
Fiber Commander™

v 2.4.3



User's Guide



HIGH PERFORMANCE ■ HIGH RELIABILITY ■ HIGH SECURITY

© Copyright 2018, Fiber SenSys®, Inc. Printed in the United States of America. All rights reserved worldwide. No part of this publication may be copied or distributed, transmitted, stored in a retrieval system, or translated in any form or by any means, electronic, mechanical, magnetic, manual, or otherwise, without the express written permission of Fiber SenSys, Inc.

This manual is provided by Fiber SenSys, Inc. While reasonable efforts have been taken in the preparation of this material to ensure its accuracy, Fiber SenSys, Inc. makes no express or implied warranties of any kind with regard to the documentation provided herein. Fiber SenSys, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Fiber SenSys, Inc. to notify any person or organization of such revision or changes.

Windows® is a registered trademark of Microsoft Corporation.

Fiber SenSys® is a registered trademark of Fiber SenSys, Inc.

All other trademarks are properties of their respective owners.

Fiber SenSys, Inc.
2925 NE Aloclek Dr.
Suite 120
Hillsboro, OR 97124
USA

Tel: 1-503-692-4430
Fax: 1-503-692-4410

info@fibersensys.com
<http://www.fibersensys.com>

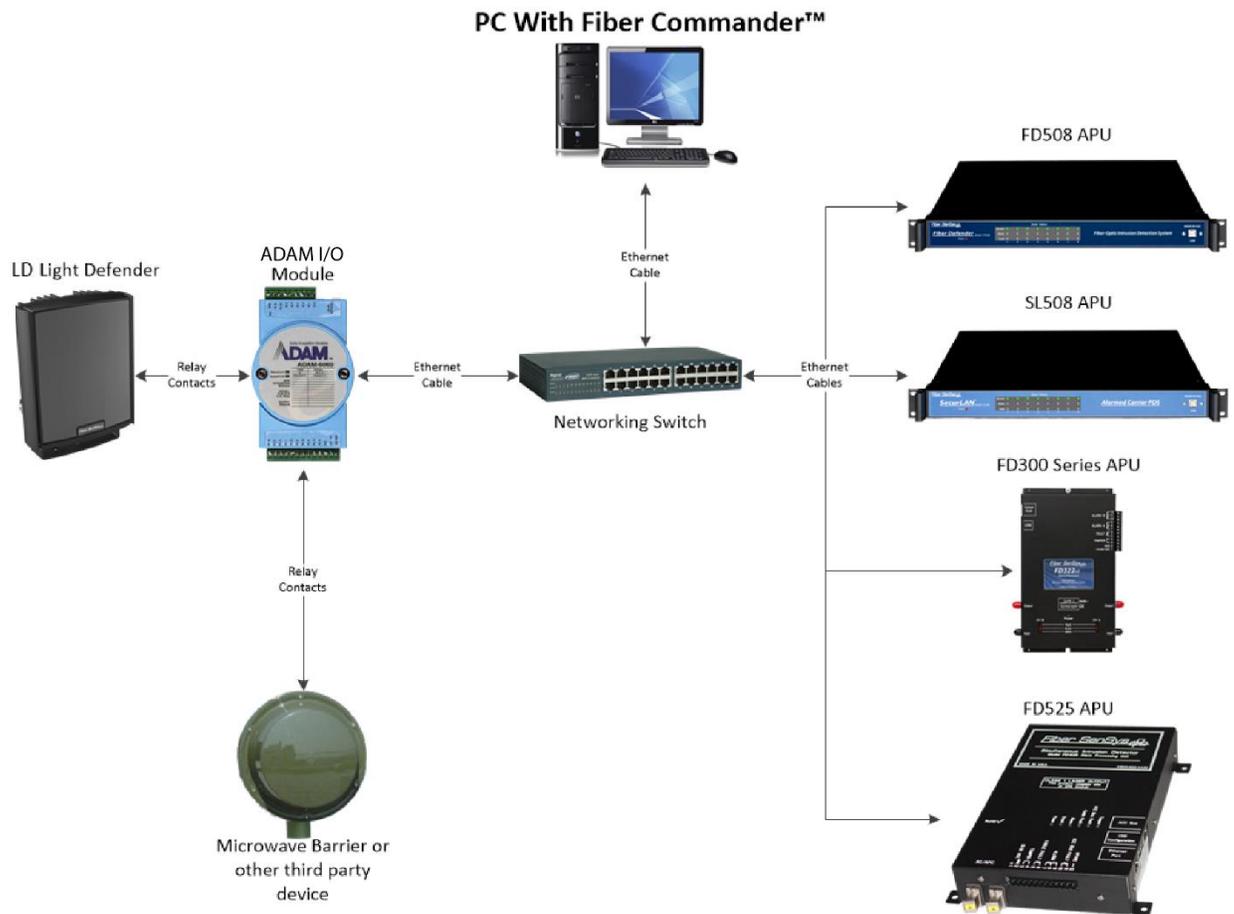
Table of Contents

1.	Introduction	3
2.	Features	4
3.	Installation	5
4.	Initial setup	6
	Choosing a different map	6
	Choosing a different alarm sound	7
	Login	7
	Configuring TCP/IP enabled APUs for use with Fiber Commander	8
	Configuring Fiber Commander to accept APU connections	8
	Configuring ADAM 6060 Devices for use with Fiber Commander	11
	Configuring ADAM 6060 Devices	14
	Setting up Output Mappings	15
5.	Main display	17
	Device Tree	18
	Inputs Tab	19
	Outputs Tab	19
	Testing Output Devices	20
	I/O Map Tab	20
	Map configuration	21
	Event handling	22
	Acknowledging	22
	Unmanned Mode	22
	Operator notes	23
	Operator instructions	25
	Controlling APU outputs (300 series only)	26
6.	Alarm Shunting	27
	Manual shunting	27
	Scheduled shunts	28
7.	Event reporting	30
	Log generation	30
	Backup scheduling	31
	Log file format	31

- Backup to optical media32
- 8. Account management.....33
 - Policies.....33
 - Accounts34
 - Creating groups & users.....34
- 9. Troubleshooting.....36
- 10. Product specifications.....39
- Appendix A – Configuring Windows Firewall40
 - Windows 10:.....40
 - Windows 8 and 8.1:.....41
 - Windows Vista and Windows 7:.....42
 - Windows XP.....42
- Appendix B – Communicating with FSN-based APUs.....44
 - Self-test for FSN units46
 - Troubleshooting FSN problems47
- Appendix C – Monitoring Sixnet-based managed networks49
 - Configuring Sixnet Switches.....53

1. Introduction

Fiber Commander™ is a head end that provides integration, command, and control for perimeter security systems. With Fiber Commander you can monitor Fiber SenSys alarm processors (APUs) via TCP/IP (using the ICD-0100 protocol). You can also control the APUs, monitor third-party sensors via general-purpose inputs, and easily upgrade/expand your system.



2. Features

Fiber Commander™ offers the following features:

- Customizable visual and audible alarms
- Customizable map display (using BMP, JPG, GIF, and PNG images) with zoom and pan
- Record alarms (multiple copies if desired) in non-volatile memory
- Store alarm acknowledgements and other operator activity in non-volatile memory
- Schedule creation of event reports on optical media (CD/DVD/BD)
- Create/support multiple log in levels; define policies for each level
- Change settings remotely on IP-enabled units.
- Use the relay outputs on 300 series APUs to actuate equipment upon alarm and user acknowledgement.
- Require operators to type an explanation before they acknowledge/clear an alarm
- Pre-define zone-specific operator instructions in the event of an alarm
- Save system configuration, allowing setup sequences to be skipped upon restarting
- Use ADAM-6060 units to trigger alarms
- Use ADAM-6060 units as output devices. They can be configured to activate various devices such as flood lights and cameras.
- Monitor the status of the TCP/IP network when using Sixnet managed switches.
- Can be put in “*Unmanned Mode*” where Fiber Commander will automatically acknowledge alarms.

3. Installation

- Insert the Fiber Commander CD. The installation wizard will start automatically. Alternatively, browse the CD and install Fiber Commander manually using “setup.exe”

Follow the instructions on the screen to complete the installation.

The folder “\Resources\Lantronix” contains software necessary for setting up TCP/IP-enabled APUs for use with Fiber Commander. Refer to the APU manual for information on configuring an APU and attaching it to your network.

The “\Resources\Advantech” folder contains the necessary software for configuring ADAM-6060 units for use with Fiber Commander. Refer to the ADAM-6060 manual for more information on configuring ADAM units.

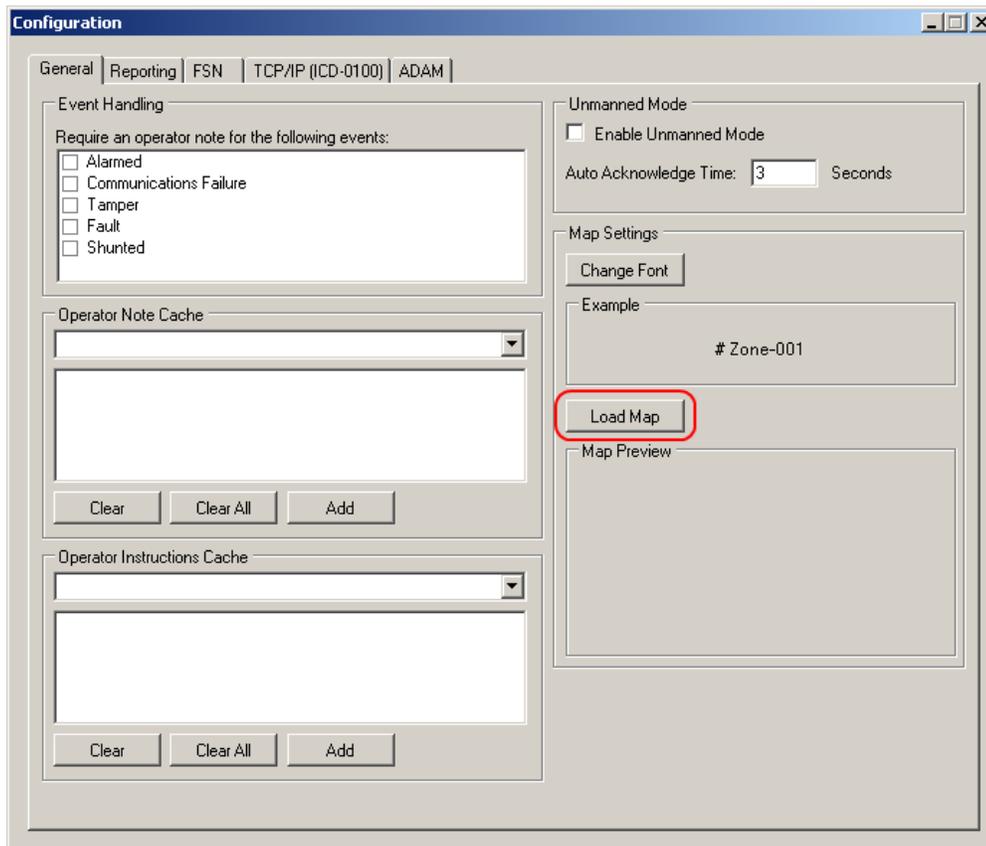


NOTE: If the computer is restarted, Fiber Commander will launch automatically. To prevent this, delete the shortcut “*Fiber Commander*” from the Windows Start menu under “*Start\Programs\Startup.*”

4. Initial setup

Choosing a different map

The map for Fiber Commander can be changed in the configurations page.



Click load map and browse to a map of your choice. Supported map files are BMP, GIF, JPG, or PNG. For best performance the map file should be less than 10MB or the pan & zoom operations may be too slow.

Choosing a different alarm sound

The alarm sounded by Fiber Commander is from a file called “Alarm.wav” in the installation folder (default location: “C:\Program Files\Fiber SenSys\Fiber Commander”). To change the alarm, delete “Alarm.wav” and replace it with a new file of the same name containing an alarm sound of your choice.

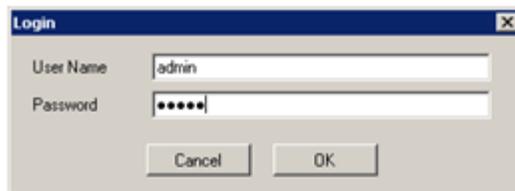
Once all equipment is configured, start Fiber Commander via the shortcut (shown below) on your desktop.



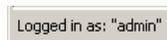
When Fiber Commander starts it will always log the user in with the default “guest” account. This account only allows you to watch the screen. To configure the system and to access the configuration page, log in as administrator.

Login

To log in as administrator, go to the “File>Login” menu and enter “admin” for User Name and “admin” for Password. This is a standard account which is created when Fiber Commander is first installed. The password should be changed after the initial installation by using the “Account Manager.” See the “Account management” chapter for more details.



The current user is identified in the lower left corner of the screen:



Configuring TCP/IP enabled APUs for use with Fiber Commander

For an APU to connect to Fiber Commander over the IP network the APU must be configured to connect to the workstation that is running Fiber Commander. The APU needs to know the IP address of the workstation running Fiber Commander and on which TCP/IP port Fiber Commander is listening for the APU (default is 10000).

Please refer to the *APU Networking Application Note (AN-SM-009)* for instructions on configuring the APUs to make “Outgoing” connections to Fiber Commander.



CAUTION: Network security products, such as Windows Firewall, must be configured to allow TCP/IP enabled APUs to communicate with Fiber Commander. See Appendix A – Configuring Windows Firewall for more information.

Configuring Fiber Commander to accept APU connections

Within Fiber Commander, go to the menu “*Options\Configuration*” and select the “*TCP/IP (ICD-0100)*” tab.

Initially, make sure the “*Lock*” and “*Enable APU Server*” checkboxes are disabled.

