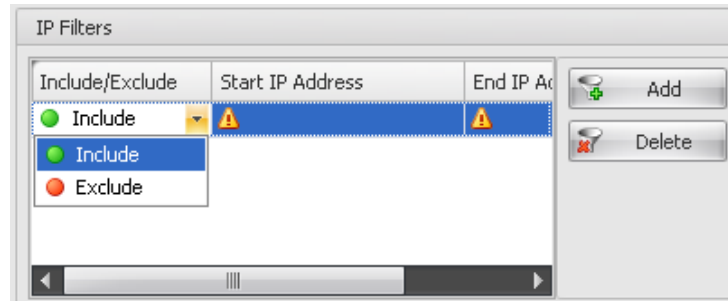
These IP address settings result in the following:

All IP addresses from 192.168.1.142 to 192.168.1.199 will have no access to the specified CDI Device with the exception of IP Address 192.168.1.168, 192.168.1.169, and 192.168.1.170.

To add an IP Filter, click the **Add** button. Select Include or Exclude from the drop down list.

Include: Defines an address range that can connect to the CDI device via IP and have full access to the device after user authentication.

Exclude: Defines an address range that will have no IP access to the CDI device.



Enter the Start IP Address and the End IP Address. Click **Add** to add another IP Filter.

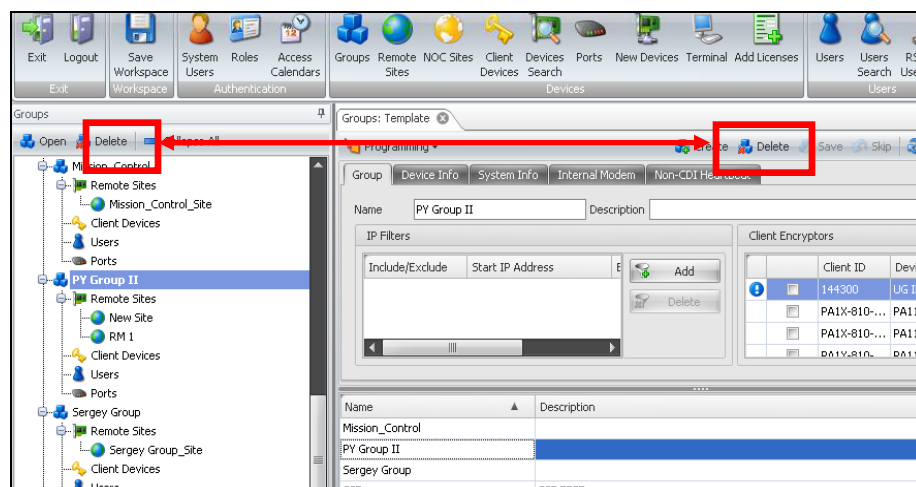
To delete an IP Filter, select the filter and click the **Delete** button.

Click the Save button for your changes to take effect or click Skip to discard them.

3.2.2 Deleting a Group

To remove a Group, select the Group in the Group tree or in the table. Check to make sure that the Group name is displayed in the Name field of the Group tab.

Click **Delete** in the Group Tree pane or **Delete** in Open Tabs pane. The Group, all Remote Sites, and all devices associated with the group will be removed. The Group name will be removed from the Group tree.



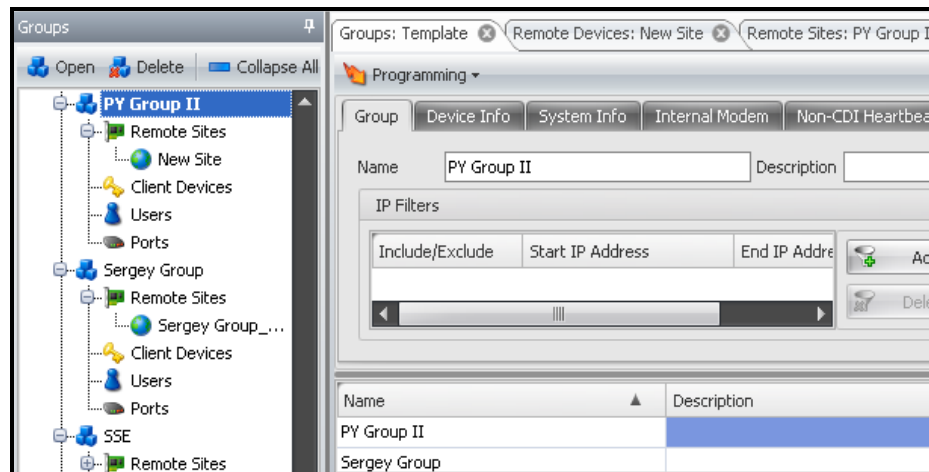
3.2.3 Renaming a Group

Open the Group template.

In the Group tree, select the Group whose name you want to change.

In the Name field, enter the new name. You may change the name in the Open Tabs pane or in the table below it.

Click **Save** to save the changes. Click **Skip** to discard the changes.



3.3 Remote Site Management

A Remote Site is a set of devices within a Group. Grouping multiple devices together by a common factor--for example, by location--makes it easier to view and manage multiple devices. A typical site may contain many NON-CDI devices and one CDI device. An example is an edge point with a Router, Firewall, Network Switch, and a PA155. All of these are added to the site and can be accessed and managed by the OBM.

A Group may have multiple Remote Sites, but a device may only belong to one remote group.

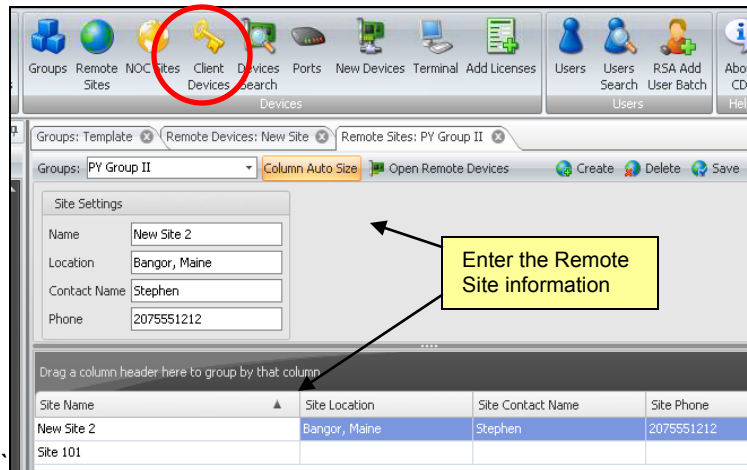
3.3.1 Adding a Remote Site

Click the **Remote Sites** button in the Security toolbar. The Remote Sites tab will open.

In the Group field, select the Group to which the Remote site will be added.

Enter the name, location, contact name, and phone for the contact person. You may enter this information in the open tab or in the table.

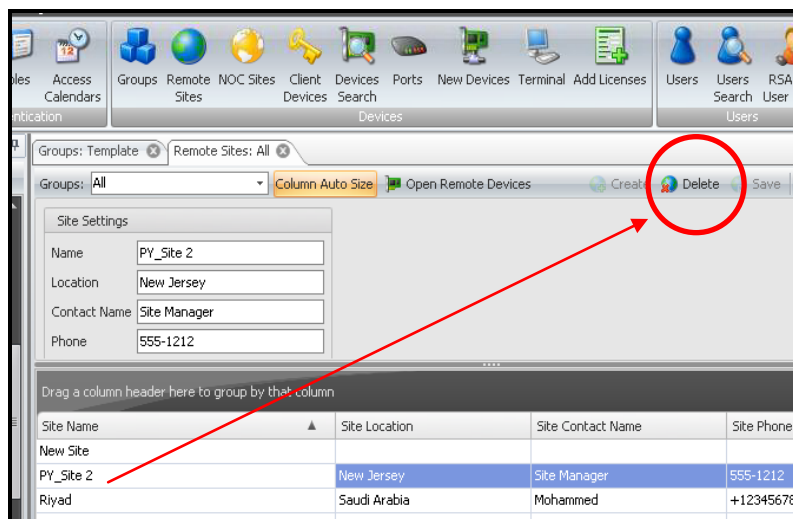
Click **Save** to save the changes. The new Remote Site will be displayed in the Group Tree pane. Click **Skip** to ignore the changes.



3.3.2 Removing a Remote Site

Click the **Remote Sites** button in the Security toolbar.

Select the site you wish to delete, and click the **Delete** button, in the top right corner of the Remote Sites page. When you remove a Remote Site, all the devices associated with the site will be removed.



3.3.3 Renaming a Remote Site

To rename a Remote Site, click **Remote Sites** in the Security toolbar.

In the Group list of the open tab view, select the Remote Site whose name you want to change.

Groups: Template Remote Sites: All

Groups: All Column Auto Size Open Remote Devices Create

Site Settings

Name PY_Site Two

Location New Jersey

Contact Name Site Manager

Phone 555-1212

Drag a column header here to group by that column

Site Name	Site Location	Site Contact Name
Mission_Control_Site	Mission_Control_Site	Mission_Control_Site
New Site		
PY_Site Two	New Jersey	Site Manager
Riyad	Saudi Arabia	Mohammed

In the Name field, enter the new name. You may change the name in the Open Tabs pane or in the table below it.

Click **Save** to save the changes. Click **Skip** to discard the changes.

Groups: Template Remote Devices: Group PY_Site

Groups: Group PY South Column Auto Size

Site Settings

Name PY_Site 2

Location New Jersey

Contact Name Site Manager

Phone 555-1212

Drag a column header here to group by that column

Site Name	Site Location	Site Contact Name
Group PY_Site	Group PY_Site	Group PY_Site
PY_Site 2	New Jersey	Site Manager

Enter the new name in Site Settings or in the information

4 WORKING WITH REMOTE DEVICES

This section describes how to.

- Add and remove devices from a remote site
- Configure a device
- Add a non-CDI device to a Remote Site
- Search for a Device
-

4.1 Remote Devices

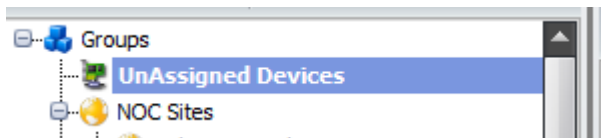
A remote device is a device in the field to which you will be connecting. Remote devices can be routers, firewalls, network switches, and CDI devices. All these devices can be access and managed via the OBM software A remote device can only belong to one Group, and only to one Remote Site within the Group.

4.1.1 Adding a Remote device

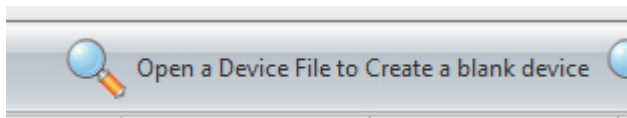
A new remote device can be added to a Remote Site of a Group. When a new device is created, the default parameters from the Group Template are applied. You may then open the Device Info and other tabs to add device-specific information.

New in Rev 6.04.00: The easiest way to add devices into the system is to use the provided Device Information File .DEV shipped with your units. If you cannot find the .DEV file contact CDI support and they can email them to you. support@commdevices.com or info@commdevices.com

Double click on the “Unassigned devices” at the top of the group tree



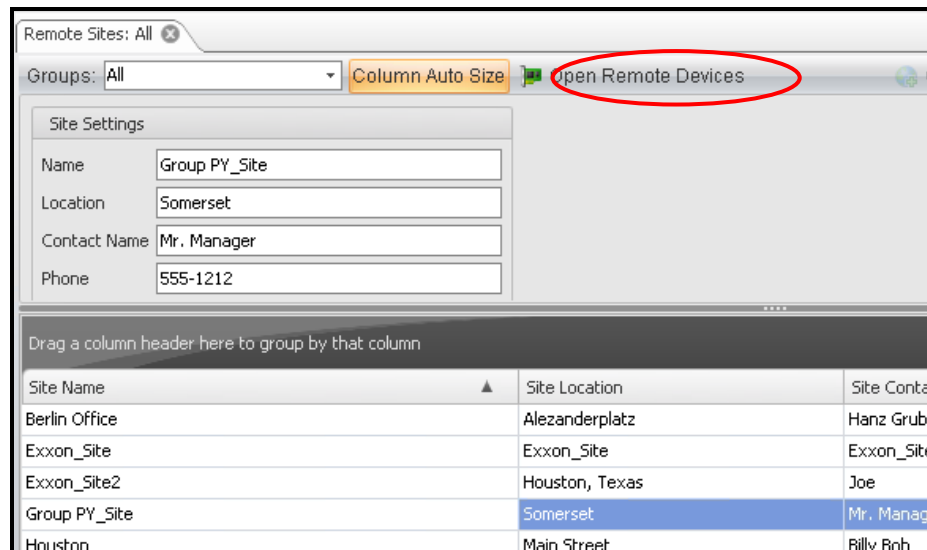
Click on the “Import Device Info File” tab on the right hand side.



Locate the .DEV file and import. This will bring one or many devices into the unassigned devices group. Now you can just drag and drop that device into an existing group or create a new group to drag it to.

The information below goes into detail about each editable field.

Click **Remote Sites** in the toolbar. The Remote Sites tab opens.



Select the Remote Site to which you want to add the device. The Remote Site name and other information about the site will be displayed in Site Settings.

Click **Open Remote Devices**. The Device Info tab is opened. To add a new device to the database, click **Create**. The Device Info tab displays "New Device" in the Name field. The default device type is displayed.

If you are adding a device of a different type, select the device type from the dropdown list.

Enter the device-specific information in the Device Info tab, System Options, and the remaining tabs. The tabs displayed depend on the device type.

The fields of each tab are described in subsequent sections.

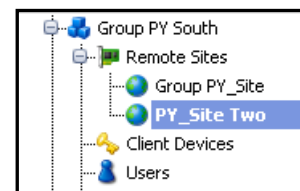
When you are finished, click Save to save your changes. Click Skip to discard them.

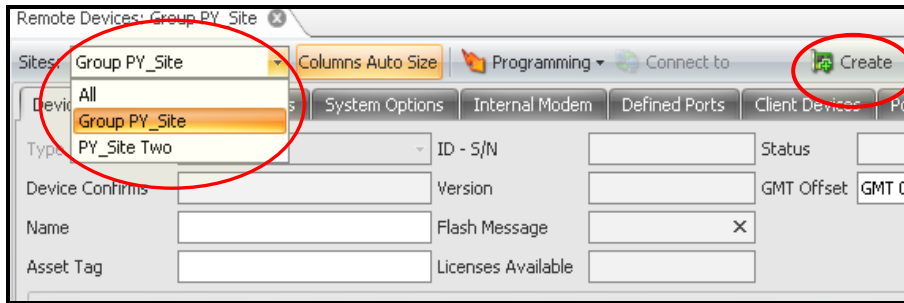
Alternatively, you may also add a device to a Remote Site by selecting the Remote Site from the Group List.

Click Remote Sites in the toolbar.

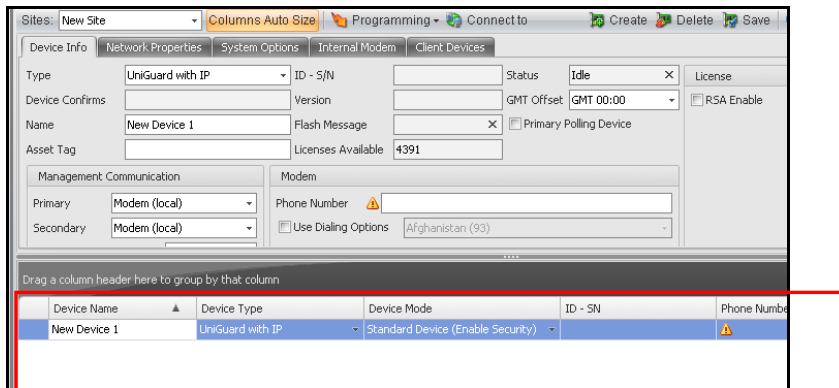
To add a remote device to a Remote Site of a Group, double-click the Remote Site name in the Group List. The Device Info tab opens.

Verify that the Remote site name to which you want to add the device is displayed in the Sites field. If it is not, select the site from the drop down menu.

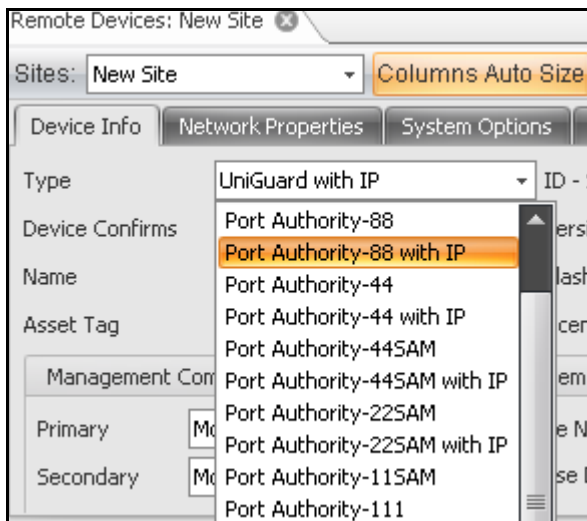




Click **Create**. The Device Info tab opens. A new device of the Default Device type will be listed in the Device panel.



To add a device of a different type, select the device type from the drop-down list.



Enter the device-specific information in the Device Info tab, System Options, and the remaining tabs. The tabs displayed depend on the device type. The fields of each tab are described in subsequent sections.

When you are finished, click **Save**.

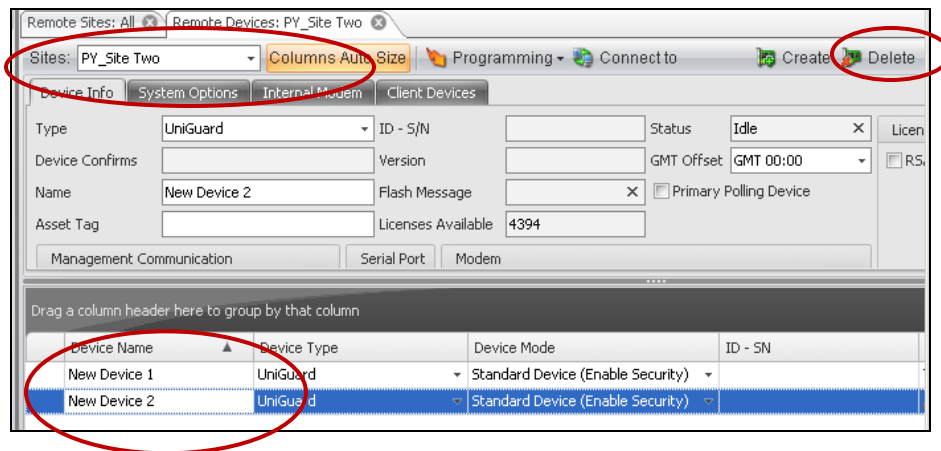
4.1.2 Removing a Device

A device may be removed from a Group.

To do this, select the remote site to which the device belongs.

Select the device.

After selecting the device, click **Delete**. You will be asked to confirm that you want to remove the selected device.



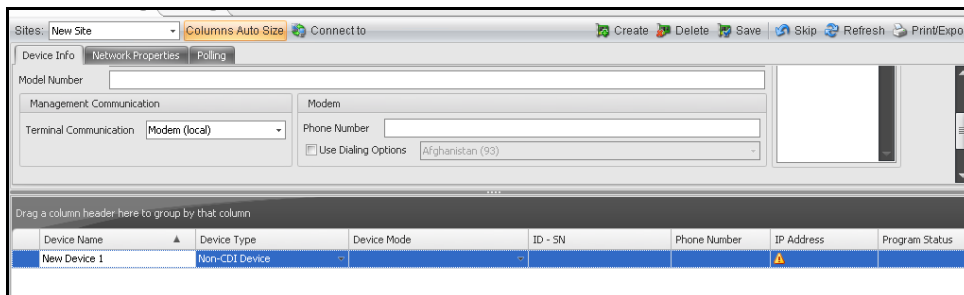
4.1.3 Modifying a Device's parameters

You may change information about a particular device. Select the Remote Site, and then the device. Open the appropriate tab or tabs, make the changes, and click Save.

4.1.4 Adding a Non-CDI device

A non-CDI device, such as a router, firewall, or network switch, can be added to the database for SSH access and/or periodic polling for activity.

To add a non-CDI device to a Group, follow the steps in section 4.1.1. Adding a Remote Device. For Device type, select "non-CDI" device.



Fill in the fields in the Device Info tab, network properties, and how you would like to access the device

SSH

Telnet

Browser

Dial up

Polling. In Polling, remember to enable polling by clicking the **Enable Polling** checkbox. The Polling feature pings the device at a given interval to make sure it is still online. This is equivalent to the “Heartbeat” feature of CDI devices.

Click **Save** to save your changes.

4.2 Device Info tab

The Device Info tab includes reference information about the device being added and defines the communication paths by which OBM will access the device.

The entries displayed are the default entries that you entered in the Group template. You may need to change these entries for the specific device that you are adding.

The screenshot shows a software window with a menu bar (Sites, Columns Auto Size, Programming, Connect to, Create, Delete, Save, Skip, Refresh, Print) and a tabbed interface. The 'Device Info' tab is selected. It contains several input fields and checkboxes. The 'Type' dropdown is set to 'Port Authority-111'. The 'Status' dropdown is set to 'Idle'. The 'License' section has checkboxes for 'RSA Enable', 'Network Enable' (checked), 'AES256 Enable', and 'SSH Enable'. The 'Management Communication' section has dropdowns for 'Primary', 'Secondary', and 'Terminal', all set to 'Network (direct)'. The 'Licenses Available' field shows '84'.

