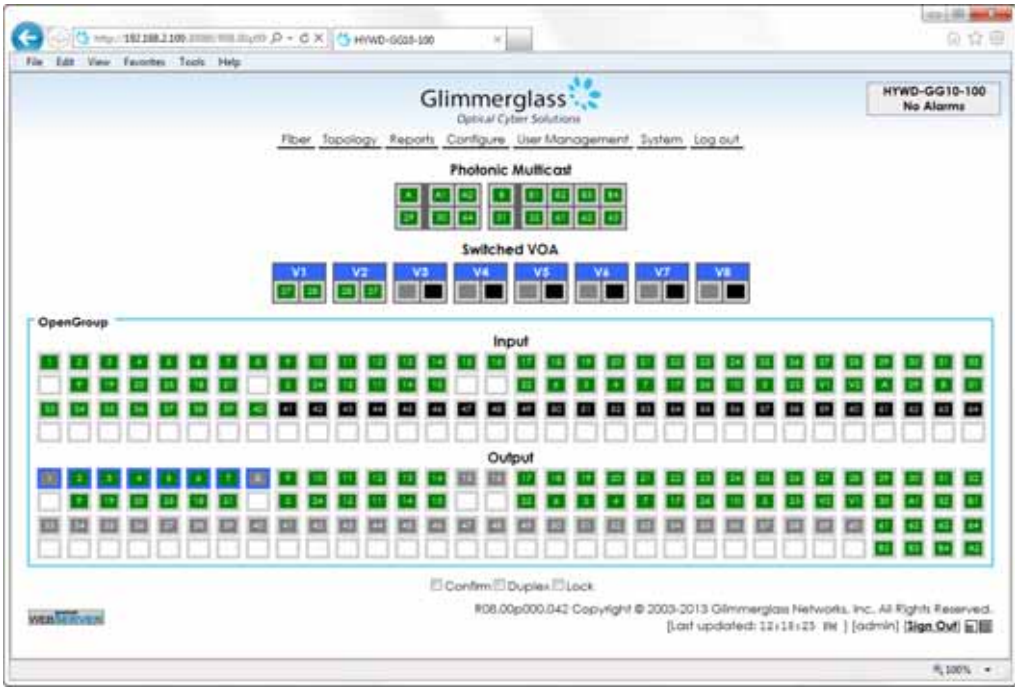
ClickFlow™ Graphical User Interface Manual

Software Release 8.0
Part Number 901-0102
Revision A



Last updated: July 11, 2013

The Glimmerglass ClickFlow™ Graphical User Interface (GUI) is a web-based interface that displays a graphical view of the Glimmerglass Intelligent Optical Switch in a standard browser to provide point-and-click operation, configuration, and monitoring of the system.

This user manual describes concepts and capabilities of the Glimmerglass Intelligent Optical Switch and how to use the ClickFlow GUI to configure the Glimmerglass System 100, System 500, and System 600 products.

Copyright 2013. Glimmerglass Networks, Inc.
ALL RIGHTS RESERVED.

Release Notice

The following table lists the version of this document that supports the current release of the Intelligent Optical Switch application:

Release Date	Glimmerglass Intelligent Optical Switch Product Release Number	Most Recent Document Version
July 2013	R08.00p000	A

Author and Copy Requests:

Glimmerglass Networks, Inc.
26142 Eden Landing Road
Hayward, CA 94545
Tel +1 510 723 1900
Fax +1 510 780 9851

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Contents

Document Overview

Document Organization 1

Overview of the ClickFlow™ Graphical User Interface (GUI)

Introduction 3
Connecting to the ClickFlow GUI 4
Logging into the ClickFlow GUI 5
Secure Sockets Layer (SSL) 7
Connection Screen 8
Port Information Box 11
Alarms Panel 14
Connection Screen Menus 15
I/O Matrix 16
Port Box and Connection Box 18
Configuration Settings 19
Software and Session Information 21
Photonic Multicasting™ Unit 22
Variable Optical Attenuation (VOA) 24
Dedicated VOA 24
Switched VOA 26
Configuring Ports and Provisioning Connections 30
Connection Provisioning 31
Confirm Operation Check Box 31
Duplex and Paired Check Boxes (Connection Types) 31
Connection Methods 32
Making a Connection 33
Breaking a Connection 35
Updating a Connection 36
Connection Locking/Unlocking 37
Photonic Multicast and Switched VOA Connections 37
Creating a Photonic Multicast Unit Connection 38
Creating a Switched VOA Connection 38
Port Configuration 39
Input Port Waveband Setting 40
Port Signal Threshold Setting 41

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Port Box Context Menu

Overview 43
Configure 45
Using the Port Configure Window to Configure a Port 47
Provision 49
Using the Port Box Context Box Provision Option to Make Connections 53
Using the Port Box Context Box Provision Option to Update Connections 54
Using the Port Box Context Box Provision Option to Break Connections 56

Fiber

Overview 57
Connect 58
Disconnect 58
Connect All 59
Connecting All Ports 59
Disconnect All 60
Disconnecting All Connections 60

Topology

Overview 61
Topology File Format Guidelines 62
Connection Mode Options 68
Import 68
Importing a Topology File 69
Export 70
Exporting a Topology 71
Quick Load 71
Applying a Topology Using Quick Load 72
Clearing the Quick Load List 73

Reports

Overview 75
Performance 77
Viewing a Performance Status Report 79
Printing a Performance Report 79
Saving the Performance Report to a File 79
Port 80
Viewing a Port Report 82
Printing a Port Report 82
Saving the Port Report to a File 83
Connections 83
Viewing a Connection Report 86
Printing a Connection Report 86

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Saving the Connection Report to a File 87
Signal Threshold 88
Waveband 90
Port Group 91
Viewing a Port Group Report 93
Printing a Port Group Report 93
System Info 93
Legend 96

Configure

Overview 99
Signal Thresholds 103
Adding a Signal Threshold 106
Modifying a Signal Threshold 107
Signal Threshold Data Entry Errors 109
Deleting a Signal Threshold 109
Ports 111
Configurable Port Attributes 112
Import/Export Port Configuration 113
Port Name/Description File Guidelines 114
Creating a Port Name/Description File for Import 116
Import File Operation 117
Importing a Port Name/Description File 118
Exporting Port Names/Descriptions 119
Change Port Configuration 119
Editing Port Attributes in the Port Configuration Window Table 121
Clear Port Parameters 122
Change Waveband Assignment 123
Change Signal Threshold Assignment 126
Change Group Assignment 130
Change Alarm Severity Assignment 135
Import/Export Group Assignment 140
Group Assignment File Guidelines 140
Importing a Port-to-Group File 141
Exporting a Port-to-Group File 143
Connections 143
Change Connection Descriptions 144
Clear Connection Descriptions 146
Port Groups 146
Adding a Port Group 148
Editing a Port Group 149
Deleting Port Groups 150
Protection Rules 151
Protection Types: Simplex and Duplex 153
Protection Rule State 154

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Arming Modes 155
Triggering Conditions 156
Condition 1: Power Falls Below the Minimum Optical Power Threshold (STMIN) 156
Condition 2: Trigger Delay 156
Protection Rule Default Configuration Settings 156
Adding a Protection Rule 157
Deleting a Protection Rule 159
Deleting All Protection Rules 160
Importing Protection Rules 160
Protection Rule File Format Guidelines 161
Exporting Protection Rules 162
Printing Protection Rules 163
Variable Optical Attenuation (VOA) 164
Modes of Operation for VOA 165
Performance Specifications for VOA 165
Configuring VOA Ports 166
Guidelines and Usage Considerations for VOA 168
Guidelines and Usage Considerations for Dedicated VOA 169
Guidelines and Usage Considerations for Switched VOA 170
Guidelines for Attenuate Power Mode 170

User Management

Overview 171
Default User Accounts 172
Privilege Levels 173
Virtual Private Switch (VPS) 177
Password and Account Policies 178
Password Complexity Policy 178
Password Change Policy 179
Password Expiration 179
Password Change Restrictions 180
Account Aging Policy 181
User Management Menu Options 182
Set Password 183
Changing an Account Password 185
Add User 186
Adding a User Account 189
Edit User 190
Editing a User Account 193
Delete User 194
Deleting a User Account 195
Import Users 196
Importing User Account Information 197
Export Users 197
Exporting User Account Information 198

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Change Port Privilege Assignments 198
User Account XML File 203
Considerations Before Editing the User Account XML File 209
Editing the User Account XML File 211

System

Overview 213
Save Configuration 216
Saving Configuration Changes 217
Session Administration 218
Terminating Sessions 219
System Backup/Restore 219
Backup 220
Backing up the System Configuration 221
Restore 221
Restoring the System Configuration 223
System Configuration 225
Name/IP 226
Changing the System Name and IP Configuration 229
Error Messages in the System Name and IP Configuration Window 230
Date/Time 231
Configuring NTP Operation 233
Setting the Date/Time for the Internal Clock 235
Error Messages in the System Date/Time Configuration Window 236
SNMP 237
Changing SNMP v2c Trap Destinations (Target Addresses) 239
Changing SNMP v1/v2c Community Strings 240
Syslog 240
Changing Syslog Configuration 242
Runtime Options 243
Autosave Enable 244
Autosave Delay 245
Connection Restore 245
Performance Switch Throttle Enable 245
Event Reporting Mode 246
Confirm Required 246
Default Connection Mode 247
Ports Per Row 248
PMUs Per Row 248
Configuring Runtime Options 248
Account Options 249
Password Complexity Policy and Password Change Policy 253
Account Aging Default 253
Maximum Invalid Login Attempts and Lockout Duration 253
No Activity Timeout 253

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Configuring Account Options 254
Startup Options 254
Configuring Startup Options 257
System Maintenance 257
System Upgrade/Rollback 259
Upgrade 260
Upgrading System Software 264
Rollback 266
Rolling Back the System Software 268
System Alarms 268
Alarm Table Operations 271
Alarm Conditions and Alarm Types 274
System Logs 276
Alarm (ALARM) Log 277
Autonomous Message (AUTO) Log 279
Security (SECU) Log 282

Web Browser SSL Certificate Warnings

Eliminating Security Certificate Warnings in Internet Explorer 7-9 285
Eliminating Security Certificate Warnings in Firefox 7-13 288

Index

Index of Terms 291

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Document Overview

1

This *ClickFlow™ Graphical User Interface Manual* describes the concepts and capabilities of the Glimmerglass Intelligent Optical Switch and how to use the ClickFlow GUI to configure the Glimmerglass System 100, System 500, and System 600 products.

Document Organization

This document contains the following chapters:

Chapter	Description
Chapter 1: Document Overview	Describes the content of this document.
Chapter 2: Overview of the ClickFlow™ Graphical User Interface (GUI)	Describes how to connect to the ClickFlow GUI and describes the elements of the Connect screen.
Chapter 3: Port Box Context Menu	Describes the Port Box context menu and the procedures for configuring ports, provisioning connections, and locking connections.
Chapter 4: Fiber	Describes the **Fiber** menu and the associated procedures.
Chapter 5: Topology	Describes the **Topology** menu and the associated procedures, including formatting for import/export files.
Chapter 6: Reports	Describes the **Reports** menu and the associated procedures, including connection, port, and system information.
Chapter 7: Configure	Describes the **Configure** menu and the associated procedures. Also describes signal thresholds, protection rules, and Variable Optical Attenuation (VOA).
Chapter 8: User Management	Describes the **User Management** menu and the associated procedures, including user account XML files.
Chapter 9: System	Describes the **System** menu and the associated procedures.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Chapter	Description
Appendix A: Web Browser SSL Certificate Warnings	Describes the procedures for eliminating SSL certificate warnings.
Index	Index of terms and key concepts.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Overview of the ClickFlow™ Graphical User Interface (GUI)

2

Introduction

The Glimmerglass ClickFlow™ Graphical User Interface (GUI) is a web-based interface that displays a graphical view of the Glimmerglass Intelligent Optical Switch in a standard browser to provide point-and-click operation, configuration, and monitoring of the system.

The ClickFlow GUI supports the following web browsers:

- Microsoft Internet Explorer version 7 through 9
- Mozilla Firefox version 7 through 21

NOTES: JavaScript and cookies must be enabled in the web browser in order to access the ClickFlow GUI.

Microsoft Internet Explorer 10 (IE10) is not fully supported due to issues with HTTPS operation. IE10 may be used if HTTPS operation is disabled. HTTP or HTTPS operation is determined by the setting of the -webSSLEnable flag:

- If -webSSLEnable = 1 (default setting), session requests from IE10 browsers will be rejected.
- If -webSSLEnable = 0, the HTTP sessions can be initiated from IE10.

When -webSSLEnable is changed to 0, all browser communication is HTTP (not encrypted).

See ”Startup Options” on page 254 for information on the -webSSLEnable parameter and how to change the setting via a supported ClickFlow browser. This setting may also be changed from the Maintenance Console. Refer to the *System Installation and Maintenance Guide* for information on logging in and using the Maintenance Console.

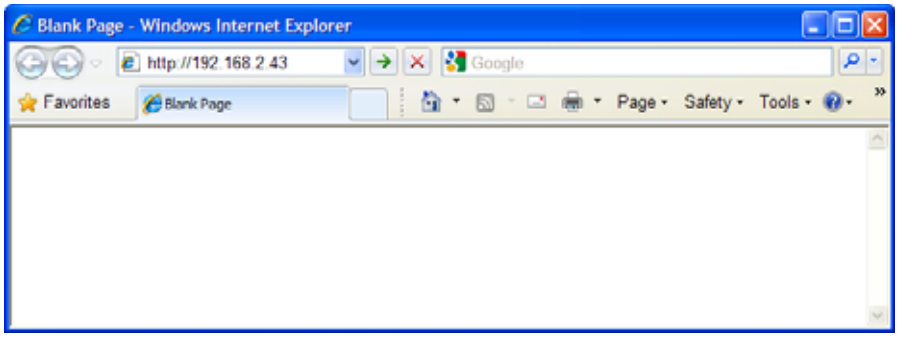
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Connecting to the ClickFlow GUI

Each Glimmerglass product is shipped with the default IP address (192.168.2.200) and can be connected to a computer either directly via an Ethernet cable or via a Local Area Network (LAN), as described in the *Glimmerglass System Installation and Maintenance Guide.*

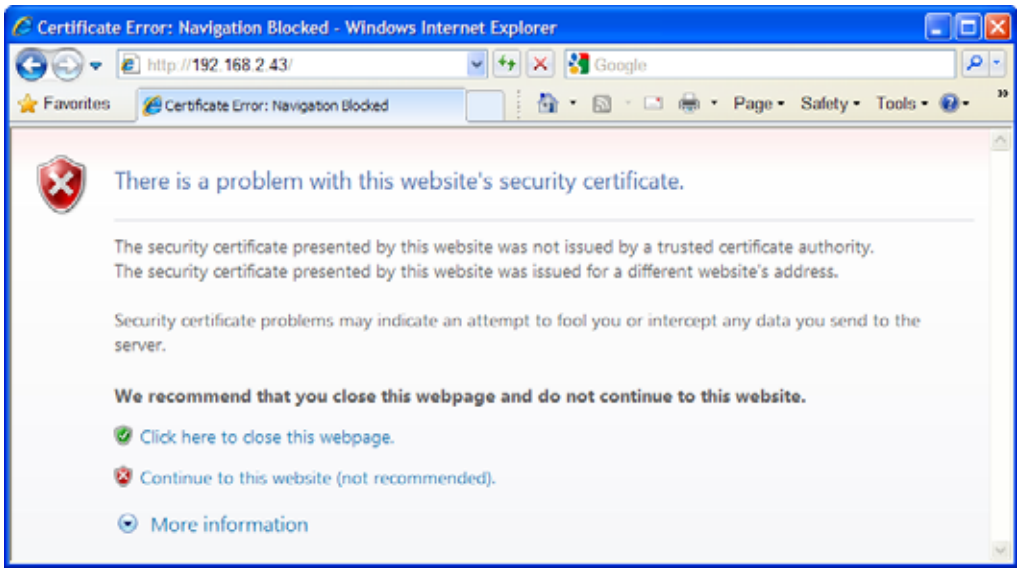
To access the ClickFlow GUI, open a web browser and enter the Glimmerglass system's IP address provided by the system administrator.

Figure 1 Entering the System IP Address (Internet Explorer 8)



When initially connecting to the system or if using a different IP address for the system, the browser application will display a security warning (Figure 2) that displays information about the security certificate for the page to be displayed (see "Secure Sockets Layer (SSL)" on page 7 for more information on security features).

Figure 2 Example Security Warning (Microsoft Internet Explorer 8)



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

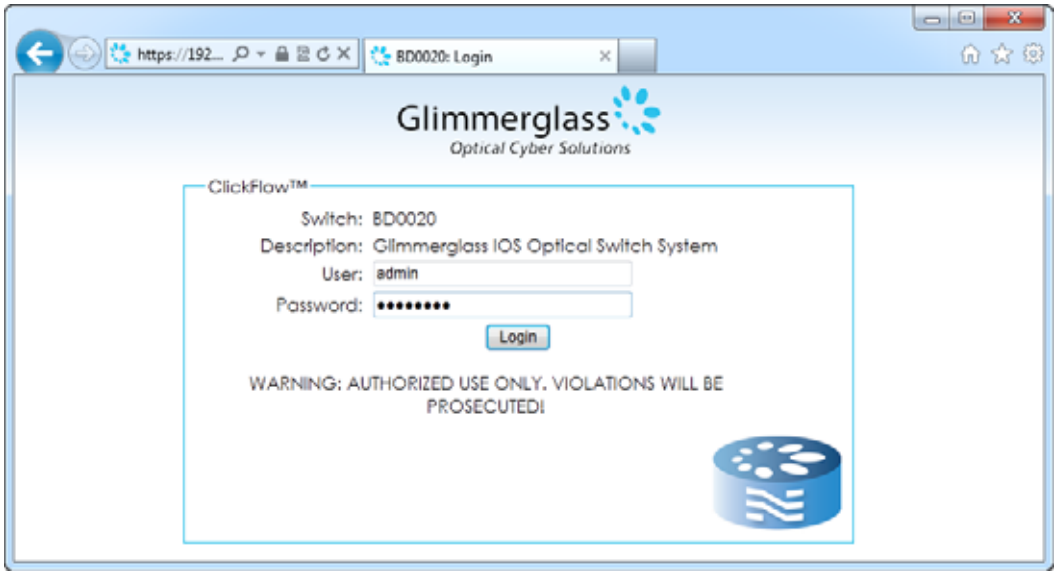
NOTE: The security warning in Figure 2 is presented by Internet Explorer 8. Mozilla presents different pop-up warnings. As the Glimmerglass GUI uses self-signed certificates, you will need to accept the security warning displayed by the browser you are using.

See Appendix A starting on page 285 for the optional procedures for eliminating the certificate errors.

Logging into the ClickFlow GUI

After entering the appropriate IP address for the system and successfully connecting, the ClickFlow GUI will display User Authentication screen (Figure 3) that requests a user name and password to access the main ClickFlow GUI screen.

Figure 3 User Authentication Screen



The system ships with the following defaults for the System Administrator account:

- User Name: admin
- Password: password

Enter the above user name and password for the first-time login. After logging in, it is strongly recommended that the user change the administrator password from the default value (see ”Changing an Account Password” on page 185).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE:	Multiple users can access the ClickFlow GUI concurrently, so changes made by any one user to the configuration of the system will be reflected in the ClickFlow GUI sessions of all users who are logged in.

The “User Management” chapter starting on page 171 has information on managing user accounts and user groups.

After a successful login the following advisory dialog boxes may be displayed:

- Failed Login Attempts (Figure 4)—The Failed Login Attempts dialogue box will be displayed if there have been any login attempts to this user account with the wrong password since the last successful login.
- Password Change Required (Figure 5)—A password change policy has been configured for this user account, the user should change the password before the date-time listed in the popup window. For further information see “Password Change Policy” on page 179. The user may change the password using the **User Management > Set Password** menu option.

Figure 4 Failed Login Attempts

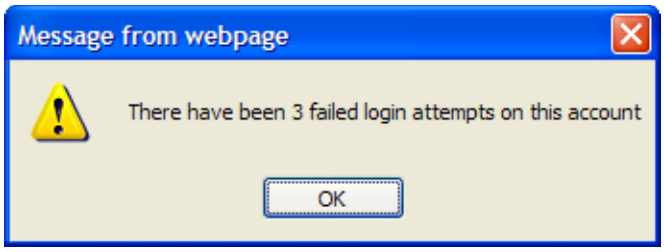
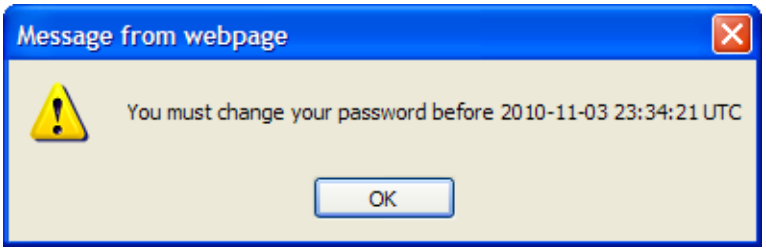


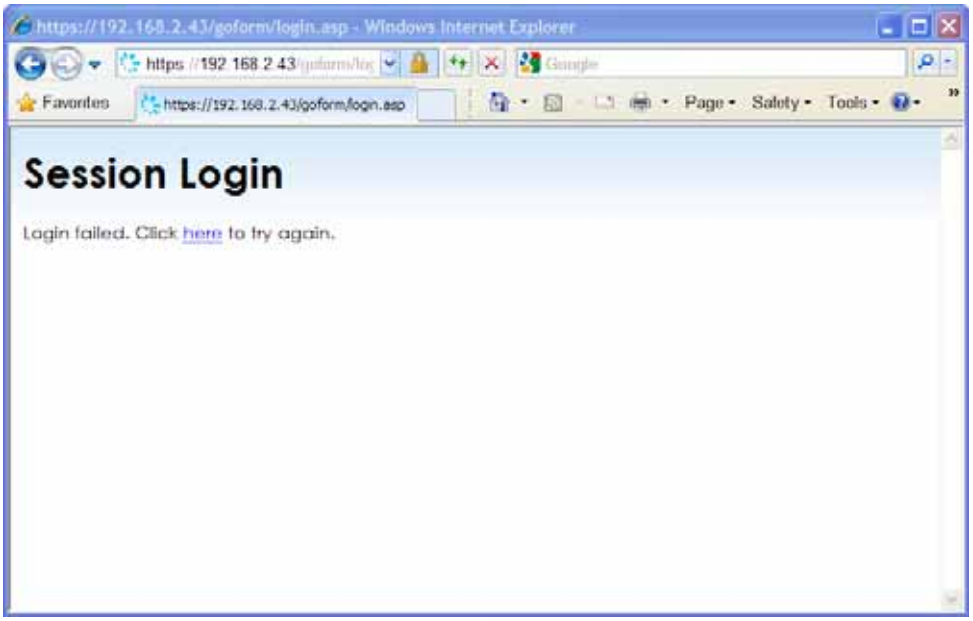
Figure 5 Password Change Required



The password change notification will be presented during the password change grace period. If the user does not change the password prior to the end of the grace period, the login will be denied and the user will be directed to the Session Login page shown in Figure 6.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 6 Session Login Screen



Secure Sockets Layer (SSL)

The Glimmerglass systems use the Secure Sockets Layer (SSL) protocol to secure connections to the following control interfaces:

- ClickFlow™ web-based Graphical User Interface (GUI)
- Transaction Language 1 (TL1) command line interface

The ClickFlow GUI supports the Secure Sockets Layer (SSL) protocol for secure connections with supported web browser clients. The SSL protocol works by exchanging a certificate between the server (the Glimmerglass system) and the client application. This certificate is used to authenticate the server and to exchange encryption keys for securing the communications link between the client and the server.

When using a web browser to connect to the ClickFlow GUI, no special action is required beyond accepting the self-signed certificate.

SSL can be enabled or disabled via the **System > System Configuration > Startup Options** menu option from the Connection screen (see ”Startup Options” on page 254).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Connection Screen

Upon successful login, the ClickFlow GUI opens to the Connection screen. The Connection screen is the home page and displays the current configuration and status of the system.

The presentation and content of the Connection screen is dependent upon the software features enabled (licensed) on the system as well as the screen settings configured by the system administrator. The Port Grouping feature, when enabled, modifies the presentation of the I/O Matrix to reflect port-to-port group assignments. The Virtual Private Switch feature, when enabled, may affect the ports presented in the I/O Matrix for each user. Lastly, the system administrator may configure the maximum number of ports to be presented on a per row basis (this is a system setting, affecting all users).

The Port Grouping and VPS features are not included in the standard software. These are optional features that may ordered when the system is purchased or may be enabled by ordering an upgrade including the license(s).

Figure 7 highlights the main elements of the Connection screen for all systems (with or without either of the above licenses). Note that the browser tab title displays the name that is assigned to the system. This name can be changed via the System menu; see “Changing the System Name and IP Configuration” on page 229).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 7 Connection Screen Elements Common to All Systems

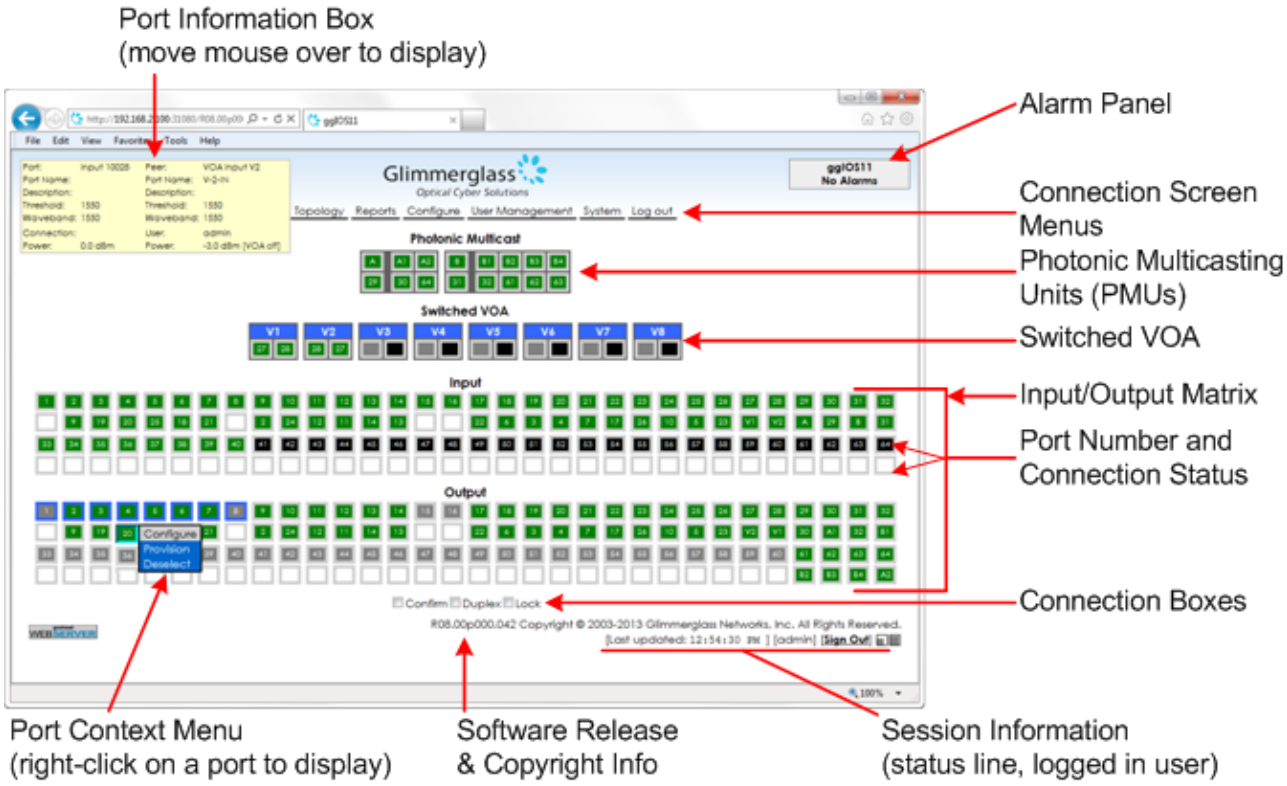
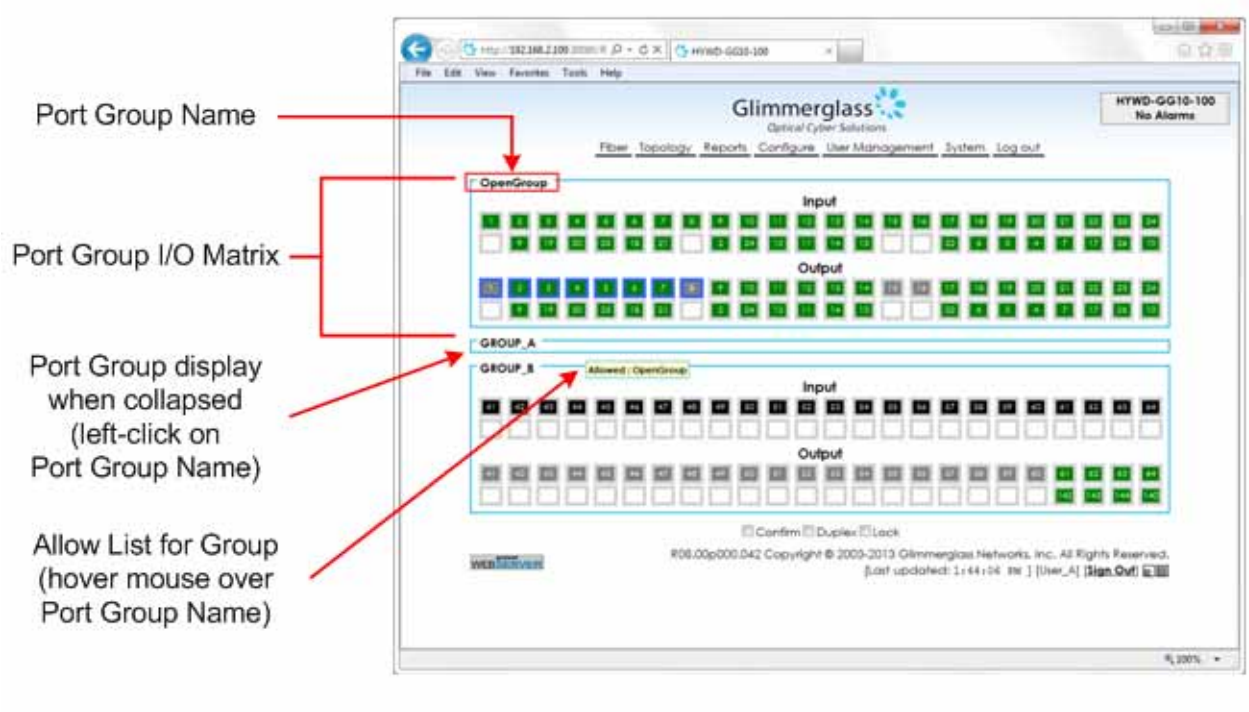


Figure 8 highlights the Connection screen elements added when the Port Grouping feature is enabled in the system. The figure shows the administrator's view of a 64x64 port system partitioned among three port groups. The system default port group, OpenGroup, is always displayed first. All other groups are presented based upon the first input port number in the group (ascending order). If OpenGroup has no assigned ports, then it is not presented. Port groups without input ports are presented below the last group containing input ports. Port groups which are configured but without any assigned ports are not displayed.

As the display of port groups requires more vertical screen space, individual groups may be collapsed as is shown for GROUP_A in the figure. A scroll bars are provided when the space required exceeds the window size.

Figure 8 Connection Screen Elements Unique to Systems with Port Grouping License



The elements of the Connection screen are described in the following sections of this chapter:

Element	Page
Port Information Box	11
Alarms Panel	14
Connection Screen Menus	15
I/O Matrix	16
Port Box and Connection Box	18
Configuration Settings	19
Software and Session Information	21
Photonic Multicasting™ Unit	22
Variable Optical Attenuation (VOA)	24
Port Box Context Menu	43

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Port Information Box

The Port Information Box is a tool tip that appears in the upper left corner of the Connection screen when the cursor is placed over a port/connection box.

Figure 9 through Figure 12 are examples of Port Information Boxes from a system licensed with the Port Grouping feature. These figures reflect the content of the Port Information Box for both unconnected and connected ports. Refer to the table starting on page 13 for definitions for each of the fields.

NOTE: On systems without the Port Grouping feature, the "Port Group:" row is not displayed, as the port group will always be "OpenGroup".

Figure 9 Mouse over Unconnected Input Port 1

Port:	input 10001	Peer:	
Port Name:	HNDOFF-D1-TX	Port Name:	
Description:	IDF-01-02-03	Description:	
Port Group:	OpenGroup	Port Group:	
Threshold:	1310-In-10GbE-LR	Threshold:	
Waveband:	1310	Waveband:	
Connection:		User:	
Power:	-6.6 dBm	Power:	N/A

Figure 10 Mouse over Unconnected Output Port 9

Port:	output 20009	Peer:	
Port Name:	BN5200-P1RX	Port Name:	
Description:	Panel-02-03-04	Description:	
Port Group:	OpenGroup	Port Group:	
Threshold:	1310-Out-10GbE-LR	Threshold:	
Waveband:	1310	Waveband:	
Connection:		User:	
Power:	-55.0 dBm	Power:	N/A

Figure 11 Mouse over Input Port 1—Connected to Output Port 9 w/ Connection Description Configured

Port:	input 10001	Peer:	output 20009
Port Name:	HNDOFF-D1-TX	Port Name:	BN5200-P1RX
Description:	IDF-01-02-03	Description:	Panel-02-03-04
Port Group:	OpenGroup	Port Group:	OpenGroup
Threshold:	1310-In-10GbE-LR	Threshold:	1310-Out-10GbE-LR
Waveband:	1310	Waveband:	1310
Connection:	AcmeCo-Circuit1	User:	admin
Power:	-6.6 dBm	Power:	-9.6 dBm

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 12 Mouse over Output Port 9—Connected to Input Port 1 w/ Connection Description Configured

Port:	output 20009	Peer:	input 10001
Port Name:	BN5200-P1RX	Port Name:	HNDOFF-D1-TX
Description:	Panel-02-03-04	Description:	IDF-01-02-03
Port Group:	OpenGroup	Port Group:	OpenGroup
Threshold:	1310-Out-10GbE-LR	Threshold:	1310-In-10GbE-LR
Waveband:	1310	Waveband:	1310
Connection:	AcmeCo-Circuit1	User:	admin
Power:	-9.6 dBm	Power:	-6.6 dBm

The port information box is displayed as long as the user has View or higher privileges for the port the user selects with the cursor. If the port selected is in a connection, the port information box will contain full information for both ports as long as the user has View or higher privileges for both the input and output port. If the user only has View or higher privileges on just one of the ports, the information for the second port will be shown as “N/A”. This situation may occur when the VPS feature is used to restrict user access to certain ports in the system (see “Virtual Private Switch (VPS)” on page 177).

Figure 13 shows an example of the Port Information Box for a port configured with the VOA option to illustrate the VOA mode and value setting. In this example, the VOA mode is “Set Power” and the value is “-15.1dBm”).

Figure 13 Port Information Box for VOA Connection

Port:	VOA output V4	Peer:	output 20022
Port Name:	V-4-OUT	Port Name:	C1001
Description:	Switched VOA 4	Description:	Panel-03-04-05
Port Group:	OpenGroup	Port Group:	OpenGroup
Threshold:	1550	Threshold:	1550
Waveband:	1550	Waveband:	1550
Connection:		User:	admin
Power:	-12.1 dBm [Set Power : -15.1]	Power:	-15.1 dBm

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The Port Information box contains the following elements:

Element	Description
Port	Displays the following information regarding the port over which the cursor is placed: • Port Type: input | output | multicast input | multicast output | VOA input | VOA Output • Port Number: 5 digit number starting with “1” for input ports and “2” for output ports • Port ID: Alphanumeric ID for PMU or Switched VOA ports For further information on port ID numbering see: • “Photonic Multicasting™ Unit” on page 22 for PMU port IDs • “Variable Optical Attenuation (VOA)” on page 24 for VOA port IDs
Peer	Displays the same information as the **Port** field except that the content applies to the 'other' port in the connection (the peer). This field will be blank if the port over which the cursor is placed is not in a connection.
Port Name	The configured or defaulted port name for the given port (either the selected port or the peer port). Photonic Multicast, Dedicated VOA, and Switched VOA ports have default port names. For further information on port naming see: • “Photonic Multicasting™ Unit” on page 22 for PMU port IDs and default port names • “Variable Optical Attenuation (VOA)” on page 24 for VOA port IDs and default port names • “Using the Port Configure Window to Configure a Port” on page 47 for assigning/editing port names
Description	Displays the description configured for the given port (either the selected port or the peer port). The field will be blank if no description has been configured.
Port Group	Displays the name of the port group of which the port is a member. The Port Group row is displayed only when the system is licensed for Port Grouping. Otherwise this information is not presented, as all ports by definition are assigned to “OpenGroup”.
Threshold	Displays the signal threshold in use by the port. See Chapter 7 starting on page 99 for information on configuring signal thresholds and assigning signal thresholds to ports.
Waveband	Displays the signal band assigned to the input port. See Chapter 7 starting on page 99 for information on signal band assignment and operation.
Connection	Displays the name assigned to the connection between the port and peer: • This field will be blank if the port on which the cursor is placed is not part of a connection. • The field will also be blank if the connection has not been named.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
User	Displays the name of the user who last updated the connection on the selected port: • If the port on which the cursor is placed is not part of a connection, then this field will be blank. • If the connection is locked, the ClickFlow GUI will display “(Locked)” next to the user name. See the section “Connection Locking/Unlocking” on page 37 for more information on locking and unlocking connections.
Power	Displays the optical power (in dBm) present at the selected port and at the peer port, if there is a connection: • This field will display “N/A” on input ports for systems without Input Detection. • If the system is equipped with Input Detection, then power information is displayed for both input ports and output ports. • For VOA ports (Dedicated or Switched), the ClickFlow GUI also displays the VOA mode (Set Power, Attenuate, or VOA Off) and the VOA setting (Figure 13 on page 12). See “Variable Optical Attenuation (VOA)” on page 164 for information on configuring VOA ports and settings.

Alarms Panel

The alarm panel is displayed at the top right corner of the Connection screen. The panel indicates if any active alarms are present in the system as well as the severity of the most significant unacknowledged active alarm.

Figure 14 below shows the Alarm Panel for a system without any active alarms. The upper section of the alarm panel will display the System Name. The bottom section will either indicate “No Alarms” or “Alarms”.

Figure 14 Alarm Panel (No Active Alarms)

As seen in Figure 15, when “Alarms” are present, the color of the upper section will reflect the highest severity active alarm.

From Figure 15, note that acknowledging alarms does not remove the alarm from active status. The acknowledgment does, however, reset the color of the upper section to reflect the highest unacknowledged alarm severity until all alarms are acknowledged.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The user may click on the System Name text in the upper section as a short-cut to open the active alarm table for viewing and acknowledging alarms. An example of the Active Alarm table opened by clicking on the System Name text is shown in Figure 16 below.

Figure 15 Alarm Panel Examples - All Severities and All Acknowledged

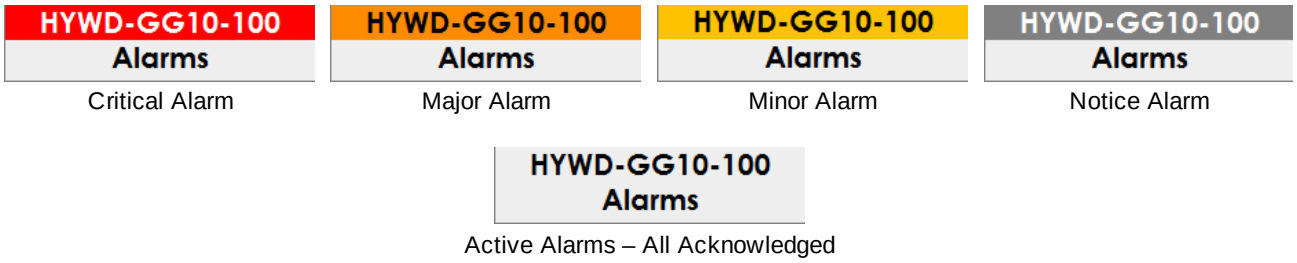
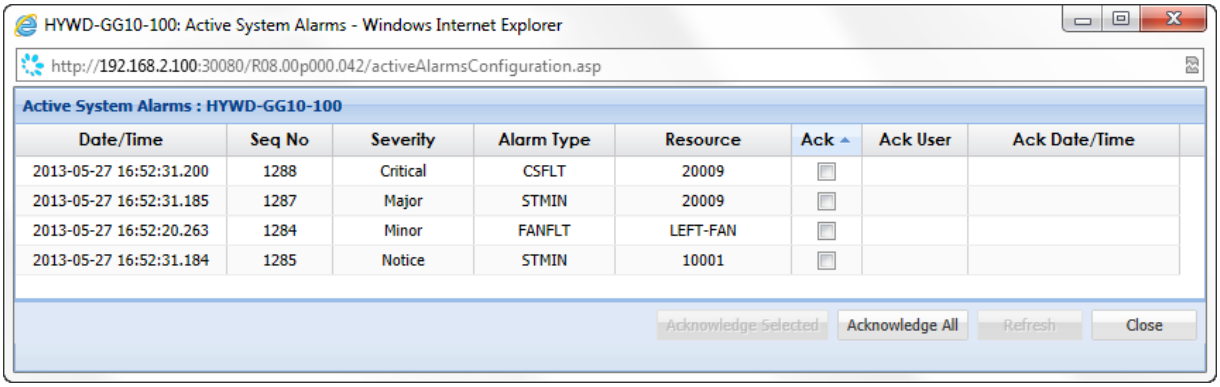


Figure 16 Active System Alarms Table Example



The alarm table in Figure 16 shows (top to bottom) one example of each alarm severity. For this table, the Alarm Panel would indicate a critical alarm. If the critical alarm was acknowledged, then the Alarm Panel would change to display a major alarm. This pattern would continue if each alarm was acknowledged until all alarms were acknowledged. Then, the Alarm Panel display would match the “Active Alarms - All Acknowledged” panel indicated in Figure 15. The operation of the Active Alarm table is discussed in “System Alarms” on page 268.

Connection Screen Menus

Configuration functions are accessed using the menus at the top of the Connection screen and by the Port Box context menu. Each menu is described in detail in separate sections of this user guide:

Menu	Page
Port Box Context Menu	43

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu	Page
Fiber	57
Topology	61
Reports	75
Configure	99
User Management	171
System	213
Logoff	(see below)

The logoff menu option allows the user to sign off and log out of the current session. The "Session Closed" page will be displayed.

I/O Matrix

The physical input and output ports on the system's patch panel are represented on the Connection screen in the I/O Matrix. Each port is represented by two boxes representing port and connection information as described in the next section. Ports are selected by mouse-clicking on the port. Only one input and output port may be selected at any one time. Subsequent menu commands or connection screen operations then operate on the selected ports.

The location, composition, and contents of the I/O Matrix is determined by the hardware-enabled features present in the system, the ports-per-row configuration, and the software features licensed on the system.

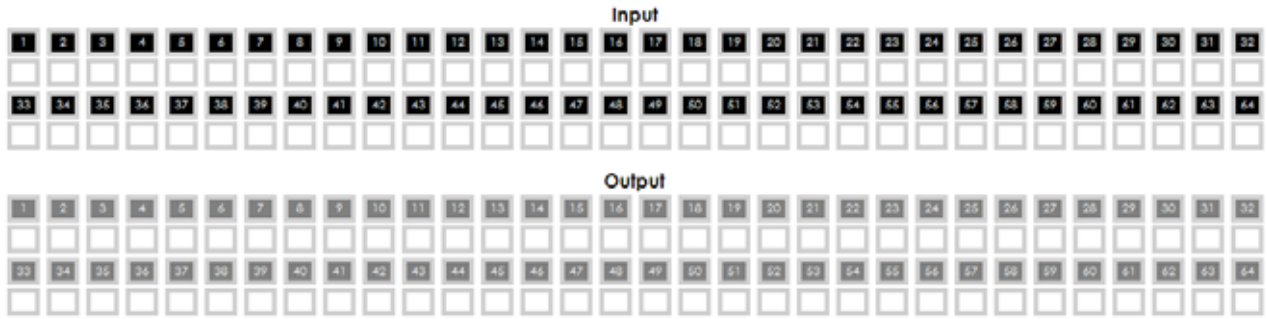
For systems with Photonic Multicasting and/or Switched VOA components, the I/O Matrix is displayed in the center of the screen below the sections reserved for these features (see Figure 7 on page 9). If neither of these features are present, the I/O Matrix is centered directly below the Connection screen menus.

By default, the system displays 32 ports on each row in the I/O Matrix. The number of ports displayed per row may be modified through configuration of the “Ports Per Row” system parameter described on page 248.

Standard systems are not licensed for the Port Grouping or VPS features (see “Port Groups” on page 146 and “Virtual Private Switch (VPS)” on page 177). For these systems there is a single I/O Matrix to display all ports. The top section of the I/O Matrix is reserved for the input ports; the bottom section is reserved for the output ports. Each section is labeled at the top (e.g., “Input,” “Output”). The labels and ports are centered on the screen based upon the ports per row setting. The system default is 32 ports per row. Partial rows are aligned at the left with the previous rows. Figure 17 shows an example of an I/O Matrix for a standard 64x64 port system

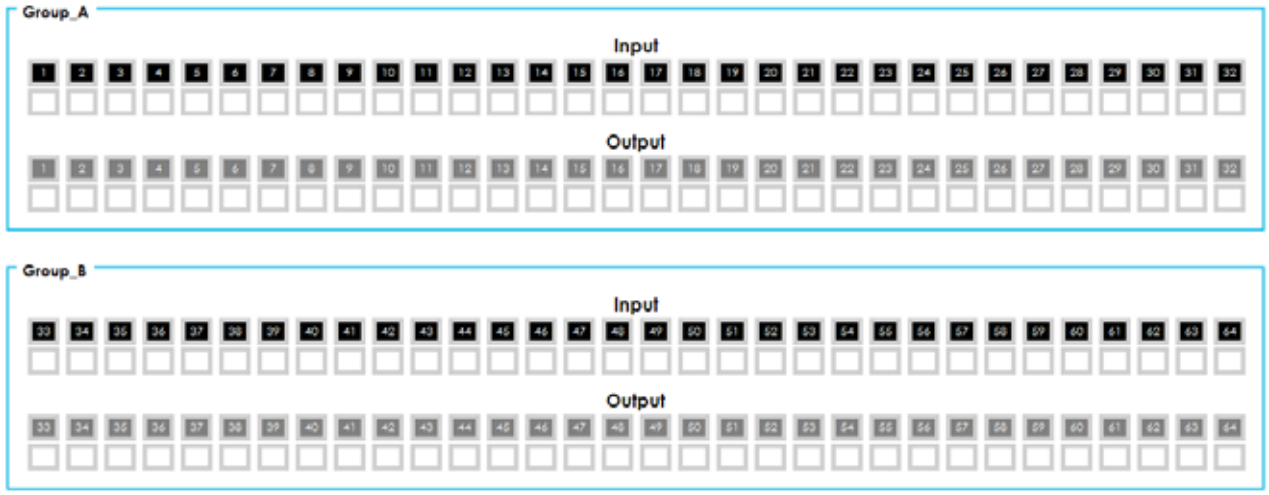
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 17 I/O Matrix Displayed for Standard 64x64 Port System (without Port Grouping Feature)



For systems with the Port Grouping license, the system displays a separate I/O Matrix for each port group with assigned ports. Each I/O Matrix is framed within a blue border bearing the name of the port group. The input and output ports belonging to the group are presented in the same fashion as a standard system (inputs at top, outputs at bottom). The maximum ports per row for the system may be configured as with the standard system. If the number of ports per row is different than the default of 32, the first line of ports will be centered in the section and partial rows will align to the left boundary of the first row. Figure 18 below shows an example of the I/O Matrix for a 64x64 port system with two port groups configured. The first group, Group_A, has input/output ports 1 - 32. The second group, Group_B, has input/output ports 33 - 64.

Figure 18 I/O Matrix for 64x64 Port System with Port Grouping Licensed



For systems with the Virtual Private Switch (VPS) license, it is possible to restrict the ports a user may access. When the user does not have privileges for all ports, then the ports and port groups displayed in the I/O Matrix for the user will be confined to only the ports to which the user is allowed access.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 19 and Figure 20 below show a user's view when the user has privileges only for the first 16 input/output ports of the same 64x64 port systems shown in the previous two figures. In both figures below, the I/O Matrix displays only Input/Output Ports 1 - 16. In Figure 20, note that Group_B is not displayed at all because the user has no privilege to any ports in Group_B.

With both Port Grouping and VPS, the Connection screen for the user shows only the port resources the user is permitted to view or use.

Figure 19 I/O Matrix with VPS licensed, Port Grouping Not Licensed, User with Privilege to First 16 Input and Output Ports Only

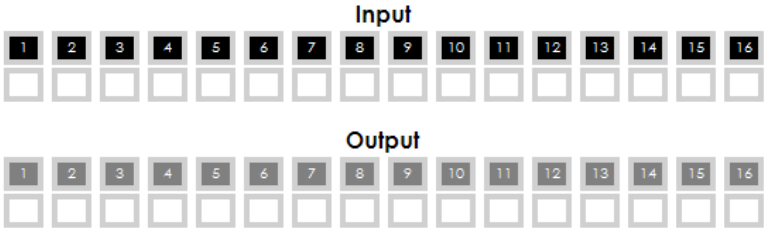
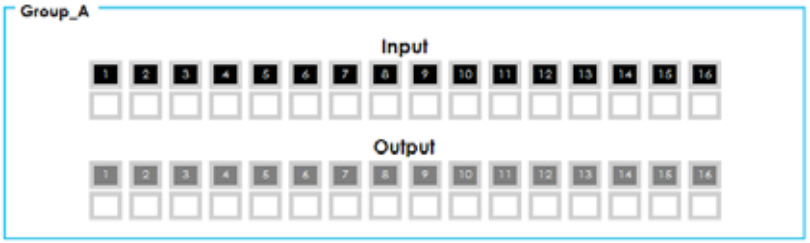


Figure 20 I/O Matrix with Both VPS and Port Grouping Licensed, User With Privilege to First 16 Input and Output Ports Only.



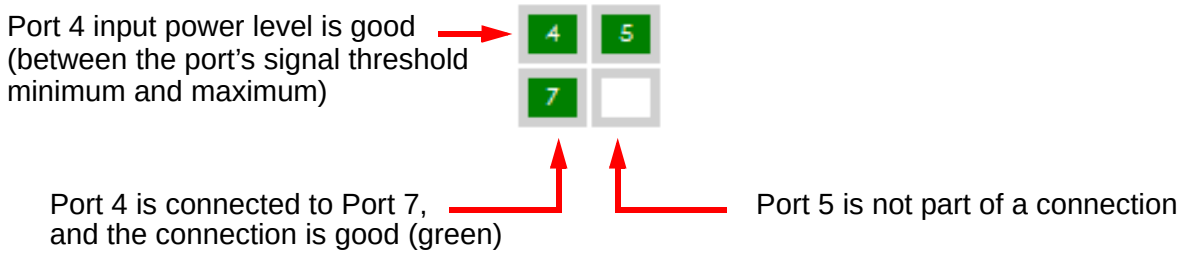
Port Box and Connection Box

The ports in the I/O Matrix are numbered sequentially from 1 to *N* for inputs and outputs, where *N* is the total number of installed ports. The ClickFlow GUI represents each port with two boxes.

The upper box for each port contains the port number, and the lower box is the connection box and contains the number of the peer port to which the port is connected, if a connection exists. If the port is not part of a connection, the lower box will be colored white and will be blank (see Figure 21).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 21 Port and Connection Box Example



ClickFlow uses colors to indicate the status of the ports and connections. See "Legend" on page 96 for a view of the color legend for the Connection Screen.

Configuration Settings

Under the I/O Matrix are a series of check boxes that may be used when configuring connections. With the exception of the **Confirm** check box, these check boxes are used to specify operations to be performed by the system when making connections from the I/O matrix or via the Fiber menu. The available settings are shown in Figure 22 and Figure 23 below.

Figure 22 Connection Box Settings - All Unchecked

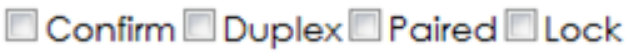
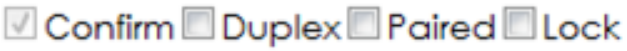


Figure 23 Connection Boxes (Confirm Box Forced by System Policy)



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The configuration settings are described in the following table:

Element	Description
Confirm	The **Confirm** check box enables or disables the Provision Connection window that appears after a connect or disconnect command is selected. When the **Confirm** check box is checked, the ClickFlow GUI will display the Provision Connection window before executing the command. This adds an extra layer of protection against unintended actions. The **Confirm** check box is unchecked by default. To establish a system policy that all users must confirm provisioning changes see “Confirm Required” on page 246.
Duplex	The **Duplex** check box enables Full-Duplex connection mode, which automatically connects two input fibers and two output fibers as a duplex port pair. This mode can save time for users who frequently establish full-duplex connections. Only users with Modify or Manage port-level privileges for all ports in the connection can create duplex connections. When the **Duplex** check box is checked, the ClickFlow GUI will automatically establish an inverse connection to complete a Full-Duplex pair. For example, if the user enables the Duplex mode and then establishes the connection IN1-OUT2, the system will automatically establish the inverse connection IN2-OUT1. **NOTE**: The Duplex setting is ignored for connections between ports with the same port number (i.e., IN1-OUT1, IN2-OUT2, etc.). When the **Duplex** check box is unchecked, the ClickFlow GUI establishes connections in Simplex mode, which connects one input fiber and one output fiber. The **Duplex** check box is unchecked (Simplex) by default. To change the default to Duplex operation, see “Default Connection Mode” on page 247.
Paired	The **Paired** check box is only present when the Paired Connection Mode optional feature is licensed. The **Paired** check box enables the paired connection mode, which automatically connects two input fibers (odd-even pair) to two output fibers (odd-even pair). Only users with Modify or Manage port-level privileges for all ports in the connection can create paired connections. When the **Paired** check box is checked, the ClickFlow GUI will automatically establish two parallel connections. For example, if the user enables the Paired mode and then establishes the connection IN1-OUT1, the system will automatically establish the parallel connection IN2-OUT2. Similarly, if the user enables the Paired mode and then establishes the connection IN2-OUT2, the system will automatically establish the parallel connection IN1-OUT1. The **Paired** check box is unchecked (Simplex) by default. To change the default to Paired see “Default Connection Mode” on page 247.

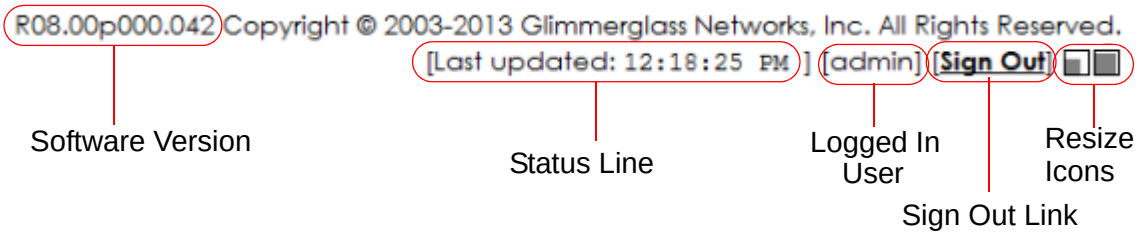
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Lock	The **Lock** check box enables the Lock feature on all subsequently created connections, whether the connections are created manually in the I/O Matrix or are created by importing a topology file (see ”Importing a Topology File” on page 69 for information on importing topology files). When a connection is locked, it cannot be disconnected by any user except the user who established the connection or a user with override privileges, such as the system administrator with Manage port-level privileges. A connection is locked based on the user account that was used to create the ClickFlow GUI session, not a particular session instance. Therefore, a connection locked during a particular session can be broken from a subsequent session as long as the same user name was used to login to the session. Furthermore, connections can be locked only by users with Modify or higher port-level privileges for both ports in the connection. See ”Connection Locking/Unlocking” on page 37 for more information.

Software and Session Information

At the bottom right of the Connection screen, the ClickFlow GUI displays information about the software and the current status of the ClickFlow GUI and user session, as shown in Figure 24.

Figure 24 System Information



Element	Description
Software Version	Displays the software version of the system.
Status Line	The last updated time is always displayed and presents the time of the last successful poll of the switch by the browser. If communication with the switch is interrupted, the cause will be displayed to the right of the last updated time.
Logged In User	User account logged in for this ClickFlow session.

Element	Description
Sign Out Link	Click the link to sign out of the user account and close the ClickFlow GUI session as well as all secondary ClickFlow GUI windows. The **Sign Out** link cancels the session credentials used by the browser, so a user name and password will be required in the future to access the ClickFlow GUI. Use the Sign Out link whenever the ClickFlow GUI is accessed on a public computer so that the ClickFlow GUI cannot be accessed by subsequent users of the computer. When using a secure computer, or when it is okay for the browser to remember the password, the browser window can just be closed without using the **Sign Out** link.
Resize Icons	Adjusts the size of the font and the port boxes used in the ClickFlow GUI display: • Click the left resize icon to use the small font size for the GUI screen. • Click the right resize icon to use the large font size for the GUI screen. The display defaults to a larger font size for systems with less than 100 inputs or outputs and defaults to a smaller font size for systems with 100 or more inputs or outputs.

NOTE: See “System Info” on page 93 for a more complete display of the system hardware and software configuration.

Photonic Multicasting™ Unit

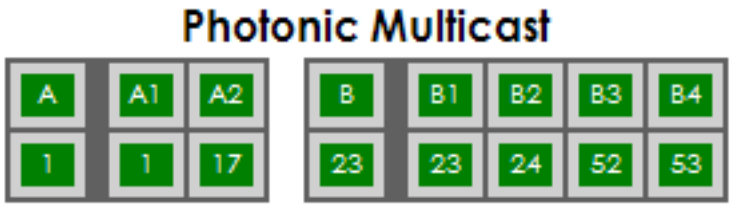
If the system is configured with one or more Photonic Multicasting Units (PMUs), the ClickFlow GUI will display the PMUs in the Connection screen above the I/O Matrix, as shown in Figure 7. A PMU is factory-installed hardware that broadcasts a single input signal to several selected output ports. The PMU itself contains one input port and several output ports. A single standard input port is connected to the PMU input port, then each of the PMU output ports is connected to a standard output port. In this way the signal is broadcast from a single input signal to several output ports. See the procedure ”Creating a Photonic Multicast Unit Connection” on page 38 for the specific steps involved in configuring the PMU to broadcast a single input signal.

The ClickFlow GUI displays the input port of the PMU on the left and identifies it with a single character, such as “A” or “B” (see Figure 25). The ClickFlow GUI displays the output ports of the PMU to the

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

right of the input port and marks them with the same letter as the associated input port as well as a number, such as “A1” or “A2.”

Figure 25 One 1:2 and One 1:4 Photonic Multicasting Units (PMUs)



As with all the ports on the system, each PMU port is represented with two boxes. The upper box contains the PMU port ID, and the lower box contains the number of the I/O port to which the PMU port is connected. The status of the PMU connections is indicated by the color codes described in ”Port Box and Connection Box” on page 18.

The table below shows the PMU port IDs and default port names displayed in the Port Information Box (see ”Port Information Box” on page 11) corresponding to the PMU configuration shown in Figure 25. PMU ports may also be referenced via their 5-digit port number. The Port Report shows the PMU port's 5-digit port number and port name (see “Port” on page 80).

PMU Port	PMU Port ID	PMU Default Port Name
First PMU, Input	A	MC-1
First PMU, Output 1	A1	MC-1-1
First PMU, Output 2	A2	MC-1-2
Second PMU, Input	B	MC-1
Second PMU, Output 1	B1	MC-2-1
Second PMU, Output 2	B2	MC-2-2
Second PMU, Output 3	B2	MC-2-3
Second PMU, Output 4	B2	MC-2-4

The PMU port names can be revised, as described in ”Ports” on page 111.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Variable Optical Attenuation (VOA)

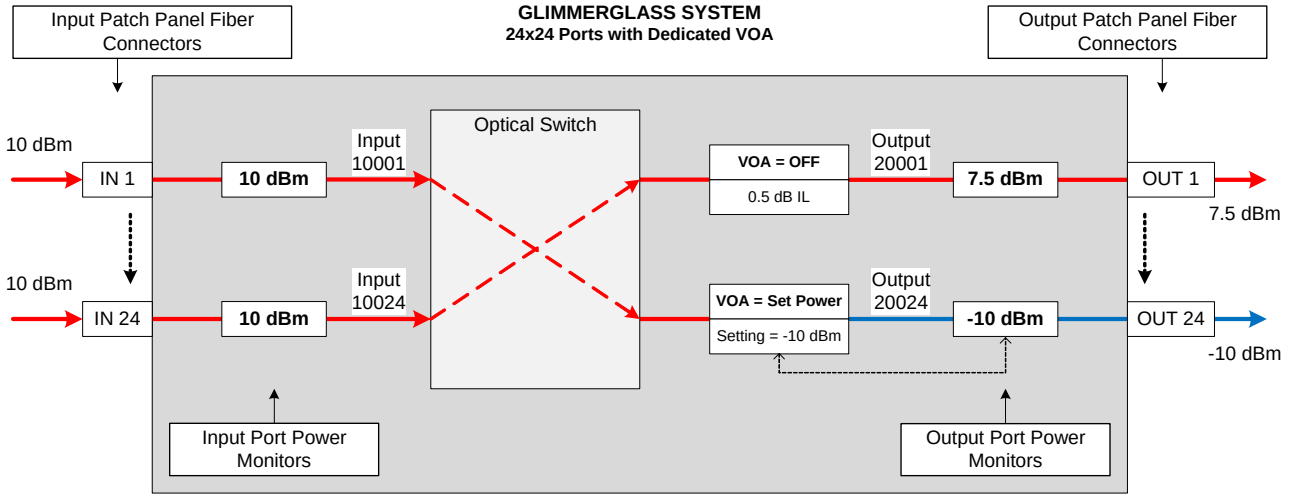
A Variable Optical Attenuation device (VOA) is a factory-installed hardware option. Each VOA device contains eight individually controllable VOA elements that allow variable attenuation of the optical power level of a signal connected through the element. Each system can support as many as four VOA devices (32 VOA elements).