Enter the port number you want Fiber Commander to listen for APUs on (default is 10000). Make sure the port number you enter is not in use by any other application. The ping interval determines how often each unit is interrogated by Fiber Commander. An involuntary disconnect (e.g. through a communications cable disconnect or power failure) will be detected within 2x this time period. Valid entries are 1 to 60 seconds. The smaller this number the more work the system will have to perform, which might become a problem when there are many units connected and the system hardware or network bandwidth is limited. Make sure you use a number which is acceptable for your application.

Enable the APU listen server by ticking the box “*Enable APU Sever*” in the lower left corner.

Configuration

General | Reporting | FSN | TCP/IP (ICD-0100)

```

5/12/2010 9:22:57 AM <-Incoming From<- (172.22.17.6) : PlatformStatusReport
5/12/2010 9:22:57 AM: ->Outgoing To-> (172.22.17.6) : Ping
5/12/2010 9:22:57 AM <-Incoming From<- (172.22.17.6) : PlatformStatusReport
5/12/2010 9:22:57 AM <-Incoming From<- (172.22.17.6) : DeviceConfiguration
5/12/2010 9:22:58 AM <-Incoming From<- (172.22.17.6) : DeviceConfiguration
5/12/2010 9:22:58 AM <-Incoming From<- (172.22.17.6) : CommandMessage

```

IP-Communication Settings

Port Number: 10000

Ping Interval [s]: 10

Enable APU Server

Connection Management

Remove Lock

Status	IP Address	APU Name
	172.22.17.6	APUNAME

Each unit which is configured to connect to Fiber Commander will show up in the IP Connections box. The status of each connection is indicated as follows:

- Socket connection established, but pinging has not commenced (a handshake needs to be performed first, as specified by the ICD-0100 protocol)
- Connected and pinging successfully
- Not connected (a ping timeout or a socket error occurred)

The APU name displayed in the “*IP Connections*” box is retrieved from the APU itself. In Fiber Commander you can assign a local alias to rename a device. To change the actual APU name, please refer to the individual APU manual.

When checked, the “*Lock*” checkbox prevents any new unit (a unit which is not listed yet) from connecting to FC.

The “*Remove*” button deletes any unit which is not connected.



CAUTION: When a device is deleted in the “*IP-Connections*” list, all related information like operator notes, aliases, I/O mappings, and map-icon placement information is also erased.

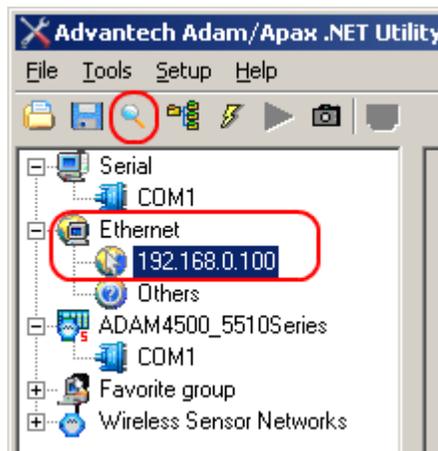
Configuring ADAM 6060 Devices for use with Fiber Commander

The Advantech ADAM Utility is used to configure ADAM-6060 units for use with Fiber Commander. The Advantech ADAM Utility is included on the Fiber Commander install CD in the “\Resources\Advantech” folder.



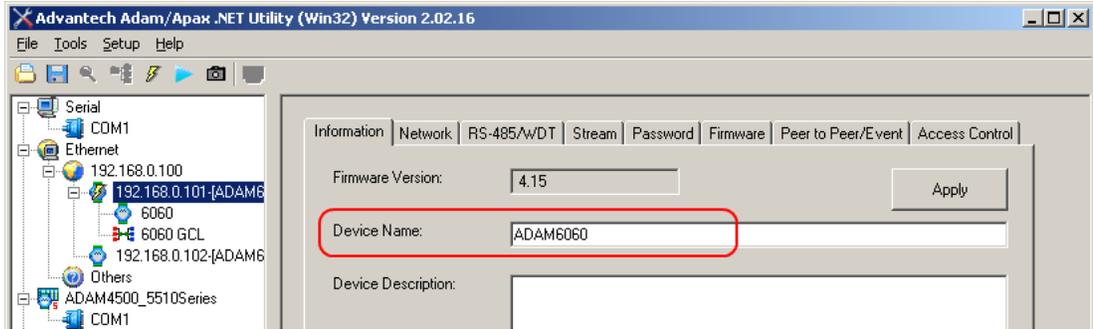
CAUTION: Network security products must be configured to allow ADAM 6060 Devices to communicate with Fiber Commander. See Appendix A – Configuring Windows Firewall for more information.

To configure an ADAM unit, first open the Advantech ADAM Utility and select the Ethernet item in the tree; then press the scan button that looks like a magnifying glass.

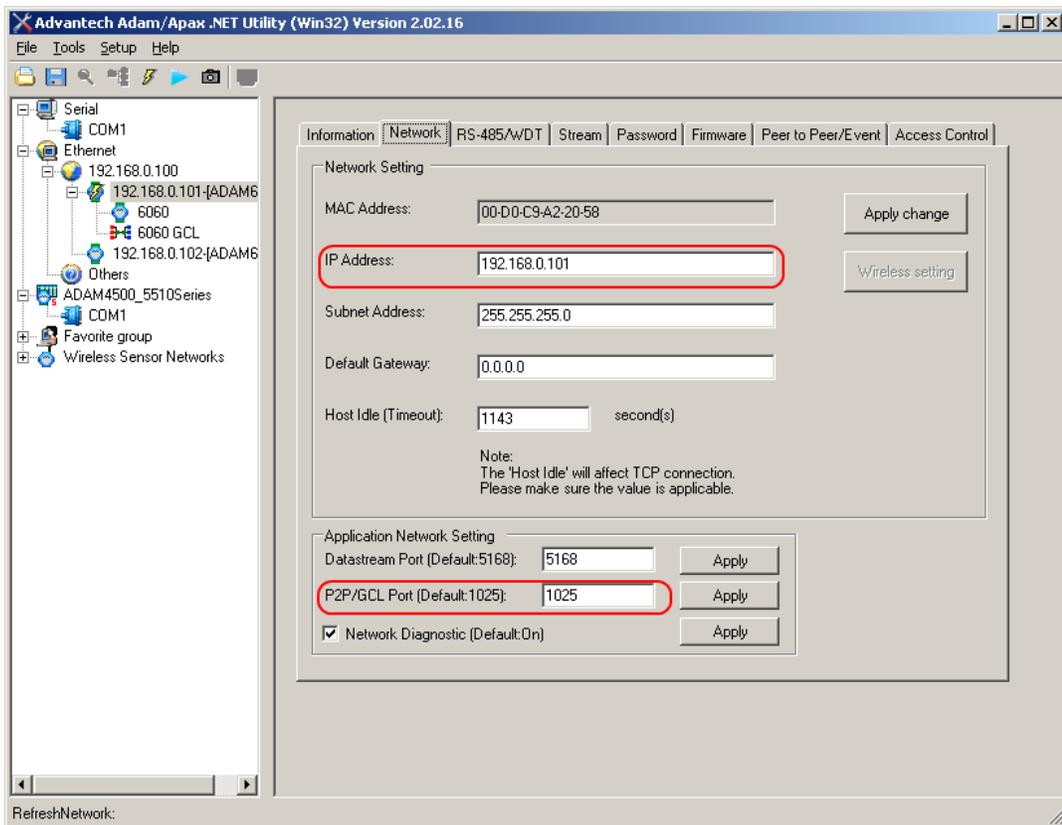


Once the list of ADAM devices is displayed, select one to change its settings. All ADAM units must be on the same subnet as the workstation running Fiber Commander and each ADAM must have a unique IP address. If the ADAM unit appears under the “*Others*” icon, then its IP address is set to a different subnet than the workstation. Change its IP address to one that is on the same subnet as the workstation before continuing. The Advantech ADAM Utility may require a password before settings on an ADAM unit can be changed. The default password is eight zeros: “00000000”.

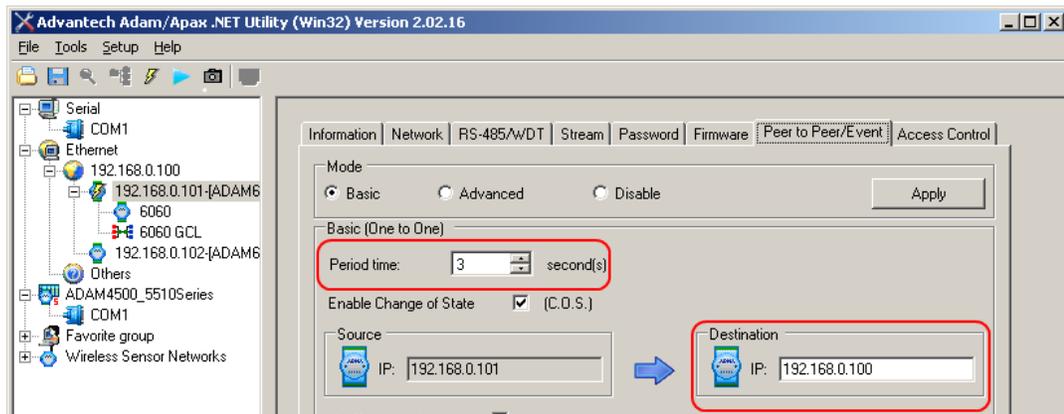
First, set the Device Name in the “Information” tab. Once the ADAM and Fiber Commander are configured, this name will show up in Fiber Commander device lists and menus.



Next, set the IP address and P2P/GCL port in the “Network” tab. Each ADAM must have a unique IP address. The default P2P/GCL port is 1025. All ADAM units must use the same P2P port and Fiber Commander must be configured using the same P2P port. See the next section on how to configure Fiber Commander’s ADAM P2P Port.

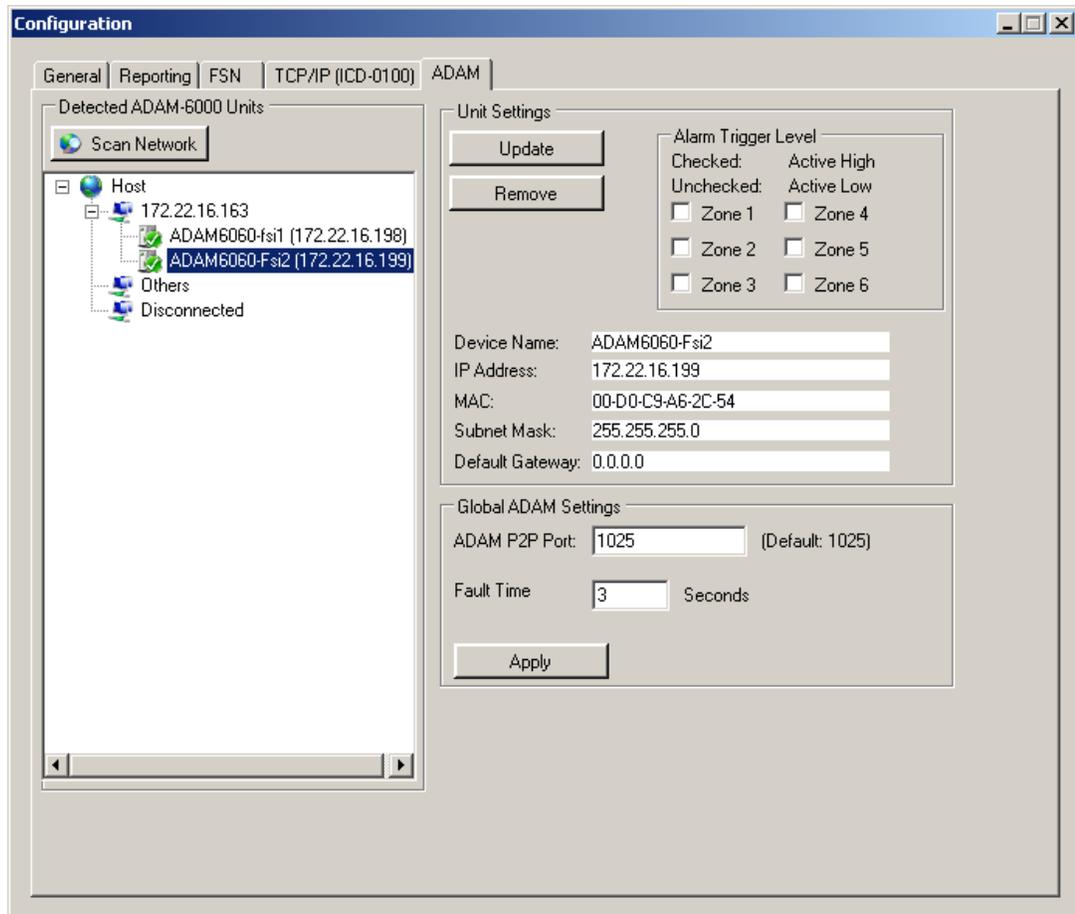


Finally, configure the ADAM's Peer to Peer/Event settings in the "Peer to Peer/Event" tab. The destination IP address must be set to the IP address of the workstation running Fiber Commander. The "Period time" setting is how often each ADAM unit will communicate with Fiber Commander. All units must have the same broadcast time and Fiber Commander's fault time in the ADAM settings must also be set to this value. See the "Configuring ADAM 6060 Devices" section for setting Fiber Commander's ADAM fault time. Faster broadcast times can detect an unplugged unit faster but put more strain on the network and the workstation running Fiber Commander. The time setting has no effect on how fast Fiber Commander responds to changes on the digital inputs or how fast it can manipulate the relays. Once the "Period time" and the destination IP address have been changed, press the "Apply List" button to save the changes.



Configuring ADAM 6060 Devices

The ADAM tab in the configuration dialog brings up the settings page for ADAM devices.



The Global ADAM Settings set the ADAM Peer-to-Peer port and the fault time. The P2P port and update times must be the same as set on the ADAM units. After the P2P port or fault time has been changed, click the “Apply” button to save the changes.

To add ADAM units to Fiber Commander, first press the “Scan Network” button. This will search the network for ADAM devices. When the scan is complete, the list brings up all ADAM units on the network, showing their IP address and name. Select an ADAM unit to view its properties, such as the name, MAC address, IP address, and other information. Units that Fiber Commander is monitoring have a green check next to their icon and units that are currently disconnected have a red X next to their icon.