Device Type: Select the device type from the dropdown list. The default setting is UniGuard.

Device Confirms: For CDI, devices, the device type is entered by the system. This field is blank for non-CDI devices.

Name: Enter a device name.

Asset Tag: (Optional) Enter additional information to better define the device.

ID – S/N: Displays the device’s serial number retrieved by the OBM and added to the database

Version: The firmware version retrieved by the OBM and added to the database.

Flash Message: Displays the status of flash memory update.

Licenses Available: Displays the number of licenses available for the device.

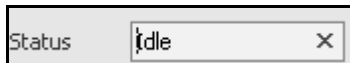
Status: Displays the connection status of the device.

 IDLE: Device is ready to connect to the OBM

 IN USE: Device is connected to the OBM

ALARM: Device is in the alarm state and cannot be connected to the OBM.

Tip: Clicking the X will return the message to IDLE but this is not necessary in normal operation. The device will automatically return to the idle state when it has completed the task.



You should only reset the message if the status hangs i.e. the device is IDLE but the OBM does not reset the device status to IDLE. Keep in mind that manually resetting the device by click the “X” only resets the status message. It does not cancel any running operations. In most cases, the device should be allowed to reset to IDLE on its own to avoid conflicts.

GMT Offset: If enabled, the GMT Offset will show the local time of the device’s location when audit information is displayed for this device.

GMT Offset will not automatically adjust for Daylight Savings Time. You will need to adjust the offset when coming in or out of Daylight Savings Time.

Primary Polling Device: If enabled, this device will be polled first when the Group is being polled. Each group can have one device that will be the primary device of Group.

Licenses The licenses listed depend on the device type. Click the appropriate boxes to assign licenses to the device. For example, you may have 100 devices, but only ten Network Enable licenses (because you only have ten on network devices). The checkboxes allow you to specify on which of your devices networking is enabled (and are thus using a network license).

Non_CDI devices do require an EDL-T (Terminal) license to be able to add them to the database. This is how the software is scaled for support purposes.

Note that these licenses can be purchased from CDI. For information on adding licenses to OBM, refer to the Adding Licenses section in this chapter.

- RSA Enable
- Network
- AES256
- SSH Enable
- Terminal Access (SSH access for non-CDI devices)

Management Connection

These fields determine the methods by which the OBM will communicate with the remote device, client device, and terminal.

Modem – A modem directly connected to the application through a serial connection (internal or external)

Network Direct – The software is connected directly to a network which will connect directly to the remote device (for example Telnet or SSH),

Serial Port – The remote device is connected directly to the serial port of the OBM software. This is used to “stage” equipment at a central location before shipping.

Client (Network Dial out) – The OBM software is connected to a network with several CDI Client devices (ex..PA111/PA222). The software will select a local client on the network through which to dial out to a remote device. The client will establish a hardware encrypted session with that remote.

Cellular Direct – if you have the MPLS network that is the same as the cell APN the devices connected to the system then you can communicate with them Cellular Direct. This means that the OBM just uses the Cell IP address and YOUR network can route directly to the cell device via a gateway to the APN network. Think of this as Network-Cell access.

Cell-Cell-Tunnel – The cell devices are normally on a private APN. This means that the cell devices cannot be reached from any other network EXCEPT the private APN (Access Point Name). Think of it as a VPN for the cell devices. One quick way to get onto the private APN is to use CDI Client devices with built in Cellular modules that are on that private APN. When the OBM wants to communicate with a remote device, it will first connect to a local CDI client via Ethernet, then jump onto the private APN via the cell module in the client, then route to the remote device on that private APN. The connection will be hardware encrypted from the client all the way to the remote. This is Cell to Cell private tunnel communications.

Cell-Network-Tunnel – This assumes that the remote CDI device's Ethernet port is on the cellular APN. When the OBM wants to communicate with a remote device, it will first connect to a local CDI client via Ethernet, then jump onto the private APN via the cell module in the client, then route to the remote device on that private APN. The remote device will have it's Ethernet port connected directly to the APN. The connection will be hardware encrypted from the client all the way to the remote.

Primary Communications: Specifies the primary method of accessing the device. Select from network, dial-up phone lines through a modem, GRPS, or through the serial port.

If Serial Port is selected; you will be prompted to enter the COM port number the OBM will use to communicate with this device.

If Modem or Client (Network Dial out) is selected, you will be prompted to enter the modem phone number and may choose to use dialing options of the OBM PC, the defined destination country code for the device, and the Phone number in the dialing process The Dialing options are set in System Settings, the Global Settings tab.

If Network (direct) or Cellular is selected, no additional information is required.

Secondary Communications: Specifies the communication path that will be used if the primary method is unavailable. The same communication paths are available for both primary and secondary communications. See *Primary Communications* for detailed information about communication path options.

Terminal Communication: The method by which OBM will communicate with a terminal. Several choices are available:

- Modem (local)
- Network Direct
- Serial Port

- Client Network Dialout
- Cellular Direct (require MPLS network accessible)
- Network Tunnel
- Network Cell Tunnel require MPLS network accessible)

Note: The Device Info tab for client devices only will include the Operation Communication field. For this field, select the communication mode to be used from the OBM to the client device before the client device dials out to a remote device. Available communication modes are AES encryption, telnet protocol, or SSH protocol.

4.3 Network Properties tab

The network proprieties tab defines properties such as IP addresses associated with the device, Syslog server, and attributes of the Syslog server, and OBM heartbeat.

The screenshot shows the 'Network Properties' tab in a configuration window. The 'Device Info' sub-tab is selected, displaying the following fields:

- Device IP Address: 192.168.0.170
- NAT Address: 192.168.0.170
- Subnet Mask: 255.255.255.0
- Gateway IP Address: (empty)
- Client PPP Address: (empty)
- Hardware Address: 00-90-2a-00-00-c5
- Port Number: 10001
- ☒ Use Default Port 10001

Other visible sections include 'SysLog Server', 'DNS Attributes', 'SNMP Attributes', and 'Radius Server'.

Device IP Address: IP address of the device

NAT Address: Normally this is the same as the Device IP address. The purpose of this address is to allow devices of an internal network to be identified by one IP address when routed to a different network.

Subnet Mask: The Subnet Mask determines to which subnet an IP address belongs by filtering with this bit pattern. If your host PC is using the wrong subnet mask, it may not be possible to correctly identify all users on that subnet and many users may be unreachable by your computer. The subnet mask is defaulted to work with an 8-bit host address. For any other host bit address, you must change the subnet mask to the proper setting.

Gateway IP Address (Optional) : The router/gateway address that allows you access to other network segments. This address must be within the local network.

Client PPP Address (Optional): The address of the host to which the CDI device will send a request to establish a PPP session.

Use Default Port 10001: Click to enable the OBM to use of the device default port for programming.

Port No: The port number used to communicate from the Network side “ex. Telnet Port Number.

Hardware Address: Only required if the device will not be programmed through a modem/dial-up connection, otherwise the OBM will automatically receive it via serial or telco communications.

If the initial programming is through the network, then the hardware address is required.

The screenshot shows the OBM configuration interface with the 'System Options' tab selected. The 'SysLog Server' section is expanded, showing the following settings:

- SysLog Server:**
 - Primary IP Address: 192.168.0.002
 - Secondary IP Address: 192.168.0.002
- OBM RealTimeLog:**
 - ☒ Enable RealTime Log
 - RealTime Log Address: 192.168.0.2
- OBM Heartbeat Attributes:**
 - ☒ Enable Heartbeat Attributes
 - Max No. of Missed Heartbeats: 3
 - HB Message Interval (minutes): 30

The background interface shows other configuration options like Device Info, Network Properties, and DNS Attributes.

Syslog Server

If a Syslog Server application is running on your network, CDI devices can report audit trail messages to the Syslog Server for monitoring purposes.

Note: To view the Syslog log, click Syslog in the Logs toolbar.

Primary IP Address: Enter the primary address of the Application Server that is handling Syslog traffic. You may then enter the Syslog IP port number that the CDI device can use for communication.

Secondary IP Address: Enter an address that will be used when the primary IP address is not available. You may then enter the Syslog IP port number that the CDI device can use for communication.

OBM RealTime Log

Enable RealTime Log: RealTime logs (RTL) allow real-time messages from remote CDI devices to be sent via the network connection to the OBM server. Without RTL enabled the remote devices will not send events in real time back to the server, they will be buffer until the unit is polled (which will need to be enabled). RTL must be enabled in order to generate alarms from missed heartbeats.

RealTime Log Address: IP address of the OBM workstation that is enabled for Real Time logs.

OBM Heartbeat Attributes

The OBM Heartbeat is an automatic "I'm alive" message that is sent periodically by a CDI remote device to the OBM application server. If heartbeat messages or any other messages are not received by the OBM application server within the given time interval, an alarm (No Contact From Device) will be triggered for this device. This would indicate that the device is in trouble or its network access is in trouble.

The Heartbeat also checks the “Telco Line Status”. The modem will go “off hook” and check for Dial Tone during each Heartbeat interval. The device will report that status of the Telco line as part of the Heartbeat response. This allows the central site to realize that a remote site has no working telco connection long before it is going to be used. If the Telco line is restored, this is also reported in the Heartbeat message. The OBM can pass this alarm to an SNMP manager, an Email Alert, or a SMS text message.

For non-CDI devices, this is accomplished using Polling. The Polling feature pings the device at a specified interval to check if it is still available and online.

Max No. Of Missed Heartbeats: Number of missed heartbeats that will trigger an alarm from the OBM workstation that is set for real time logs. The default is three to allow for latency and/or collisions in a network

Heartbeat Message Interval: The time in minutes between heartbeats sent by the remote device. For example, an interval of 60 would generate a heartbeat once an hour by the remote device. This interval would be programmed into the device.

Example: If the Maximum Number of Missed heartbeats is set to three beats and the Heartbeat Message Interval to 60 minutes, a “No Contact From Device” error is generated by the OBM each time the device does not respond with 180 minutes (3 x 60).

Note: In order to receive heartbeat messages or alarms, OBM RealTime logs must enabled. If real-time logs are not enabled, no heartbeat messages will be received even though the heartbeat attributes have been defined. OBM Real Time logs are enabled in Common System Settings tab.

The screenshot shows the OBM configuration interface with the 'DNS Attributes' dialog box open. The background window has tabs for 'Device Info', 'Network Properties', 'System Options', 'Internal Modem', 'Defined Ports', and 'Client Devices'. The 'System Options' tab is active, showing fields for 'SysLog Server', 'DNS Attributes', and 'Radius Server'. The 'DNS Attributes' dialog box has the following fields:

- DNS Attributes:**
 - DNS Server Address: [Empty]
 - Domain Name: [Empty]
- SNMP Attributes:**
 - Community Name: public
 - Primary IP Address: 192.168.0.039 : 162
 - Secondary IP Address: [Empty] : [Empty]

The background window also shows fields for 'Device IP Address' (192.168.0.0170), 'NAT Address' (192.168.0.0170), 'Subnet Mask' (255.255.255.000), 'Gateway IP Address', 'Client PPP Address', 'Hardware Address' (00-90-2a-00-00-c5), 'Port Number' (10001), and 'Use Default Port 10001' (checked). The 'SysLog Server' section has 'Primary IP Address' (192.168.0.035), 'Secondary IP Address' (192.168.0.034), 'OBM RealTimeLog' (checked), 'Enable RealTime Log' (checked), and 'RealTime Log Address' (192.168.0.2). The 'OBM Heartbeat Attributes' section has 'Enable Heartbeat Attributes' (checked), 'Max No. of Missed Heartbeats' (3), and 'HB Message Interval (minutes)' (30).

DNS Attributes

DNS Server Address: Enter the DNS server IP address. This is only needed if you want to use a DNS server that is different from the one used by your network’s routers.

Domain Name: Enter the Domain name. This is only needed if you are not using the DNS server used by your network’s routers.

SNMP Attributes

Community Name: The Community string (“password”) that the first trap receiver uses to validate traps.

Primary IP Address: IP Address of the first SNMP Trap Receiver to which you want the traps sent.

Secondary IP Address: IP Address of the optional second SNMP Trap Receiver to which you want the traps sent.

The screenshot shows the 'Network Properties' window with several tabs: 'Device Info', 'Network Properties', 'System Options', 'Internal Modem', 'Defined Ports', and 'Client Devices'. The 'Network Properties' tab is active, displaying fields for Device IP Address, NAT Address, Subnet Mask, Gateway IP Address, Client PPP Address, Hardware Address, and Port Number. A 'SysLog Server' section includes fields for Primary and Secondary IP Addresses and Port Numbers, with checkboxes for 'Enable RealTime Log' and 'Enable Heartbeat Attributes'. A 'DNS Attributes' section includes fields for DNS Server Address and Domain Name. A 'Radius Server' section includes fields for Primary and Secondary IP Addresses and a Radius Key. A 'SNMP Attributes' section includes fields for Community Name, Primary and Secondary IP Addresses, and Port Numbers. A 'Radius Server' dialog box is open, showing fields for Primary IP Address, Secondary IP Address, and Radius Key.

Radius Server

Primary IP Address: Enter the Radius IP Address of the Radius server.

Secondary IP Address: Enter an IP address to be used fir the Primary IP address is not available.

Radius Key Optional: Enter the Radius Key. A maximum of 128 characters can be entered.

4.4 Cellular Module Properties

The parameters for the Cellular Modules are found in the NETWORK PROPERTIES tab. Fist the Cellular Module needs to be enabled in the INTERNAL MODEM tab. Then all properties are set in the network properties tab.

The screenshot shows the 'Cellular properties' window. It includes fields for Cellular IP Address, Cellular Modem Text Number, APN-Access Point Name, User Name, and Password. A 'Cellular SysLog Server' section includes fields for IP Address and Port Number, with checkboxes for 'Enable Cellular OBM Address' and 'Enable Cellular RealTimeLogs'. A 'Cellular SNMP Attributes' section includes fields for Community Name and IP Address. A 'Cellular OBM RealTimeLogs/Heartbeat Attributes' section includes checkboxes for 'Enable Cellular OBM Address' and 'Enable Cellular RealTimeLogs', and fields for OBM Address, Max No. of Missed Heartbeats, and HB Message Interval (minutes). A 'Number of Antennas' dropdown menu is set to 'One Antenna'.

Cellular IP Address – This is the address assigned to the Cellular Module by the Carrier. It is a fixed IP address. This address can be entered into the OBM if you are reaching out via cell to program the remote device. Or if you are programming locally via serial or network, it will be pulled from the device.

Note: the device must connect to the network BEFORE it can pull its IP address from the Carrier.

Cellular Modem Text Number: This is a future function at this point. This number is used to send commands via SMS message to the remote device.

APN-Access Point Name: The APN is required by certain carriers to provide a private network connection. This information should be provided by your carrier. It is also pulled out of the device if it is programmed via any other connection than the cellular.

User Name: Optional for APN access on most carriers.

Password: Optional for APN access on most carriers.

Cell CCID/ESN Number: This will be pulled out of the device when programmed. It is basically the serial number of the cellular module.

Number of antennas: Device is shipped with one antenna. If an Diversity antenna is used please select 2 in this window as the cellular module needs to be told how many antennas are being used.

Cellular Syslog Server: This can be a syslog server connected directly to the APN network, or it can be a CDI Cellular Client address that will relay the syslog data to the network syslog server.

Cellular SNMP Attributes: This can be an SNMP server connected directly to the APN network, or it can be a CDI Cellular Client address that will relay the SNMP data to the network SNMP server.

Cellular OBM Real Time Log/Heartbeat Attributes – This can be an OBM connected directly to the APN or a CDI Cellular Client IP address that will in turn relay the data to a network connected OBM server.

4.5 System Options

The parameters on this screen enable you to set user security levels, system password and key information, and first message delay time. The parameters displayed may vary depending on the device.

The screenshot shows the 'System Options' tab in a software interface. The top navigation bar includes tabs for 'Device Info', 'Network Properties', 'System Options', 'Internal Modem', 'Defined Ports', and 'Client Devices'. The 'System Options' section contains the following fields and controls:

- AES Mode:** A group box containing three checkboxes: 'AES128' (unchecked), 'AES192' (unchecked), and 'AES256' (checked).
- Device Mode:** A dropdown menu set to 'Standard Device (Enable Security)'.
- Network Access to Modem:** A dropdown menu set to 'Disabled'.
- Encryption Engine Version:** A text field containing '4.00'.
- System Key:** A sub-section containing:
 - Sys Password:** A text field with masked characters '*****' and an information icon.
 - Sys Key:** A text field with masked characters '*****' and an information icon, followed by a 'Generate Key' button.
 - Sys Key Signature:** A text field containing the hexadecimal string '474B9FE187B22555474B9FE187B22555474B9FE187B22555'.
- First Message Delay (secs):** A spin box set to '5'.
- Host DTR/RTS Loss of Signal (secs):** A spin box set to '5'.
- Disable IP Authentication Encryption:** An unchecked checkbox.

AES Mode or TDES mode or AES/TDES mode: The encryption modes displayed depend on the device.

Device Mode: Select the security type. The available types are listed below:

- Standard Device (Enable Security). Default
- Device Authentication/Encryption – this device will only communicate with CDI Clients in an encrypted mode. The device will automatically attempt to exchange a key once a connection has been established. The user will not be prompted for a userID.
- RSA SecurID Device. The device will act like a legacy RSA SecurID device. This is a mode created specifically to mimic a latency SecurID device and is only recommended for applications requiring strict legacy compatibility. The boarder use is for an RSA token to be used in the encryption mode or the standard mode with RSA enabled.
- Standard Device (Bypass Security): Security is disabled for this device.

Network Access to Modem: Select the option for network access to the modem. When this option is enabled, you can access the modem and dial out from the network. This can be a security concern because the modem is enabling this will make the modem available for dial out from the network.

- Disabled
- Enabled /No Encryption
- Enabled / Encryption

System Key

Sys Password: This is the password used by OBM to access the device. Enter a password by the OBM to access and program the device. If asterisks are displayed, a password already exists. You may change the password by deleting the current one and entering a new one. For security purposes, the password will be displayed as asterisks.

Sys Key: This is the key used by OBM to access and encrypt data with the device.. By using the sys key, communication between the OBM and the device encrypted. The system key must have 48 hex characters. The Sys Key may be entered or system-generated. To have the system generate it, click Generate.

First Message Delay Time (sec): This is a delay before the first message is displayed upon connection. Enter the time in seconds until the “Enter User ID” prompt is displayed.

Host DTR / RTS Loss of Signal: Sets the number of seconds that the host signals have been lost before an alarm is generated and sent back to the OBM. A loss of signal from the host device can signify the device is in trouble, a loss of power, or a cable being removed from the device. The connection to the host has been lost

Applies only to Port Authority devices

Disable IP Authentication Encryptor: Click the checkbox to enable this feature. When enabled, encryption is disabled after successfully authenticating to the device via IP communication.

Applies only to UniGuard devices

Power/IP Port Option: Select the mode for the power port/ip port. The available modes are listed below.

- Program Only – Port used for serial programming only
- Power port connection – Port used to control a PCM only
- IP\Authentication – The UniGuard has an network port instead of a serial maintenance
- Network dial out – The port is a network port and is used for network dialout in the Client mode.

Host DTR: This option monitors or ignores the DTR (Data Terminal Ready) signal from the Host port of the UniGuard. The default is Monitor. Note that when the host drops DTR during a modem connection, the connection will drop. This is standard for the RS232 interface.

Host Dialout: Set whether the host can dial out using the device's modem

- Enable: Allows the host to dial out using the device's internal modem
- Disable: Prevents the host from dialing out using the device's internal modem
- Device Authenticate: When Device authentication has been selected and a connection is made, the device will immediately attempt to exchange a key with whatever is on the other end prior to even asking for a user ID. This is mainly used in machine to machine connections or when a central RADIUS authentication is used prior to allowing dial out from the NOC.

Host "AT" Command Access; (Only UniGuards in the AT Command State)
Enables the Host to access the modem in the AT Command State. This is used primarily when the connected device needs to interact with a modem for the application to run and is normally in legacy applications.

4.6 Analog Internal Modem

The fields of the Communications screen enable you to define modem/host port parameters of the UniGuard and the modem port of the Port Authority. If you select CELLULAR MODULE, all the parameters will be inserted in the network properties tab.

4.6.1 Internal Modem Type:

Select either Analog or Cellular as the internal modem type. If Cellular is selected, the device needs to have a Cellular module installed and it's parameters are set in the network properties tab.

Extra AT Command Settings

Modem Type:

4.6.2 Modem Inactivity timer (min):

Specify the number of minutes of no activity detected by the modem before the modem disconnects.

Enter 0 to disable this feature.

4.6.3 Serial AT Commands:

Click the checkbox to program the AT command into the modem. You do not have to enter an AT in the front of command string and do not include spaces or delimiters between commands.

Modem

4.6.4 Modem Port Bits/Parity:

Select the modem port bits and parity from the drop down list.

4.6.5 Modem Port Baud Rate:

Select the baud rate of the modem port from the drop down list.

4.6.6 Defined Messages

User-defined messages can be sent out either before or after the authentication process begins.

4.6.7 Primary:

Enter a user-defined message sent before the authentication process starts. This is typically "Welcome to XYZ Company

only valid users should be using this system”, and may be followed by additional legal warnings.

4.6.8 Secondary:

A user-defined message sent after the first user authentication prompt response has been processed. This is typically “we really meant what we said in the first message and will prosecute any trespassers” followed by the appropriate legal warnings.