There are two possible hardware implementation options for VOA, Dedicated VOA and Switched VOA, which are described in the following two sections of this chapter. Both implementations may be ordered on the same system, but the two different implementations cannot share a single eight-port VOA device.

Dedicated VOA

With Dedicated VOA, the eight elements of the VOA device are placed in-line on standard output ports that are specified by the user when the system is ordered. This means that in order to control the input power level for receivers and test equipment, the equipment must be connected to the output ports that house VOA elements. Figure 26 shows a functional representation of the implementation of Dedicated VOA in the system switch fabric.

Figure 26 Dedicated VOA Implementation



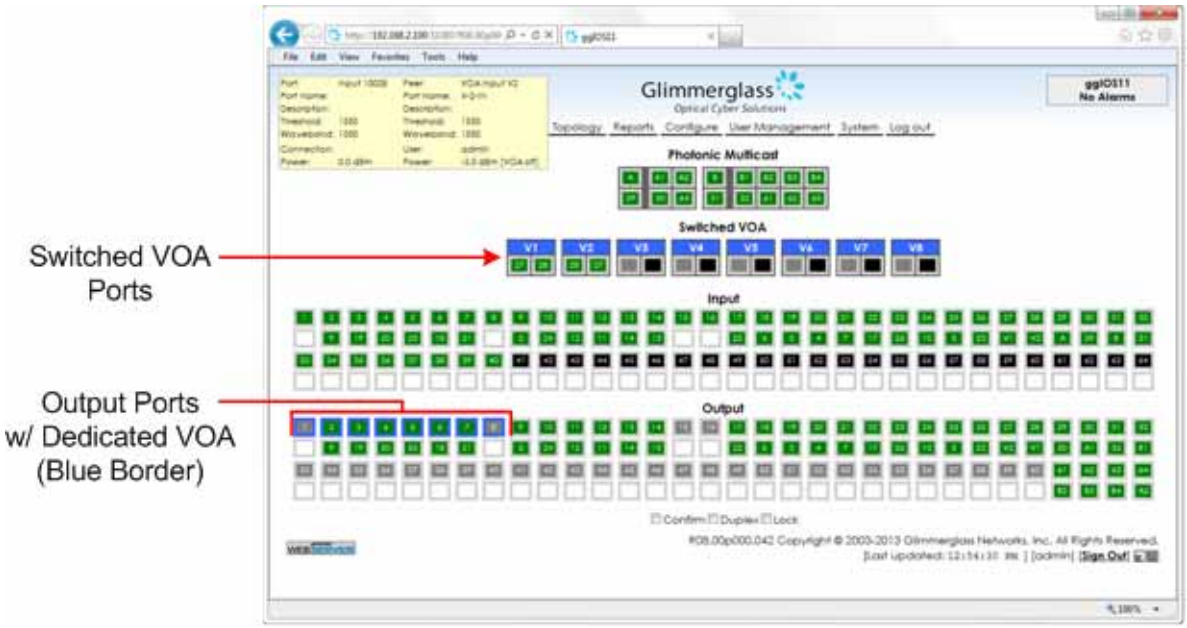
As can be seen in Figure 26, the output power of the signal corresponds to user-specified output power level configured for the VOA element. Because of this, Dedicated VOA supports only the Set Power mode of operation (see “Modes of Operation for VOA” on page 165). Once the power level is specified by the user, the VOA element will automatically attenuate the switched signal to maintain the proscribed dBm level at the output port. The VOA elements inserted inline have an intrinsic loss of between 0.4dB to 1dB depending upon the waveband (loss on higher end for 1310nm). From

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 26, the connection to OUT 1 shows that the loss is higher for connections even when the VOA is off.

The ClickFlow GUI highlights the Dedicated VOA output ports by displaying them with a blue border in the output section of the I/O Matrix, as shown in Figure 27.

Figure 27 VOA Displays in the ClickFlow GUI



The ClickFlow GUI also displays the VOA settings and peer port information in the Port Information box (see “Port Information Box” on page 11). Move the mouse cursor over the Dedicated VOA port to view the Port Information box for the Dedicated VOA element. The table below shows the Dedicated VOA port numbers and default port names corresponding to the eight Dedicated VOA elements shown in Figure 27.

Dedicated VOA Output Port ID	Dedicated VOA Port Number	Dedicated VOA Default Port Name
1	20001	VO-1
2	20002	VO-2
3	20003	VO-3
4	20004	VO-4
5	20005	VO-5
6	20006	VO-6
7	20007	VO-7

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Dedicated VOA Output Port ID	Dedicated VOA Port Number	Dedicated VOA Default Port Name
8	20008	VO-8

The Dedicated VOA/output port names can be revised, as described in ”Ports” on page 111.

Unlike Photonic Multicast or Switched VOA ports, Dedicated VOA output ports are in the I/O Matrix. From the connection point of view, these ports are treated as normal output ports and may be connected using the ”Connection Methods” on page 32.

For information on configuring the VOA mode and settings, see”Configuring VOA Ports” on page 166.

Switched VOA

With Switched VOA, the elements of the VOA are connected internally between the input and output ports on the optical switch, so that they can be used for connections between any input port and any output port.

NOTE: The Switched VOA implementation is available only on systems that have the Input Detection feature.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 28 and Figure 29 show functional representations of the implementation of Switched VOA in the system switch fabric with set power mode (Figure 28) and with attenuate mode (Figure 29).

Figure 28 Switched VOA Implementation (Set Power Mode) View

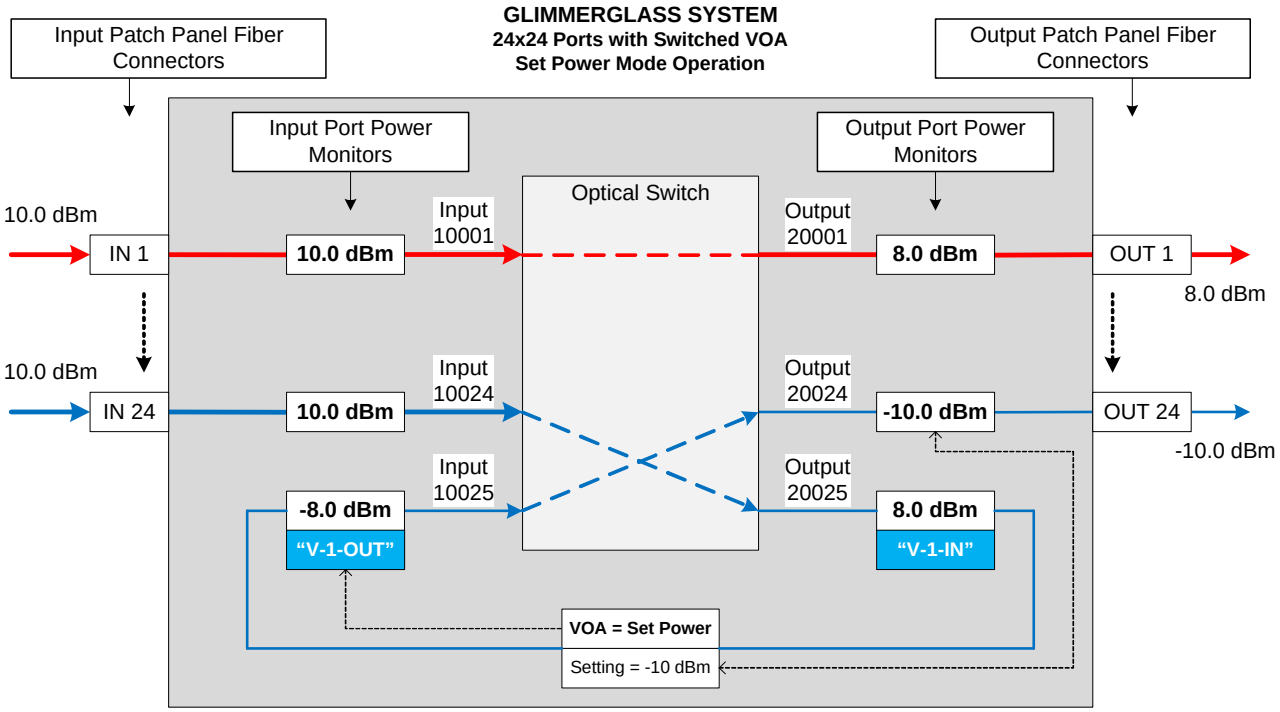
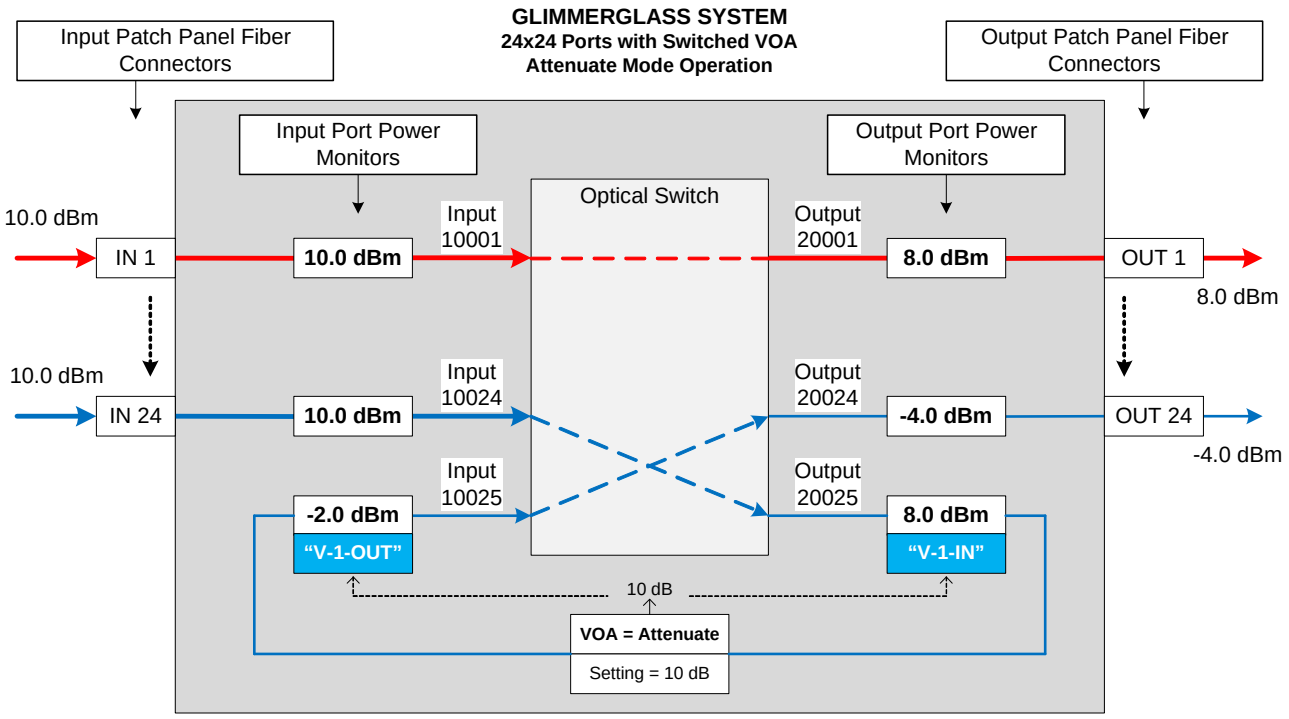


Figure 29 Switched VOA Implementation (Attenuate Mode)



As shown in Figure 28 and Figure 29, Switched VOA elements are not dedicated to output ports. The VOA elements are a shared resource and any user input port can connect to any user output port through the Switch VOA element. The input of the VOA element is connected to the output side of the switch. Similarly, the output of the VOA element is connected to the input side of the switch.

For example, Figure 28 shows a connection between input port 24 ("10024") and output port 24 ("20024") through the VOA. Notice that this end-to-end connection is formed by making two separate connections. The first leg of the connection is from input user port 24 to the input side of the VOA, "V-1-IN". The second leg of the connection is from the output side of the VOA, "V-1-OUT", to user output port 24. The signal passes from the output side of the optical switch through the VOA and back to the input side of the optical switch. The labeling of Switched VOA ports is discussed below in this section. Switched VOA ports, like Photonic Multicast ports, are reference ports with no external connection. In the ClickFlow interface, they are represented by names as opposed to their port numbers.

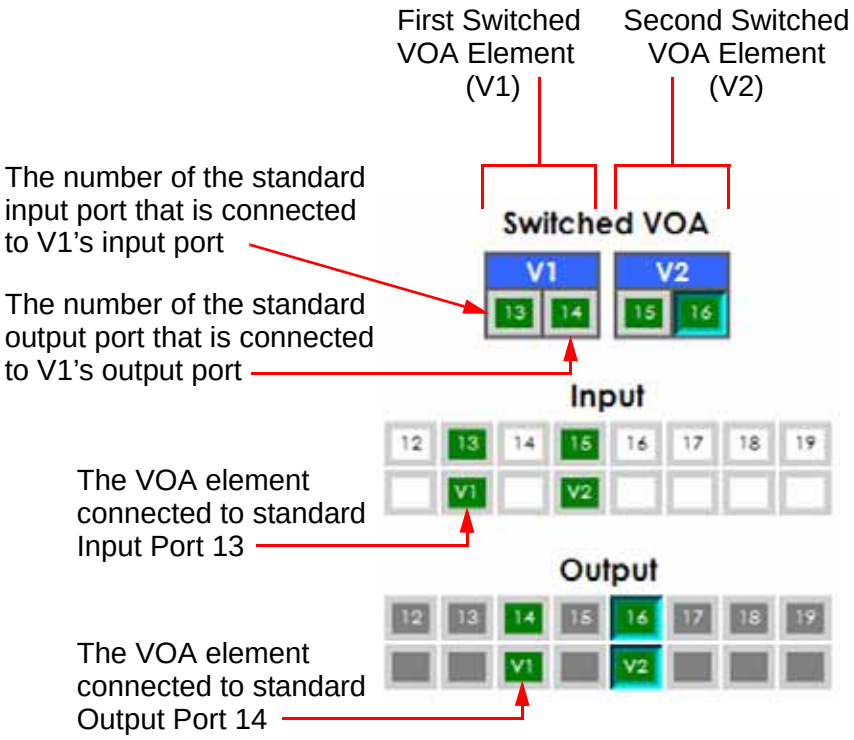
Switched VOA supports both the Set Power mode of operation and the Attenuate Power mode of operation (see "Modes of Operation for VOA" on page 165).

The ClickFlow GUI displays each Switched VOA element in a standalone, two-port box above the I/O Matrix. The VOA elements are numbered sequentially starting with V1 (for Switched VOA element

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

number 1) and each VOA element is represented by two ports: The input to the VOA on the left and the output of the VOA on the right. Figure 30 shows an example Switched VOA display.

Figure 30 Switched VOA Display



The ClickFlow GUI display in Figure 30 depicts two discrete Switched VOA elements, named "V1" and "V2." V1 is inserted into the connection between Input Port 13 to Output Port 14. Therefore, the connection from Input Port 13 to Output Port 14 is actually composed of two separate connections:

- Input Port 13 to the VOA input on V1 (V-1-IN)
- The VOA output on V1 (V-1-OUT) to Output Port 14

Similarly, V2 supports a connection between Input Port 15 and Output Port 16. Note that the Switched VOA element number is shown as the connected port in the input and output connection matrices (e.g., Input Port 13 is connected to V1 and Output Port 14 is connected to V1).

The status of the VOA connections is indicated by the color codes described in "Port Box and Connection Box" on page 18.

The ClickFlow GUI also displays the VOA settings and peer port information in the Port Information box (see "Port Information Box" on page 11). Move the mouse cursor over the Switched VOA display to view the Port Information box for the Switched VOA element.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The table below shows the Switched VOA port IDs and default port names corresponding to the first four Switched VOA elements shown in Figure 27 on page 25. Switched VOA ports may also be referenced via their 5-digit port number. The Port Report shows the Switched VOA port's 5-digit port number and port name (see “Port” on page 80).

Table 1 Switched VOA Port IDs and Default Port Names

Switched VOA Port	Switched VOA Port ID	Switched VOA Default Port Name
First Switched VOA input	V1	V-1-IN
First Switched VOA output	V1	V-1-OUT
Second Switched VOA input	V2	V-2-IN
Second Switched VOA output	V2	V-2-OUT
Third Switched VOA input	V3	V-3-IN
Third Switched VOA output	V3	V-3-OUT
Fourth Switched VOA input	V4	V-4-IN
Fourth Switched VOA output	V4	V-4-OUT

The Switched VOA port names can be revised, as described in ”Ports” on page 111.

See the following sections of this manual for information on connecting and configuring Switched VOA ports:

- See ”Creating a Switched VOA Connection” on page 38 for information on connecting Switched VOA ports.
- See ”Configuring VOA Ports” on page 166 for information on configuring VOA ports.

Configuring Ports and Provisioning Connections

ClickFlow provides several methods for configuring ports and provisioning connections (making, breaking, updating, and assigning connection attributes).

Port configuration may be performed directly on the Connection screen or under the Configuration menu. The methods and differences are described in ”Port Configuration” on page 39.

With the exception of importing topologies (Chapter 5), all connection activity is performed directly on the Connection screen. The following section “Connection Provisioning” describes the various connection types, modes and methods.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Connection Provisioning

This section provides an overview of both the types of connections which may be provisioned using ClickFlow as well as the methods provided to make, break, or update these connections. The above activities are controlled by the **Confirm**, **Duplex**, and **Paired Connection** check boxes.

Confirm Operation Check Box

ClickFlow supports two modes of operation for making and breaking connections.

- The No Confirmation mode (**Confirm** check box is unchecked) does not require confirmation by the user. This mode only supports making/breaking connections. As no confirmation is required, the operation occurs immediately.
- The Confirm mode (**Confirm** check box is checked) requires all provisioning (make/break) requests to be confirmed by the user prior to being executed. This mode opens a Provisioning Window appropriate to the connection type (simplex, duplex, or paired). The provisioning windows and operation are described in Chapter 3 ”Port Box Context Menu” on page 43.

Duplex and Paired Check Boxes (Connection Types)

ClickFlow supports three connection types: simplex, duplex, and paired. The connection type is based upon the settings for the Duplex and Paired check boxes. These boxes are mutually exclusive (both cannot be checked). If both are unchecked, the connection type is Simplex (default). The connection types are described below:

- Simplex (Figure 31)—A simplex connection is a connection between an input port and output port. The signal is unidirectional and flows from the input fiber to the output fiber as shown in Figure 31 below.
- Duplex (Figure 32)—A duplex connection requires 2 input ports and 2 output ports and is used to connect devices requiring separate transmit and receive fibers as shown in Figure 32 (e.g., 2-fiber SFP/XFP).
- Paired (Figure 33)—A paired connection requires 2 input ports and 2 output ports as well. However, devices are connected straight through. Typically, one connection carries video data and the other connection carries BIDI signals for control of the device providing the video feed.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE: Connections involving Photonic Multicast or Switched VOA ports are simplex connections. These ports cannot be used in duplex or paired connections. For information on making connections using Photonic Multicast or Switched VOA ports, see ”Photonic Multicast and Switched VOA Connections” on page 37.

Figure 31 Signal Flow of a Simplex Connection

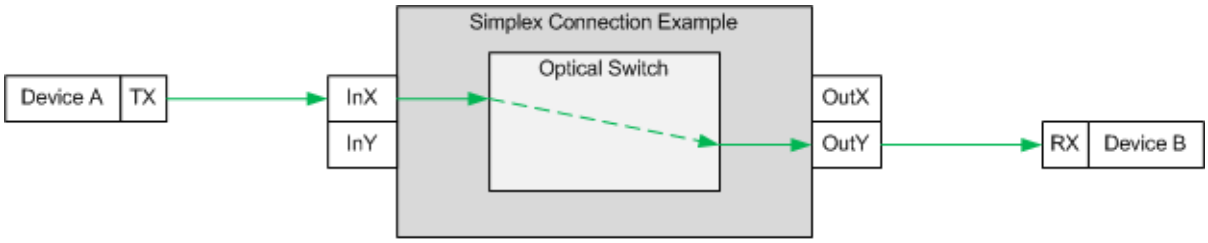


Figure 32 Signal Flow of a Duplex Connection

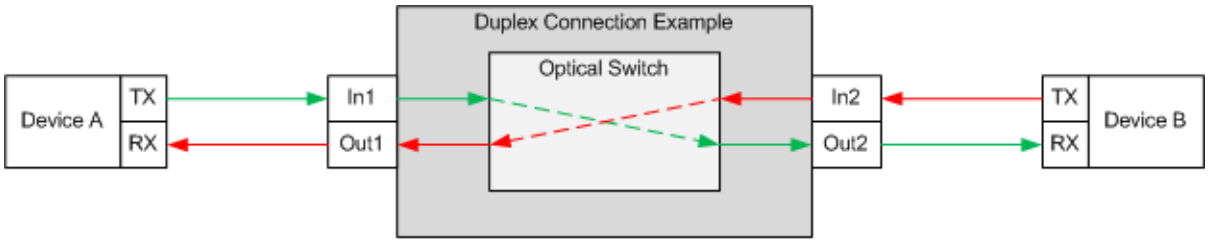
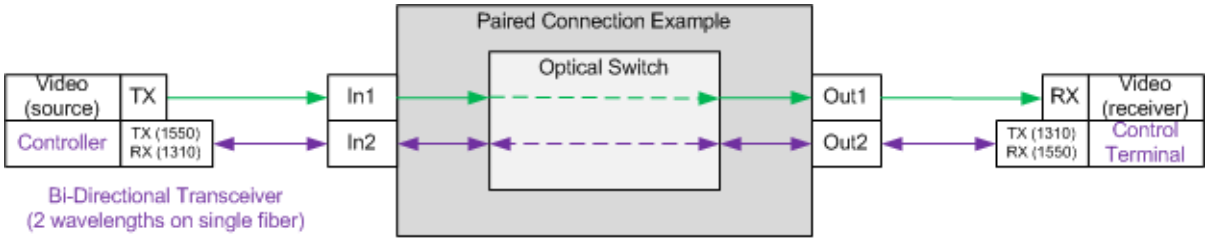


Figure 33 Signal Flow of a Paired Connection



Connection Methods

The following methods are available for provisioning connections on the Connection screen:

- Double-click
- Fiber menu (**Fiber > Connect** or **Fiber > Disconnect**)
- Right-click

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

If the Confirm check box is unchecked (No Confirm mode) then the first two methods may be used to quickly make/break connections. In No Confirm mode, the user will not be able to update the configuration for existing connections.

If the Confirm check box is checked, then both these methods will cause a provisioning window to open. The provisioning window opened will be based upon the Duplex and Paired check box settings.

The right-click method will always open a provisioning window which corresponds to the settings for the Duplex and Paired connection configuration check boxes. If both are unchecked, the provisioning window will correspond to a simplex connection. The following tables describe how these methods are used when making, breaking or updating connections.

Making a Connection

The table below lists alternate ways for establishing a connection.

NOTES: The ports to be connected cannot be part of an existing connection.
Port-level privilege of Modify or higher is required on all ports in the connection.
To connect all ports in a single operation, see ”Connecting All Ports” on page 55.

Method	Steps for Making a Connection
Double-click	1. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set for the desired connection type. 2. Left-click on one port for the connection 3. Double-click on the other port for the connection 4. If the **Confirm** check box on the Connection screen is checked, then a provisioning window will open allowing entry of configuration information and requiring user to explicitly make the connection: • Optionally revise the connection description, connection lock, connection alarm severity, or make changes to port configuration (names, descriptions, thresholds, waveband) • Click the **Make Connection** button in the Provision Connection window

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Method	Steps for Making a Connection
Fiber > Connect menu option	1. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set for the desired connection type. 2. Left-click on one port for the connection 3. Left-click on the other port for the connection 4. Select **Fiber > Connect** from the Connection screen menu 5. If the **Confirm** check box on the Connection screen is checked, then a provisioning window will open allowing entry of configuration information and requiring user to explicitly make the connection: • Optionally revise the connection description, connection lock, connection alarm severity, or make changes to port configuration (names, descriptions, thresholds, waveband) • Click the **Make Connection** button in the Provision Connection window
Right-click	1. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set for the desired connection type. 2. Left-click on one port for the connection 3. Right-click on the other port for the connection 4. Select the **Provision** option from the Port Box context menu 5. Optionally revise the connection description, connection lock, connection alarm severity, or make changes to port configuration (names, descriptions, thresholds, waveband) 6. Click the **Make Connection** button in the Provision Connection window

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Breaking a Connection

The table below lists alternate ways for breaking a connection.

Method	Steps for Making a Connection
Double-click	1. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set corresponding to the connection type to break. 2. Double-click on one of the ports in the connection to be broken. 3. If the **Confirm** check box on the Connection screen is checked, then a provisioning window will open showing the connection configuration and configuration of the ports in the connection. Review the information in the provisioning window to verify this is the correction connection to break: • If this is the correct connection, click the **Break Connection** button and the connection will be broken. • If this is not the correct connection, click the **Cancel** button to abort the operation and close the provisioning window.
Fiber > Disconnect menu option	1. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set corresponding to the connection type to break. 2. Left-click on one of the ports in the connection to be broken. 3. Select **Fiber > Disconnect** from the Connection screen menu 4. If the **Confirm** check box on the Connection screen is checked, then a provisioning window will open showing the connection configuration and configuration of the ports in the connection. Review the information in the provisioning window to verify this is the correction connection to break: • If this is the correct connection, click the **Break Connection** button and the connection will be broken. • If this is not the correct connection, click the **Cancel** button to abort the operation and close the provisioning window.
Right-click	1. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set corresponding to the connection type to break. 2. Right-click on one of the ports in the connection to be broken. 3. Select the **Provision** option from the Port Box context menu. 4. Review the information in the provisioning window to verify this is the correction connection to break: • If this is the correct connection, click the **Break Connection** button and the connection will be broken. • If this is not the correct connection, click the **Cancel** button to abort the operation and close the provisioning window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Updating a Connection

The table below lists alternate ways for updating a connection without interrupting the connection.

NOTES: Port-level privilege of Modify or higher is required on all ports in the connection. Port-level privilege of Manage or higher is required on one of the ports in the connection if the connection is locked by another user.

Method	Steps for Making a Connection
Double-click	1. Ensure that the **Confirm** check box on the Connection screen is checked. 2. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set corresponding to the connection type to update. 3. Double-click on one port for the connection. 4. Review the information in the provisioning window to verify this is the correction connection to update: • If this is not the correct connection, click the **Cancel** button to abort the operation and close the provisioning window. • If this is the correct connection, revise the connection description, connection lock, connection alarm severity, or make changes to port configuration (names, descriptions, thresholds, waveband as required. 5. Click the **Update Connection** button to update the connection.
Fiber > Connect menu option	1. Ensure that the **Confirm** check box on the Connection screen is checked. 2. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set corresponding to the connection type to update. 3. Left-click on one port of the connection to be updated. 4. Select **Fiber > Connect** from the Connection screen menu 5. Review the information in the provisioning window to verify this is the correction connection to update: • If this is not the correct connection, click the **Cancel** button to abort the operation and close the provisioning window. • If this is the correct connection, revise the connection description, connection lock, connection alarm severity, or make changes to port configuration (names, descriptions, thresholds, waveband as required. 6. Click the **Update Connection** button to update the connection.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Method	Steps for Making a Connection
Right-click	1. Ensure that the Connection screen **Duplex** and **Paired** check boxes are set corresponding to the connection type to update. 2. Right-click on one port of the connection to be updated. 3. Select the **Provision** option from the Port Box context menu 4. Review the information in the provisioning window to verify this is the correction connection to update: • If this is not the correct connection, click the **Cancel** button to abort the operation and close the provisioning window. • If this is the correct connection, revise the connection description, connection lock, connection alarm severity, or make changes to port configuration (names, descriptions, thresholds, waveband as required. 5. Click the **Update Connection** button to update the connection.

Connection Locking/Unlocking

The **Lock** check box may be used to both lock and unlock connections. When the **Lock** box is checked, all the above methods in ”Making a Connection” on page 33 will make the connection and assign the lock to this user. No other user will be able to disconnect this connection unless the user has the Manage port privilege for at least one of the ports in the connection.

When a provisioning window is used to make a connection the user may override the setting of the **Lock** check box on the Connection screen by using the **Lock** check box contained in the provisioning window.

Users may also change the connection lock setting from the provisioning window when using the window to perform and update on an existing connection

Photonic Multicast and Switched VOA Connections

All connections involving either Photonic Multicast or Switched VOA ports are simplex connections.

The fibers to/from these optical devices (splitter and VOA elements respectively) are internally spliced between an output port on the switch and one or more input ports on the switch (more than one port for a splitter, one port for the VOA). This allows these devices to be shared resources. Any I/O Matrix input port may connect to the device's input and then the device's output(s) may be connected to any I/O Matrix output port.

The ClickFlow screen I/O Matrix presentation for these devices uses labels instead of port numbers to indicate the input to the device and output from the device. In the port reports, however, port num-

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

bers are used. When reviewing the reports, remember that the input to a device is actually an internal output port on the optical switch (20xxx port number) and device outputs are actually internal input port(s) (10xxx port numbers) on the optical switch.

The steps to make connections involving both Photonic Multicasting and Switch VOA units are described in the following sections:

- “Creating a Photonic Multicast Unit Connection” (below)
- “Creating a Switched VOA Connection” (page 38)

Creating a Photonic Multicast Unit Connection

If the system is configured with one or more Photonic Multicasting Units (PMUs), the ClickFlow GUI will display the PMUs in the Connection screen above the I/O Matrix (see “Photonic Multicasting™ Unit” on page 25)

Perform the following steps to establish a multicast connection between an input port and multiple output ports using the Photonic Multicasting Unit (PMU):

1. Make a connection between a port in the I/O Matrix Input section and a Photonic Multicast input port, for example between “1” (input 10001) and “A” (multicast input A). (See ”Making a Connection” on page 33 for the steps to creating a connection.)

2. Make a connection between a port in the I/O Matrix Output section and a Photonic Multicast output port, for example between “11” (output 20011) and “A1” (multicast output A1).

3. Repeat step 2 for other I/O Matrix Output section ports and Photonic Multicast output ports as required, for example between “12” (output 20012) and “A2” (multicast output A2).

Creating a Switched VOA Connection

If the system is configured with Switched VOA elements (SVOA), the ClickFlow GUI will display the SVOA ports in the Connection screen above the I/O Matrix (see ”Switched VOA” on page 29 for details about the SVOA).

Perform the following steps to establish a multicast connection between an input port and an output port involving a SVOA element.

1. Make a connection between a port in the I/O Matrix Input section and a Switched VOA input port (the gray port on the left), for example between “1” (input 10001) and “V1” (VOA input V1). See ”Making a Connection” on page 33 for the steps to creating a connection.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

2. Make a connection between a port in the I/O Matrix Output section and the Switch VOA output port (the port on the right), for example between “11” (output 20011) and “V1” (VOA output V1).

3. Configure the VOA. See ”Configuring VOA Ports” on page 166.

”Configuring VOA Ports” on page 166When using Switched or Dedicated VOAs, remember that the VOA mode/setting are attributes of the VOA element. Any connection through the device will subject to the VOA mode/setting and these may be adjusted before or after the connection to achieve the desired performance.

Port Configuration

Several methods are provided to configure port attributes. The ability to configure ports is provided both from the port boxes on the Connection Screen (Chapter 3, ”Port Box Context Menu” on page 43) as well as from the Connection Screen Main Menu (Chapter 7, ”Configure” on page 99).

The port box method is well suited for modifying one or a few ports. For changing all ports or ranges of ports, the best methods are the options presented in Chapter 7.

Table 2 below indicates the configuration methods available for each port attribute. The notes at the end of the method indicate the scope available with each operation. This table assumes the user has the port privileges required to make the changes. The privileges and requirements for the operations are discussed along with the procedures for each method.

Table 2 Accessing Port Configuration Operations

Port Attribute	Methods to Configure	Scope
Port Name, Port Description	Port Box Context Menu > Configure Port Box Context Menu > Provision Configure > Ports > Change Port Configuration Configure > Ports > Import/Export Port Configuration	(one-at-a-time) (all ports in connection) (all ports, one-at-a-time) (all ports)
Port Group	Port Box Context Menu > Configure Port Box Context Menu > Provision Configure > Ports > Change Port Configuration Configure > Ports > Import/Export Port Configuration	(one-at-a-time) (all ports in connection) (all ports, one-at-a-time) (all ports)

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Port Attribute	Methods to Configure	Scope
Port Group	Port Box Context Menu> Provision Configure > Ports > Change Group Assignment Configure > Ports > Import/Export Group Assignment	(one-at-a-time) (all ports by port group) (all ports)
Signal Threshold	Port Box Context Menu > Configure Port Box Context Menu > Provision Configure > Ports > Change Port Configuration Configure > Ports > Change Signal Threshold Assignment	(one-at-a-time) (all ports in connection) (all ports, one-at-a-time) (all ports by threshold)
Waveband	Port Box Context Menu >Configure Configure > Ports > Change Waveband Assignment	(one-at-a-time) (all ports)
MinPwrSev, MaxPwrSev, ConnAlmSev	Port Box Context Menu >Configure Configure > Ports > Change Alarm Severity Assignment	(one-at-a-time) (all ports by severity)

Input Port Waveband Setting

The waveband input port attribute is used to specify the transmission waveband of the signal on the fiber connected to an input port. In the switch, the power monitors are calibrated using 1310nm and 1550nm sources. In addition, connection optimization utilizes the waveband setting. Assign the correct waveband to the input port to achieve the best switch times and output power stability as well as for the most accurate optical power readings.

Two waveband options, 1310 and 1550, are provided to assign to the input ports. When a connection is made, the input signal band is automatically applied to the connected-to output port. The table below shows the correct waveband to assign to the input port based upon the wavelength transmission band on the fiber connected to the port.

Table 3 Signal Band Assignments for Each Wavelength Transmission Band

Transmission Band	Description	Wavelength Range	Waveband to Assign
O-band	Original Band	1270nm - 1360nm	1310
E-band	Extended Band	1360nm - 1460nm	1310
S-band	Short Band	1460nm - 1530nm	1550
C-band	Conventional Band	1530nm - 1565nm	1550
L-band	Long Band	1565nm - 1625nm	1550

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Port Signal Threshold Setting

A signal threshold record defines power levels and hysteresis for reporting and clearing optical power alarms for a port. The power levels (minimum and maximum acceptable power) are determined by the user based upon the requirements for the signal being connected through the system (see “Signal Thresholds” on page 103 for information on configuring signal thresholds).

For example, if all incoming signals for an input port should be no less than -5dBm and any incoming signal with a power less than -5dBm is suspect and should generate an alarm, the user can create a signal threshold with a minimum power alarm at < -5dBm and assign that signal threshold to the input port.

Similarly, if for an output port the user knows the loss budget to the downstream receiver, the user can set the minimum optical power alarm to occur if the output power reading falls below the value indicated by the loss budget. On the maximum power side, the user may know the saturation specifications of the receiver (optical power is too high) and so the user can set a maximum power alarm threshold so that the system will alarm and notify the user for this condition as well.

Signal thresholds allow the user to establish the correct criteria for any port in the system. The user may create as many signal thresholds as are required. Alternatively, all ports may be configured to use a single signal threshold if there is no requirement to have different thresholds for input and output ports.

Again, the power readings which are used by the system to evaluate the optical power against the signal threshold settings are determined by the waveband setting for the port. If the signal at the input port is changed, re-evaluate if the signal threshold assignment needs to change as well.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

THIS PAGE INTENTIONALLY LEFT BLANK

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Port Box Context Menu

3

Overview

The Port Box Context Menu options (Figure 34 below) allow users to configure port and connection parameters directly from the Connection screen by right-clicking on a port box in the I/O Matrix (see page 16 for more information on the I/O Matrix). This method for configuring ports is well suited for making modifications concurrent with making/breaking connections and/or modifying a few ports identified as requiring changes.

Figure 34 Port Box Context Menu (Right-click on Upper Port Box

Methods to configure ranges of ports are available as well (see ”Ports” on page 111). In addition to configuration by ranges, methods are available to import files for port names/description and port group assignment or to edit all port name/descriptions from a table showing all ports. See ”Connections” on page 143 for a description of the methods to view and change connection descriptions from a table showing all established connections.

Refer to Chapter 6, “Reports,” on page 75, for information regarding tabular reports for viewing both port configuration as well as connection configuration

The table below describes the Port Box context menu options and provides the page numbers where the menu options are further detailed in this chapter.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

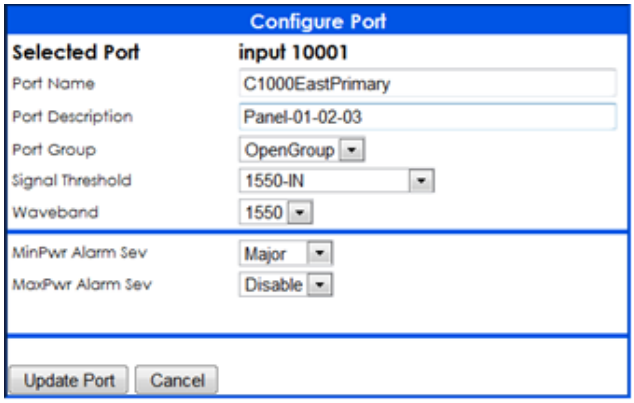
Menu Option	Description	Page
Configure	Opens the Configure Port window. The Configure Port window supports modification of the following port configuration items: • Port Name • Port Description • Port Group (only if the Port Group license is enabled) • Port Signal Threshold • Waveband (only present for Input Ports) • MinPwr Alarm Sev • MaxPwr Alarm Sev • Connection Alarm Sev (only present for Output Ports) With the exception of Port Group, the above fields may be configured by a user with the port privilege of Modify for the port. Port Group modification requires the port privilege of Manage. Users with View privilege for the port will be able to open the window to view the configuration but will not be able to update the configuration.	45
Provision	Opens one of three Provision Connections windows depending on the Connection Box Settings. These windows are: • Provision Connection • Provision Duplex Connection (when Duplex box is checked) • Provision Paired Connection (when Paired box is checked) The provision windows allow configuration of port attributes (excluding alarm severities) and connection attributes. This may be done when the connection is being made or later as an update to the connection configuration (without affecting the connection integrity).The following modifications are supported: • Connection Description • Connection Lock • Connection Alarm Severity • Port Names • Port Descriptions • Signal Thresholds • Waveband All of the above operations require the user to have Modify privileges for both ports in the connection. To override another user's connection lock requires Manage port privileges. The **Provision** option is only presented when the user has the required privileges to make, update, or break the connection.	49
Deselect	Deselect all I/O Matrix ports of the same input/output type. This menu selection is only used for ClickFlow GUI testing.	N/A

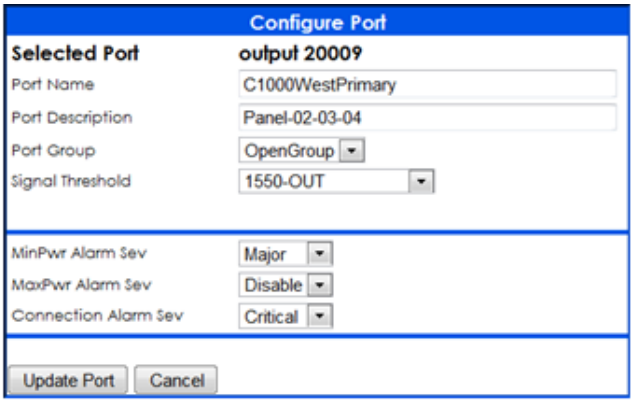
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Configure

The **Configure** option in the Port Box context menu opens the Configure Port window from which the port configuration may be viewed or revised. The window is slightly different for input and output ports, reflecting the fact that some parameters are direction dependent. Figure 35 below shows the Configure Port window for both input (left) and output (right) ports.

Figure 35 Configure Port Window





Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The table below describes the elements of the Configure Port window.

NOTES: With the exception of the Port Group pull-down, the fields in the Configure Port window may be configured by a user with the port privilege of Modify for the port.

The Port Group pull-down is present only on systems licensed for Port Grouping. On licensed systems, the pull-down is read-only (dimmed) unless the user has Manage privileges for all ports in the system.

All ClickFlow fields preclude entry of invalid characters as well as entries which exceed the maximum supported string length for the field.

Element	Description
Selected Port	Displays the port type and port number/ID of the selected port.

Port Name	Displays the current name configured for the selected port.
	• Text box:
	  • 32 character maximum
	  • Port names must be unique (two ports cannot have the same port name)
	  • The following punctuation characters are not permitted in a port name: quote, apostrophe, semi-colon, colon, backslash, comma, and whitespace.
	• Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege

Port Description	Displays the current description configured for the selected port.
	• Text box:
	  • 32 character maximum
	  • The semi-colon character may not be used in a port description.
	• Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege

Port Group	Displays the name of the Port Group to which the port is assigned. This field is only displayed on systems licensed for Port Grouping. • Pull-Down: List of all port groups configured in the system • Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Signal Threshold	Displays the name of the signal threshold assigned to the selected port. • Pull-Down: List of all signal thresholds configured in the system • Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege
Waveband	Input Port Only: Displays the name of the waveband assigned to the selected port. • Pull-Down: Two options: 1310 or 1550 • Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege
MinPwr Alarm Sev	Displays the severity used when reporting a signal threshold minimum (STMIN) alarm on the selected port. • Pull-Down: Choices are: Critical, Major, Minor, Notice and Disable • Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege
MaxPwr Alarm Sev	Displays the severity used when reporting a signal threshold maximum (STMAX) alarm on the selected port. • Pull-Down: Choices are: Critical, Major, Minor, Notice and Disable • Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege
Connection Alarm Sev	Output Port Only: Displays the severity used when reporting a connection failure (CSFLT) alarm on the selected port. • Pull-Down: Choices are: Critical, Major, Minor, Notice and Disable • Edit Privilege: Modify or higher for port, read-only (dimmed) for View privilege
Update Port Button Update Port	This button applies changes made by the user. The button is inactive for users with View privileges for the port.
Cancel Button Cancel	This button exits the Configure Port window without applying changes. When clicked, the Configure Port window will close immediately.

Using the Port Configure Window to Configure a Port

The steps below describe the process for using the Configure Port window to revise a port's configuration. Modify or higher privilege is required to change all fields, with the exception of Port Group. Manage privilege for all ports is required to change the port group assignment.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

1. Right-click on a port in the I/O Matrix to open the Port Box context menu (Figure 34 on page 43).

2. Select **Configure** in the Port Box context menu to open the port's Configure Port window (Figure 35 on page 45).
   - To change the port's name, select and edit in the **Port Name** field
   - To change the port's description, select and edit in the **Port Description** field
   - To change the port's port group assignment, click on the **Port Group** pull-down in the window and select the desired group from the pull-down list. (See "Port Groups" on page 146 for information on port groups.)
   - To change the port's signal threshold, click on the **Signal Threshold** pull-down in the window and select the desired threshold name from the pull-down list. (See "Port Signal Threshold Setting" on page 41 for information on signal thresholds.)
   - (For input ports only:) To change the port's waveband, click on the **Waveband** pull-down in the window and select the desired waveband from the pull-down list. (See "Input Port Waveband Setting" on page 40 for information on wave-bands.
   - To change the port's minimum power alarm (STMIN) severity, click on the **MinPwr Alarm Sev** pull-down in the window and select the desired severity from the pull-down list.
   - To change the port's maximum power alarm (STMAX) severity, click on the **MaxPwr Alarm Sev** pull-down in the window and select the desired severity from the pull-down list.
   - (For output ports only:) To change the port's connection alarm (CSFLT) severity, click on the **Connection Alarm Sev** pull-down in the window and select the desired severity from the pull-down list

3. Click the **Update Port** button to save the port configuration changes, or click the **Cancel** button to cancel the configuration changes and close the Configure Port window.

NOTES: After clicking the **Update Port** button, the Configure Port window will display "Port updated successfully" for a few seconds and then close. If an error occurs, for example if the entered port name is a duplicate, the Configure Port window will display an error message and remain open.

Modifying the severity of an alarm for port with and existing active alarm for this condition will not change the severity of the already logged alarm. Changing the severity to Disable, however, will clear this active alarm for the port.

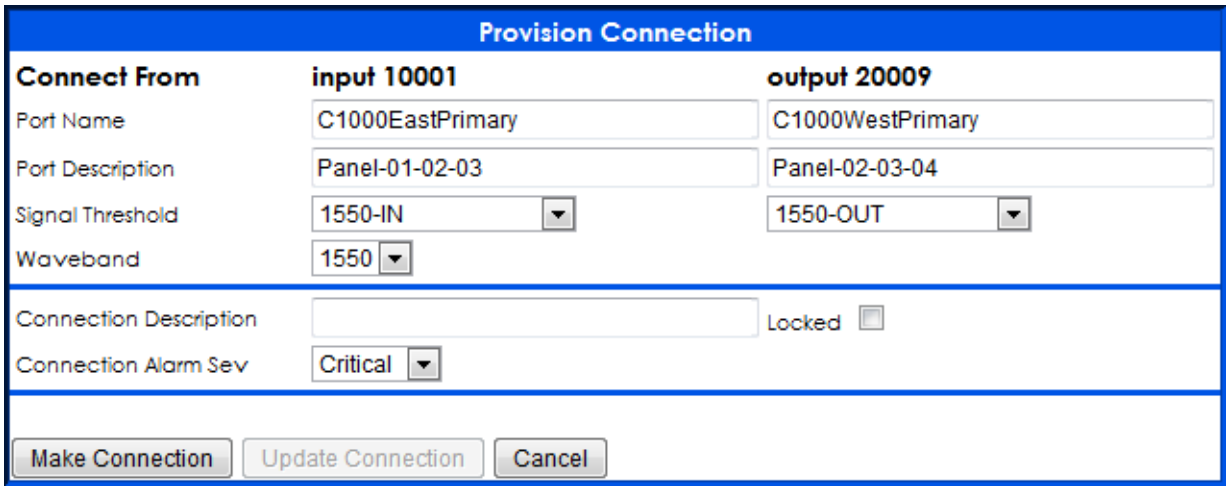
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Provision

The **Provision** option in the Port Box context menu will open one of three provisioning windows depending on the ports selected in the Connection screen and the state of the Duplex and Paired check boxes at the bottom of the Connection screen.

If neither check box is checked, the Provision Connection window will open (similar to the one shown in Figure 36). The **Make Connection** button at the bottom left indicates that these two ports have been selected to be connected.

Figure 36 Provision Connection Window (Make Connection)



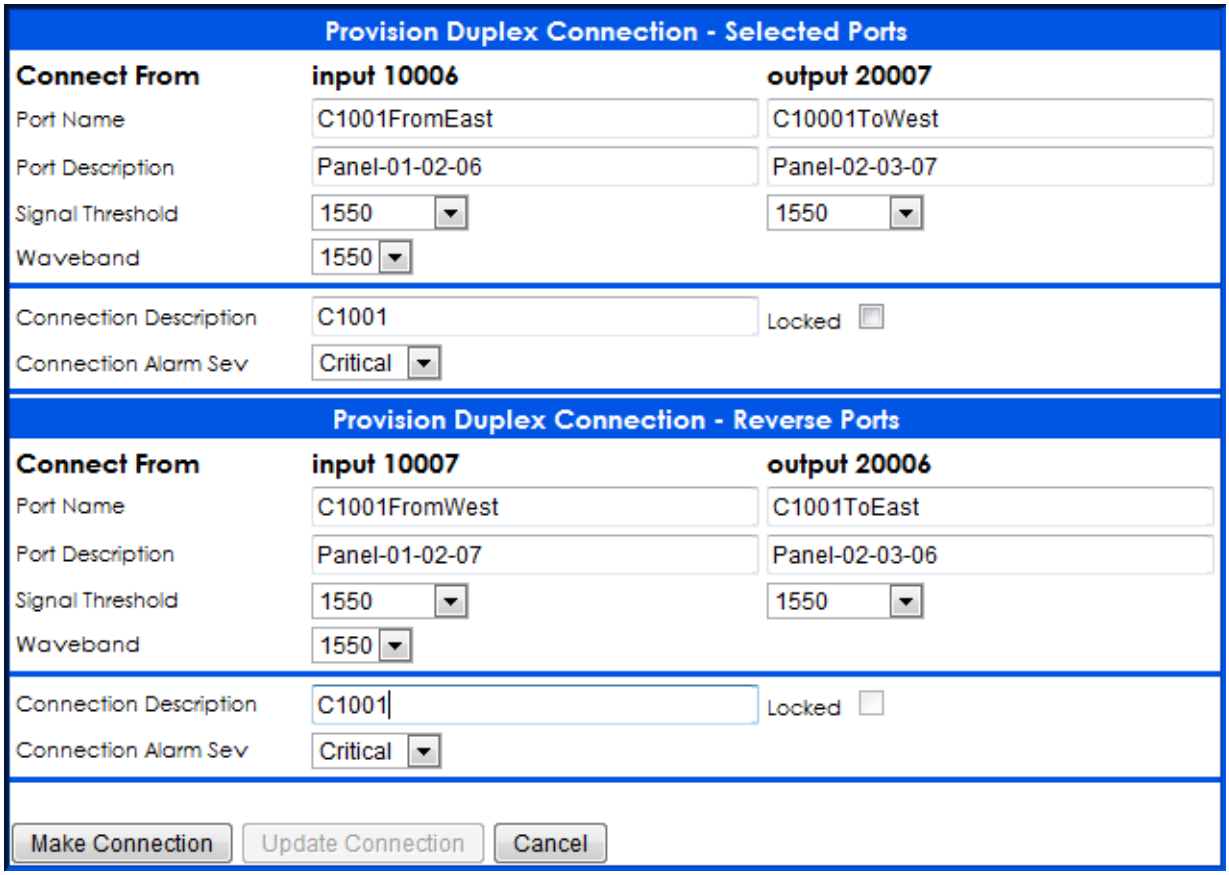
For duplex connections, the bulleted criteria below must be met for making, updating, or breaking a duplex connection. Duplex connections consist of two connections crossed between the specified input and output ports. Therefore, if input 5 and output 20 are connected with the duplex check-box enabled, then the system will automatically establish the reverse direction connection between input 20 and output 5.

- The **Duplex** check-box must be checked
- Neither port may be a Photonic Multicast or Switched VOA port (make connection check)
- The selected input an output port numbers must be different (make connection check)
- For break and update, an error pop-up will occur if the reverse connection is not found for connection selected.

If the above criteria are met, the window opened will be the Provision Duplex Connection window like the one shown in Figure 37.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 37 Provision Duplex Connection Window (Make Connection)



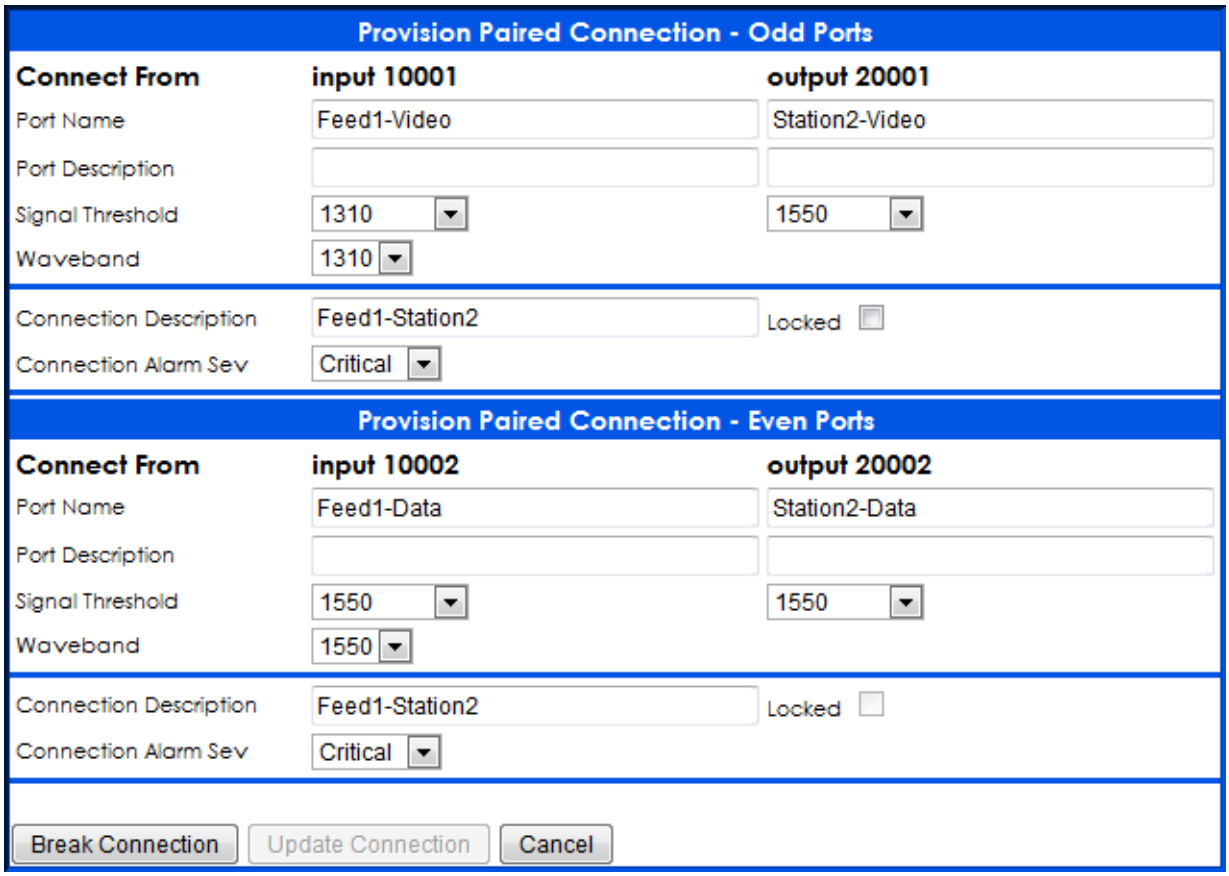
For paired connections, the bulleted criteria below must be met for making, updating, or breaking a paired connection. Paired connections are highly specialized. They require that adjacent odd/even numbered input ports be connected to adjacent odd/even numbered output ports (odd-odd, even-even). Therefore, if input 1 and output 11 are connected with the paired check-box enabled, then the system will automatically establish a connection between input 2 and output 12. If the even number ports are specified, the adjacent odd port the number previous. So, if input 12 is connected to output 24 then the system will automatically connect input 11 to output 23.

- The **Paired** check-box must be checked
- Neither port may be a Photonic Multicast or Switched VOA port (make connection check)
- The selected input an output port numbers must both be odd numbers or both even numbers (make connection check)
- For break and update, an error pop-up will occur if the adjacent connection is not found for connection selected

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

If the above criteria are met, the window opened will be the Provision Paired Connection window like the one shown in Figure 38.

Figure 38 Provision Paired Connection Window Example (Break Connection)



All three windows allow the user to configure/modify connection and view the pertinent port information in support of making, updating, or deleting connections. The difference among the windows is that the Duplex and Paired options allow concurrent configuration for both connections requested by the Duplex or Paired specification.

If the **Confirm** check box in the Connection screen is checked, then the appropriate provisioning window will always be presented regardless of the method used to make, update, or break connections. The various connection methods are described in “Connection Methods” on page 32. The two methods below are the most common to make and break connections:

- Click on an unconnected port (input or output), then double-click on an unconnected port of the opposite type (output or input). The Provision Connection window opens to allow confirmation of the make connection request (e.g., Figure 36 on page 49 and Figure 37 on page 50). The user may make the connection with the current settings,

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

or the user may fully provision the connection (configure ports and configure connection) and then make the connection.

- Double-click on a connected port. The provision connection window opens to allow confirmation of the break connection request or provided the opportunity to update the configuration of the existing connection(s) (e.g., Figure 38 on page 51). Note that the **Update Connection** button becomes active only if one of the parameters in the window is changed.

The table below describes the elements of the Provision Connection windows. The input port information is in the left column of the Provision Connection window, the output port information is in the right column.

NOTES: Modify privileges are required on both ports to configure the fields in the Provision Connection window. If the user has only View privilege (for one or both ports) then the fields are view-only. Exceptions to the Modify privilege rule for both ports:

- Manage privilege is required on one of the ports to break or update a connection which has been locked by another user. Without the required privilege, the break/update buttons will not be active.
- To break an unlocked connection, it is sufficient to have the Modify privilege on only one of the ports in the connection.

Element	Description
Connect From	Displays the port type and port number/ID of the selected input port (left column) and output port (right column).
Port Name	Displays the current names configured for the input port and output port.
Port Description	Displays the current descriptions configured for the input port and output port.
Signal Threshold	Displays the name of the signal threshold assigned to the input port and the name of the signal threshold assigned to the output port.
Waveband	Displays the name of the waveband currently assigned to the input port.
Connection Description	Displays the configured connection description of the selected connection. When opening a provision connection window to make a connection, the connection description will be blank.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Locked	This check box displays the Lock status of the connection. When making a connection, this check box will default to the setting of the **Lock** check box on the Connection screen (which may be overridden here).
Connection Alarm Sev	Displays the connection alarm severity (CSFLT) of the output port in this connection or to be used when making a connection.
Make/Break Connection Button Make Connection Break Connection Break Connection	When clicked, this button will apply any configuration changes made by the user to port and connection attributes. The text in and the status of this button are context dependent. • For making connections, the button will display “Make Connection”. • For an existing connection, this button will display “Break Connection” and be active if the user has the port privileges required to disconnect. • If the user does not have the required privileges, the “Break Connection” button will be inactive.
Update Connection Button Update Connection Update Connection	When clicked, this button will apply any configuration changes made by the user to port and connection attributes. The button becomes active when the user (with the required port privileges) modifies one of the fields in the provisioning window. Otherwise, the button will be inactive. If the user does not have the required privileges, the button will stay inactive (as all field are read-only)
Cancel Button Cancel	This button exits the provisioning window without applying changes. When clicked, the provisioning window will close immediately.

Using the Port Box Context Box Provision Option to Make Connections

Unconnected ports can be connected by a user with port-level privilege Modify or higher on all ports to be connected. Perform the following steps to establish a connection or connections (duplex or paired).

1. Check or uncheck the Connection Boxes based upon the type of connection to be provisioned (single, duplex, or paired).

2. In the I/O Matrix, left-click on one port for the connection to select the port.

3. Also in the I/O Matrix, right-click on the second port to be connected to open the Port Box Context Menu (Figure 34 on page 43).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

4. Select the **Provision** option from the context menu to open the appropriate provisioning window.

5. In the provisioning window, the following actions may be taken prior to making the connection:
   - To modify a port name, select and edit in the **Port Name** field for the desired input and/or output port(s).
   - To modify a port description, select and edit in the **Port Description** field for the desired input and/or output port(s).
   - To change a port signal threshold, click on the **Signal Threshold** pull-down and select a threshold name from the pull-down list for the desired input and/or output port(s).
   - To change the waveband, click on the **Waveband** pull-down and select the desired waveband from the pull-down list.
   - To assign a description to the connection(s), select and edit in the **Connection Description** field(s).
     NOTE: For duplex and paired connections, the connection description entered for the top connection is automatically assigned to the lower connection unless overridden by an entry in the lower connection field.
   - To set the connection(s) lock status, check/uncheck the box labeled **Locked**.
     NOTE: For duplex and paired connections, the lock state is automatically assigned to both connections.
   - To change the connection alarm severity, click on the **Connection Alarm Sev** pull-down and select a severity from the pull-down list. This must be done for each connection when duplex or paired. This field is not automatically assigned like the connection description.

6. Click the **Make Connection** button to save the configuration changes and make the connection, or click the **Cancel** button to cancel the configuration changes and close the Provision Connection window without making the connection.

NOTE:	After clicking the **Make Connection** button, the Provision Connection window will display “Connection updated successfully” for a few seconds and then close. If an error occurs, for example a duplicate port name, the Provision Connection window will display an error message and remain open.

Using the Port Box Context Box Provision Option to Update Connections

Connection/port information can be updated by a user with port-level privilege Modify or higher on all ports in the connection(s). Perform the following steps to update a connection(s). This activity will not

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

cause any disruption to the existing connections; these changes simply update the connection information.

1. Check or uncheck the Connection Boxes based upon the type of connection to be updated (single, duplex, or paired).

2. In the I/O Matrix, right-click on one of the ports in the connection(s) to open the Port Box Context Menu (Figure 34 on page 43).

3. Select the **Provision** option from the context menu to open the appropriate provisioning window.

4. In the provisioning window, update the information as desired:
   - To modify a port name, select and edit in the **Port Name** field for the desired input and/or output port(s).
   - To modify a port description, select and edit in the **Port Description** field for the desired input and/or output port(s).
   - To change a port signal threshold, click on the **Signal Threshold** pull-down and select a threshold name from the pull-down list for the desired input and/or output port(s).
   - To change the waveband, click on the **Waveband** pull-down and select the desired waveband from the pull-down list.
   - To modify connection description(s), select and edit in the **Connection Description** field(s).
   - To change the connection(s) lock status, check/uncheck the box labeled **Locked**.
     NOTE: For duplex and paired connections, the lock state is automatically assigned to both connections.
   - To change the connection alarm severity, click on the **Connection Alarm Sev** pull-down and select a severity from the pull-down list. This must be done for both connections when duplex or paired.