The “Alarm Trigger Level” boxes control whether a logic high (+Vcc) on the ADAM digital input is considered an alarm, or if a logic low (GND) should be considered an alarm.

Selecting the “Add” button will add the unit to Fiber Commander as both an input device and output device.

To add an ADAM unit, select it, set each input as either active high or active low, and press “Add”.

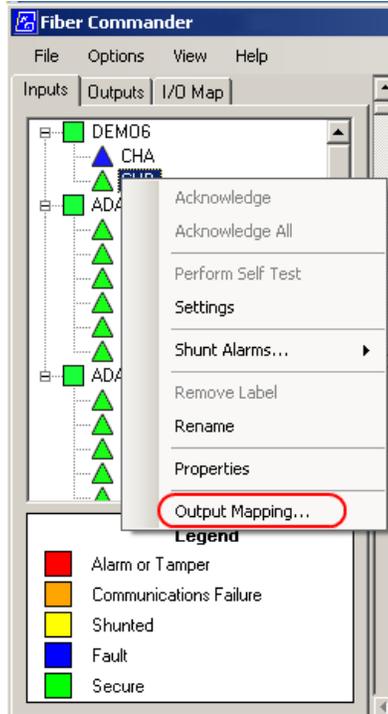
To remove an ADAM unit from Fiber Commander, select the unit and press “Remove”. This will tell Fiber Commander to stop monitoring the unit. Any output mappings associated with the ADAM unit will also be deleted.



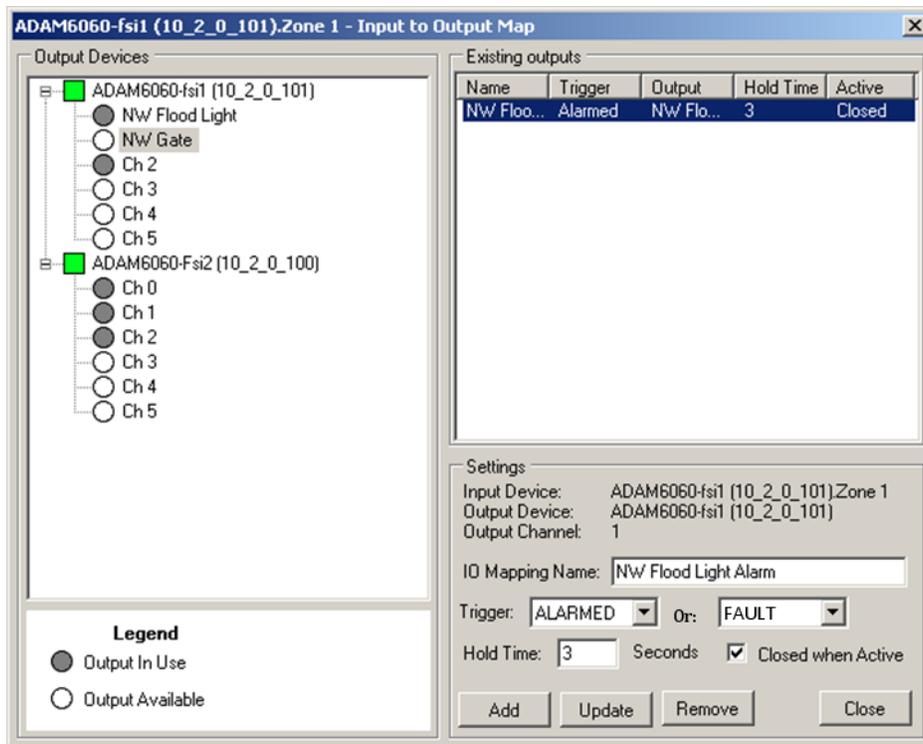
CAUTION: When a device is removed, all related information like operator notes, aliases, I/O mappings, and map-icon placement information is also erased.

Setting up Output Mappings

Fiber Commander can use ADAM-6060 units as output devices. When an alarm or other event occurs, relays on the ADAM-6060 units can be configured to engage or disengage. This feature is called “Output Mappings”. To setup a new output mapping, right-click on the desired input device that will cause the trigger and select “Output Mapping”. This will open the “Input to Output Map” dialog.



The input to output map dialog is used to assign output relays to activate on different conditions, such as an input zone going into alarm. Each output can only be used with a single mapping. After an output is in use, it is unavailable for other IO mappings.



To add a new output map, first select the output device to use. Next, enter a descriptive name such as "NW Flood Light". Then select what will trigger the output. You can select two types of triggers. Each can be Alarm, Fault, or other triggers. Setting a hold time will keep the output active for the given time after the event has been acknowledged (whether by the operator or by unmanned mode). The "Closed when Active" box determines if the relay closes as a response to the event, or if it opens as a response to the event. Finally, click "Add" to add the new output mapping.

Output devices that are currently in use and therefore unavailable for a new mapping are shown with gray icons. Available output devices have white icons.

5. Main display

Once the input and output devices are configured, the Configuration window can be closed. The main display has a list of devices and zones (called the device tree) along the left-hand side of the display, a map in the center right, and alarm information along the bottom (see the representative figure below).

Time	Device Name	Event Description	Device ID	Operator
5/12/2010 9:55:08 AM	FC	COM1: Polling network nodes. (expecting 3)	FC	admin
5/12/2010 9:50:13 AM	APUNAME	Ping interaction begun	APUNAME (172.22.17.6)	admin
5/12/2010 9:50:09 AM	Ethernet port: "10000"	IP connection made	172.22.17.6:10000	admin
5/12/2010 9:50:07 AM	Ethernet	'Start XML Listening' activated by operator	Ethernet port: "10000"	admin
5/12/2010 9:50:03 AM	FC	Logged in as: "admin"	FC	admin

The device tree shows the system configuration and provides access to all device functions.

The following symbols represent the different types of devices in a TCP/IP network:

-  APUs
-  Hyperzones (500 series only)
-  Zones

The event window, at the bottom of the screen, displays alarm status and other system information including most actions the operator has performed. This enables the operator to review the event history and to debug the system as needed.

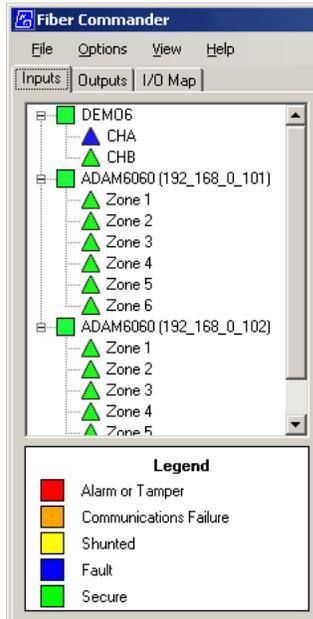
The bottom left of the screen shows the overall system status and quick links to often-used controls such as “Silence and Acknowledge all.” This gives a highly visible and quick view of the system status (“secure” versus “alarm”) without having to look at the details.

The map has zoom and panning features. Panning is done by dragging the map around or using the scrollbars at the bottom and right. Zooming is done with the mouse scroll-wheel or with the scrollbar in the top left.

Device Tree

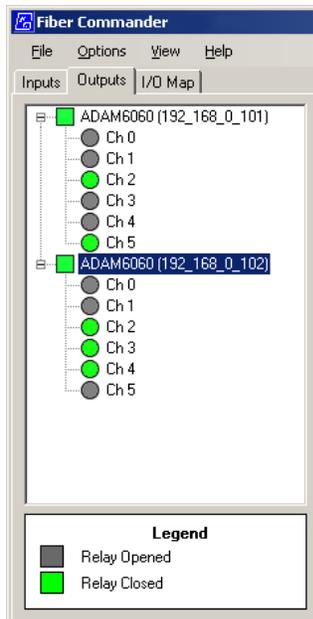
The device tree has three tabs. The “*Input*” tab shows the input devices, the “*Output*” tab shows the output devices and the “*I/O Map*” tab shows the output mappings.

Inputs Tab



The input devices tab shows all the input devices and their status.

Outputs Tab

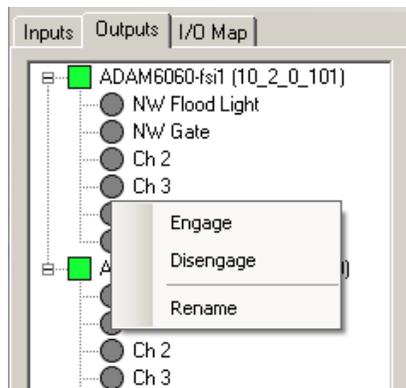


The output devices tab shows the output devices and their status. A gray icon indicates the output relay is open and a green icon indicates the output relay is closed.

Individual output channels can be renamed by right clicking on the channel and selecting “Rename”.

Testing Output Devices

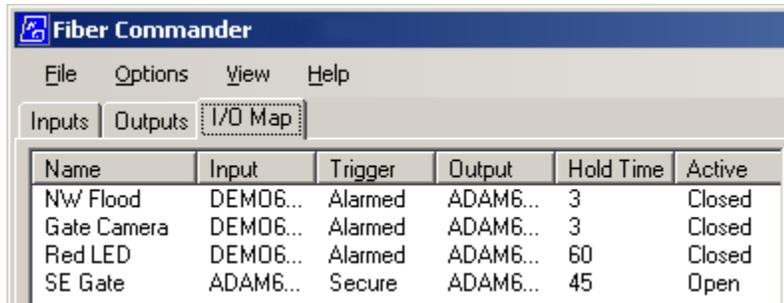
For testing purposes, output devices can be manually activated and deactivated by right clicking on them and selecting “Engage” or “Disengage”. The user who is currently logged in must have “*manual output device operation*” permissions to engage or disengage the outputs.



The device will remain engaged or disengaged until it is manually activated again or an event occurs that causes an output mapping to change the state of the output.

I/O Map Tab

The “*I/O Map*” tab shows all the configured output mappings. In this tab one can easily see the details of each output mapping.



Name	Input	Trigger	Output	Hold Time	Active
NW Flood	DEM06...	Alarmed	ADAM6...	3	Closed
Gate Camera	DEM06...	Alarmed	ADAM6...	3	Closed
Red LED	DEM06...	Alarmed	ADAM6...	60	Closed
SE Gate	ADAM6...	Secure	ADAM6...	45	Open

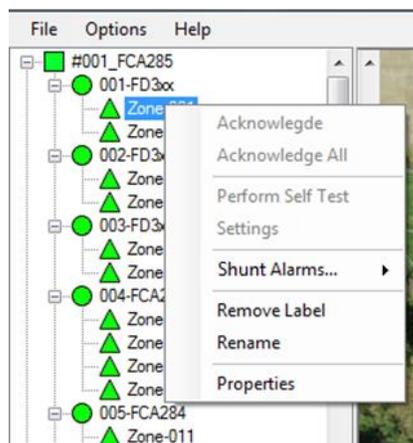
To edit an output mapping, right click on it and select “*Output Mapping*”. This will bring up the Output Mapping dialog.

Name	Input	Trigger	Q
NW Flood	DEM06...	Alarmed	A
Gate Camera	DEM06	Alarmed	A
Red Light	Output Mapping...		
SE Gate	ADAMB...	Secure	A

Map configuration

Fiber Commander can be configured to display a map. The map can be changed in the configuration settings. See “Choosing a different map” for more details. The display can also be augmented to show the locations of zones and sensors. To do this, drag the zone/device from the device tree to the appropriate location on the map.

To rename a zone or device, right-click on it in the device tree and select “Rename.” Type in the desired name and enter. A zone or device can only be dragged and dropped on the map once. To remove a label from the map, select the “Remove Label” option in the same menu.



CAUTION: While the system allows you to enter duplicate device and zone names, this is not advisable.



NOTE: When you click on a unit or a zone (in the device tree) that has been previously dragged to the map, a label with information about the zone will come into view, flashing blue and white for a few seconds to draw your attention to it.

Event handling

During normal operation, when an event such as an alarm or a user logging in occurs, the events are chronologically listed in the event window.

The type of event is displayed in the column labeled “Event Description”. When the event is an Alarm, Communication Failure, Sensor Fault or Tamper, the audible alarm sounds and the main display (if minimized) is maximized. If a label for this device or zone was placed on the map, it will be centered and start flashing. The operator must acknowledge these events to return the system to “Secure” status.

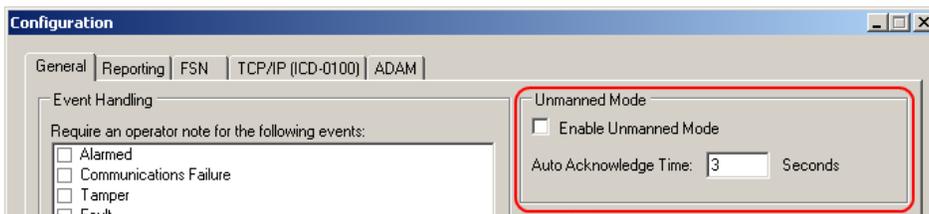
Time	Device Name	Event Description	Device ID	Operator
5/20/2010 10:27:56 AM	APUNAME	FAIL	APUNAME (172_22_18_180)	admin
5/20/2010 10:27:56 AM	172.22.18.180	No response from unit located at IP address: 172....	APUNAME (172_22_18_180)	admin
5/20/2010 10:27:38 AM	CHA	Acknowledged Alarm	APUNAME (172_22_18_180) .CHA	admin
5/20/2010 10:27:35 AM	CHA	ALARM	APUNAME (172_22_18_180) .CHA	admin
5/20/2010 10:27:24 AM	CHA	Acknowledged Alarm	APUNAME (172_22_18_180) .CHA	admin
5/20/2010 10:27:21 AM	CHA	FAULT Recovered	APUNAME (172_22_18_180) .CHA	admin
5/20/2010 10:27:20 AM	CHA	FAULT	APUNAME (172_22_18_180) .CHA	admin
5/20/2010 10:26:44 AM	Zone-004	Shunt Reset	#001_FCA285.001-FCA284.Zone-004	admin
5/20/2010 10:26:34 AM	Zone-004	User note: wer	#001_FCA285.001-FCA284.Zone-004	admin
5/20/2010 10:26:32 AM	Zone-004	Shunted for always	#001_FCA285.001-FCA284.Zone-004	admin
5/20/2010 10:26:06 AM	APUNAME	Ping interaction begun	APUNAME (172_22_18_180)	admin
5/20/2010 10:25:45 AM	FC	IP listen server started	FC	guest

Acknowledging

To acknowledge an alarm, right-click the label on the map or the device in the device tree and click “*Acknowledge*.” You may also use “*Acknowledge All*” to acknowledge all events simultaneously.