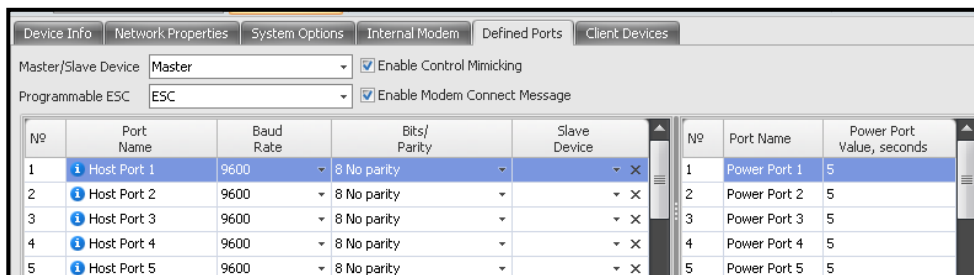
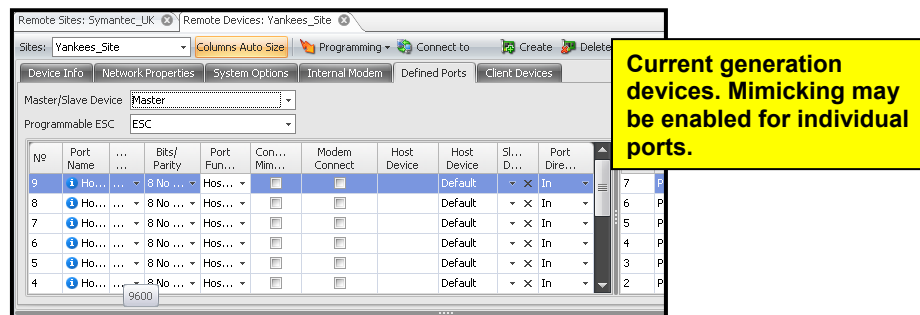
4.7 Cellular Internal Modem

All Cellular module properties are found in the Network Properties Tab as it is network based communications

4.8 Defined Ports

The parameters in the Defined Ports tab enable you to set communication parameters for the Host and Power ports of the Port Authority and Port Authority SAM. Defined Ports is not available for the UniGuard device since it is a single-port device.

NOTE: For the current generation of devices, you may enable and disable Mimicking and the Modem Connect message for individual ports. For previous generation devices, ports may not be set individually.



Master/Save Device: A Port Authority device can be defined as Master or Slave. This will allow the host ports of a Master Port Authority to connect to the Maintenance port of a Slave Port Authority. Using the Master/Slave function can expand the Port Authority up to 64 ports.

The number of Ports available in a Master/Slave connection is equal to the Number of Port Authorities multiplied by 8, minus the number of Slave units.

A diagram showing an example of Port Authority Master-Slave cable connections is shown in Appendix 1

Programmable ESC: Select the character that a user presses to exit a port.

After accessing and modifying a host or power port of a Port Authority device, a user exits the port by entering the esc character. The user may then access a different host or power port.

If the ESC character interferes with other functions of the host application, the user may need to use a different character. The Programmable ESC code option allows the user to change the ESC code from one character to another. The default esc character will be changed and the new ESC code character will be installed after the DDM has programmed the Port Authority device.

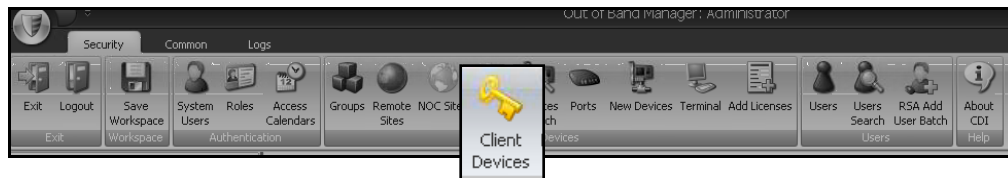
Programmable ESC Combo list functionality is only for Port Authority devices with firmware at or above 3.05.xx.

Enable Control Mimicking: Mimicking will allow the Host port of the Port Authority to copy the control signals of the Dial-In modem port. The default setting is “Disabled.” This is the recommended setting

Enable Modem Connect Message: The Modem Connect message may be enabled or disabled. If enabled the modem connect message is sent to the Host Port. . The default setting is “Disabled.” This is the recommended setting.

4.9 Client Devices

To view a list of client devices by Group, click Client Devices in the toolbar.



Client devices are all located in the NOC site(s). Groups can be assigned to these client devices to establish an encrypted session between the NOC site and the remote device. Groups not using hardware encryption do not need to be assigned to client encryptors.

When the Client Devices tab is opened, a list of client devices associated with the group is displayed. For each client device, the device name, client ID, device type, device mode, ID and Serial Number, Phone number, IP address, and Program status are listed.

Client Devices: Yankees

Groups: Yankees Columns Auto Size Programming Connect to Refresh

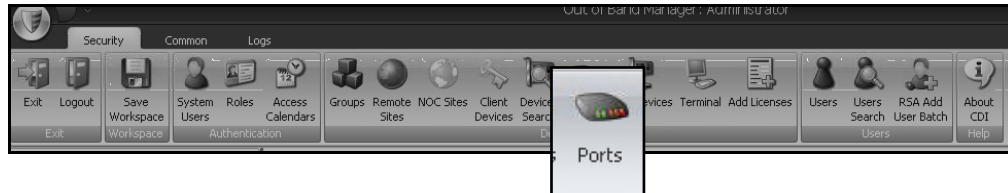
Drag a column header here to group by that column

Device Name	Client ID	Device Type	Device Mode	ID - SN	Phone Number	IP Address	Program St...
PA111 Client 176	PA11-111-100005	Port Authority-111	Client Device	PA11-111-100005	117	192.168.000.176	No Contact Fr...
PA111 Client 177	PA11-811-100015	Port Authority-111	Client Device	PA11-811-100015	117	192.168.000.177	No Contact Fr...
UGRD Client N178	812759	UniGuard with IP	Client Device	UGMO-A20-812759	118	192.168.000.178	No Contact Fr...

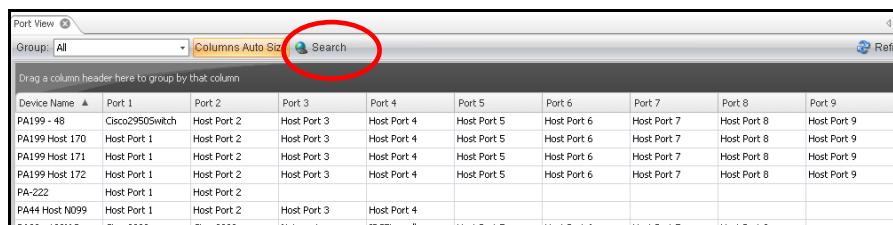
For information on connecting to a particular device, please refer to the Communication Center section.

4.10 Ports View

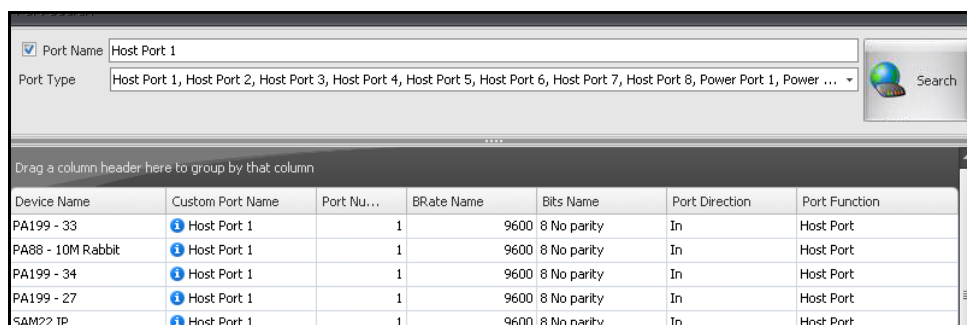
The Ports View displays what is connected to each port of all devices of all Groups, to all devices of a one group, or to a specific port or port type.. To display the Ports View, click **Ports** in the toolbar.



The Port View tab is opened. From the Groups drop down list, select a specific group, or **All** to view all devices of all groups.



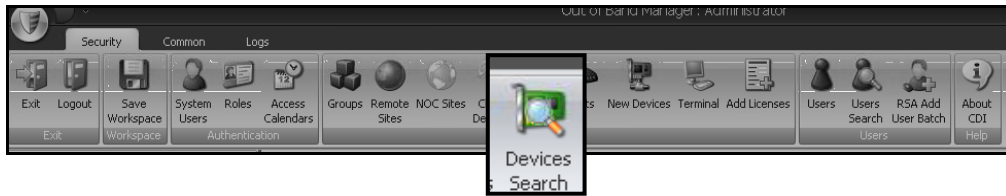
To view detailed information about a specific port or port type, including the Baud Rate, Bits Name, Port Direction and Port Function, click **Search**. The Port Search screen is displayed.



To view the port connections of a specific port or port type, enter the search criteria and then click **Search**. The results of your search will be displayed.

4.11 Device Search

You can search for a device by name, device type, hardware address, asset or IP address. To do this, click Devices Search in the toolbar.



4.11.1 Displaying a list of all Devices

To display a list of all devices, do not enter any search criteria.

4.11.2 Displaying a list of Specific Devices

Open the Device Search tab. Enter the search criteria and click **Search**. You can search by Device Name, Device Type, Hard Address, Device Asset, Device IP Address, or a combination of these. Your search can be limited to those devices not contacted or to only client devices.

The results of the search are displayed in the Device pane. Click on a column heading to sort by that column.

Device Name	Device Type	Device Mode	Groups	Site Name	Version	Phone Number	IP Address	Asset	Hard A...
PARemote164	Port Authority-44 with IP	RSA SecurID Device	Jim Gro...	Jim Group ...	4.13.11	128	192.168.000...	00-03-F4...	
PA_RABIT	Port Authority-44 with IP	Standard Device (Enab...	Legacy	Legacy_Site	4.13.11		192.168.000.151	00-90-C2...	
PORT44DES	Port Authority-44 with IP	Standard Device (Enab...	Sergey ...	Sergey Gro...	3.14.00	124	192.168.000.144	00-90-C2...	
PA44164	Port Authority-44 with IP	Client Device	Jim Gro...	Default NOC...	4.13.14		192.168.000...	00-03-F4...	
PA88 Host N173	Port Authority-88 with IP	RSA SecurID Device	Yankees	Yankees_Site	4.13.15	119	192.168.000.173	00-03-F4...	
PA155_Houston	Port Authority-155	Standard Device (Enab...	Exxon	Exxon_Site2			192.168.000.201		
BlunderOffice	Non-CDI Device		Exxon	Exxon_Site			192.168.000.004		

4.12 Adding Licenses

Each device added to the OBM must have a license; this is how the software is scaled. There are several types of licenses that may be uploaded.

Device licenses: Apply to all CDI legacy devices . (UniGuard, PA44, PA84, PA88, SAM11, SAM22, SAM44)

RSA Licenses: These licenses are used to enable any CDI device to use RSA tokens for authentication.

OBM / Seat Licenses: Allow multiple current instances of an OBM client to be used. Each simultaneous connection to the database requires a seat license. This number should be at least equal to the number of client encryptors if encryption is being used.

Enhanced Device Licenses (EDL) apply only to PA100 and PA200 series products. (Port Authority 111, 155, 199, 211, 222, 244). These EDLs allow management and additional functionality to the devices.

To upload a license, click **Add Licenses** and select the license type from the drop down list. Select the file name and click **Open**.

Note: You can view the number of used and available licenses in Common System Settings tab. To open this tab, click Common. From the toolbar click System Settings, and then the Common System Settings tab.

5 MANAGING CLIENT DEVICES

This section explains how to manage client devices. A client device is a CDI device that is used to connect to another remote CDI device when a session must be encrypted. Client devices may also be referred to as client encryptors.

All client devices are in the NOC Group. Each client device may then be attached to one or more Groups.

This section explains how to do the following:

Add and configure the Port Authority, SAM, UniGuard, SSE Client devices as client devices.

Attach and detach client devices from Groups.

View a list of client devices that are attached to a Group.

5.1 NOC Group

The NOC Group is a system-created Group to which all client devices are added. Click NOC Sites in the toolbar to:

Add or delete a NOC remote site

Create a Client Device

Create a SSE Device

Program a client device

Connect to a client NOC Device

Attach a NOC device to a Group

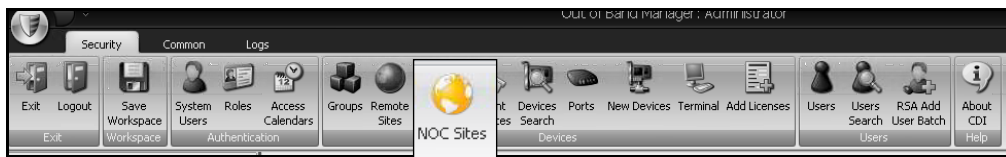
The Default NOC Site within the NOC Group is generated by the system and may not be renamed or deleted. User-created NOC sites may be renamed or deleted as required.

Client devices are added to the NOC Sites Group. Once it has been added to the NOC Sites Group, the client device may be attached to one or more Groups.

5.1.1 Viewing All Client Devices

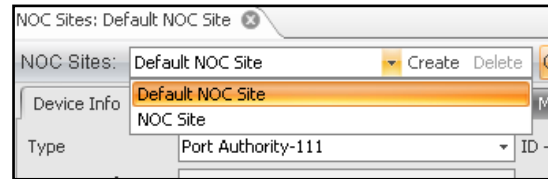
You may view all client devices in the NOC Group, or the client devices of one remote site within the NOC Group.

To view all the client devices, click NOC Sites in the toolbar.



The NOC Sites tab opens for a NOC remote group. In the Open View portion of the screen, a list of client devices is displayed.

To view the client devices of a NOC remote site, select the site from the drop down list of the NOC Sites field.



drag a column header here to group by that column

Device Name	Client ID	Device Type	Device Mode	ID - SN	Phone Number	IP Address	Program Status	Groups
chevron client	000000	Port Authority-111	Client Device			123.123.123.105	No Contact From ...	Chevron
PA - 111 - 161	PA11-910-000046	Port Authority-111	Client Device	PA11-910-000046		192.168.0.161		Jim Group
PA111 - 20	PA11-810-000020	Port Authority-111	Client Device	PA11-810-000020	101	192.168.0.120		Exxon
PA111 - 22	PA1X-810-000022	Port Authority-111	Client Device	PA1X-810-000022	103	192.168.0.122		Exxon, Jim ...
PA111 - 23	PA1X-810-000023	Port Authority-111	Client Device	PA1X-810-000023	104	192.168.0.123		Exxon, Jim ...

For each Client Device, the following information is displayed:

Device Name

Client ID

Device Mode

ID-SN

Phone Number

IP Address

Program Status

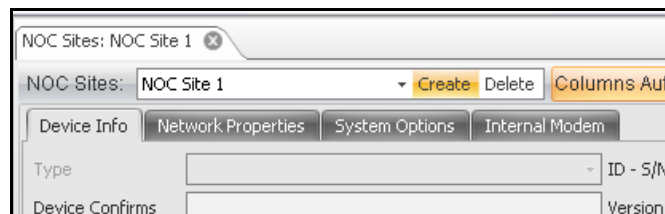
Groups

5.1.2 Adding a site to the NOC Sites Group

The Default NOC Site has been generated by the system. This site cannot be deleted or renamed. You may, however, create additional sites.

To add a NOC Site, click NOC Sites in the toolbar. A NOC site will be created with a default name (NOC Site #). You may change the name. .

Client devices may be added to the Default NOC Site or to a NOC site that you created. To do this, click Create and select either a Client Device or an SSE device to be created. Port Authority and UniGuard devices may be added as client devices.



5.1.3 Deleting a NOC Site

NOC sites that you added may be deleted. To delete a NOC site, make sure the site name is displayed in the NOC Sites field.

Click **Delete**. All devices associated with the NOC site will also be deleted.

Note: The Default NOC site is system-created and cannot be deleted.

5.2 View the Client Devices of a Group

Client Devices in the toolbar displays a list of client devices attached to a particular group.

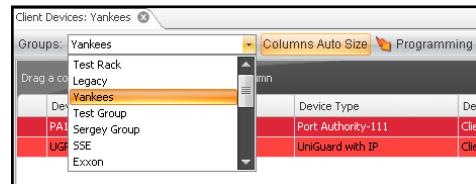
Note: To program a device, select the device and then click the appropriate programming option.



Select the Group from the dropdown list

A list of client devices attached to the group is displayed.

For each device, the following information is displayed:



Device name

Client ID

Device Type

Device Mode

ID-SN

Phone Number

IP Address

Program Status

Client Devices: Yankees

Groups: Yankees Columns Auto Size Programming Connect to Refresh

Drag a column header here to group by that column

Device Name	Client ID	Device Type	Device Mode	ID - SN	Phone Number	IP Address	Program Sta...
PA111 Client 176	PA111-111-100005	Port Authority-111	Client Device	PA111-111-100005	117	192.168.0.176	No Contact Fro...
UGRD Client N178	812759	UniGuard with IP	Client Device	UGMO-A20-812759	118	192.168.0.178	No Contact Fro...

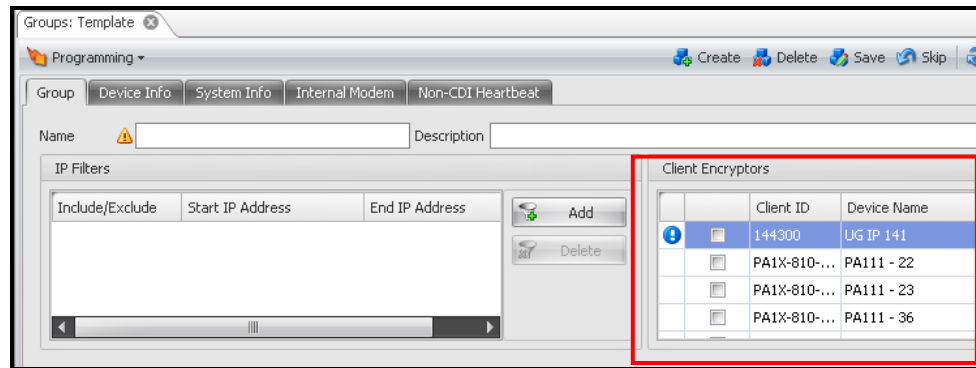
5.3 Attaching a Client Device to a Group

A client device may be attached or detached from a group from the Group Template or from the NOC Sites tab.

5.3.1 Attaching a Client Device from the Group Template

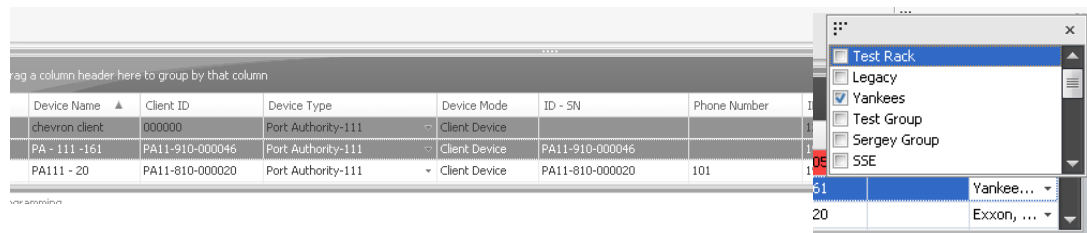
To attach a client device to a Group from the Group Template, display the Group template for the group.

The Client Encryptors displays a list of all client devices that have been added to the NOC Sites Group. To attach a client device to the group, click the checkbox. A client device may be attached to more than one Group. To remove an client device from a Group, uncheck the box.



5.3.2 Attaching a Client Device from NOC Sites tab

To attach a client device to a Group from the NOC sites tab, locate the device in the list. In the Group column of the selected device, click the down arrow. A list of Groups is displayed. Click the checkbox of each Group you would like to attach to the device.



5.4 Adding an SSE Device

The SSE (Secure Session Encryptor – CDI USB Token) acts as a client encryptor and includes a unique 6-digit ID. The SSE Triple DES/AES key can only be programmed by the OBM. Through the OBM, remote users can securely connect to CDI devices via Trip DES/AES communications using the SSE.

The SSE is installed by attaching one end of the included USB cable to a USB port of the PC. The other end is connected to the SSE hardware device. A device license is required for the SSE hardware device to be managed by the OBM.

To add an SSE Client to the NOC Sites Group, click **Create**. From the drop down list, select SSE Client. The SSE Client tab is opened.

IOC Sites: Default NOC Site

NOC Sites: Default NOC Site Create Delete Columns Auto Size Programming Connect to Create Delete Save Skip Refresh

SSE Client

Device Info Client Info Description

Device Info

Device Name New Device 2 Status Idle ...

Device S/N SSE ID 000000

SSE Version Unlock / Lock SSE UnLock

Minimum Pin Length 4 ☒ Requires Pin Validation

SSE Licenses Available 56 ☒ Requires New Pin

Client Info

AES/TDES Mode AES128

Key 9850868073928BEEEECD94C8E9E756171DC16C9EDCCB900A

Key Signature BCD0960F6FF628EF9B4EAB4A40E136A8254442FC93E0D20ACE9

Communication

Communication Type Modem Dial Out

Use Dialing Options Country Region Afghanistan (93)

Dialout Modem Number

The Device Info fields enable you to enter information about the SSE device.

Device Name: The name given to the device by the user.