5. Click the **Update Connection** button to save the configuration changes, or click the **Cancel** button to cancel the configuration changes and close the Provision Connection window without making the updates.

NOTES: After clicking the **Make Connection** button, the Provision Connection window will display “Connection updated successfully” for a few seconds and then close. If an error occurs, for example a duplicate port name, the Provision Connection window will display an error message and remain open.

Modifying the connection alarm severity for a connection with an existing active alarm will not change the severity of the already logged alarm. Changing the severity to Disable, however, will clear connection alarm.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Using the Port Box Context Box Provision Option to Break Connections

Breaking connection(s) requires the user to have Modify or higher port privileges on at least one port in the connection. In addition, Manage privileges on at least one port are required to overcome a connection lock set by another user. Perform the following steps to break a connection(s). Note: If the user has Modify privileges for all the ports, it is possible to change the port configuration as in the previous two sections (making/updating connections). These changes will be applied concurrent with removing the connection(s). However, the steps below simply cover a normal break procedure.

1. Check or uncheck the Connection Boxes based upon the type of connection to be updated (single, duplex, or paired).

2. In the I/O Matrix, right-click on one of the ports in the connection to display the Port Box context menu (Figure 34 on page 43).

3. Select the **Provision** option in the Port Box context menu to open the Provision Connection window (Figure 38 on page 51).

4. View the information in the Provision Connection window to verify that this is the connection to be broken.

5. Click the **Break Connection** button to break the connection(s), or click the **Cancel** button to close the Provision Connection window without breaking the connection(s).

NOTE:	After clicking the **Break Connection** button, the Provision Connection window will display “Connection broken successfully” for a few seconds and then close. If an error occurs, the Provision Connection window will display an error message and remain open.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Fiber

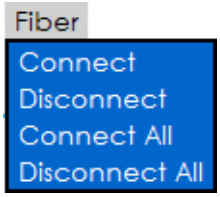
4

Overview

The **Fiber** menu options configure the connections between the input and output ports selected in the I/O Matrix (see page 16 for more information on the I/O Matrix).

NOTE:	The terms “port” and “fiber” are used interchangeably in this document.

Figure 39 Fiber Menu



The table below describes the **Fiber** menu options and provides the page numbers where the menu options are further detailed in this chapter.

Menu Option	Description	Page
Connect	Creates a connection between the input port and output port selected in the I/O Matrix.	58
Disconnect	Deletes a connection between the input port and output port selected in the I/O Matrix.	58
Connect All	This option is displayed only to users with the system-level privilege of Manage. When used, Connect All will attempt to make straight-through connections between all input and output ports in the I/O Matrix (i.e., IN1-OUT1, IN2-OUT2, IN3-OUT3, IN4-OUT4, etc.).	59

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description	Page
Disconnect All	This option is displayed only to users with the system-level privilege of Manage. When used, this command disconnects all connections which the user has the port privilege to disconnect. If the user has Modify or higher port privileges to all ports, then all connections are disconnected.	60

NOTES:
- To establish a connection, the user must have at least Modify privileges for both ports.
- To disconnect, the user must have at the Modify privilege for one of the ports in the connection.
- Port group rules override user port privileges. No user can connect two ports (regardless of port privilege) if the connection would violate port grouping rules.
- In addition to the above, the **Connect All** and **Disconnect All** options are displayed in the menu only for users with the system privilege of Manage.

Connect

The **Fiber > Connect** menu option creates a connection between the selected input port and selected output port. This is one of three methods by which an individual connection may be established (see ”Connection Methods” on page 32 for a description of all methods).

Disconnect

The **Fiber > Disconnect** menu option disconnects the selected connection. This is one of three methods by which an individual connection may be broken (see ”Connection Methods” on page 32 for a description of all methods).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Connect All

The **Fiber > Connect All** menu option establishes a 1:1 connection between all standard input ports and output ports in the I/O Matrix (i.e., IN1-OUT1, IN2-OUT2, IN3-OUT3, IN4-OUT4, etc.).

NOTES:
- If the system is installed in a duplex networking environment carrying IP traffic, the Connect All operation could cause packet forwarding loops. Please use this command with caution.
- The Connect All operation is constrained by port grouping.
- The Connect All operation will disconnect existing connections as required to form the new straight through connections.
- The Connect All operation applies only to the input/output ports in the I/O Matrix. Photonic Multicast and Switched VOA ports are not connected.
- The Connect All menu option is available only to users with the system privilege of Manage. These users do not necessarily have Modify privileges for all ports. The Connect All operation observes the user's port privilege assignments.

Connecting All Ports

To connect all input and output ports in a 1:1 configuration:

1. From the main Connection screen, select the **Fiber > Connect All** menu option.
2. Click **OK** in the confirmation box to verify and execute the 1:1 configuration.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Disconnect All

The **Fiber > Disconnect All** menu option clears all connections in the I/O Matrix, Photonic Multicasting Units (if installed), and Switched VOA (if installed).

NOTE:	This menu option is displayed only to users with Manage system-level privileges. The Disconnect All operation abides by the user's port privilege assignments. So if the port-privilege level is View or less on both ports, the user cannot disconnect the port using Disconnect All. Furthermore, if the port-privilege is Modify or less, the user cannot disconnect connections locked by another user.

Disconnecting All Connections

To disconnect all connections in the I/O Matrix, Photonic Multicasting Units, and Switched VOA elements:

1. In the main Connection screen, select the **Fiber > Disconnect All** menu option.
2. Click **OK** in the confirmation box to verify and execute the Disconnect All operation.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Topology

5

Overview

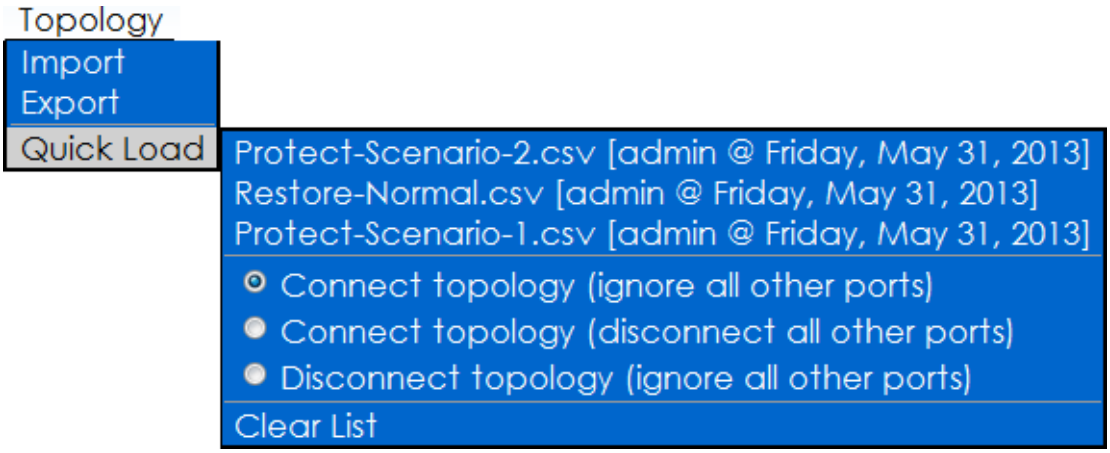
The term “topology” refers to a defined set of connections in the system. A topology (connection set) may be created in two ways:

- Off-system, by specifying connections in a .csv or .txt file and then applying the file to the system using the topology import operation defined in this chapter.
- Exporting: Capturing the current connections on the system and recording these connections to an external topology file (see ”Exporting a Topology” on page 71). The export topology operation is provided for this capability. Exporting known connection sets for later import (see ”Importing a Topology File” on page 69) is often used as a method to rapidly restore a known good topology or to apply one of many saved topologies which record the connections required for different purposes.

In addition to the above, the system will retain the last ten topologies loaded in a quick load list, allowing these previously imported topologies to be applied immediately.

Figure 40 shows the **Topology** menu in the ClickFlow GUI.

Figure 40 Topology Menu



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The required format for a topology files is discussed in ”Topology File Format Guidelines” on page 62. That section also presents the format for exported files and describes how the fields in the file are treated upon import.

The table below describes the **Topology** menu options and provides the page numbers where the menu options are further detailed in this chapter.

NOTE: When a user applies a topology to the system, the user's port privileges for the ports in the file are ascertained and enforced. If the user's privileges preclude making or breaking certain connections, then those connections will not be made or broken. The topology import or quick load application will be constrained appropriately.

Menu Option	Description	Page
Import	Imports (applies) a connection topology from a .csv file to the system then stores the file in the Quick Load list if the file name does not conflict with an existing name in the list. **NOTE**: The system will connect or break connections based upon the user's port privileges. Therefore, it is possible that not all contained connections will be made or disconnected.	68
Export	Exports the current connection topology from the system to a .csv file. This operation is subject to the following constraint: **NOTE**: The file will contain only the connections which are fully viewable by the user.	70
Quick Load	Maintains a list of the last ten imported connection topology files (uniquely named) and enables single-click importing of topologies directly from the system memory. Quick Load provides an efficient way to import frequently-used topologies. Quick Load is subject to the same constraints as Import.	71

Topology File Format Guidelines

One way to create a topology file is to simply export the current topology to a file and then save the file (see “Exporting a Topology” on page 71 for this procedure). Figure 41 shows the contents of a topology.csv file exported from a switch with six active connections.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 41 Example of Exported Topology File Exported

#Glimmerglass Optical Switch Topology File					
#SwitchName: LN0001					
#UserName: admin					
#Generated: Fri May 31 18:21:11 2013					
#<This comment entered when the connection set was exported.>					
#Format: 8.0					
#<Input>	<Output>	[<SignalBand>]	[<ConnectionDescription>]	[<InputSigThresh>]	[<OutputSigThresh>]
InPort1	OutPort1	1310	Connection1	1310-In	1310-Out
InPort2	OutPort2	1550	Connection2	1550-In	1550-Out
InPort3	OutPort3	1550	Connection3	1550-In	1550-Out
10004	20004	1310	Connection4	1310	1310
10005	20005	1550		1550	1550
10006	20006	1310		Test	Test

Referencing Figure 41, the format of a topology file may contain the following elements as described in the table below. The table also indicates which fields are mandatory and which are optional.

NOTES:
- For connecting ports using the topology, the only required fields are the ports to be connected.
- If an invalid name or incorrect long port number is used (e.g., 30xxx), then the entire import request will fail.
- The import request tolerates incomplete or incorrect information in the optional fields. This is for two reasons: First, it may be of paramount importance to quickly restore connectivity and not be blocked by inconsistent values. Second, it is possible to create topologies with only the input and output fields entered - allowing the system to use the existing port configuration in conjunction with the connection.
- When the optional values are present and are valid (e.g., the signal threshold named is configured), then these values will be applied.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
#Comment Lines (Optional)	The user may enter comments at the top of the file (before the start of the comma separated values). Comments are not mandatory, but if included they must be marked with a hash (#) character at the start of each line as shown in the first seven lines in Figure 41: • (Title line): Glimmerglass Optical Switch Topology File • SwitchName: <SystemName from which topology was exported> • UserName: <ID of the user that exported the topology> • Generated: <Date/time when export was performed> • (Comment line): This line will contain any comments entered at the time of export. This line is optional; If nothing is entered, the line is not included. • Format: <Software release on the system from which topology was exported> • (Column title line): This is a reference line showing the order of entry for the values which may be entered in comma separated format. These fields are defined in the following rows of this table and are marked as required or optional.
<Input> (Required Field)	The input port for the connection; must be either the long port number (e.g., 10xxx) or the unique port name. When exported, the field value is: • The port's name if one exists. If not, then the long port number. • For PMU and VOA ports, the default system name will be used if the user has not configured a specific name. Errors impacting connect/disconnect: • An invalid port number or port name will block the import and no connections will be made/broken. • A valid port number that does not exist either in the system or for the user will be ignored. Line with invalid port numbers are ignored; the rest of the lines are completed.
<Output> (Required Field)	The output port for the connection; must be either the long port number (e.g., 20xxx) or the unique port name. (See the description for the <Input> element for field values and possible errors.)

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
[<SignalBand>] (Optional Field)	The signal band of the input port. • Possible values: 1310, 1550, or <null> • When exported, the field value is the waveband currently assigned to the input port in the connection. • When creating or editing a topology file, this value may be left empty (null). The system will use the current value for the input port when connecting the topology. Possible errors (when using import to connect): • Invalid Signal Band value is entered. Import will ignore the value. The current value for the input port will be used when making the connection.
[<ConnectionDescription>] (Optional Field)	A description for the connection. • When exported, the field value is the connection description already in use for the connection. This field will be empty (null) if a description is not configured. • When creating or editing a topology file, this value may be left empty (null). The system will not assign a connection description when making the connection. If the connection already exists and has a name, the name value will not be changed when the topology is applied. Possible errors (when using import to connect): • Connection Description entered is too long. Import will ignore the value. The connection will be made without a connection description.
[<InputSignalThresh>] (Optional Field)	The existing signal threshold to use for the input port in the connection • When exported, the field value is the signal threshold value assigned to the input port. • When creating or editing a topology file, this value may be left empty. The system will use the current value for the input port when making the connection. Possible errors (when using import to connect): • Signal Threshold name is invalid (does not exist in the system). Import will ignore the value. The connection will be made. The signal threshold assigned to the input port will not change.

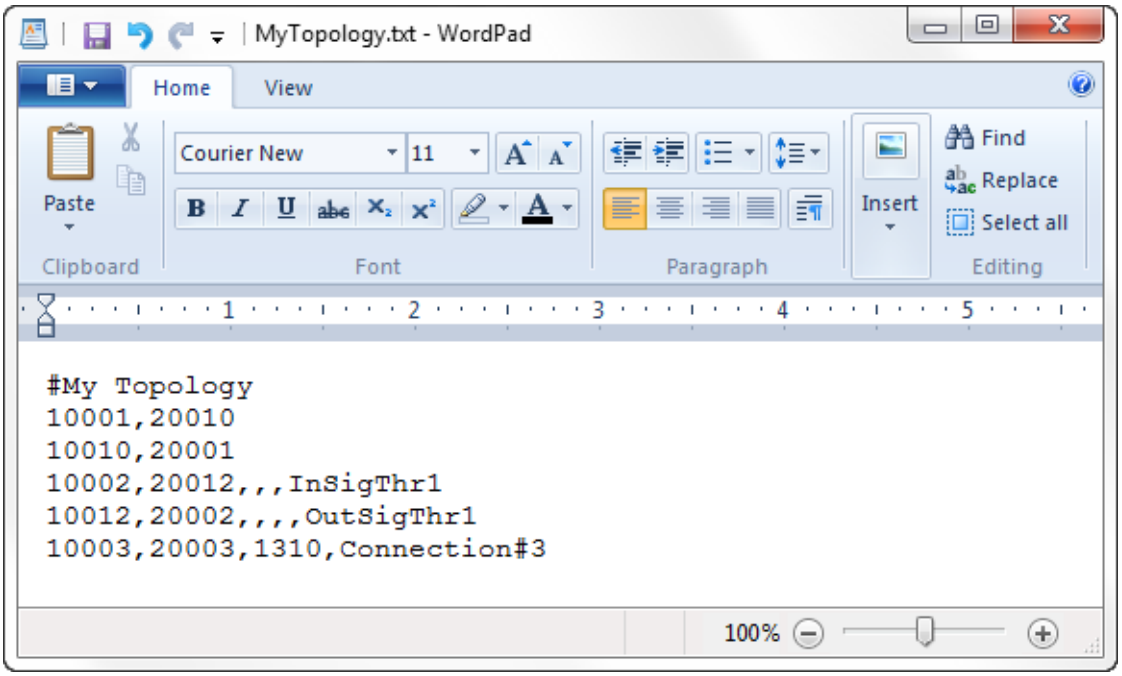
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
[<OutputSignalThresh>] (Optional Field)	The existing signal threshold to use for the output port in the connection • When exported, the field value is the signal threshold value assigned to the input port. • When creating or editing a topology file, this value may be left empty. The system will use the current value for the input port when making the connection. Possible errors (when using import to connect): • Signal Threshold name is invalid (does not exist in the system). Import will ignore the value. The connection will be made. The signal threshold assigned to the output port will not change.

The easiest method for working with topology files is to export a file from the system and then modify the comments and information as required in a spreadsheet application such as Excel. This allows the benefits of the working in the spreadsheet as well as the option to save as a .csv file. The image in Figure 41 on page 63 is pulled from Excel. Alternatively, open a new file in Excel and use the grid to represent each of the required fields and then save as a .csv file.

Another method to create topology file is using a text editor such as WordPad or Notepad. Figure 42 shows a simple example of a file, “MyTopology”, containing a single comment and a few connections as a demonstration of how simple it is to create topology files. In this case, the file is saved as a .txt file.

Figure 42 Example of Topology File Created with a Text Editor



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Note that commas are required to indicate the position of each field when a subsequent field is entered for the connection:

- The first two lines in Figure 42 indicate only the first two fields for the connection (<Input> and <Output>). Since no additional fields are entered for the connection there is no comma required after the <Output> field.
- The fourth and fifth lines include the first two fields, then leave the next two optional fields empty, then provide a value for the fifth field. The empty fields must be indicated by empty commas, as shown.
- The last line contains values for the first three fields with a comma separating each field. The rest of the fields are left empty so the subsequent commas can be left out.

Note that the best method would be to include the comma separator for all fields, both mandatory and optional.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Connection Mode Options

Before importing a topology from a text file to the system, a connection mode must be specified to instruct the ClickFlow GUI on how existing connections are to be treated during the import process. The following table describes the three connection modes.

Term	Description
Connect Topology (Ignore all other ports)	This mode is used to make all connections in the topology file. All other connections (not involving ports in the topology file) will not be affected.
Connect Topology (Disconnect all other ports)	This mode is used to make all connections in the topology file and to disconnect any existing connections not included in the topology file.
Disconnect Topology (Ignore all other ports	This mode is used to break all connections included in the topology file. All other connections in the system are not affected.

NOTES: For connecting topologies:

- If all connections in the topology are already connected, connecting the topology will not disturb the connections. However, any signal threshold, connection description, or signal thresholds differences will be applied.
- Existing connections will be broken if one of the ports in the connection is specified in the topology to be connected to a different port.
- Port grouping rules are enforced. A connection in a topology will not be made if the connection violates port grouping rules.
- Connection locking and port privilege constraints are enforced on the user attempting to apply the topology.

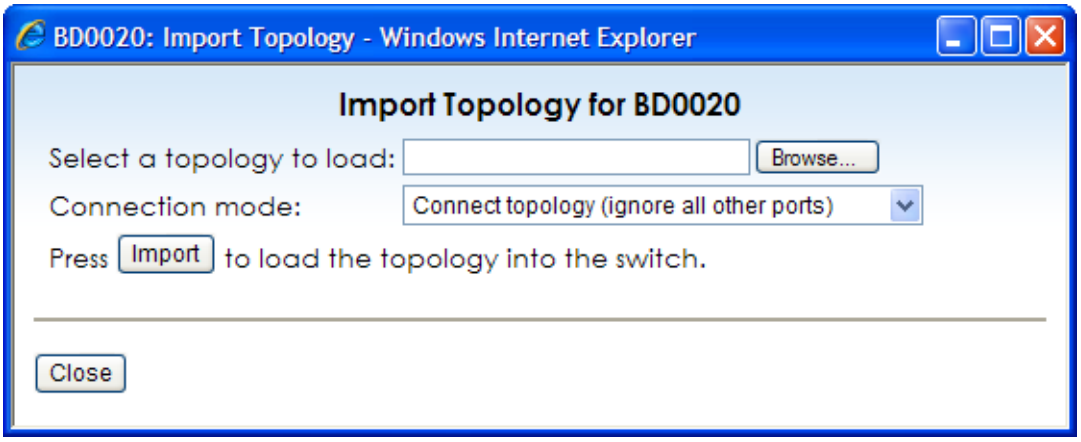
Import

The **Topology > Import** menu option opens the Import Topology window (Figure 43), from which topology files can be imported and the connection mode options can be configured.

- See ”Topology File Format Guidelines” on page 62 for information on how to create a topology text file for importing to the system.
- See ”Connection Mode Options” on page 68 for information on the different ways in which existing connections can be handled during the import process.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 43 Import Topology Window



Importing a Topology File

NOTES:
- When importing or quick loading a topology, the only connections that will be made are those which do not violate current port group rules and where the user has at least Modify privileges on both ports.
- When importing or quick loading a topology with the disconnect option, connections will be broken if the user importing the file has at least Modify privilege for one of the ports in the existing connection.

To import a topology from a text file:

1. Select the **Topology > Import** menu option from the Connection screen to view the Import Topology window (Figure 43).

2. From the Import Topology window, click the **Browse...** button to display the Choose File window.

3. Select a text topology file and click the **Open** button.
   The name and location of the selected file is displayed in the Import Topology window.

4. Select an option from the **Connection Mode** drop-down menu (see “Connection Mode Options” on page 68 for a description of the Connection Mode options).

5. Click **Import** to import the topology configuration.
   The topology is imported into the I/O Matrix and a results confirmation window is displayed, showing the file comments from the imported file.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

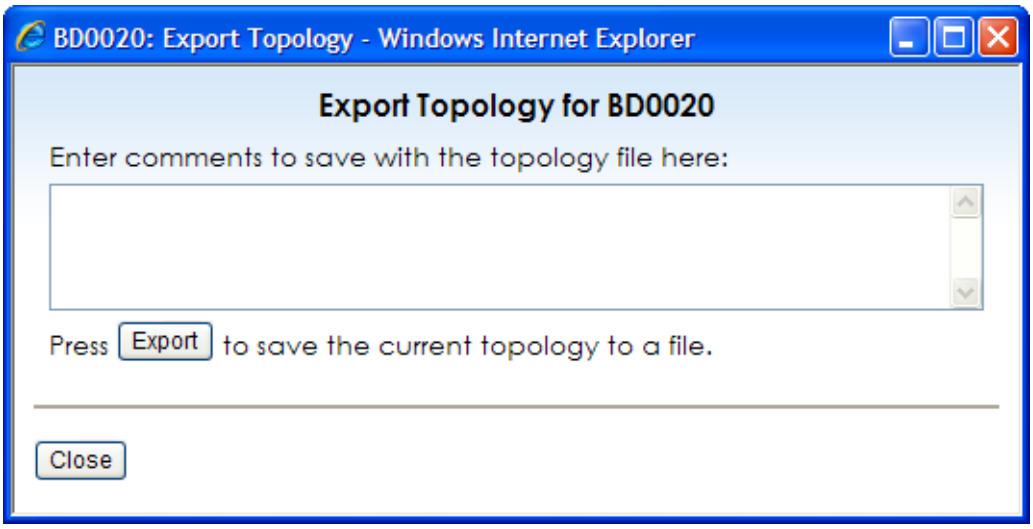
6. Click **OK** in the results confirmation window.

NOTE:	If the topology file to be imported contains syntax errors, duplicate port entries, or port names that have been deleted/revised, the import will fail (no change to connection matrix). If you are a user with port privilege restrictions check the Connection Matrix to ensure that all indicated actions have been performed.

Export

The **Topology > Export** menu option opens the Export Topology window (Figure 44), from which the current topology and any comments can be exported to a file. See ”Topology File Format Guidelines” on page 62 for information on the contents of the exported file.

Figure 44 Export Topology Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Exporting a Topology

NOTE:	**Port Privilege Impact:** When exporting the connection matrix, only connections for which the user has View or higher privileges on one of the ports in the connection will be included in the exported file.

To export a topology from the system to a text file:

1. Select **Topology > Export** from the Connection screen to view the Export Topology window (Figure 44 on page 70).

2. In the Export Topology window, enter comments to be saved with the topology file, such as a description of the configuration. These comments will be inserted in the heading at the beginning of the file. If the Comments section is left blank, the default heading is inserted at the beginning of the file.

3. Click **Export** to view the (web browser dependent) File Download window.

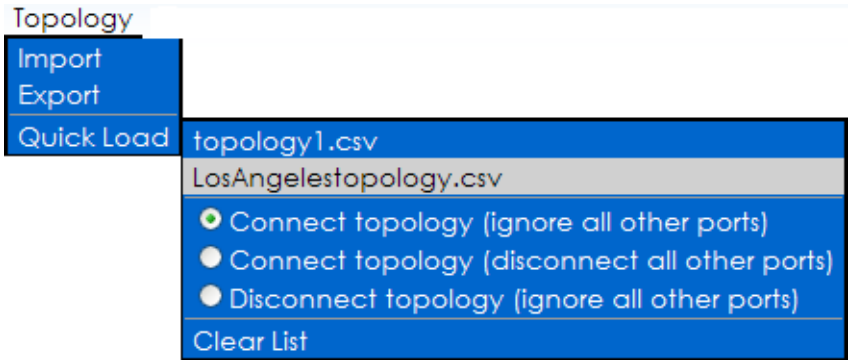
4. From the File Download window:
   - Click **Open** to view the exported topology file
   - Click **Save** to select a name and location to save the topology file

Quick Load

The ClickFlow GUI maintains a copy of the topology files that have been imported to the system. Each time a new file is imported into the system, the ClickFlow GUI automatically stores the topology into flash and adds the file name, user, and date to the top of the Quick Load list (shown in Figure 45). When a file is imported into the system or when a file is selected from the Quick Load list, the system moves the file to the top of the Quick Load list. The system stores a maximum of ten topology files and deletes files from the bottom of the Quick Load list to make room for newer topology files. The Quick Load list is preserved across reboots of the system

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 45 Topology File Quick Load Menu Options



Applying a Topology Using Quick Load

NOTES: **Port Privilege Impact:**

When importing or quick loading a topology file, the only connections formed are those for which the user has Modify or higher privilege for both ports in the connection.

When importing or quick loading with the disconnect option, connections where the user has Modify or higher privileges for one of the ports in the existing connection will be disconnected.

To apply a topology from the Quick Load list using the **Quick Load** menu option:

1. Select **Topology > Quick Load** from the Connection screen to view the Quick Load Menu (Figure 45 on page 72).

   NOTE: The Quick Load list will be empty until at least one topology file has been imported previously. To add a topology file to the Quick Load list, import the topology file as described in the section “Importing a Topology File” on page 69.

2. In the Quick Load menu, click on the desired **Connection Mode** option (see “Connection Mode Options” on page 68 for a description of these options).

3. In the Quick Load menu, click on the name of the topology file to be imported.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

4. Click **OK** in the confirmation dialog.

NOTE:	If the topology file to be imported contains port names that have been deleted/revised, the import will fail (no change to Connection Matrix). If you are a user with port privilege restrictions, check the Connection Matrix to ensure all indicated actions have been performed.

Clearing the Quick Load List

To clear the Quick Load topology file list:

1. Select **Topology > Quick Load** from the Connection screen to view the Quick Load Menu (Figure 45).

2. From the Quick Load list, select the **Clear List** menu option.

3. Click **OK** in the confirmation dialog.
   The Quick Load list will now display **<EMPTY>**.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

THIS PAGE INTENTIONALLY LEFT BLANK

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

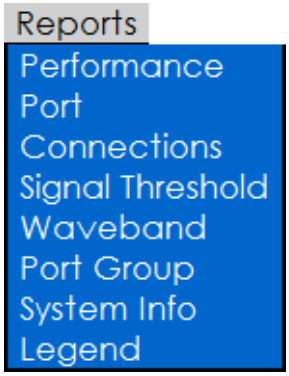
Reports

6

Overview

The **Reports** menu options shown in the figure below support real-time viewing of port powers as well as configuration information regarding ports, connections, and system features.

Figure 46 Reports Menu



The table below describes the **Reports** menu options and provides the page numbers where the menu options are further detailed in this chapter.

Menu Option	Description	Page
Performance	Displays a continuously updated performance report for all input ports and for connected output ports displayed to the user in the I/O Matrix. The user must have View or higher port privileges to see port/connection information for a port.	77
Port	Displays the configuration of all ports. The user must have View or higher port privileges to see port configuration information for a port.	80
Connections	Displays current data on all connections. The user must have View or higher port privileges to see port/connection information for a port.	83

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

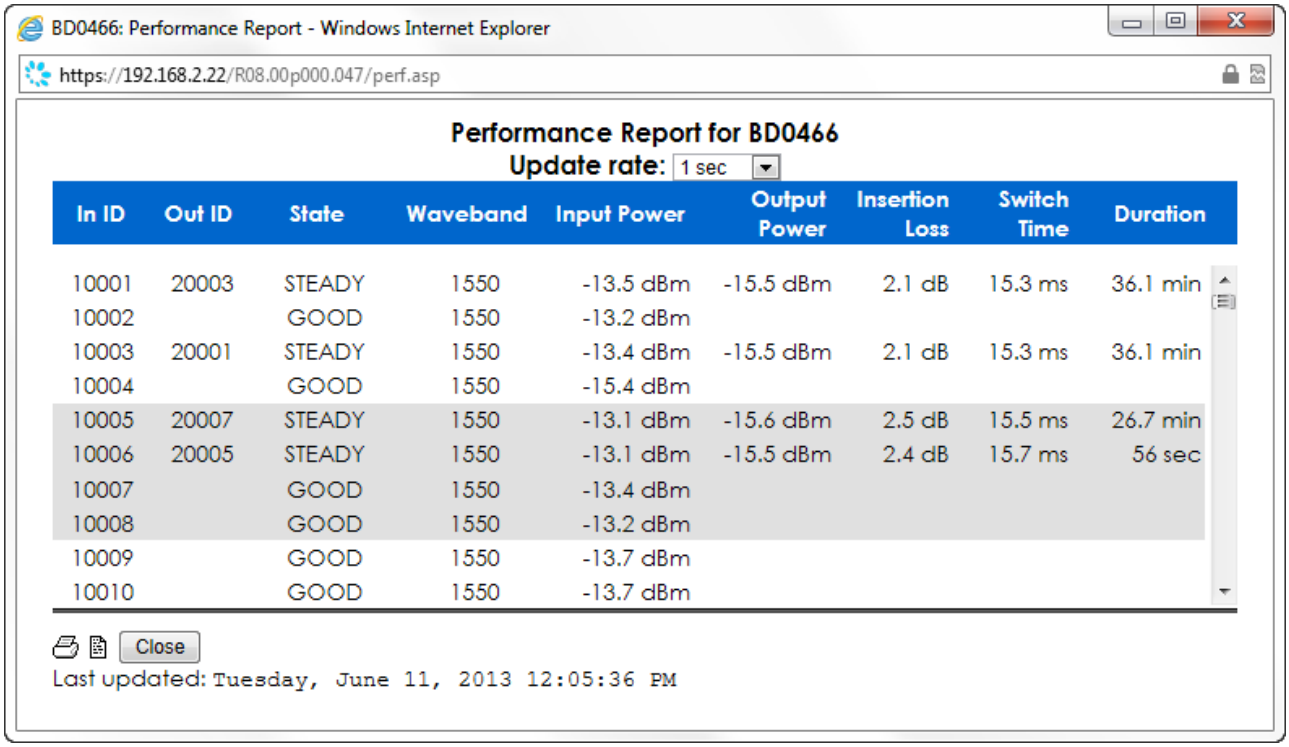
Menu Option	Description	Page
Signal Threshold	Displays the configuration for all signal thresholds and the ports assigned to each signal threshold. Only ports for which the user has View or higher privilege are shown in the assigned ports section.	88
Waveband	Displays the ports assigned to each waveband. Only ports that the user has View or higher privilege are shown in the assigned ports section.	90
Port Group	Displays the configuration for all port groups and the ports assigned to each port group. This menu option is displayed only to users with the system-level privilege of Manage on systems licensed for Port Grouping.	91
System Info	For administrative users, displays the hardware configuration, port information, license information and software information for the system.	93
Legend	Displays the State Color Code Legend window that details the colors used represent the optical power observed at a port as well as connection status. All users can view the legend.	96

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Performance

The **Reports > Performance** menu option displays a continuously updated status report of all activated ports in the I/O Matrix, as shown in Figure 47. The Performance Report window also displays PMU and VOA ports, if the system is equipped with them. The user must have View or higher port privileges to see port/connection information for a port.

Figure 47 Performance Report Window



In ID	Out ID	State	Waveband	Input Power	Output Power	Insertion Loss	Switch Time	Duration
10001	20003	STEADY	1550	-13.5 dBm	-15.5 dBm	2.1 dB	15.3 ms	36.1 min
10002		GOOD	1550	-13.2 dBm				
10003	20001	STEADY	1550	-13.4 dBm	-15.5 dBm	2.1 dB	15.3 ms	36.1 min
10004		GOOD	1550	-15.4 dBm				
10005	20007	STEADY	1550	-13.1 dBm	-15.6 dBm	2.5 dB	15.5 ms	26.7 min
10006	20005	STEADY	1550	-13.1 dBm	-15.5 dBm	2.4 dB	15.7 ms	56 sec
10007		GOOD	1550	-13.4 dBm				
10008		GOOD	1550	-13.2 dBm				
10009		GOOD	1550	-13.7 dBm				
10010		GOOD	1550	-13.7 dBm				

The Performance Report window contains the following elements:

Element	Description
In ID	The long port number or the alpha-numeric port ID for PMU/VOA ports of the input port.
Out ID	The long port number or the alpha-numeric port ID for PMU/VOA ports of the output port of the connection.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
State	The current state of the input port or the connection state if the input port is in a connection: • GOOD: Unconnected port is available for use • STEADY: Connection from port is optimized • PENDING: Connection from port is pending completion • FAULT: Connection from port is in a unknown fault condition • LOL INPUT: Port is in connection but no signal is present at the input. Must have input detection as a hardware option for this reading. • LOL OUTPUT: Port is in connection but no signal is present at the output.
Waveband	The waveband (signal band) assigned to the input port (see ”Waveband” on page 90).
Input Power	The optical power (in dBm) of the signal present on the input port. If the system is not configured with Input Detection, then the Input Power will be displayed as “N/A”.
Output Power	The optical power (in dBm) of the signal present on the output port of the connection.
Insertion Loss	The insertion loss (in dB) for the selected connection. If the system is not configured with Input Detection, then the Insertion Loss value will be displayed as “N/A”.
Switch Time	The time that it took to establish the connection.
Duration	The length of time that the selected connection has been established after the connection is made or restored after a power cycle. • This information is lost after a restart/reboot and “N/A” will be displayed • The duration will start counting from the initialization time if the system is power cycled.
Print Icon	Click the icon to display a printable version of the performance report in a new browser window. See ”Printing a Performance Report” on page 79.
File Icon	Click the icon to save the performance report to a file. See ”Saving the Performance Report to a File” on page 79.
Close Button	Click the **Close** button to close the window.
Last Updated	The date and time at which the information in the Performance Report window was last refreshed from the system.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Viewing a Performance Status Report

To view a performance report, select the **Reports > Performance** menu option from the Connection screen. The Performance Report window (Figure 47) is displayed and is updated continuously with real-time performance information.

NOTE:	The user must have View or higher port privileges to see port/connection information for a port.

Printing a Performance Report

To print a performance report:

1. Select the **Reports > Performance** menu option from the Connection screen to view the Performance Report window (Figure 47 on page 77).
2. Click the **Print** icon located at the bottom-center of the window. This will open a new browser window that contains a printer-friendly version of the Performance Report window.
3. From the browser window with the printer-friendly performance report, select **File > Print ...** from the web browser menu bar.
4. From the Print window, select a printer and click **Print**.

Saving the Performance Report to a File

To save a performance report to a file:

1. Select the **Reports > Performance** menu option from the Connection screen to view the Performance Report window (Figure 47 on page 77).
2. Click the **Save** button located at the bottom-center of the window. This will open the (web browser dependent) File Download window.
3. Click the **Save** button in the File Download dialog box.
4. Enter a file name and choose a destination in the Save As dialog box, then click **Save** to save the performance report as a file. The file will be saved as a text file (.csv format) and can be viewed with any third-party text editor (Notepad) or spreadsheet (Excel) application.

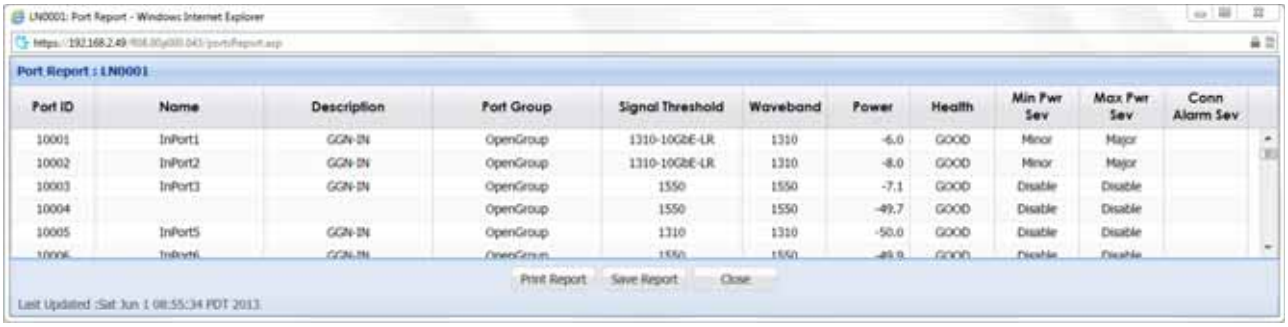
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Port

The **Reports > Port** menu option displays a snapshot report showing the configuration, health, and optical power of all licensed ports at the time that the report is requested. The user must have View or higher port privileges to see port configuration information for a port.

The default presentation sorts by port number, so that all input ports are shown first, followed by output ports. Figure 48 shows the first few input ports of a system. The report window can be resized and supports a vertical scroll bar so that all ports can be viewed. A horizontal scroll bar will appear if the window is resized to a smaller horizontal dimension.

Figure 48 Port Report Window (System with Port Grouping License)



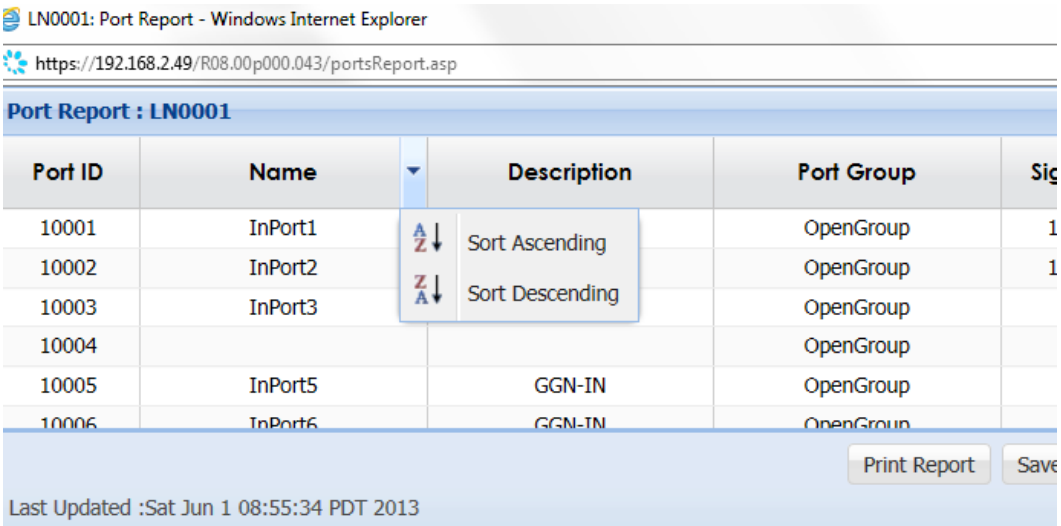
Port ID	Name	Description	Port Group	Signal Threshold	Waveband	Power	Health	Min Pwr Sev	Max Pwr Sev	Conn Alarm Sev
10001	InPort1	GGN-IN	OpenGroup	1310-10GbE-LR	1310	-6.0	GOOD	Minor	Major	
10002	InPort2	GGN-IN	OpenGroup	1310-10GbE-LR	1310	-8.0	GOOD	Minor	Major	
10003	InPort3	GGN-IN	OpenGroup	1550	1550	-7.1	GOOD	Disable	Disable	
10004			OpenGroup	1550	1550	-49.7	GOOD	Disable	Disable	
10005	InPort5	GGN-IN	OpenGroup	1310	1310	-50.0	GOOD	Disable	Disable	

NOTE:	The Port Group column is displayed only on systems with the Port Grouping license.

Each column heading supports selection of an ascending or descending sort as illustrated in Figure 49. This can be activated by simply clicking in the column header or selecting the pull-down which is activated by placing the mouse in the header cell.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 49 Port Report Window (Descending Sort on Port Group Column)



The report may also be printed or saved to an off-system file. Note that the Port Power column reflects the optical power at the time the report was requested and is not dynamically updated.

The Port Report window contains the following elements:

Field	Description
Port ID	The long port number for the port.
Name	The user assigned port name or the system default port name for PMU and VOA ports. For non-PMU/VOA ports, this field will be blank if no name has been entered for the port.
Description	The user assigned port description. This field will be blank if no description has been entered for the port.
Port Group	The name of the port group in which this port is assigned. Only shown on systems licensed with the Port Grouping feature.
Signal Threshold	The name of the signal threshold in use by this port.
Waveband	The waveband in use by this port.
Power	A snapshot of the optical power (dBm) measured at the port at the time the report was requested.
Health	The port state. If the port health is “GOOD”, the port may be used for connections.
Min Pwr Sev	The minimum power alarm severity (STMIN) configured for this port.
Max Pwr Sev	The maximum power alarm severity (STMAX) configured for this port.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
Conn Alarm Sev	The connection alarm severity (STMAX) configured for this output port. This field will be blank for all input ports.
Print Report Button	Click the **Print Report** button to display a printable version of the report in a new browser window. See “Printing a Port Report” on page 82.
Save Report Button	Click the **Save Report** button to save the report to a file. See “Saving the Port Report to a File” on page 83.
Close Button	Click the **Close** button to close the window.
Last Updated	The date and time at which the information in the Port Report window was last opened.

Viewing a Port Report

To view a port report, select the **Reports > Port** menu option from the Connection screen. The Port Report window (Figure 48 on page 80) is displayed.

NOTE: The user must have View or higher port privileges to see port configuration information for a port.

Printing a Port Report

To print a port report:

1. Select the **Reports > Port** menu option from the Connection screen to view the Port Report window (Figure 48 on page 80).
2. Click the **Print Report** button located at the bottom-center of the window. This will open a new browser window that contains a printer-friendly version of the Port Report window.
3. From the browser window with the printer-friendly port report, select **File > Print ...** from the web browser menu bar.
4. From the Print window, select a printer and click **Print**.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Saving the Port Report to a File

To save a performance report to a file:

1. Select the **Reports > Port** menu option from the Connection screen to view the Port Report window (Figure 48 on page 80).

2. Click the **Save** button located at the bottom-center of the window. This will open the (web browser dependent) File Download window.

3. Click the **Save** button in the File Download dialog box.

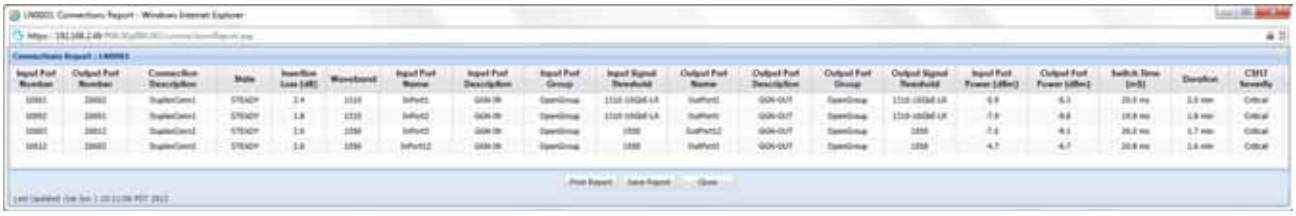
4. Enter a file name and choose a destination in the Save As dialog box, then click **Save** to save the port report as a file. The file will be saved as a text file (.csv format) and can be viewed with any third-party text editor (Notepad) or spreadsheet (Excel) application.

Connections

The **Reports > Connections** menu option displays a snapshot report showing all existing connections in the system. The report contains all relevant connection information as well as relevant configuration information regarding the ports in the connection. The user must have View or higher port privileges to see port/connection information for a port

The default presentation sorts by input port number. Figure 50 shows the first four connected ports in a system. The report window may be resized and supports a vertical scroll bar so that all connections can be viewed. A horizontal scroll bar will appear if the window is resized to a smaller horizontal dimension. (See Figure 51 on page 84 for larger images of these column headers.)

Figure 50 Connection Report Window (System with Port Grouping License)

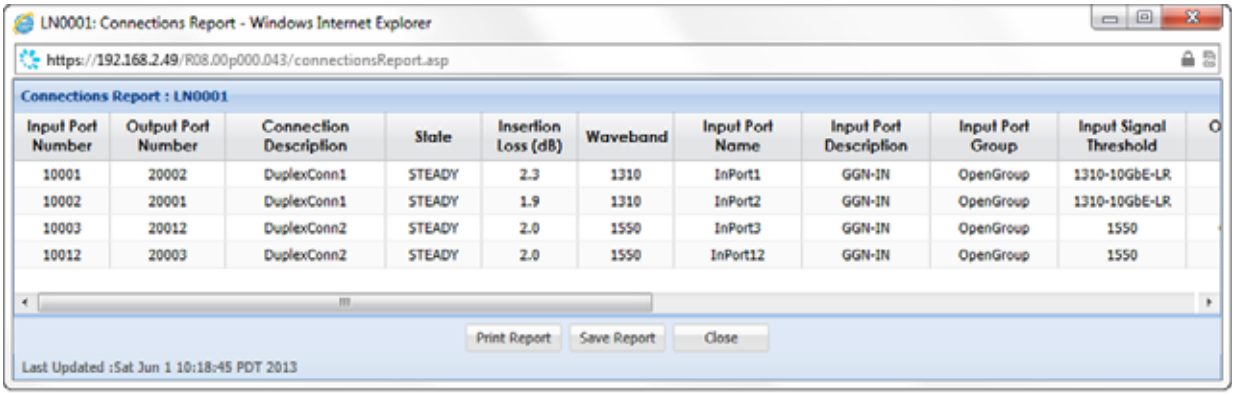


NOTE:	The Port Group column is displayed only on systems with the Port Grouping license.

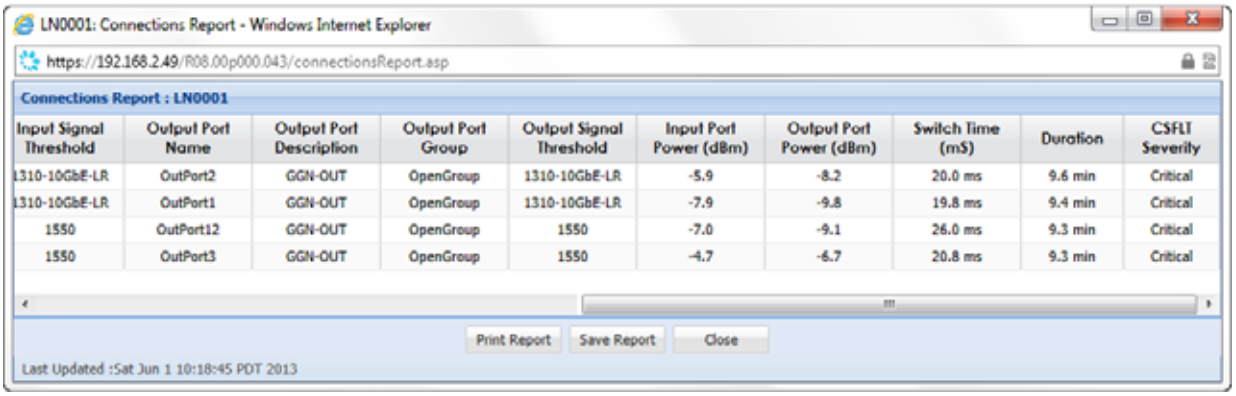
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 51 shows use of the scroll bar in the Connection Report window (both right and left halves of the window are displayed).

Figure 51 Using the Scroll Bar in the Connection Report Window



Input Port Number	Output Port Number	Connection Description	State	Insertion Loss (dB)	Waveband	Input Port Name	Input Port Description	Input Port Group	Input Signal Threshold
10001	20002	DuplexConn1	STEADY	2.3	1310	InPort1	GGN-IN	OpenGroup	1310-10GbE-LR
10002	20001	DuplexConn1	STEADY	1.9	1310	InPort2	GGN-IN	OpenGroup	1310-10GbE-LR
10003	20012	DuplexConn2	STEADY	2.0	1550	InPort3	GGN-IN	OpenGroup	1550
10012	20003	DuplexConn2	STEADY	2.0	1550	InPort12	GGN-IN	OpenGroup	1550



Input Signal Threshold	Output Port Name	Output Port Description	Output Port Group	Output Signal Threshold	Input Port Power (dBm)	Output Port Power (dBm)	Switch Time (mS)	Duration	CSFLT Severity
1310-10GbE-LR	OutPort2	GGN-OUT	OpenGroup	1310-10GbE-LR	-5.9	-8.2	20.0 ms	9.6 min	Critical
1310-10GbE-LR	OutPort1	GGN-OUT	OpenGroup	1310-10GbE-LR	-7.9	-9.8	19.8 ms	9.4 min	Critical
1550	OutPort12	GGN-OUT	OpenGroup	1550	-7.0	-9.1	26.0 ms	9.3 min	Critical
1550	OutPort3	GGN-OUT	OpenGroup	1550	-4.7	-6.7	20.8 ms	9.3 min	Critical

As with the Port Report, the Connections Report supports ascending/descending sorting by selecting a column header. The Connections Report fields displayed for each connection are described in the table below.

Field	Description
Input Port Number	The long port number for the input port (e.g., 10xxx).
Output Port Number	The long port number for the output port (e.g., 20xxx).
Connection Description	The connection description. This field will be blank if no description has been entered for this connection.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
State	The state condition for the connection: • STEADY = Good (Optimized Connection) • PENDING = Connection request incomplete • FAULT = Failed connection • LOL INPUT = Connection without input power (dark connection or LOL). This condition only applies for systems with input detection hardware. • LOL OUTPUT = Connection without output power. Dark connection or LOL on systems without input detection hardware.
Insertion Loss (dB)	The insertion loss of this connection in dB. Requires a valid connection and Input Detection, otherwise the value is “N/A.”
Waveband	The waveband used for this connection (derived from input port configuration).
Input Port Name	The port name of the input port. This field will be blank if no name has been entered for this port.
Input Port Description	The port description for the input port. This field will be blank if no description has been entered for the port.
Input Port Group	The name of the port group in which the input port is assigned. Only shown on systems licensed with the Port Grouping feature.
Input Signal Threshold	The name of the signal threshold in use for the input port.
Output Port Name	The port name of the output port. This field will be blank if no name has been entered for this port.
Output Port Description	The port description for the output port. This field will be blank if no description has been entered for the port.
Output Port Group	The name of the port group in which the output port is assigned. Only shown on systems licensed with the Port Grouping feature.
Output Signal Threshold	The name of the signal threshold in use for the output port.
Input Port Power	The optical power (dBm) measured at the input port.
Output Port Power	The optical power (dBm) measured at the output port.
Switch Time (ms)	The elapsed time to make the connection in milliseconds.
Duration	The length of time that the selected connection has been established after the connection is made or restored after a power cycle. This information is lost after a restart/reboot and N/A will be displayed The duration will start counting from the initialization time if the system is power cycled.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
CSFLT Severity	The connection alarm severity (CSLFT) configured for the output port in this connection.
Print Report Button	Click the **Print Report** button to display a printable version of the connection report in a new browser window. See “Printing a Connection Report” on page 86.
Save Report Button	Click the **Save Report** button to save the connection report to a file. See “Saving the Connection Report to a File” on page 87.
Close Button	Click the **Close** button to close the window.
Last Updated	The date/time the window was opened. The data displayed is the configuration and power values as of the indicated time.

Viewing a Connection Report

To view a port report, select the **Reports > Connections** menu option from the Connection screen. The Connection Report window (Figure 50 on page 83) is displayed.

NOTE: The user must have View or higher port privileges to see port/connection information for a port.

Printing a Connection Report

To print a connection report:

1. Select the **Reports > Connections** menu option from the Connection screen to view the Connection Report window (Figure 50 on page 83).

2. Click the **Print Report** button located at the bottom-center of the window. This will open a new browser window that contains a printer-friendly version of the Port Report window.

3. From the browser window with the printer-friendly port report, select **File > Print ...** from the web browser menu bar.

4. From the Print window, select a printer and click **Print**.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Saving the Connection Report to a File

To save a connection report to a file:

1. Select the **Reports > Connections** menu option from the Connection screen to view the Connection Report window (Figure 50 on page 83).

2. Click the **Save** button located at the bottom-center of the window. This will open the (web browser dependent) File Download window.

3. Click the **Save** button in the File Download dialog box.

4. Enter a file name and choose a destination in the Save As dialog box, then click **Save** to save the connection report as a file. The file will be saved as a text file (.csv format) and can be viewed with any third-party text editor (Notepad) or spreadsheet (Excel) application.

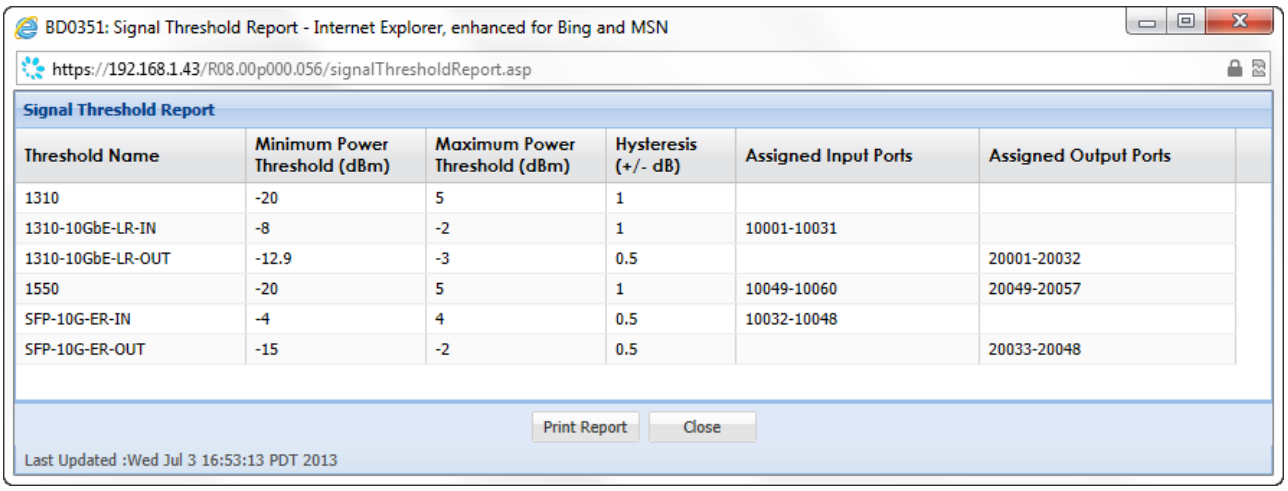
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Signal Threshold

The **Reports > Signal Threshold** menu option all the configuration of and ports assigned to each signal threshold in the system. The data presented is a snapshot of the configuration and assignments as of when the report window was opened. The user must have View or higher port privileges to see signal threshold information for a port.

The signal threshold information is presented in a table as shown in Figure 52. The table contents are defined below the figure. By default, the table is sorted alphabetically by signal threshold name. Each column supports and ascending/descending sort.

Figure 52 Signal Threshold Report Window



Threshold Name	Minimum Power Threshold (dBm)	Maximum Power Threshold (dBm)	Hysteresis (+/- dB)	Assigned Input Ports	Assigned Output Ports
1310	-20	5	1		
1310-10GbE-LR-IN	-8	-2	1	10001-10031	
1310-10GbE-LR-OUT	-12.9	-3	0.5		20001-20032
1550	-20	5	1	10049-10060	20049-20057
SFP-10G-ER-IN	-4	4	0.5	10032-10048	
SFP-10G-ER-OUT	-15	-2	0.5		20033-20048

The Signal Threshold Report window contains the following elements:

Element	Description
Threshold Name	The signal threshold name. Signal thresholds are assigned to ports by name.
Minimum Power Threshold (dBm)	The minimum optical power threshold for ports assigned this signal threshold. This power threshold value is used with the ± Hysteresis value to determine when STMIN alarms are reported/cleared for the port.
Maximum Power Threshold (dBm)	The maximum optical power threshold for ports assigned this signal threshold. This power threshold value is used with the ± Hysteresis value to determine when STMAX alarms are reported/cleared for the port.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Hysteresis (± dB)	The hysteresis value used to prevent alarm flooding. The optical power must cross above/below the power threshold value ± the hysteresis value for the alarm to set or clear. The alarm direction depends on the power threshold. • For STMIN alarms, the alarm occurs when the power falls below the threshold – hysteresis value. • For STMAX, the alarm occurs when the power rises above the threshold + hysteresis value.
Assigned Input Ports	The input ports assigned to this signal threshold. The ports are displayed as specified below: • For a range, the starting and ending numbers are displayed with a hyphen between the numbers. For example: 10001-10024 • Individual numbers are separated from each other or a range by white space. For example: 10001-10024 10100 10120 10130-10140
Assigned Output Ports	The output ports assigned to this signal threshold. The ports are displayed as specified below: • For a range, the starting and ending numbers are displayed with a hyphen between the numbers. For example: 20001-20024 • Individual numbers are separated from each other or a range by white space. For example: 20001-20024 20100 20120 20130-20140
Print Report Button	Click the **Print Report** button to display a printable version of the report in a new browser window.
Close Button	Click the **Close** button to close the window.
Last Updated	The date/time at which the window was opened. The data displayed is the configuration and port assignments as of the indicated time.

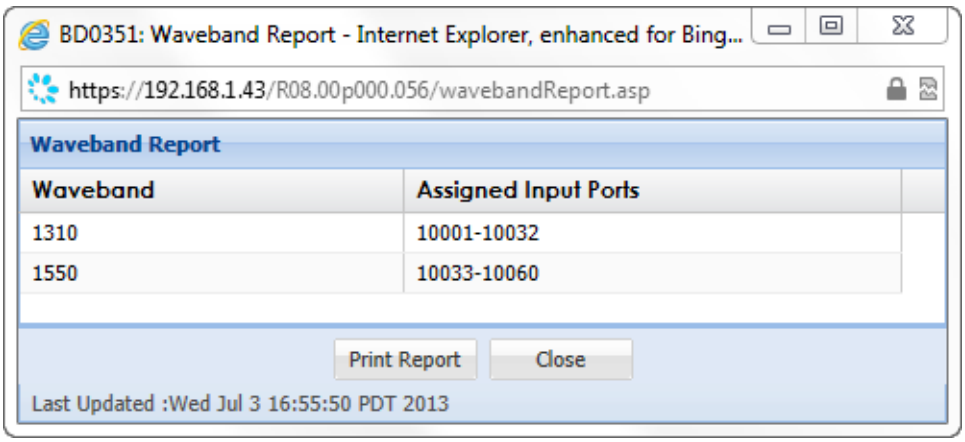
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Waveband

The **Reports > Waveband** menu option all the configuration of and ports assigned to each waveband in the system. The data presented is a snapshot of the configuration and assignments as of when the report window was opened. The user must have View or higher port privileges to see waveband information for a port.

The waveband information is presented in a table as shown in Figure 52. The table contents are defined below the figure. By default, the table is sorted alphabetically by waveband name. Each column supports and ascending/descending sort.

Figure 53 Waveband Report Window



The Waveband Report window contains the following elements:

Element	Description
Waveband	Two wavebands, 1310 a 1550, are provided for input port assignment. The waveband designation indicates the waveband carried on the input fiber per the following rules: • Input ports are assigned to the 1310 waveband when the signal at the input port is in the O or E Bands (1260nm -1460nm) • Input ports are assigned to the 1550 waveband when the signal at the input port is in the S, C or L Bands (1460nm -1630nm)
Assigned Input Ports	The input ports assigned to this signal threshold. The ports are displayed as specified below: • For a range, the starting and ending numbers are displayed with a hyphen between the numbers. For example: 10001-10024 • Individual numbers are separated from each other or a range by white space. For example: 10001-10024 10100 10120 10130-10140

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

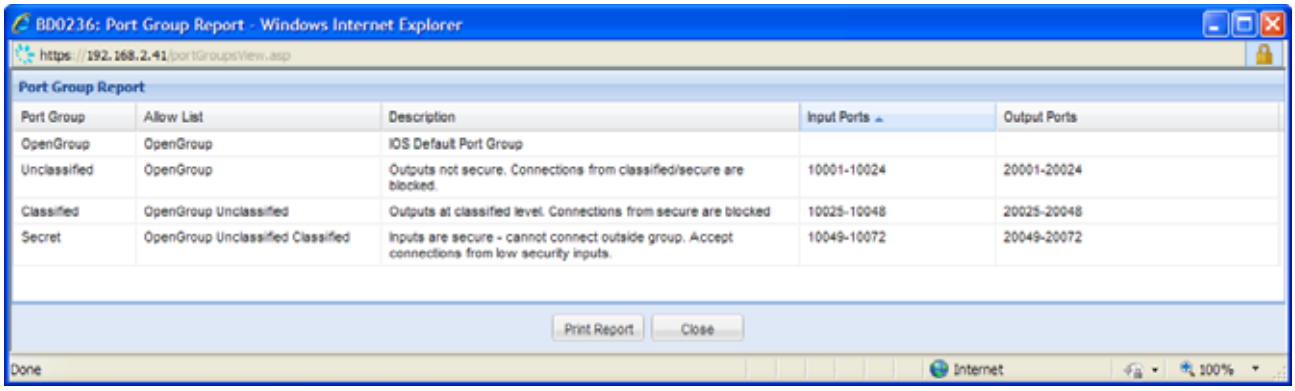
Element	Description
Print Report Button	Click the **Print Report** button to display a printable version of the Waveband report in a new browser window.
Close Button	Click the **Close** button to close the window.
Last Updated	The date/time at which the window was opened. The data displayed is the configuration and port assignments as of the indicated time.