Unmanned Mode

In unmanned mode, alarms and other events are acknowledged automatically. This allows Fiber Commander to be used unattended. To enable unmanned mode, click the “*Enable Unmanned Mode*” box in the configuration menu.



The “*Auto Acknowledge Time*” is how long Fiber Commander waits after an event before acknowledging it. Unmanned mode can be useful when Fiber Commander

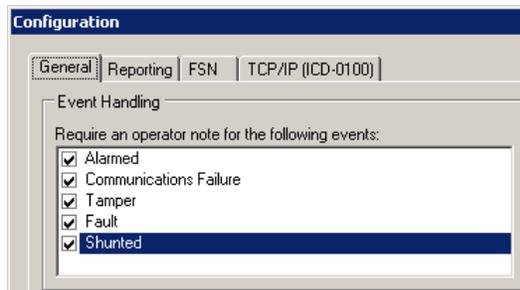
is used with output devices. For example, by using the output mapping feature, an output can be toggled when an alarm is triggered. With unmanned mode enabled, Fiber Commander will automatically acknowledge the alarm and will be ready for the next alarm.



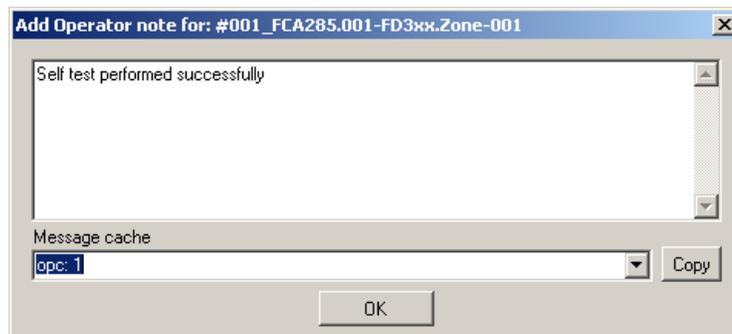
CAUTION: Unmanned mode completely automates Fiber Commander and takes precedence over requiring operators to enter notes for events.

Operator notes

Administrators can configure Fiber Commander to require a written explanation before an operator can clear certain types of events (see figure below). To exercise this option, go to the menu “Options\Configuration” and select the first tab “General.”



When an event of the specified type occurs, while the option is set, the following dialog box appears:

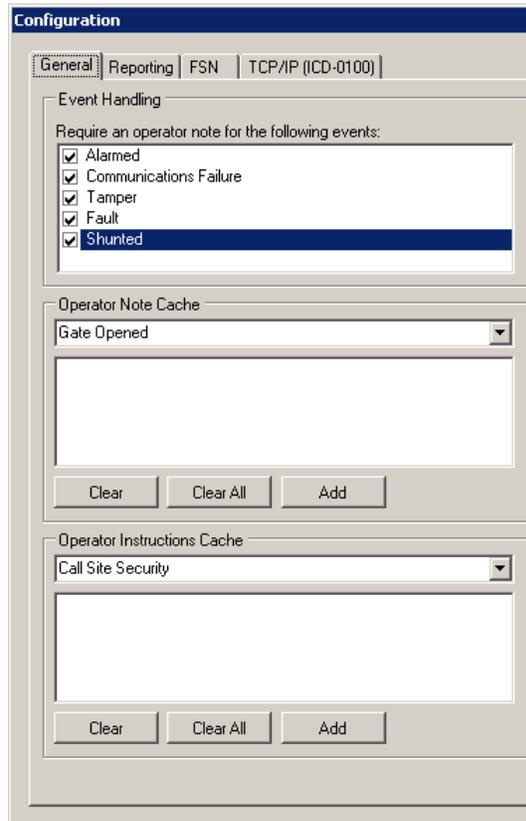


To clear the event, the operator must enter a written explanation. The “Message cache” stores these notes in a drop-down list.



NOTE: To enter a note from the drop-down list, click the “Copy” button after a message from the drop-down list is selected.

The list of stored operator notes can be maintained in the Configuration dialog on the “General” tab as shown:



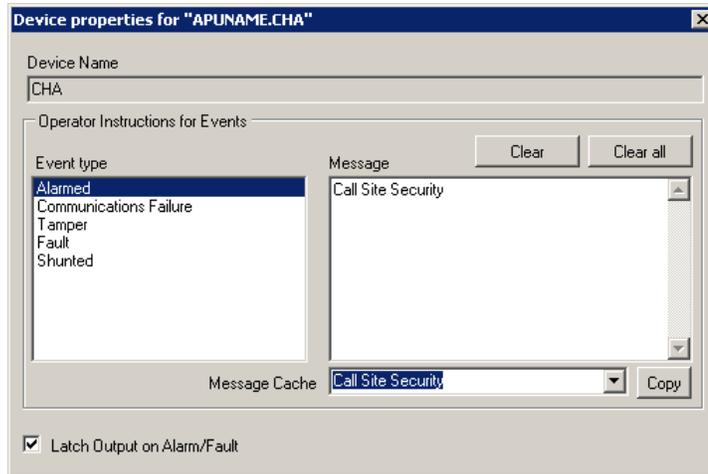
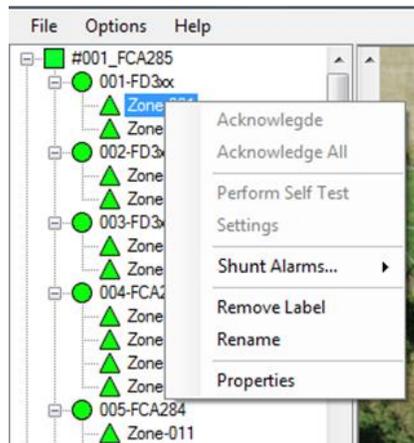
NOTE: When the “*Acknowledge All*” option is used, only one operator note has to be entered instead of one for each item.

Operator instructions

“Operator instructions” give directions to the operator when they acknowledge an event. These instructions are entered (per unit and event type) by right-clicking a device in the device tree and selecting “Properties.”

There is a message cache at the bottom of the dialogue box that helps to speed the processes of entering the same instructions for multiple devices.

The “Clear” button clears the current event message, and “Clear All” clears the messages for all event types.



CAUTION: The device messages and notes are only manually saved via the menu option “*Options\Save System Configuration*” or at the prompt when exiting Fiber Commander.

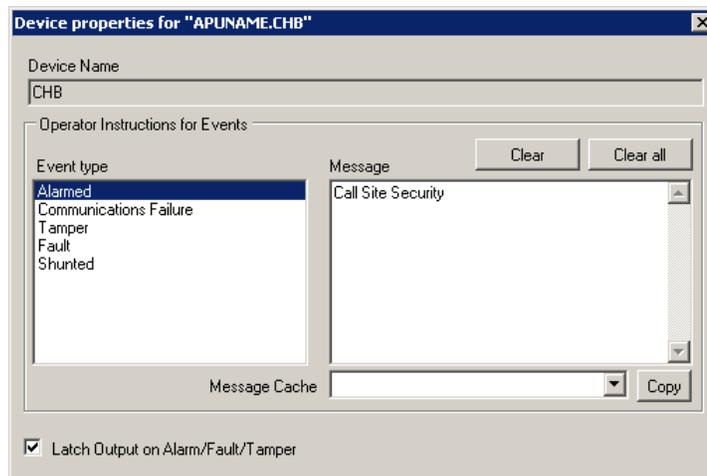
Controlling APU outputs (300 series only)

For 300 series APUs, Fiber Commander can be configured to control the alarm output (and APU control is disabled) relays on the APU itself. This feature might be used in combination with Fiber SenSys' optical cutoff switch, floodlights, or sirens. When this feature is used, the output is latched until the alarm is acknowledged.



NOTE: The relay which is toggled is always the one corresponding to the relevant channel (e.g. when enabled on channel B on a FD342-IP, relay output "Alarm B" will go active when an alarm occurs). If you need more control over relay activation, use an ADAM-6060 unit instead.

To enable the feature, right-click the unit's zone and select the checkbox "Latch Output on Alarm/Fault/Tamper".



When first enabled, Fiber Commander will change a setting in the APU, "User Controlled Relay Mode" such that it gains control over the relays.



NOTE: To change the relay functionality to the default, use the APU settings option explained in the next chapter and set the option "User Controlled Relay Mode" back to "False".

6. Alarm Shunting

Fiber Commander can be told to shunt certain inputs. For example, you may wish to shunt the input from a gate that is being left open and manually guarded. You can also set up a schedule to control automatic shunting.

When a zone is shunted, alarms or faults on that zone will not be reported. When an APU is shunted, tamper conditions will not be reported; however, communications failures will be reported and alarms and faults on the APU's zones be reported.

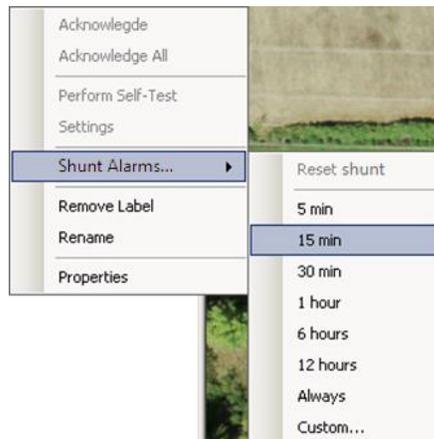


CAUTION: After the configuration is changed (e.g., devices renamed, labels placed on the map, devices shunted) it is necessary to save the configuration manually via the menu option “*Options\Save System Configuration*” for Fiber Commander to retain the settings after a restart.

Manual shunting

To shunt an input, right-click the appropriate zone (or APU) and select one of the shunting options from the menu. The device icon will change to yellow in the device tree.

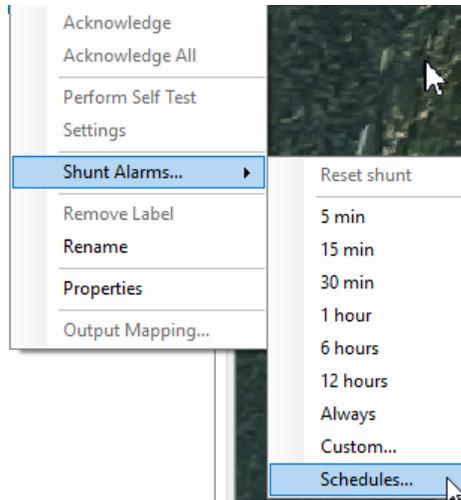
If any timed options are selected, the device tree will show a countdown timer for that device. The option “Custom...” allows you to enter any amount of time from one second to 24 hours. The option “Always” will shunt the device permanently. It will remain shunted until reset with the “Reset Shunt” option.



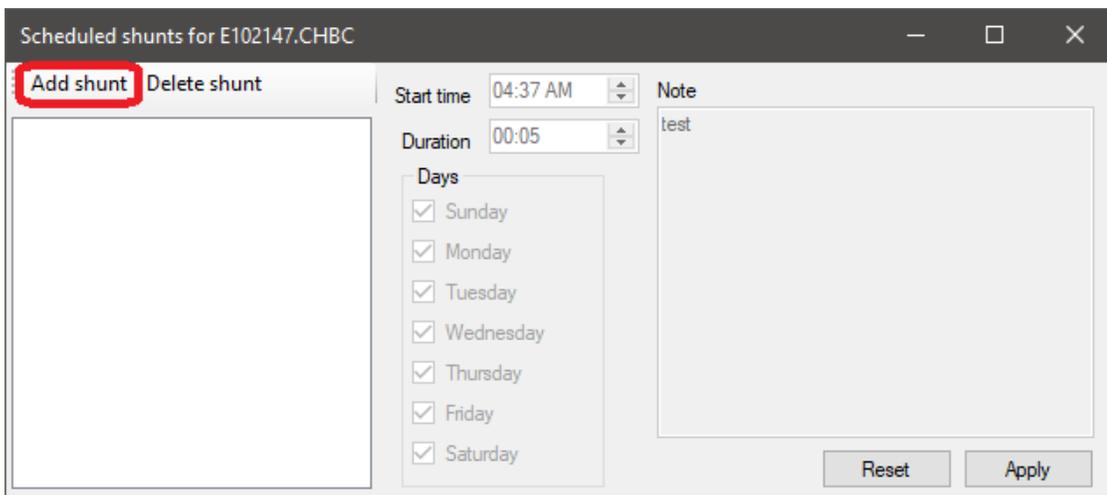
If a shunt is in progress (whether manual or scheduled) and a new manual shunt is started, the manual shunt duration will override the current duration.