Device S/N: The serial number will be provided by the OBM.

SSE Version: Provided by the OBM

Minimum Pin Length: The least number of characters that may be entered for the pin. The range is from 4 to 12 characters.

SSE Licenses Available: Provided by the OBM

Status: The status of the device. Provided by the OBM.

SSE ID: The Client ID of the SSE. Provided by the OBM.

Unlock / Lock SSE: The SSE can be unlocked or locked (default is unlocked).

After a consecutive number of failed logon attempts, the SSE is put into a locked state. When locked, the SSE device cannot do encryption. Once locked, the SSE must be unlocked before logons can be attempted. When unlocked the SSE is put in new pin mode.

Note: To set the number of failed logon attempts before the SSE is put into a locked state is set in System Settings, Global System Settings tab.

Requires Pin Validation: If enabled (default is enabled), the user must enter a pin to logon to the SSE device.

Requires New Pin: If enabled (default is enabled), the user must enter a pin to logon to the SSE device.

The Client Info fields specify the encryption mode and communication type.

IOC Sites: Default NOC Site

NOC Sites: Default NOC Site Create Delete Columns Auto Size Programming Connect to Create Delete Save Skip Refresh

SSE Client

Device Info Client Info Description

Device Info

Device Name New Device 2 Status Idle ...

Device S/N SSE ID 000000

SSE Version Unlock / Lock SSE UnLock

Minimum Pin Length 4 ☒ Requires Pin Validation

SSE Licenses Available 56 ☒ Requires New Pin

Client Info

AES/TDES Mode AES128

Key 9850868073928BEEEECD94C8E9E756171DC16C9EDCCB900A

Key Signature BCD0960F6FF628EF9B4EAB4A40E136A8254442FC93E0D20ACE9

Communication

Communication Type Modem Dial Out

Use Dialing Options Country Region Afghanistan (93)

Dialout Modem Number

AES/TDES Mode: Select Triple DES or AES128 mode. This is the encryption mode that will be used by the SSE.

Key: Enter the encryption "Seed Key". The Client Primary Key must consist of 64 hex digits. To generate a key, click on the left arrow in the Key field.

Key Signature: Signature of the Primary Key. The Key Signature of remote Encryptors is compared with this Key Signature. If both Signatures are the same then the Keys will be the same.

Communication

Communication Type: This is the communication type that the OBM uses to communication with the SSE device.

Communication Type	Description
Modem Dial Out	<p>Selecting Modem Dial Out will require that you enter the phone number in the Dialout Modem Number field. You can also choose to use dialing options and select the country/region.</p> <p>Note: Dialing Options for a specific modem are set in System Settings, Global System Settings tab.</p>
Modem Dial In	<p>Selecting Modem Dial in will require entering the number of minutes that the OBM will wait for a connection in the Wait for Connection field. The maximum value is 15 minutes. A communication port must also be selected.</p>
Direct to COM Port	<p>Selecting Direct to a COM Port will require entering the desired COM port and the number of minutes that the OBM will wait for a connection in the Wait for Connection field</p>
Local USB Port	<p>Selecting the Local USB Port will require choosing the COM Port to which the SSE device is connected.</p>
IP Dialout	<p>Selecting Modem Dial Out will require that you enter the phone number in the Dialout Modem Number field. You can also choose to use dialing options and select the country/region.</p> <p>Note: Dialing Options for a specific modem are set in System Settings, Global System Settings tab.</p>

5.5 Adding a UniGuard or Port Authority Client Device

A CDI UniGuard or Port Authority device can be programmed as a client encryptor by the OBM. The client device then allows remote users to connect securely to CDI devices via Triple DES/AES communications.

Select the NOC site to which the device is to be added. In most cases, this is the Default NOC Site.

To add a client device to this site, click Create and select Client Device from the drop down menu. The Device Info tab opens. Select the device type from the drop list.

The screenshot shows the 'Device Info' tab of a configuration interface. It contains several sections: 'General' with fields for Type, ID - S/N, Status, License, Device Confirms, Version, Name, Flash Message, Asset Tag, Lenses Available, Add to Client Dialout List, Enable Cell Syslog Gateway, Program Users in Client Device, and Remove from Preferred Client List; 'Management Communication' with Primary, Secondary, and Terminal dropdowns, an SSH checkbox, and an Operation Communication dropdown; 'Modem' with a Dialing Type dropdown, PBX Access Code, Domestic Access Code, International Access Code, and Country/region dropdown; and 'Access Methods' with checkboxes for Network Enable, AES 128 Enable, RawTCP, Modem, and SSH Enable.

Device Info tab

Only fields that are unique to client devices are described in this section. Fields common to both client devices and remote devices are described in the previous section.

Add to Client Dialout List (optional): If enabled, the UniGuard or Port Authority IP Client can be included in the OBM Network Dialout List, which can be used to communicate (program) with other CDI devices whose OBM communicates is set for Network Dialout. The device must have an IP Address defined in the Network Properties tab.

Enable Cell Gateway – This will allow a Cell Client to act as a gateway for telemetry data back to the hard network.

Network Enable – This enables the network port on the CDI device

AES 128 Enable – This enables AES 128 on the CDI device

RAW TCP – this enables RAW TCP for acces to the CDi device. A CDI network tunnel uses RAW TCP for communications transport.

Modem – Enable the modem in the CDI Device.

SSH – Enables SSH protocol to the CDI device.

Program Users in Client device. This will allow the Client to act as an authentication point before a user can dial out of the network. Optionally you can set the Client to use RADISU or TACACS+ and talk to a network server.

Remove from Preferred Client list – this will remove the client from the proffered list.

Operation Communication: If all AES/TDES Modes have been selected in System Options tab, then you need to select by which mode the OBM will communicate to the client device before the client device dials out to a remote device.

Network Properties

All fields are the same as when a remote device is created. Please refer to the Devices section of this manual for detailed information about the fields and entries.

Note: Network Properties tab is only available for UniGuard and Port Authority devices with a network interface.

System Options:

The options displayed depend on the device type selected. Only fields that are unique to client devices are described in this section. Fields common to both client devices and remote devices are described in the previous section.

AES Mode: Select All, AES128, AES192, AES256 or All. These are the methods by which OBM can communicate with a client device before the client device dials out to a remote device.

“All” enables the device to operate with host encryptors (UniGuard and Port Authority devices) in all modes. Note that the UniGuard client must also have an AES Engine connected to its link port to be able to do AES.

The screenshot shows the 'System Options' tab for a client device. The 'AES Mode' section has 'All' selected. The 'System Key' section has 'Sys Password' as '*****', 'Sys Key' as '*****', and 'Sys Key Signature' as '474B9FE187B22555474B9FE187B22555474B9FE187B22555'. The 'Client Key' section has 'Key' as '*****' and 'Key Signature' as '99C714F8054F2F8CB732B0AC7457EE63BECEDF21E8E2F50D07'. The 'Host DTR/RTS Loss of Signal (secs)' is set to 5.

System Options for UniGuard Devices

The screenshot shows the 'System Options' tab for a UniGuard device. The 'AES/TDES Mode' section has 'All' selected. The 'Device Mode' is 'Client Device'. The 'Power/JP Port Option' is 'Power Port Connection'. The 'Host "AT" Command Access' is 'Enabled Transparent'. The 'Client Key' section has a red circle around the 'Key' field, which contains '*****'. The 'Key Signature' is '99C714F8054F2F8CB732B0AC7457EE63BECEDF21E8E2F50D07'. The 'Host DTR/RTS Loss of Signal (secs)' is set to 5.

AES Mode/TDES mode: The encryption modes displayed depend on the device.

Device Mode: Select the security type. The available types are listed below:

- Standard Device (Enable Security). Default

- Device Authentication/Encryption – this device will only communicate with UniGuard Clients in an encrypted mode.
- RSA SecurID Device
- Standard Device (Bypass Security): Security is disabled for this device.

System Password: This is the password used by OBM to access the device. When editing an existing device, asterisks are displayed in the password field.

System Key: This is the key used by OBM to encrypt data with the device. A key used by the OBM to access and program the device. This encrypts the communication between the device and the OBM,

You can define your own system key or click the Generate button to have the system generate a key.

Client Key: This is the key that the client will use to encrypt data with remote CDI devices. Enter a key or click the *Generate button* to have the OBM create one.

Key Signature: This is a representation of the key without revealing the key. Signature of the Primary Key. The Key Signature of remote Encryptors is compared with this Key Signature. If both Signatures are the same then the Keys will be the same.

Power Port/IP Port Option: (*applies to UniGuard devices only*). The power port / IP port of a UniGuard device can be set to one of the following modes.

Program only: Only allows the OBM to have access to this port for serial programming.

Power Port Connection: Port is used as a Power port connection

IP Authentication: The device is network enabled and User authentication is allowed on port

Network Dialout: UniGuard can be used as a Network Dialout connection.

Internal Modem tab

All the fields for a client device are the same as those for a remote device of the same device type. Please refer to the Devices section for detailed information about each field.

6 USER MANAGEMENT

The OBM has a set of tools that enable you to manage system users, roles and access calendars. This section describes how to use the tools these tools to manage system users, roles, and access calendars.

System users may be added, modified, and deleted as required. When a system user is added, a role is assigned that determines the user's privileges and the time period during which the OBM may be accessed.

This section describes how to do the following:

Add, modify, and delete system users

Manage roles

Set up access calendars

6.1 User Management tab features

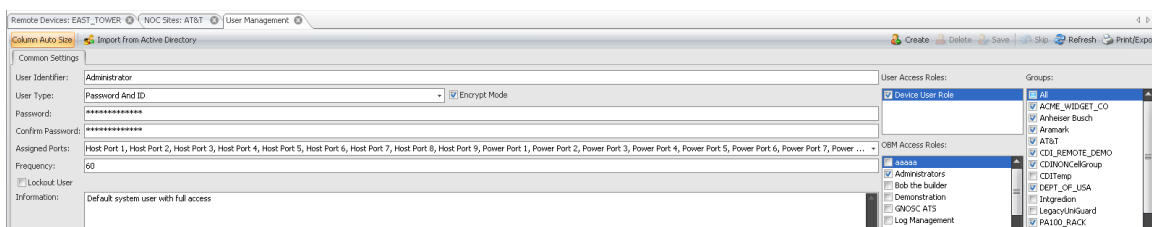
User Info Tab: The fields in this tab enable you to add or edit user information.

User List: A list of all users in the OBM database. If you have entered search criteria, then all users who meet the search criteria are listed.

User Access Roles: Allows user to access devices and the OBM database.

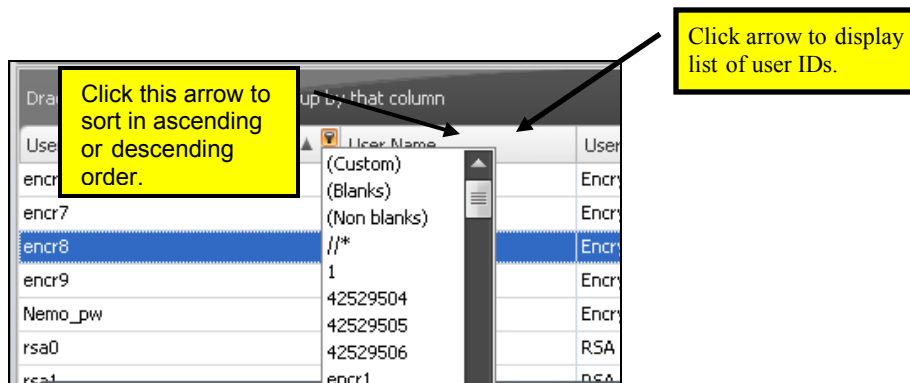
OBM Access Roles: Defines OBM access roles for the user

Group List: A list of all groups in the OBM database. To add a user to a group or groups, select the group by clicking the checkbox of the group.



6.1.1 Sorting the user list

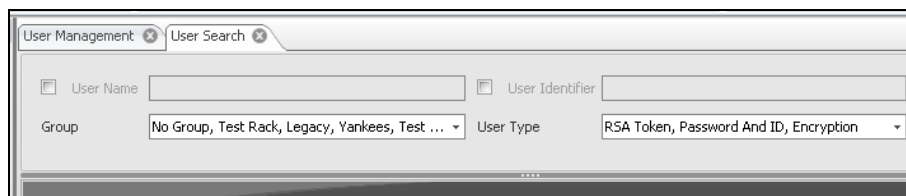
Click the column heading to display arrows that enable you to sort the list in ascending or descending order, or to display a “quick list” of users.



6.2 Finding a User

You can search for a user by name, identifier, user type, group, or by a combination of these.

To find a user, click **Users Search** in the ribbon bar. The **User Search** tab is opened.



In the appropriate fields, enter any or all of the following search criteria.

User Name

Group

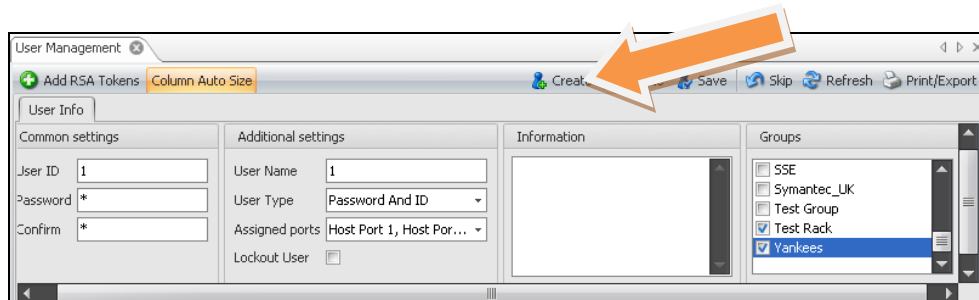
User Identifier

User type

Click **Search**. The results will be displayed beneath the User Search open tab.

6.3 Adding a User

To add a user, click **Users** in the ribbon bar. The **User Info** tab is opened. The fields of the User Info tab are organized into four sections: Common settings, Additional settings, Information, and Groups.



Click **Create** to add a new user to the database. .

Enter information about the user.

User ID: The ID that the user will enter to log on to the system. The User ID may have a maximum of 10 characters in length.

User Type: From the drop down list, select the User Type: The User Type determines the type of access the user will have, and thus the security level.

If the selected User Type is Password and ID or Encryption, you will need to enter a Password at this point.

Password: Enter the password that you user will enter in order to access the system.

Confirm: Enter the password again. If it does not match the one entered in the Password field, a message will be displayed.

If RSA token has been selected as the User Type, the token information in the RSA SecurID Token Info tab must be entered Open the RSA SecurID Token Info tab and enter token information.

Token Management

Token Number: 125309858

Birth Date: 9/9/2011 12:00:00 AM

Death Date: 9/30/2013 12:00:00 AM

Token Pin: *****

Attached User: support

New Pin Mode: ☐

Drag a column header here to group by that column

Token Number	User
42529506 : EXPIRED	42529506
42529507 : EXPIRED	
125309858	support
125309859	rsa9859
125309860	rsa9860
125309861	rsa
125309862	

Serial Number: The permanent number on the token. Once you select a token from the drop down list, the RSA Toke Pin fields become active. .

Birth Date: Date the token was activated by RSA

Death Date: Date the token will expire (and will require replacing)

Token Pin: PIN that is used to authenticate the user. The PIN should have eight characters.

New Pin Mode checkbox: Usually enabled the first time the user is entered into the database. If this is enabled, the user will be allowed to authenticate and obtain the pin from the device. If this has not enabled, then the user will not be able to authenticate and obtain from the device; in this case the user must KNOW the pin.

The next time it programs the device; the OBM retrieves this information and the New Pin Mode checkbox is not checked.

In the Additional Settings and Information sections enter more information about the user.

User Name: Enter the name of the user. You may enter the actual name or a nickname.

User Type: From the drop down list, select the User Type: The User Type determines the type of access the user will have, and thus the security level.

From the pull-down option list, select the type of authentication that will be used to confirm the user identity. Available user types and descriptions are listed in the following table.

User Type	Description
RSA SecurID Token	User must have an RSA token and pin to use the passcode to gain access to a device,
Password and ID	User inputs a User ID and password to gain access
Encryption	User ID and Password must be entered, and the whole session is encrypted. For an encrypted session, the user must dial out through a UniGuard Client or normal modem with an SSE.

Assigned Ports: From the drop down list, select the ports to which the user will have access. Users for Port Authority devices can be granted access to any single port, group of ports, or to all ports. If a user is to have access to all the ports in the Port Authority, then the *Select All* box may be checked.

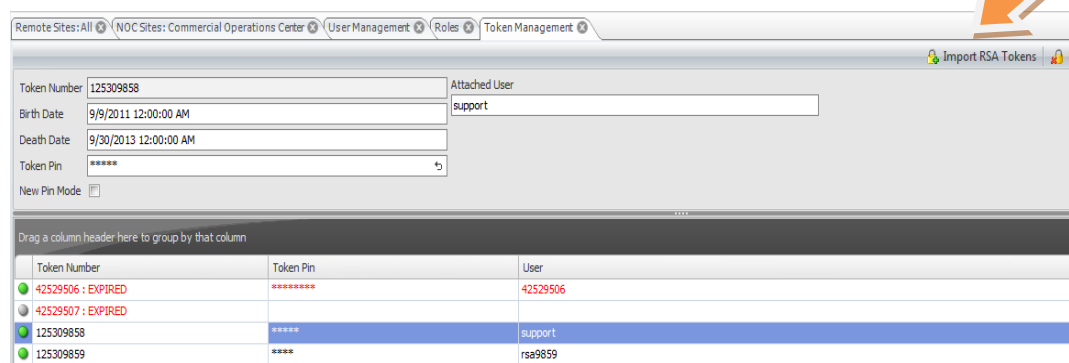
Information: Enter additional information about the user, if desired; otherwise leave blank.

Lockout User checkbox: Click the checkbox to lock out a user from a group without having to delete their profile. The user will then be included in the locked user list.

In the Groups box, select the Groups to which the user is assigned. A user may belong to single group or to multiple groups.

Click **Save** to save your changes or **Skip** to discard them.

To add an RSA token seed record XML file click “Import RSA Tokens”



The screenshot shows the 'User Management' tab in a software interface. The 'Token Management' sub-tab is active. On the right side of the ribbon, the 'Import RSA Tokens' button is highlighted with an orange arrow. Below the ribbon, there are input fields for 'Token Number' (125309858), 'Birth Date' (9/9/2011 12:00:00 AM), 'Death Date' (9/30/2013 12:00:00 AM), and 'Token Pin' (*****). The 'Attached User' field shows 'support'. Below these fields is a table with columns 'Token Number', 'Token Pin', and 'User'. The table contains three rows: the first two are expired tokens (42529506 and 42529507) and the third is the active token (125309858) for user 'support'.

Token Number	Token Pin	User
42529506 : EXPIRED	*****	42529506
42529507 : EXPIRED	*****	
125309858	*****	support

6.4 Modifying a User

You can change the password, name, type or other settings of a user.

To do this, locate the user in the user list. Rather than scrolling through the user list, you may sort the list by any column heading or you may use the User Search tool in the toolbar.

In the User Info tab, enter the new information. Click Save to save the changes or Skip to discard them.

6.5 Deleting a User

To remove a user from the database, click **Users** in the ribbon bar. The User Management tab is displayed.

In the User list displayed under User Info, click to select the user that you would like to delete.

TIP: To locate a particular user, users of a group or of a particular user type, or user type, you may use the search tool or sort any column in ascending or descending order.

Once you have selected the user, click **Delete**. A window will be displayed reminding you that some of the selected users are attached to groups and asking you to confirm that you want to delete users from the system.

Click **Yes** to Continue (the user will be removed from the system) or No to Stop.

Click **Save** to the changes.

6.6 RSA Add User Batch

The RSA Add User Batch tool lets you add several RSA users at the same time. If you have many users who use RSA tokens, it saves time. To do this upload an XML file containing the RSA user information. This can be created from an RSA ACE server.

The screenshot shows the 'RSA Add User Batch' application window. At the top, there are two buttons: a green plus icon labeled 'Add RSA Tokens' and a green checkmark icon labeled 'Save'. Below these are two main sections. The left section, titled 'Ports and Groups', contains two dropdown menus: 'Ports' with the text 'Host Port 1, Host Port 2, ...' and 'Groups' with the text 'Test Rack, Legacy, Yanke...'. The right section, titled 'Existing RSA Users', contains two radio buttons: 'Overwrite user' (which is selected) and 'Skip User'. Below these sections is a table with two columns, 'State' and 'Token Number'. Above the table is a dark grey bar with the text 'Drag a column header here to group by that column'.

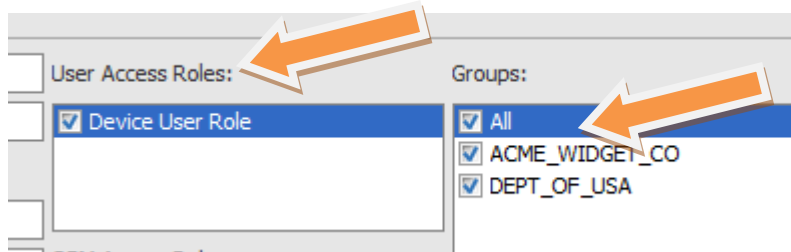
State	Token Number
-------	--------------

6.7 Adding a System User

A system user can access the OBM and perform administrative functions, such as adding other systems users, assigning roles, managing devices, specifying global system settings, and other functions

An administrator may add system users and assign them the appropriate role. By default, there is only an “Administrator” role.