Port Group

The **Report > Port Group** menu option displays both port group configuration and port-to-group assignments. The data presented is a snapshot as of when the report window was opened. This menu option is displayed only to users with the system-level privilege of Manage.

The port group information is presented in a table as shown in Figure 54. The table contents are defined below the figure. By default, the table is sorted alphabetically by group name. Each column supports an ascending/descending sort. In Figure 54, the table is sorted by input ports as indicated by the highlighted column header with the up arrow indicating an ascending sort.

Figure 54 Port Group Report Window



Field	Description
Port Group	The name of the port group.
Allow List	The port groups allowed to connect to the outputs assigned in this port group.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
Description	A text field supporting entry of a description or comments regarding this port group. This field supports 96 characters.
Input Ports	The input ports assigned to this group are presented per the following rules: • For a range, the starting and ending numbers are displayed with a hyphen between the numbers. For example: 10001-10024 • Individual numbers are separated from each other or a range by white space. For example: 10001-10024 10100 10120 10130-10140
Output Ports	The outputs ports assigned to this group are presented per the following rules: • For a range, the starting and ending numbers are displayed with a hyphen between the numbers. For example: 20001-20024 • Individual numbers are separated from each other or a range by white space. For example: 20001-20024 20080 20083
Print Report Button	Click the **Print Report** button to display a printable version of the port group report in a new browser window. See “Printing a Port Group Report” on page 93.
Close Button	Click the **Close** button to close the window.

From Figure 54, this system has three port groups configured: Unclassified, Classified, and Secret. There are no ports assigned to OpenGroup.

This configuration indicates the following usage:

- Only unclassified input signals may be connected to unclassified output ports.
- Classified inputs may be connected to classified or secret output ports. Unclassified input signals may be connected to classified output ports.
- Inputs carrying 'secret' data may only be connected to secret output ports. Unclassified or Classified input ports may be connected to secret output ports.

The above utilization ensures no input signal can be connected to a security classification which is less secure than the signal itself. It does permit simplex connections from low security inputs to higher security outputs. In this configuration, full duplex connections are only allowed within a security classification. OpenGroup is empty and will not be displayed on the Connection screen.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Viewing a Port Group Report

To view a port group report, select the **Reports > Port Group** option from the Connection screen main menu. The Port Group Report window (Figure 54 on page 91) is displayed.

NOTE:	The **Port Group** menu option and the ability to view port group configuration for the entire system is provided only to users with the system-level privilege of Manage.

Printing a Port Group Report

To print the Port Group report:

1. Open the Port Group Report window by selecting **Reports > Port Group** from the Connection screen menu.
2. Click the **Print Report** button located at the bottom center of the window. This will open a new browser window that contains a printer-friendly version of the Port Group Report window.
3. From the browser window displaying the printer-friendly report, select **File > Print…** from the web browser menu bar.
4. From the Print window, select a printer and click **Print**.
5. Close the browser window displaying the report.
6. Click the **Close** button in the Port Group Report window.

System Info

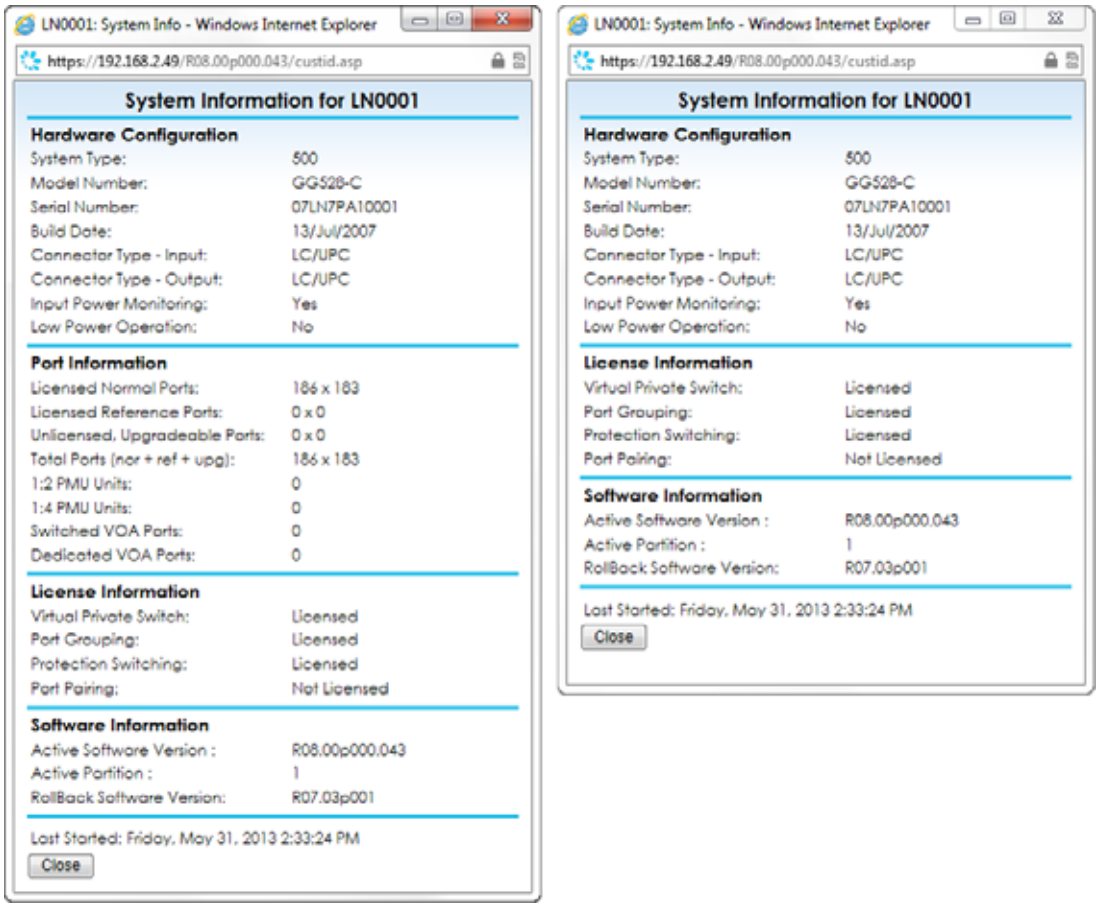
The **Reports > System Info** menu option presents the System Information window shown in Figure 55. The System Information window details system specific hardware and software feature configuration as well as software release information and system initialization information.

The window shown on the left in Figure 55 is presented to users with View system privilege and full port privileges. The window shown on the right is presented to users with View system privilege and partial port privileges.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE: Please be prepared to provide the Serial Number and Active Software Version when contacting Glimmerglass Customer Support.

Figure 55 System Information Window



The System Information window contains the following elements. Note that the “Last Started” date is always presented as the switch time, which is set to UTC.

Field	Description
Hardware Configuration	
System Type	System type: 100, 300, 500, 600, unknown. This field will contain “unknown” for older systems (prior to implementation). See the *Glimmerglass System Installation and Maintenance Guide* for a description of the system types/models. This information, as well as the model number and serial number, also appears on the serial number label on the system.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
Model Number	System chassis type identification.
Serial Number	Serial number of the system.
Build Date	Build date for the system.
Connector Type - Input	The connector type used on the patch panel for the input ports: Unknown, LC/UPC, LC/APC, SC/UPC, SC/APC, FC/UPC, FC/APC, ST/UPC, E2000/APC, F3000/UPC, MTP-12F, MTP-12M, MTP-8F, MTP-8M This field will contain “unknown” for older systems (prior to implementation).
Connector Type -Output	The connector type used on the patch panel for the output ports: Unknown, LC/UPC, LC/APC, SC/UPC, SC/APC, FC/UPC, FC/APC, ST/UPC, E2000/APC, F3000/UPC, MTP-12F, MTP-12M, MTP-8F, MTP-8M This field will contain “unknown” for older systems (prior to implementation).
Input Power Monitoring	Yes = Input Detection hardware is installed No = No Input Detection hardware is installed
Low Power Option	Yes = System’s acceptable input power range is extended (-35dBm to 15dBm) No = Standard power range (-25dBm to 20dBm)
Port Information	
Licensed Normal Ports	The switch matrix ports (input x output) enabled at the patch panel.
Licensed Reference Ports	The switch matrix ports used internally to support PMUs and Switched VOA
Unlicensed, Upgradable Ports	The switch matrix ports which exist at the patch panel but are not licensed. (These ports may be activated by purchasing a port upgrade.)
Total Ports (nor + ref + upg)	The total number of ports available on the system: the sum licensed normal/reference and unlicensed upgradeable ports.
1:2 PMU Units	The count of 1:2 PMU units in the system
1:4 PMU Units	The count of 1:4 PMU units in the system
Switched VOA Ports	The number of Switched VOA port pairs in the system.
Dedicated VOA Ports	The number of Dedicated VOA port pairs in the system.
License Information	
Virtual Private Switch	“Licensed” if the feature is purchased, otherwise “Not Licensed.”

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
Port Grouping	“Licensed” if the feature is purchased, otherwise “Not Licensed.”
Protection Switching	“Licensed” if the feature is purchased, otherwise “Not Licensed.”
Port Pairing	“Licensed” if the feature is purchased, otherwise “Not Licensed.”
Software Information	
Active Software Version	The active software release
Active Partition	The partition (0 or 1) in which the active release resides.
Rollback Software Version	The previous software version.
Last Started	Date and time the system was last started (UTC). This value changes upon power cycle, reboot, or restart of the system.

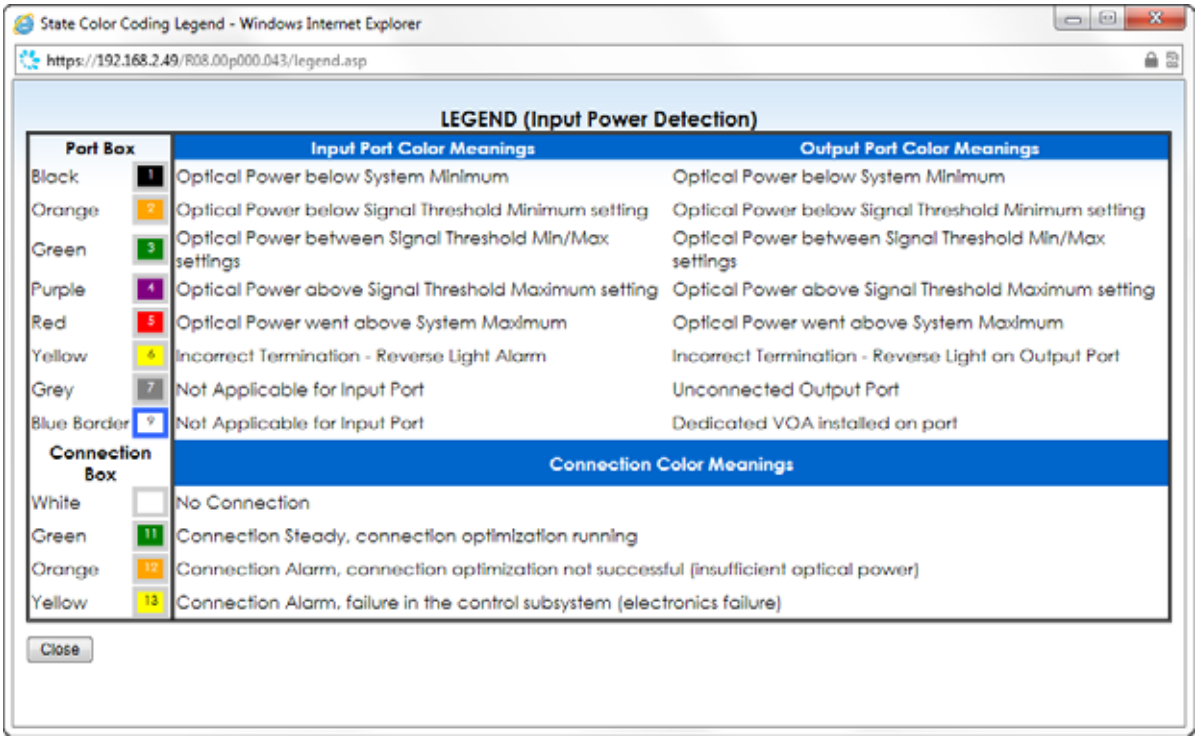
Legend

The **Reports > Legend** menu option displays the State Color Coding Legend window that details the meanings for the colors used in the Port and Connection Boxes in the Connection screen.

Figure 56 shows the Color Coding Legend window that describes the meaning of each color for systems that include the Input Power Detection feature, while Figure 57 shows that for systems that do not include the Input Power Detection feature. The legend appropriate for the installed features is accessed through the ClickFlow GUI by selecting the **Reports > Legend** menu option from the Connection screen.

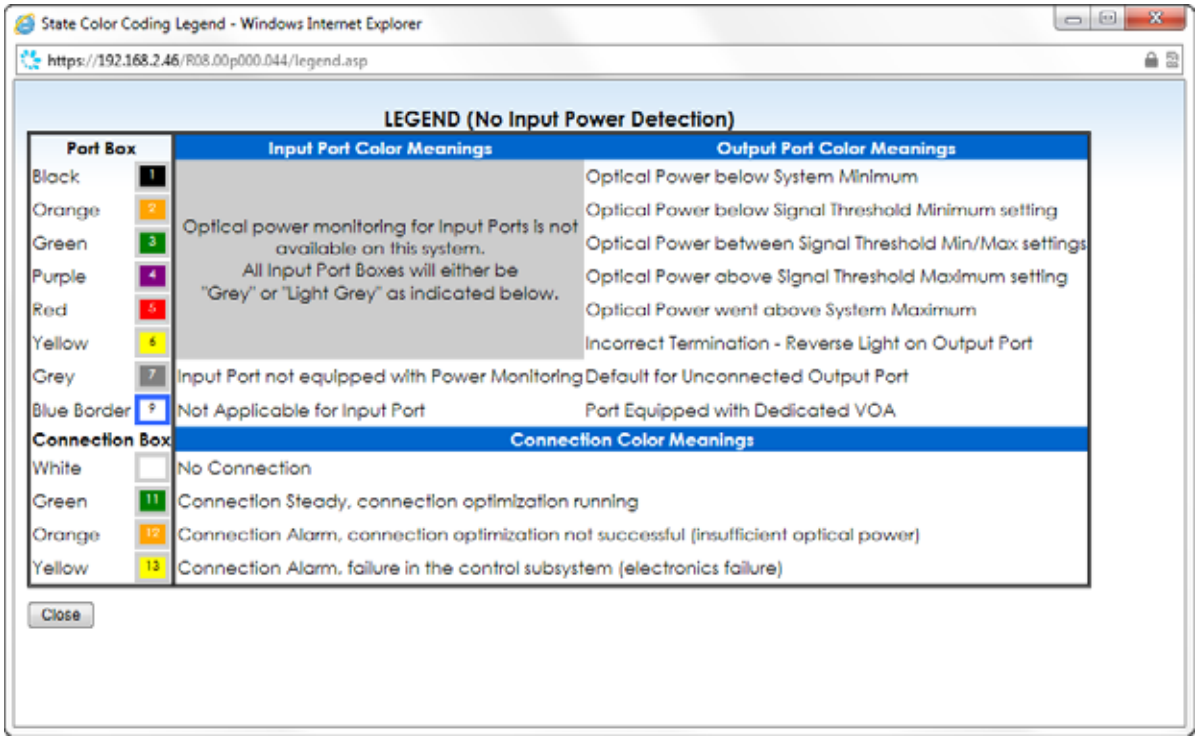
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 56 State Color Coding Legend (with Input Power Detection)



Port Box		Input Port Color Meanings	Output Port Color Meanings
Black	1	Optical Power below System Minimum	Optical Power below System Minimum
Orange	2	Optical Power below Signal Threshold Minimum setting	Optical Power below Signal Threshold Minimum setting
Green	3	Optical Power between Signal Threshold Min/Max settings	Optical Power between Signal Threshold Min/Max settings
Purple	4	Optical Power above Signal Threshold Maximum setting	Optical Power above Signal Threshold Maximum setting
Red	5	Optical Power went above System Maximum	Optical Power went above System Maximum
Yellow	6	Incorrect Termination - Reverse Light Alarm	Incorrect Termination - Reverse Light on Output Port
Grey	7	Not Applicable for Input Port	Unconnected Output Port
Blue Border	9	Not Applicable for Input Port	Dedicated VOA installed on port
Connection Box		**Connection Color Meanings**	
White		No Connection	
Green	11	Connection Steady, connection optimization running	
Orange	12	Connection Alarm, connection optimization not successful (insufficient optical power)	
Yellow	13	Connection Alarm, failure in the control subsystem (electronics failure)	

Figure 57 State Color Coding Legend (without Input Power Detection)



NOTES: Note the following information about standard systems with reference to the preceding legends:

- The system minimum optical power is -40dBm (black)
- The system maximum optical power is 20dBm (for standard systems) (red)
- The Signal Threshold minimum optical power is specified in a Signal Threshold record. The value in this record is used by ports that are assigned to that record (by Signal Threshold name). (orange)
- The Signal Threshold maximum optical power is specified in a Signal Threshold record. The value in this record is used by ports that are assigned to that record (by Signal Threshold name). (purple)
- All output ports are configured with power detection hardware.
- Reverse light (light coming into the system on the output fiber) is invalid and an alarm condition for standard (non-bidirectional) systems. (yellow)
- Input Detection is optical power detection at input ports and is hardware-enabled feature (see “System Info” on page 930.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Configure

7

Overview

The **Configure** menu options allow configuration for all port and connection attributes:

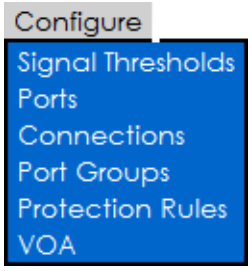
- For ports, the configurable attributes include names, descriptions, port group assignment, alarm severity, waveband, and signal threshold assignment as well as creation of protection rules and changing VOA settings.
- For connections, the sole configurable attribute is the connection description. The connection fault severity is configured as an output port attribute.

Signal Thresholds are configured via the **Configure** menu as well. These signal thresholds are then assigned to ports under the **Ports** sub-menu.

System configuration items (e.g., system name, IP information, security policies) are covered in Chapter 9.

The configuration menu options relating to ports and connections are shown in the figures below.

Figure 58 Configure Menu



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 59 Configure Menu (Ports Sub-menu

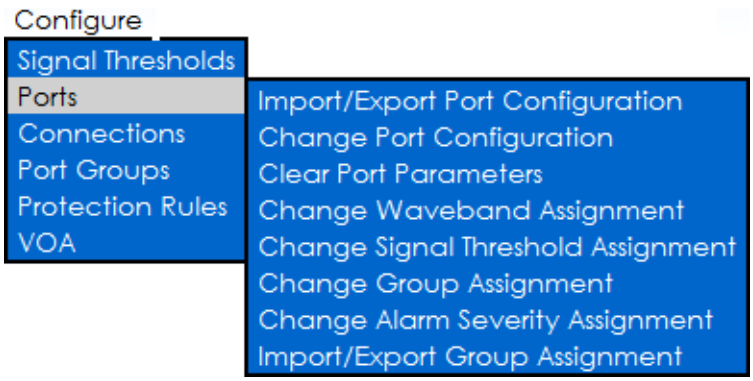
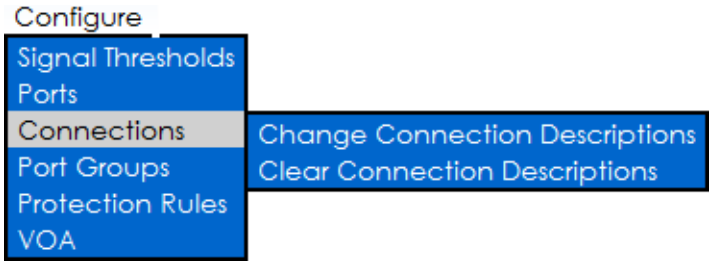


Figure 60 Configure Menu (Connections Sub-menu)



NOTES: The following **Configure** menu items are not displayed if the associated feature is not enabled:

- **Port Groups** (Port Grouping license)
- **Protection Rules** (Protection Switching license)
- **VOA** (VOA hardware present)
- **Ports > Import/Export Group Assignment** (Port Grouping license)

The following **Configure** menu items are not displayed if the user does not have full management privileges for system.

- **Port Groups** (Port Grouping license)
- **Ports > Import/Export Group Assignment** (Port Grouping license)
- **Ports > Import/Export Group Assignment** (Port Grouping license)

Full management privilege is defined as:

- System privilege = Manage
- Port privilege = Manage for all ports in the system

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The table below describes the **Configure** menu options and provides the page numbers where the menu options are further detailed in this chapter.

NOTES: Port Configuration Privileges:
Modify port-level privileges are required when configuring ports (entering names, descriptions, or assigning wavebands, signal thresholds and severities). Assigning ports among port groups requires Manage privileges for all ports. Below are some exceptional cases:

- Clearing ALL port names/descriptions: This activity is restricted. The only names/descriptions that will be cleared are the ports where the user has Manage privileges. All other ports will be unaffected.
- Exporting port names/descriptions: The export file will only contain the ports which the user can see in the I/O Matrix (view or higher privilege)
- Importing port names/descriptions: Regardless of the ports included in the file, the import will only apply to ports where the user has Modify or higher port privileges.

Connection Configuration Privileges:

Modify port-level privileges are required on both ports when modifying the connection description.

- Clearing ALL connection descriptions: This activity is restricted. The only descriptions that will be cleared those where the user has Manage privileges both ports in the connection. All other connections will be unaffected.

Menu Option	Description	Page
Signal Thresholds	Opens the Signal Threshold Configuration window allowing creation, modification or deletion of signal threshold records. Only users with the system privilege of Modify or higher may perform these operations.	103

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description	Page
Ports	Presents a sub-menu containing the following options: • Import/Export Port Configuration—Allows exporting and importing of port names and descriptions for some or all ports. • Change Port Configuration—Opens a window with a table showing all ports and supports editing of port names, descriptions, port group membership, and signal threshold assignment. • Clear Port Parameters—Opens sub-menu with options to clear all port names and/or port descriptions. • Change Waveband Assignment—Allows ranges of input ports to be assigned to a waveband. • Change Signal Threshold Assignment—Allows ranges of ports to be assigned to a signal threshold. • Change Group Assignment—Allows ranges of ports to be assigned to a selected port group. • Change Alarm Severity Assignment—Allows ranges of ports to be assigned a specific severity for each configurable optical alarm type. • Import/Export Group Assignment—Allows exporting and importing of port to port group assignments. The **Change Port Group** and **Import/Export Group Assignment** options are displayed only when the Port Grouping license is enabled and the user has the privileges required to make port-to-port group assignments.	111
Connections	Presents a sub-menu containing the following options. • Change Connection Description—Opens window with table showing all connections and supports editing of the descriptions. • Clear Connection Descriptions—Opens sub-menu with options to clear all connections names	143
Port Groups	Opens the Port Group Configuration window, which allows a system administrator to create/modify/delete port group records.	146
Protection Rules	Opens the Protection Rules window, which allows users with Manage port privileges to add, delete, or import protection rules. This menu option is displayed only when Protection Switching is licensed on the system.	151

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description	Page
Variable Optical Attenuation (VOA)	Opens the VOA Settings window, from which the Variable Optical Attenuation feature can be enabled for ports and specific output power values can be set. This operation requires the Modify port privilege for the VOA ports. This option is displayed only when VOA hardware is detected in the system.	164

Signal Thresholds

The values specified in a signal threshold record determine when alarms for optical power changes are presented and cleared for a port assigned the signal threshold. In addition, the colors shown in the Port Box on the connection screen are updated based upon the minimum and maximum optical power settings configured in the signal threshold record.

A Signal Threshold is a record composed of the following information:

- The name of the signal threshold
- A minimum optical power level setting (represents a dBm value)
- A maximum optical power level setting (represents a dBm value)
- A hysteresis value (represents a ± dB value centered both the power level settings)

The minimum optical power setting and hysteresis operate as follows:

- The Port Box color for the port will be orange if the measured optical power is below the minimum optical power setting and above the system's minimum power value of -40dBm
- An STMIN (signal threshold minimum) alarm will be issued when:
  - The measured optical power at the port has been above the minimum power threshold
    and
  - The measured power at the port then drops below:
    (Min. Pwr. Threshold) - (Hysteresis)
- An STMIN alarm clear will be issued when:
  - An active STMIN alarm condition exists
    and
  - The measured optical power at the port rises above:
    (Max. Pwr. Threshold) + (Hysteresis)

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The maximum optical power setting and hysteresis operate as follows:

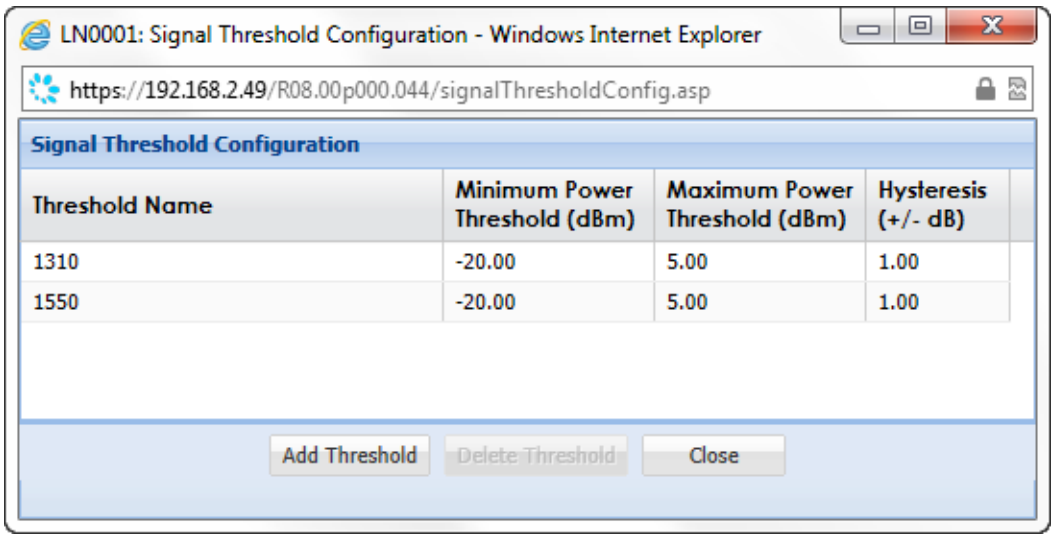
- The Port Box color for the port will be purple if the measured optical power is above the maximum optical power setting and below the system's maximum power value of 20dBm
- An STMAX (Signal Threshold Maximum) alarm will be issued when:
  - The measured optical power at the port has been below the maximum power threshold
    and
  - The measured optical power at the port rises above:
    (Max. Pwr. Threshold) + (Hysteresis)
- An STMAX alarm clear will be issued when:
  - The measured optical power at the port has been above the maximum power threshold
    and
  - The measured optical power at the port drops below:
    (Max. Pwr. Threshold) - (Hysteresis)

Once a signal threshold is created, it may be assigned to any port or to range of ports. There is no requirement that the same signal threshold be used on an input and output port in a connection. In fact, it may be desirable to use different thresholds.

There are two default signal thresholds in the system, name “1310” and “1550”. Both default to a minimum power level of -20dBm, a maximum power level of 5dBm with a hysteresis value of ±1dB.

The **Configure > Signal Thresholds** option opens the Signal Threshold Configuration window.

Figure 61 Signal Threshold Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The Signal Threshold Configuration window presents a table with four columns: one column for each signal threshold parameter value. Descriptions for the parameters are provided in the table below. Add, delete, and modify operations are described in the following sections.

NOTE: To edit the values for an existing signal threshold, double-click on the row for the signal threshold. See Figure 63 on page 108 in ”Modifying a Signal Threshold” on page 107 for the an example showing this operation.

Element	Description
Threshold Name	The name assigned to identify a specific threshold/hysteresis configuration. This name is used when assigning the threshold/hysteresis set to ports. • Value: String, maximum length = 32 characters • Allowed characters: Alphanumeric and hyphen, underscore, and period There are 2 default threshold names: 1310 and 1550 These default values support upgrades from earlier releases; they cannot be deleted but the threshold values and hysteresis value may be modified.
Minimum Power Threshold (dBm)	Set the optical power value above the minimum power value required for this port. An alarm will occur when the measured power falls below this value minus the hysteresis value. • Value: Decimal number between -25.00 (dBm) and less than the Maximum Power Threshold
Maximum Power Threshold (dBm)	Set the optical power value below the maximum power value required for this port. An alarm will occur when the measured power falls below this value plus the hysteresis value. • Value: Decimal number greater than the Minimum Power Threshold and 20.00 (dBm) which is the maximum optical power limit for standard systems.
Hysteresis	The ± offset used in conjunction with both the above thresholds for presenting or clearing alarm conditions. Ensure this is accounted for when setting the above levels. The hysteresis value is used to prevent alarm flooding. Do not set the value so low as to cause normal power fluctuations to trigger alarms. • Value: Decimal number greater than 0.10 and less than the difference of the maximum and minimum power thresholds.
Add Threshold Button	Click this button to create a new row in the table for configuration.
Delete Threshold Button	Click this button to delete the configuration of the selected row in the table. This button will activate when a row in the table is selected.
Close Button	Click the button to close window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Adding a Signal Threshold

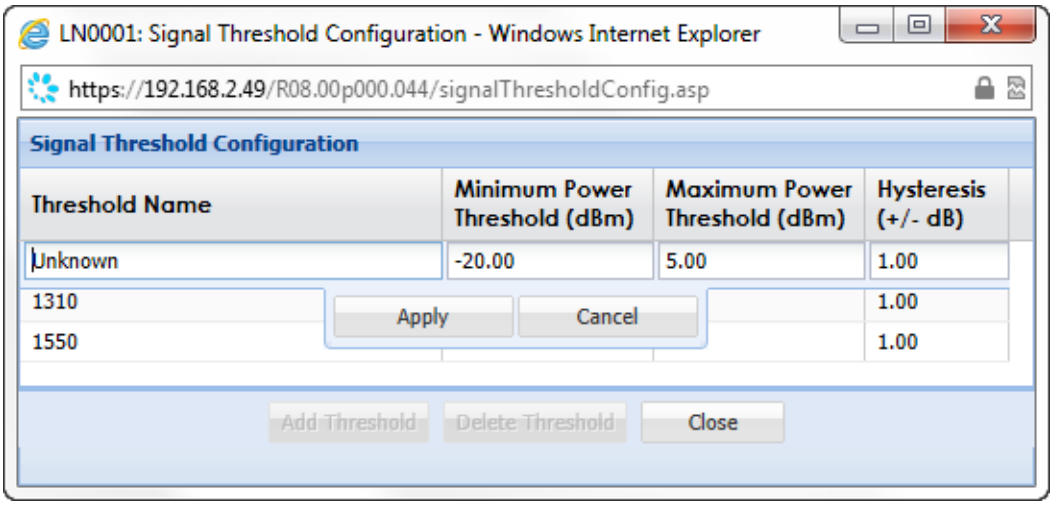
Users with the system-level privilege of Modify or higher may add signal threshold records.

To add a Signal Threshold:

1. Open the Signal Threshold Configuration window (**Configure > Signal Thresholds**).

2. From the Signal Threshold Configuration window, click the **Add Threshold** button. Figure 62 shows the changes to the window to allow configuration of the Signal Threshold values. A new row will be added to the display with the text “Unknown” written in the threshold name and default values for the optical power settings. In addition, the row will have both an **Apply** button and a **Cancel** button.

Figure 62 Signal Threshold Configuration



NOTES: For data entry help, position the mouse over the column header (e.g., **Threshold Name**) for information on maximum length, allowed characters, and input limits. These are defined in the field definitions in the previous section.

3. Enter a unique Threshold Name by overwriting the “Unknown” text in the **Threshold Name** column.

4. Edit the shown power values in the threshold fields and hysteresis field to the desired values.

5. Click the **Apply** button to save the record or click the **Cancel** button to abort the operation (remove the row). Using the window's **Close** button will both cancel the operation and close the window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

If the threshold name and power values are valid, then a status message will display briefly in the bottom right hand portion of the window: “Signal Threshold added successfully.” The window will refresh showing the addition of this signal threshold with the others currently in the system (in alphabetical order). The window will remain open to be ready for further additions, deletions, or modifications.

If the information entered for the signal threshold is invalid, a pop-up window will be presented with a message indicating the failure. See ”Signal Threshold Data Entry Errors” on page 109 for possible errors and corrective actions to take to fix each error.

Modifying a Signal Threshold

Users with the system-level privilege of Modify or higher may modify signal threshold records. The signal threshold name cannot be modified; only the threshold and hysteresis values may be changed.

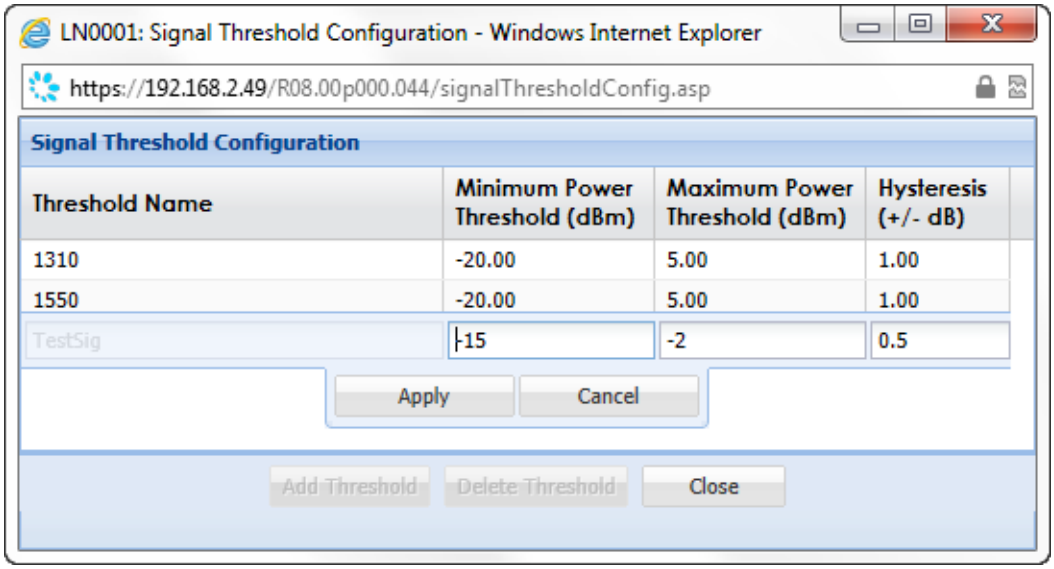
To modify a signal threshold:

1. Open the Signal Threshold Configuration window (**Configure > Signal Thresholds**).

2. From the Signal Threshold Configuration window, double-click in the signal threshold row of the signal threshold to be modified. Figure 63 shows the window after this action was performed on the signal threshold named “TestSig”. Note that the field in the **Threshold** cell is grayed out, indicating that this field is not modifiable.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 63 Signal Threshold Configuration



NOTES: For data entry help, position the mouse over the column header (e.g., **Threshold Name**) for information on maximum length, allowed characters, and input limits. These are defined in the field definitions in the previous section.

3. Edit the power values in the threshold fields and hysteresis field to the desired values.

4. Edit the shown power values in the threshold fields and hysteresis field to the desired values.

5. Click the **Apply** button to save the record or click the **Cancel** button to abort the operation (restore the pre-modification values). Using the window's **Close** button will both cancel the operation and close the window.

If the power values are valid, then a status message will display briefly in the bottom right hand portion of the window: “Signal Threshold modified successfully.” The window will refresh showing the changes to this signal threshold. The window will remain open to be ready for further additions, deletions, or modifications.

If the information entered for the signal threshold is invalid, a pop-up window will be presented with a message indicating the failure. See ”Signal Threshold Data Entry Errors” on page 109 for possible errors and corrective actions to take to fix each error.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Signal Threshold Data Entry Errors

If the information entered for the signal threshold is invalid, a pop-up window will be presented with a message indicating the failure. The possible errors are listed below. Clicking the **OK** button in the pop-up window will close this window and return to the Signal Threshold Configuration window. To fix the error, identify the row with the error and double-click the row to correct the error. Closing the Signal Threshold Configuration without correcting the error will cancel the addition or edit operation.

Error Messages:

- “Duplicate Signal Threshold Name <name> already exists”
  To correct: Change the name for the added signal threshold to a unique value
- “Minimum Power Threshold cannot be greater than the Maximum Power Threshold”
  To correct: Correct the power threshold values
- “Minimum Power Threshold cannot be less than -25”
  To correct: Choose a value no lower than -25.00
- “Minimum Power Threshold cannot be less than 20"
  To correct: Choose a value no greater than 20.00
- “Hysteresis cannot be less than 0.1"
  To correct: Choose a value no less than 0.10

Deleting a Signal Threshold

Users with the system-level privilege of Modify or higher may delete signal threshold records. The default signal thresholds 1310 and 1550 may not be deleted.

If ports are assigned to a signal threshold that is deleted, the ports will automatically be reassigned to either the 1310 or 1550 signal threshold, depending on the waveband in use by the port. If the waveband is 1310, then the signal threshold will be 1310. Similarly, 1550 will be used if the waveband is 1550.

To delete a signal threshold:

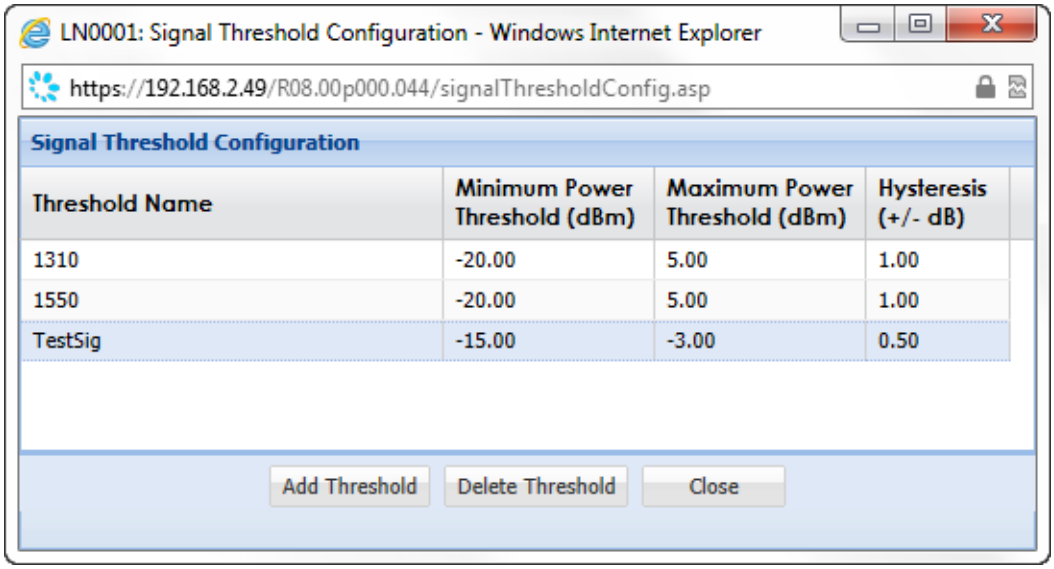
1. Open the Signal Threshold Configuration window (**Configure > Signal Thresholds**).

2. From the Signal Threshold Configuration window, select (left-click) in the signal threshold row for deletion. Figure 64 shows the window after this action was performed on the signal threshold named “TestSig”. Note that the row for “TestSig” is highlighted in light blue and the **Delete Threshold** button is now active.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

3. From the Signal Threshold Configuration window, double-click in the signal threshold row of the signal threshold to be modified. shows the window after this action was performed on the signal threshold named “TestSig”. Note that the field in the **Threshold** cell is grayed out, indicating that this field is not modifiable.

Figure 64 Deleting a Signal Threshold



4. Click the **Delete Threshold** button to delete the record.
   - Using the window's **Close** button will both cancel the operation and close the window.
   - Clicking the **Add Threshold** button will abort the operation and start the Add a Signal Threshold operation.

5. After clicking the **Delete Threshold** button a confirmation pop-up window will appear with the message “Press OK to delete or Cancel” as well as both **OK** and **Cancel** buttons.

6. Click the **OK** button to delete record. Click the **Cancel** button to abort the operation.

If the **OK** button is used, a status message, “Signal Threshold deleted successfully”, will display briefly in the bottom right hand portion of the window and the window will refresh showing the remaining signal thresholds. If the Cancel button is used, the window returns to the condition shown in Figure 64. The window will remain open ready for further actions.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Ports

The **Configure > Ports** sub-menu options (Figure 65) allow configuration of all port attributes.

Figure 65 ***Configure > Ports*** *Menu Options*

The table below enumerates these menu options. The first section, ”Configurable Port Attributes” on page 112, defines all the attributes that may be either configured or changed.

Section	Description	Page
Configurable Port Attributes	This section lists all configurable port attributes, the port privilege required to change the attribute, as well as any special rules regarding limitations on the values (characters, values).	112
Import/Export Port Configuration	This section covers the operation of the Import and Export Port Configuration windows, which allow port names and descriptions to be applied from a file generated off-system.	113
Change Port Configuration	This section covers the operation of the Port Configuration window that supports viewing and editing of port names, descriptions, port group membership, and signal threshold assignment.	119
Clear Port Parameters	This section covers the operation of global clearing of all port names and/or port descriptions.	122
Change Waveband Assignment	This section covers the assignment of waveband designation to ports. The Waveband Assignment window shows all current port to waveband assignments and supports re-assignment of ports (individually or in ranges) between the two supported wavebands (1310 and 1550).	123
Change Signal Threshold Assignment	This section covers the assignment of signal thresholds to ports. The Signal Threshold Assignment window shows all current port to signal threshold assignments and supports re-assignment of ports (individually or in ranges) among the available signal thresholds.	126

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Section	Description	Page
Change Group Assignment	This section covers the assignment of ports among available port groups. The Port Group Assignment window shows the current assignments and allows re-assignment of ports (individually or in ranges) among the available port groups.	130
Change Alarm Severity Assignment	This section covers the assignment of severities for port and connection alarms. The Alarm Severity Assignment window shows the current severity assignments and allows re-assignment of the severity used by ports (individually or in ranges).	135
Import/Export Group Assignment	This section covers the operation of the Import and Export Group Assignment windows allowing port to port group assignments to be applied from a file generated off-system.	140

Configurable Port Attributes

The table below lists the port configuration attributes and describes the usage, valid entries, and privileges required to change the values or value assignments.

Configurable Port Attribute	Description
Port Name	Port names are used as an alternate method to port numbers to identify ports in the system. As such, port names must be unique. • Value: String, maximum of 32 characters • Invalid characters (blocked, cannot enter): quote (“), apostrophe(‘), colon (:), semi-colon (;), backslash (\), and whitespace Requires port privilege of Modify or higher to configure.
Port Description	Port descriptions support entry of information about the port which may be helpful for identification or troubleshooting. There is no uniqueness requirement for this field. • Value: String, maximum of 32 characters • Invalid characters (blocked, cannot enter): semi-colon (;) Requires port privilege of Modify or higher to configure.
Port Group	Port groups may be used to restrict connections between ports in the system. Port grouping is a licensed feature. If not licensed, port group configuration is hidden • Value: Port Group Name Requires port privilege of Manage on all ports to assign

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Configurable Port Attribute	Description
Waveband	The waveband specifies the wavelength range of the signal on the input fiber. This value is used for calibration and power monitoring. The value is assigned to the input port and automatically assigned to an output port when a connection is made • Values: 1310 or 1550 1310: Use when the signal is between 1260nm and 1460nm 1550: Use when the signal is between 1460nm and 1630nm Requires port privilege of Modify or higher to assign
Signal Threshold	Signal thresholds are used to assign optical power thresholds that establish alarm reporting conditions for the minimum optical power threshold (STMIN) and maximum optical power threshold (STMAX) alarm types. • Value: Signal Threshold Name Requires port privilege of Modify or higher to change
Alarm Severities	There are five severity settings which may be set for the optical power threshold alarm types (STMIN and STMAX) as well as for a the connection fault alarm type (CSFLT). In ClickFlow, the alarm types are designated as: • Min Power Alarm (STMIN) - applies to both input and output ports • Max Power Alarm (STMAX) - applies to both input and output ports • Connection Alarm (CSFLT) – applies only to output ports The severity associated (reported) for the above alarms may be configured for each port. Thus, an STMIN alarm may be considered Critical for one port, Minor for another port, and disabled (not reported) for yet another port. The severity values are shown below: • Values: Critical, Major, Minor, Notice, Disable Notice: The alarm will be detected and logged but no notification will be sent to external alarm management systems (e.g., SNMP managers). Disable: The alarm condition is disabled the alarm will not be reported. Requires port privilege of Modify or higher to change

Import/Export Port Configuration

A user can import port names and descriptions after creating a port number to port name and port description mapping file (.csv format) using a text editor or spreadsheet program. However, only the ports for which the user has port-level privilege of Modify or higher will be changed.

All users may export port names and descriptions to a file. However, the exported file will only contain the ports for which the user has View or higher port-level privileges.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Port Name/Description File Guidelines

Figure 66 below shows the contents of a names.csv file exported from a system without PMU or VOA ports.

Prior to the export, port names were configured for inputs 10001 and 10002, and port descriptions were entered for inputs 10002 and 10003. This file was opened with Excel, and the figure shows the default output (comments, rows, and columns) generated along with actual data for the configured ports. If not changed by the user, the default file name will be *names.csv.*

Figure 66 Example Exported Names File

	A	B	C
1	# Glimmerglass Optical Switch Port Name File		
2	# SwitchName: LN0001		
3	# UserName: admin		
4	# Generated: Mon Jun 3 14:20:13 2013		
5	# <Comments entered by user when exporting this file>		
6	# Format: 8.0		
7	# <port>	<name>	<description>
8	10001	InPort1	
9	10002	InPort2	Port_Comment
10	10003		Port_Comment

Referencing Figure 66, the format of a names file may contain the elements described in the table below. The table also indicates which fields are mandatory and which are optional.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
#Comment Lines (Rows 1 -7) (Optional)	The user may enter comments at the top of the file (before the start of the comma separated values). Comments are not mandatory, but if included they must be marked with a hash (#) character at the start of each line. For exported files, Figure 66 shows the comments that are included. • (Title line): Glimmerglass Optical Switch Port Name File • SwitchName: <SystemName from which names were exported> • UserName: <ID of the user that exported the names> • Generated: <Date/time when export was performed> • (Comment line): This line will contain any comments entered at the time of export. This line is optional; If nothing is entered, the line is not included. • Format: <Software release on the system from which topology was exported> • (Column title line): This is a reference line showing the order of entry for the values which may be entered in comma separated format. These fields are defined in the following rows of this table and are marked as required or optional.
<port> (Required Field)	The long port number (e.g., 10xxx or 20xxx) for the port to be assigned a name and or description. This field is required when adding ports to the file for assigning names or numbers. When exported, rows with port configuration data will be provided for ports when: • The port has previously been assigned a name or comment • If PMU and/or VOAs are present in the system, the port numbers for these ports will always appear and the name column will contain the default system port name for the PMU/VOA (unless the user has assigned a unique name which will then be displayed). • No rows will appear for ports where both the port name and port description are empty in the system (null values). References: • See ”Photonic Multicasting™ Unit” on page 22 for default PMU names. • See ”Variable Optical Attenuation (VOA)” on page 24 for default VOA names.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
<name> (Required)	The unique name to assign to this port. See ”Configurable Port Attributes” on page 112 for port naming rules. When the configuration is exported: • The port name will appear if one is configured or if the port is used with either a PMU or VOA. • This value may be empty (null) if a name is not configured but a port description is configured. Import errors: • The entire import will fail if the port name is not unique or violates the port naming conventions.
<description> (Required)	The description to assign to this port. See ”Configurable Port Attributes” on page 112 for port description rules. When exported, the field value is: • The port description will appear if one is configured for the port. • This value may be empty (null) if a description is not configured but a port name is configured. Import errors: • The entire import will fail if the port description violates port description rules.

The bullets below summarize the rules for creating a file for the purpose of importing port names and descriptions:

- The file must be saved as either a .csv file or a .txt file.
- Comments must be at the top of the file and the comment line must start with a # character.
- Each line of data must be formatted as shown below:
  <Long Port #>,<PortName>,<PortDescription>
- The value fields must be separated by a comma.
- Port name and description entries must be valid per the rules in ”Configurable Port Attributes” on page 112.

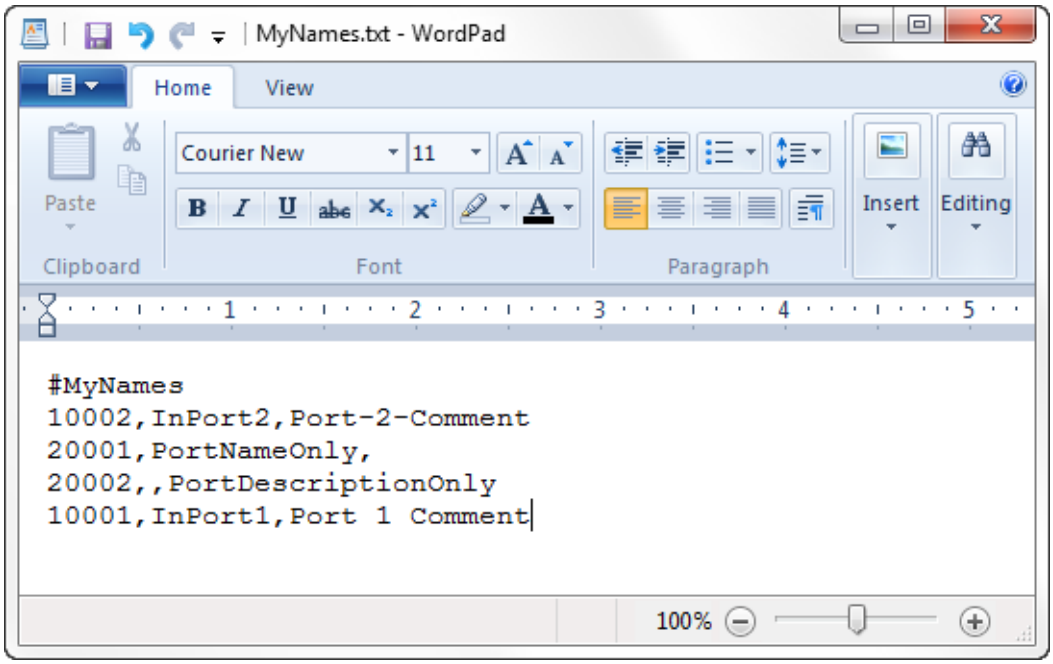
Creating a Port Name/Description File for Import

Figure 66 on page 114 shows a names.csv file created by exporting the current port names/descriptions from the system. This is a good method for creating a default file as well (export the existing file then modify as appropriate). However, it is possible to create files from scratch for import to the system. This can be done using a spreadsheet program and saving the file as a .csv file or using a text editor such as WordPad.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 67 below shows an example of a file, *MyNames.txt*, created using WordPad for import into a system.

Figure 67 Example Port Name/Description File Created with Text Editor



The above file, when imported, will change the names and descriptions for the four ports to the values shown in the file. The existing values for these ports will be replaced.

Import File Operation

When a file is imported, the file is checked for errors in the data. If any of the errors listed below are detected, the import operation is aborted and the user is presented a pop-up indicating the first error found in the file:

- A duplicate or illegal port number is found in the first column.
- A duplicate port name if found in the second column.
- An invalid character is included in a port name or port description.

After the data in the file is validated, then both the port names and descriptions are applied for all ports included in the file (providing the user has the required privilege). Therefore, if either the name or description fields are blank (null) for any port number, the existing value will be set to null. Ports which are not included in the file are not affected by the import. The names and descriptions configured for those ports will remain in effect if not included in the file.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

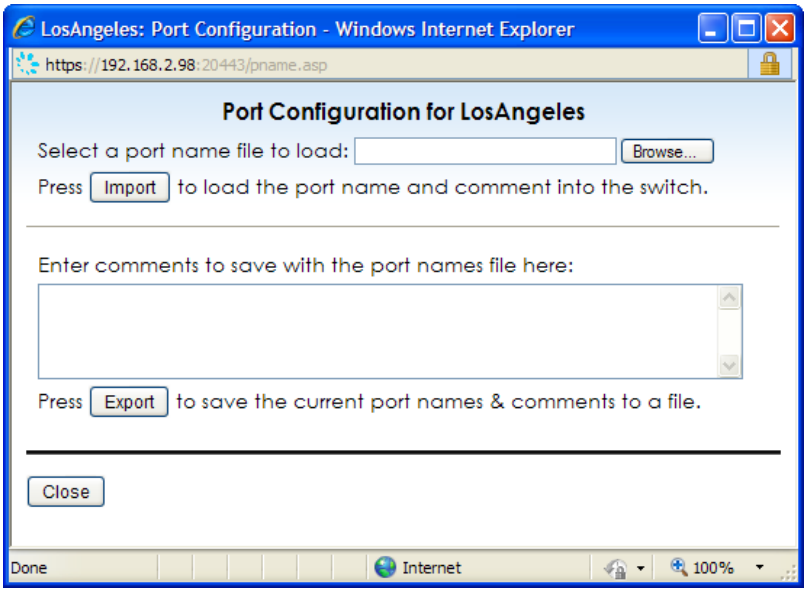
Importing a Port Name/Description File

A user can import port names and descriptions from a port names/descriptions file. However, only ports for which the user has Modify or higher port-level privileges will be updated.

To import a port name/description file that assigns custom port names and descriptions:

1. Select the **Configure > Ports > Import/Export Port Configuration** menu option from the Connection screen to view the Import/Export Port Configuration window (Figure 68).

Figure 68 Import/Export Port Configuration Window



2. In the Port Configuration window, click the **Browse...** button to display the Browse window.

3. In the Browse window, navigate to the port name/description .csv or .txt file to be imported.

4. Select the file and click the **Open** button. The Browse window closes and the file path is listed in the Port Configuration window.

5. In the Port Configuration window, click the **Import** button to load the port name/description file.

6. Click the **OK** button in the dialog box to confirm that the file has been successfully imported.

NOTE: If the names file to be imported contains syntax errors or duplicate port names (two ports with the same port name), the import will fail (no change to the system port names/descriptions).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Exporting Port Names/Descriptions

A user can export the currently assigned port names/descriptions of ports for which their port-level privilege is View or higher into a .csv file for viewing/editing. Note that the port numbers are always presented in the 5-digit format.

To export the port names currently used by the system to a text file:

1. Select the **Configure > Ports > Import/Export Port Configuration** menu option from the Connection screen to view the Port Configuration window (Figure 68 on page 118).

2. In the Port Configuration window, enter descriptions to be saved with the port names. These descriptions are inserted into the default heading at the beginning of the file (see Figure 66 on page 114). If the **Comments** section is left blank, the default heading is inserted at the beginning of the file.

3. In the Port Configuration window, click the **Export** to view the (web browser dependent) File Download window.

4. From the File Download window:
   - Click **Open** to view the exported port name file.
   - Click **Save** to select a name and location to save the port name file.

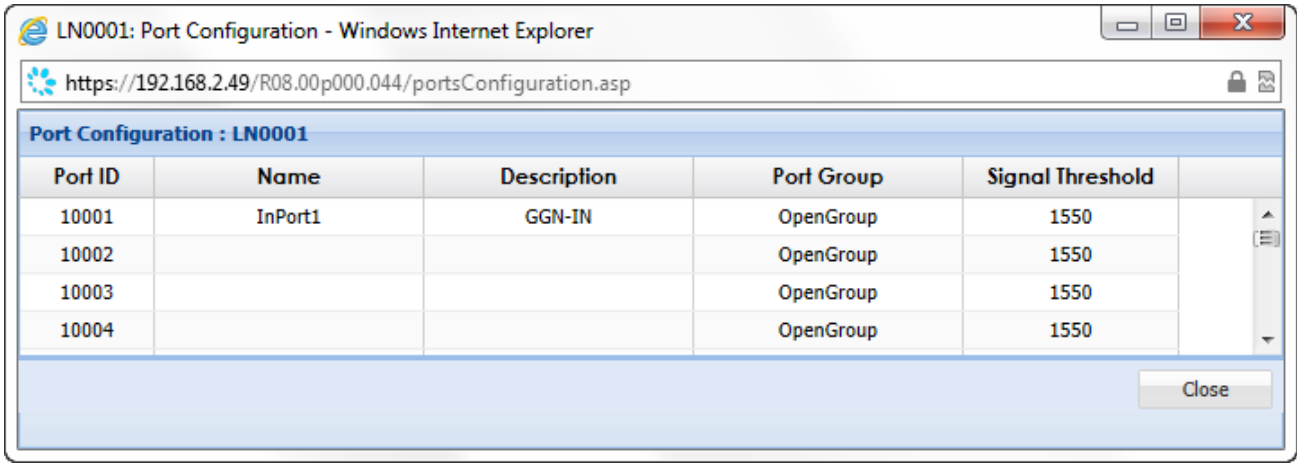
NOTE: The exported file will contain only the ports for which the user has View or higher port-level privileges.

Change Port Configuration

The **Configure > Ports > Change Port Configuration** menu option opens the Port Configuration window shown in Figure 69 below. This window allows entry of port names and port descriptions as well as changing the port group and signal threshold assignments. The Port Configuration window displays only ports for which the user has Modify or higher port privileges.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 69 Port Configuration Window (System with Port Grouping License)



The ports are displayed in numerical order based upon the long port number in the Port ID field. The remaining columns, Name, Description, Port Group, and Signal Threshold are the attributes for the ports that may be modified from this window.

The Port Group column is displayed only for systems with the Port Grouping license enabled. All fields displayed in the window are described in the table below.

Element	Description
Port ID (read-only)	This is the key for the record and contains the port number
Name	Text Box for editing the port name.
Description	Text Box for editing the port description.
Port Group	Pull-Down menu containing all port groups in the system. (Displayed only on systems licensed for Port Grouping; requires full system administrative privileges to change.)
Signal Threshold	Pull-Down menu list containing all signal thresholds in the system.

All column headers support ascending/descending sort for grouping by the values contained. Tool tips are provided when placing the mouse on the column header for the columns supporting modifications. Vertical and horizontal scroll bars will appear when the window size is too small to show all entries.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Editing Port Attributes in the Port Configuration Window Table

Perform the following steps to edit the port attributes.

NOTES: The Port Group field cannot be opened for edit unless the user has full system administrative privileges.

Port name and description changes are reflected immediately for all users.

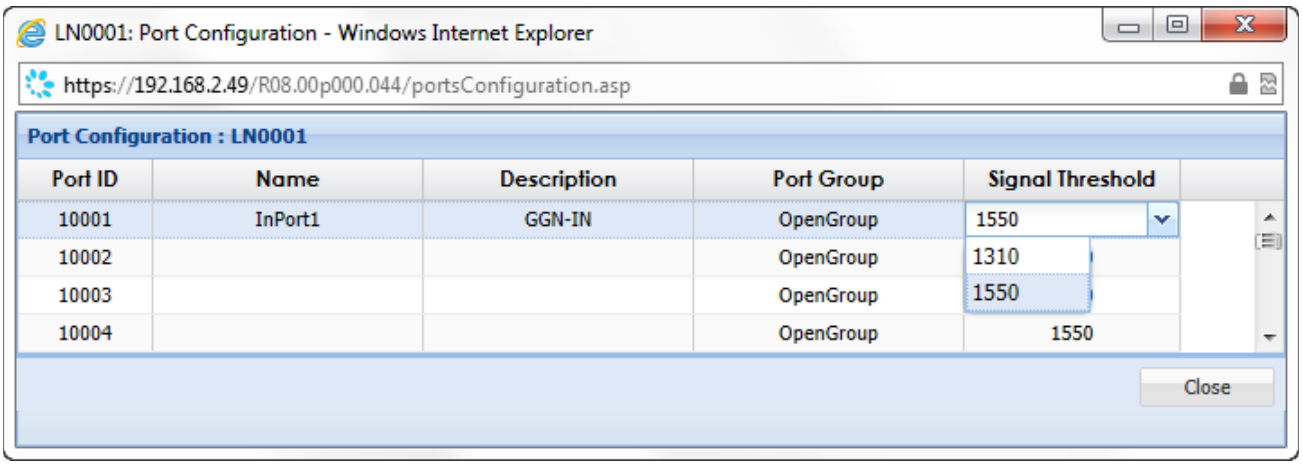
Port group assignment changes are immediate, but the user must refresh the screen to see the updated display of the I/O Matrix.

To perform bulk changes most efficiently, use the Export/Import functions described in ”Import/Export Port Configuration” on page 113.

1. Open the Port Configuration window by selecting **Configure > Ports > Change Port Configuration**

2. In the row for the port, double-click on the value to be modified.
   - For the **Name** and **Description** fields, the cell will change to a text box supporting entry of a text string. Enter the desired new value.
   - For the **Port Group** and **Signal Threshold** fields, the provided pull-down menu presents the available values. Select the desired value from the pull-down menu (see Figure 70).

Figure 70 Modifying Port Configuration



3. After the value is entered or selected for the field (or left unchanged), use one of the following methods to accept the changed value (or leave the value unchanged):
   - Hit the **<Tab>** key. This will accept the entry and automatically open the next field for modification. Using this method, it is possible to move through ports and values and selectively modify only the desired fields.
   - Hit the **<Enter>** key.

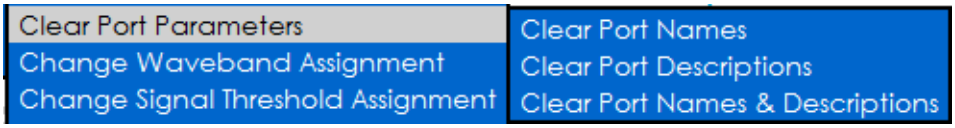
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- Left click outside the field being modified.
- Double-click on the next port/value cell to be modified.