Scheduled shunts

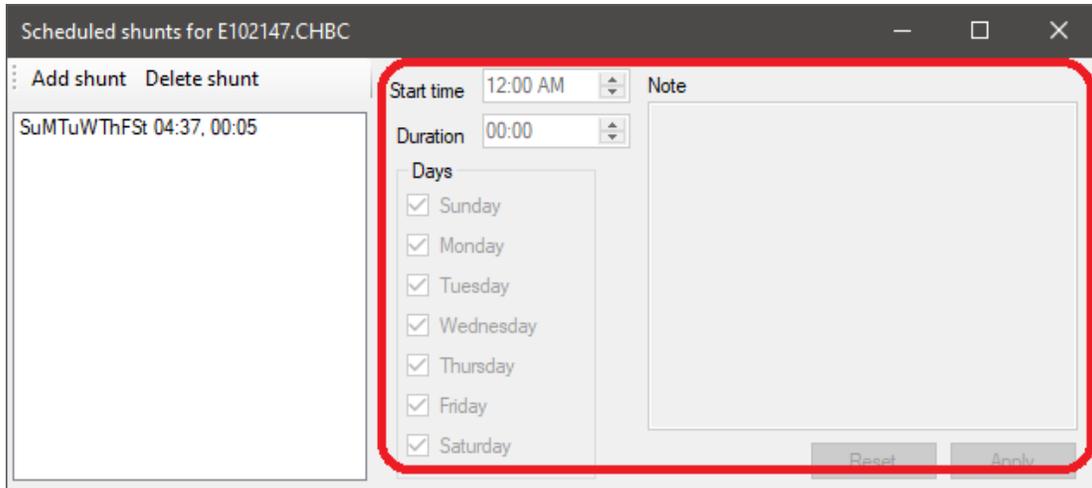
Shunting can also be automatic, based on a schedule. To begin, select a zone (or APU), and select the “Schedules...” item.



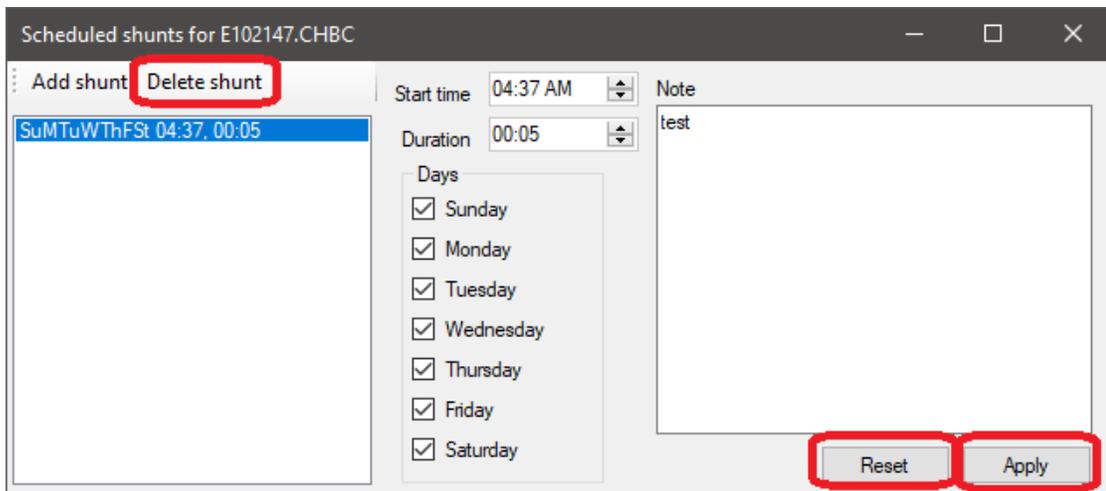
This will pop up the shunt scheduler window for that zone (or APU). The first time you do this, no shunts have been scheduled, so you will need to press “Add shunt” to create a new shunt.



When a shunt is selected, you can change the start time and duration for the shunt. If the duration is zero, no shunting will occur. The shunt will only operate for the selected days in the week. If no days are selected, no shunting will occur. You must press “Apply” to modify the shunt schedule. This is to prevent shunts for occurring while you are still editing the shunt.



The panel on the left contains the list of scheduled shunts for the selected input. The list contains a shorthand for the days in the week, start time, duration and operator note. To edit the entry, select it, make the changes, and press “Apply”. To discard your changes, press “Reset”. To delete the entry, press “Delete shunt”.



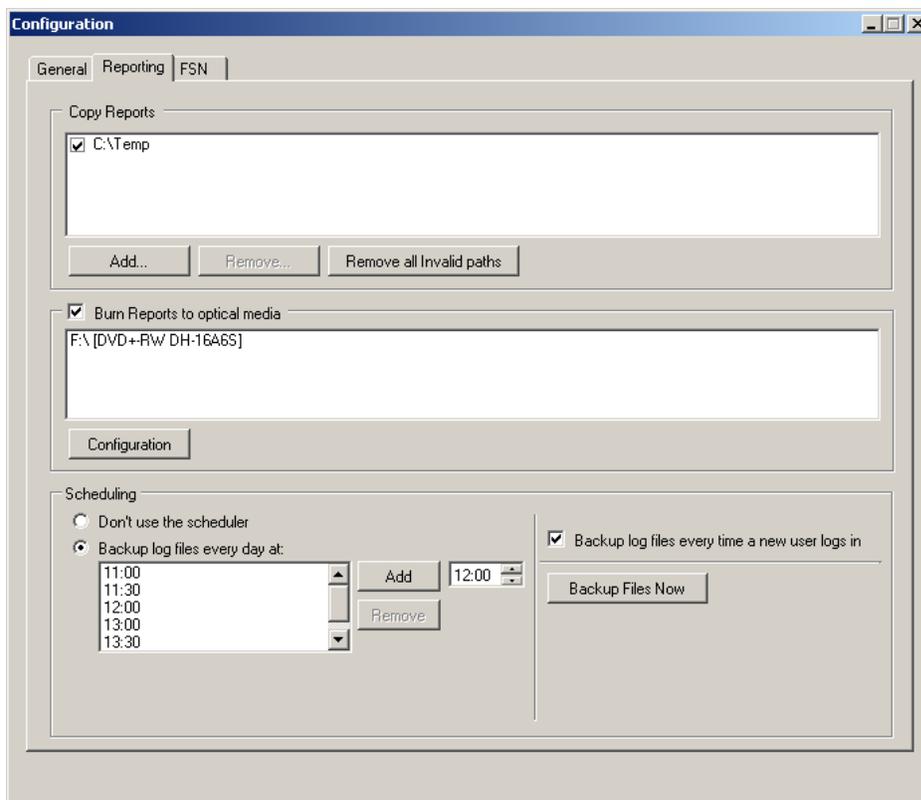
CAUTION: If a shunt is active when it is deleted from the schedule, this does not reset the active shunt. If you do not want the shunt to remain active, if you must reset it manually.

7. Event reporting

Log generation

Upon defining a suitable path to the hard drive, Fiber Commander automatically logs event data in the file FC_Log_ddmmmyyyy_hr_mm_ss.txt , where dd = day of the month, mmm = month of the year, yyyy = year, hr = hour, mm = minute, and ss = second.

The data on the hard drive can be backed up multiple times daily to an optical drive using the “Reporting” tab in the “Options\Configuration” dialog. After a file is backed up from the hard drive to an optical drive, Fiber Commander starts a new log file in the same directory on the hard drive.



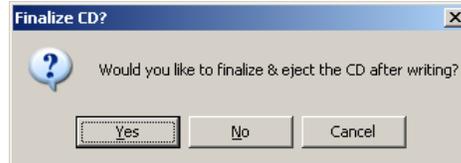
Multiple paths to the hard drive can be listed, where log files are stored. If no events occur the log file is still backed up, and the file simply contains the date and time it was created. This allows you to verify that the system is operating properly.



CAUTION: No log files will be written to the hard drive if there is no file path in the “Copy Reports” section.

Backup scheduling

Backups can be generated at set times every day by adding backup times to the schedule list. A new log file will be created in each directory listed in the “Copy Reports” section, and the old log file will be closed. When the checkbox “Backup log files every time a new user logs in” is checked, backups will be created when a user logs in. The button “Backup Files Now” generates a backup instantly. If backing up to optical media has been selected, the following prompt will appear, giving you the option to finalize a disk for archiving on demand:



Log file format

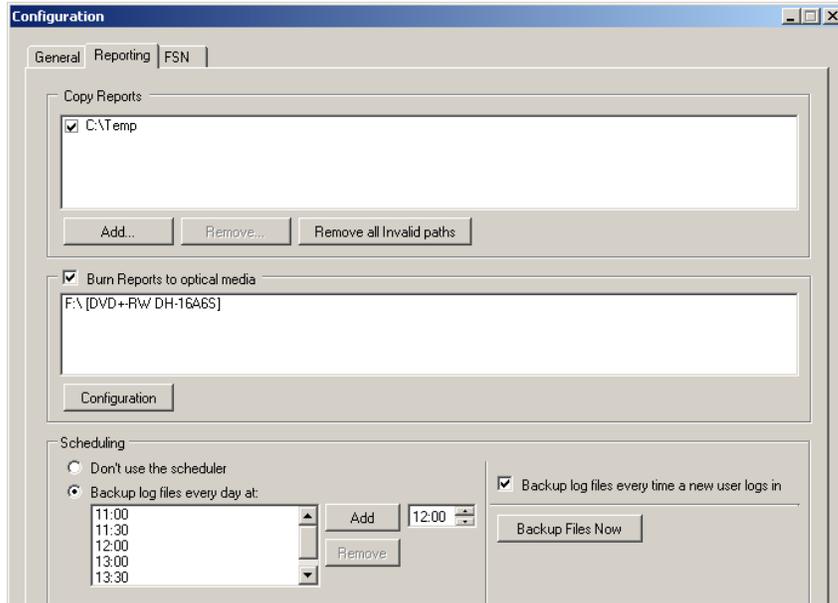
The log file is in comma-delimited text format. The entries are formatted as in the event window. The columns contain:

- Date & Time
- Device Name (that generated the event)
- Event Description
- Device ID (unique identifier of the device which generated the event)
- Operator (operator who was signed on at the time of the event)

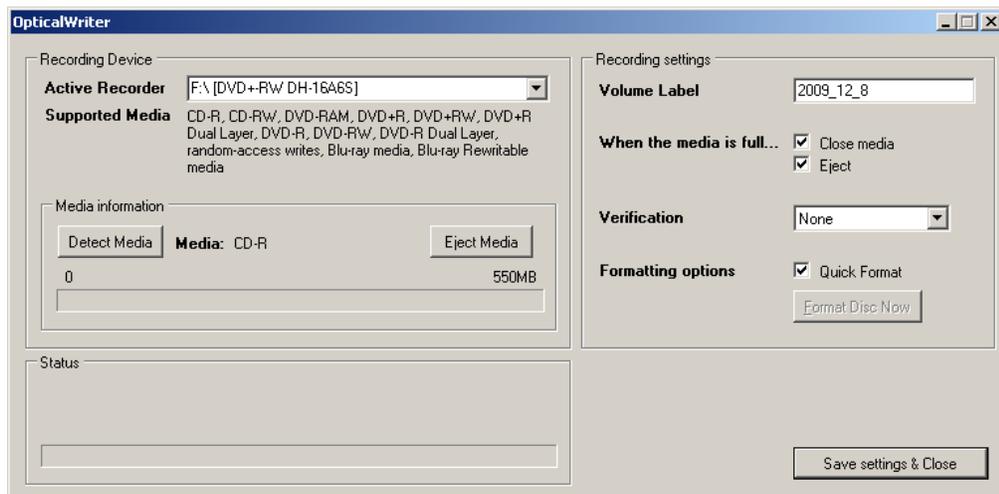
```
===== 12/9/2009 8:17:44 AM Fiber Commander v0.4.0.20 =====
12/9/2009 8:17:44 AM,      FC,      Logged in as: "guest",      FC,      guest
12/9/2009 8:17:50 AM,      FC,      Initialized: System status set to secure,      FC,      guest
12/9/2009 8:17:50 AM,      FC,      Fiber Commander v0.4.0.20 started,      FC,      guest
12/9/2009 8:24:32 AM,      FC,      Logged in as: "admin",      FC,      admin
12/9/2009 10:03:14 AM,      Zone-001, ALARM.,      #001_FCA285.001-FD3xx.Zone-001,      admin
12/9/2009 10:03:17 AM,      Zone-001, User note: Gate Opened,      #001_FCA285.001-FD3xx.Zone-001,      admin
12/9/2009 10:03:17 AM,      Zone-001, Acknowledged Alarm,      #001_FCA285.001-FD3xx.Zone-001,      admin
12/9/2009 10:03:19 AM,      Zone-002, Masked for always,      #001_FCA285.001-FD3xx.Zone-002,      admin
12/9/2009 10:03:27 AM,      FC,      User requested a close of the application,      FC,      admin
12/9/2009 10:04:00 AM,      FC,      Application is closing,      FC,      admin
===== 12/9/2009 8:24:32 AM END =====
```

Backup to optical media

The second section on the “Reporting” tab in the “Options\Configuration” dialog provides the ability to configure an optical writer to make backups. To setup the optical writer, click on the “Configuration” button.

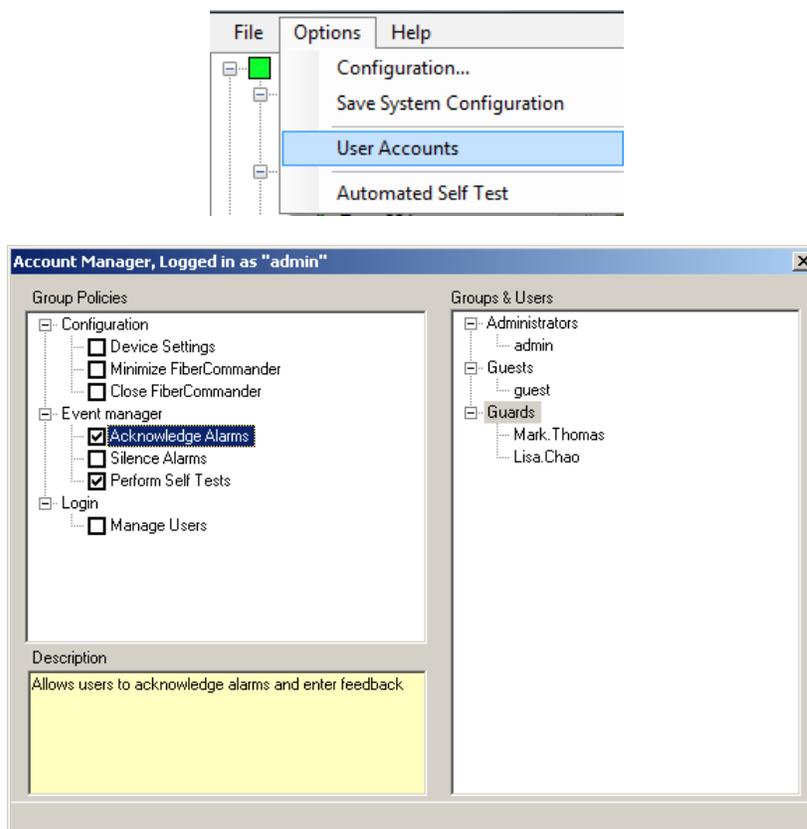


By clicking the “Configuration” button, the optical writer dialog appears (below). If there is more than one recording device available, select the desired recorder from the drop-down menu at top left. At the right side of the dialog, the recording options can be configured. For most users, the default settings will be appropriate. A CD is “closed” and ejected when it is full or by clicking on “Eject Media.” Data will be buffered until a new CD is inserted. Closing a CD is necessary so that further writing is not possible and to make sure any CD drive can read the data (not all drives support “non-closed” disks).