By checking “Device User Role” the system user now also has access to devices. A devices user needs to be associated to groups located to the right



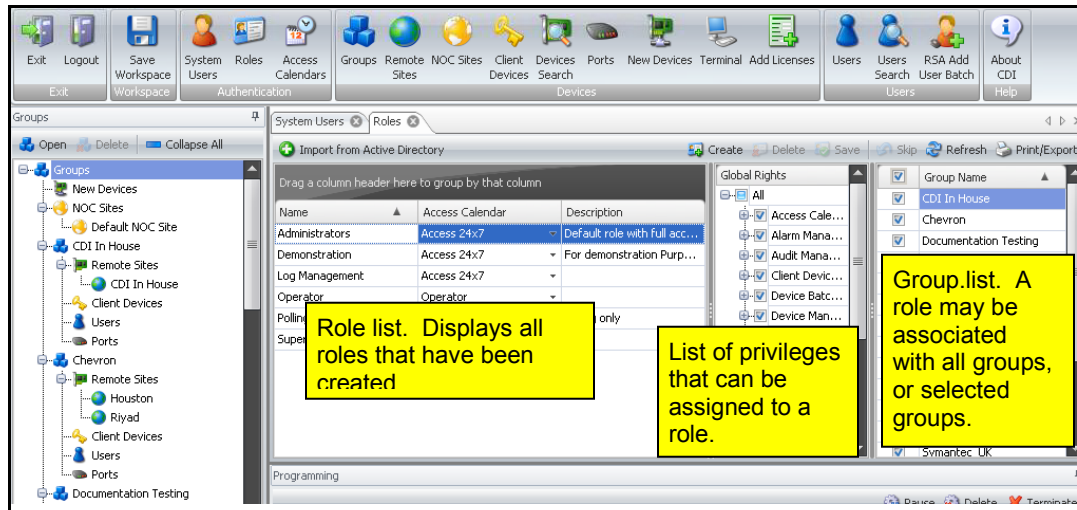
TIP: To locate a particular user, users of a group or of a particular user type, or user type, you may use the search tool or sort any column in ascending or descending order.

6.8 Managing Roles

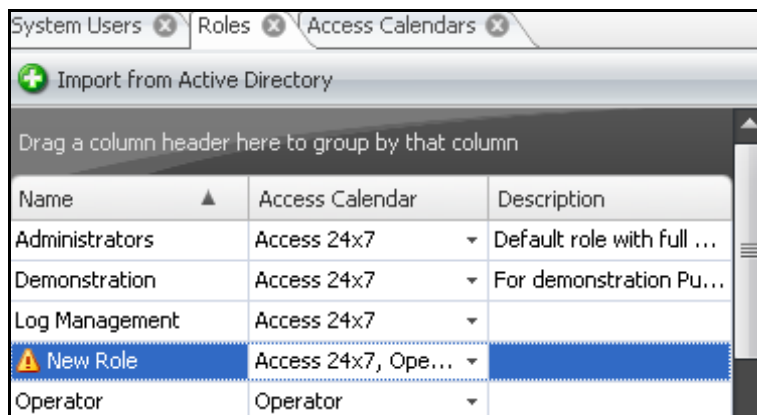
The privileges of a system user are defined by the role that has been assigned. Initially, the only role defined is the administrator role. It is the organization that determines the roles and the privileges assigned to that role.

6.8.1 Creating a Role

To create role, click **Roles** in the Toolbar. The Role tab opens.



Click **Create**. A new role is listed in the Role list.



Enter a name for the role.

Select an Access Calendar which specifies the time period during which the user with that assigned role can access the OBM.

In the Description column, enter informational text if desired.

Under Global Rights, select the privileges that the role will have. Click the checkbox to include rights, click the checkbox in the column heading.

Under Group Name, column, select the groups to which the role is associated. To select all groups, click the checkbox in the column heading.

Click **Save** to save your changes.

6.8.2 Modifying a Roles

A role may be modified by adding or removing Rights, changing the time period during which access is allowed, and changing the groups to which the role is associated.

Click **Roles** in the toolbar.

Select the role from the list.

Add or remove rights by clicking the appropriate check box. Add or remove Groups in similar fashion.

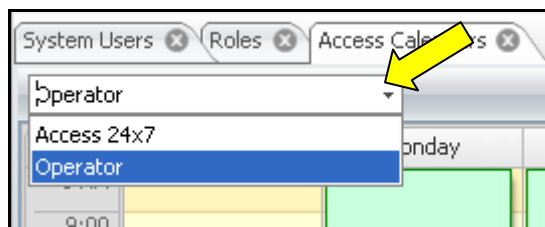
Click **Save** to save your changes.

6.9 Managing Access Calendars

The time period during which a system user may access the OBM is determined by the Access calendar assigned. You may create and remove Access calendars as necessary. Keep in mind that when an access calendar is removed or modified, the change affects all roles associated with that calendar.

6.9.1 Viewing Available Access Calendars

Before creating a new calendar, you might want to view the existing calendars. To do this, click Access Calendars in the toolbar. To see a list of available calendars, click the arrow in the Access calendar name field to display a list of available calendars.



To view the details of the calendar, select the calendar from the list. The calendar will be displayed with the access times indicated.

The Access Calendar Operator shows that a system user with the 'operator' role can only access the OBM Monday through Friday from 8:00 am to 6:00 pm.

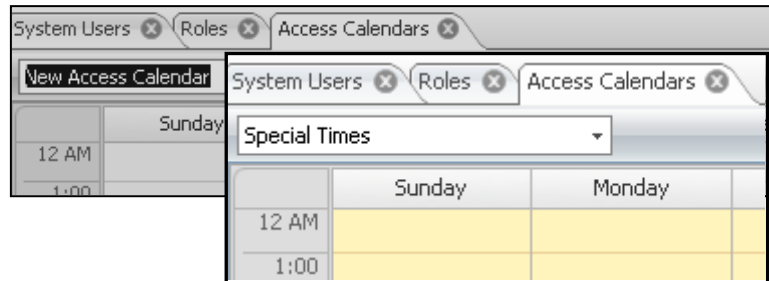
A screenshot of the 'Access Calendar Operator' view. It shows a table with columns for days of the week (Sunday through Saturday) and rows for time slots (7 AM through 7 PM). The table is filtered for the 'Operator' role. The access times are indicated by green boxes with a checkmark and the word 'Access' inside. The access is granted from 8:00 AM to 6:00 PM on Monday through Friday. The background of the table is yellow.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
7 AM							
8:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
9:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
10:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
11:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
12 PM		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
1:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
2:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
3:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
4:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
5:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
6:00		✓ Access	✓ Access	✓ Access	✓ Access	✓ Access	
7 PM							

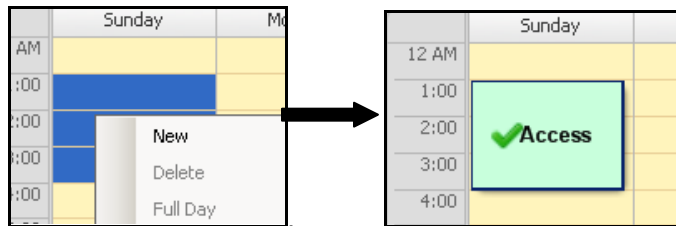
6.9.2 Adding an Access Calendar

To add an Access Calendar, click **Access Calendars** in the toolbar.

Click **Create**. Enter a name for the calendar. In this example, “Special Times” has been entered as the calendar name.

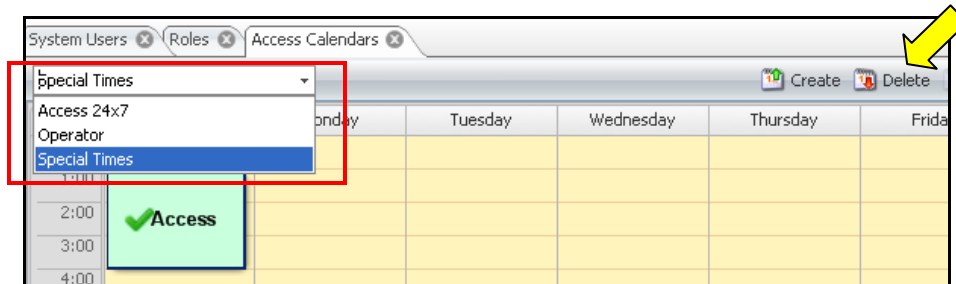


Highlight the area with the times that you like the user to have access. Right-click and select **New**. Repeat this procedure to add another time.



6.9.3 Deleting an Access Calendar

To delete an access calendar, make sure the Access Calendars tab is open. Select the calendar from the list. Click **Delete**.



6.9.4 Modifying an Access Calendar

To modify an access calendar, open the Access Calendar tab and select the calendar from the list.

To remove an existing access period, right-click in the Access period, and then select **Delete** from the drop down list.

To add a time, highlight an area, right-click on the area and select **New**.

7 PROGRAMMING

What is unique to the CDI set of Out of Band Management products is that they all have their own internal security database that can work without the network being in operation. This is what defines CDI's products as "true out of band". If the network is functioning properly, then out of band is not required to manage and access a network. To accomplish this, each CDI device needs to have its security database "pushed" out to it via the OBM. Whenever changes are made to the OBM database concerning a remote device; a "push" or "reload" of its database is required to know about the changes.

All CDI devices are shipped WITHOUT any configuration on purpose. An OBM load of each device is required to activate and use the product. This eliminates rogue operators from attempting to usurp a security policy developed by each enterprise.

This section describes how to use the OBM program to manage UniGuard, Port Authority, and SAM devices. When the database is modified or a device is added, the devices need to be programmed with information from the OBM computer database. The device may be reloaded with information from database of the OBM computer or updated with any information that is new.

This section describes the following tasks:

Program all the Remote Devices of a Group

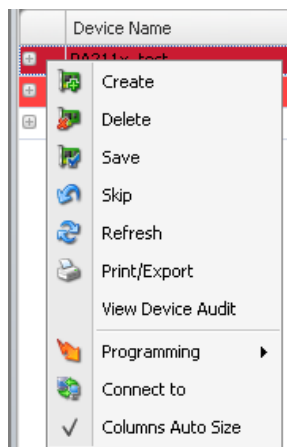
Program a single device or multiple devices

Clear a device's alarms

Telnet to a device

7.1 Programming Devices

You may choose to program all devices of a Group, or a single device. By right clicking on the far left + sign on the device list you will get a pull down to program the device.




After you select the appropriate option, the status of the programming operation is displayed in the Programming pane. You may **Pause**, **Delete**, or **Terminate** the operation. Note that an operation in progress may not be deleted.

Programming

Pause

Delete

Terminate

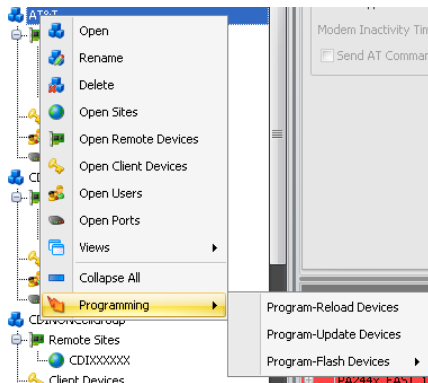
	Device	Operation	Status	Description
	PA199 Host 172	Configure Device's IP C...	InProgress	Connect to device: initialize connec...

When the programming of the device or devices has been successfully completed, the message “Successfully Programmed:” is displayed. If the operation is not successful, a popup window with an error message is displayed. An entry in the Program Operation log will indicate the success or failure of the operation. This log may be displayed by clicking Program Operation Log in the Log toolbar.

7.2 Programming a Group

You can program or reset all the devices of a Group.

Right click on the name of the group



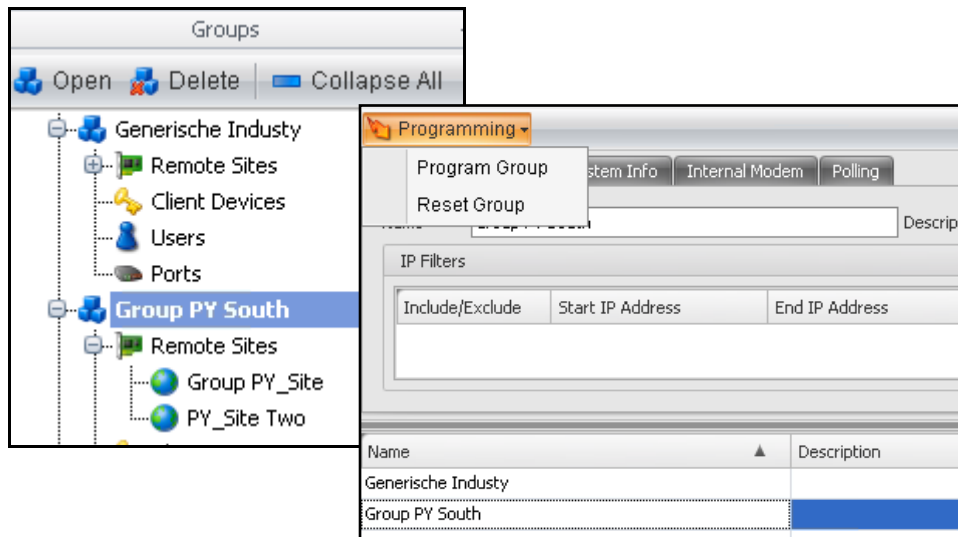
Program Group: Programs all devices in the selected group based on the changes made to the database residing on the OBM PC. Program Group adds and deletes users from the database of each device of the group. Program Group does not clear the default parameters of a device; it updates the devices with the changes since the last time the devices were programmed.

Reset Group: Clears all devices in the selected Group to the default settings, and then programs each device with the date and time, system options, port options, and the client ID list (if it is not a client).

Click Groups in the toolbar.

Select the Group from the open view list of Groups.

From the dropdown Programming list, select either **Program Group** or **Reset Group**.



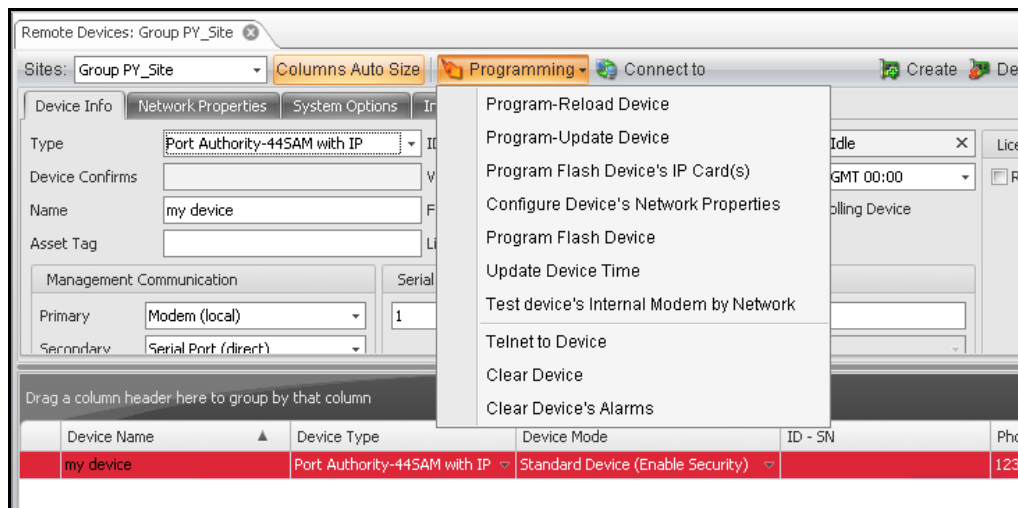
7.3 Programming a Single Device

A single device of a Remote Site may be programmed.

Select the device from the open view Device List.

Click Programming to display a list of programming options. The Programming options displayed depend on the device type of the selected device. Select the appropriate option.

Tip: You can start a new program operation while a previous one is still in progress, or you can select multiple devices at ones, and then select Program Reload.



Program-Reload Device: Clears the memory of the device then re-programs it with all the settings in the device record information. The device record contains all the information, parameters, settings, and properties that the OBM stores about a device.

Program-Update Device: Updates the device by adding any changes configured in the device record since the last time the device was programmed.

Program Flash Device's IP Card(s): Programs the firmware of the internal IP card(s) of the selected device.

Configure Device's Network Properties: Allows you to just push out the configuration of the devices network card.

Tip: If you have only changed the network settings of a device, select "Configure a Device's Network Properties" to just push out the network settings of the device, and thus save time. While "Program Load" also pushes out the configuration of the device's network card, it also pushes out the user list and other device settings.

Program Flash Device: Programs the firmware of the selected flash device. This is used for updates to remote firmware versions.

Update Device Time: Resets the date and time of the device.

Test device's Internal Modem to Network Tests the internal modem by connecting to the device via network communications.

Note: Devices without an IP card have all the programming options listed above except Program Flash Device's IP Cards and Configure Device's Network Properties. Newer PA100 and PA200 devices need their network ports enabled via EDL's files. The network port will be available for access by the OBM to install EDL-N's but will not operate for any other function until the ports is enabled.

Telnet To Device: Opens a Telnet Session to a device with an internal IP Card or network port.

Clear Device: Clear all security credentials (system password and system key) from the device. The device must then be reprogrammed before it can be accessed.

Clear Device's Alarms: Clears the device's alarms and returns the status to idle.

Program Group Flash Devices IP Card: Programs the Firmware of the IP Card for all devices in the selected group.

Test Device's Internal Modem by Network: Tests the internal modem by connecting to the device via network communications.

Clear Device: Clear all security credentials (system password and system key) from the device. The device must then be reprogrammed before it can be accessed.

7.4 Programming Multiple Devices

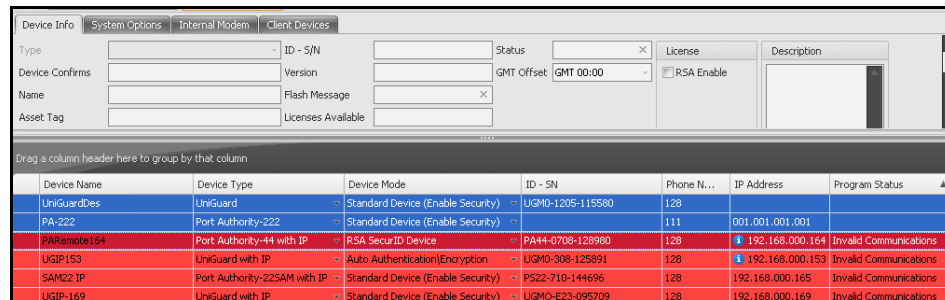
Multiple devices may be programmed at the same time.

Click **Devices Search** in the toolbar. Select the device types from the dropdown list. You can search for devices of a specific type or types, or all types. You may also enter other search criteria.

Alternatively, in the Group List, click **Remote Sites** of the Group whose devices you wish to program. The Device Info tab opens and the devices of that Group are listed.

Select the devices and then click **Programming**.

Select the appropriate option Programming option.



Device Name	Device Type	Device Mode	ID - SN	Phone N...	IP Address	Program Status
UniGuardDes	UniGuard	Standard Device (Enable Security)	UGM0-1205-115580	128		
PA-222	Port Authority-222	Standard Device (Enable Security)		111	001.001.001.001	
PARemote164	Port Authority-44 with IP	RSA SecurID Device	PA44-0708-128980	128	192.168.000.164	Invalid Communications
UGIP153	UniGuard with IP	Auto Authentication/Encryption	UGM0-308-125891	128	192.168.000.153	Invalid Communications
SAM22 IP	Port Authority-22SAM with IP	Standard Device (Enable Security)	PS22-710-144696	128	192.168.000.165	Invalid Communications
UGIP-169	UniGuard with IP	Standard Device (Enable Security)	UGM0-E23-095709	128	192.168.000.169	Invalid Communications

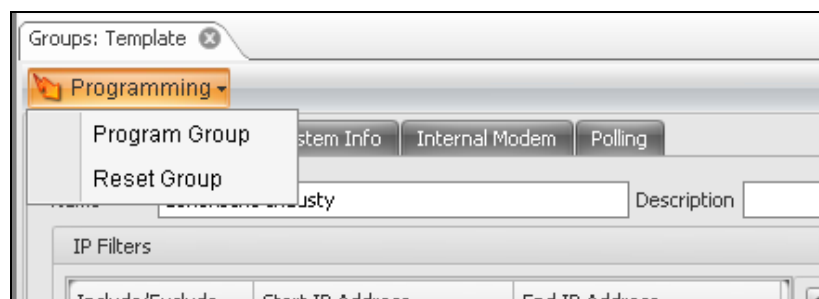
7.5 Programming all Devices of a Group

All the devices of a group may be programmed or reset.

Click **Groups** in the toolbar. The Groups will all be listed in the Open View portion of the screen.

Select the Group to be programmed.

Click Programming. Select Program Group or Reset Group.



7.6 Telnet to a Device

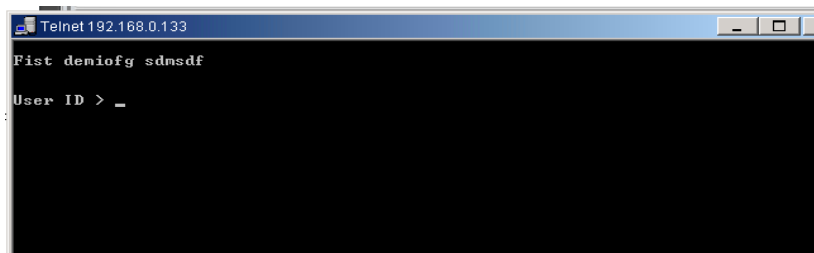
Select the device from the device list.