Clear Port Parameters

The **Configure > Clear Port Parameters** menu option supports the three sub-menu option shown in Figure 71 below.

Figure 71 Clear Port Parameters Sub-menu



These options allow a user to clear (set to null value) port names and descriptions on ports for which the user has port-level privilege of Manage. The other port attributes (signal threshold, waveband, port group, and alarm severities) cannot be set to a null value.

- To clear all port names only, select **Configure > Ports > Clear Port Parameters > Clear Port Names**. A pop-up confirmation box will appear requesting confirmation for the clear.
- To clear all port descriptions only, select **Configure > Ports > Clear Port Parameters > Clear Port Descriptions**. A pop-up confirmation box will appear requesting confirmation for the clear.
- To clear all port names and descriptions, select **Configure > Ports > Clear Port Parameters > Clear Port Names & Descriptions**. A pop-up confirmation box will appear requesting confirmation for the clear.

NOTES: Due to the scope of the operation, the “clear all” options operate only on ports where the user has Manage port privilege. If a user without the Manage privilege executes the operation, the pop-up confirmation box indicates that only ports where the user has Manage privilege will be cleared. Nothing will happen on all other ports.

The same user with Modify privileges is allowed to edit port names and descriptions individually or import a port names file to change port names. However, there is less chance of accidentally deleting this information.

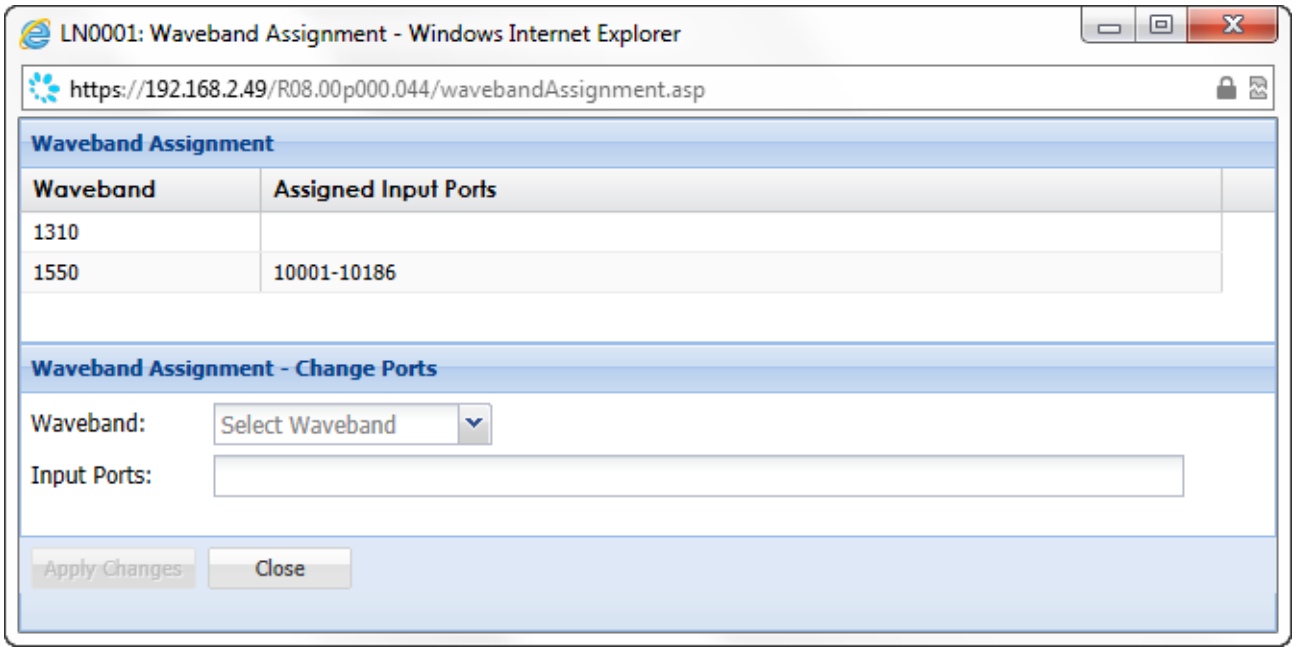
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Change Waveband Assignment

The **Configure > Ports > Change Waveband Assignment** menu option opens the Waveband Assignment window shown in Figure 72 below. This window supports reassigning one or many inputs ports from one waveband to the other. Only ports for which the user has Modify or higher port privileges are shown. The port privilege of Modify is required to change a port's waveband assignment.

NOTE: The Configure Port context menu described in Chapter 3 may also be used to reassign the waveband for a port. This method is accessed directly from the I/O Matrix and is convenient when acting on one or a few ports.

Figure 72 Waveband Assignment Window



Referencing Figure 72, the Waveband Assignment window is composed of two sections:

- The upper section has a row for each waveband showing the ports currently assigned to each waveband.
- The lower section is used to change port assignments. The following fields are provided:
  - **Waveband** - Pull-down menu used to select the appropriate waveband.
  - **Input Ports** - Text box used to enter the port numbers to assign to the selected waveband.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTES: Tool tips are provided when the mouse is placed over either field in the lower section. The tool tips convey the following information for data entry:

Waveband Selection Criteria

- Select 1310 for input signals between 1260nm and 1530nm
- Select 1550 for input signals between 1530nm and 1625nm

Entering port numbers in the **Input Ports** text box:

- Use long port numbers (e.g., 10xxx for input)
- Use a hyphen between port numbers to specify a range of ports
- Use a comma as a separator between port numbers or port ranges.

Example **Input Ports** entry:

- 10001,10010,10020-10030,10040-10050,10060

Two buttons are provided at the bottom left of the window: **Apply Changes** and **Close**. The **Apply Changes** button will be inactive until the user starts the assignment process in the lower section by selecting a waveband then entering input port numbers. The **Close** button will close the window.

To change the waveband assignment for a port, perform the following steps:

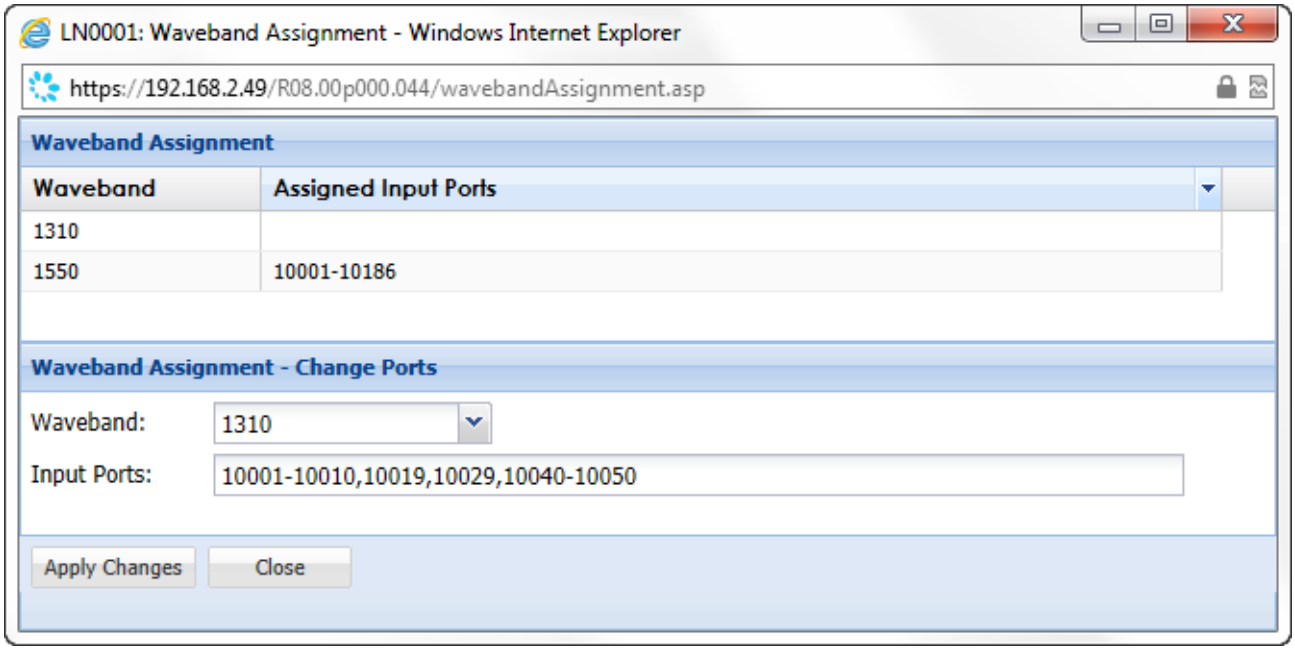
1. Open the Waveband Assignment window (**Configure > Ports > Change Waveband Assignment**)

2. From the **Waveband** pull-down menu, select the desired waveband.

3. In the **Input Ports** text box, enter the port number, port numbers and/or port number range for assignment to this waveband. The **Apply Changes** button will activate. Figure 73 below depicts the Waveband Assignment window after selecting a waveband and entering the desired input ports.

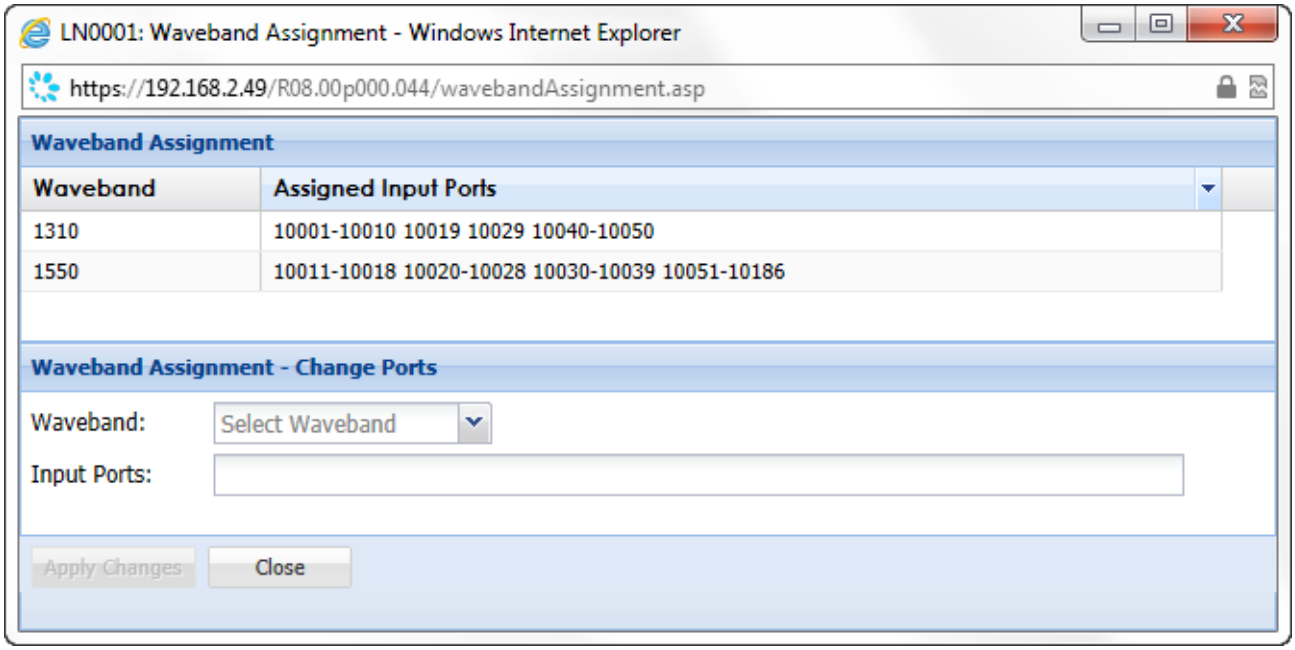
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 73 Waveband Assignment Window (After Entering Waveband Assignment Data)



4. Click the **Apply Changes** button to change the waveband assignment for the entered input ports. After a moment, the window will refresh. The upper section will display the new port waveband assignments as shown in Figure 74 below.

Figure 74 Waveband Assignment Window (After Applying Changes)



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

5. Once finished with waveband assignment, click the **Close** button to exit the window. Otherwise, continue with the next set of port assignments.

The area below the **Apply Changes** button is used to post status messages reporting success or failure of the waveband assignment. These status messages automatically clear after a few seconds.

The possible status messages shown after applying changes are described below. For errors, selections in the upper sections of the window will remain unchanged. The lower section is cleared and the window is ready to accept corrected data.

Status Messages:

- "Success: All updates completed"
  This message indicates that the ports and/or port ranges entered were composed of valid port numbers.
- "Success: All updates completed for valid port numbers"
  This message indicates that the port list contained invalid port numbers (numbers not represented in the upper section). In this case, the requested change was made for the valid port numbers and the invalid numbers were ignored. The upper section reflects the new configuration.
- "Error: Invalid Port Number or Invalid Port Range"
  This message indicates that all the port numbers entered in the input port list are resolved as invalid. For a range, this may occur if only the starting number of the range is invalid. If only some port numbers are invalid, then the status would be "Success: All updates completed for valid port numbers"
- "Error: Missing Port Group and/or Ports"
  This message indicates one of the following:
  - Input ports were entered (activates **Apply Changes** button) and then the **Apply Changes** button was used without selecting a waveband.
  - The **Waveband** value was selected then input ports were entered. Then, the port field was erased (now blank) and the **Apply Changes** button was used.

Change Signal Threshold Assignment

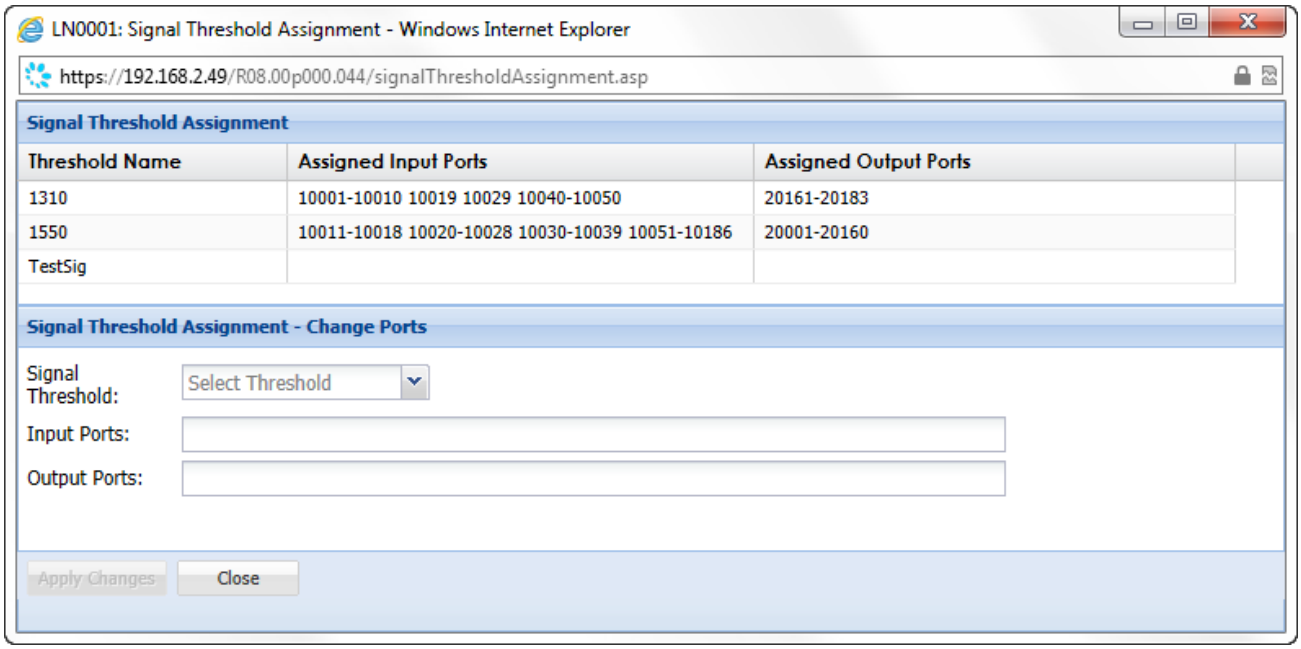
The **Configure > Ports > Change Signal Threshold Assignment** menu option opens the Signal Threshold Assignment window shown in Figure 75 below. This window supports reassigning ports from among the signal thresholds configured in the system. Only ports for which the user has Modify

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

or higher port privileges are shown. The port privilege of Modify is required to change a port's signal threshold assignment.

NOTE: The Configure Port context menu described in Chapter 3 may also be used to reassign the signal threshold for a port. This method is accessed directly from the I/O Matrix and is convenient when acting on one or a few ports.

Figure 75 Signal Threshold Assignment Window



Referencing Figure 75, the Signal Threshold Assignment window is composed of two sections:

- The upper section has a row for each signal threshold showing the ports currently assigned to each signal threshold.
- The lower section is used to change port assignments. The following fields are provided:
  - **Signal Threshold** - Pull-down menu used to select the appropriate signal threshold.
  - **Input Ports** - Text box used to enter the input port numbers to assign to the selected signal threshold.
  - **Output Ports** - Text box used to enter the output port numbers to assign to the selected signal threshold.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTES: Tool tips are provided when the mouse is placed over either field in the lower section. The tool tips convey the following information for data entry:

Signal Threshold Selection Criteria:

- Select the threshold name which matches the optical thresholds required.

Entering port numbers in the **Input Ports** or **Output Ports** text boxes:

- Use long port numbers (e.g., 10xxx for input, 20xxx for output)
- Use a hyphen between port numbers to specify a range of ports
- Use a comma as a separator between port numbers or port ranges.

Example **Input Ports** entry:

- 10001,10010,10020-10030,10040-10050,10060

Two buttons are provided at the bottom left of the window: **Apply Changes** and **Close**. The **Apply Changes** button will be inactive until the user starts the assignment process in the lower section by selecting a signal threshold then entering input port numbers and/or output port numbers. The **Close** button will close the window.

To change the signal threshold assignment for a port, perform the following steps:

1. Open the Signal Threshold Assignment window (**Configure > Ports > Change Signal Threshold Assignment**)

2. From the **Signal Threshold** pull-down menu, select the desired signal threshold.

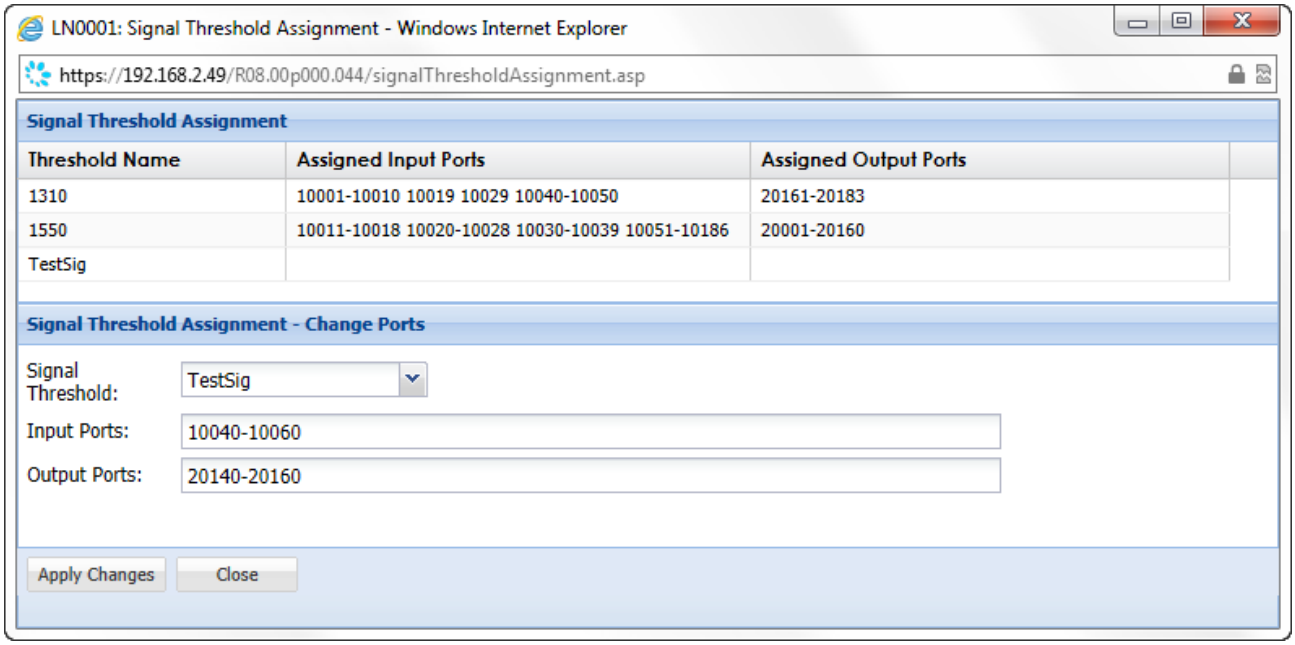
3. In the **Input Ports** text box, enter the input port number, port numbers, and/or port number range for assignment to this signal threshold. (This step is optional: This field can be left empty if assigning only output ports.)

4. In the **Output Ports** text box, enter the output port number, port numbers, and/or port number range for assignment to this threshold. (This step is optional: This field can be left empty if assigning only input ports.)

   Once port numbers are entered, the **Apply Changes** button will activate. Figure 76 below depicts the Signal Threshold Assignment window after selecting a signal threshold and entering the desired input ports.

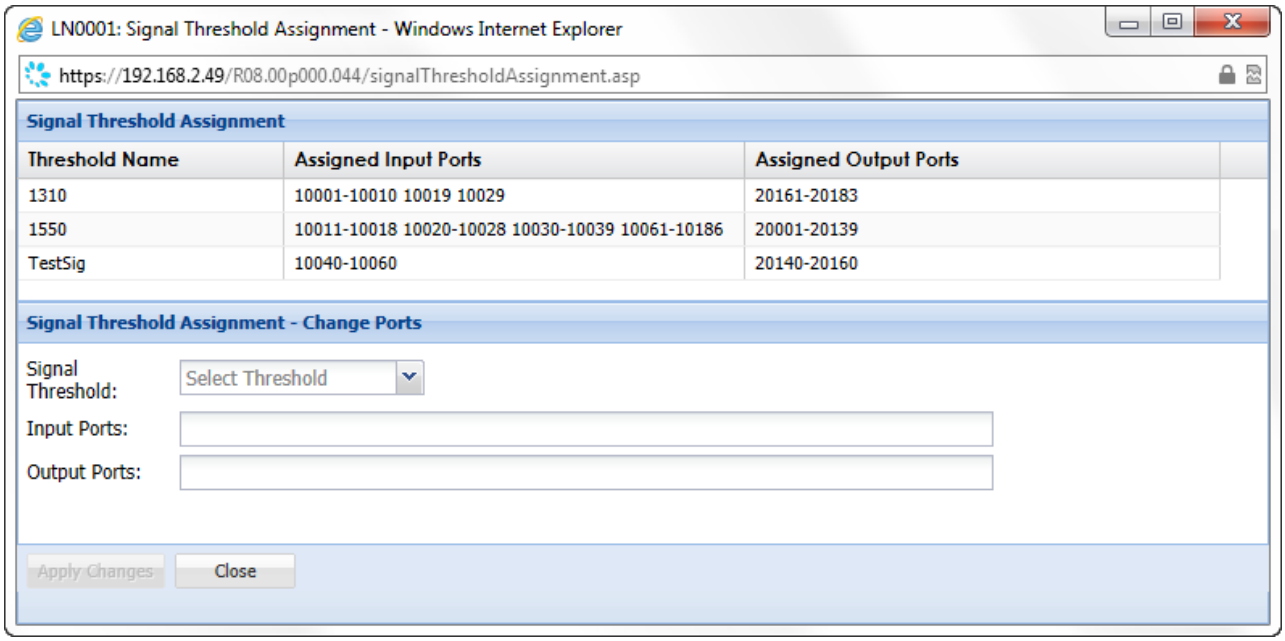
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 76 Signal Threshold Assignment Window (After Specifying Port Changes)



5. Click the **Apply Changes** button to change the signal threshold assignment for the entered ports. After a moment, the window will refresh. The upper section will display the new port signal threshold assignments as shown in Figure 77 below.

Figure 77 Signal Threshold Assignment Window (After Applying Changes)



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

6. Once finished with signal threshold assignment, click the **Close** button to exit the window. Otherwise, continue with the next set of port assignments.

The area below the **Apply Changes** button is used to post status messages reporting success or failure of the signal threshold assignment. These status messages automatically clear after a few seconds.

The possible status messages shown after applying changes are described below. For errors, selections in the upper sections of the window will remain unchanged. The lower section is cleared and the window is ready to accept corrected data.

Status Messages:

- "Success: All updates completed"
  This message indicates that the ports and/or port ranges entered were composed of valid port numbers.
- "Success: All updates completed for valid port numbers"
  This message indicates that one or both port lists contained invalid port numbers (numbers not represented in the upper section). In this case, the requested change was made for the valid port numbers and the invalid numbers were ignored. The upper section reflects the new configuration.
- "Error: Invalid Port Number or Invalid Port Range"
  This message indicates that all the port numbers entered in both port lists are resolved as invalid. For a range, this may occur if only the starting number of the range is invalid. If only some port numbers are invalid, then the status would be "Success: All updates completed for valid port numbers"
- "Error: Missing Port Group and/or Ports"
  This message indicates one of the following:
  - Input or output ports were entered (activates **Apply Changes** button) and then the **Apply Changes** button was used without selecting a signal threshold.
  - The **Signal Threshold** value was selected then input ports were entered. Then, the port fields were erased (now blank) and the **Apply Changes** button was used.

Change Group Assignment

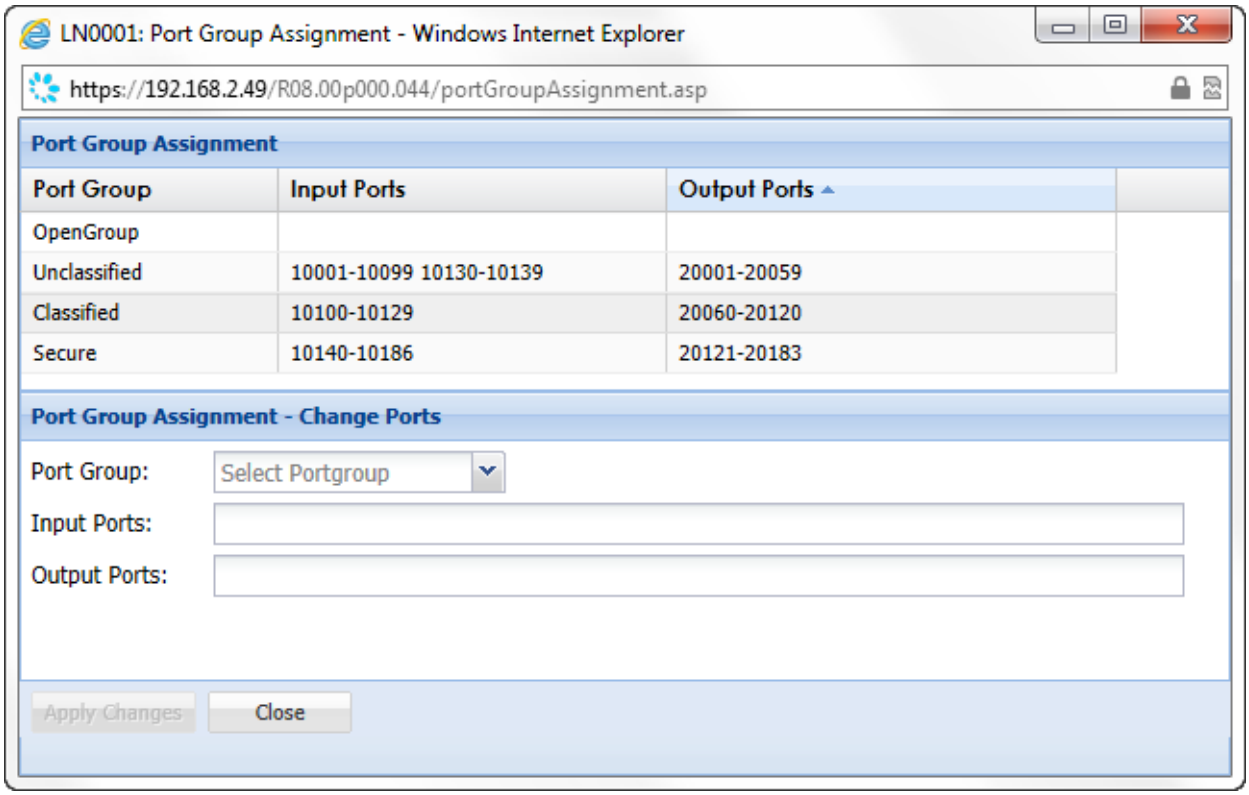
The **Configure > Ports > Change Group Assignment** menu option opens the Port Group Assignment window shown in Figure 78 below. This window supports reassigning ports from among the port groups configured in the system. This option is available only on systems with the Port Grouping

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

license, and on those systems the option is available only for users with Manage level system and port privileges for all ports in the system (e.g., a full system administrator).

NOTE: The Configure Port context menu described in Chapter 3 may also be used to reassign the port group for a port. This method is accessed directly from the I/O Matrix and is convenient when acting on one or a few ports.

Figure 78 Port Group Assignment Window



Referencing Figure 78, the Port Group Assignment window is composed of two sections:

- The upper section has a row for each port group configured in the system showing the ports currently assigned to each port group.
- The lower section is used to change port assignments. The following fields are provided:
  - **Port Group** - Pull-down menu used to select the appropriate port group.
  - **Input Ports** - Text box used to enter the input port numbers to assign to the selected port group.
  - **Output Ports** - Text box used to enter the output port numbers to assign to the selected port group.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTES: Tool tips are provided when the mouse is placed over either field in the lower section. The tool tips convey the following information for data entry:

Port group:

- Select the group name from the upper section to which the ports are to be assigned.

Entering port numbers in the **Input Ports** or **Output Ports** text boxes:

- Use long port numbers (e.g., 10xxx for input, 20xxx for output)
- Use a hyphen between port numbers to specify a range of ports
- Use a comma as a separator between port numbers or port ranges.

Example **Input Ports** entry:

- 10001,10010,10020-10030,10040-10050,10060

Two buttons are provided at the bottom left of the window: **Apply Changes** and **Close**. The **Apply Changes** button will be inactive until the user starts the assignment process in the lower section by selecting a port group then entering input port numbers and/or output port numbers. The **Close** button will close the window.

To change the port group assignment for a port, perform the following steps:

1. Open the Port Group Assignment window (**Configure > Ports > Change Group Assignment**)

2. From the **Port Group** pull-down menu, select the desired port group.

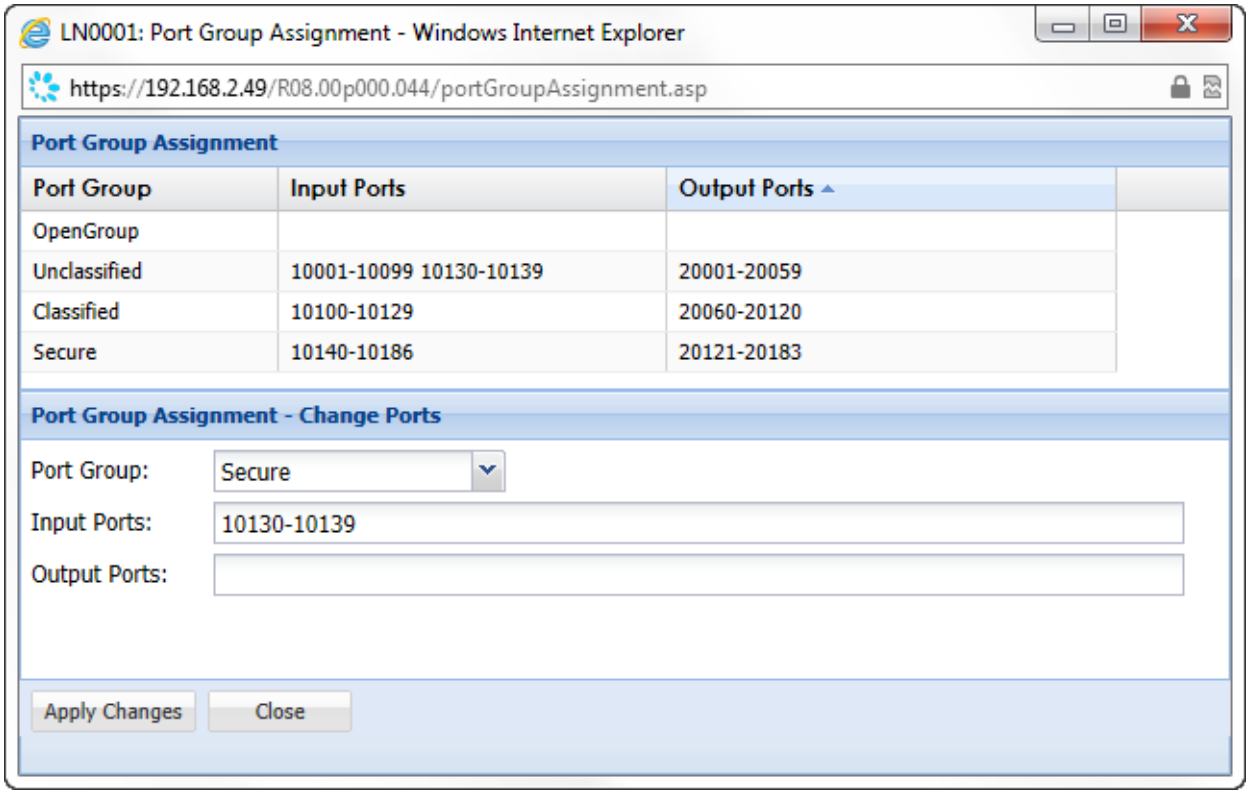
3. In the **Input Ports** text box, enter the port number, port numbers, and/or port number range for assignment to this port group. (This step is optional: This field can be left empty if assigning only output ports.)

4. In the **Output Ports** text box, enter the output port number, port numbers, and/or port number range for assignment to this port group. (This step is optional: This field can be left empty if assigning only input ports.)

   Once port numbers are entered, the **Apply Changes** button will activate. Figure 79 below depicts the Port Group Assignment window after selecting a port group and entering the desired ports.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

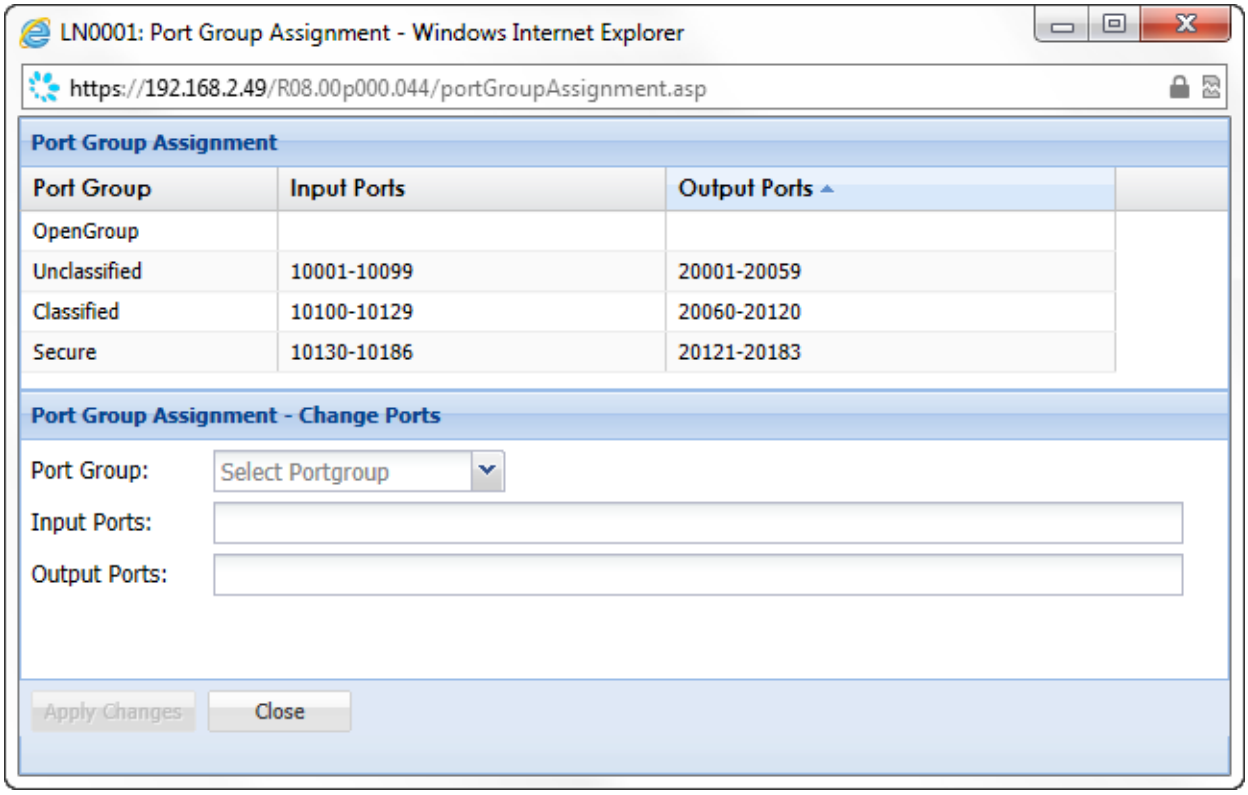
Figure 79 Port Group Assignment Window (After Specifying Port Changes)



5. Click the **Apply Changes** button to change the port group assignment for the entered ports. After a moment, the window will refresh. The upper section will display the new port group assignments as shown in Figure 80 below.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 80 Port Group Assignment Window (After Applying Changes)



6. Once finished with port group assignment, click the **Close** button to exit the window. Otherwise, continue with the next set of port assignments.

The area below the **Apply Changes** button is used to post status messages reporting success or failure of the port group assignment. These status messages automatically clear after a few seconds.

The possible status messages shown after applying changes are described below. For errors, selections in the upper sections of the window will remain unchanged. The lower section is cleared and the window is ready to accept corrected data.

Status Messages:

- "Success: All updates completed"
  This message indicates that the ports and/or port ranges entered were composed of valid port numbers.
- "Success: All updates completed for valid port numbers"
  This message indicates that one or both port lists contained invalid port numbers (numbers not represented in the upper section). In this case, the requested change was made for the

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

valid port numbers and the invalid numbers were ignored. The upper section reflects the new configuration.

- "Error: Invalid Port Number or Invalid Port Range"
  This message indicates that all the port numbers entered in both port lists are resolved as invalid. For a range, this may occur if only the starting number of the range is invalid. If only some port numbers are invalid, then the status would be "Success: All updates completed for valid port numbers"
- "Error: Missing Port Group and/or Ports"
  This message indicates one of the following:
  - Input or Output ports were entered (activates **Apply Changes** button) and then the **Apply Changes** button was used without selecting a signal threshold.
  - The **Port Group** value was selected then input ports were entered. Then, the port fields were erased (now blank) and the **Apply Changes** button was used.

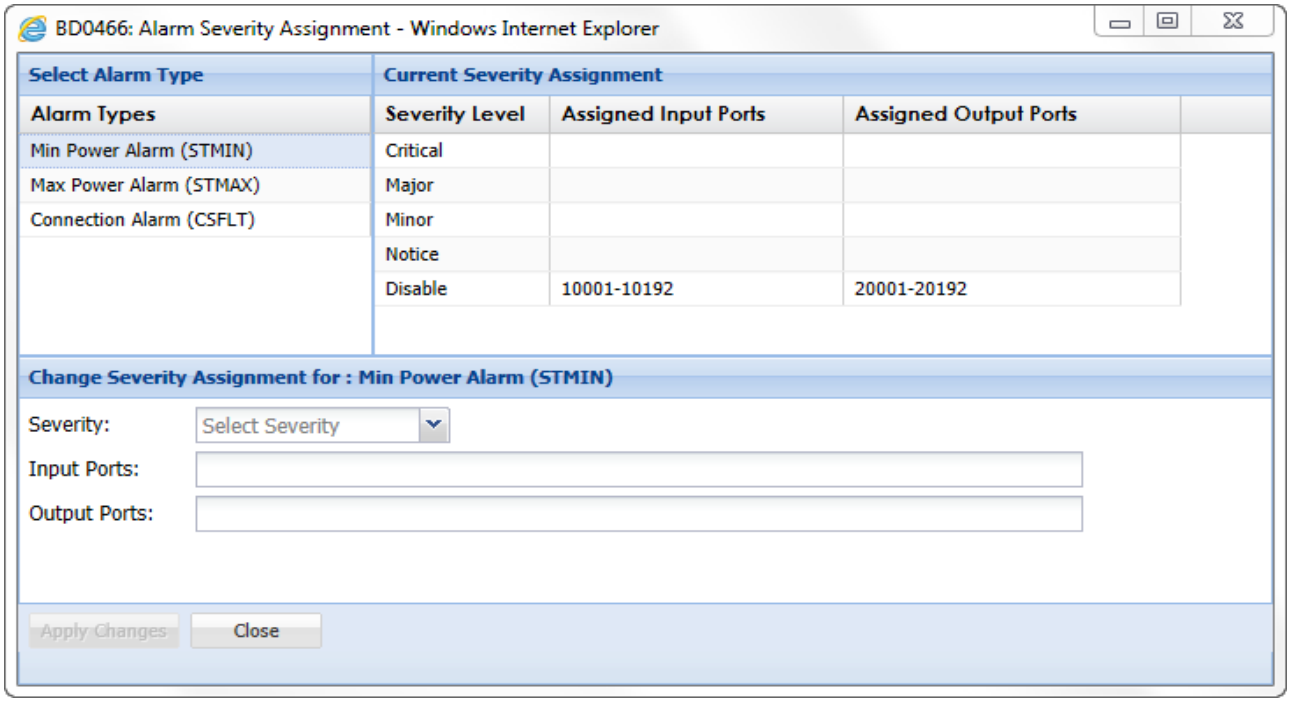
Change Alarm Severity Assignment

The **Configure > Ports > Change Alarm Severity Assignment** menu option opens the Alarm Severity Assignment window shown in Figure 81 below. This window supports modifying the severity used when reporting minimum threshold power, maximum threshold power, and connection fault alarms for ports. Only ports for which the user has Modify or higher port privileges are shown. The port privilege of Modify is required to change any of the alarm severities for a port.

NOTE:	The Configure Port context menu described in Chapter 3 may also be used to reassign the alarm severity for a port. This method is accessed directly from the I/O Matrix and is convenient when acting on one or a few ports.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 81 Alarm Severity Assignment Window



Referencing Figure 81, the Alarm Severity Assignment window is composed of three sections:

- At the upper left port of the window, the Select Alarm Type section shows the three alarm types of which the user can change the severity on a per-port basis. The first two alarm types, Min Power Alarm (STMIN) and Max Power Alarm (STMAX), apply to both input and output ports. The last alarm type, Connection Alarm (CSFLT), applies only to output ports. The user selects (left-clicks) on the alarm type to start the process of changing the severity used when reporting this alarm for a port or group of ports.
- After the selection is made, the data in the upper-right section, Current Severity Assignment, is filled in showing the five possible severity levels and the ports assigned to each level. This area is initially blank. In Figure 81 above, the Min Power Alarm (STMIN) has been selected (note the blue background).
- The lower section of the window is used to change port alarm severity assignments for the alarm type selected in the Alarm Severity Assignment section. The following three fields are provided:
    - **Severity Level** - Pull-down menu for selecting the severity to assign.
    - **Assigned Input Ports** - Text box used to enter the input port numbers to assign to the selected severity.
    - **Assigned Output Ports** - Text box used to enter the output port numbers to assign to the selected severity.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTES: Tool tips are provided when the mouse is placed over either field in the lower section. The tool tips convey the following information for data entry:

Severity:

- Select the desired severity from the pull-down menu.

Entering port numbers in the **Input Ports** or **Output Ports** text boxes:

- Use long port numbers (e.g., 10xxx for input, 20xxx for output)
- Use a hyphen between port numbers to specify a range of ports
- Use a comma as a separator between port numbers or port ranges.

Example **Input Ports** entry:

- 10001,10010,10020-10030,10040-10050,10060

Two buttons are provided at the bottom left of the window: **Apply Changes** and **Close**. The **Apply Changes** button will be inactive until the user starts the assignment process in the lower section by selecting a alarm severity then entering input port numbers and/or output port numbers

The **Close** button will close the window.

To change the alarm severity assignment for a port, perform the following steps:

1. Open the Alarm Severity Assignment window (**Configure > Ports > Change Alarm Severity Assignment**)

2. In the Alarm Severity Assignment section, select (left-click) on the alarm type (**Min Power Alarm**, **Max Power Alarm**, or **Connection Alarm**) for which severity assignment changes are required. After a moment, the current port severity assignments will display in the Current Severity Assignment section to the right. Additionally, the title bar for the lower section will change to:

   Change Severity Assignment for: <selected alarm type>

3. In the lower section of the window, select the desired severity to assign from the **Severity** pull-down menu.

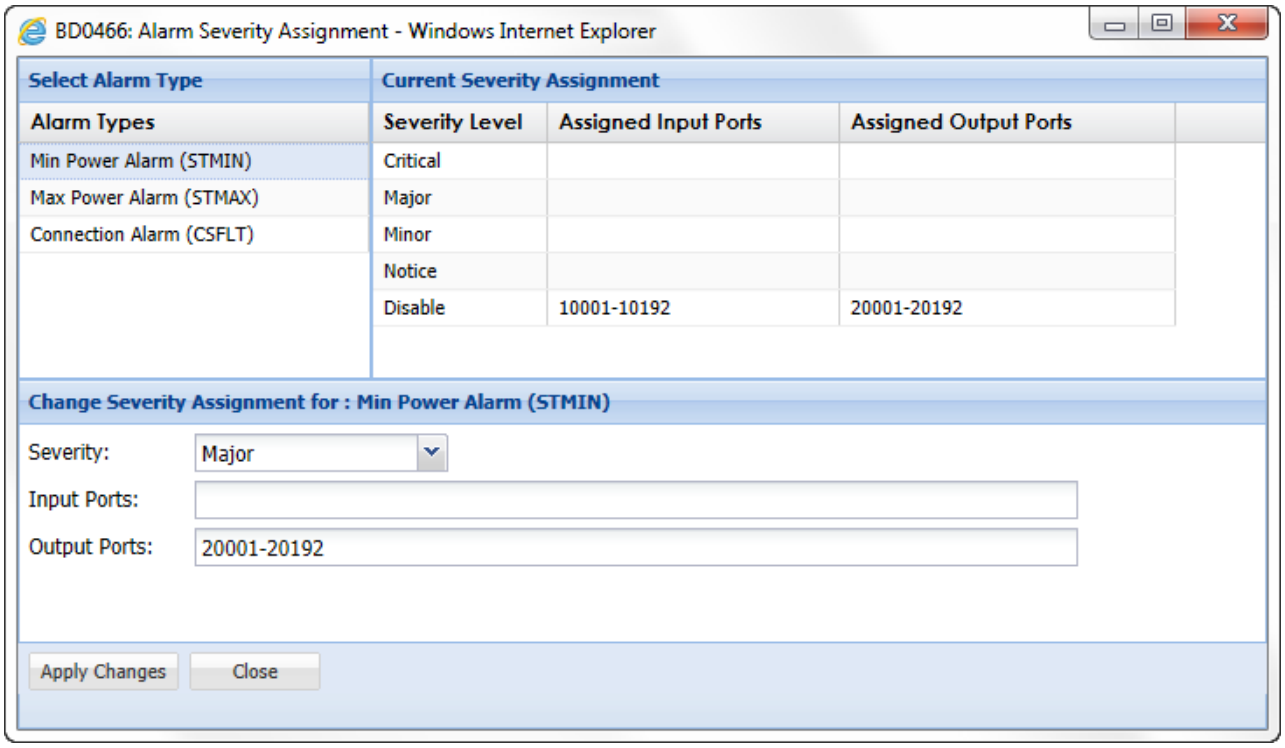
4. In the **Input Ports** text box, enter the input port number, port numbers, and/or port number range for assignment to this signal threshold. (This step is optional: This field can be left empty if assigning only output ports. Also, this field is not shown when the **Alarm Type** selected is Connection Alarm (CSFLT).)

5. In the **Output Ports** text box, enter the output port number, port numbers, and/or port number range for assignment to this threshold. (This step is optional: This field can be left empty if assigning only input ports.)

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Once port numbers are entered, the **Apply Changes** button will activate. Figure 82 below depicts the Alarm Severity Assignment window after selecting an alarm type and specifying ports requiring a severity change.

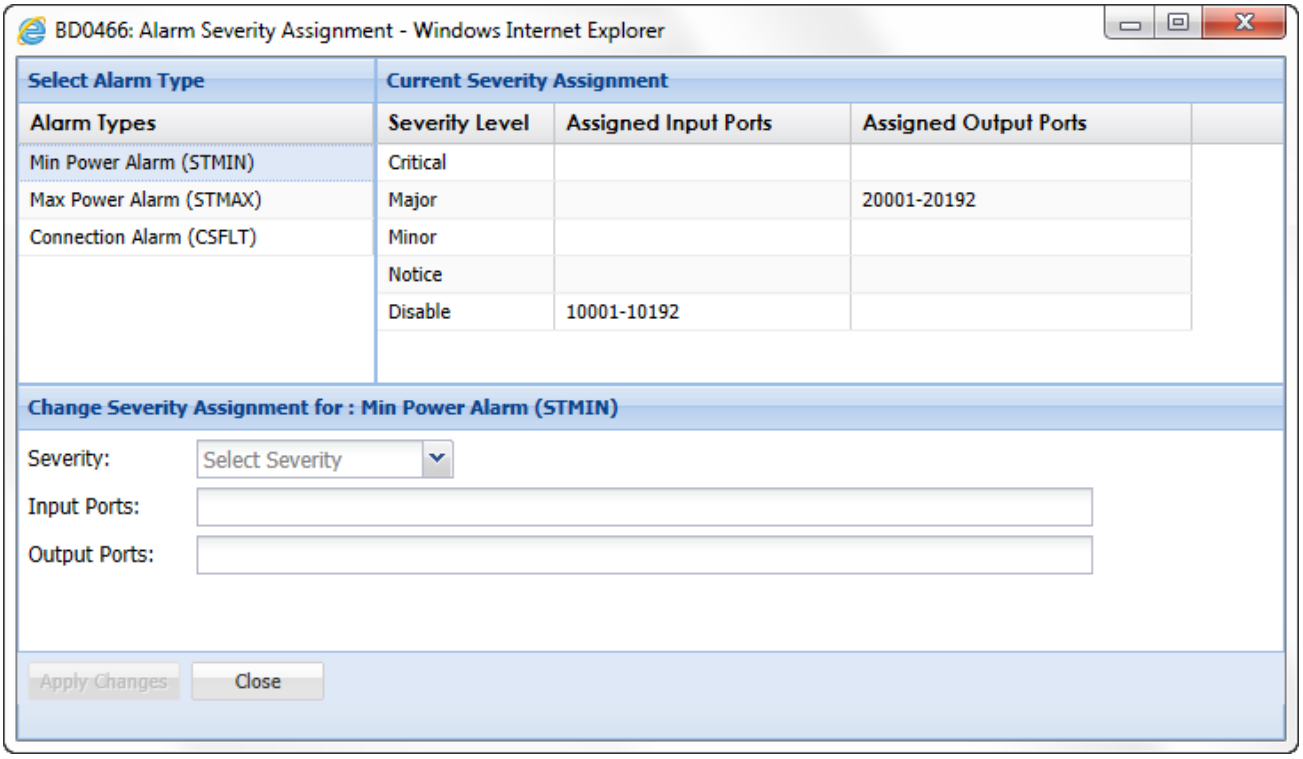
Figure 82 Alarm Severity Assignment Window (After Specifying Port Changes)



6. Click the **Apply Changes** button to change the alarm severity assignment for the entered ports. A status message will appear below the **Apply Changes** button indicating success or failure. After a moment, the window will refresh. The upper section will display the new alarm severity assignments for this alarm type as shown in Figure 83 below (if successful). All status messages (cause and result) are defined at the end of this instruction.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 83 Alarm Severity Assignment Window (After Applying Changes)



7. Once finished with alarm severity assignment, click the **Close** button to exit the window. Otherwise, continue with the next alarm type for which port severity assignments are desired

The area below the **Apply Changes** button is used to post status messages reporting success or failure of the alarm severity assignment. These status messages automatically clear after a few seconds.

The possible status messages shown after applying changes are described below. For errors, selections in the upper sections of the window will remain unchanged. The lower section is cleared and the window is ready to accept corrected data.

Status Messages:

- “Success: All updates completed”
  This message indicates that the ports and/or port ranges entered were composed of valid port numbers.
- “Success: All updates completed for valid port numbers”
  This message indicates that one or both port lists contained invalid port numbers (numbers not represented in the upper section). In this case, the requested change was made for the

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

valid port numbers and the invalid numbers were ignored. The upper section reflects the new configuration.

- “Error: Invalid Port Number or Invalid Port Range”
  This message indicates that all the port numbers entered in both port lists are resolved as invalid. For a range, this may occur if only the starting number of the range is invalid. If only some port numbers are invalid, then the status would be “Success: All updates completed for valid port numbers”
- “Error: Missing Port Group and/or Ports”
  This message indicates one of the following:
  - Input or output ports were entered (activates **Apply Changes** button) and then the **Apply Changes** button was used without selecting an alarm severity.
  - The **Severity** value was selected then either input or output ports were entered. Then, the port fields were erased (now blank) and the **Apply Changes** button was used.

Import/Export Group Assignment

Ports can be assigned to existing port groups by importing a mapping file (.csv file) in the same fashion that port configuration is imported/exported (see “Import/Export Port Configuration” on page 113).

Only users with system administrative privileges (system privilege = Manage, port privilege = Manage for all ports in system) are permitted to import/export group assignment files. This menu item is displayed only to users with system administrative privileges.

Group Assignment File Guidelines

A port-to-group file may be created by exporting the existing mapping from the system, or the file may be created from scratch using a text editor or spreadsheet program.

When exported, all ports with their current port group assignment are placed in the file.

The rules for Port-to-Group file creation and editing are as follows:

- The file must be saved as a .csv or .txt file.
- Comments about the intended content/usage may be included at the top of the file. Comment lines must start with the "#" character.
- After the comment lines, each port to port group assignment must be listed on separate lines using the following convention:

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

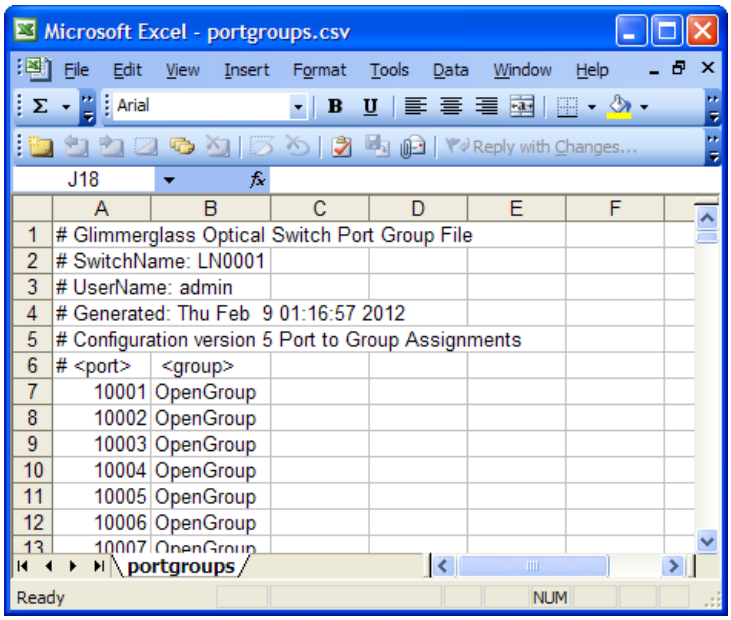
<port number>,<group>

The rules for editing port numbers and groups are as follows:

- The port number must be the 5 digit number for the port (e.g., 10001, 20001).
- The port group name must be the name of an existing port group in the system.
  - The name entry is case-insensitive.
  - If left blank, the import operation will assign the port to the default group (OpenGroup).
  - If the group name includes white space, enter the group name inside double quotes.

For creating files using text editors, refer to the “Import/Export Port Configuration” on page 113. Figure 84 below shows an excerpt of a file exported then opened using Excel. This figure depicts the required format.

Figure 84 Example of Port Group Excel file



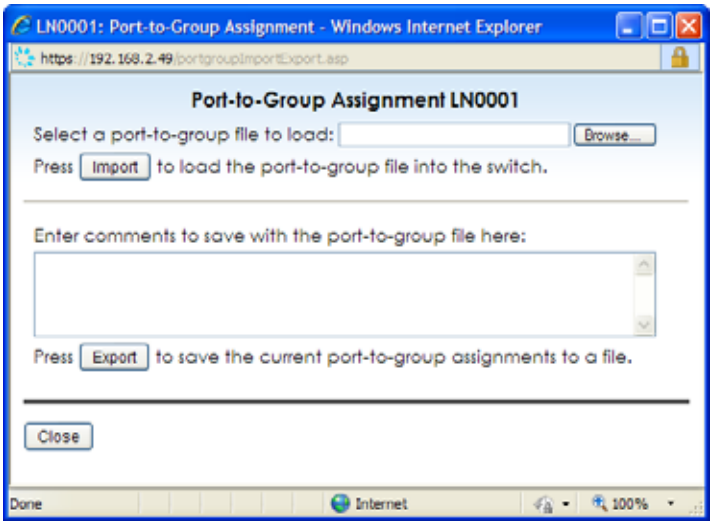
Importing a Port-to-Group File

To import a port-to-group file:

1. Select the **Configure > Ports > Import/Export Group Assignment** menu option to open the Port-to-Group Assignment window (Figure 85).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 85 Port-to-Group Assignment Window



2. Click the **Browse…** button to open the file upload window for your browser.

3. In the file upload window, navigate to the location of the Port-to-Group file to be imported.

4. Select the file and click the **Open** button. The file upload window will close and the path to the file will be displayed in the text field to the left of the **Browse** button.

5. Click the **Import** button to load the Port-to-Group mappings from the file to the system.

6. A pop-up window will appear reporting the success/failure of the import:
   - If successful, click the **OK** button.
   - If the import fails, note the reported error then click the **OK** button. Correct the data in the file and attempt the import again.

7. To view group assignment changes on the Connection screen, click the browser refresh to repaint the screen. If the changes are final, then continue to step 8. If more changes are required, then modify the file and re-import.

8. (Recommended) Select the **System > Session Administration** menu option to open the Session Administration window.
   - For all existing ClickFlow sessions, click the **Select Session** box,
   - Click the **Logoff Selected Sessions** box to force logoff all ClickFlow users.
   - Click the **Close** button to exit the window. Upon re-login, all ClickFlow users will see the changed settings that apply to him or her.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

If the csv file contains incorrect data, the entire import will fail (no partial completion). Possible sources for data entry errors are as follows:

- The file structure is incorrect
- An invalid port number is entered
- A non-existent port group name is entered
- A port number is repeated in the file

NOTES:
- To observe the new port-to-group assignments, the user must refresh the browser display or log out and then log back in.
- The new port-to-group assignments are not reflected automatically in existing sessions for other logged-in users. Other users must either refresh or log out and log back in. System administrators may force a logoff of all existing sessions using the **System > Session Administration** window. The logged-off users will see the new I/O Matrix layout once the user has logged back in.
- Though the I/O Matrix display is not updated, all changes are in effect. The system will not allow invalid connections to be made by users. Users will still be able to disconnect connections where they have the required privileges.

Exporting a Port-to-Group File

To export a port-to-group file:

1. Select the **Configure > Ports > Import/Export Group Assignment** menu option to open the Port-to-Group Assignment window (Figure 85 on page 142).

2. Enter any comments to be saved in the file with the port-to-group assignments. User entered comments are inserted after the default file header information.

3. Click the **Export** button to view the (web browser dependent) File Download window.

4. From the file download window:
   - Click the **Open** button to view the file before saving.
   - Click the **Save** button to select a name and a location in which to save the file.

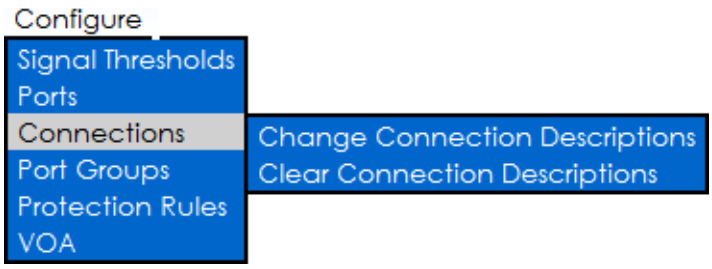
Connections

The **Configure > Connections** sub-menu (Figure 86) allows the user to change or clear connection descriptions. Connection descriptions are displayed in the Port Information Box and the Connection

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Report. Connection descriptions are saved in the system, but are removed when the ports forming the connection are disconnected. A connection description may be from 1 to 32 characters long. There is no requirement for connection descriptions to be unique.

Figure 86 ***Configure > Connections*** *Menu Options*



The following sections outline the procedures and guidelines associated with the **Connections** sub-menu:

- ”Change Connection Descriptions” on page 144
- ”Clear Connection Descriptions” on page 146

Change Connection Descriptions

The **Configure > Connections > Change Connection Descriptions** menu option allows a user to individually add, edit, or remove connection descriptions for connections for which they have the Modify or higher port-level privilege for both ports in the connection.