8. Account management

Fiber Commander has a built-in Account Manager, which enforces policies on a user-group basis. As many groups (and users per group) can be created as needed. All users in a group have the same access. A user is a member of a group and has a unique username and an optional password. To access the Account Manager, go to the menu option “Options\User Accounts”:



Policies

The tree on the left side in the Account Manager window displays the policies enforced by the system. When an item is selected a description is displayed at the bottom. The tree on the right side contains all groups and users. When a group or a user in a group is selected, the policies tree displays the policy settings for that group.



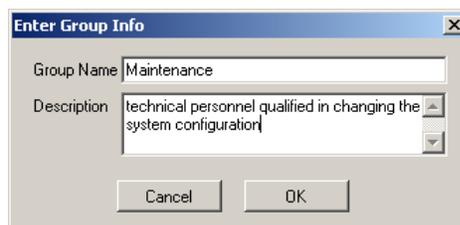
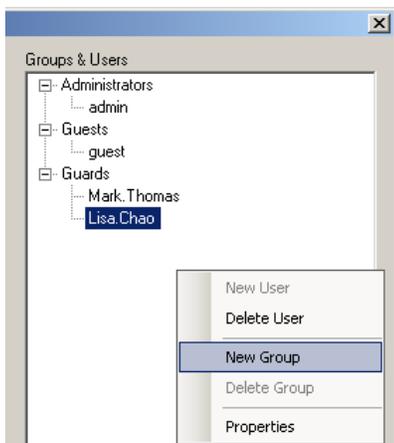
NOTE: Disabling the Windows Task Manager may be required to prevent an operator from interfering with the monitoring system. Please note that this can be achieved through either the operating system policies or registry. For more information, please refer to your operating system vendor.

Accounts

There are two default groups: Administrators and Guests. There are two default users: Admin and Guest. The Administrator group has all policies enabled (this cannot be changed) and the Guests group has all policies disabled by default; however, these can be modified. For “Admin” the default password is “admin” which can be changed. For “Guest” there is no password (this cannot be changed).

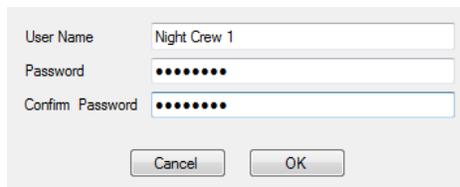
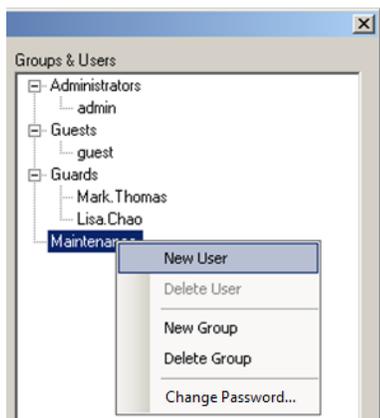
Creating groups & users

To create a new group, right-click in the “Groups & Users” section and select “New Group.”



The description field is optional and not used for any particular function.

To add a user to a group, right-click the group and select “New User.” A password is optional.

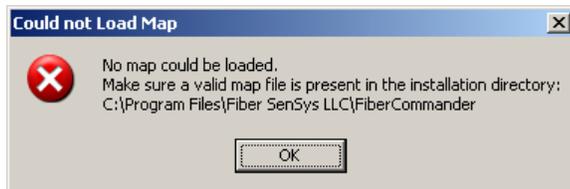


To change a user's password or a group's description, right-click the item, select "Change Password..." and enter a new value.

9. Troubleshooting

This section describes some problems customers have encountered with the most common uses of Fiber Commander. If you are using Fiber Commander with FSN units, please refer to the Appendix for additional troubleshooting items.

Error message: “Could not Load Map”



This message occurs when Fiber Commander fails to load a map during startup. Use the configuration page to select a map for Fiber Commander to use. See “Choosing a different map” for more details.

Event Description: “FAIL”

Time	Device name	Event Description	Device ID	Operator
12/9/2009 5:11:47 PM	#001_FCA285	FAIL	#001_FCA285	admin

A unit connected via TCP/IP is unreachable or is in the process of connecting. When first starting Fiber Commander, the unit might take up to 3 minutes to complete the connection.

Event Description: “FAULT”

Time	Device name	Event Description	Device ID	Operator
12/9/2009 5:29:31 PM	Zone-001	FAULT	#001_FCA285.001-FD3xx.Zone-001	admin

A “FAULT” event can occur in the following situations:

- In the case of a sensor fault, the sensing loop is open, and the fiber is either cut, pinched, or a connector is bad.
- The APU for a unit reports a fault condition due to a problem with the unit itself or due to the test button being pressed.

ADAM Units repeatedly report “FAIL” then “Acknowledged Alarm”

Time	Device Name	Event Description	Device ID	Operator
10/26/2011 12:47:57 PM	Zone 2	Acknowledged Alarm	ADAM6060-fsi1 (172_22_16_198).Zone 2	admin
10/26/2011 12:47:57 PM	ADAM6060-fsi1 (172_22_16_198)	Acknowledged Alarm	ADAM6060-fsi1 (172_22_16_198)	admin
10/26/2011 12:47:56 PM	Zone 2	FAIL	ADAM6060-fsi1 (172_22_16_198).Zone 2	admin
10/26/2011 12:47:56 PM	ADAM6060-fsi1 (172_22_16_198)	FAIL	ADAM6060-fsi1 (172_22_16_198)	admin
10/26/2011 12:47:54 PM	Zone 2	Acknowledged Alarm	ADAM6060-fsi1 (172_22_16_198).Zone 2	admin
10/26/2011 12:47:54 PM	ADAM6060-fsi1 (172_22_16_198)	Acknowledged Alarm	ADAM6060-fsi1 (172_22_16_198)	admin
10/26/2011 12:47:53 PM	Zone 2	FAIL	ADAM6060-fsi1 (172_22_16_198).Zone 2	admin
10/26/2011 12:47:53 PM	ADAM6060-fsi1 (172_22_16_198)	FAIL	ADAM6060-fsi1 (172_22_16_198)	admin

- The fault time is not set correctly in the ADAM settings in Fiber Commander. The fault time must be set to the “*Peer to Peer time*” on the ADAM units.

ADAM units report “FAIL” but relay outputs can manually be engaged or disengaged

- Verify the “Windows Firewall” or other security products are not blocking UDP network traffic from the ADAM units to Fiber Commander. See Appendix A – Configuring Windows Firewall for more information on how to configure the “*Windows Firewall*”.

Fiber Commander is unable to find devices that are plugged into the network

- Check that the devices are powered and that the network cable is securely plugged in.
- Make sure the “*Windows Firewall*” or other security products are not blocking network traffic between Fiber Commander and the devices. See Appendix A – Configuring Windows Firewall for more information on how to configure the “*Windows Firewall*”.
- Verify that each device has a unique IP address and has the same subnet mask as the workstation running Fiber Commander.
- Sixnet switches must have the SNMP read string correctly set before Fiber Commander will see them.

Scheduled shunts are not activating

- Confirm that the shunt is set on the zone or APU. (It may be set on a different zone or APU.)
- Confirm that the start time AM / PM value is correct.
- Confirm that the days of the week are selected. If no days are selected, the shunt will never be activated.
- Confirm that the duration is not set to zero. If the duration is zero, the shunt will never be activated.

Error message: “.NET Framework Initialization Error”



- Fiber Commander requires the .NET Framework 4 Client Profile to be installed on the workstation. The installer is included on the Fiber Commander CD in the “*FiberCommander\DotNet*” directory.
- Windows Server 2003 requires that the “*Windows Imaging Component (WIC)*” be installed before installing the .NET Framework 4 Client Profile. The WIC installer is included on the Fiber Commander CD in the “*Resources\Windows Imaging Component*” directory.

Unable to use optical backup feature on Windows XP or Server 2003

- Windows XP and Server 2003 require *Windows feature pack for storage 1.0*. for the optical backup feature. This can be downloaded from:
<http://www.microsoft.com/downloads/>

10. Product specifications

Specifications	
Log in	Multiple Log in levels, fully customizable
Maximum number of IP-connections	50
Maximum number of zones	200
Event annunciation	Visual and audible
Event management	Acknowledge and clear events, write a note for the event, silence alarms, shunt zones, and rename zones
Event logging	All events and operator actions saved in log file
Shift reports	Shift reports (included in log files) can be backed up on optical media (CD/DVD/BD) at user-defined times
Map image format	BMP, JPG, GIF, and PNG
Map display	Supports Drag and Drop, Zoom, and Pan
Accidental restart	System starts with the saved configuration settings
System Requirements	
Operating systems	Windows 7, 8, 8.1, 10
Supporting software	Microsoft.NET framework 4.0 (supplied with the installation CD)
Minimum hard drive space	50 MB for Fiber Commander installation, 1 GB recommended for saving log files
Processor	2.8GHz Intel Pentium 4 or 2.0 GHz Dual Core or faster
Minimum RAM	512 MB
Optical drive	Optical drive capable of writing CD, DVD or BD required for optical backup feature

Appendix A – Configuring Windows Firewall

Networking security products may prevent Fiber Commander from properly communicating with APUs or other networked equipment. This appendix describes how to configure Windows Firewall for use with Fiber Commander. Contact your network administrator to configure other network security products that may prevent Fiber Commander from working properly.

When Fiber Commander runs for the first time on a workstation with the Firewall enabled, a “*Windows Security Alert*” may appear, stating that Fiber Commander has been blocked. To unblock Fiber Commander, so it can communicate with APUs and other networked equipment, click the “*Allow access*” button.



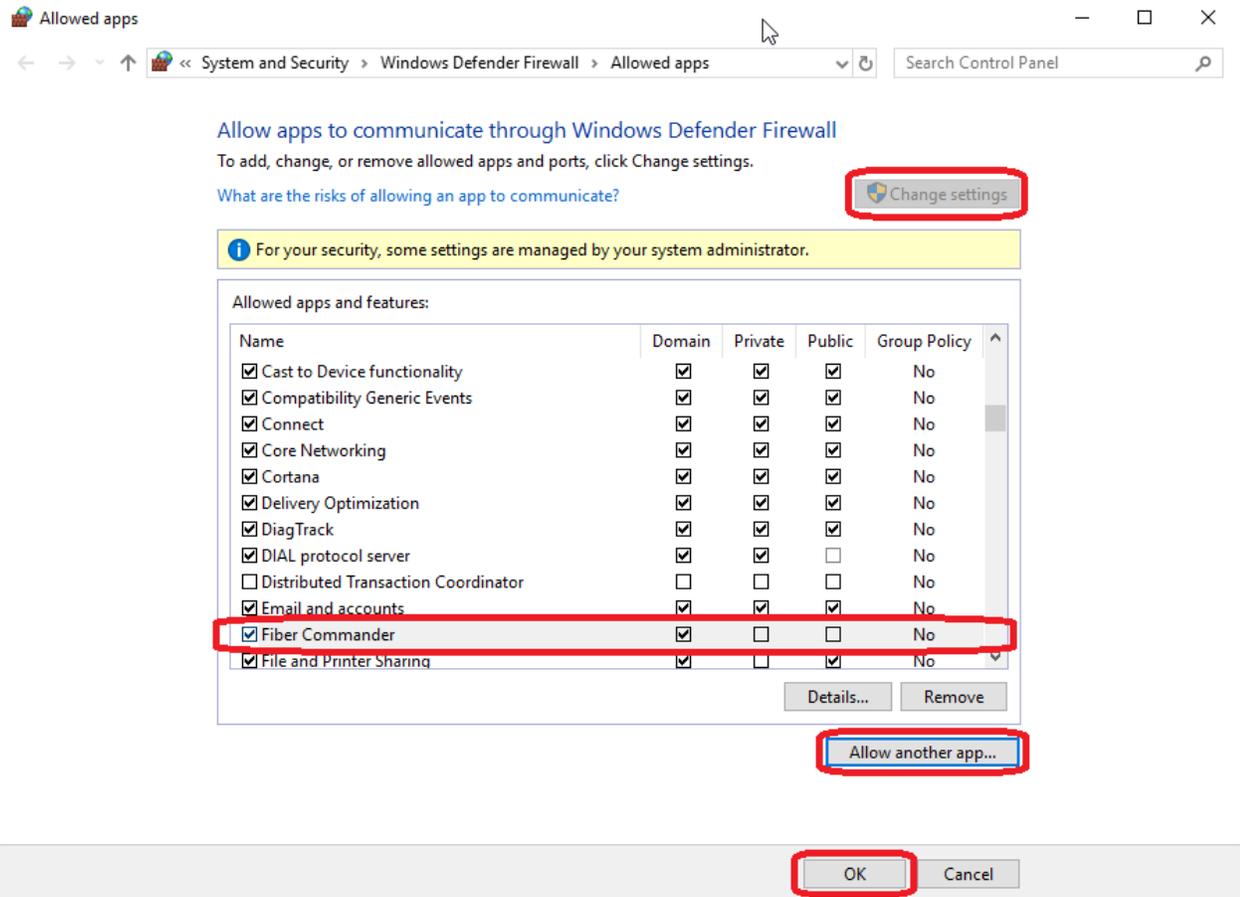
If this dialog did not appear, then you may need to use the Control Panel to allow access to Fiber Commander. The details for this procedure depend on the operating system.