To display a list of all devices, click Device Search in the toolbar. Depending on the search criteria that you enter, you may display all devices or particular devices.

To display the devices of a Remote Site, click on the Remote Site name in the Group List.

Select the device.

Click **Programming**, and choose **Telnet to Device**. A telnet connection to the selected device will be established and the telnet window is displayed.



7.7 Clear Device

This option clears all the security credentials from the selected device. The device must then be reprogrammed before it can be accessed.

To reprogram a cleared device, select Program-Reload.

7.8 View Alarms

To view a list of all alarms, click **Alarms** in the Programming pane. A list of alarms is displayed.

Alarms						
DateTime	Severity	Device	User	Event	Description ▲	PortNumber
9/7/2011 2:32 PM	Major	PA199 - 27		User ID/Password Error	"	M
9/7/2011 2:32 PM	Major	PA199 - 27		User ID/Password Error	"	M
9/7/2011 2:32 PM	Major	PA199 - 27		User ID/Password Error	"	M
9/7/2011 2:32 PM	Major	PA199 - 27		User ID/Password Error	"	M
9/7/2011 2:32 PM	Information	PA199 - 27		Device Is Alive	"	
9/7/2011 2:32 PM	Information	PA199 - 27		Device Is Alive	"	
9/7/2011 2:32 PM	Information	PA199 - 27		Device Is Alive	"	
Alarms Programming						

Alarms						
<div> Clear Refresh Print/Export </div>						
DateT...	Sev...	Device	User	Event	Description	PortNumber
6/7/2011...	Inform...	PA111 - 36		Device Is A...	"	
6/7/2011...	Inform...	PA111 - 23		Device Is A...	"	
6/7/2011...	Inform...	PA111 - 24		Device Is A...	"	
6/7/2011...	Inform...	PA199 - 28		Device Is A...	"	
6/7/2011...	Inform...	PA199 - 27		Device Is A...	"	
6/7/2011...	Inform...	PA199 - 26		Device Is A...	"	
6/7/2011...	Inform...	PA88 Host...		Network C...	"	N
6/7/2011...	Inform...	PA88 Host...		Network C...	"	N
6/7/2011...	Inform...	PA199 - 33		Device Is A...	"	
6/7/2011...	Inform...	PA199 - 48		Device Is A...	"	
6/7/2011...	Inform...	PA199 - 34		Device Is A...	"	
6/7/2011...	Inform...	PA88 Host...		Network C...	"	N
6/7/2011...	Inform...	PA88 Host...		Network C...	"	N
Alarms Programming						

7.9 Clear Alarms

To clear the alarms of a device, select the Remote Site to which the device belongs. Select the device and click **Programming**. From the dropdown menu, select **Clear Alarms**.

The alarms for the selected device will be cleared.

8 CONNECTING TO REMOTE DEVICES

Note: OBM is not required to access devices but can be used as a nice GUI tool to provide this function along with full keystroke monitor of each session.

The primary day- to- day functionality of the OBM is to allow network engineers to easily connect via SSH to all network devices on the edge points of the network. If these edge point devices are inaccessible, then OBM allows the engineer to utilize the CDI device for out-of-band encrypted access from the same set of screens. This is what we call the “cockpit” view which allows full in band and out of band connectivity from the same set of screens.

This section describes how to connect to remote CDI and non-CDI devices using the OBM running on a manager’s PC

8.1 Overview

The OBM allows network engineers to access a remote CDI device from the OBM client software running on a network connected machine. The OBM client works in conjunction with the OBM application server which in turn talks to the OBM SQL database contained on the server.

The OBM can use CDI client encryptors to provide FIPS-140-2 validated security to the remote devices. If FIPS 140-2 encryption is not required, the OBM can provide strong two-factor authentication or 128 bit AES encryption with the commercial versions of the products.

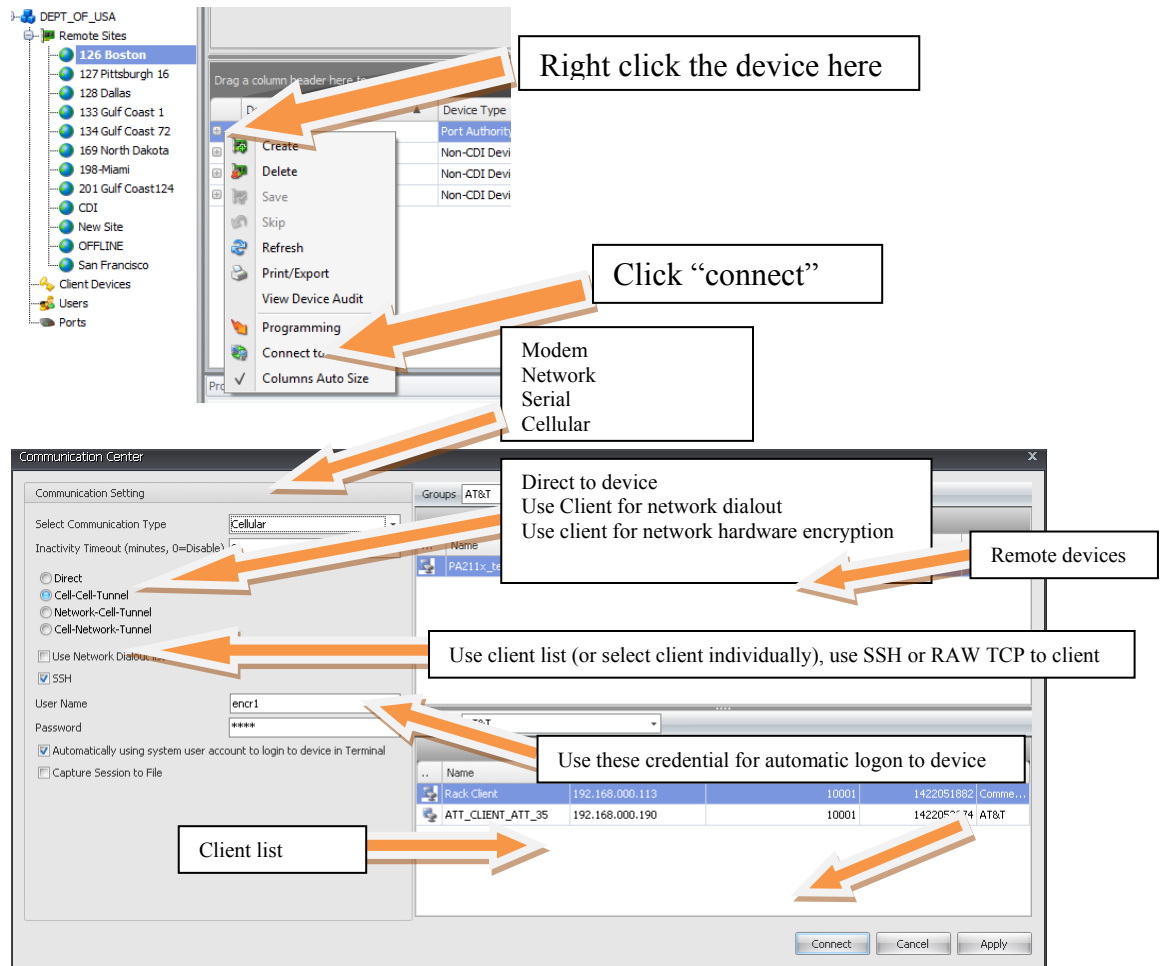
Each OBM user has defined roles which allows or blocks certain functions. For instance a NOC engineer will typically be allowed access to remote device but will not be able to view or modify security credential for those devices. A security administrator will typically be able to view and modify security credentials but will not have access to remote devices. A project manager may only be able to add or delete devices from the database.

8.2 Terminal screen features

The terminal screen allows you to interface with CDI and non-CDI devices via telnet or SSH.

8.2.1 Connecting to a device

To connect to a device, click Terminal in the toolbar. The terminal screen opens. You can also right click on the device in the sites menu from the far left column and select “connect”



You will get a screen preset for the connection setup of that device. You may change the connection method by changing "select communication Type". Once you press "connect" you will be passed to the terminal screen and your keyboard will be directly mapped to the connection.

```

Connect to Client : 192.168.000.114
??

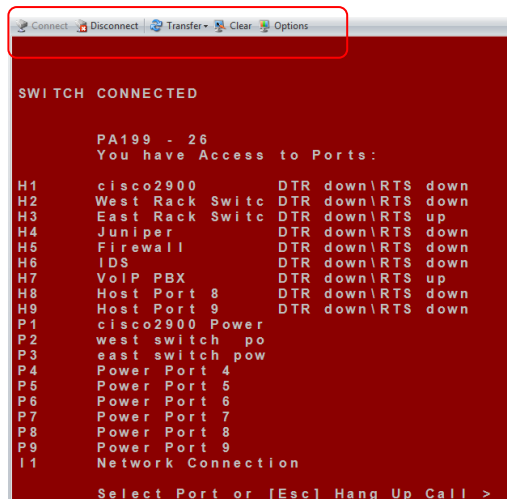
PA111_114
You have Access to Ports:

M1      Modem Port 1 - Port In Use
I1      Network Connection

Select Port or [Esc] Hang Up Call > M1

```

The terminal will echo back all the commands being sent to the client device and connection commands to the remote device. The terminal will automatically enter IP addresses, phone numbers, and credentials (if checked) until the device is handed off to the user for use.



The buttons at the top of the screen allow you to perform the following operations:

Connect: Connect displays the Communication Center screen. In this screen you select the communication method and the device to which you want to connect.

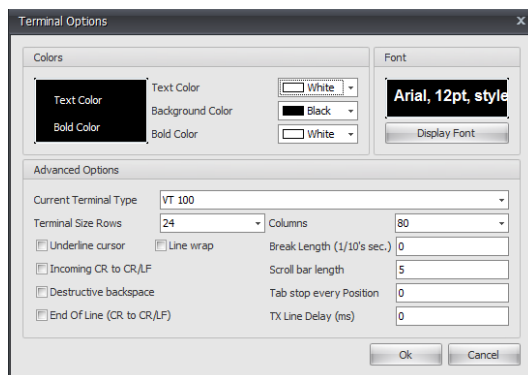
Disconnect: Drops the connect between the device and the OBM computer.

Clear: Clears the terminal screen.

Options: Displays the Terminal Options screen which allows you to change the screen colors and font size, select the terminal type, and other options.

Transfer: Allows a file to be sent or received. The transfer button allows you to send a file, character by character, to a device. This would typically be used, for example, to automatically key in a long config on a router, switch, etc.

8.2.2 Terminal Options



Colors

You can choose the font and text, background, and colors.

Advanced Options

Current Terminal Type: The terminal emulation can be changed using this window. Select the Terminal Type from the scroll down list.

Terminal size, Rows and Columns: Select the number of rows and columns displayed on the terminal screen.

Underline Cursor: Check this box to replace the cursor with an underline.

Line wrap: Check this box to break up long lines (lines without Returns and/or Return/Linefeeds)

Destructive Backspace: When a remote device sends a Backspace it can backspace the cursor or delete the backspace character and backspace the cursor. If this box is checked, everything you type will be deleted when you press Enter.

Incoming CR to CR/LF: Check this box to incoming end of line (Return) to a Return and a Line Feed.

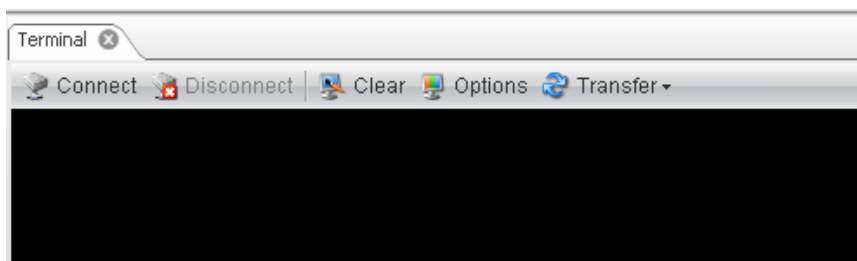
End of Line (CR to CRLF): Check this box to change the typed end of line (Return) to Return and a Line Feed.

Scroll Bar length: Maximum number of rows it will buffer to the display. Default is 192 rows.

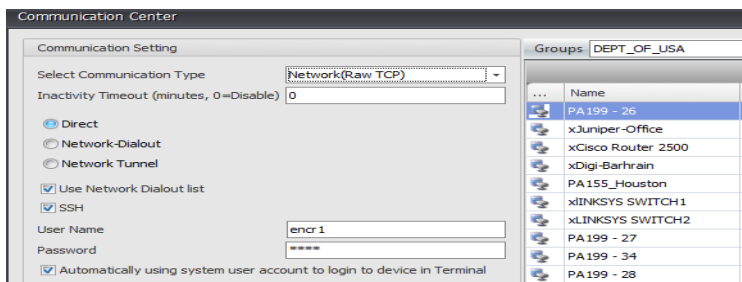
Tab stops every position: Set the number of character positions that a TAB will produce.

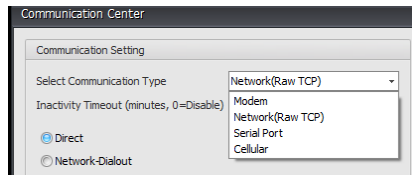
8.3 Connecting to a Device

Click **Terminal** in the toolbar. The Terminal screen opens. The terminal screen allows you to interface with CDI and non-CDI devices via telnet or SSH. .



Click **Connect** The Communication Center is displayed. The Communication Center screen enables you to view the Connection List and preferences for the communication type.





Select the Communication Type. The communication types displayed depend on the device selected.

8.3.1 Modem:

This will use a standard modem connected to a serial port of the client machine.

8.3.2 Network:

Can be used in conjunction with the buttons below:

8.3.2.1 Serial:

Will be a direct network connection from the workstation to the remote device w/wo SSH if checked/unchecked

8.3.2.2 Network Dialout:

Will use a network connected CDI client to dialout to a remote device.

8.3.2.3 Network Tunnel:

Will use a CDI network connected client to establish a hardware encrypted tunnel from the CDI client to the remote device.

8.3.3 Serial:

Will use a local serial port on the workstation to connect to the CDI device.

8.3.4 Cellular:

Can be used in conjunction with the buttons below.

8.3.4.1 Direct:

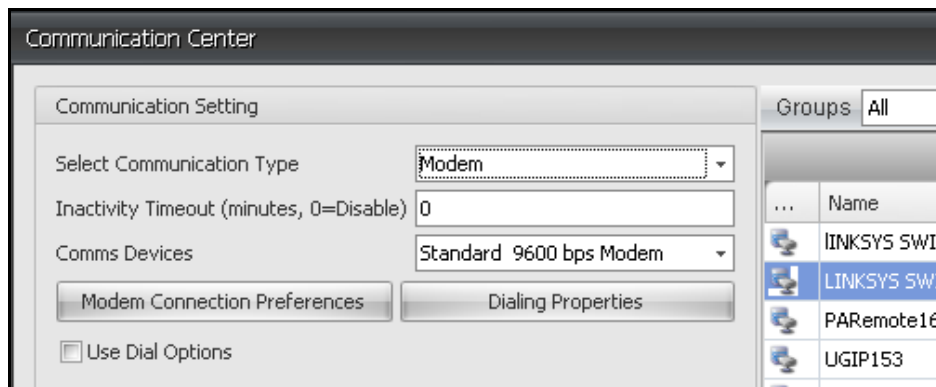
The OBM will use a direct network connection to establish a TCP connection to the remote cellular device. The remote cellular device has a TCP address for connection.

8.3.4.2 Network Tunnel:

- Standard CDI Client
 - The OBM will use a local CDI client to establish a secure Network tunnel from the CDI client to the remote Cellular device using a network TCP connection from the client to a cellular TCP connection on the remote.
- Cellular CDI Client
 - The OBM will use a local cellular CDI client to establish a secure cellular Network tunnel from the CDI client directly to the remote Cellular device using the cellular radio in the local device. Ie total cellular connection.

After you select the communication type and select the select the Device.

8.3.5 Modem Communications



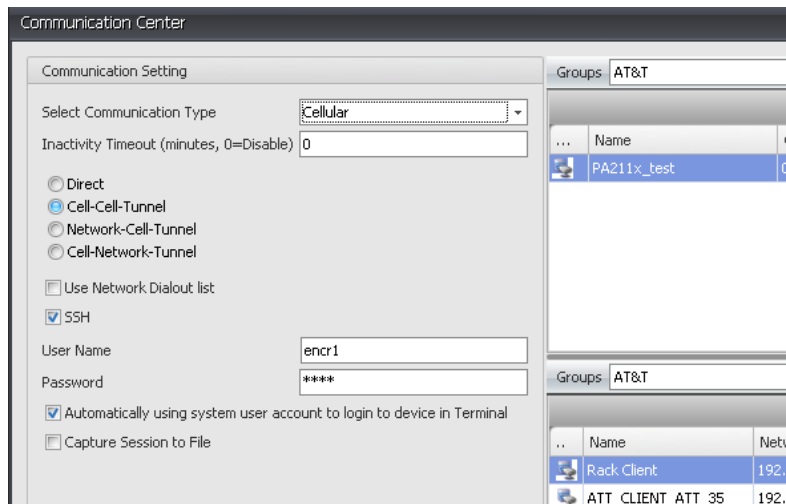
Inactivity Timeout: This value is defined in minutes. The default value is 0 (Disabled). When the value is set to greater than 0 minutes and there is no activity (transmit and receive data) during the inactivity timeout period, the session will be dropped (disconnected automatically).

Comms Devices: Select the modem that will be used for communication from the drop down list.

Use Dial Options: Use the Dial Options that have been defined in System Settings / Global System Settings tab.

The Modem Properties and Dialing Options that have been defined in System Settings / Global System Settings will be used. If it is necessary to change the modem properties, click Modem Communication Preferences. Click Dialing Properties to change dialing options.

8.3.6 Cellular Communications



Direct: MPLS network must be connected to same network as OBM. OBM will use the cell address to connect directly to the remote cell device.

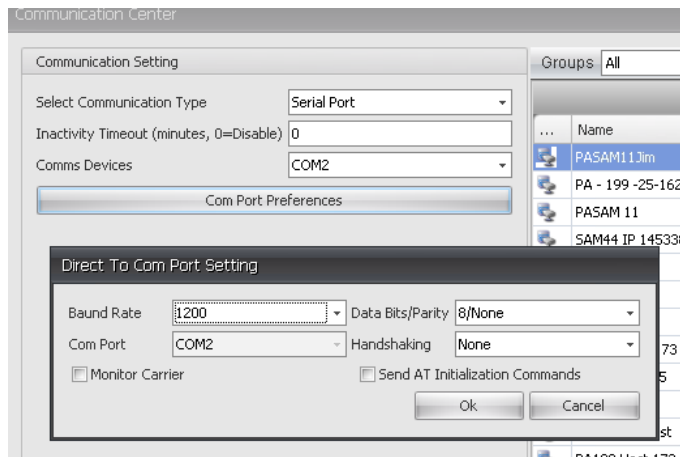
Cell-Cell-Tunnel – OBM will SSH to a local CDI client, authenticate to that client and then jump onto the Cell network through the client. A hardware encrypted session will exist between the client and the remote.

Network-Cell-Tunnel – OBM will SSH to a local CDI client, authenticate to that client and then use the existing Ethernet network to jump to the MPLS network from the client to the remote cell address.. A hardware encrypted session will exist between the client and the remote.

Cell- Network-Tunnel – OBM will SSH to a local CDI client, authenticate to that client and then jump onto the Cell network through the client. The remote device will be Ethernet connected to the same cellular APN network. A hardware encrypted session will exist between the client and the remote.

8.3.7 Serial Communications

Serial communications allows the OBM to communicate to a device through the com port.

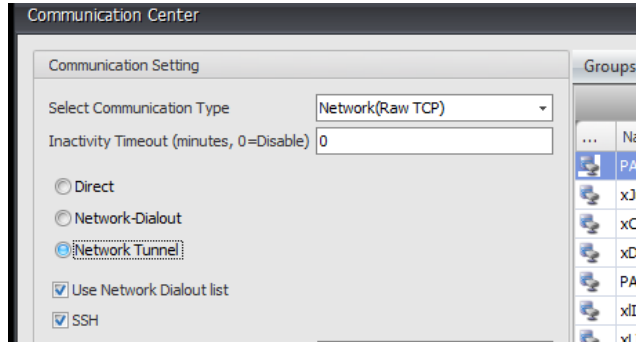


Comm Devices: Select the com port through which the OBM will communicate with a device.

Com Port Preferences: Allows you to change com port settings, such as baud rate and handshaking.

Send AT Initialization Commands: This option is used for only Serial communication type. This option sends (user) pre-defined AT commands to the modem before the dialing process is initiated.

8.3.8 Network Communications



Inactivity Timeout: This value is defined in minutes. The default value is 0 (Disabled). When the value is set to greater than 0 minutes and there is no activity (transmit and receive data) during the inactivity timeout period, the session will be dropped (disconnected automatically).

Use Remote Client/IP Dialout Address List: The IP Dialout allows access to a modem for Dialout purposes but first connects to the modem via a Network IP Address (virtual modem port, e.g. Terminal Server).

Select the Communication mode from the list.

Direct: Connects directly to the selected device via the network (no client).

Network-Dialout – Uses a network connected client to “dialout” to a remote CDI “modem enabled” device for OOB access.