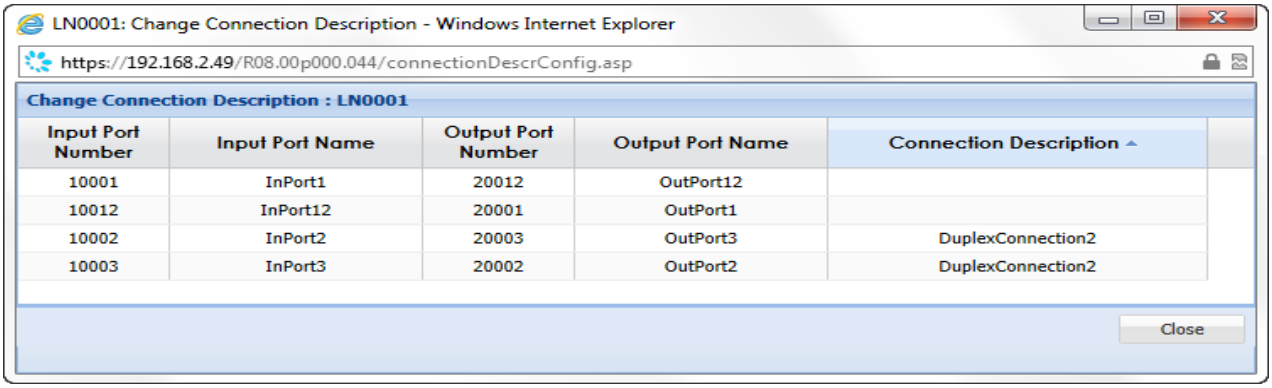
To add, edit, or remove a connection description, perform the following steps:

1. Select the **Configure > Connections > Change Connection Descriptions** menu option from the Connection screen.

2. The Connection Descriptions window (Figure 87) will appear. This window has the following features:
   - From left to right, are the columns Input Port Number, Input Port Name, Output Port Number, Output Port Name, and Connection Description.
   - The port numbers and names allow identification of the connection to describe. Port names and descriptions cannot be modified here. Only the **Connection Description** field can be edited.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 87 Configure Connection Descriptions Window

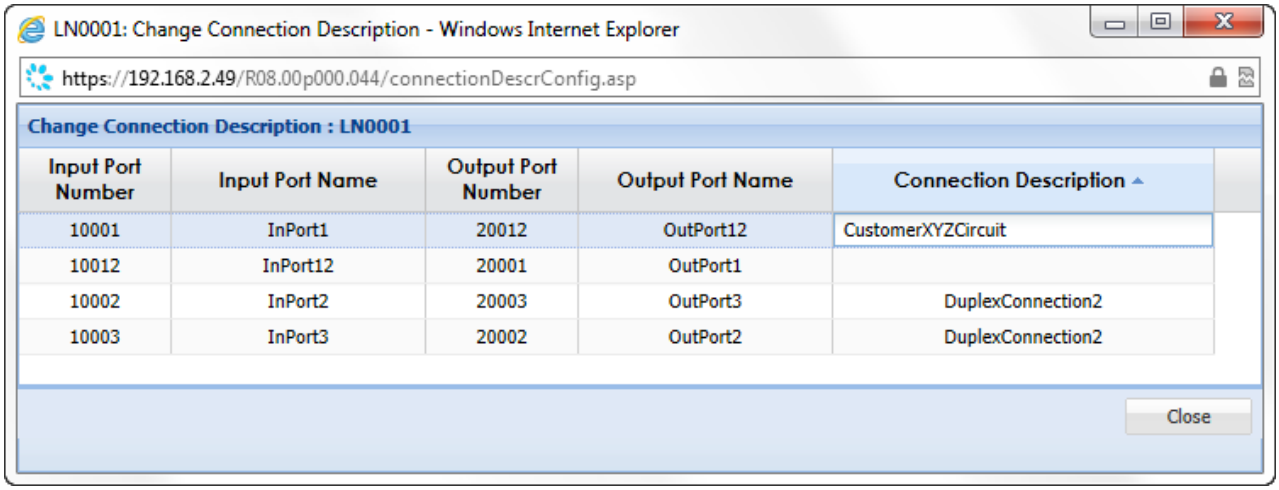


Input Port Number	Input Port Name	Output Port Number	Output Port Name	Connection Description
10001	InPort1	20012	OutPort12	
10012	InPort12	20001	OutPort1	
10002	InPort2	20003	OutPort3	DuplexConnection2
10003	InPort3	20002	OutPort2	DuplexConnection2

3. To assign/edit or remove a connection description for a particular connection, double-click in the appropriate **Connection Description** cell. The cell will change to edit mode as shown in Figure 88.

4. Enter, modify, or delete the connection description in the text box (see Figure 88 for an example).

Figure 88 Connection Description Entry (or Modification)



Input Port Number	Input Port Name	Output Port Number	Output Port Name	Connection Description
10001	InPort1	20012	OutPort12	CustomerXYZCircuit
10012	InPort12	20001	OutPort1	
10002	InPort2	20003	OutPort3	DuplexConnection2
10003	InPort3	20002	OutPort2	DuplexConnection2

5. After editing the text, either use the **Enter** key, the **Tab** key, or left-click outside the text field on the screen.

NOTES:
- Deleting a connection will also delete the connection description.
- Connection description editing in this window observes all previously stated requirements regarding user port-level privileges.
- After changes, the new connection descriptions are observable in the Connections Report and Port Information Box.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Clear Connection Descriptions

The **Configure > Connections > Clear Connection Descriptions** sub-menu provides options to clear all connection descriptions for which the user has the port-level privilege of Manage on both ports.

To clear all connection descriptions, perform the following step:

1. Select **Configure > Connections > Clear Connection Descriptions**. A pop-up confirmation box will appear requesting confirmation for the clear.

Port Groups

A system administrator can configuring port group in order to control connections among ports in the system as well as to express associations among ports in the I/O Matrix. The configuration of port groups is only possible if the Port Grouping feature is licensed. By default, all ports in the system belong to a system-defined group named "OpenGroup".

User-defined port groups have three attributes: the assigned port group name, an allow list, and a description. The operation of user-defined port groups is as follows:

- If the port group contains input and output ports, then connections between these inputs and outputs are always permitted.
- Connections to/from this group to ports in the OpenGroup are always permitted (if OpenGroup has ports assigned to it).
- Connections from this group to other groups are not permitted unless the names of other port groups are entered in the allow list for this group.

Up to 48 port groups may be configured in the system. The allow list for a group can support up to other port groups (meaning that any port group may allow connections from up to 8 other groups as well as the default OpenGroup).

If duplex connections are required between user-defined port groups, ensure that each group allows the other group to connect (each group appears in the allow list of the other group).

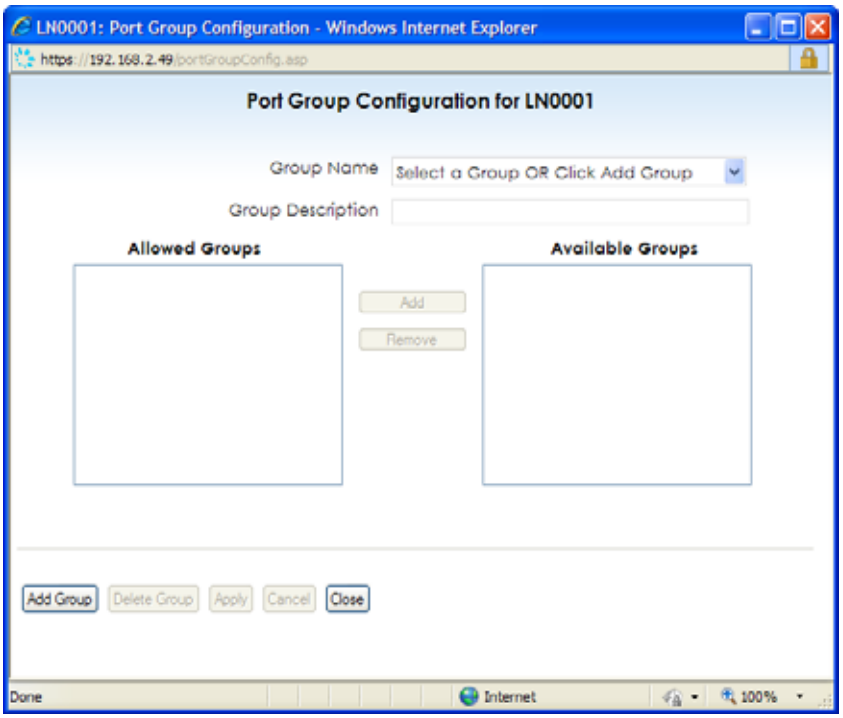
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTES: The system-defined group “OpenGroup” has the following characteristics:

- OpenGroup cannot be deleted.
- For systems without the Port Grouping license, all ports are assigned to OpenGroup.
- Input ports in OpenGroup are allowed to connect to output ports in all user-defined groups.
- Output ports in OpenGroup may be connected to/from any user-defined group.
- When Port Grouping is licensed, all ports may be assigned out of Open-Group among user-defined groups if the operation of the two previous bullets is not desired.

Figure 89 shows the Port Group configuration window. This window may be accessed only by a user with system administrative privileges (system privilege = Manage, port privilege = Manage for all ports in the system).

Figure 89 Port Group Configuration Window (default display when opened)



Adding a Port Group

Port groups must be created before they can be assigned in the allow list for another group. To create a port group:

1. Open the Port Groups window by selecting **Configure > Port Groups**.
   In the Port Groups window, the Group Name pull-down field indicates "Select a Group or Click Add Button".

2. Click the **Add Group** button.
   The cursor will be placed in the **Group Name** field and configuration help information will be displayed in the area below the Port Groups window boxes.

3. Enter the name for this port group in the **Group Name** field.

4. Optionally, enter a brief description for this port group in the **Group Description** field.

5. Optionally, configure the allow list for the group (existing port groups whose input ports are allowed to connect to output ports in this group).
   - Select the names of up to 8 existing port groups from the **Available Groups** list. (The **Add** button will become active when a group name is selected.)
   - Click the **Add** button to move the selected groups to the **Allowed Groups** list box. If a group is mistakenly added to the **Allowed Groups** list, select the port group name and click the **Remove** button to move it back to the **Available Groups** list.

6. Click the **Apply** button to complete the process. A success or failure message for the operation will be posted in the message area below the **Allowed Groups**/**Available Groups** boxes.

7. Click the **Close** button to exit the window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTES: The **Cancel** button may be used to abort the add and return the window to default display.

After the group is added, ports may be assigned to the group by one of the following methods:

- Using the Port Configuration window (see “Change Port Configuration” on page 119)
- Importing a Port-to-Group Assignment file (see “Import/Export Group Assignment” on page 140)
- Using the Configure Port Box Context Menu (see “Configure” on page 45)

The port group will not appear in the I/O Matrix until ports are assigned.

- Groups are displayed only to users with permissions to view at least one port in the group. The Port Group I/O Matrix will display only the ports the user is allowed to view.

Editing a Port Group

Port group names cannot be modified. Only the allow list and description attributes of a port group may be modified. If the requirement is to change the name of an existing group with assigned ports, then add a new group and reassign the ports. Afterwards, delete the old group name if desired. If a port group is deleted, the ports assigned are moved to OpenGroup by default. The above avoids having the ports generally available during this change.

1. Open the Port Groups window by selecting **Configure > Port Groups**.
   In the Port Groups window, the **Group Name** pull-down field indicates "Select a Group or Click Add Button".

2. Click the **Group Name** pull-down menu and select the group to be modified.
   The selected name will appear in the **Group Name** field and configuration help information will be displayed in the area below the **Allowed Groups**/**Available Groups** boxes.

3. Select and edit the **Group Description** field if required.

4. To add groups to the **Allowed Groups** list, select the desired group(s) from the **Available Groups** list box and then click the **Apply** button.

5. To remove groups from the **Allowed Groups** list, select the desired group(s) from this list and then click the **Apply** button.

6. After the **Apply** button is clicked, a success/failure message will be posted in the message area below the Allow/Available list boxes.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

7. Click the **Close** button to exit the window.

NOTES:
- The **Cancel** button may be used to abort the edits and return the window to default display.
- Existing connections which violate the new rules are not automatically disconnected. There is no impact on existing connections when group assignments are changed.
- Refresh the browser after changing allow lists to see the changes reflected when mousing over the port group name on the Connection Screen.

Deleting Port Groups

Deleting a port group will result in all ports in that group being assigned to the system default port group OpenGroup. To avoid this, reassign all ports to another group prior to deleting the group.

1. Open the Port Groups window by selecting **Configure > Port Groups**.
   The Group Name pull-down field will display "Select a Group OR Click Add Button".

2. Click the **Group Name** pull-down and select the group to be deleted from the pull-down list.

3. Click the **Delete Group** button.
   The message "Press Apply to confirm deletion of <groupname>" will appear as a confirmation request in the area below the **Allowed Groups**/**Available Groups** boxes.

4. Click the **Apply** button to complete deleting the group. A confirmation message will appear in the message area.

5. Click the **Close** button to exit the window.

NOTES:
- The **Cancel** button may be used to abort the delete and return the window to default display.
- Existing connections which violate the new rules are not automatically disconnected. There is no impact on existing connections when group assignments are changed.
- Refresh the browser after changing allow lists to see the changes reflected when mousing over the port group name on the Connection Screen.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Protection Rules

Protection is an optional, licensed feature that allows the user to assign Working and Protect relationships between input ports on the system. This enables automatic failover protection switching at the physical layer.

If Protection is enabled on the system, a protection rule can be established between any two input ports. One of the ports is designated the “Working” input and the other is designated the “Protect” input. Traffic is routed through the Working port unless the protection rule is invoked (triggered). Once triggered, the following will occur:

- For Simplex protection, a new connection is made between the Protect port and the same output port previously connected to the Working port.
- For Duplex protection, a new Duplex Connection is made between the Protect port and its associated output port and the input/output port pair previously connected to the Working port (and its associated output port).

NOTES: A **Duplex Connection** defines a specific connection involving 4 ports, two input ports and two output ports. By definition, the input of one port is connected to the output of the second port and vice versa.

A **Duplex Protection Rule**, by definition, is between two input ports with the purpose of protecting one side of a Duplex Connection. A Duplex Connection, therefore, can be protected on one side only or on both sides.

See ”Protection Types: Simplex and Duplex” on page 153 for more information on Duplex and Simplex protection types.

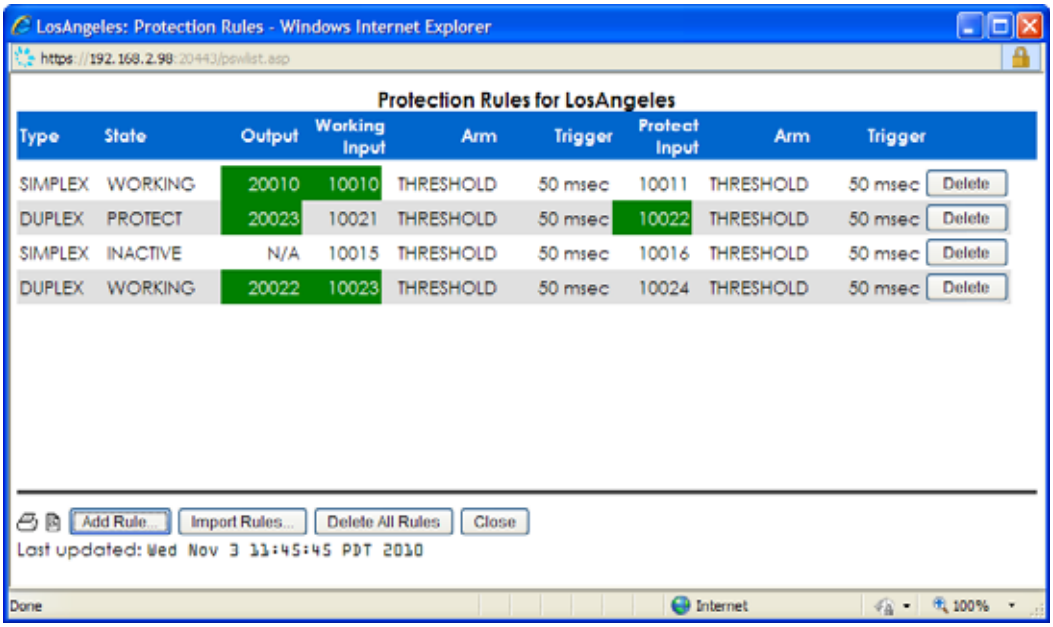
The protection rule has additional configuration parameters for controlling how and when a protection switch occurs. The rule is divided into a Working configuration and a Protect configuration. The Working configuration controls how and when a protection switch from the Working input to the Protect input can occur. The Protect configuration provides the same functionality in reverse. Normally, the Working and Protect configurations are the same. This type of rule is called a symmetric rule. For systems without Input Detection, however, asymmetric configurations may be required, depending on the desired recovery behavior.

Protection rules are triggered based upon a qualification time for loss of valid light. Loss of valid light is determined by the signal threshold for the connection (Minimum Optical Power). The qualification time is determined by the Trigger time configured for the rule. Finally, in order to trigger, a protection rule must first be “Armed”. See ”Adding a Protection Rule” on page 157 for information on creating protection rules.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The **Configure > Protection Rules** menu option displays the Protection Rules window shown in Figure 90. The Protection Rules window displays the status of each input port pair that has been assigned Working/Protect protection rules.

Figure 90 Protection Rules Screen



The Protection Rules window contains the following elements that are described in the specified sections of this chapter:

Element	Description
Type	Indicates whether the protection rule is Simplex or Duplex. See ”Protection Types: Simplex and Duplex” on page 153 for a description of these protection types.
State	Indicates current status of the protection rule. See ”Protection Rule State” on page 154 for a description of possible values and their meanings.
Output	The number of the output port of the connection.
Working Input	Indicates the number of the Working input port for the protection rule.
Arm	Indicates whether the working port arming is time-based or threshold-based. See ”Arming Modes” on page 155 for a description of the arming values.
Trigger	Indicates the working port triggering condition. See “Triggering Conditions” on page 156.
Protect Input	Indicates the number of the Protect input port for the protection rule.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Arm	Indicates whether the protect port arming is time-based or threshold-based. See ”Arming Modes” on page 155 for a description of the arming values.
Trigger	Indicates the protect port triggering condition. See “Triggering Conditions” on page 156.
Buttons	
Delete	Deletes the adjacent protection rule (see ”Deleting a Protection Rule” on page 159).
Add Rule...	Opens the Add Protection Rule window (see ”Adding a Protection Rule” on page 157).
Import Rules...	Opens the Import Protection Rules window (see ”Importing Protection Rules” on page 160).
Delete All Rules	Deletes all protection rules on the system (see ”Deleting All Protection Rules” on page 160).
Close	Closes the Protection Rules window.

Protection Types: Simplex and Duplex

A Simplex protection rule establishes an association between two input ports and a single output port. If a protection rule is triggered on the Working input port, then the system will switch to the Protect input port, still using the same output port. So the protection association has a single output port, regardless of whether the Protect or Working input port is in use.

A Duplex protection rule establishes and provides a second input/output port pair to protect one side of a duplex connection. Using letters instead of numbers, a duplex connection requires Input Port A to be connected to Output Port B and Input Port B to be connected to Output Port A. With Duplex protection, a third Input and Output port pair is used. Again, using letters, Input Port C can be placed in a Duplex protection rule with Input Port A. Since a duplex connection requires and input and an output port, Output Port C is also reserved by the rule. This would result in Input Port A being considered the “Working” input and Input Port C being considered the “Protect” input. If this Duplex protection rule is triggered, the resulting NEW duplex connection would be between Input Port C and Output Port B as well as Input Port B and Output Port C.

Note that in the above example, the other Input Port of the original duplex connection (Input Port B) was not protected. This is an instance of one side of a duplex connection being protected. This configuration requires six total ports (four for the original duplex connection and two additional ports for the Duplex protection rule).

To protect both sides (both the original duplex connection inputs) of a duplex connection, a second Duplex protection rule would be required. Using the above example, Input Port B would become a

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

"Working" input and an Input Port D would be assigned as the "Protect" port. This requires a total of eight ports (four for the original duplex connection and four additional for the two Duplex protection rules).

The protection type of a protection rule indicates whether the protection rule is Simplex or Duplex. The table below describes these two types of protection.

Type	Description
SIMPLEX	Protects Simplex connections by allowing a Working connection through the system to automatically switch to the Protect connection (and vice versa) in the presence of a triggering event (qualified loss of light).
DUPLEX	Protects one side of a Duplex Connection by allowing a Working Duplex connection through the system to automatically switch to a Protect Duplex connection (and vice versa) in the presence of a triggering event (qualified loss of light).

Protection Rule State

The protection state of a protection rule indicates the current status of the connection. There are four possible states for each pair of protected inputs

State	Description
INACTIVE	Neither input of the port pair is connected to an output, or no protection rule is provisioned.
ACTIVATING	A connection exists from one of the rule's inputs to an output port, and the arming condition has not been satisfied yet. The rule is monitoring for the arming condition and will transition to the WORKING or PROTECT (active) state when met.
WORKING or PROTECT (active)	A connection exists from one of the rule's inputs to an output port, and the arming condition has been satisfied. The rule is monitoring for the trigger condition, and causes a protection switch when met.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

State	Description
FAILED	A connection exists from one of the rule's inputs to an output port, but neither input has a valid signal. NOTE: The Failed state will only occur when there is no valid signal power on either the Working or Protect input ports. When equipped with Input Detection, the system will check for valid input power prior to executing a failover switch. If there is no valid input power on the Protect input port, then the system reports a FAILED condition and does not execute the switch.

Arming Modes

The arming mode indicates whether the protection rule mode is set to **THRESHOLD** or to **TIMED**. These modes are described in the following table:

Condition	Description
THRESHOLD	Threshold-based arming ensures the validity of a connection before arming a protection rule. The Threshold Arming Mode requires that: • The active connection has successfully reached the STEADY connection state. • The input power also must be greater than the signal threshold minimum expected power. NOTE: Only use the Threshold Arming Mode on systems equipped with Input Detection. For systems without Input Detection, use the Timed Arming Mode.
TIMED	Time-based arming indicates that the connection will be armed a certain period of time (specified in milliseconds) after the connection is first established. This condition requires that: • The active connection has successfully reached the STEADY connection state. • The specified arming delay time elapses from when the connection was first established. • If the system is equipped with Input Detection, the input power also must be greater than the signal threshold minimum expected power. NOTE: This is the recommended arming condition for systems that are NOT configured with Input Detection.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Triggering Conditions

Once an active connection has been armed successfully, an automatic failover switch event is triggered, as long as both of the following trigger conditions are met:

Condition 1: Power Falls Below the Minimum Optical Power Threshold (STMIN)

To satisfy this trigger condition, the optical power of the connection output must fall below the threshold determined by the signal threshold minimum expected power and hysteresis values configured for the ports involved in the Active connection.

Example:
If the Active input is configured with the default signal threshold values (i.e., Expected Power Min =
-20dBm, Hysteresis = +/- 1dB), then the relevant trigger threshold is -21dBm (-20 - 1).

Condition 2: Trigger Delay

This condition delays the triggering of a protection switch event for a specified period of time (specified in milliseconds) after Condition 1 has been met. To satisfy Condition 2, the connection output power must be below the Condition 1 threshold at the end of the specified delay period.

NOTE:	If the output power rises above the threshold determined by the expected power minimum value and the hysteresis value, then the trigger is reset and no protection switch takes place.

Example:
If the active input port is configured with the default signal threshold values (Expected Power Min = -20dBm, Hysteresis = +/- 1dB) and the Trigger Delay is set to 200ms, then a protection switch will be triggered if the connection output power drops below -21dBm (-20 - 1) and is still below -19dBm (-20 + 1) 200 ms later. If the output power rises above -19dBm (-20 + 1) during the delay period, then the trigger is reset.

Since triggering always operates in Threshold mode, the **Trigger** field of the Protection Rules screen only displays the current **Trigger Delay** value configured for each input port.

Protection Rule Default Configuration Settings

All protection rules are configured initially with the following default settings:

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Protection Rule	Default Setting
TRIGGER Delay	50 ms
ARM Mode	THRESHOLD
SYMMETRIC	YES (same settings apply to both input ports)
Protection Type	SIMPLEX

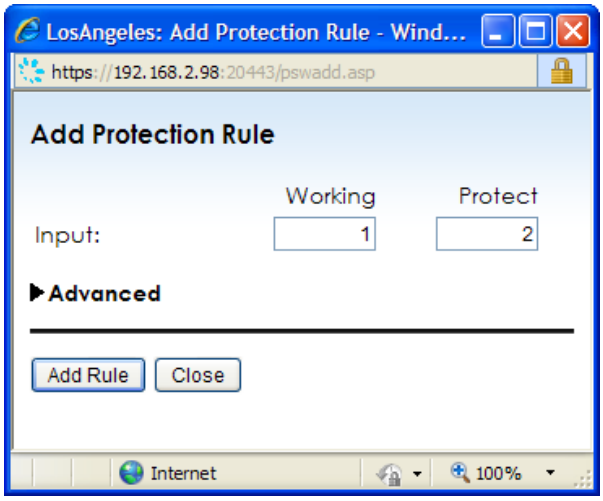
Adding a Protection Rule

Users with port-level privilege of Manage on both input ports (working and protect) can add a protection rule. To add a protection rule:

1. Select the **Configure > Protection Rules** menu option from the Connection screen to view the Protection Rules window (Figure 90).

2. Click the **Add Rule...** button to display the Add Protection Rule window (see Figure 91).

Figure 91 Add Protection Rule Window



3. In the Add Protection Rule window, enter the port numbers for the **Working** and **Protect** input ports. The 5-digit port number and numeric Port ID formats are acceptable. The alphanumeric Port ID for PMU and Switched VOA ports is not acceptable (use the 5-digit port number instead).

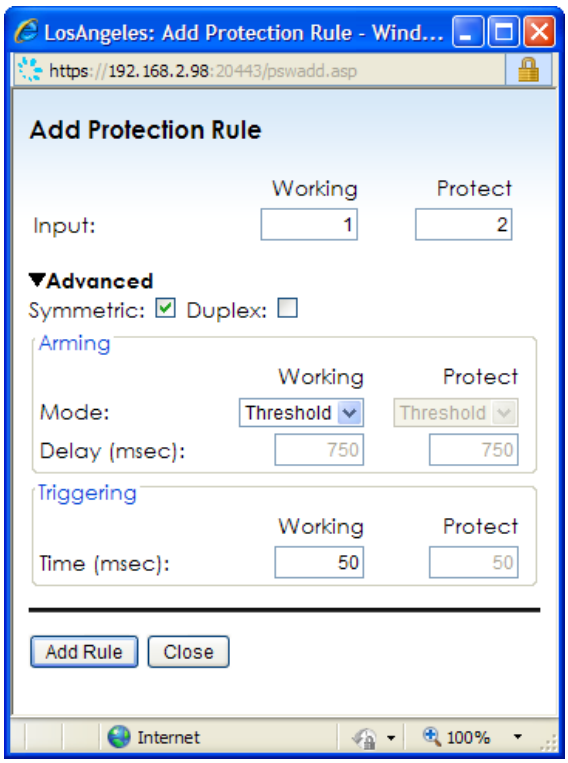
4. Once the Working and Protect port values are entered, do one of the following:
   - To accept the default rule settings for the protection rule, skip to step 11.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- To customize the protection rule settings, continue to step 5.

5. Click the **Advanced** arrow to display the advanced rule configuration options (see Figure 92).

Figure 92 Add Protection Rule Window (Advanced Configuration Options)



6. In the **Symmetric** box of the Advanced settings, do one of the following:
   - Leave the **Symmetric** box checked to apply the same arming and triggering settings to both the Working and Protect ports. When checked, the Protect port options will be grayed out.
   - Unchecked the box to select different settings for each input.

7. In the **Duplex** box of the Advanced settings, do one of the following:
   - Check the **Duplex** box to create a Duplex protection rule.
   - Leave the box unchecked to create a Simplex protection rule.

8. In the Arming area of the window, click on the **Mode** pull-down menu for the **Working** port and select whether the arming mode is to be **Threshold** or **Timed** (see ”Arming Modes” on page 155 for more information).
   If the **Symmetric** box was unchecked in step 6, select a **Mode** value for the **Protect** port as well.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

9. If the **Timed** arming mode was selected in step 8, enter a trigger delay value (in milliseconds) in the **Delay** text box. Enter “0” (zero) to specify no delay.
   If the **Symmetric** box was unchecked in step 6, enter a **Delay** value for the **Protect** port as well.

10. In the **Triggering** area of the window, enter a triggering time value (in milliseconds) in the **Time** text box.
    If the **Symmetric** box was unchecked in step 6, enter a **Time** value for the Protect port as well.

11. Click on the **Add Rule** button to apply the protection rule settings.

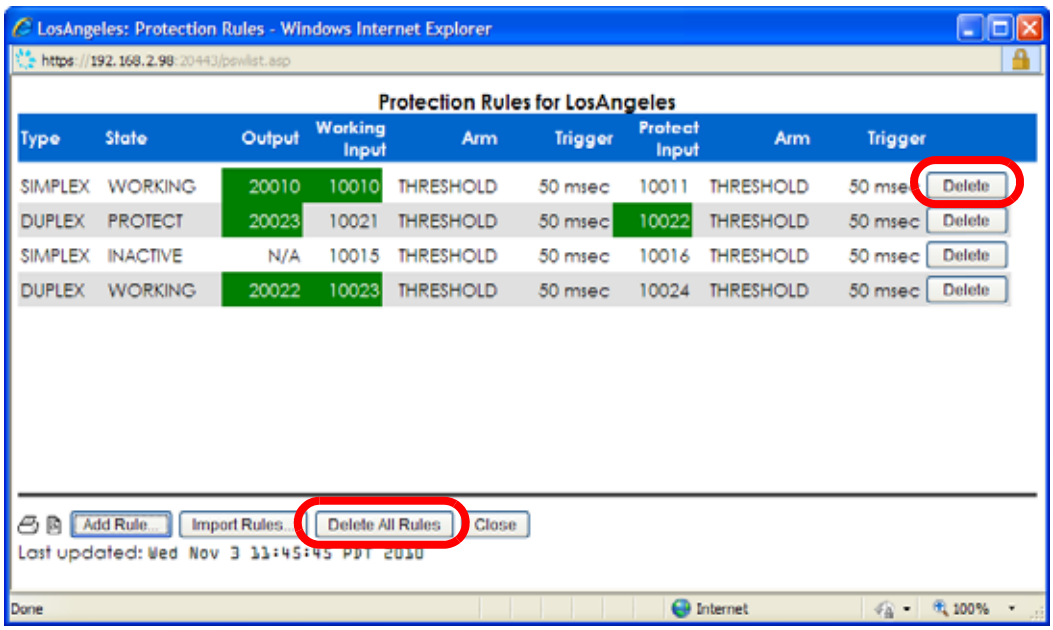
12. Click the **OK** button in confirmation dialog.

13. Click the **Close** button to close the Add Protection Rule window.

Deleting a Protection Rule

A user with port-level privilege of Manage on both input ports (working and protect) of a protection rule may delete the protection rule. The Protection Rules window contains a **Delete** button for each configured protection rule (see Figure 93).

Figure 93 Delete Protection Rule(s) Buttons



To delete a protection rule from a pair of input ports:

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

1. Select the **Configure > Protection Rules** menu option from the Connection screen to view the Protection Rules window (Figure 93).

2. Click the **Delete** button for the specific rule to be deleted.

3. Click the **OK** button in the confirmation box to delete the rule.

Deleting All Protection Rules

With a single command, the **Delete All Rules** button in the Protection Rules window removes all of the configured protection rules for which the user has port-level privilege of Manage on both input ports.

To delete all of the configured protection rules:

1. Select the **Configure > Protection Rules** menu option from the Connection screen to view the Protection Rules window (Figure 93).

2. Click the **Delete All Rules** button at the bottom of the Protection Rules window.

3. Click the **OK** button in the confirmation box to delete all of the configured rules.

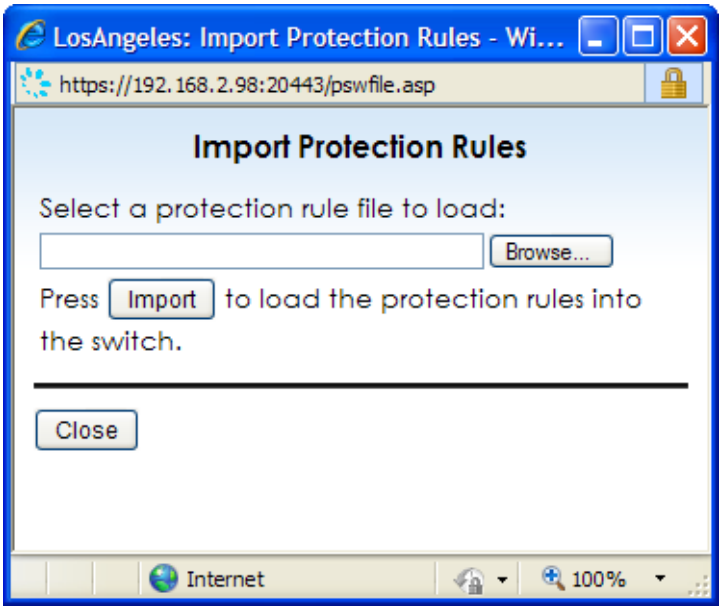
Importing Protection Rules

Multiple Protection Rules can be assigned by creating and importing a Protection Rule text file in any third-party text editor or spread sheet program (see Figure 95). Protection rules will be assigned/ changed only where the user has port-level privilege for both input ports.

The Protection Rules window contains a **Import Rules...** button that opens the Import Protection Rules window (see Figure 94).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 94 Import Protection Rules Window



Protection Rule File Format Guidelines

Before importing protection rules from a text file to the system, a protection rules file must be created using a third-party text editor (Notepad) or spreadsheet (Excel) application. In order to import the protection rules file to the system, the protection rules file must be formatted so that the ClickFlow GUI will interpret the file correctly. The protection rules file guidelines are as follows:

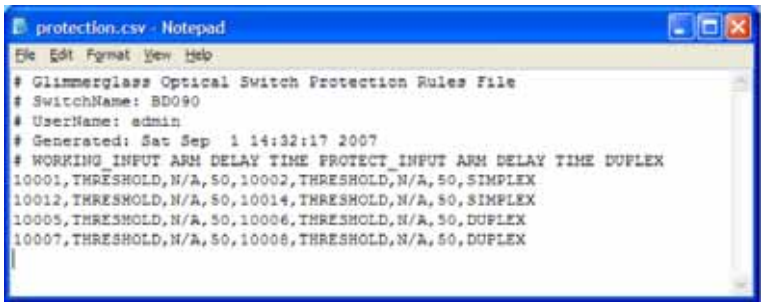
- A protection rules file must be saved as a text file using either .csv or .txt as the file extension.
- Any comments must be added to the beginning of the file and must be preceded by the "#" character.
- After the comment lines, each desired protection rule must be listed in a separate line using the following format:
  <work input>, <arm mode>, <arm delay>, <trigger delay>, <protect input>, <arm delay>, <trigger delay>, <protection type>
- The **work input** and **protect input** values must be in 5-digit port number format, where Input 1 = 10001.
- The **arm mode** value must be THRESHOLD or TIMED.
- The **arm delay** value must be **N/A** for threshold arming mode, or the desired numeric value (in milliseconds) for timed arming mode.
- The **trigger delay** value is the desired numeric value (in milliseconds).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- If the protect arm mode, arm delay and trigger delay parameters are omitted, then the working parameters will be applied to both the Working and Protect inputs. This is the same as selecting the Symmetric box shown in Figure 92 on page 158.
- The **protection type** value must be SIMPLEX or DUPLEX.

Figure 95 shows an example protection rules file created using the Notepad text editor application.

Figure 95 Sample Protection Rules File Created with Notepad Text Editor



To import protection rules from a file:

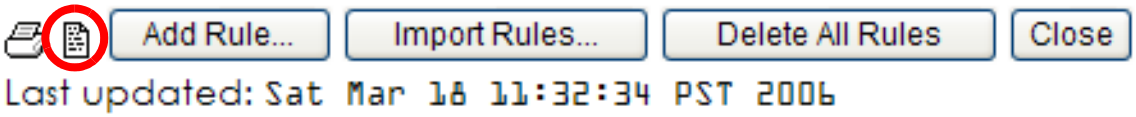
1. Select the **Configure > Protection Rules** menu option from the Connection screen to view the Protection Rules window (Figure 90).
2. Click the **Import Rules** button to display the Import Protection Rules window (Figure 94)
3. In the Import Protection Rules window, click the **Browse** button to display the Choose File window.
4. In the Choose File window, navigate to the protection rules file to be imported.
5. Select the protection rules file and click the **Open** button.
   The Browse window closes and the file path is listed in the Import Protection Rules window.
6. In the Import Protection Rules window, click the **Import** button to load the file.
7. Click the **OK** button in the dialog box to confirm that the file has been successfully imported

Exporting Protection Rules

The Protection Rules window contains a **File** icon (shown in Figure 96) that can be clicked to save the protection rules to a text file. This file can be viewed and edited in a third-party text editor.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 96 Export File Icon in the Protection Rules Window



To export the current protection rules to a text file:

1. Select the **Configure > Protection Rules** menu option from the Connection screen to view the Protection Rules window (Figure 90).

2. From the bottom left corner of the Protection Rules window, click on the **File** icon (Figure 96).
   This will open the (web browser dependent) File Download window.

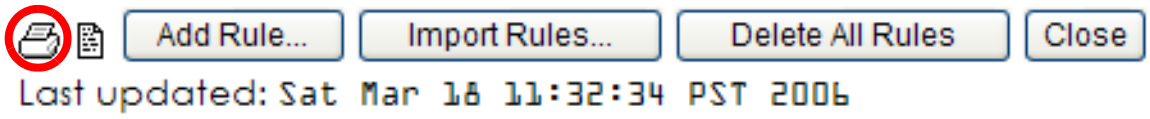
3. Click the **Save** button in the File Download dialog box.

4. Enter a file name and choose a destination in the Save As dialog box, then click **Save** to save the performance report as a file. The file will be saved as a text file (.csv format) and can be viewed with any third-party text editor (Notepad) or spreadsheet (Excel) application.

Printing Protection Rules

The Protection Rules window contains a **Print** icon (shown in Figure 97) that can be clicked to open a printer-friendly version of the protection rules used by the system.

Figure 97 Print Icon in the Protection Rules Window



To print the protection rules used by the system:

1. Select the **Reports > Protection Rules** menu option from the Connection screen to view the Protection Rules window (Figure 90).

2. From the bottom left corner of the Protection Rules window, click on the **Print** icon (Figure 97).
   This will open a new browser window that contains a printer-friendly version of the Protection Rules window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

3. From the browser window with the printer-friendly protection rules, select **File > Print ...** from the web browser menu bar.

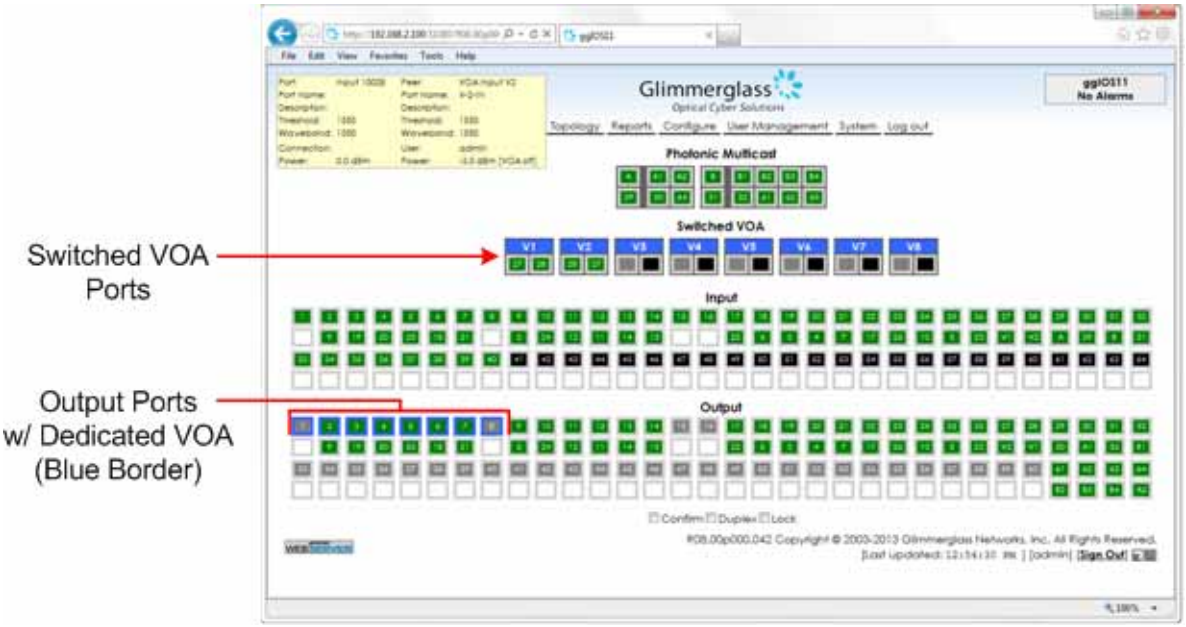
4. From the Print window, select a printer and click **Print**.

Variable Optical Attenuation (VOA)

Variable Optical Attenuation (VOA) is an optional hardware feature that allows a user to attenuate the output power levels for optical connections through the system (see ”Variable Optical Attenuation (VOA)” on page 24 for details about the VOA feature).

If the system is configured with Dedicated VOA, the ClickFlow GUI will use a blue border to distinguish the output ports that contain Dedicated VOA from the non-VOA output ports in the I/O Matrix of the Connection screen. For Switched VOA, the ClickFlow GUI displays each Switched VOA element in a standalone, two-port box above the I/O Matrix. Figure 98 shows how the ClickFlow GUI displays Switched VOA and Dedicated VOA.

Figure 98 VOA Displays in the ClickFlow GUI



Note that the VOA element settings are configured for each VOA port, and not for the connection. This means that a power setting is associated with the VOA port and is preserved for the VOA port regardless of which standard port is connected to the VOA port. The next section of this chapter provides information for configuring the settings of the VOA ports on the system.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Modes of Operation for VOA

VOA element settings are controlled by a user either through the TL1 interface (see the Glimmerglass *Transaction Language 1 Manual*), or through the ClickFlow GUI, as described in ”Variable Optical Attenuation (VOA)” on page 164 of this manual. The Glimmerglass system can attenuate optical power in two modes:

- Set Power mode—Sets the output power for the signal to a fixed optical power level value (in dBm). This output power level will be maintained by the system as long as the input signal optical power level is higher than the specified output power signal level by the inherent insertion loss of the connection (e.g. PWR_{in} - $IL_{connection}$ > PWR_{out}). (See Table 4 on page 165.) The Set Power mode is supported by both Dedicated VOA and Switched VOA implementations.
- Attenuate Power mode—Sets the loss value (in dB) through the element. The user-configured loss value setting will be applied to any connection made through this element. The overall loss of connection using the VOA element will be the sum of the inherent connection loss and the VOA loss value. The Attenuate Power mode is supported only on systems with the Switched VOA hardware implementation.

See ”Guidelines and Usage Considerations for VOA” on page 168 for information on implementing VOA on the Glimmerglass system.

Performance Specifications for VOA

Table 4 shows the typical and maximum VOA insertion loss values for Glimmerglass systems for each type of VOA when the VOA element is set to its minimum attenuation value (OFF).

NOTE: The insertion loss values in Table 4 apply for LC/UPC connectors at 25°C for systems with Input Detection.

Table 4 Insertion Loss at Minimum Attenuation VOA Setting

VOA Type	Typical (dB)	Max (dB)
Standard (no VOA)	2.2	3.7
Dedicated VOA	2.6	4.5
Switched VOA	4.8	8.2

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Table 5 contains the operational parameters specific to each VOA element.

Table 5 VOA Operational Parameters

Parameter	Value	Description
Response Time	<10ms	Time required for VOA configuration settings to take effect.
Resolution	0.1	Granularity for VOA dBm (Output-Power) or dB (Incremental Loss) settings.
Output Power Value	>= -39dBm	Lowest output power setting.

Configuring VOA Ports

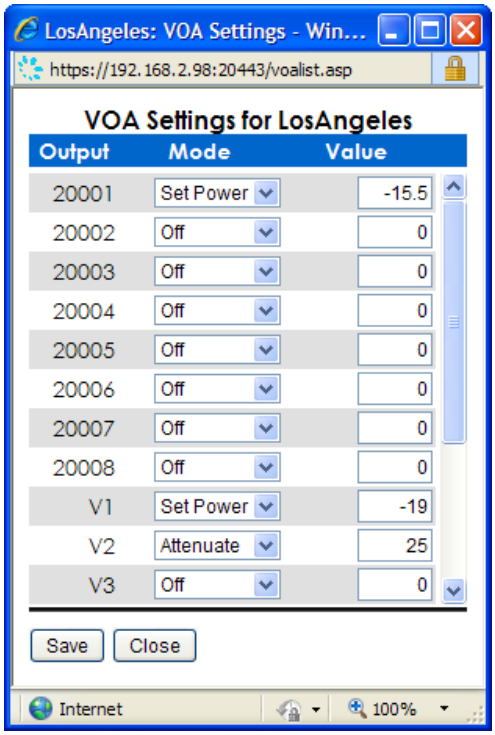
If the system is configured to support VOA functionality, then the **Configure > VOA** menu option will display the VOA Settings window (Figure 99). If the system is configured for Switched VOA, you can also access the VOA Settings window by clicking on the VOA device name (e.g., “V1”, “V2”, etc.) in the Switched VOA display above the I/O Matrix in the Connection screen.

The VOA Settings window lists all of the VOA ports on the system, which includes both the Switched VOA devices and the output ports that contain Dedicated VOA elements.

A user with port-level privilege of Modify may configure VOA settings.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 99 VOA Settings Window



The VOA Settings window contains the following elements:

Element	Description
Output	Depending on the VOA hardware implementation, displays one or both of the following: • For Dedicated VOA, displays the port number of the output ports that contain a Dedicated VOA element. (These output ports are displayed with a blue border in the I/O Matrix of the Connection screen.) • For Switched VOA, displays the name of the Switched VOA device (e.g., “V1”, “V2”, etc.).
Mode	Displays the operating mode of the VOA element: • Off—VOA Disabled (the VOA element is set to its minimum attenuation value) • Set Power—Specify the absolute output power level (in dBm) for a connection • Attenuate—Specify the insertion loss (in dB) for the VOA element. This loss will be added to the inherent loss of the connection. (This mode is supported for Switched VOA only.) See ”Modes of Operation for VOA” on page 165 for more information.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Value	Displays the target power value. The value displayed is a function of the mode: • For Set Power Mode, the value represents the desired output power setting (in dBm). • For Attenuate Mode, the value represents the insertion loss through the VOA (in dB).
Save	Saves the VOA settings to the permanent configuration file.
Close	Closes the VOA Settings window without saving any VOA configuration changes that were made in the window.

To enable and configure VOA on the system:

1. Select the **Configure > VOA** menu option from the Connection screen to view the VOA Settings window (Figure 99).
   The VOA Settings window opens and displays a list of all the Dedicated VOA output ports and Switched VOA elements.

2. Locate the VOA port or device to be configured.

3. To enable VOA for the port or device, click on the **Mode** pull-down list and select the desired mode of operation (see ”Modes of Operation for VOA” on page 165 for more information).

4. In the **Value** text box for the port, enter a value for the desired power value:
   - For Set Power Mode, the value represents the desired output power setting (in dBm).
   - For Attenuate Mode, the value represents the insertion loss through the VOA (in dB).

5. Follow step 2 through step 4 for each of the ports to be configured for VOA.

6. Click the **Save** button to save these configuration settings to the permanent configuration file.

7. Click the **Close** button to return to the Connection screen.

Guidelines and Usage Considerations for VOA

When configuring VOA on the system, note the following configuration guidelines and VOA behaviors:

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- The lowest output attenuation setting will be in the range specified for the corresponding system in Table 4 on page 165. The actual value is ascertained by measuring the connection loss with the VOA set to OFF.
- The VOA element cannot have negative loss. If the requested output power is greater than the input power minus the connection loss, the VOA element will be set to its minimum attenuation (OFF) setting.
- The VOA element setting is a property of the VOA output port, not the connection. A previously configured power setting is preserved when different input ports are connected to the VOA output port.
- The VOA responds to dynamic changes of the input power within 10ms to maintain the prescribed output-level dBm value (for Set Power mode).
- The user-configured VOA settings can be saved explicitly to the permanent configuration file from the VOA Settings window (see Figure 99 on page 167).
- VOA behavior after a power cycle:
    - If the VOA configuration settings for a VOA connection are not saved to the permanent configuration file, the configuration settings will be lost after a power cycle. If Connection Restoration is set to “Restore”, VOA connections restored after the power-cycle will NOT be attenuated.
    - If the VOA configuration settings for a VOA connection have been saved to the permanent configuration file, the VOA setting for the connection will be restored with the connection after a power cycle.

In additional to the above considerations, the following sections describe the special guidelines and usage considerations for the different VOA hardware configurations (Dedicated VOA and Switched VOA), and the special considerations for the Attenuate Power mode of operation:

- ”Guidelines and Usage Considerations for Dedicated VOA” on page 169
- ”Guidelines and Usage Considerations for Switched VOA” on page 170
- ”Guidelines for Attenuate Power Mode” on page 170

Guidelines and Usage Considerations for Dedicated VOA

For the Dedicated VOA implementation, note the following:

- When establishing a connection to a VOA output port, the VOA element is set to minimum attenuation until the connection reaches the "Steady" state and then the attenuation configured for the VOA element is applied. This means that receivers connected to the output port may receive the connected signal without attenuation for a period up to 10ms.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- If the VOA configuration settings for a VOA connection have been saved to the permanent configuration file, the connection will be automatically restored after a power cycle. However, the VOA connection will not be attenuated until the newly reestablished connection reaches the "Steady" state. The connected signal may not be attenuated for a period of up to 10ms.

Guidelines and Usage Considerations for Switched VOA

For the Switched VOA implementation, note the following:

- The VOA setting is a property of the VOA, not the connection. The previously configured VOA setting is preserved when different input ports are connected through the VOA element to an output port.

Guidelines for Attenuate Power Mode

In addition to the considerations for Switched VOA (see the previous section), note for the Attenuate Power mode of operation that the maximum incremental insertion loss setting resulting in a “Steady” connection is constrained by the Optical Power Minimum value configured for the Named signal threshold set on the user input port. The resulting output power level must be greater than or equal to the Optical Power Minimum setting.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

User Management

8

Overview

This chapter presents the background information necessary for managing user accounts on the system as well as presenting the **User Management** menu options for administering user accounts. With the exception of the option allowing users to change their own password, access to user administration options requires the user to have the system-level privilege of Manage.

The table below enumerates the topics covered in this chapter.

Menu Option	Description	Page
Default User Accounts	This section presents the default user accounts used by ClickFlow.	172
Privilege Levels	This section defines the system-level and port-level privileges and enumerates the privileges required for switch operations.	173
Virtual Private Switch (VPS)	This section describes the Virtual Private Switch (VPS) feature. This feature is only available when the VPS license is purchased.	177
Password and Account Policies	This section presents the password complexity/change policies and user account aging policy	178
User Management Menu Options	This section presents the User Management menu options and provides the information on using these options. These options are: • Set Password (allows users to change their own password) • Add User • Edit User • Delete User • Import Users • Export Users • Change Port Privilege Assignments	182

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Default User Accounts

All Glimmerglass systems have three default user accounts. Two of these, admin and madmin, are accounts with full system administrative privileges. The third account, snmpuser, is used by the system for tracking changes through the SNMP interface. The characteristics for each account are described below.

admin user account:

- Factory default password = password
- Factory default state = In Service
- System Privilege = manage
- Port Privilege = manage
- The admin account cannot be deleted, or set out-of-service.
- The system and port privileges for the admin account cannot be modified.

madmin user account:

- Factory default password = password
- Factory default state = Out-of-Service
- System Privilege = manage
- Port Privilege = manage
- The madmin account cannot be deleted
- The madmin account may be set out-of-service by the admin account.
- The system and port privileges for the madmin account cannot be modified.

snmpuser user account:

- The system will not allow login by the snmpuser
- This account is used for tracking internal operations on the SNMP interface
- This account cannot be deleted, modified or set out-of-service

With the exception of snmpuser, all user accounts may be used to log into either TL1 or ClickFlow; the user accounts are shared by both interfaces.

The madmin user account is used by the CyberSweep™ Path Manager server for administrative access and control of the system. When Path Manager is used to manage the system, Path Manager will manage password changes for this user as well as the admin user.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

For systems not managed from a Path Manager server, the madmin account may be left disabled to preclude any requirements for administering the account.

Privilege Levels

The switch user privilege mode supports two privilege categories, system and port. Each category supports four privilege levels: Manage, Modify, View, and None.

A user's access to an operation is therefore determined by either his assigned system-level privilege or port-level privilege.

The table below shows all ClickFlow operations (direct or via menu options) and specifies the minimum required system- or port-level privilege to make configuration changes if the item supports changes. These operations are grouped under the menu in which they appear or as Connection screen operations if they are not found in a menu. Note that users with View privileges can access many of the operations or windows for viewing only. If the operation or window does not support access by users with the View privilege (system- or port-level), the comments column will indicate this condition.

When either the system-level or port-level privilege has no bearing on the operation, the box for this privilege contains a hyphen (e.g., Not Applicable). A few operations require a combination of system-level and port-level privileges.

Operation Access	System Privilege	Port Privilege	Comments
Connection Screen Operations			
Alarm Panel	None	-	All users may view the alarm state.
Port Boxes	-	View	May view Port Box colors for port and connection.
Port Information Box	-	View	May view port configuration, connection configuration, port powers, and connection loss.
Port Box Context Menu	-	View	May view the Configure Port and Provision Connection windows.
Configure Port Window (name, description, signal threshold assignment)	-	Modify	May modify port names and description and assign signal thresholds (input port).
Configure Port Window (port group assignment)	Manage	Manage	May modify port group assignment when the user has Manage privileges for all ports.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Operation Access	System Privilege	Port Privilege	Comments
Provision Connection Window	-	Modify	Required on both ports to provision. View privilege can view existing connection.
Fiber Menu			
Connect	-	Modify	Required on both ports to connect.
Disconnect	-	Modify	Required only on one of ports to disconnect.
Connect All	Manage	Modify	Both system and port privileges required. Modify required on both ports.
Disconnect All	Manage	Modify	Both system and port privileges required. Required only on one of ports to disconnect.
Topology Menu			
Import	-	Modify	Will only make connections where privilege is met for both ports in connection. Will break connections where privilege is met on one of the ports in a connection.
Export	-	View	Will export connections where privilege is met on one of the ports in the connection.
Quick Load	-	Modify	Will only make connections where privilege is met for both ports in connection. Will break connections where privilege is met on one of the ports in a connection.
Reports Menu			
Performance Report	-	View	Data presented for all viewable ports.
Port Report	-	View	Data presented for all viewable ports.
Connections Report	-	View	Data presented for all viewable ports.
Port Groups	Manage	Manage	Not displayed in menu unless user has privilege.
System Information Report	View	-	Not displayed in menu unless user has privilege.
Port Color Legend	None	-	All users may view the Legend Report.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Operation Access	System Privilege	Port Privilege	Comments
Configure Menu			
Signal Threshold	Modify	-	Required for creating, editing, modifying Not displayed in menu unless user has privilege.
Port > Import Port Names/ Descriptions	-	Modify	Will modify the port names/descriptions for ports where user has privilege. All other ports in system will be unchanged.
Port > Export Port Names/ Descriptions	-	View	Ports where privilege is View and higher are exported.
Port > Change Port Configuration	-	Modify	Displays ports where the user's privilege is modify or higher.
Port > Clear Parameters > Clear Port Names > Clear Port Descriptions > Clear Port Names & Descriptions	-	Manage	Each option will only clear port names or descriptions on the ports that the user is assigned manage level port privileges. All others are unchanged.
Port > Change Waveband Assignment	-	Modify	Displays ports where the user's privilege is modify or higher.
Port > Change Signal Threshold Assignment	-	Modify	Displays ports where the user's privilege is modify or higher.
Port > Change Group Assignment	Manage	Manage	Not displayed in menu unless have privilege
Port > Change Alarm Severity Assignment	-	Modify	Displays ports where the user's privilege is modify or higher.
Port > Import Group Assignment	Manage	Manage	Not displayed in menu unless have privilege
Port > Export Group Assignment	Manage	Manage	Not displayed in menu unless have privilege
Connections > Change Connection Descriptions	-	Modify	Displays connections where the user's privilege is modify or higher on one port.
Connections > Clear Connection Descriptions	-	Manage	Will only clear descriptions for connections where the user is assigned manage privileges on both the input and output ports. All others are unchanged.
Port Groups	Manage	Manage	Required for creating, editing, modifying. Not displayed in menu unless have privilege

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Operation Access	System Privilege	Port Privilege	Comments
Protection Rules	Manage	Manage	Window opens if have View privilege only, attempts to edit in insufficient privilege error.
VOA	-	Modify	Window opens if have View privilege only, attempts to edit results in insufficient privilege error.
User Management Menu			
Set Password	None	-	All users may set his/her own password.
Add User	Manage	-	Not displayed in menu unless user has privilege.
Edit User	Manage	-	Not displayed in menu unless user has privilege.
Delete User	Manage	-	Not displayed in menu unless user has privilege.
Import Users	Manage	-	Not displayed in menu unless user has privilege.
Export Users	Manage	-	Not displayed in menu unless user has privilege.
Change Port Privilege Assignment	Manage	Manage	Not displayed in menu unless user has privilege.
System Menu			
Save Configuration	Modify	-	Not displayed in menu unless user has privilege.
Session Administration	Manage	-	Window opens if user has only View privilege. However, View users cannot force logoff of other users.
System Backup/Restore > Backup > Restore	Manage	Manage	Not displayed in menu unless user has privilege.
System Configuration > Name/IP > Date/Time > SNMP > Syslog > Runtime Options > Account Options > Startup Options	Manage	-	View privilege users may View the contents of the Name/IP and Date/Time windows.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Operation Access	System Privilege	Port Privilege	Comments
System Maintenance > Reboot > Restart > Shutdown > Reset to Factory Defaults	Manage	-	Not displayed in menu unless user has privilege.
System Upgrade/Rollback > Upgrade > Rollback	Manage	-	Not displayed in menu unless user has privilege.
System Alarms	View	View	Hardware and Software alarms are shown when user has system privilege of View. Optical Alarms are shown for ports where the user has the port privilege of View. Modify privilege is required to acknowledge alarms in each category above
System Logs > ALARM > AUTO	View	View	Will only see log messages for ports where privilege is View or higher for the port.
System Logs > SECU	Manage	-	Not displayed in menu unless user has privilege.

Virtual Private Switch (VPS)

Virtual Private Switch (VPS) is an optional (licensed) software feature allowing administrators to customize a user's port privileges.

Without the VPS feature, administrators are allowed to change a user's port privilege level. However, the assigned privilege level will apply to all ports in the system.

With the VPS feature, the administrator may customize a user's port privileges. Therefore, it is possible allow a user to configure and connect some ports in the system and only view other ports in the system. When a user's privilege for a port is set to the privilege level of None, the ports are not shown to the user. They will not see the ports in the I/O Matrix, in report or configuration screens, nor in alarm tables and system log files.

When the VPS feature is enabled, the **User Management > Change Port Privilege Assignments** menu option will be available to customize port privileges for users. When the feature is enabled, the **Export Users** and **Import Users** menu options also support viewing and customizing port privileges for users. See ”Export Users” on page 197, ”Import Users” on page 196, and ”User Account XML File” on page 203 for more information on these processes.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Password and Account Policies

The following sections describe the operation describe password and account security policies in the system:

- “Password Complexity Policy” (below)
- ”Password Change Policy” on page 179
- ”Password Expiration” on page 179
- ”Password Change Restrictions” on page 180
- ”Account Aging Policy” on page 181

Password Complexity Policy

The password complexity policy is composed of the following eight requirements (below), seven of which may be configured by “Account Options” on page 249.

- Password Minimum Length (5-20, default 8): This value establishes the required minimum password length.
- Minimum Punctuation Characters (0-20, default 1): This value establishes the required minimum number of punctuation characters.
- Minimum Numeric Characters (0-20, default 1): This value establishes the required minimum number of numeric characters (0-9).
- Minimum Lowercase Characters (0-20, default 1): This value establishes the required minimum number of lowercase characters (a-z).
- Minimum Uppercase Characters (0-20, default 0): This value establishes the required minimum number of uppercase characters (A-Z).
- Maximum Same Character (0-20, default 0): This value establishes the maximum number of times the same character may be used in a password. For example if the maximum is 2 then "banana.1" would fail because there are three "a" characters. Uppercase and lowercase are considered as different characters, so "bananA.1" would pass. A value of 0 disables this requirement.
- May not contain the User Name (0 or 1, default 1): The password must not contain the user name spelled forward or backward. This comparison is case insensitive. For example the password for user account "admin" may not include "admin", "nimda", "ADMIN", etc. A value of 0 disables this requirement.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- May not contain the following characters: Space, comma (,), question mark (?), colon (:), single quote ('), double quote ("), and backslash (\). This restriction is not configurable and cannot be disabled.

NOTES:
- The Password Complexity Policy applies to an administrator setting a password via “Add User” on page 186, “Edit User” on page 190, and to a user changing her/his password via “Set Password” on page 183.
- The Password Complexity Policy applies to the default administrative accounts "admin" and "madmin".

Password Change Policy

The password change policy includes two categories:

- Password Change Required (see “Password Expiration” on page 179)
- Password Change Restrictions (see “Password Change Restrictions” on page 180)

NOTES:
- The Password Change Policy only applies to a user changing her/his password via “Set Password” on page 183, it does not apply to an administrator changing a user's password via “Edit User” on page 190.
- Password Expiration does not apply to the default administrative accounts "admin" and "madmin".