Windows 10:

The alternate way to allow Fiber Commander access is to use the Firewall “*Allowed Programs*” Control Panel window. This can be accessed using the following steps:

- While holding the Windows key, press the X key.
- Click on “Settings”.
- In the Windows Settings dialog, click the “Network & Internet” icon, then scroll down, click on “Windows Firewall”, then click on “Allow an app through firewall”.

- This should bring up the “Allowed apps” window. Click “Change Settings” to gain access. If Fiber Commander is already in the list, then make sure the network boxes are checked.
- If Fiber Commander is not in the list, press the “Allow another app...” button, then then browse for the Fiber Commander executable. This is usually “C:\Program Files (x86)\Fiber SenSys\Fiber Commander\FiberCommander.exe”
- Finally, press “OK” to save the changes.



Windows 8 and 8.1:

The alternate way to allow Fiber Commander access is to use the Firewall “Allowed Programs” Control Panel window. This can be accessed using the following steps:

- While holding the Windows key, press the X key.
- Click on “Control Panel”.

- In the Control Panel, click the “Windows Firewall” icon, then the “Allowed Programs” button.

This should bring up the Allowed Programs window. Please read the Windows 10 description above for how to use the Allowed Programs window.

Windows Vista and Windows 7:

The alternate way to allow Fiber Commander access is to use the Firewall “*Allowed Programs*” Control Panel window.

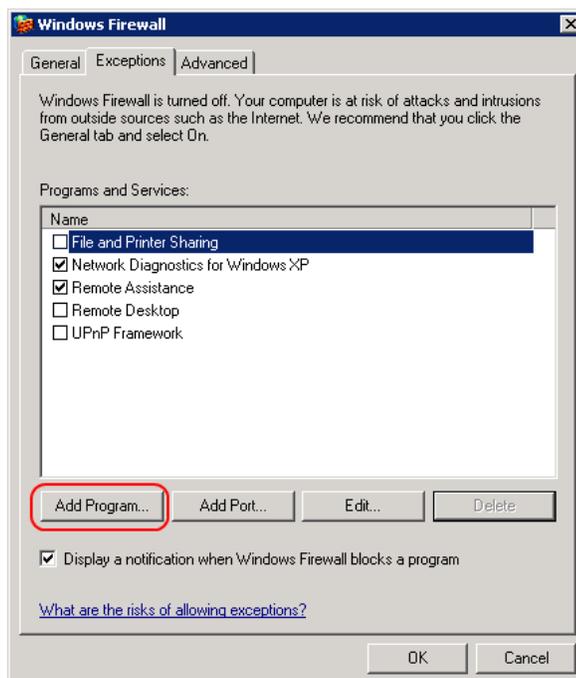
This can be accessed by pressing the Start button, typing “allow a program”, and pressing the ENTER key.

This should bring up the Allowed Programs window. Please read the Windows 10 description above for how to use the Allowed Programs window.

Windows XP

The alternate way to allow Fiber Commander access is to use the “Windows Firewall” Control Panel window. This can be accessed using the following steps:

- Press the Start button, then click “Control Panel”.
- In the Control Panel, click the “Windows Firewall” icon.
- Then click on the “Exceptions” tab.



Select “Add Program...” and browse to Fiber Commander. The typical path is “C:\Program Files\Fiber SenSys\Fiber Commander\FiberCommander.exe”

Press **OK** to save the settings.

Appendix B – Communicating with FSN-based APUs

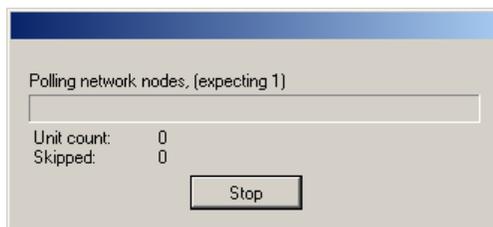
Fiber Commander retains support for communications via the older FSN network. All FSN networks must be initialized before starting Fiber Commander. Please refer to the FSN and APU manuals for configuration instructions. The simplest way to connect to a FCA-285 is to use a computer with a serial port. If your computer doesn't have a serial port, but has a USB port, then use a USB-to-serial converter.

To connect with the FSN network, go to the menu "Options\Configuration" and select the "FSN" tab. The "Inputs" list shows all FCA-285 connections. Select the COM port that your FCA-285 is connected to and click the "Connect" button.



CAUTION: Before connecting a FCA-285 to Fiber Commander, first initialize the loop as described in the FSN manual.

After clicking the "Connect" button, the following window is displayed showing the status of the FSN initialization:



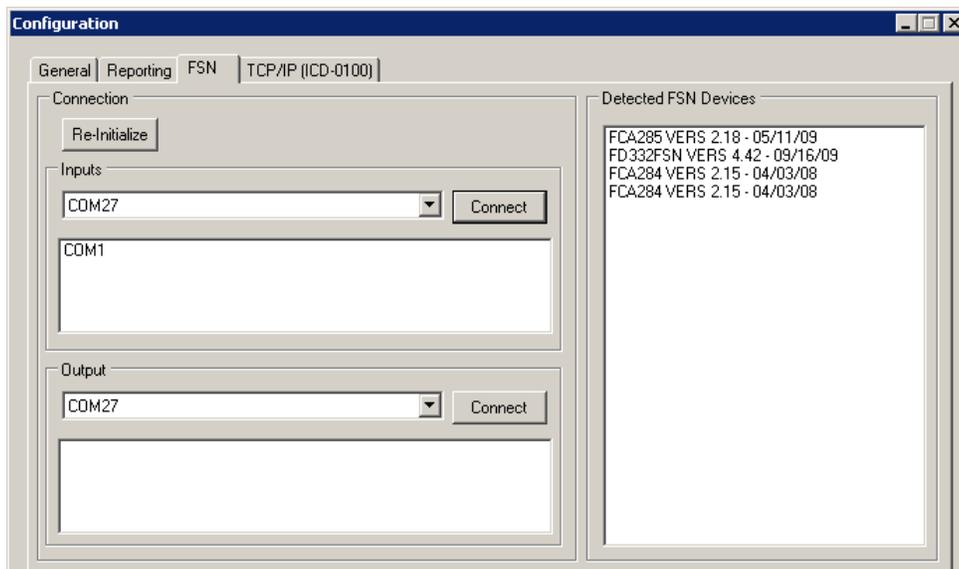
The system then interrogates the FSN loop, identifies all units, and initializes Fiber Commander. When the process is completed, the right column lists information about the detected units.

If an FCA-287 (ASCII converter) is connected to the system, select its COM port in the "Output" panel and click the "Connect" button next to it. The alarm messages of each item in the "Inputs" list will be repeated on each output port in the "Outputs" list. The alarm messages of all FSN units on all configured FSN loops that have not been shunted will be displayed. Note that the output will be in the format it was received (e.g. no zone aliases from Fiber Commander are applied). If the unit is named "unit 001" in the FSN loop, it will be reported that way on the output port. The output ports operate at 9600 baud, 1 stop bit, no parity, 8 data bits and no flow control.

The “Re-Initialize” button clears the configuration and all associated data (device and zone aliases, map labels, etc.). If an FSN loop is modified (for example, by adding or removing a unit), you must also:

- Initialize the FCA-285 per the procedure described in the FSN manual
- Re-initialize the loop in Fiber Commander by clicking the “Re-Initialize” button

After connecting to a new FSN loop or selecting the COM port for a previously connected FSN loop, the devices on the loop are displayed.



In the main display, the following symbols represent the different types of devices in an FSN network:

- FCA-285
- Units (alarm processors and input devices)
- ▲ Zones

Self-test for FSN units

Fiber Commander includes an automated self-test feature for FSN units, which is accessible from the menu “Options\Automatic Self Test.” Units connected via TCP/IP do not support this feature.



The test triggers every device in every FSN loop via the built-in FSN test functionality by generating an event on all units.

Time	Device name	Event Description	Device ID	Operator
12/10/2009 8:13:17 AM	FC	Automated self test completed	FC	admin
12/10/2009 8:13:16 AM	001-FD3xx	Unit test performed	#001_FCA285.001-FD3xx	admin
12/10/2009 8:13:15 AM	#001_FCA285	Unit test performed	#001_FCA285	admin

The self-test triggers one device about every second so larger systems might take several minutes to complete. When the test is finished, the results can be accessed in the alarm log. The test status for individual units can be verified (during or after the test sequence) in the event window or the device tree.

To stop the self-test before it is completed, click “Stop Automated Self Test” in the “Options” menu.



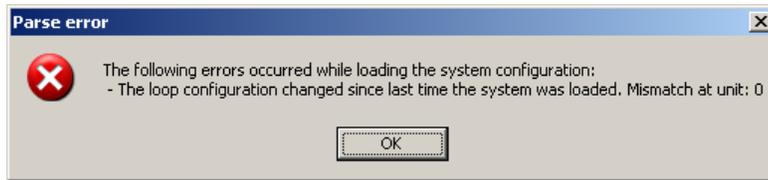
Units can be individually tested (assuming the APU supports such a test) by right-clicking on the unit in the device tree and selecting “Perform Self-Test.”



CAUTION: On very large systems (> 70 units per loop) it is possible (though unlikely) that some units may not trigger an alarm during “Automated Self Test.” If this occurs, the self-test can be separately performed on those units by selecting the “Perform Self-Test” option in the right-click menu of the device.

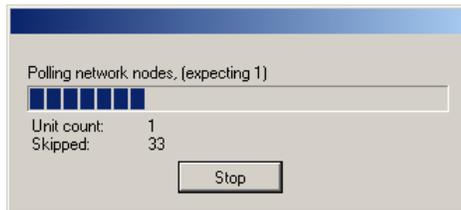
Troubleshooting FSN problems

Error message: “Parse error”



This error occurs when the system fails to load unit configuration during startup. This can happen when the loop configuration of one or more FSN loops has changed. For example, if a unit is added to a loop, that loop must be re-initialized by Fiber Commander. The chapter “Configuring the FSN interface” contains instructions on how to re-initialize a system.

Status message: “Skipped” number is ≥ 1



The “Skipped” number in the polling-status dialog box should be zero. If the number is greater than zeros a unit might be missing in the FSN loop or might be unresponsive. This is an indication of a problem with the FSN loop. To correct the problem

- Re-initialize the FSN loop itself (refer to the FSN manual)
- Restart Fiber Commander

Event Description: “FAIL”

Time	Device name	Event Description	Device ID	Operator
12/9/2009 5:11:47 PM	#001_FCA285	FAIL	#001_FCA285	admin

A “FAIL” event can occur in the following situations:

- FSN loop error: the loop is broken and the FCA-285 is not able to communicate with all units. When a break occurs, a “Data Failed” message is generated by the unit immediately after the break. Starting from the input (dark) connector on the FCA-285, the FSN loop will be complete up to the unit reporting the error. Keep in mind this kind of problem can be generated by a faulty patch-cord or a faulty unit.
- A unit in an FSN loop is either missing or broken (a loop error is generated by the FCA-285).

- An FD-208 FSN unit cannot internally communicate with its alarm processor. This occurs when the unit is set in stand-alone mode (a general error is generated by the FCA-285).
- A duplicate unit is present in an FSN loop. To resolve this situation, the unit which caused the problem must be re-initialized. This is done by using the “Loop” and “Show” commands in the FCA-285 terminal mode (please refer to the FSN manual). Afterwards the loop in Fiber Commander must be reinitialized.
- An unknown unit is present in an FSN loop. This may occur when an initialized unit (a unit which already has an ID assigned) is added to an initialized loop. To resolve this, reinitialize the new unit separately, add it to the loop and re-initialize the loop in Fiber Commander. Please refer to the FSN manual for more details.

Appendix C – Monitoring Sixnet-based managed networks

If your TCP/IP network is implemented using Sixnet switches, you can monitor the overall status of the network using Fiber Commander.

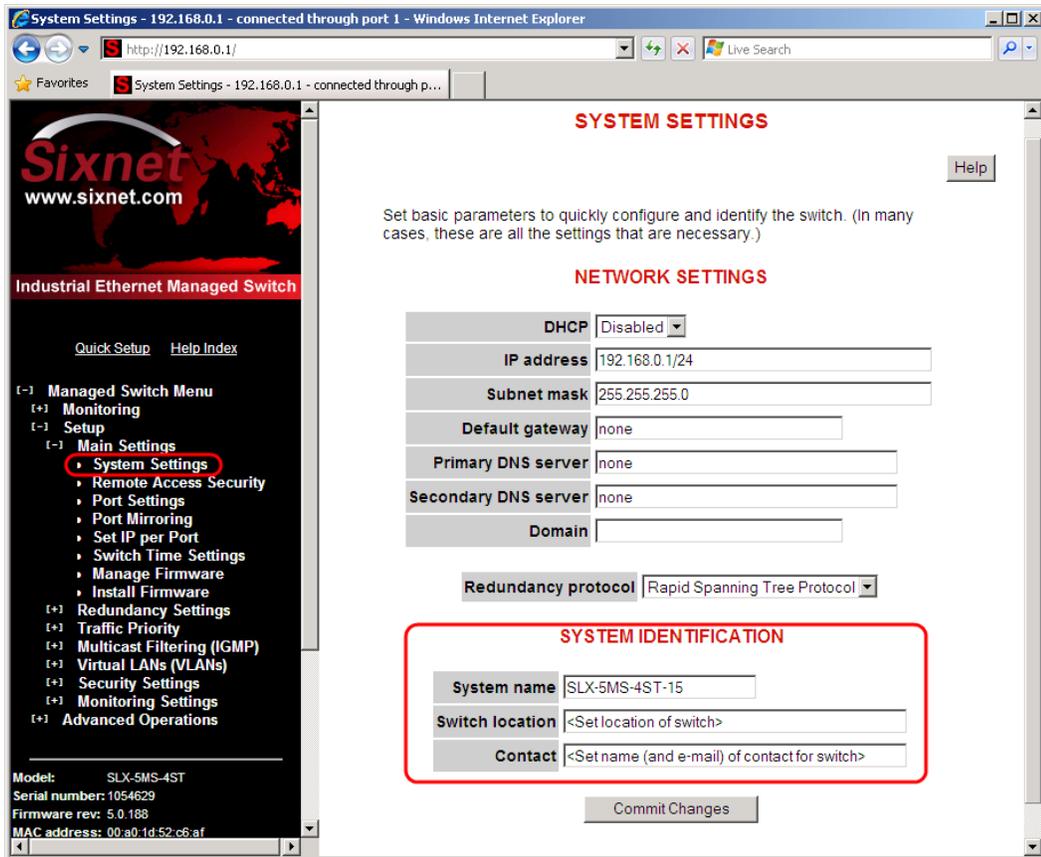
Sixnet switches are configured via a web interface. The web interface can be accessed from a web browser by typing the switch's IP address into the address bar and pressing ENTER. The default IP address is 192.168.0.1 or 10.2.0.1. The switch may ask for a username and password to access the configuration page. The default username is "admin" and the default password is "admin". See the documentation that came with the switch for more information on how to access the web interface.