Network Tunnel: - Uses a network connected client to establish a hardware encrypted network tunnel with a remote CDI “network enabled” device. This will provide hardware level AES encryption up to 256 bit.

The remote's and client devices are now grouped in the connection list.

Select the **Group** to which the devices and client devices belong.

Select the **device** (upper pane).

Select a **client device** (lower pane).

...	Name	Network Address	Network Addr...	Phone Number	Serial ...
	PASAM11Jim		10001	128	1
	PA - 199 -25-162	192.168.000.162	10001	128	3
	PASAM 11		10001	128	3
	SAM44 IP 145338	199.199.199.001	10001	110	1
	PA88 NON IP		10001	105	1
	PA_RABIT	192.168.000.151	10001		0
	UG - .142	199.199.199.001	10001	85,121	0

Groups All				
Clients				
..	Name	Network Address	Network Address Port	Timestamp
	PA - 111 -161	192.168.000.161	10001	1313607799
	SuppEnc	192.168.000.105	10001	1313614913
	PA111 - 20	192.168.000.120	10001	1313696566
	PA111 - 22	192.168.000.122	10001	1313696669
	PA111 - 36	192.168.000.136	10001	1313696815
	PA111 - 23	192.168.000.123	10001	1313700296

8.3.9 SSH Communications:

If SSH is checked the communication to the local client will use SSH encryption. If no client is used (DIRECT), the direct network connection will use SSH encryption.

Refer to SSH section for detailed information about field entries.

Inactivity Timeout (minutes, 0=Disable) 0

☐ Direct
☐ Network-Dialout
☒ Network Tunnel

☒ Use Network Dialout list
☒ SSH

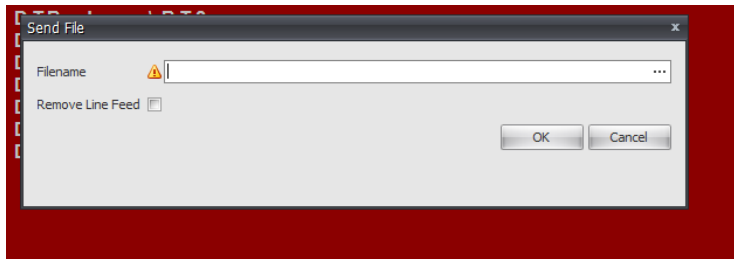
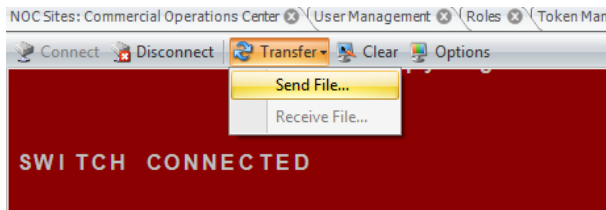
User Name encr1
 Password *****

☒ Automatically using system user account to login to device in Terminal

8.4 Sending and Receiving Files

The Transfer button displays a menu that has options to a send a file (**Send File**) or **Receive file**. The sending or receiving of files can only be accomplished when a call is in process and when in Serial or Modem Communications mode.

Caution: This only operates in Clear Text mode (NO ENCRYPTION)



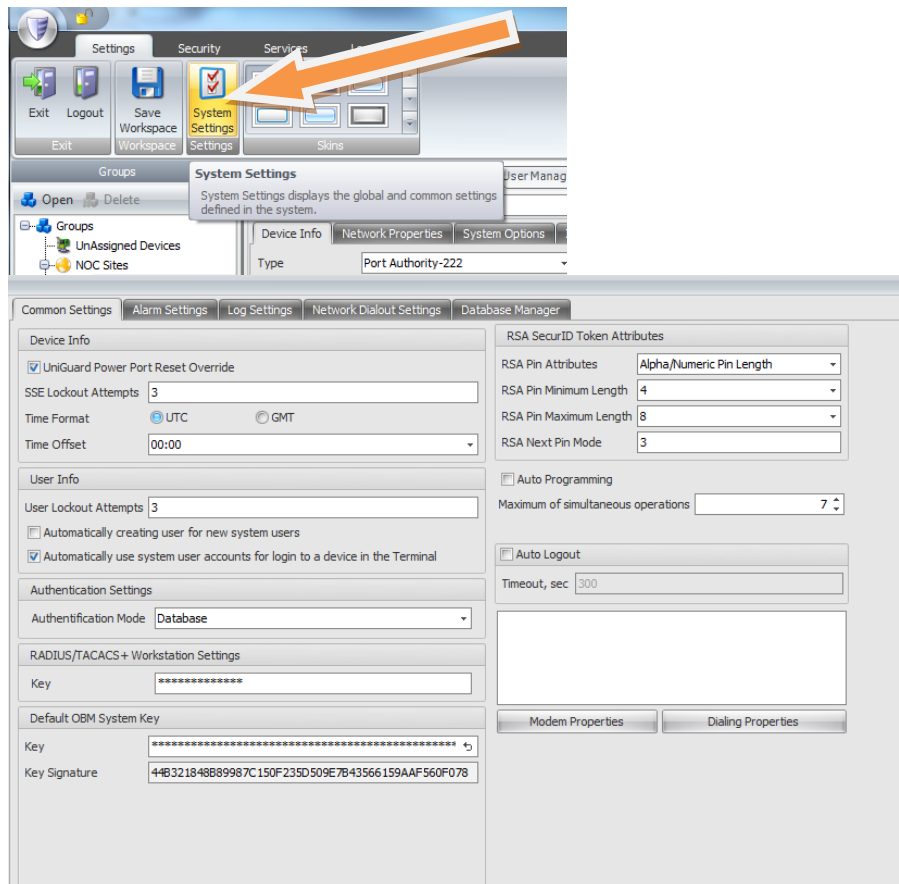
9 SYSTEM SETTINGS

The options of the Settings menu allow you to specify OBM system-wide settings and to perform system wide functions. .

The following topics are included in this section:

- Set global system settings such as auto programming, SNMP events, and user information
- Set up email alerts
- View the number of licenses used and available
- Set RSA SecurID token attributes
- Select log purge settings
- View network dialout item settings
- View RSA token list
- Perform certain database tasks
-

9.1 System Settings



UniGuard Power Port Reset Override: If enabled, the OBM will send a Reset command to the UniGuard device that has its Power IP Port Option set for Power Port mode. The default is disabled.

Warning!

This may trip the power control module if it is connected.

SSE Lockout Attempts: The number of times that a user can enter incorrect logon information while attempting to logon to an SSE device before being locked out of the SSE device. The default is 5. If set to 0, this feature is disabled.

User Info

User Lockout Attempts: The number of times that a user can enter incorrect logon information before being locked out of the system. The default is 5. To disable this feature, set User Lockout Attempts to 0.

Authentication Mode:

Authentication Methods

Database: Uses the information in the OBM database

Active directory: Uses active directory for authentication to the database.

RADIUS/TACAS+ KEY

Key for RADIUS or TACACS+ server.

Default OBM System Key

Key: When new groups are added, this default System Key will be the System Key for all new devices added to these respective groups.

IT IS STRONGLY RECOMMENDED TO CHANGE THE DEAFULT SYSTEM KEY TO PREVENT SYSTEM COMPROMISE.

Key Signature: The Key Signature of remote devices is compared with this Key Signature. If both signatures are the same then the keys will be the same.

RSA token attributes

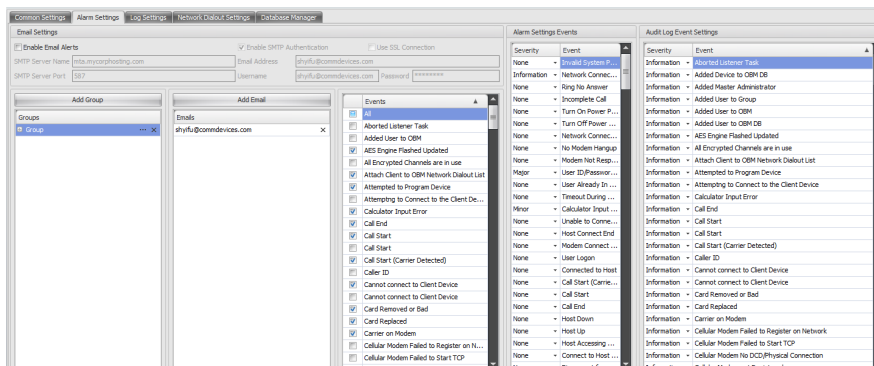
These are parameters for the RSA PIN.

Programming Setting

Auto Programming: When selected, a device will automatically be added to the programming queue when any change is made to the OBM that will need to be pushed out to the device. This could be any change to the device's system options, network settings, a user added to the group where the device resides, etc

Maximum of simultaneous operations: The Maximum number of simultaneous operations option allows the OBM to program multiple devices in the programming queue in parallel. This is limited by the number of resources the OBM has available to program devices. For instance if the maximum number of simultaneous operations is 3 and there are only 2 Network Dialout Clients, only 2 remote devices will be programmed at once.

9.2 Alarm Settings



9.3 Email Alerts

The Email Alarm Events tab contains the information used by the OBM to send email alerts. The OBM can email alarm alerts to the following:

- Specify email settings
- Alerts from all devices of to all users of a Group
- Alerts from specified devices to all users of a Group
- Alerts from all devices of all Groups to individual users

Example

For example email user John Doe1 has the following events defined.

User ID/Password Error

RSA Token Expired

And email user John Doe2 has the following events defined.

User ID/Password Error

Connected to an Invalid Device UniGuard.

And email user John Doe3 has the following events defined.

RSA Token Expired

Connected to an Invalid Device UniGuard.

This OBM Client sends a manual Reset Device or Program Device command to UniGuard device. When retrieving the audit trail from this device, a "User

ID/Password Error” event is received. An email will be sent to John Doe1 and JohnDoe2.

11/11/2004 11:11:00 Device Name User ID Port No. User ID/Password Error

Then an “RSA Token Expired” event is received. . This DDM Client will send out an email to John Doe3 and JohnDoe1.

11/11/2004 11:11:00 Device Name User ID Port No. RSA Token Expired

9.3.1 Email Settings

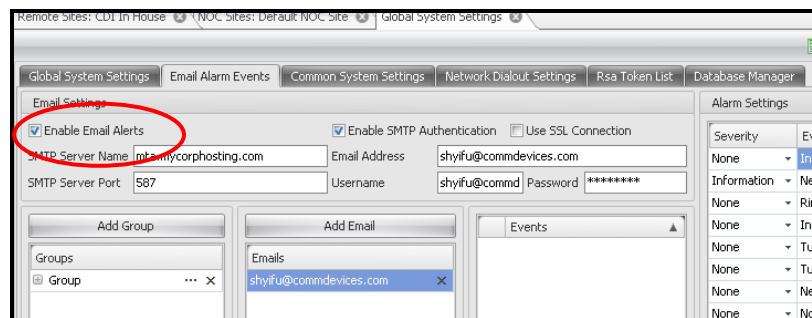
To receive alerts, Groups and users must already be listed in the Email Alarm Alert list for the OBM Client to send email alerts. To enable this feature, check the “Enable Email Alerts” box. The information displayed in this tab is used by the OBM to send email alarm alerts.

The Email Settings section is the information needed for this OBM Client to send out email alarm alerts.

SMTP Outgoing Server name and SMTP Port number (usually 25) parameters can be found in your Mail Account properties (ex. Microsoft Outlook or Netscape Mail).

Enable SMTP Authentication: If this is enabled (checked), then you will need your User Name (which can be found in your Mail Account properties) and email account password. The email password will be displayed as asterisks and is saved in encrypted format.

If the *Enable SMTP Authentication* checkbox is not checked, then the *Username* and *Password* fields are not used. The OBM Client will try to connect to the SMTP Server without security.



9.3.2 Adding a Group to receive alarms

To add a Group to receive alarms, click Add Group. The Email Group Settings window is displayed. Select either By Groups mode or By Devices mode.

By Groups:

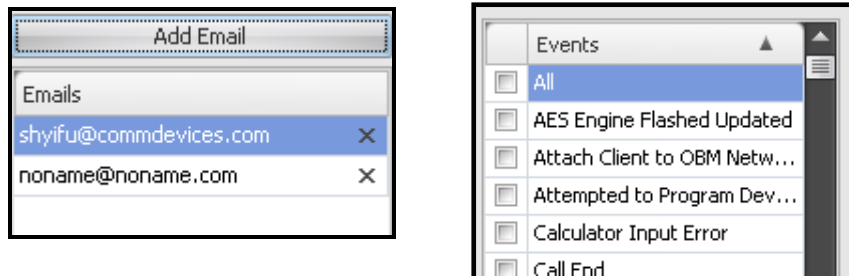
Select **All Groups** or the specific Groups to receive email alerts. You may also type in a Group name in Email Group Name field and select specific Events that will be email to users of that Group.

By Devices: Lets you select specific devices of selected Groups from which to receive alerts.

Click Apply when you are finished. To discard your entries, close the Add Groups window.

9.3.3 Adding an individual user

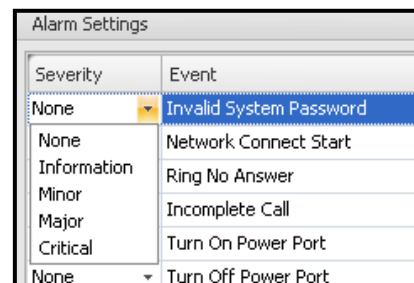
Enter the User Name and Email Address of the user who is to receive the alarms. From the Email Alarm List, select “All” to email all events to the user or select specific events. To add another user, click “Add Email.” Replace the sample address with the user’s address. In the Events list, select “All” to receive all events or select specific ones from the list.



TIP: Most mobile phone providers allow you to send SMS messages via email. It varies from provider to provider, but, one could configure the OBM to send an email to the appropriate address (as per the provider) which would then result in a text message going to your NOC engineer’s mobile phone.

9.3.4 Defining the Severity Level of an Event

The Alarm settings window enables you to set the severity level of an event. In the Severity column, click the down arrow of the event for which you want to assign a severity level.



9.4 Log Settings

9.4.1 Define OBM SNMP Events

These parameters enable you to specify the SNMP Manager's address(es) to which messages initiated by CDI devices will be sent.

SNMP Manager's IP Address 1: IP Address of the first SNMP Trap Receiver that you want the traps to be sent to.

SNMP Community Name 1: The Community string ("password") that the first trap receiver uses to validate traps.

SNMP Manager's IP Address 2: IP Address of the optional second SNMP Trap Receiver that you want the traps to be sent to.

SNMP Community Name 2: Community string that the optional second trap receiver uses to validate traps.

SNMP Manager's IP Address 3: IP Address of the optional third SNMP Trap Receiver that you want the traps to be sent to.

SNMP Community Name 3: Community string that the optional third trap receiver uses to validate traps.

SNMP Version: Select the version of SNMP trap that is being sent.

SNMP Event List: A list of all the possible SNMP traps that can be generated.

Event List box displays a list of possible SNMP events that can be monitored. To select an event that will be monitored, click the checkbox of the event. To remove an event, uncheck the checkbox of the event.

9.4.2 OBM RealTime Log Setting

You can enable or disable OBM RealTime logs.

OBM RealTime logs must be enabled for real-time logs in order to receive heartbeat messages or alarms. If real-time logs are not enabled, no heartbeat messages will be received even though the heartbeat attributes have been defined.

9.4.3 Custom Field Settings

You can make display the name field of 5 fields. To make it visible, click the checkbox adjacent to the field you would like to be visible.

9.4.4 Log Purge Settings

These fields let you set the number of days a log will be kept. To manually purge, click **Manual Purging** button. To purge the logs automatically each day at a specific time each, enable “Automatically purge log every day at.” You will have to enter a specific time. You can also enable Diagnostic Flash and Programming Log.

9.5 Common System Settings

This tab enables you to set parameters that are common for all groups and to view the number of used and available Seat licenses and EDL licenses. EDL licenses include Management, Network, AES256, SSM, Terminal and RSA.

Global System Settings | Email Alarm Events | Common System Settings | Network Dialout Settings | RSA Token List | Database Manager

Remote Sites: CDT In House | NOC Sites: Default NOC Site | Global System Settings

Add Licenses | Save Changes | Skip Change

License Type	Used	Available
UniGuard	19	4391
PortAuthority	34	4014
SSE	2	58

☒ RSA License

License Type	Used	Available
UniGuard	1	25
PortAuthority	6	138

☒ Seat License

OBM RealTime Log (300)

☒ Enable Key Stroke Log

Mode: Receive Only

Log Type: Text File

Text Log Folder: \\Natasha-m3509\\Temp\\CDI

Log Purge Settings

Log Type: SysLog

Maintain Log, days: 12

Manual Purge Log

☐ Automatically purge log every day at 12:00 AM

OBM Programming Log Settings

☒ Enable Diagnostic Flash and Programming Log

Information - Added Mast...
Information - Added User ...
Information - Added User ...
Information - AES Engine ...
Information - Attach Clie...
Information - Attempted t...
Information - Calculator I...
Information - Call End
Information - Call Start
Information - Call Start (C...
Information - Cannot con...
Information - Card Remov...
Information - Card Replaced
Information - Carrier on M...
Information - Changed M...
Information - Client Devic...
Information - Client Devic...
Information - Client ID Do...
Information - Core Port is i...
Information - Communicat...

9.6 Network Dialout Settings

The network dialout settings for a device selected from the list can be viewed in this tab. You also can enable AT Commands and set the number of consecutive failed attempts.

9.7 Network Dialout Settings

Group: All

Common Settings Alarm Settings Log Settings Network Dialout Settings Database Manager

Network Dialout Item Settings

Device Name PA111 - 36

Network Address 192.168.000.136

Status Idle

Extra AT Commands X4

Common Settings

Number of consecutive failed attempts 0

Device Name	IP Address	IP Port	Status
<input checked="" type="checkbox"/> PA111 - 36	192.168.000.136		Idle
<input checked="" type="checkbox"/> PA111 - 20	192.168.000.120		Idle
<input checked="" type="checkbox"/> PA111_114	192.168.000.114		Error
<input checked="" type="checkbox"/> PA111_112C	192.168.000.112		Error
<input checked="" type="checkbox"/> PA111 - 22	192.168.000.122		10001 Idle
<input checked="" type="checkbox"/> PA111 - 24	192.168.000.124		10001 Idle
<input type="checkbox"/> PA222 Client A	192.168.000.156		Idle
<input type="checkbox"/> PA222 Client B	192.168.000.159		Idle

9.8 Database Manager

The Database Manager tab has utilities that are used to backup, compact, and repair OBM databases. The Server Settings section lets you specify the SQL Server name, defined the backup folder for the network Security parameters, and define job settings.

Global System Settings Email Alarm Events Common System Settings Network Dialout Settings Rsa Token List Database Manager

Operations

- Backup
- Restore
- Update and Shrink
- Clear
- Server Logins

Server Settings

SQL Server

Server Name

☒ Windows Authentication

☐ SQL Server Authentication

Database NetworkSecurity

Backup

Folder

File Name NetworkSecurity.bak

Backup

Job Settings

☒ Save as Job

Name

Description

ID	Name
----	------

Add ...

Pick ...

Edit ...

Remove

10 REPORT MANAGEMENT

This section describes the reports listed below and how to customize them.

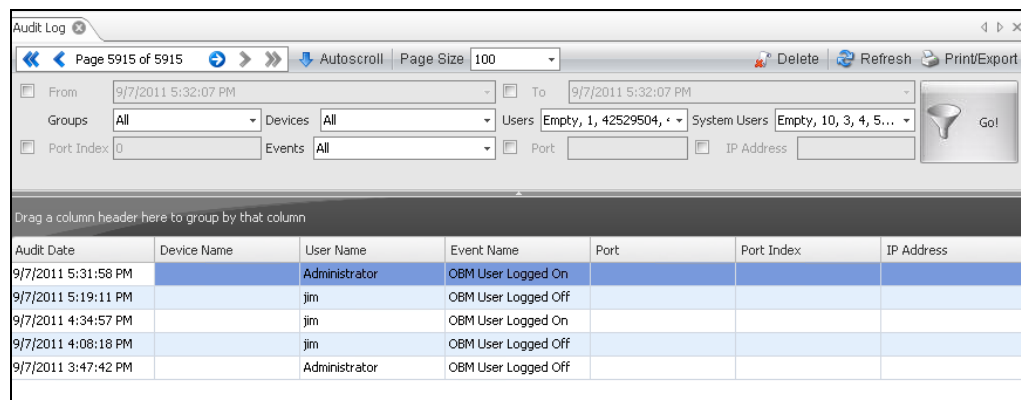
- OBM Audit
- Device Audit
- Custom Report
- Keystroke Log
- Device Status Report

10.1 OBM Audit

The OBM Audit is a report of OBM events, such as adding a user to a group, adding a device to the OBM database, deleting a user, and a user logging on or off. You may choose to filter the report by selecting specific devices, groups, or events, or date range.

Optional fields include Port, Port Index, and IP Address.

After you have made your selections, click **Go**.