Password Expiration

When adding or editing a user account, an administrator may configure the user account to require the user to periodically change the login password.

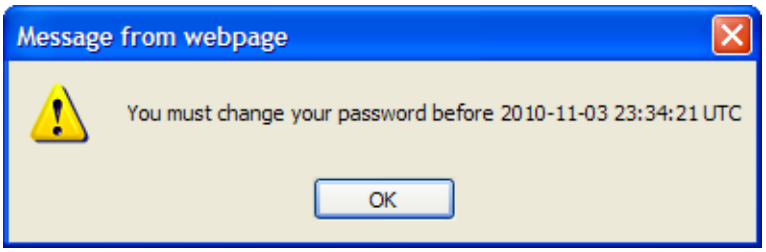
The password expiration policy is governed by two user account parameters:

- **Password Aging Interval** (0-999 days, default 0): This value establishes a period of time between the last password change and when the user will be notified that a password change is required. The password aging policy is disabled if the Password Aging Interval is "0".
- **Password Change Interval** (0-999 days, default 0): This value establishes a grace period during which the user may continue to use the expired password to access the system. During this grace period, the user will receive warning notifications to change the password. If the user changes the password during the grace period, the account state returns to “In Service” and the Password Aging Interval is restarted (Figure 100 below). If the user does not change the password prior to the end of the grace period, the account state changes to “Out Of Service” and the user will not be able to log onto the system. The user

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

account will immediately transition from “In Service Expired” to “Out of Service” if the Password Change Interval is “0”.

Figure 100 Password Change Required



For ease of administration, when adding a new user the Password Aging Interval and Password Change Interval are defaulted from the Account Options parameters Password Aging Default and Password Change Default respectively (see ”Account Options” on page 249).

Password Change Restrictions

The password change restrictions include the following four restrictions, three of which may be configured by “Account Options” on page 249.

- **Password Minimum Interval** (0-999 days, default 0): This value establishes a period of time between the last password change and when the user may again change the password.
- **Maximum Characters from Prior Password** (0-20, default 0): This value establishes limits on similarity between the current password and the new password. It compares strings of consecutive characters in the current and new password. For example, with a value of 3 and current password "banana.1", a proposed new password "unanalyzable.2" would fail because they both contain "nana" whose length is greater than 3. The comparison is case-sensitive, so in the latter example ""unAnalyzable.2" would pass. A value of 0 disables this requirement.
- **Password Reuse History** (0-24, default 0): The password hashes for the last 24 passwords are retained in a password history list. This value establishes the depth of comparison in the password history list. The user may not reuse a password that is in the password history list within the comparison depth. The list does not contain the current password, only the previously used passwords. Changing this value does not clear or truncate the password history list, it only affects the depth of comparison. A value of 0 disables this requirement.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- **Same as Current Password**: The new password cannot be the same as the old/current password. This restriction is not configurable and cannot be disabled.

NOTES:
- A non-zero Password Minimum Interval value prevents a user from defeating the Password Reuse policy by quickly changing the password 24 times and then setting the original password.
- If the Password Minimum Interval value is set to a value equal to the Password Aging value then the password can only be changed during the password change required warning period.

Account Aging Policy

When adding or editing a user account, an administrator may configure an account aging policy. The account aging policy operates by establishing a maximum allowable time period between successful logins to a user account. If no login occurs during this period, the account is placed out of service and the user will need to contact the administrator to re-enable access.

The account aging policy is governed by the **Account Aging Interval** user account parameter (0-999 days). For ease of administration, when adding a new user the Account Aging Interval is defaulted from the Account Aging Default in the Account Options page (see ”Account Options” on page 249).

Account State	Description
In Service (IS)	No password change required. User may access the system with the current password.
In Service Expired (IS-EXP)	Password has expired; user may access system until the grace period expires. User will receive warnings to change the password during the grace period.
Out Of Service (OOS)	User may not access the system. User must contact a system administrator to restore the account to IS or IS-EXP. **NOTE**: Administrators may deliberately set accounts to OOS and the account may also be automatically placed OOS by the password aging policy or the account aging policy.

The user's account state may transition automatically from IS to IS-EXP or OOS due to password expiration (see “Password Change Policy” on page 179) or the account aging policy (“Account Aging Policy” on page 181). A system administrator can also explicitly establish a user's account state (see “Adding a User Account” on page 189) or revise a user's account state (see “Editing a User Account” on page 193).

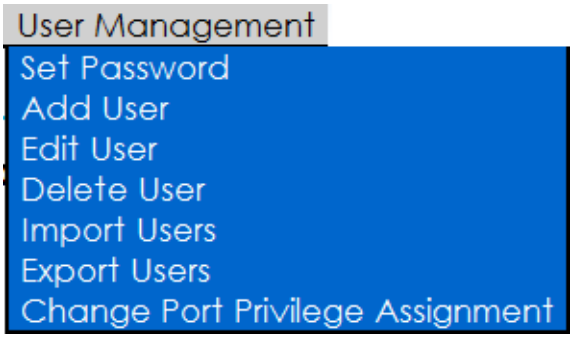
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Change Account State to	Concurrently Assign New Password	Effect of Operation
IS	No	• User's account access is restored with the previous password. • The password aging and change intervals restart. • User may continue to use the old password until the next expiration or change the password and restart the intervals.
IS-EXP	No	• User's account access is restored with the previous password. • The password change interval restarts. • User receives notification to change the password upon login.
IS	Yes	• User's account access is restored with admin provided password. • The password aging and change intervals restart. • If allowed by the password change policy, the user may change this password and restart the intervals.
IS-EXP	Yes	• User's account access is restored with admin provided password. • The password change interval starts. • User received notification to change the password upon login.

User Management Menu Options

The **User Management** menu options allow users with the system-level privilege of Manage to add, edit, and delete users for the system, set user passwords as well as configuring system-level and port-level privileges for users.

Figure 101 User Management Menu



NOTE: The full **User Management** menu is displayed only to users with Manage system-level privileges. For all other users, the only option displayed is “Set Password”.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

All Glimmerglass systems ship preconfigured with the default “admin” user account. This account is assigned Manage privileges and whose installation default password is "password".

The table below describes the **User Management** menu options and provides the page numbers where the menu options are further detailed in this chapter.

Menu Option	Description	Page
Set Password	Sets a new password for the user account of the user currently logged into the system.	183
Add User	Adds a user account to the system.	186
Edit User	Edits a user account on the system.	190
Delete User	Deletes a user account from the system.	194
Import Users	Imports a user account database to the system from an XML file.	196
Export Users	Exports the current user account database from the system to an XML file.	197
Change Port Privilege Assignments	Change a user's port privilege for specified ports This option is only provided when the VPS feature is licensed.	198

Set Password

The **User Management > Set Password** menu option opens the Set Password window (Figure 102), from which a logged-in user may change their password. To change a password on another user’s account, use the Edit User menu option instead (see ”Editing a User Account” on page 193).

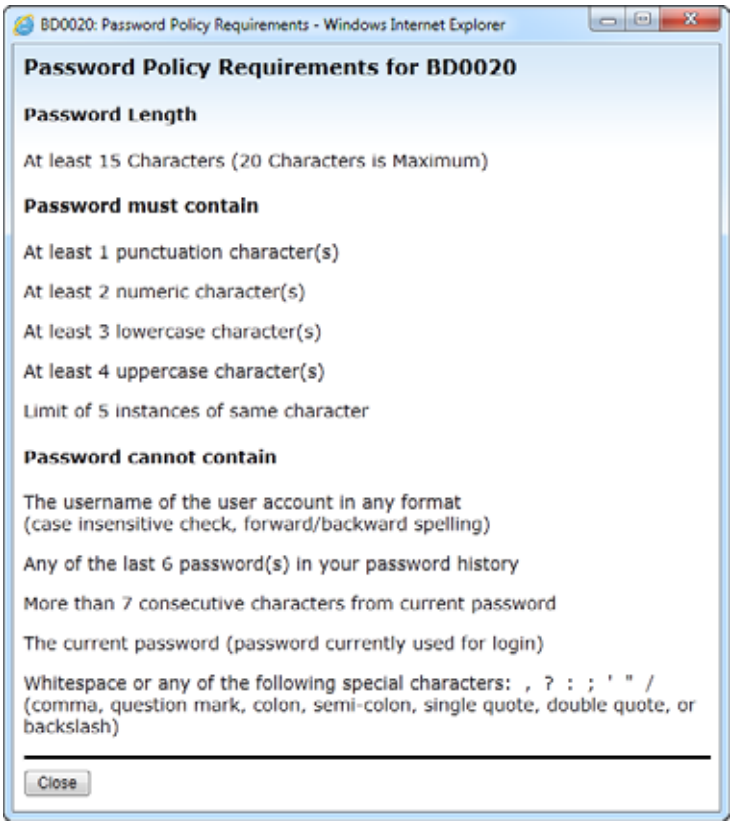
NOTE: Password values are encrypted when SSL is enabled for communication with the Webserver (https://). SSL is enabled by default for ClickFlow sessions.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 102 Set Password Window

The **Set Password > Password Policy** Advisory Window (Figure 103) displays the policies relating to entry of a new password via Set Password. The policies include both the Password Complexity Policy and the Password Change Policy configured via “Account Options” on page 249. Password policies that are disabled (by a zero value) are not displayed.

Figure 103 Password Policy Advisory Window for Set Password



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE:	In the above example all of the password policies have been configured via Account Options with non-zero values so as to display all possible requirements.

Changing an Account Password

To set a new password for the logged-in user account:

1. Select the **User Management > Set Password** menu option from the Connection screen to view the Set Password window (Figure 102).

NOTE:	A user may be prohibited from changing their own password via Set Password if an administrator has configured a password change policy, see “Password Change Restrictions” on page 180.

2. (Optionally) Click the **Password Policy** button to display the password requirements (Figure 103 on page 184). For more information see “Password and Account Policies” on page 178 and “Password Change Policy” on page 179.

3. Type the current password in the **Old password** text box.

4. Type the new password in the **New password** text box.
   The password text is hidden as it is typed and only bullet or asterisk symbols are shown to represent each character in the password.

5. Type the new password again in the **Confirm password** text box to verify the password value.

6. Click the **Set Password** button to assign the new password to the current user account. (Or to cancel the password change, go to step 7 without clicking the **Set Password** button.) If the new password does not meet the password policy criteria, an error dialogue box will indicate the specific criteria not met. If an error appears, revise the password and then click the **Set Password** button again.

7. Click the **Close** button to return to the Connection screen.

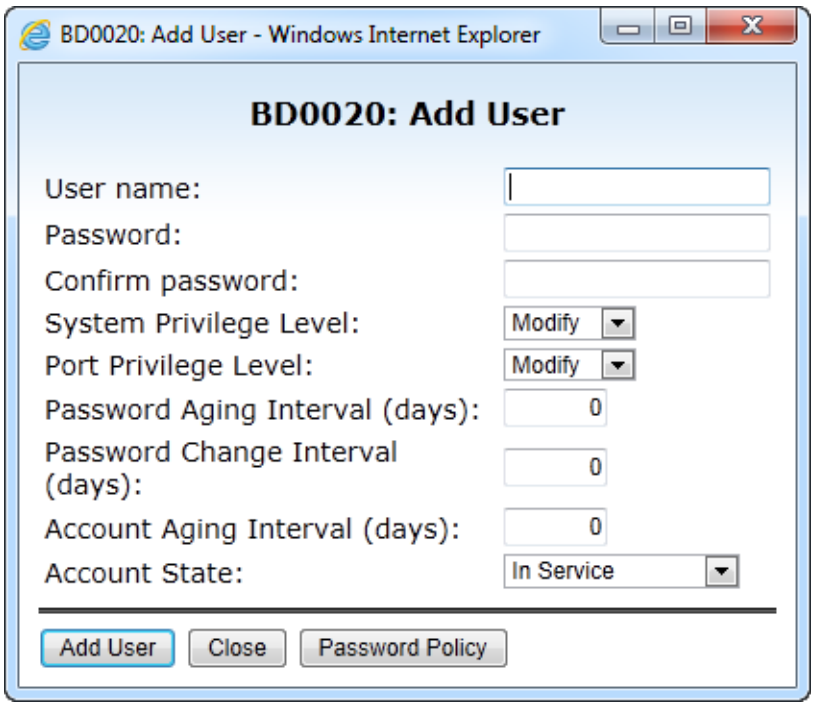
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Add User

The **User Management > Add User** menu option opens the Add User window (Figure 104), from which a user account can be added to the system and assigned system-level privileges for administration and provision of the system through the ClickFlow user interface.

NOTES:
- User accounts created via ClickFlow are also allowed to access TL1 (and vice versa). Regardless of which interface is used to create the user account, the system and port privileges are enforced. The user's TL1 user access privileges are automatically set to match the system and port privilege levels. See the *Glimmerglass Transaction Language 1 Manual* for definitions of user access and command access privileges.
- Password values are encrypted when SSL is enabled for communication with the Webserver (https://). SSL is enabled by default for ClickFlow sessions.
- SNMPv3 supports an independent user/permissions model. Accounts created under ClickFlow or TL1 cannot be used to authenticate via SNMP.
- The system-defined user accounts for accessing the Maintenance Console Main Menu (serial port, SSH) are separate from the ClickFlow and TL1 user accounts.

Figure 104 Add User Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The following table describes the elements in the Add User window.

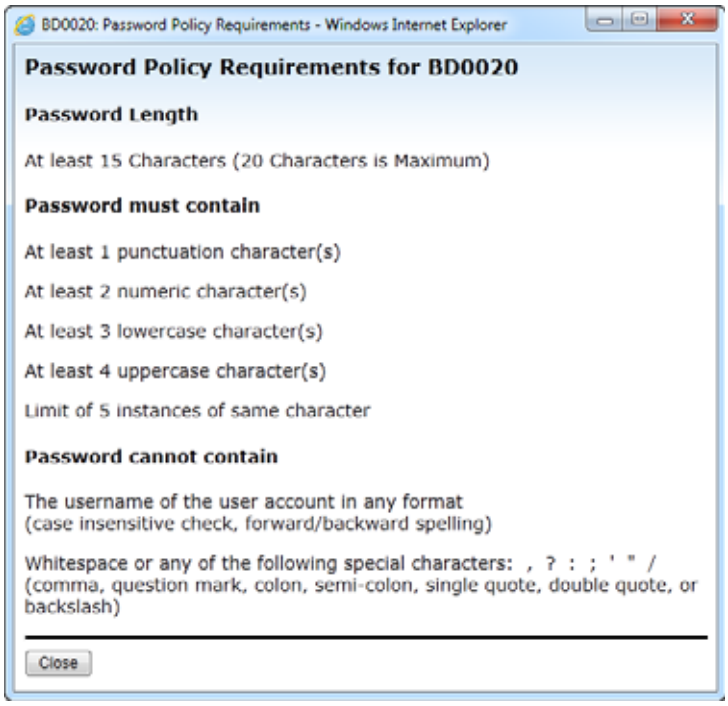
Element	Description
User Name	Assign a user name for this user account. • Alphanumeric, case sensitive • Requirement: 3 – 20 characters (min – max) User name cannot contain punctuation characters nor white space.
Password	Assign a Password for this user's account. To display the configured password complexity requirements, click the **Password Policy** button (see “Password and Account Policies” on page 178 for more information).
Confirm Password	Re-enter the password to confirm (must match the password from above).
System Privilege Level	Pull-down selection to assign user's system-level privilege. • Values: Manage, Modify, View, None Default: Modify
Port Privilege Level	Pull-down selection to assign user's privilege level for all ports in the system. • Values: Manage, Modify, View, None Default: Modify
Password Aging Interval (days)	Limit on number of days until the user's password expires after the account is created. Account State will change to "In Service Expired" after limit is reached. • Integer value (number of days) • Valid Range: 0 and 999, 0 means operation is disabled Default = Value of Password Aging Default account option
Password Change Interval (days)	Limit on number of days the user will be notified to change an expired password. Account state will change to "Out Of Service" after limit is reached. • Integer value (number of days) • Valid Range: 0 and 999, 0 means operation is disabled Default = Value of Password Aging Default account option
Account Aging Interval (days)	Limit on number of days without user login. Account is placed out of service if limit is reached. • Integer value (number of days) • Valid Range: 0 and 999, 0 means operation is disabled Default = Value of "Account Aging Default" Account Option

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Account State	Pull-down selection to change the current state of the user's account. • Values: In Service, In Service Expired, Out Of Service Default = In Service **NOTE**: To force a user to change his account's password from the administrator assigned password, set the **Password Change Interval** to a non-zero value, and set the **Account State** to In Service Expired.
Add User	Click the **Add User** button to create the user account.
Password Policy	Click the **Password Policy** button to display the currently configured Password Complexity Policy Options (Figure 105).
Close	Click **Close** to close the Add User window. If Close is clicked prior to the **Add User** button then the account creation is canceled.

The **Add User > Password Policy** window (Figure 105) displays the password requirements when entering a user account password via Add/Edit User. Password policies that are disabled (by a zero value) are not displayed. The Password Complexity Policy is configured via “Account Options” on page 249.

Figure 105 Password Policy Advisory Window for Add/Edit User



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE:	In this example all of the password policies have been configured via Account Options with non-zero values so as to display all possible requirements.

Adding a User Account

A user with the Manage system-level privilege can add new user accounts. To add a user account:

1. Select the **User Management > Add User** menu option from the Connection screen to view the Add User window (Figure 104 on page 186).

2. (Optionally) Click the **Password Policy** button to display the password requirements (Figure 105 on page 188). For more information see “Password and Account Policies” on page 178.

3. Enter a name in the **User name** text box.

4. Type a password in the **Password** text box. The password text is hidden as it is typed and only bullet symbols are shown to represent each character in the password.

5. Type the password again in the **Confirm password** text box to confirm the password.

6. From the **System Privilege Level** pull-down list, select the privilege level to be assigned to the new user account (None, View, Modify, or Manage).

7. From the **Port Privilege Level** pull-down list, select the privilege level for all ports to be assigned to the new user account (None, View, Modify, or Manage).

8. The **Password Aging Interval** box contains the system Password Aging Default value. If a different password aging value is required, enter the new value in this box (0-999 days). Otherwise, skip to step 9.

9. The **Password Change Interval** box contains the system Password Change Default value. If a different password change value is required, enter the new value in this box (0-999 days). Otherwise, skip to step 10.

10. The **Account Aging Interval** box contains the system Account Aging Default value. If a different password change value is required, enter the new value in this box (0-999 days). Otherwise, skip to step 11.

11. The **Account State** pull-down defaults to “In Service”. If a different account state is desired, use the pull-down to select the desired account state. Otherwise, skip to step 12.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

12. Click the **Add User** button to create the user account. If all data is correctly entered, a confirmation dialogue box will appear to confirm the addition of the user. If the data is not correct (e.g., passwords do not match or the password does not meet the password policy criteria), an error dialogue box will indicate the specific error. If an error appears, correct and then click the **Add User** button again.

13. Click **OK** in the confirmation box to return to the Add User window.

14. If no other users are to be created at this time, click the **Close** button to exit the window. If more users are to be added, repeat step 3 though step 14 until complete.

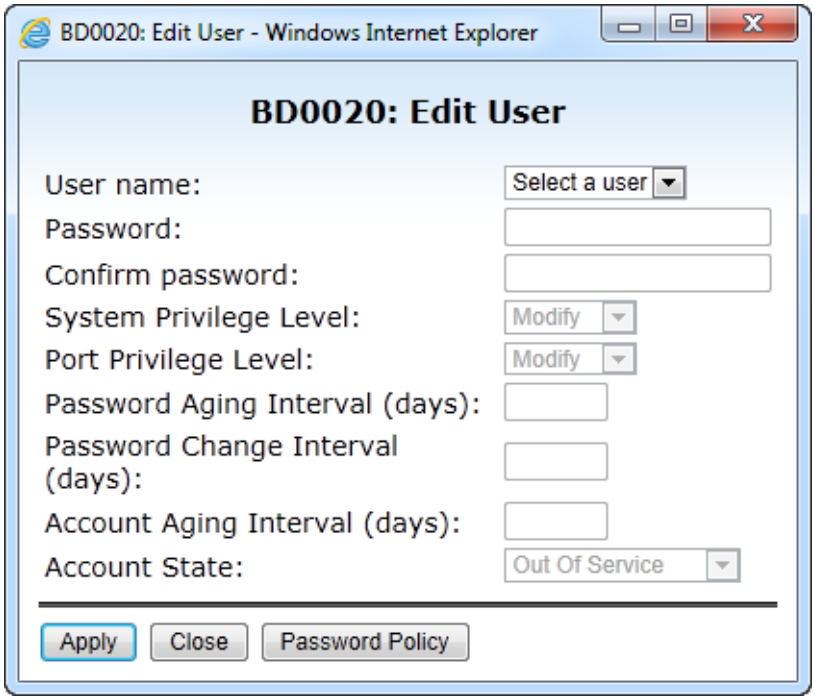
Edit User

The **User Management > Edit User** menu option opens the Edit User window (Figure 106), from which the default admin user or a user with the system-level privilege of Manage may change a user's password, system-level privilege, port-level privilege (for all ports), the state of the user account, or the password/account expiration policy for the user.

NOTES:
- Edit User will update the user's TL1 user access privileges to match the system and port privilege levels. The user's TL1 privileges can be refined through the TL1 interface. A user's affective TL1 command privilege can be more restrictive than that of ClickFlow, but it cannot exceed that of ClickFlow. See the *Glimmerglass Transaction Language 1 Manual* for definitions of user access and command access privileges.
- Password values are encrypted when SSL is enabled for communication with the Webserver (https://). SSL is enabled by default for ClickFlow sessions.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 106 Edit User Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The table below describes the elements in the Edit User window.*Not displayed in menu unless user*

Element	Description
User name	Pull-down menu containing all users. Select a user. Once selected, the configurable fields below (with the exception of the password fields, will display the currently configured values for the user.
Password	Change Password for the selected user. If no entry is made here or in the Confirm Password field, the user's password will not be changed. The configured password complexity requirements may be displayed by selecting the Password Policy button, for more information see “Password and Account Policies” on page 178
Confirm Password	Re-enter Password to confirm - must match new Password (if changed).
System Privilege Level	Pull-down selection to modify the user's system-level privilege • Values: Manage, Modify, View, None
Port Privilege Level	Pull-down selection to modify the user's privilege level for all ports in the system. • Values: Manage, Modify, View, None **NOTE**: If the value displayed for modification is "Mixed", then the switch has the Virtual Private Switch feature and the user has been assigned custom privileges for multiple port ranges. Changing this value will erase the customized ranges/privileges and replace with the specified privilege for all ports in the system.
Password Aging Interval (days)	Change the limit for the number of days until the user's password expires after a password change. Account State will change to "In Service Expired" after limit is reached. • Integer value (number of days) • Valid Range: 0 and 999, 0 means operation is disabled
Password Change Interval (days)	Change the limit for the number of days the user will be notified to change an expired password. Account State will change to "Out Of Service" after limit is reached. • Integer value (number of days) • Valid Range: 0 and 999, 0 means operation is disabled
Account Aging Interval (days)	Change the limit for the number of days without user login. Account is placed out of service if limit is reached. • Integer value (number of days) • Valid Range: 0 and 999, 0 means operation is disabled This change will take effect upon the next password change by the user.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Account State	Pull-down selection to change the current state of the user's account. • Values: In Service, In Service Expired, Out Of Service
Apply	Click the **Apply** button to save the changes to the user account.
Password Policy	Click the **Password Policy** button to display the currently configured Password Complexity Policy Options (Figure 105 on page 188).
Close	Click **Close** to close the Add User window. If **Close** is clicked prior to the **Apply** button then the account changes are discarded.

has privilege.

The **Edit User > Password Policy** window (Figure 105 on page 188) displays the password requirements when entering a user account password via Add/Edit User. Password policies that are disabled (by a zero value) are not displayed. The Password Complexity Policy is configured via Account Options (page 249).

Editing a User Account

A user with the Manage system-level privilege can edit user accounts. To edit a user account:

1. Select the **User Management > Edit User** menu option from the Connection screen to view the Edit User window (Figure 106 on page 191).

2. (Optional) Click the **Password Policy** button to display the password requirements (Figure 105 on page 188). For more information see “Password and Account Policies” on page 178.

3. From the **User name** pull-down menu, select the name of the user account to be edited.

4. If the password is to be changed, type a password in the **Password** text box. If not changing he password, skip to step 6. The password text is hidden as it is typed and only bullet or asterisk symbols are shown to represent each character in the password.

5. Type the password again in the **Confirm password** text box to confirm the password changed in step 4.

6. From the **System Privilege Level** pull-down list, select the privilege level to be assigned to the new user account (None, View, Modify, or Manage). If no change is required, skip to step 7.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

7. From the **Port Privilege Level** pull-down list, select the privilege level for all ports to be assigned to the new user account (None, View, Modify, or Manage). If no change is required, skip to step 8.

NOTE: If the current value for **Port Level Privilege** is "Mixed", then the user's access to ports in the system has been customized using the VPS feature. Changing this value will remove the custom changes and replace them with a single port privilege for all system ports.

8. Enter a new value in the **Password Aging Interval** box to change the password aging value. If no change is required, skip to step 9.

9. Enter a new value in the **Password Change Interval** box to change the password change value. If no change is required, skip to step 10.

10. Enter a new value in the **Account Aging Interval** box to change the account aging value. If no change is required, skip to step 11.

11. From the **Account State** pull-down, select the desired account state. If no change is required, skip to step 12.

12. Click the **Apply** button to apply the above changes to the user account. If all data is correctly entered, a confirmation dialogue box will appear to confirm the addition of the user. If the data is not correct (e.g., passwords do not match or the password does not meet the password policy criteria), an error dialogue box will indicate the specific error. If an error appears, correct and then click the **Apply** button again.

13. Click **OK** in the confirmation box to return to the Edit User window.

14. If no other users are to be edited at this time, click the **Close** button to exit the window. If more users are to be edited, repeat step 3 though step 14 until complete.

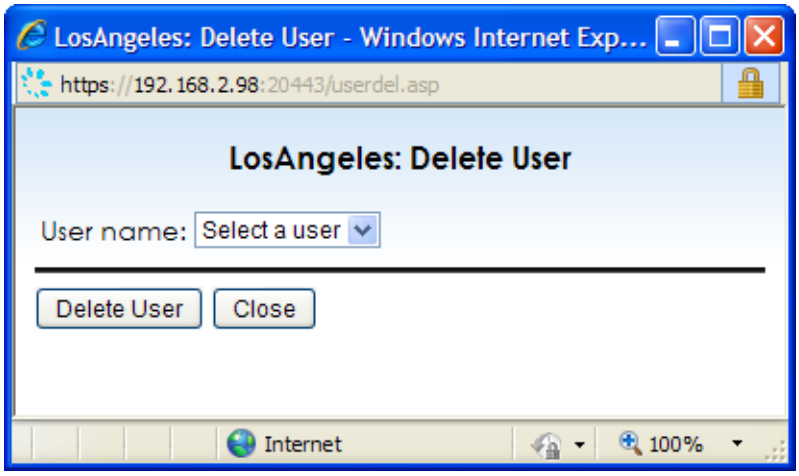
Delete User

The **User Management > Delete User** menu option opens the Delete User window (Figure 107), from which the default admin user or a user with the system-level privilege of Manage may delete user accounts.

NOTE: The corresponding TL1 user account will also be deleted by this operation.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 107 Delete User Window



Deleting a User Account

To delete a user account:

1. Select the **User Management > Delete User** menu option from the Connection screen to view the Delete User window (Figure 104).

2. From the **User name** pull-down menu, select the name of the user account to be deleted.

   NOTES: The admin user (all systems), snmpuser user (all systems), and madmin user (systems with the Glimmerglass Console feature) can not be deleted.

   The system will end the current user session if the current user's account is deleted.

3. Click the **Delete User** button to delete the user account from the system.
   The Delete User window displays a confirmation request before deleting the user account.

4. To continue with the delete, click **OK** in the confirmation request box.
   The Delete User window displays a confirmation that the user account was deleted.

5. Click **OK** in the confirmation box to return to the Delete User window.

6. Repeat step 2 through step 5 for all user accounts to be deleted.

7. Click **Close** to close the Delete User window and return to the Connection screen.

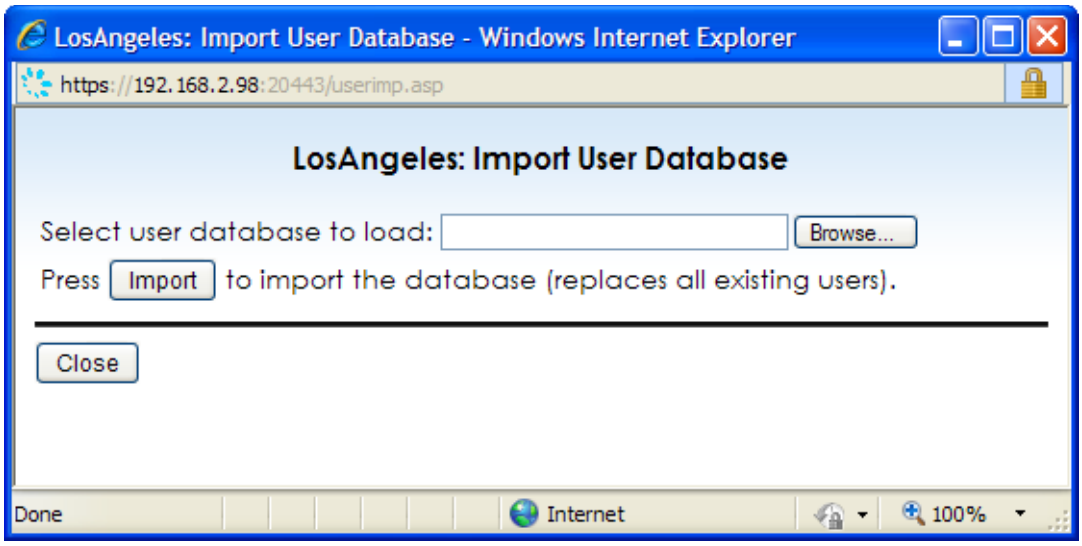
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Import Users

The **User Management > Import Users** menu option opens the Import User Database window (Figure 108), from which the default admin user or a user with the system-level privilege of Manage may import a previously exported/modified copy of the system's user database (users.xml file). An Import of the user database completely replaces the version of the user database on the system. Partial or incremental imports are not supported.

NOTE: Importing a previously exported and modified users.xml file is the ClickFlow-based method of apportioning ports for assignment of port-level privileges. Modifying the users.xml file is detailed in “User Account XML File” on page 203. Port range and port-level privilege assignments can also be performed through TL1 directly, without requiring an export, modification, and subsequent import. The TL1 method is suggested as a method of assigning port-level privileges if the user is uncomfortable with the XML file format. The Glimmerglass Console option is recommended if administering port-level privileges for multiple users and multiple switches.

Figure 108 Import User Database Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Importing User Account Information

To import user accounts from an XML file:

NOTE: Before importing the user account XML file, review the section “Considerations Before Editing the User Account XML File” on page 209. This section includes a recommendation that the current user database be exported to create a backup file.

1. Select the **User Management > Import Users** menu option from the Connection screen to view the Import User Database window (Figure 108).

2. From the Import User Database window, click the **Browse...** button to display the Choose File window.

3. Select an XML file and click the **Open** button.
   The name and location of the selected file is displayed in the Import User Database window.

4. Click **Import** to import the user database.
   The database is imported onto the system and a results confirmation window is displayed, indicating that the user database was loaded successfully.

5. Click **OK** in the results confirmation window.

6. Click **Close** to close the Import User Database window and return to the Connection screen.

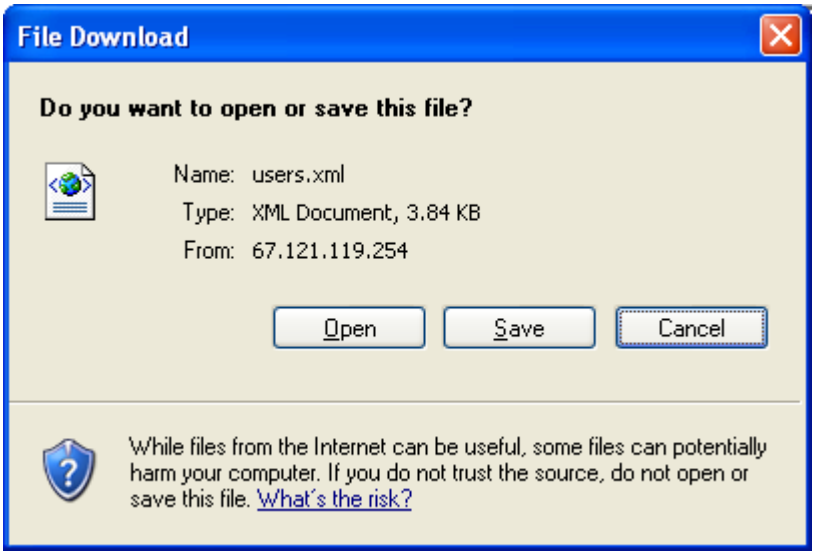
NOTE: Note, once this file is imported, the change will also be in effect for the TL1 user accounts.

Export Users

The **User Management > Export Users** menu option opens the (web browser dependent) File Download window (Figure 109), allowing the default admin user or a user with the system-level privilege of Manage to export the system's user database to an XML file with the default name “users.xml”.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 109 File Download Window (Internet Explorer 8)



Exporting User Account Information

To export the user database from the system to an XML file:

1. Select **User Management > Export Users** from the Connection screen to view the (web browser dependent) File Download window (Figure 109).

2. From the File Download window:
   - Click **Open** to view the exported configuration file.
   - Click **Save** to open a Save As window in which to enter a name and location for the XML file. Once you've entered the name and location for the file, click **Save** in the Save As window. The XML file will be saved in the specified location.

NOTE: When saving the exported XML file, verify that the "Save as type:" field in the browser window indicates "XML Document."

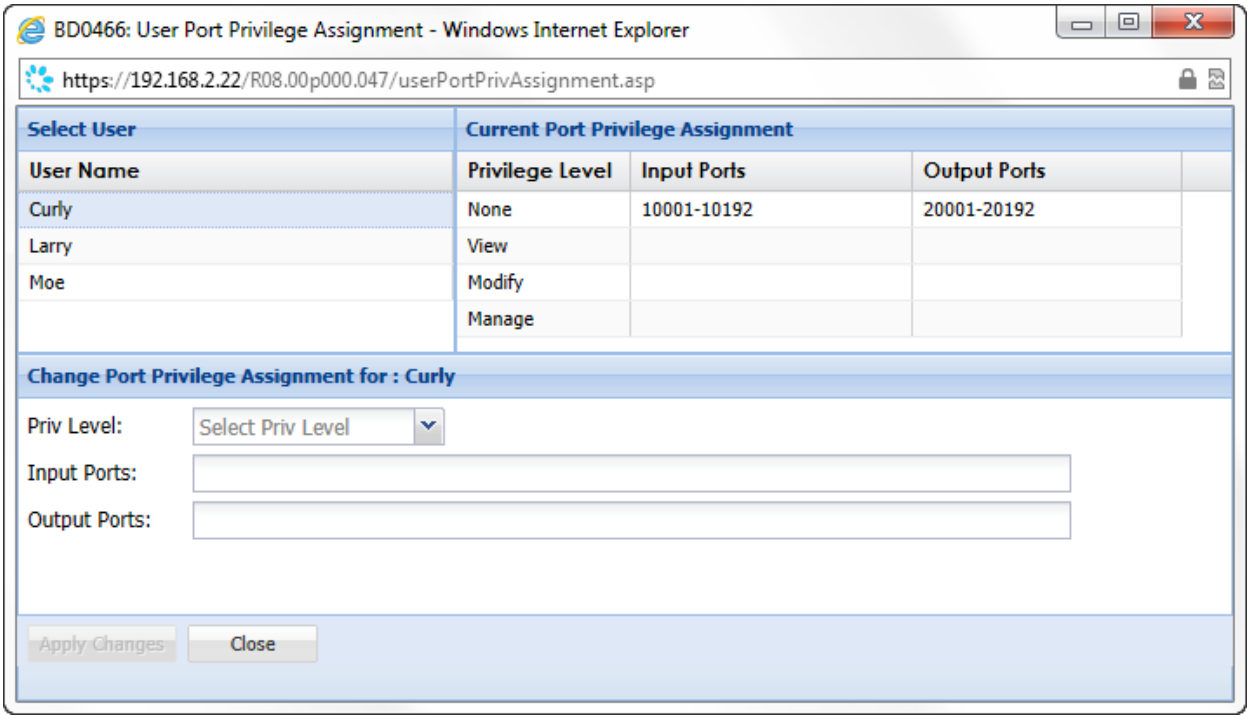
See the following section, "User Account XML File" for information on how to modify the XML user file once it has been exported.

Change Port Privilege Assignments

The **User Management > Change Port Privilege Assignments** menu option opens the User Port Privilege Assignment window shown in Figure 110 below. Configuring port privileges requires full administrative privileges (manage for system and for all ports).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 110 User Port Privilege Assignment Window



Referencing Figure 110, the User Port Privilege Assignment window is composed of three sections. The upper two sections of the screen are for selecting a user and viewing the current privilege level assignments for that user for all ports in the system. The lower section is used to modify assignments for the selected user.

- At the upper left port of the window, the Select User section shows all the users configured in the system. Left-click on a user name to select the user and start the process of changing this user's port privileges.
- After the selection is made, the data in the upper-right section (Current Port Privilege Assignment), is filled in showing the four privilege levels with the ports assigned to each level. This area is initially blank. In Figure 110 above, the user name Curly has been selected (note the blue background).
- The lower section of the window is used to change the selected user's privilege level assignment for input and output ports. The following three fields are provided:
    - **Priv Level** - Pull-down menu for selecting the privilege to assign ports.
    - **Input Ports** - Text box used to enter the input port numbers to assign to the selected privilege.
    - **Output Ports** - Text box used to enter the output port numbers to assign to the selected privilege.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTES: Tool tips are provided when the mouse is placed over either field in the lower section. The tool tips convey the following information for data entry:

Priv Level:

- Select the desired privilege from the pull-down menu.

Entering port numbers in the **Input Ports** or **Output Ports** text boxes:

- Use long port numbers (e.g., 10xxx for input, 20xxx for output)
- Use a hyphen between port numbers to specify a range of ports
- Use a comma as a separator between port numbers or port ranges.

Example Input Ports entry:

- 10001,10010,10020-10030,10040-10050,10060

Two buttons are provided at the bottom left of the window: **Apply Changes** and **Close**. The **Apply Changes** button will be inactive until the user starts the assignment process in the lower section by selecting a value for **Priv Level** then entering input port numbers and/or output port numbers (either or both).

To customize the port privileges for a user, perform the following steps:

1. Open the User Port Privilege Assignment window (**User Management > Change Port Privilege Assignments**).

2. In the **Select User** section, select (left-click) on the desired user name. After a moment, the current port privilege assignments will display in the **Current Port Privilege Assignment** section to the right. Additionally, the title bar for the lower section will change to: “Change Port Privilege Assignment for: <user name>”

3. In the lower section of the window, select the desired privilege level to assign from the **Priv Level** pull-down menu.

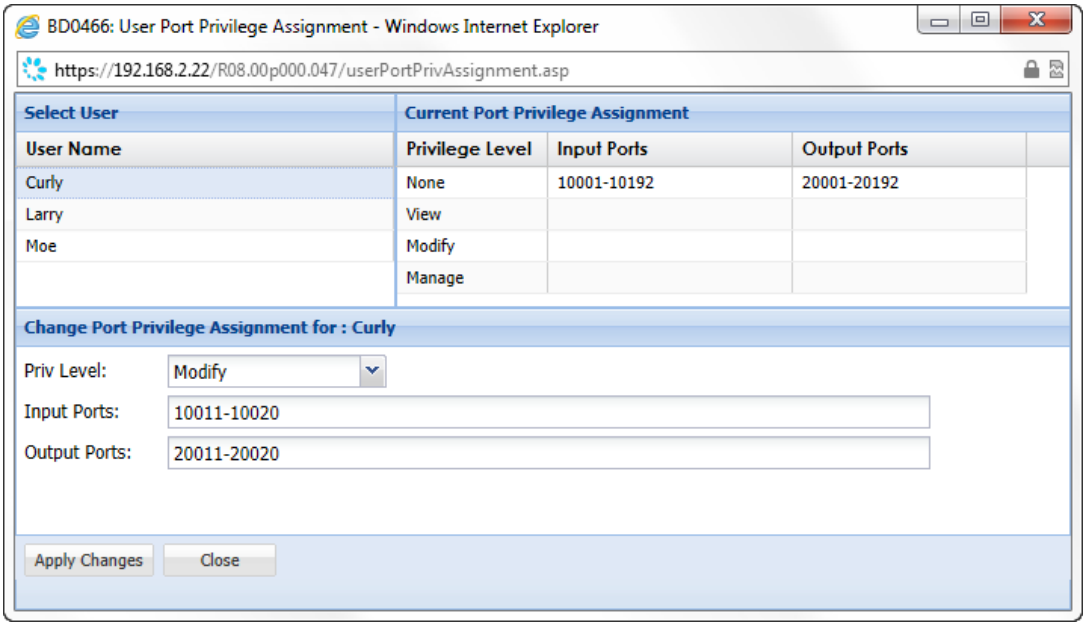
4. In the **Input Ports** text box, enter the input port number, port numbers, and/or port number range for assignment to this privilege level. This step is optional (this field can be left empty if only assigning output ports).

5. In the **Output Ports** text box, enter the output port number, port numbers, and/or port number range for assignment to this privilege level. This step is optional (this field can be left empty if only assigning input ports).

6. The **Apply Changes** button will activate. Figure 111 below depicts the Alarm Severity Assignment window after selecting an alarm type and specifying ports requiring a severity change.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

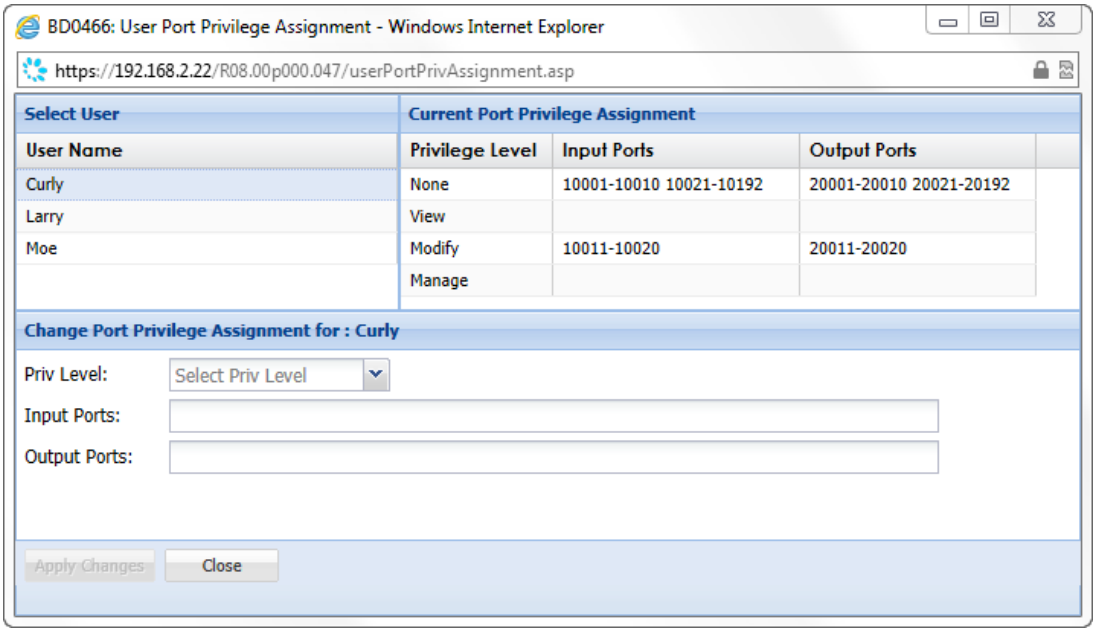
Figure 111 User Port Privilege Assignment Window (After Specifying Port Privilege Changes)



7. Click the **Apply Changes** button to change the privilege assignment for the entered ports. A status message will appear below the **Apply Changes** button indicating success or failure. After a moment, the entire window will refresh. The upper section will display the new port privilege assignments as shown in Figure 112 below (if successful). All status messages (cause and result) are defined at the end of this procedure.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 112 User Port Privilege Assignment Window (After Applying Changes)



8. If finished with privilege assignments, then click the **Close** button to exit the window. Otherwise, continue by selecting the next user for which port privilege customization is desired.

The area below the **Apply Changes** button is used to post status messages reporting success or failure of the port privilege assignment. These status messages automatically clear after a few seconds.

The possible status messages shown after applying changes are described below. For errors, selections in the upper sections of the User Port Privilege Assignment window will remain unchanged. The lower section is cleared and the window is ready to accept corrected data.

Status Messages:

- “Success: All updates completed”
  This message indicates that the ports and/or port ranges entered were composed of valid port numbers.
- “Success: All updates completed for valid port numbers”
  This message indicates that one or both port lists contained invalid port numbers (numbers not represented in the upper section). In this case, the requested change was made for the valid port numbers and the invalid numbers were ignored. The upper section reflects the new configuration.
- “Error: Invalid Port Number or Invalid Port Range”
  This message indicates that all the port numbers entered in both port lists are resolved as

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

invalid. For a range, this may occur if only the starting number of the range is invalid. If only some port numbers are invalid, then the status would be “Success: All updates completed for valid port numbers”

- “Error: Missing Priv Level and/or Ports”
  This message indicates one of the following:
  - Input or output ports were entered (activates **Apply Changes** button) and then the **Apply Changes** button was used without selecting a Priv Level.
  - The Priv Level was selected then either input or output ports were entered. Then, the port fields were erased (now blank) and the **Apply Changes** button was used.

User Account XML File

After exporting the user database file using the **User Management > Export Users** menu option, an XML file is created and stored in the specified directory. The default file name for the XML file is “users.xml”, but a new file name can be specified at the time the XML file is exported.

The users.xml file may be edited with a text editor such as WordPad. Figure 113 shows an example XML file for a 144x144 port system with the VPS feature.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 113 Example users.xml File


```xml
<?xml version="1.0" ?>
<userPrivDB version="1.0" portPriv="enable">
  <user name="User1" uid="2156598698"
   passwd="gxn1:83b6238972fa1dc9a8e823b474aaac691b48ec11cf30e96b6efa2452"
   level="modify" passwordAgeLimit="0" passwordWarnLimit="0" accountAgeLimit="0"
   serviceState="IS"
   passwordExpirationTime="infinity" passwordChangeTime="2012-05-30 21:45:17"
   latestLoginTime="infinity">
   <passHistory
   passwd="gxn1:08d0308fdde260f56175ecba25e2307bcf86546433149bab4a1425dc" />
   <passHistory
   passwd="gxn1:d1e1d84eac393fcc1314b4602fa1ecebfa42a8b3697dc4014e9f524e" />
   <passHistory
   passwd="gxn1:359e8692430a82ae883c5ebe8abf84d6f2a4f0b4c171703888bc91dd" />
   <portRange from="10001" to="10072" level="view" />
   <portRange from="10073" to="10108" level="modify" />
   <portRange from="10109" to="10144" level="manage" />
   <portRange from="20001" to="20072" level="view" />
   <portRange from="20073" to="20108" level="modify" />
   <portRange from="20109" to="20144" level="manage" />
  </user>
  <user name="admin" uid="1"
   passwd="gxn1:bd76bfc690438c5f63a52d301f4ddef61483b351121e03cf310a092e"
   level="manage" passwordAgeLimit="0" passwordWarnLimit="0" accountAgeLimit="0"
   serviceState="IS"
   passwordExpirationTime="infinity" passwordChangeTime="2012-05-29 17:52:49"
   latestLoginTime="2012-05-30 21:38:14">
   <passHistory
   passwd="gxn1:5908fa4491d4f50c2139cb4b0dd4cf813a61411c8e4d1355f32ff064" />
   <portRange from="10001" to="10144" level="manage" />
   <portRange from="20001" to="20144" level="manage" />
  </user>
  <user name="madmin" uid="3"
   passwd="gxn1:c7a88b7c37332d2e0d993ce88636f9a8b1df184203523fb3a514070f"
   level="manage" passwordAgeLimit="0" passwordWarnLimit="0" accountAgeLimit="0"
   serviceState="IS"
   passwordExpirationTime="infinity" passwordChangeTime="2012-05-29 17:52:49"
   latestLoginTime="infinity">
   <passHistory
   passwd="gxn1:f1505e3096fa7e8b2b6c6e720218f030057bd35f46816167cd1d6539" />
   <portRange from="10001" to="10144" level="manage" />
   <portRange from="20001" to="20144" level="manage" />
  </user>
  <user name="snmpuser" uid="4"
   passwd="gxn1:53b623886bf3cf01a0d55a299b6a7f9bca717aa3f0c4d5382a7a8f86"
   level="manage" passwordAgeLimit="0" passwordWarnLimit="0" accountAgeLimit="0"
   serviceState="IS"
   passwordExpirationTime="infinity" passwordChangeTime="2012-05-29 17:52:25"
   latestLoginTime="infinity">
   <portRange from="10001" to="10144" level="manage" />
   <portRange from="20001" to="20144" level="manage" />
  </user>
</userPrivDB>
```


Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

As shown above, WordPad displays each XML attribute and the value assigned to the attribute using the following format:

```
attribute = “value”
```

For each user on the Glimmerglass system, WordPad includes an entry beginning with:

```
<user name=
```

The attributes and their assigned value for the user are listed in this entry. WordPad indicates the end of the entry for each user with the line:

```
</user>
```

For reference, the first complete user record in the figure is highlighted in blue in Figure 113 on page 204.

For example, the admin user entry is displayed like this:

```
<user name="admin" uid="1"
   passwd="gxn1:bd76bfc690438c5f63a52d301f4ddef61483b351121e03cf310a092e"
   level="manage" passwordAgeLimit="0" passwordWarnLimit="0"
   accountAgeLimit="0" serviceState="IS"
   passwordExpirationTime="infinity" passwordChangeTime="2012-05-29 17:52:49"
   latestLoginTime="2012-05-30 21:38:14">
 <passHistory
   passwd="gxn1:5908fa4491d4f50c2139cb4b0dd4cf813a61411c8e4d1355f32ff064" />
   <portRange from="10001" to="10144" level="manage" />
   <portRange from="20001" to="20144" level="manage" />
</user>
```

All of the fields for a user's record are described in the table below.

For systems with the VPS feature (see “Virtual Private Switch (VPS)” on page 177), the “portPriv” field in this XML file will contain the value “enable” and the default port ranges for new users will default to the actual input and output port counts for the system. For systems without the VPS feature, each user will have the two port ranges shown below.

```
<portRange from="10001" to="19999" level="manage"/>
<portRange from="20001" to="29999" level="manage"/>
```

The range from "10001" to "19999" is the default for all possible input ports. The range from "20001" to "29999" is the default for all possible output ports. The default admin and madmin user accounts are also assigned these "all ports" port ranges. Without the VPS feature (portPriv=enabled), these ranges cannot be modified and each range must have the same port privilege assigned. In the example above, the port privilege level is "manage" for both ranges which is the default for the admin and madmin accounts. For non-VPS systems, the privilege level for these port ranges is normally set through either the ClickFlow Edit User window or the TL1 ED-USER-SECU command.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The following table describes the attributes of the XML file, and indicates whether or not each attribute can be modified directly in the XML file.

XML File Attribute	Description	Editable?
XML and Glimmerglass System Attributes		
xml version	The XML version used by the file.	No
userPrivDB version	The Glimmerglass user privilege database version.	No
portPriv	Indicates whether port privilege configuration is allowed on the Glimmerglass system. The value “disable” indicates that VPS is not licensed on the system and, therefore, the port privileges cannot be modified/imported (see the section “Virtual Private Switch (VPS)” in the *Glimmerglass ClickFlow™ Graphical User Interface Manual*).	No
User Account Attributes (displayed for each user configured on the system)		
name	The name of the user account (provided by the administrator when creating the user account). **NOTE**: This value cannot be modified for the admin user (all systems) nor the madmin user (for systems with the Glimmerglass Console feature).	Yes
uid	The system-defined value used to track the user account, independent of the account name. **NOTE**: If this value is modified, the user account would need to be deleted and recreated.	No
passwd	Encoded (hashed) password information. **NOTE**: If this value is modified, the password for the user account would be unknown and the user account would need to be deleted and recreated. Password hashes allow verification of a password but cannot be used to retrieve the decoded password.	No
level	The system-level privilege level assigned to the user account. The value can be modified to one of the four valid privilege level values: • "manage" • “modify" • "view" • "none" **NOTE**: This value cannot be modified for the admin user (all systems) nor the madmin user (for systems with the Glimmerglass Console feature).	Yes

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

XML File Attribute	Description	Editable?
passwordAgeLimit	Integer value representing the password aging interval value for the user account. The range of valid values is 0 to 999 where 0 indicates there is no limit on the password age (feature is disabled).	Yes
passwordWarn-Limit	Integer value representing the password change interval value for the user account. The range of valid values is 0 to 999 where 0 indicates there is no grace period to change the password (feature is disabled).	Yes
accountAgeLimit	Integer value representing the account aging interval value for the user account. The range of valid values is 0 to 999 where 0 indicates that there is no check on latestLoginTime and the account will not be place out-of-service if not used (feature is disabled).	Yes
serviceState	String value representing the account state of this user account. Values are IS (In-Service), IS-EXP (In-Service Expired), and OOS (Out-of-Service).	Yes
passwordExpira-tionTime	Displays the date-time when the user account will be set out-of-service if the password is not changed. **NOTE**: If password changes are not required for this account, the value will display as "infinity"	No
passwordChange-Time	Displays the date-time of the last password change for the user account. If no password change has occurred, the value will be displayed as "epoch"	No
latestLoginTime	Displays the date-time of the last login by user. If no login has occurred for the account, the value will display as "epoch"	No
passHistory	Hashes of the most recent 24 passwords (per passwd), 0 to 24 entries. Password hashes allow verification of a password but cannot be used to retrieve the decoded password.	No

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

XML File Attribute	Description	Editable?
Port-Level Privilege Attributes		
portRange from	The first port in the port range for which the user has port-level privileges. The input port and output port values must use the 5-digit format (such as 10008, 20009, etc.). For Switched VOA and PMU ports, use the **Reports > Port** menu option to retrieve port numbers. Note the following: • Multiple portRange entries can be included for each user to specify multiple port ranges and port-level privileges assigned to the user. • Each user may be assigned multiple input/output port ranges, and each of these port ranges may have a different port-privilege level. See Figure 113 on page 204 for an example of multiple portRange entries. • Multiple users can share port ranges, each having different port privileges and system privileges. • If a user does not have any port-level privileges, there will be no portRange entries for that user. This means that all port-level privileges for a user can be removed by deleting any portRange entries for that user in the XML file. This has the same effect as specifying a port-level privilege of “none” to the user. **NOTE**: Port ranges cannot be modified for the admin user (all systems), for the madmin user (for systems with the Glimmerglass Console feature), nor for systems not licensed for the VPS feature. The admin and madmin accounts default with port ranges of 10001 to 19999 and 20001 to 29999 for input and output port ranges, respectively.	Yes
to	The last port in the port range for which the user has port-level privileges. The input port and output port values must use the 5-digit format (such as 10008, 20009, etc.). For Switched VOA and PMU ports, use the **Reports > Port** menu option to retrieve port numbers. **NOTE**: Port ranges cannot be modified for the admin user (all systems), for the madmin user (for systems with the Glimmerglass Console feature), nor for systems not licensed for the VPS feature. The admin and madmin accounts default with port ranges of 10001 to 19999 and 20001 to 29999 for input and output port ranges, respectively.	Yes

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

XML File Attribute	Description	Editable?
level	The port-level privilege level assigned to the user for the specified port range. The value can be modified to one of the four valid privilege level values: • "manage" • “modify" • "view" • "none" **NOTE**: This value cannot be modified for the admin user (all systems) nor the madmin user (for systems with the Glimmerglass Console feature).	Yes

To summarize, the format for each user account record is shown below. The attributes that can be modified for user accounts (other than the admin and madmin accounts) are shown in italics. The value “SDV” indicates system-defined values that cannot be edited. The values allow for the password limit, account limit, and service state parameters are indicated as "IntVal" for integer value. The limits for these parameters are in the table above.

```
<user name="UserName" uid="SDV" passwd="SDV" level="system-level privilege"
    passwordAgeLimit="IntVal" passwordWarnLimit="IntVal"
    accountAgeLimit="IntVal" serviceState="state"
    passwordExpirationTime="SDV" passwordChangeTime="SDV"
    latestLoginTime="SDV"  >
  <passHistory passwd="SDV" />
  <portRange from="InPort#" to="InPort#" level="port-level privilege"/>
  <portRange from="OutPort#" to="OutPort#" level="port-level privilege"/>
 </user>
```

Considerations Before Editing the User Account XML File

Although most of the attributes in the XML are editable, there are several considerations to take into account before changing the XML attribute values.

Before editing the user account XML file for any Glimmerglass system, consider the following:

- Export the file just prior to editing. Do not use an "old" file as the time fields enumerated in the next bullet will have stale dates. Importing with stale dates may cause user accounts to be placed out-of-service.
- Do not modify the following parameters.
  - xml version
  - userPrivDB version
  - portPriv
  - uid

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

    - passwd
    - passwordExpirationTime
    - passwordChangeTime
    - latestLoginTime
- Each passHistory element may be entirely deleted but may not be otherwise modified.
- Importing a modified user account XML file will overwrite all existing user database entries, including user names and passwords.
    - Bear in mind that old user account XML files (exported in the past) may have old passwords for the users. Importing an outdated XML file will set the user passwords back to the previous values. It is advisable to export the current database prior to executing modifications to port-level privileges. It is advisable to make a backup copy of the exported current database.
- Port ranges are inclusive of all ports in the “from” and “to” range and must be separately performed for input and output ports. So, if the user will be given “View” privileges to input ports 1 through 10, “Modify” privileges for input ports 11 through 19, and then “View” privileges for input ports 20 through 30, three port range entries must be created.
- Observe the formatting shown in the Figure 113 on page 204. All modified parameters must be enclosed in double quotes and port range field must start with the < character and end with the /> characters.

Before editing a user account on Glimmerglass systems with the VPS feature, consider the following:

- Port-level privilege ranges can be configured by the following methods:
    - Exporting, editing, and importing the user account XML file via the ClickFlow User Management menu.
    - Editing user accounts directly via the TL1 interface, using the SET-PRIV-FIBER command to configure port ranges and privileges by user. The RTRV-PRIV-FIBER command can be used to view the privilege settings.
    - The Glimmerglass Console option provides a graphical user interface for configuring port ranges and privileges and is recommended if administering port-level privileges for multiple users and multiple switches.
- Port-level privileges (port ranges and port privileges) apply to both the ClickFlow and TL1 user accounts regardless of the interface used to set these privileges.
    - Exporting, editing, and importing the user account XML file via the ClickFlow User Management menu.
- The port-privilege level of "None" precludes the user from viewing the port (the port will be displayed in light grey in the ClickFlow GUI).
    - For connections, if the user has a higher privilege level than "View" for one of the ports in the connection, the user will have the capabilities of the higher priv-

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

ilege level for that connection. However, if the user, for example, breaks this connection, they will not be able to re-establish the connection.

Editing the User Account XML File

NOTES: Importing a previously exported and modified users.xml file is the ClickFlow-based method of apportioning ports for assignment of port-level privileges.

Port range and port-level privilege assignments can also be performed directly via the TL1 interface, without requiring an export, modification, and subsequent import. The TL1 method is suggested as a method of assigning port-level privileges if the user is uncomfortable with the XML file format. The Glimmerglass Console option is recommended if administering port-level privileges for multiple users and multiple switches.

Before modifying the user account XML file, review the previous section, “Considerations Before Editing the User Account XML File” on page 209.

To modify the user database XML file:

1. Open the Microsoft WordPad application.

2. Select **File > Open...** from the WordPad menu.
   WordPad displays the Open window, from to select the desired file.

3. In the Open window, select the value “All Documents (*.*)” from the “Files of type:” pull-down menu.

4. Navigate to the location of the user configuration XML file. (The default name for this file is “users.xml.”)

5. Select the XML file and click **Open**.
   WordPad will display the XML file (see Figure 113 for an example).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

6. Edit the user attributes as desired. See the table starting on page 206 for a description of the user attributes that can be edited in the XML file.

NOTES: Observe and maintain the file formatting (indentation).

New port range entries must be added as shown in Figure 113 on page 204 (each entry must start with “<“a end with “/>”) and must be indented appropriately.

All attribute values must be enclosed in double quotes (e.g. level="view")

Do not modify the fields indicated as not editable in table starting on page 206.

7. After the file is edited as desired, select **File > Save As...** and enter a new name for the edited file. (It is recommended that you do not overwrite the original exported users.xml file, in case you have made errors when updating the file.)