CAUTION: Network security products must be configured to allow Sixnet Switches to communicate with Fiber Commander. See Appendix A – Configuring Windows Firewall for more information.

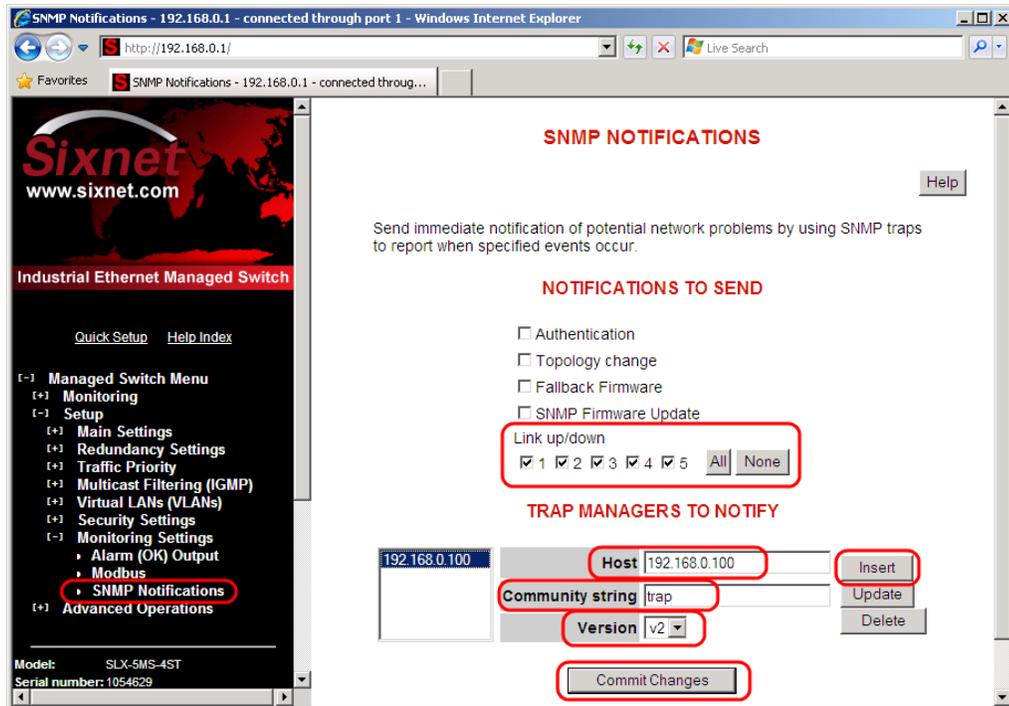
To configure the switch for use with Fiber Commander, its system settings, SNMP notifications, and security settings will need to be configured.

First configure the system identification settings by selecting "Setup" ► "Main Settings" ► "System Settings" from the items on the left side of the page.



The items under “System Identification” will show up in Fiber Commander. Specifically, the “System name” will be the default device name that shows up in Fiber Commander’s device tree. It is highly recommended to use a unique name for each switch.

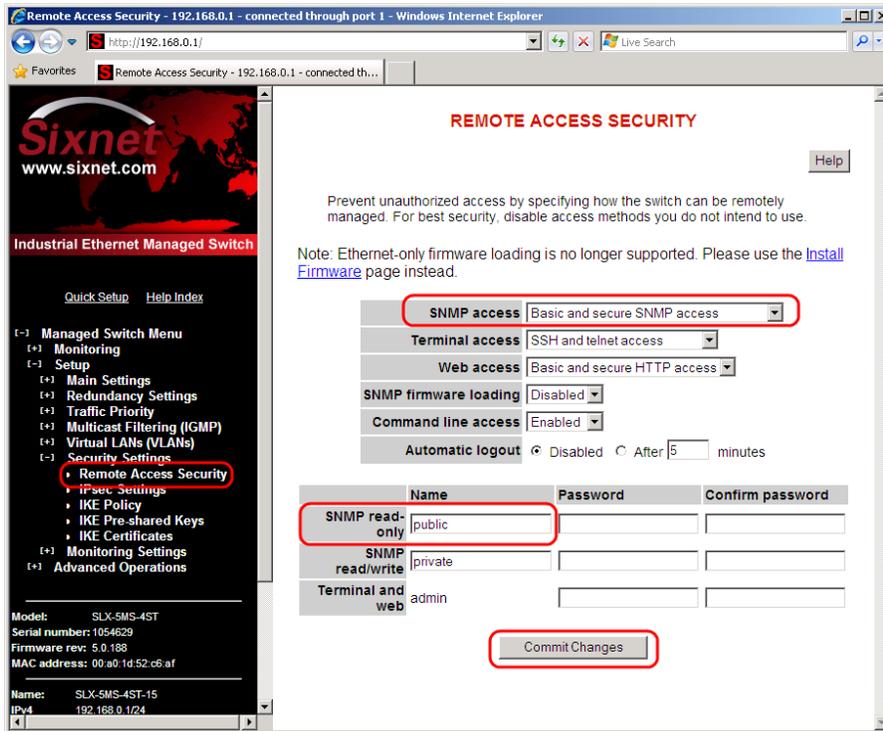
Next, navigate to the SNMP Notifications page by going to “Setup” ► “Monitoring Settings” ► “SNMP Notifications” on the left side of the page. Some Sixnet switches SNMP Notifications page may be located at “Setup” ► “Main Settings” ► “SNMP Notifications”. Fiber Commander uses SNMP notifications to determine when a network port is unplugged from the switch.



To configure the switch to notify Fiber Commander when a network port is unplugged, do the following:

1. Place a check in all the check boxes in the Link up/down section.
2. Enter the IP address of the workstation running Fiber commander in the “Host” field.
3. Enter “trap” for the community string,
4. Version V2 from the drop-down list.
5. Press the “Insert” button
6. Press the “Commit Changes” button.

Finally, navigate to the “Remote Access Security” page by going to “Setup” ► “Security Settings” ► “Remote Access Security”.

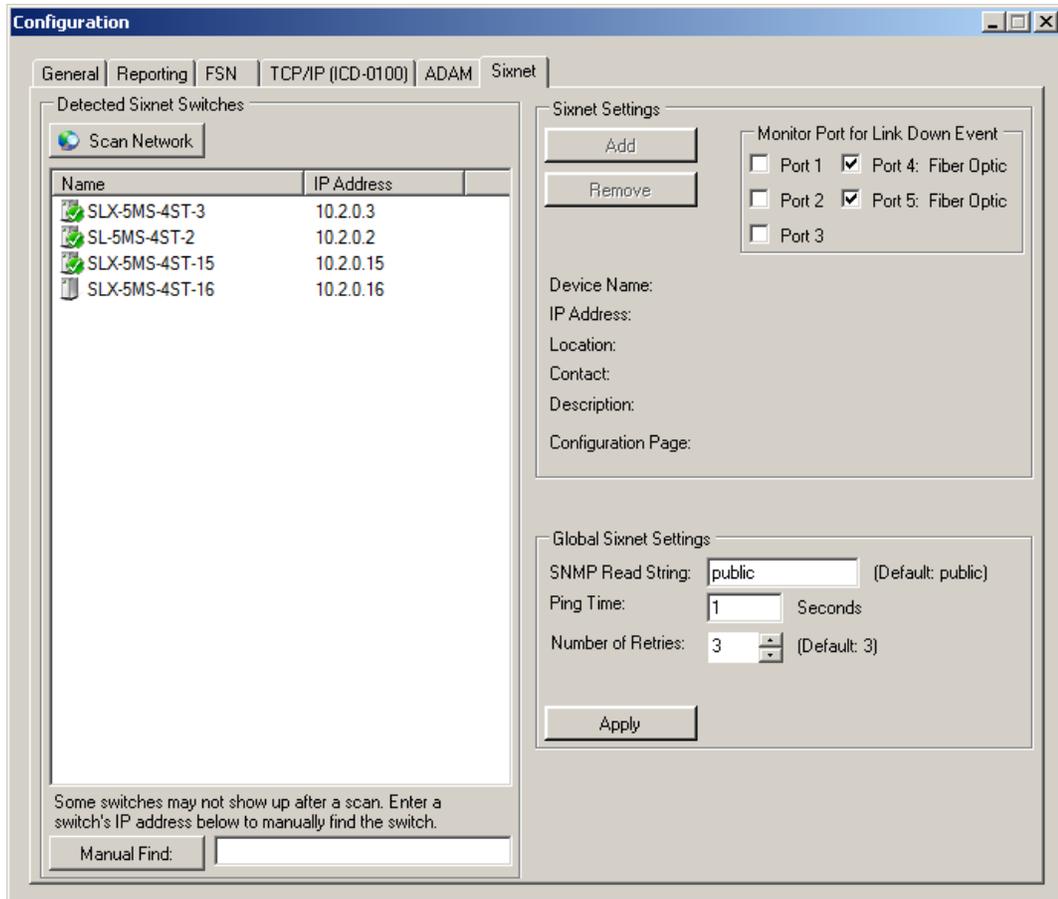


Fiber Commander uses the SNMP read-only name to communicate with the switch. Every switch must have the same SNMP read-only name. The default read-only name is “public”. Fiber Commander does not use or care about the SNMP read-only password so it can be set to anything. Make sure to do the following:

1. Enable Basic and secure SNMP access.
2. Set the SNMP read-only name the same on all Sixnet switches.
3. Press the “Commit Changes” button after making any changes.

Configuring Sixnet Switches

The Sixnet tab in the Fiber Commander configuration dialog brings up the settings page for Sixnet switches. The page allows adding, removing, and configuration of Sixnet Switches.



The “*Global Sixnet Settings*” box contains settings that affect all Sixnet switches. Fiber Commander communicates to Sixnet switches using SNMP v2c. The SNMP read string is similar to a password. All Sixnets must have the same SNMP read string and that string must be entered into the “*SNMP Read String*” field. After changing the “*SNMP Read String*” field, make sure to press the “*Apply*” button.



NOTE: If a Sixnet switch is not showing up in Fiber Commander make sure the switch’s SNMP read string is the same in the as the “*SNMP Read String*” in Fiber Commander’s Sixnet Configuration tab.

To add Sixnet switches to Fiber Commander, first press the “*Scan Network*” button. This will search the network for Sixnet switches. When the scan is complete the list brings up all the Sixnet switches on the network, showing their name and IP address.



NOTE: Some versions of Sixnet switches may not show up after a scan. The IP addresses of the missing switches can be manually entered in to the field at the bottom of the configuration window to have Fiber Commander find switches individually.

Switches that Fiber Commander is monitoring and are connected have a green check next to their icon. Switches that Fiber Commander is configured to monitor but are disconnected from the network have a red X next to their name.

Select a Sixnet switch to view additional properties such as the name, location, and contact information of the switch. Additionally, there is a link to the Sixnet configuration page. Clicking on the link opens the configuration page for that device in the default web browser.

Individual Sixnet switch ports can be monitored. The “*Monitor Port for Link Down Event*” box contains a check box for each port on the switch. Use the check boxes to select the ports Fiber Commander will monitor. Ports that are monitored will show up in the input tab in Fiber Commander. If that port is unplugged, Fiber Commander will alert the user of the problem. By default, the fiber optic ports 4 and 5, typically used in redundant ring configurations, are selected to be monitored.

To tell Fiber Commander to start monitoring a switch and its individual ports select the switch from the list of found switches then press the “*Add*” button.

To update the ports on a Sixnet switch that Fiber Commander monitors, do the following: first select the switch from the list; next change the check boxes in the “*Monitor Port for Link Down Event*” box; finally press the “*Update*” button.

To remove a Sixnet switch, select the switch and click “*Remove*”. This will remove the switch from the list of switches being monitored by Fiber Commander.



CAUTION: When a switch is removed, all related information like operator notes, aliases, I/O mappings, and map-icon placement information is also erased.

Fiber Commander monitors Sixnet switches by communicating with them at regular intervals. The “*Ping Time*” controls the interval, in seconds, between attempts to communicate with the Sixnet switches. Set ping times faster to detect communication failures faster. Set ping times slower to use less network and system resources.

The “*Number of Retries*” field controls how many times Fiber Commander tries to communicate with Sixnet switches before it considers them to have a communication failure.

After the SNMP read string, ping time, or number of retries has been changed, click the “*Apply*” button to save the changes.



CAUTION: The ping time and number of retries depends on your network characteristics and must be chosen to balance the amount of network management traffic, false alarms, and response time. Determining the proper balance is a normal function of network management. Consult your network administrator for guidance.