The screenshot shows the 'Audit Log' window. At the top, it displays 'Page 5915 of 5915' and 'Autoscroll' is checked. The 'Page Size' is set to 100. There are buttons for 'Delete', 'Refresh', and 'Print/Export'. Below these are filter fields: 'From' (9/7/2011 5:32:07 PM), 'To' (9/7/2011 5:32:07 PM), 'Groups' (All), 'Devices' (All), 'Users' (Empty, 1, 42529504, ...), 'System Users' (Empty, 10, 3, 4, 5...), 'Port Index' (0), 'Events' (All), 'Port' (empty), and 'IP Address' (empty). A 'Go!' button is on the right. Below the filters is a table with the following data:

Audit Date	Device Name	User Name	Event Name	Port	Port Index	IP Address
9/7/2011 5:31:58 PM		Administrator	OBM User Logged On			
9/7/2011 5:19:11 PM		jim	OBM User Logged Off			
9/7/2011 4:34:57 PM		jim	OBM User Logged On			
9/7/2011 4:08:18 PM		jim	OBM User Logged Off			
9/7/2011 3:47:42 PM		Administrator	OBM User Logged Off			

10.2 Device Audit

The Device Audit includes information about devices and associated events. Events include "Host Down," "User Logon", "Next Pin Mode", and many others.

You can select specific devices, users, and events to be included in the report. Optionally, you can include Port, Port Index, and a date range. Both CDI and non-CDI devices can be included.

Device Audit Audit Log

Page 5915 of 5915 Autoscroll Page Size 100

From: 9/7/2011 6:20:24 PM To: 9/7/2011 6:20:24 PM

Groups: All Devices: All Users: Empty, 1, 42529504, 425295... System Users: Empty, 10, 3, 4, 5, 6, 7, 8... Go!

Port Index: 0 Events: All Port: IP Address:

Drag a column header here to group by that column

Audit Date	Device Name	User Name	Event Name	Port	Port Index	IP Address
9/7/2011 5:31:58 PM		Administrator	OBM User Logged On			
9/7/2011 5:19:11 PM		jim	OBM User Logged Off			
9/7/2011 4:34:57 PM		jim	OBM User Logged On			
9/7/2011 4:08:18 PM		jim	OBM User Logged Off			
9/7/2011 3:47:42 PM		Administrator	OBM User Logged Off			

10.3 Syslog

The Syslog report lists alarm events and facilities (processes) for selected devices.

Device Batch Log Syslog

Page 87 of 87 Autoscroll Page Size 100

From: 9/7/2011 6:49:48 PM To: 9/7/2011 6:49:48 PM

Message: Source Address: Go!

Severity: Alert: Action Must Be Taken, Critical Condition, Debug-Level Message, E... Facility: Authorization/Privacy, Clock Daemon, Clock Daemon 2, FTP Daemon, Kernel, Lin...

Drag a column header here to group by that column

Device Name	Source Address	Message	Date	Severity Code Name	Facility Code Name
PA111 - 20	192.168.0.120	DEVICE IS ALIVE	9/6/2011 12:27:43 PM	Informational Message	Log Audit
PA199 HOST 171	192.168.0.171	NO TELCO CONNECTION FOR ...	9/6/2011 8:26:06 AM	Informational Message	Kernel
PA111 - 22	192.168.0.122	NO TELCO CONNECTION FOR ...	9/6/2011 12:24:50 PM	Informational Message	Kernel
PA111 - 23	192.168.0.123	DEVICE IS ALIVE	9/6/2011 12:24:21 PM	Informational Message	Log Audit
PA111 - 36	192.168.0.136	DEVICE IS ALIVE	9/6/2011 12:25:05 PM	Informational Message	Log Audit
PA199 - 27	192.168.0.127	DEVICE IS ALIVE	9/6/2011 12:21:33 PM	Informational Message	Log Audit

10.4 Custom Report

You can create a Custom Report by selecting groups, devices, user ids, users and events. Optionally, you can include port index, port, and IP address.

Device Audit Device Batch Log Syslog Programming Log Audit Log Custom Report

Page 2 of 2 Autoscroll Page Size 100 New Filter11 Add Filter Delete Filter Save Filter Skip Changes

Last Days: 0 From: 9/8/2011 12:01:02 AM To: 9/8/2011 12:01:02 AM Go!

Group: CDI In House, Chevron, Documentati... Device: Empty, Access De... User ID: Empty, 1, 42529504 System Users: Empty, 10, 3, 4, 5, 6, 7, 8, 9, Administrat... Event: Added Device to OBM DB, Added ...

Port Index: 0 Port: IP Address:

Drag a column header here to group by that column

Date Time	Device Name	User Id	Event	Port	Port Index	User Name	Client Device	IP Address
9/16/2011 12:49:4...	Access Device		Dialing Device	DM				
9/15/2011 8:26:01...	Access Device		Communication Dro...	M				
9/15/2011 8:24:59...	Access Device		Dialing Device	DM				
9/15/2011 8:24:47...	Access Device		Communication Dro...	M				

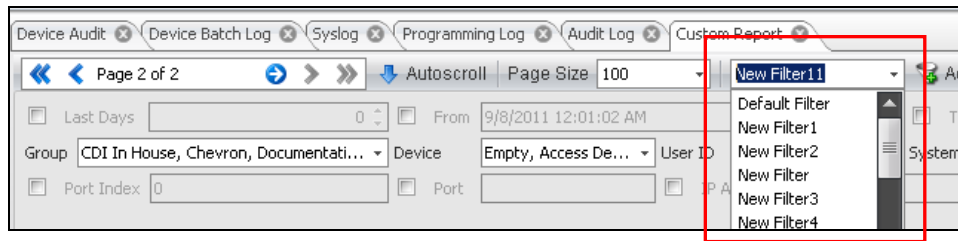
10.4.1 Adding a Filter

With custom reports, you can create and save a filter. A filter is criteria which will be used to select the items included in the report. A filter may be saved for use in the future.

1. To create a filter, click Add Filter. A system-generated name for filter is displayed. The name may be changed to something meaningful.
2. Select the criteria.
3. Click **Save Filter** to save filter. Click **Go** to run the report using the filter.

10.4.2 Deleting a Filter

To delete a filter, select the filter name from the drop down list. Click **Delete Filter**.



10.5 Keystroke Log

The keystroke log records all of the keystrokes issued to a device. It can be stored as a txt file, or within the database.

10.6 Deleting a Report

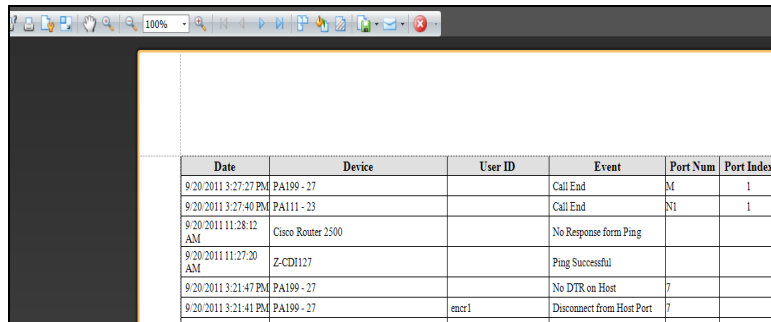
Click Delete to delete the report according to the filter. For instance, if you selected a specific date and time, then Delete would delete all entries in that date range.

10.7 Printing or Exporting a Report

A powerful export function is included in the OBM that allows almost all reports to be exported in a variety of formats included below. Reports may be printed, exported, or emailed.

- PDF
- HTML
- MHT
- RTF
- XLS
- XLSX
- CSV
- Text File
- Image File

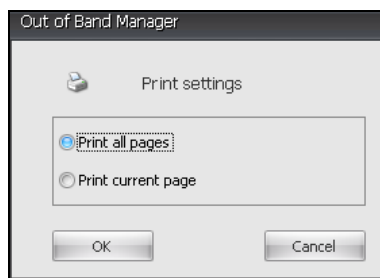
A sample report is shown below:



Date	Device	User ID	Event	Port Num	Port Index
9/20/2011 3:27:27 PM	PA199 - 27		Call End	M	1
9/20/2011 3:27:40 PM	PA111 - 23		Call End	N1	1
9/20/2011 11:28:12 AM	Cisco Router 2500		No Response form Ping		
9/20/2011 11:27:30 AM	Z-CD1127		Ping Successful		
9/20/2011 3:21:47 PM	PA199 - 27		No DTR on Host	7	
9/20/2011 3:21:41 PM	PA199 - 27	encr1	Disconnect from Host Port	7	

10.7.1 Printing a Report

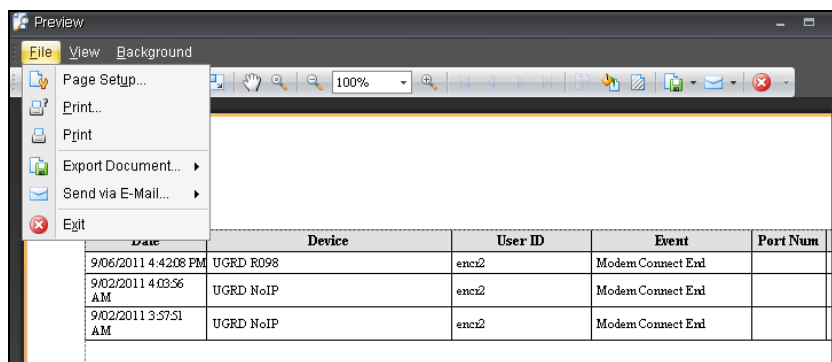
To print a report, click Print/Export. A window displays and you can select to print the current page or all pages.



After you make your selection, click OK. The Preview window displays. Click File, and then select **Print**.

10.7.2 Exporting a Report

In the Preview window, click File. Select Export Document and choose the File format. You will then need to enter additional information specific to the selected file format.



10.7.3 Emailing a Report

In the Preview window, click File. Select Email Document. Choose the File format. You will then need to enter additional information specific to the selected file format.

10.8 Report Filters Summary

Filter	Description	Applies to
Batch Commands	Select the batch commands to be included.	Device Batch Log
Devices	Select All or specific devices from the list. Click the down arrow to display a list of devices.	All except Syslog
Events	Select events to be included. Events include "Added User to Group" and "OBM Reboot."	OBM Audit, Device Audit, Custom
Facility	Click the down arrow to view of list of processes, and select those that are to be included in the Syslog.	Syslog only
From	The starting date and time. If an end date ("To") is not entered, all entries from the start date to the present date are included.	All log types
Groups	Select the Groups to be included. Click the down arrow to display a list of groups.	OBM Audit Log, Device Batch Log, Device Audit, Custom
IP Address	Enter the IP Address	Device Audit, OBM Audit Log, Device Audit, Custom
Last Days	Includes results from the previous n number of days	Custom Report
Message	Enter the message to filter the be included (such as "DEVICE IS ALIVE".)	Syslog only
Operation Name	Select the operation(s) to be included. Operations include Clear device, Program Flash Device, etc.	Programming Op Log
Port	Enter the number of the port to be included.	Device Audit, OBM Audit, Custom
Port Index		Device Audit, OBM Audit, Custom
Severity	Click the down arrow to view	Syslog only

Filter	Description	Applies to
	a list of alarms and select those to be included in the Syslog report.	
Source IP Address	The source IP address of the device	Syslog
Status	Select the status of the operation. Choices are Failed, Success, or All.	Programming Op Log
System Users	Select the users to be included. Click the down arrow to display a list of system users.	OBM Audit Log, Custom
To	The ending date and time. If a start date ("From") is not entered, all entries from the start date to the present date are included.	All log types
User ID	Select the user name	Custom report
User Name		
User Name	The name of the user who initiated the operation.	Programming Op Log
Users	Select the users to be included. Click the down arrow to display a list of users.	OBM Audit Log

11 POLLING SERVICE MANAGEMENT

This section describes how to set up, configure, and manage polling services. Polling Management is located in the Common toolbar.

11.1 About Polling Services

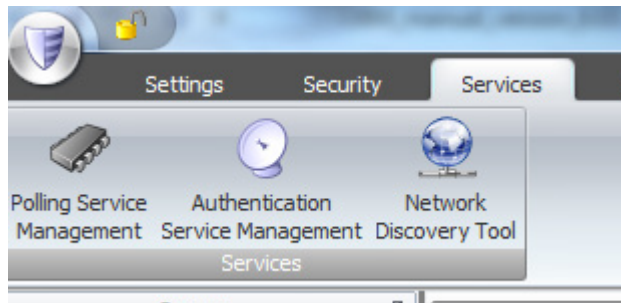
The OBM CDIPollingService can manage a maximum of 99 concurrent polling operations. Upon reaching a pre-defined schedule, it will automatically start the defined polling service.

:

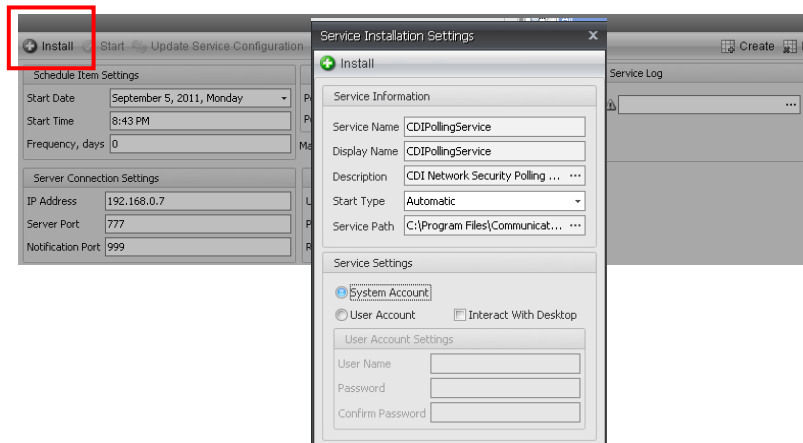
11.2 Setting up and Configuring the Polling Service

Before the Polling service can be scheduled, the service must be set up and configured. After the service is installed, you may set up the polling schedule. The service only has to be setup and configured once.

Click Polling Service Management in the Common toolbar.



The selected service tab opens. Click **Install** to setup and configure the service.



Service Name, Display Name, Description, and Service Path fields are filled in automatically by the system.

Start Type: Select the start type from the drop down list. The following are the available service types:

Automatic: Polling starts at system logon.

Manual: Polling starts as required or when called from an application.

Disabled: Disables the service and prevents it and its dependencies from running

Select the appropriate Service Setting:

System Account: The system account uses the local system account for the service. When System Account is selected, additional information is not required.

User Account: User account associates a polling service with a user. This account will need a password and confirmation of the password. The user must have been granted the appropriate rights.

Interact with Desktop: This box is typically checked if the service has user interface components.

When you have finished, click **Install**.

11.3 Scheduling Polling

After the service is installed, set up the polling schedule. To set up polling, click Polling Service Management in the Common toolbar. The Polling tab opens. Click **Create** to establish a new polling service.

The screenshot shows a window titled 'Update Service Configuration' with a toolbar at the top containing 'Install', 'Start', and 'Update Service Configuration' buttons. The window is divided into several sections:

- Schedule Item Settings:** Includes 'Start Date' (September 5, 2011, Monday), 'Start Time' (8:43 PM), and 'Frequency, days' (0).
- Select Mode:** Includes 'Poll By Groups' (selected), 'Poll By Devices', and 'Maximum number of concurrent operations' (1).
- Enable Service Log:** A checkbox that is checked, with a 'Log File' field below it.
- Server Connection Settings:** Includes 'IP Address' (192.168.0.7), 'Server Port' (777), and 'Notification Port' (999).
- System User credentials:** Includes 'User name', 'Password', and 'Role' fields, each with a warning icon.

Schedule Item Settings

Start Date: Select the date that polling is to start.

Start Time: Enter the time in local time that polling is to start. The format is hh:mm AM or PM

Frequency, days: Enter how often, in days; the polling is to take place.

Server Connection Settings

The following information is needed so that the service can communicate with the OBM server.

IP Address: Enter the IP address of the OBM server

Server Port: Enter the OBM server port number.

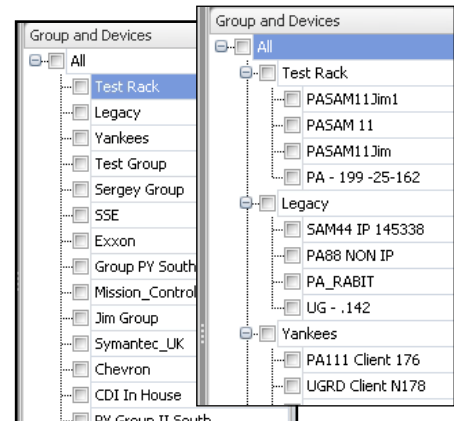
Notification Port: Enter the notification port number. This must match the notification port set in the server configuration.

Select Mode

Polls By Groups: Select this option to choose the groups to be polled by this service. When this mode is selected, a list of Groups is displayed. Click the checkbox of each Group you would like to poll.

Poll By Devices: Select this mode to choose the devices to be polled. When this mode is selected, the Groups and Devices pane displays devices by Group. Click the checkbox of each device you would like to poll.

Maximum number of concurrent operations: The maximum number of polling operations that can occur at the same time.



System User Credentials

Only systems users with the appropriate roles may request the polling service.

User Name: Enter the name of the user requesting the polling service. The user must have been granted the appropriate rights.

Password: Enter the password of the user.

Role: Select the Role from the drop down list.

Enable Service Log: Click to enable the service log.

When you have finished, click **Save** to save your changes.

11.4 Authentication Management

The screenshot displays the 'Authentication Management' window. On the left, a tree view shows the hierarchy: Groups, Sites, Remote Sites, and Client Devices. Under 'Remote Sites', several locations are listed, including ATLANTA_PA222, CHICAGO_PA_222, DALLAS_PA_211, NEW_YORK_PA244x, and SAN_FRAN_PA-288. The main panel shows the configuration for the 'Radius' service. The 'Server IP Address' is set to 127.0.0.1. The 'Network Interface List' is empty. The 'Use like Proxy Server' checkbox is unchecked. The 'Remote Server IP Address' is also 127.0.0.1. The 'Services' section has 'Radius' selected, with a 'Port' of 49. The 'User Name Prompt' is 'Username:' and the 'Password Prompt' is 'Password:'. The 'Enable Service Log' checkbox is checked, and the 'Log File' is 'RadiusServiceLog.txt'.

Authentication Service Management Network Discovery Tool Services

Groups
Delete
Signed Devices
Sites
Commercial Operations ...
Government Operation...
E_WIDGET_CO
Remote Sites
ATLANTA_PA222
CHICAGO_PA_222
DALLAS_PA_211
NEW_YORK_PA244x
SAN_FRAN_PA-288
Client Devices
Users
Ports
_OF_USA
Remote Sites
126 Boston
127 Pittsburgh 16
128 Dallas

NOC Sites: Commercial Operations Center User Management Roles

Uninstall Start Update Configuration

Settings

Server IP Address 127.0.0.1

Network Interface List

☐ Use like Proxy Server

Remote Server IP Address 127.0.0.1

Services

Tacacs+ Radius

Port 49

User Name Prompt Username:

Password Prompt Password:

☒ Enable Service Log

Log File RadiusServiceLog.txt

11.5 Network Discovery Tool

The screenshot displays the 'Network Discovery Tool' window. The top tabs include 'NOC Sites: Commercial Operations Center', 'User Management', 'Roles', 'Token Management', 'Remote Devices: 126 Boston', and 'Global System Settings'. The main panel is divided into 'Network Discovery Settings' and 'Schedules'. The 'Network Discovery Settings' section has 'IP Address From' and 'IP Address To' both set to 127.0.0.1. The 'CDI Devices Only' checkbox is unchecked, while 'Ping Required' and 'Automatic Save' are checked. The 'Connections' table lists four connections: Browser (Port 80), Telnet (Port 23), SSH (Port 22), and CDI Device (Port 9999). The 'Schedules' section is empty. At the bottom, a table header shows columns for Status, Network Address, Device Name, Mac Address, and Description.

NOC Sites: Commercial Operations Center User Management Roles Token Management Remote Devices: 126 Boston Global System Settings

Uninstall Stop Update Scan Now

Network Discovery Settings

IP Address From 127.0.0.1

IP Address To 127.0.0.1

☐ CDI Devices Only

☒ Ping Required

☒ Automatic Save

Connections

	Name	Port
<input checked="" type="checkbox"/>	Browser	80
<input checked="" type="checkbox"/>	Telnet	23
<input checked="" type="checkbox"/>	SSH	22
<input checked="" type="checkbox"/>	CDI Device	9999

Schedules

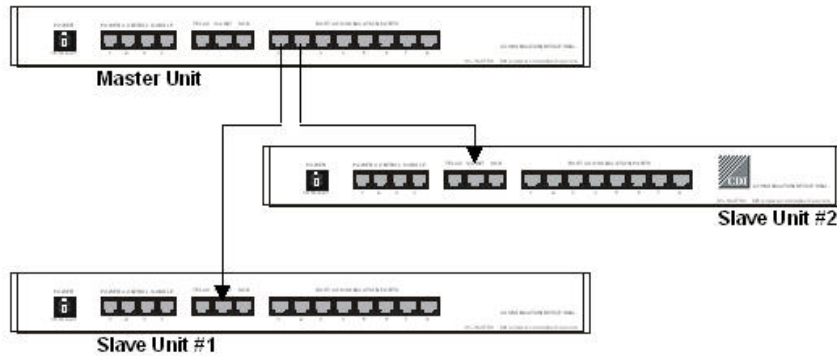
IP Address From	IP Address To	Start Time
-----------------	---------------	------------

Status Network Address Device Name Mac Address Description

APPENDIX A Cabling Diagrams

Port Authority Master-Slave Cabling Diagrams

The cable connection shows a Master Port Authority connected to two Port Authority Slave units. The interconnecting cables, Part # CBL CAT5 Yellow, are yellow to distinguish them from other cables can be obtained from CDI.



NOTE MAINT (Maintenance) port is changed to Serial Port (this is a running change).