Once the user configuration file has been edited and saved, the XML file can be re-imported into the Glimmerglass system, so that the edited user settings are applied to the user accounts (see “Importing User Account Information” on page 197).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

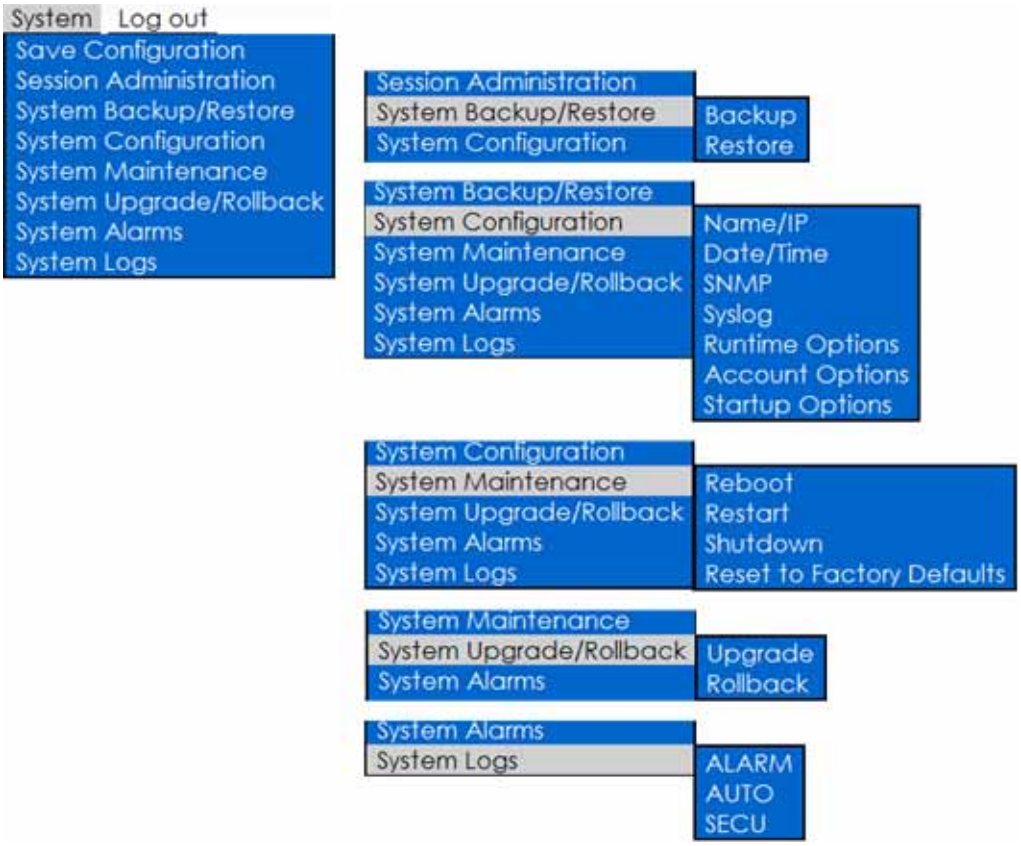
System

9

Overview

This chapter presents the configuration and maintenance operations supported under the **System** menu. The **System** menu options and the options supported under sub-menus are shown in Figure 114. Port and connection configuration is covered in Chapter 7, “Configure”. The configuration operations supported under the **System** menu govern the system itself (e.g., IP configuration, system name, NTP, SNMP, Syslog) or system parameters and system security policies.

Figure 114 System Menu (left) and Menu Option Sub-menus (right)



The table below describes the **System** menu options and provides the page numbers where the menu options are further detailed in this chapter.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description	Page
Save Configuration	Saves configuration changes to non-volatile memory. Configuration changes not saved will be lost upon a power cycle of the system; this does not include connections which are immediately saved to non-volatile memory. This menu option will be displayed only to users with a system-level privilege of Modify or higher. The section “Save Configuration” describes other methods by which to save configuration changes.	216
Session Administration	Opens the Session Admin window (Figure 115 on page 218), which displays the user name, IP address, and duration of all logged-in sessions for the system. System administrators may use this window to force a logoff for user sessions. This menu option will be displayed only to users with a system-level privilege of View or higher. Only users with the system-level privilege of Manage may force termination of sessions.	218
System Backup/Restore	The System Backup/Restore menu item provides the following sub-menu options: • Backup—Backup the system configuration to a system configuration XML file • Restore—Restore the system configuration from a system configuration XML file This menu option is displayed only to users assigned the system-level privilege of Manage.	219

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description	Page
System Configuration	The System Configuration menu item provides the following sub-menu options: • Name/IP—System name, description and Ethernet ports • Date/Time—Set date/time, or enable and configure NTP (Network Time Protocol) • SNMP—SNMP Trap Destinations (IP address and port) and SNMP Community Strings • Syslog—Syslog server IP addresses and logging level • Runtime Options—Autosave, connection restore, confirmation mode, connection mode, ports/row, etc. • Account Options—System account & password policies • Startup Options—TCP/UDP port numbers and SSL operation All sub-menu options are available only to users with the system privilege of Manage. Users with either the View or Modify system-level privilege may view only the configuration information under the **Name/IP** and **Date/Time** options. The other sub-menu items are not displayed. No sub-menu options are displayed to users with the system-level privilege of None.	225
System Maintenance	The System Maintenance menu item provides the following sub-menu options: • Reboot—Shutdown and reboot the system • Restart—Shutdown and restart the system application • Shutdown—Shutdown the system in preparation for power-off • Reset to Factory Defaults—Break all connections, clear the system configuration database and reboot This menu option is displayed only to users assigned the system-level privilege of Manage.	257
System Upgrade/Rollback	The System Upgrade/Rollback menu item provides the following sub-menu options: • Upgrade—Import and upgrade the system software • Rollback—Revert to the previous software version This menu option is displayed only to users assigned the system-level privilege of Manage.	259

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description	Page
System Alarms	Opens the Active System Alarms window which displays the contents of the Active Alarm table. This window may also be opened by left-clicking on the System Name in the Alarm Panel. When opened, all users may view active hardware and software alarms. Optical alarms for ports and connections will only be presented to users with View or higher privileges for the port(s) in alarm.	268
System Logs	The System Upgrade/Rollback menu item provides the following sub-menu options: • ALARM • AUTO • SECU The SECU log may only be viewed by users with a system privilege of manage. This option is not presented to other users. The ALARM and AUTO logs may be viewed by users with a port privilege of View or higher. For port records, the user will only see records for ports for which the privilege is at least View. All other records are not displayed.	276

Save Configuration

The **System > Save Configuration** menu option performs an immediate save of configuration changes to persistent memory (non-volatile memory). Configuration changes not saved will be lost upon a power cycle of the system. There are several methods by which to save configuration changes:

- **System > Save Configuration** menu option (see page 217)
- The **Reboot**, **Restart**, and **Shutdown** options from the **System > System Maintenance** sub-menu (see ”System Maintenance” on page 257)
- Autosave operation (see ”Autosave Enable” on page 244)
- WRT-DB command in TL1 (see the *Glimmerglass Transaction Language 1 Manual*)

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The following table lists the system operations that save files to non-volatile memory and the category of files saved by that operation.

Operation	Files Saved to Persistent Memory
Autosave every Autosave Delay period	Configuration files changed since the last save. Log files (TL1 AUTO and SECU log files) if they have not been saved in the last 24 hours.
ClickFlow Save Configuration	
TL1 WRT-DB with force=0	
ClickFlow Reboot, Restart, and Shutdown	Configuration files changed since the last save. Log files.
Maintenance Console Reboot, Restart, and Shutdown	
TL1 SYS-INIT Reboot, Restart, and Shutdown	
TL1 WRT-DB with force=1	All configuration files. Log files.

NOTE: Connection changes are persisted immediately, they are not governed by the above operations.

Saving Configuration Changes

Users with the system-level privilege of Modify or above can save the configuration to persistent memory. Perform the following steps to save the configuration:

1. Select **System > Save Configuration** from the Connection screen.
   A dialog box will appear upon completion of the configuration save.

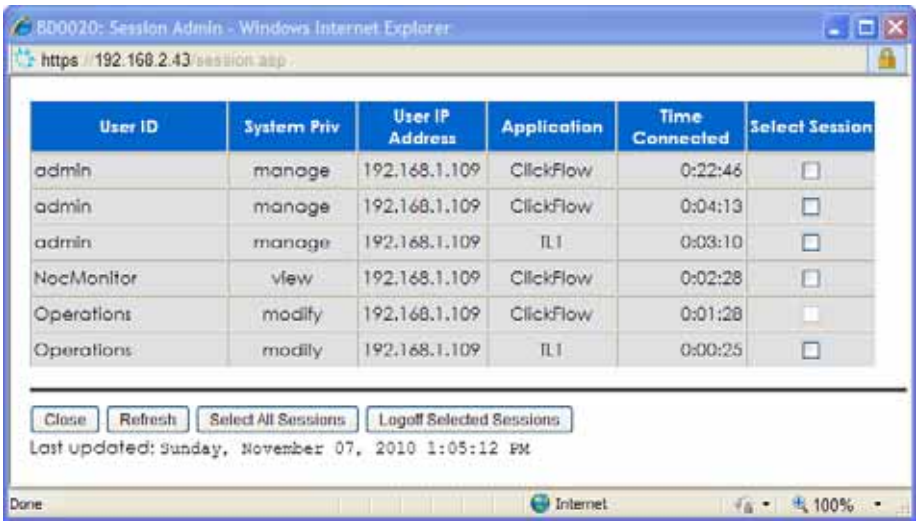
2. Click the **OK** button.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Session Administration

The **System > Session Administration** menu option opens the Session Admin window (Figure 115), which displays the user name, IP address, and duration of all logged-in sessions for the system. System administrators may use this window to force a logoff for user sessions.

Figure 115 Session Admin Window



The table below describes the fields and functions of the Session Admin window.

Field	Description
User ID	Lists the user name of each active user account on the system.
System Priv	The user account's system-level privilege.
User IP Address	The IP address of the computer used by the user to log into the system.
Application	The interface used by the user to log into the system.
Time Connected	The amount of time the user has been logged in to the system.
Select Session	Check box to select user account(s) for a logoff operation (using the **Logoff Selected Sessions** button described below).
Close	Closes the System Admin window.
Refresh	Updates the information displayed in the System Admin window.
Select All Session	Checks each of the check boxes for all of the user sessions displayed in the System Admin window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
Logoff Selected Sessions	Ends the user sessions of the selected user accounts. (Select individual user accounts by checking the **Select Session** check box for each user account, or select all of the displayed user sessions by clicking the **Select All Session** button.)

Terminating Sessions

Users with the system-level privilege of View or higher may view the current sessions. Only users with the system-level privilege of Manage may terminate sessions. Perform the following steps to terminate sessions.

1. Select the **System > Session Administration** menu option from the Connection screen menus. The Session Admin window (Figure 115 on page 218) will appear.

2. Click in the **Select Session** check box by each user session to be terminated, or alternatively click the **Select All Sessions** button to select all user sessions.

3. After all selections are made, click the **Logoff Selected Sessions** button.

4. Click the **Close** button to close the Session Admin window

System Backup/Restore

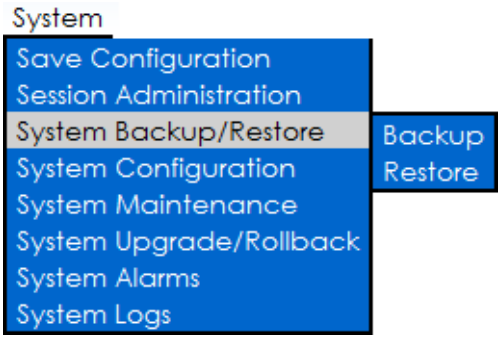
The **System > System Backup/Restore** sub-menu options (Figure 116) allow the user to backup/restore the system configuration to/from a system configuration XML file. Access to these options is only presented to users with the system-level privilege of Manage.

The system configuration may be backed up to an XML file and restored from an XML file via the ClickFlow, SNMP and TL1 interfaces. The ClickFlow web browser (HTTPS), TL1 (FTP), or SCP/SFTP or may be used to copy (export/import) the system configuration file to/from a Linux server or Windows PC.

The system configuration XML file includes identifying information such as: system name, serial number, when the file was created, by whom (user-id) and an optional user entered comment/description. The XML file also includes read-only information about the system (hardware features, licenses and embedded software version); the read-only information is not restored by Restore System Configuration.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

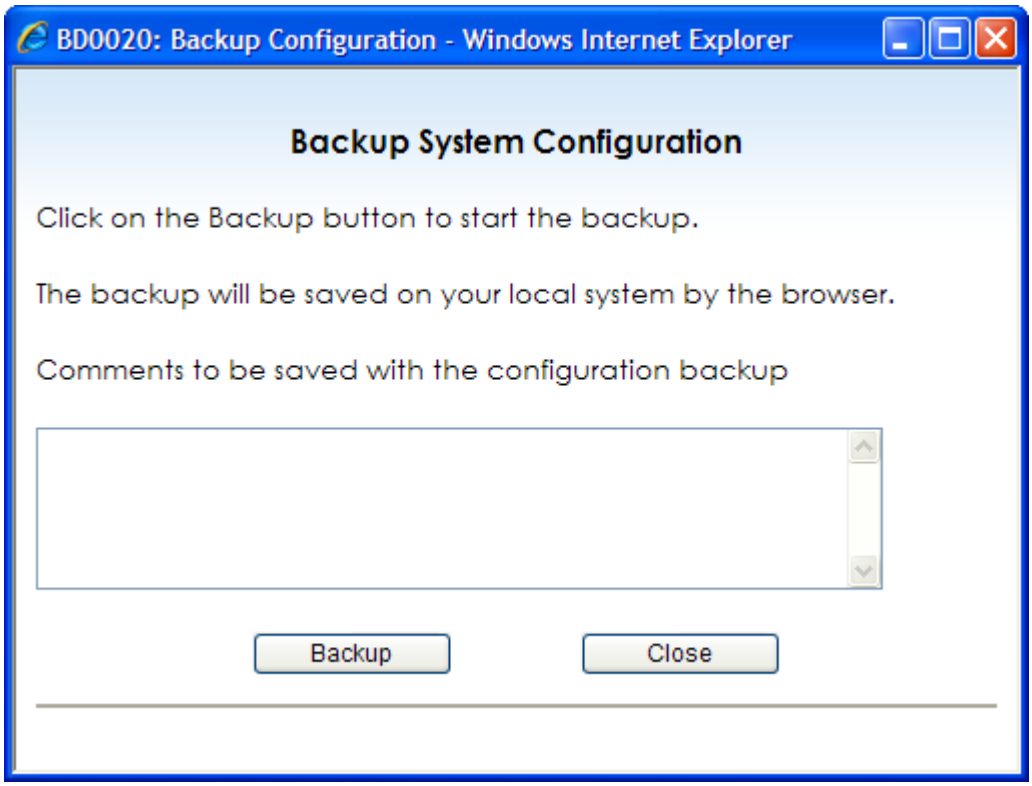
Figure 116 ***System > System Backup/Restore*** *Menu Options*



Backup

The **System > System Backup/Restore > Backup** menu option opens the Backup System Configuration (Figure 117), from which the system configuration may be backed up to a system configuration (backup) XML file and exported by a user with system-level privilege of Manage.

Figure 117 Backup System Configuration Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Backing up the System Configuration

Users with the system-level privilege of Manage may backup the system configuration to a system configuration XML file. Perform the following steps to backup the system configuration and export/download the system configuration file:

1. Select **System > System Backup/Restore > Backup** from the Connection screen to open the Backup System Configuration window (Figure 117 on page 220).

2. To enter a comment that will be included in the backup XML file, click in the comments entry box in the Backup System Configuration window and type a comment.

   NOTE: This optional comment is displayed by the Restore System Configuration window (Figure 118 on page 222)

3. Click the **Backup** button, a browser dependent File Download window opens.

4. From the File Download window, click **Save** to select a name and location to save the system configuration backup XML file.

Restore

The **System > System Backup/Restore > Restore** menu option opens the Restore System Configuration (Figure 118 on page 222), from which a system configuration (backup) XML file may be imported and restored by a user with system-level privilege of Manage.

If the **Restore All** checkbox is checked (the default) then the complete configuration is restored. However, the user may elect to restore selected sections of the configuration file by unchecking **Restore All** and checking one/more individual items, see Figure 119 on page 223.

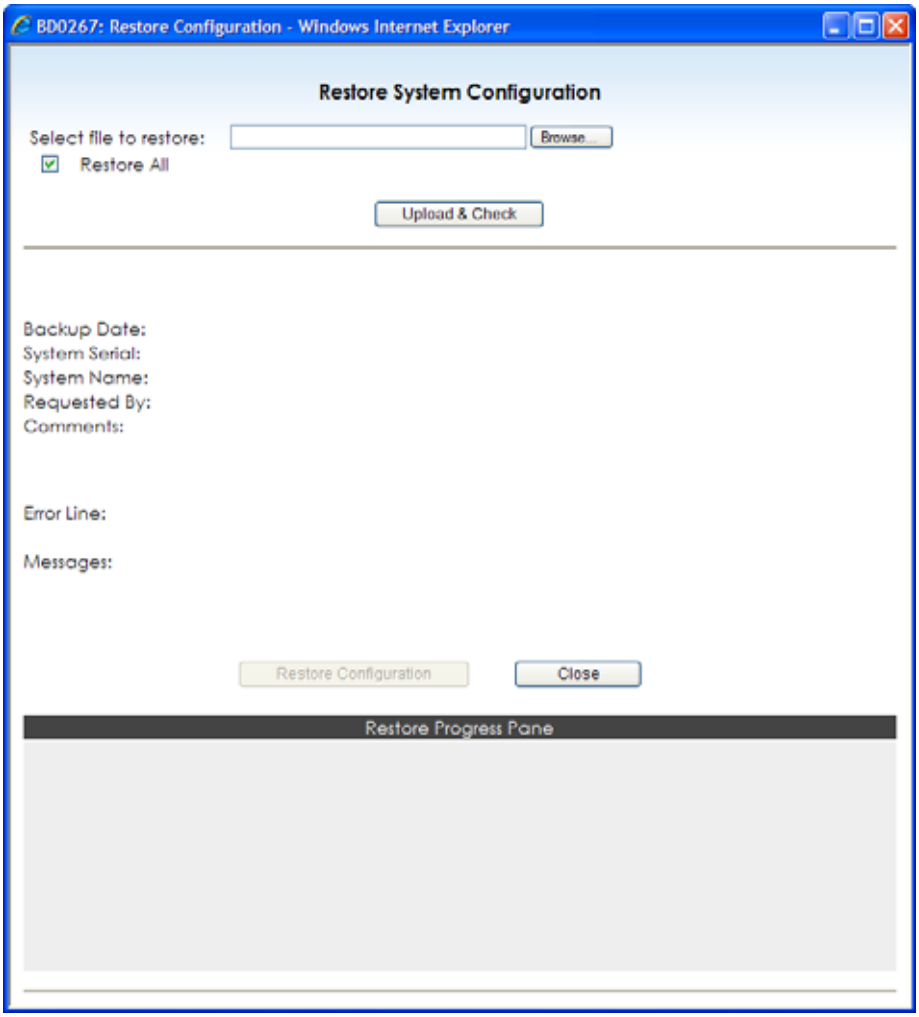
WARNING: Selective restoration should be used with caution in that there may be relationships between sections. For example a the signal threshold used by a port, or the user that made a connection.

If the restored system configuration revised the system network parameters (Ethernet IP address, gateway, etc.) the network parameter changes will not take effect until the next system reboot. Similarly if the applied configuration revised the startup parameters (TCP port numbers) the startup parameter changes will not take effect until the next system restart or reboot.

WARNING: Restore will change the system connections to those in the restored system configuration file, which are those at the time the system was backed up, so it may impact existing connections.

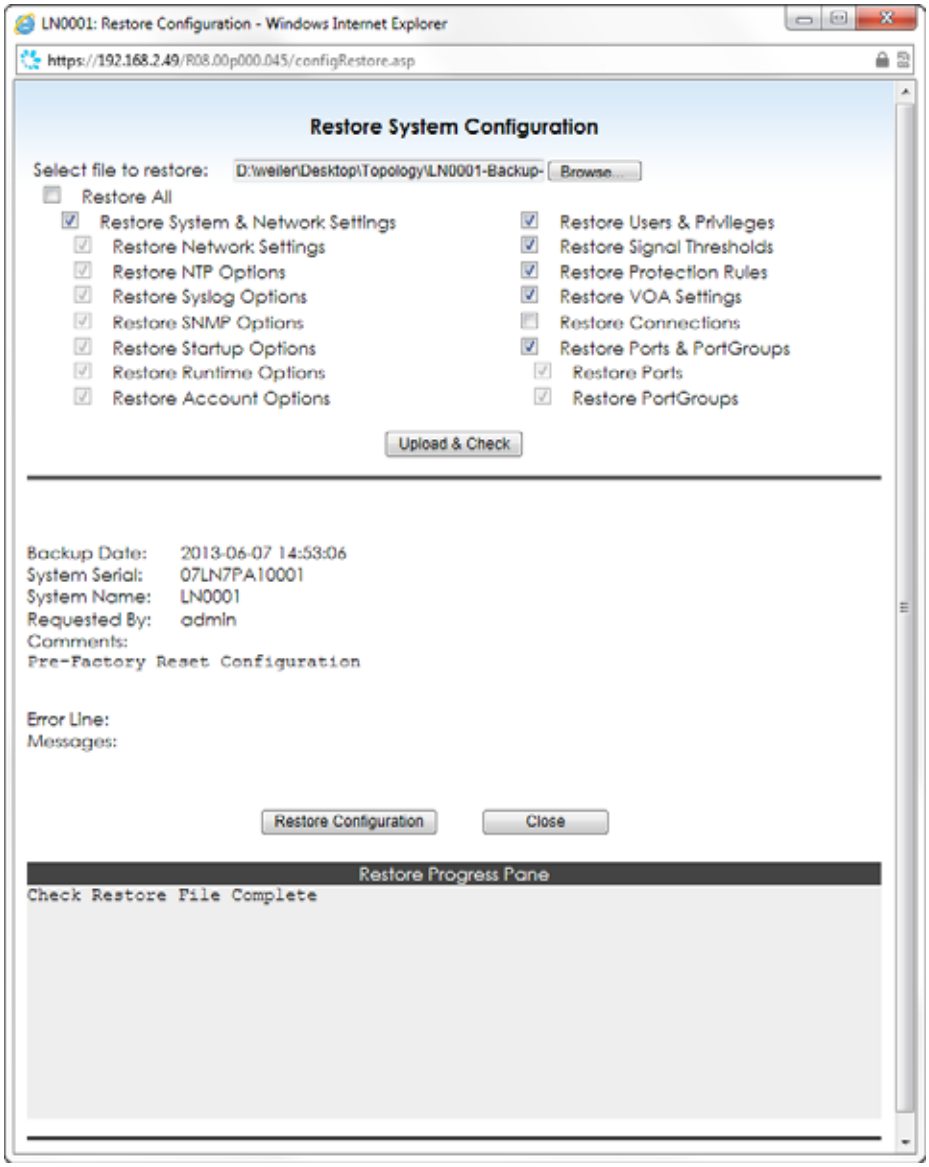
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 118 Restore System Configuration Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 119 Restore System Configuration Window—Selective Restoration



Restoring the System Configuration

Users with the system-level privilege of Manage may restore the system configuration from a system configuration (backup) XML file. Perform the following steps to import/upload the system configuration file and restore the system configuration:

1. Select **System > System Backup/Restore > Restore** from the Connection screen to open the Restore System Configuration window (Figure 118 on page 222).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

2. From the Restore System Configuration window, click the **Browse…** button to display the browser-dependent Choose File to Upload window.

3. Select a system configuration (backup) XML file and click the **Open** button.
   The name and location of the file is displayed in the Restore Configuration window.

4. Click the **Upload & Check** button.
   The file is uploaded and is checked, there are three check outcomes:
   - Error—The file is not a valid system configuration file, or it is a valid file but it is not applicable to this system. For example, the number of installed ports does not match. An error message is displayed and the **Restore Configuration** button remains disabled.
   - Warning—The file is a valid system configuration file (its configuration is applicable to this system), but the system serial numbers do not match. Backup file information is displayed (backup date, system serial number, system name, backup user ID, backup comments), a warning message is displayed, and the **Restore Configuration** button is enabled. This situation may occur if a system has failed and is being replaced by an identical replacement system.
   - Valid—The file is a valid system configuration file (its configuration is applicable to this system) and the system serial numbers match. Backup file information is displayed (backup date, system serial number, system name, backup user ID, backup comments), a success message is displayed, and the **Restore Configuration** button is enabled.

5. (Optionally) For selective configuration restoration, uncheck **Restore All** and selectively check the configuration sections to be restored (Figure 119 on page 223 is an example where all but the connections are restored).

6. Click the **Restore Configuration** button.
   Restore will proceed and progress messages are displayed in the Restore Progress Pane. Restoration usually takes 5-10 seconds.

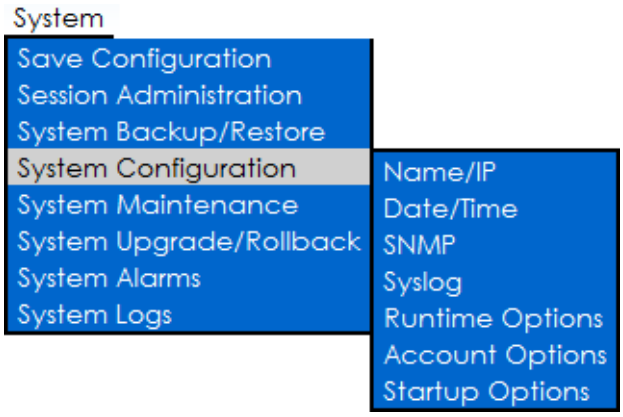
NOTE: If the restored system configuration revised the system network parameters (Ethernet IP address, gateway, etc.) the network parameter changes will not take effect until the next system reboot. Similarly, if the applied configuration revised the startup parameters (TCP port numbers) the startup parameter changes will not take effect until the next system restart or reboot.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

System Configuration

The **System > System Configuration** menu options (Figure 120) allow the user to set parameters governing system-wide operational behavior. Users with the system-level privilege of View or higher may examine the system configuration. Only users with the system-level privilege of Manage may modify the system configuration.

Figure 120 ***System > System Configuration*** *Menu Options*



The System Configuration menu options are described in the following sections:

Menu Option	Description	Page
Name/IP	Opens the System Name and IP Configuration window, from which the system name, description, login warning message and Ethernet ports (IP address, mask and gateway) may be configured.	226
Date/Time	Opens the System Date/Time Configuration window, from which the system's date/time can be changed, or NTP (Network Time Protocol) may be enabled and NTP servers IP addresses configured.	231
SNMP	Opens the SNMP Configuration window, from which SNMP v2c Trap Destinations (IP address and port) and SNMP v1/v2c Community Strings may be configured.	237
Syslog	Opens the System Syslog Configuration window, from which the syslog servers (IP addresses) and logging level may be configured.	240
Runtime Options	Opens the Runtime Options window, from which the preferences can be configured for Autosave, Connection Restore, Performance Switch Throttle, Event Reporting Mode, and Connection Configuration Settings.	243

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description	Page
Account Options	Opens the Account Options window, from which the user can configure system parameters supporting password complexity policy and password change policy, as well as system-wide policies for intrusion detection/reporting and no-activity timeout	249
Startup Options	Opens the Startup Options window, from which the system TCP/UDP port numbers and SSL operation of the system can be configured.	254

Name/IP

Users with the system-level privilege of View or higher may open the System Name and IP Configuration window (Figure 121). In this window, users with the system-level privilege of Manage can configure the system's name, description, login warning message and Ethernet ports (IP address, mask and gateway).

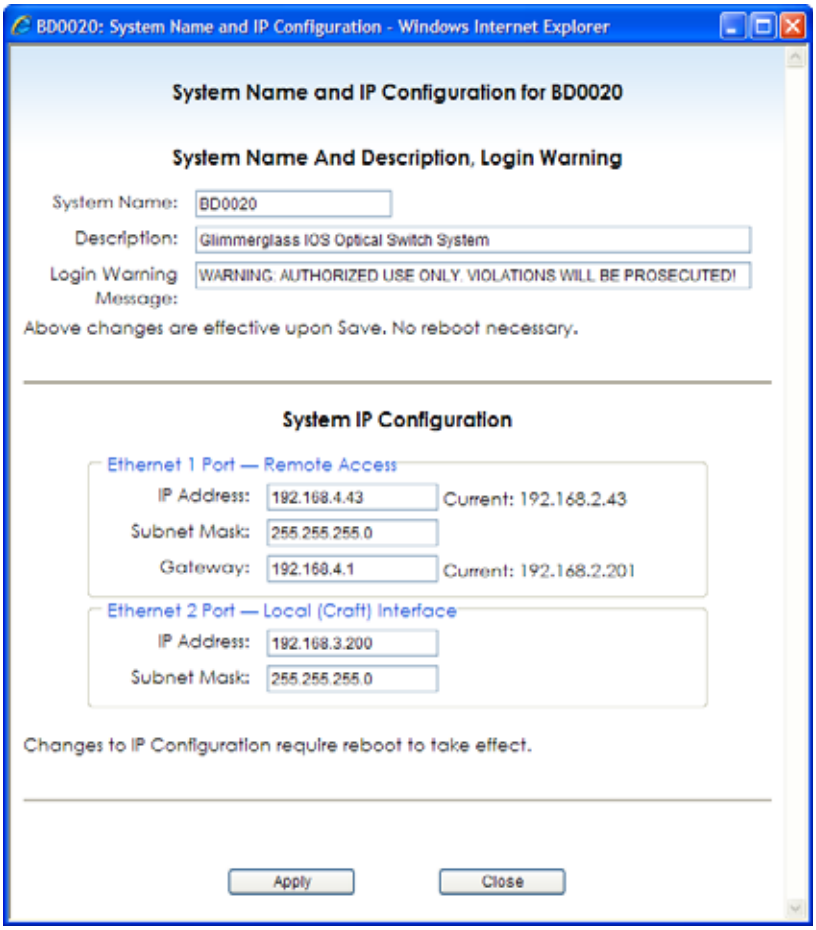
The current system name is displayed in the Alarms display. The factory default for the system switch name and system host name are the same, and are derived from the system's serial number. The switch name may be revised by this option or by the TL1 SET-SID command (see the *Glimmerglass Transaction Language 1 Manual*). The host name may be independently revised by the Maintenance Console **Configure Network** selection (see the *Glimmerglass System Installation and Maintenance Guide*) or by the TL1 ED-NE-GEN command.

At the time of the system installation, the system IP address may be configured via:

- Glimmerglass Maintenance Console, using a Notebook PC with a terminal emulator, with a serial cable connected to the system's RS232 port (see the *Glimmerglass System Installation and Maintenance Guide*).
- ClickFlow GUI, using a Notebook PC, with an RJ45 Cat5 cross-over cable connected to the system’s Ethernet 2 port.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 121 System Name and IP Configuration Window



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The table below describes the fields and functions of the System Name and IP Configuration window.

Field	Description
System Name and Description, Login Warning	
System Name	The logical name of the system, also known as the TL1 system ID (SID). The factory default for the system switch name and system host name are the same, and are derived from the system's serial number. Changing the system name does not change the system host name and vice-versa. • Maximum length is 20 characters. • Characters may be alphanumeric and may also include the period (“.”), dash ("-"), and underscore ("_") characters. • Entry of non-supported characters is blocked. • The logical name is updated immediately when the **Save** button is clicked.
Description	The description is provided for customer use in adding a short description regarding the system. The description is displayed in the Login screen (see Figure 3 on page 5). The factory default value is shown in Figure 121. • Maximum length is 64 characters.
Login Warning Message	The login banner is provided for presenting a banner in the Login screen, such as a login warning (see Figure 3 on page 5). The factory default value is shown in Figure 121. • Maximum length is 64 characters.
System IP Configuration	
Ethernet 1 Port	Ethernet 1 is used for remote access to the system. The following fields provide information for the Ethernet 1 port: • IP Address—System IP address (IPv4) in dotted decimal notation. The factory default value is 192.168.2.200 • Subnet Mask—IP subnet mask in dotted decimal notation • Gateway—IP address of the subnet gateway/router in dotted decimal notation.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
Ethernet 2 Port	Ethernet 2 is used for local network craft access to the system. The following fields provide information for the Ethernet 2 port: • IP Address—IP address (IPv4) in dotted decimal notation. This must not be on the same subnet as Ethernet 1. The factory default value is 192.168.3.200. • Subnet Mask—IP subnet mask in dotted decimal notation **NOTE**: Older Glimmerglass systems have only a single Ethernet port (Ethernet 1). For these systems, the Ethernet 2 port configuration will not be displayed.
Buttons	
Apply	Saves to the database all modifications to the fields. **NOTE**: In case there is an error in applying the updates, an error message will appear above the **Apply** button. See “Error Messages in the System Name and IP Configuration Window” on page 230.
Close	Closes the window. If closed without save, cancels all modifications.

Changing the System Name and IP Configuration

Users with the system-level privilege of Manage may modify the system name and IP configuration. Perform the following steps to configure the system name and IP:

1. Select **System > System Configuration > Name/IP** from the Connection screen to open the System Name and IP Configuration window (Figure 122 on page 230).

2. Select and modify the fields as required.
   Users with the system-level privilege of Manage may modify the switch parameters. All fields may be modified and saved individually or concurrently.

3. After all changes are made click the **Apply** button, or click the **Close** button to cancel the configuration changes and close the window.
   If the modifications are successful, a "Changes saved successfully" message will be displayed for five seconds directly above the **Apply** button. If the data entered contains a error, a descriptive error message will displayed for five seconds above the **Apply** button.

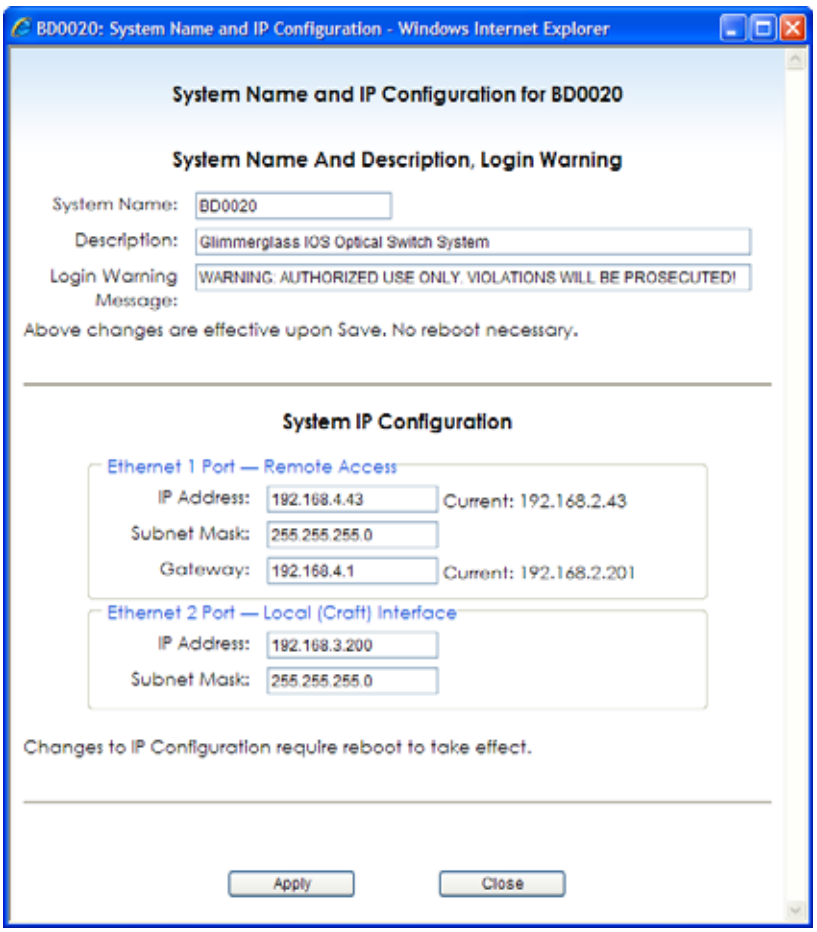
4. Click the **Close** button to close the System Name and IP Configuration window.

Changes to the system name, description, and login warning messages are in effect immediately after the **Apply** button is clicked (as indicated by the text in the window).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Changes to the system IP configuration require a reboot to take effect after the edits have been saved. Help text in the window indicates this requirement as well. When the system IP or system name information is updated and saved, the system will change the window display to show the current in-use value next to the modified field to indicate that the reboot required to complete the change has not been completed. This effect as well as the status message area location above the **Apply** button are shown in Figure 122. In this figure, the Ethernet 1 IP address and gateway have been modified and the "Current" values are displayed next to the configured values. After a reboot, the current values will disappear as the database and memory values will match.

Figure 122 System Name and IP Configuration Window Showing Current and Saved Values



Error Messages in the System Name and IP Configuration Window

If incorrect data is entered, the System Name and IP Configuration window displays the following error messages above the **Apply** button:

NOTE:	These messages appear only after the user clicks **Apply.**

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- If the Ethernet 1 IP address, subnet mask or gateway has an invalid format, then one of following error messages is displayed:
  - IP Address (Port 1) not valid
  - Subnet Mask (Port 1) not valid
  - Gateway (Port 1) not valid
- If the Ethernet 2 IP address or subnet mask has an invalid format, then one of following error messages is displayed:
  - IP Address (Port 2) not valid
  - Subnet Mask (Port 2) not valid

When the error message appears, the cursor is automatically placed in the field where the error was detected.

Only one error is reported in the error message. If multiple data entry errors exist, the next error will be listed in the error message once the user corrects the first error and clicks **Apply**.

Date/Time

The Glimmerglass system date and time are in UTC. The time zone is not configurable. The system date and time may be set in the following ways:

- Automatically via NTP (see ”Configuring NTP Operation” on page 233)
- Manually via the ClickFlow GUI (see ”Setting the Date/Time for the Internal Clock” on page 235)

Users with the system-level privilege of View or higher may open the System Date/Time Configuration window (Figure 123). In this window, users with the system-level privilege of Manage can configure the system's date/time, or can enable NTP (Network Time Protocol) and configure NTP servers IP addresses.

NOTES:	The factory default date/time configuration is Internal Clock with no NTP Server IP addresses configured. If the system date and time are set manually, the internal clock will slowly drift over time. Because of this, the system time should be periodically corrected via the application interfaces.

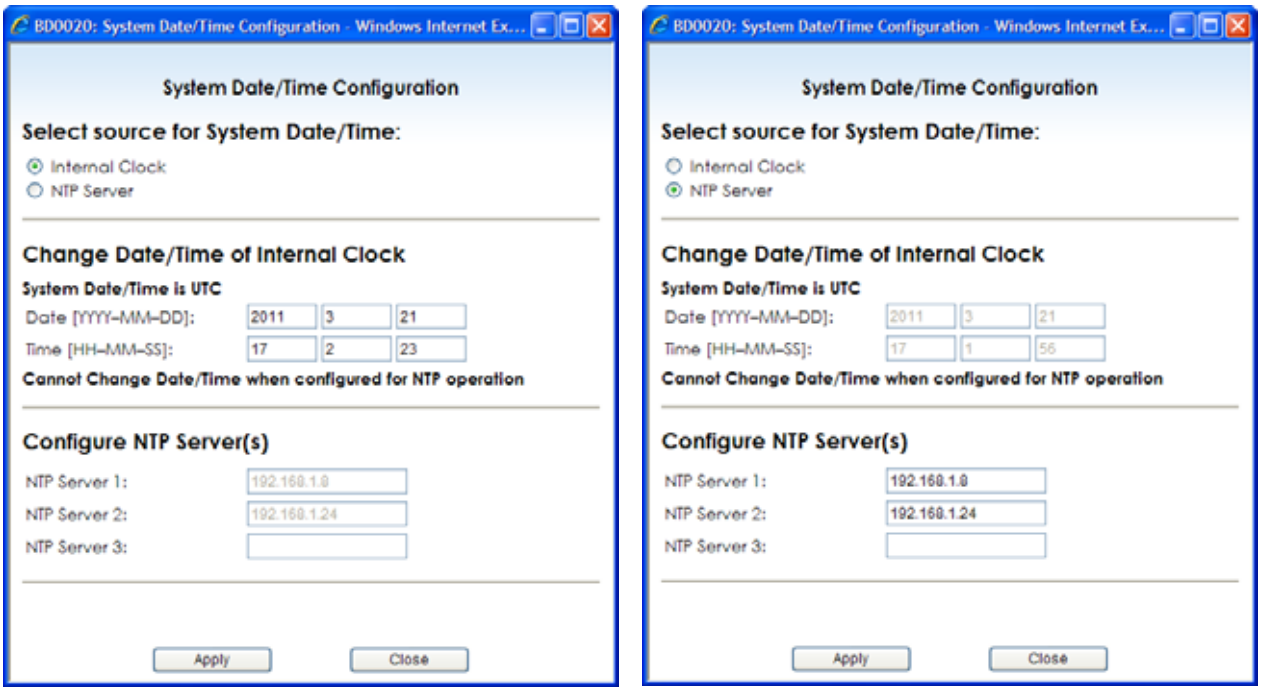
When NTP is enabled the system is an NTP Client that accesses up to three NTP Servers via the (Network Time Protocol). The system NTP client does not support DNS hence the NTP Server addresses are specified as IP addresses versus names or NTP pool names.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 123 shows two examples of the ClickFlow System Date/Time Configuration window, which is accessed through the System Menu (**System > System Configuration > Date/Time**). The left picture shows the window when the system is configured without an external time reference source (Internal Clock) and the right picture shows the window when the system is configured for NTP operation.

The two views illustrate that the fields available to be modified in the window are contingent upon which source is selected (Internal Clock or NTP Server).

Figure 123 System Date/Time Configuration Window Examples



The following table describes the fields in the **System Date/Time Configuration** window.

Field	Description
Select source for System Date/Time:	This area consists of two radio boxes labeled "Internal Clock" and "NTP Server," and this selection controls whether the user may configure the date/time for the internal clock directly, or whether the user can configure NTP Servers for the system to use as references for the internal clock. • When **Internal Clock** is selected, the **Change Date/Time of Internal Clock** section will allow the date and time to be set directly and the **Configure NTP Server(s)** section will be dimmed (not modifiable). • When **NTP Server** is selected, the **Configure NTP Server(s)** section will allow NTP Server IP addresses to be entered and the **Change Date/Time of Internal Clock** section will be dimmed (not modifiable).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Field	Description
Change Date/Time of Internal Clock:	This area provides data entry boxes to set the date and time. Only UTC date/time should be entered; the format for time entry is based upon a 24 hour clock. A separate box is provided for each field. If incorrect data is entered, an error message is displayed in the window above the **Apply** button. The initial values presented in these boxes represent the date and time at which the window was opened.
Configure NTP Server(s):	This area supports the configuration of up to three NTP Servers. Enter the IP address of the NTP server in the text box to the right of the NTP Server labels. The IP address must be in dotted-decimal notation. Glimmerglass does not support DNS look-up, so server names are not permitted. If incorrect data is entered, an error message is displayed in the window above the **Apply** button.
Buttons	
Apply	Once changes are made to the configuration, the **Apply** button is used to affect and save the changes. The following messages will appear above the **Apply** button shortly after operating the button. • **Using Internal Clock**—This message will appear when clicking the **Apply** button with the **Internal Clock** radio button selected. Using the **Apply** button without having first modified the date or time fields will not change the time. • **NTP Started**—This message will appear when clicking the **Apply** button when the NTP Server radio button is selected. Using the **Apply** button without making changes to IP addresses for the NTP servers will stop and restart the NTP service using the existing NTP Server IP addresses. **NOTE**: If there is an error in applying the updates, an error message will appear above the **Apply** button. See “Error Messages in the System Date/Time Configuration Window” on page 236.
Close	Closes the window. If the window is closed without applying the updates, all modifications in the window are cancelled.

Configuring NTP Operation

Configuring the system for NTP operation entails using the **System Date/Time Configuration** window to select the **NTP Server** as the system time source and to configure one to three NTP Servers as time source targets. The Glimmerglass system does not support DNS look-up, so the NTP Server IP addresses must be entered in dotted-decimal format (names are not supported).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Note the following about configuring the system for NTP:

- When NTP operation is enabled, the system date/time cannot be set directly from any other interface (Maintenance Console, SNMP, or TL1). An error message indicating NTP operation is in effect will be returned.
- When NTP is enabled, events are issued to the Glimmerglass Console to inform of the NTP configuration and the starting of the NTP service. Corresponding entries are placed in the system's AUTO log.
- The NTP Server IP addresses cannot be validated at entry.
- An alarm will be issued within ten minutes if synchronization cannot be established with any of the server IPs entered.
- An event will be issued and recorded in the AUTO log when synchronization is established with at least one NTP server.
- If communication to all NTP servers is lost, an alarm will be generated along with a corresponding AUTO log event. If this situation clears itself, an alarm clear event will be issued and a the AUTO log will be updated with an entry indicating synchronization is successful.
- When the time change (from current time) is large, the system should be restarted or rebooted. Neither activity affects traffic.
- When the time change forward exceeds the no activity timeout, users will be automatically logged out and the Session Closed screen will be displayed. The Session Closed screen provides a link that may be used to return to the Login Screen to sign in again.

A user with system-level privilege of Manage may configure the system for NTP operation, as described in the following steps:

1. Open the **System Date/Time Configuration** by selecting **System > System Configuration > Date/Time** from the Connection screen menus (Figure 123 on page 232).

2. Click on the **NTP Server** radio button (if not already enabled).

3. In the input box to the right of the **NTP Server 1** field, enter an IP address for an NTP server or modify/delete an existing IP address entry. The NTP server IP address entered must be accessible by this system (internal network or through gateway).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE: ClickFlow will not allow all three IP addresses to be deleted. This will also cause an error message if NTP Server operation is enabled. When NTP Server Operation is disabled, the previous NTP Server IPs configured will remain. If NTP Server operation is re-enabled by selecting the NTP Server radio button and not changing IP configuration, the system will start the NTP service using the existing NTP Server IP addresses.

4. Repeat step 3 for the **NTP Server 2** and **NTP Server 3** fields as required.

5. After all changes are made, click the **Apply** button, or click the **Close** button to cancel the changes and close the window.

   The message "NTP Started" will appear above the **Apply** button to confirm that the NTP service has been started if the IP addresses are correctly formatted. If incorrectly formatted, an error indicating location/problem with the entered data will be presented. Correct the error and click **Apply** again.

6. Click the **Close** button to close the window.

NOTES: When NTP operation is enabled, the system date/time cannot be set directly from any other interface (Maintenance Console, SNMP, or TL1). An error message indicating NTP operation is in effect will be returned.

Configuring NTP posts events to the Glimmerglass Console for the configuration and starting of the NTP service. Corresponding entries are placed in the systems AUTO log.

The NTP Server IP addresses cannot be validated at entry. An event will be posted when synchronization is established, or has not been established within ten minutes. Similarly subsequent loss and restoration of synchronization will post events.

Setting the Date/Time for the Internal Clock

A user with system privilege of Manage may change the system date/time. To set the date and time for the system, perform the following steps:

1. Open the **System Date/Time Configuration** by selecting **System > System Configuration > Date/Time** from the Connection screen menus (Figure 123 on page 232).

   When the window opens, the date and time displayed will be the UTC time from the internal clock as of the time the request was made to open the window. The "Last Updated" time shown at the bottom of the browser reflects the client's local time (offset from UTC based upon the computer's time zone setting).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

2. Click on the **Internal Clock** radio box (if not already enabled).

3. In the input boxes to the right of the **Date [YYYY-MM-DD]** field, enter the year (YYYY), month (MM), and day (DD) appropriate for the UTC date. Possible values:
   - Year: Current 4-digit year
   - Month: 1-12
   - Day: 1-31

NOTE: Always enter the UTC date/time.

4. In the input boxes to the right of the **Time [HH-MM-SS]** field, enter the UTC time as hours (HH), minutes (MM), and seconds (SS) appropriate for the UTC time. Possible values:
   - Hour: 00-23
   - Minute: 0-59
   - Second 0-59

5. After all changes are made, click the **Apply** button, or click the **Close** button to cancel the changes and close the window.

   The message "Using Internal Clock" will appear above the **Apply** button to confirm the change. If incorrectly formatted, an error indicating location/problem with the entered data will be presented. Correct the error and click **Apply** again.

6. Click the **Close** button to close the window.

NOTES: If the system was previously configured for NTP Server operation, selecting the **Internal Clock** radio box and clicking the **Apply** button will disable NTP operation and the system time will not change. Alternatively, the date/time may be changed concurrent with this operation.

An event recording the date/time change will be generated and the system AUTO log will be updated with an entry for this change.

Error Messages in the System Date/Time Configuration Window

If incorrect data is entered, the System Date/Time Configuration window displays the following error messages above the **Apply** button:

NOTE: These messages appear only after the user clicks **Apply.**

- For errors in the NTP Server section:
  - Bad IP Address in Primary NTP Server IP Address!
  - Bad IP Address in Secondary NTP Server IP Address!
  - Bad IP Address in Tertiary NTP Server IP Address!

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- For errors in the Date/Time section:
  - Hours of time (hh): Value out of range [0 , 23]
  - Minutes of time (mm): Value out of range [0 , 59]
  - Seconds of time (ss): Value out of range [0 , 59]
  - Day of date (dd): Value out of range [1 , 31]
  - Month of date (mm): Value out of range [1 , 12]
  - Please enter date in YYYY-MM-DD format

When the error message appears, the cursor is automatically placed in the field where the error was detected.

Only one error is reported in the error message. If multiple data entry errors exist, the next error will be listed in the error message once the user corrects the first error and clicks **Apply**.

SNMP

The **System > System Configuration > SNMP** menu option opens the SNMP Configuration window (Figure 124), from which SNMP v2c Trap Destinations (IP address and port) and SNMP v1/v2c Community Strings may be configured by a user with system-level privilege of Manage. Users with the system-level privilege of View or higher may examine the SNMP configuration.

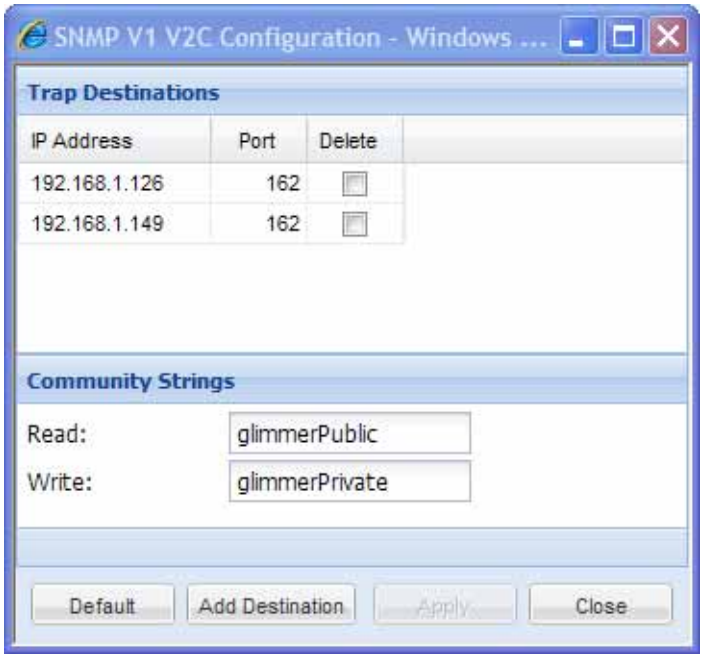
The ClickFlow SNMP Configuration window is provided for basic management of SNMP v2c trap target addresses and SNMP v1/v2c community strings; the window only operates on SNMP table rows with the following attributes:

SNMP Table	Attribute	Value
snmpTargetAddrTable	snmpTargetAddrName	*<ipaddress>/<port>* For example: "192.168.1.149/162"
	snmpTargetAddrTagList	"ggV2NotifyProfile"
	snmpTargetAddrParams	"ggV2TargetProfile"
snmpCommunityTable	snmpCommunityIndex	"glimmerPublic" or "glimmerPrivate"
	snmpCommunitySecurityName	"glimmerPublic" or "glimmerPrivate"

For management of SNMP snmpTargetAddrTable/snmpCommunityTable rows that do not meet the above criteria, use SNMP v3. SNMP v3 USM/VACM may used to configure multiple SNMP community strings each with different access views. See the *Glimmerglass Intelligent Optical System SNMP User Manual* for more information.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 124 SNMP Configuration Window



The table below describes the fields in the SNMP Configuration window.

Element	Description
Trap Destinations Section	
IP Address column	Trap Destination IP Address; existing IP addresses may be revised
Port column	Trap Destination port number; existing port numbers be revised
Delete column	Check the checkbox to delete the corresponding row when Apply is selected
Community String Section	
Read	SNMP v1/v2c read-only community string (password) for usmUserName glimmerPublic
Write	SNMP v1/v2c read/write community string (password) for usmUserName glimmerPrivate
Buttons	
Default button	Set the read and write community strings to their default values: • glimmerPublic for usmUserName glimmerPublic • glimmerPrivate for usmUserName glimmerPrivate

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Add Destination button	Add a new trap destination row with default values: • IP Address: 0.0.0.0 Revise this value before clicking **Apply** • Port: 162
Apply button	Save the trap destination and community names changes.
Close button	Close the window; cancel any changes that have not been applied.

Changing SNMP v2c Trap Destinations (Target Addresses)

Users with the system-level privilege of Manage may change the SNMP configuration. Perform the following steps to change the SNMP v2c trap destinations:

1. Select **System > System Configuration > SNMP** from the Connection screen to open the SNMP Configuration window (Figure 124 on page 238).

2. To add a new trap destination address:
   - Click on the **Add Destination** button
   - A new Trap Destinations row is inserted with IP address value 0.0.0.0, port value 162, and the cursor is in the IP address field.
   - Revise the IP address from 0.0.0.0 to the desired value.
   - Optionally click on the new row's port number and change it to the desired value.

   NOTES: An invalid IP address or port number is underlined in red.
   Changed fields are marked by a red triangle in the top left corner.

3. To delete an existing trap destination, click (check) the check box in the Delete column by the destination to be deleted.

4. To revise an existing trap destination IP address or port number, click on the IP address or port number and change it to the desired value.

5. After all the changes are made click on the **Apply** button to apply the changes, or click on the **Close** button to cancel the changes and close the window.

   NOTE: If the SNMP Target Address table contains the maximum number of ten entries then adding a new trap destination will be rejected with error message "SNMP Configuration Trap Destination Add Error". There may be less than 10 entries displayed in the SNMP Configuration window because the latter only displays rows that meet the criteria listed in the table at the beginning of this section.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Changing SNMP v1/v2c Community Strings

Users with the system-level privilege of Manage may change the SNMP configuration. Perform the following steps to change the SNMP v1/v2c community strings:

1. Select **System > System Configuration > SNMP** from the Connection screen to open the SNMP Configuration window (Figure 124 on page 238).

2. To change the read or write community string, click on the community string and change it to the desired value.

3. To default the read and write community strings, click on the **Default** button

4. After all of the changes are made, click on the **Apply** button, or click on the **Close** button to cancel the changes and close the window.

Syslog

The **System > System Configuration > Syslog** menu option opens the Syslog Configuration window (Figure 125 on page 241), from which Syslog destinations (IP address) and Syslog logging level may be configured by a user with system-level privilege of Manage. Users with the system-level privilege of View or higher may examine the Syslog configuration.

NOTE:	The Syslog protocol uses UDP port 514 for client to server log messages. The packet payload is unencrypted plain text which can include user names, client and system IP addresses. Hence, transmission over non-secure networks is not advised.

Up to three external Syslog Destinations (Syslog server IP addresses) may be configured. When multiple Syslog server IP addresses are specified, the log messages are posted to each of the servers. The latter Syslog servers may in turn be configured to forward the messages to other Syslog servers

The Syslog logging service level may be:

- OFF—Do not post any log messages to the Syslog servers.
- AUTO—Post all but security log messages to the Syslog servers (post messages that are logged to the TL1 AUTO log). These include user actions that change the system configuration, alarm events, and advisory events. The latter excludes actions and events that are related to security, which are posted to the SECU log.

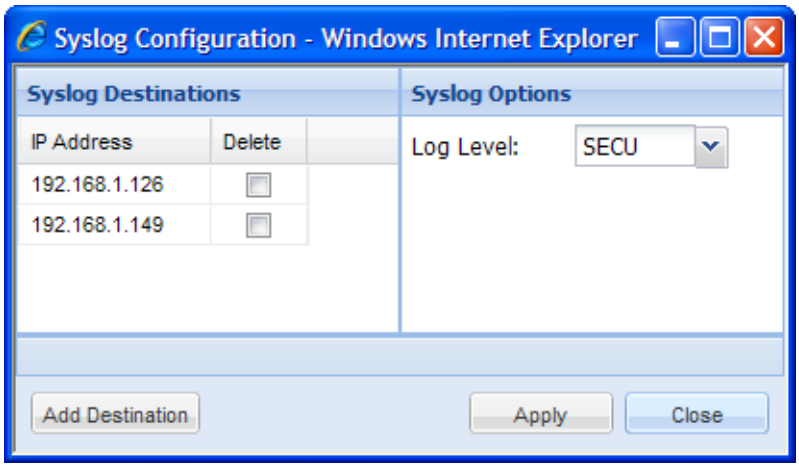
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- SECU—Post all log messages to the Syslog servers (post messages that are logged to the TL1 SECU log and also messages that are logged to the AUTO log).

The Syslog message priority is composed of a severity code and facility code:

- Severity=Critical(2)—A critical/major alarm message; the text in the message specifies the alarm severity (critical or major)
- Severity=Notice(5)—A minor alarm message; the text in the message specifies the alarm severity (minor)
- Severity=Informational(6)—An informational message (configuration change or advisory event) or an alarm clear.
- Facility=User(1)—All messages are posted by the system switch "application", versus the Linux Operating System, hence the messages are categorized by SYSLOG as "user".

Figure 125 Syslog Configuration Window



The table below describes the elements in the SNMP Configuration window:

Element	Description
Syslog Destinations Section	
IP Address column	Syslog destination IP Address. Existing IP addresses may be revised.
Delete column	Check the checkbox to delete this row when the **Apply** button is clicked.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Syslog Options Section	
Log Level	Select logging level: • OFF—Do not post any log messages to the Syslog servers • AUTO—Post all but security log messages to the Syslog servers • SECU—Post all log message to the Syslog servers
Buttons	
Add Destination button	Add a new Syslog destination row: • IP Address: 0.0.0.0 Revise this value before clicking **Apply**.
Apply button	Save the Syslog destination and log level changes.
Close button	Close the window; cancel any changes that have not been applied.

Changing Syslog Configuration

Users with the system-level privilege of Manage may change the Syslog configuration. Perform the following steps to change the Syslog destinations and/or Syslog logging level:

1. Select **System > System Configuration > Syslog** from the Connection screen to open the Syslog Configuration window (Figure 125 on page 241).

2. To add a new Syslog destination address:
   a. Click on the **Add Destination** button.
   A new Syslog Destinations row is inserted with IP address value 0.0.0.0, and the cursor is in the IP address cell.
   b. Revise the IP address from 0.0.0.0 to the desired value.

NOTES: The Add Destination button will be disabled if the Syslog Destinations table already contains the maximum of three destinations.

Invalid IP addresses are underlined in red.

Changed fields are marked by a red triangle in the top left corner

3. To delete an existing Syslog destination address, click (check) the check box in the Delete column by the address to be deleted.

4. To revise an existing Syslog destination address, click on the IP address to be revised and change it to the desired value.

5. To revise the syslog logging level, click on the Log Level drop-down list, then select one of the listed values:
   - OFF—Do not post any log messages to the Syslog servers
   - AUTO—Post all but security log messages to the Syslog servers

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- SECU—Post all log message to the Syslog servers

6. After all syslog configuration changes have been made, click on the **Apply** button, or click on the **Close** button to cancel the changes and close the window.

Runtime Options

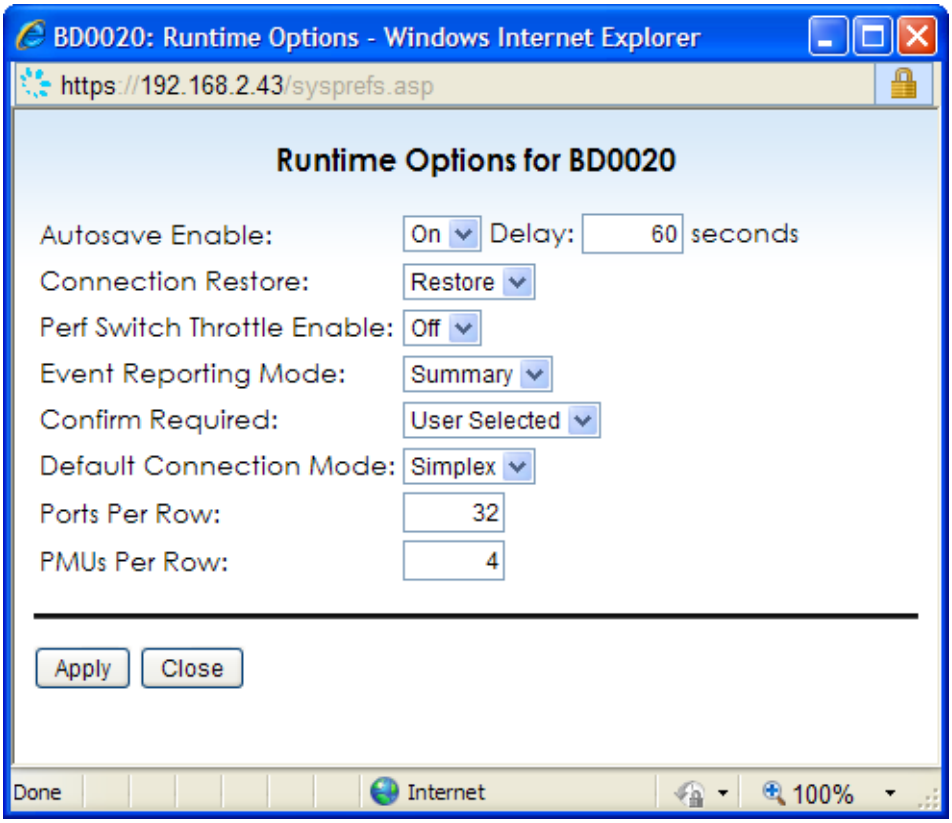
Users with the system-level privilege of View or higher may examine the configuration. Only users with the system-level privilege of Manage may modify account options.

The **System > System Configuration > Runtime Options** menu option opens the Runtime Options window (Figure 126), from which the following options can be configured:

- Autosave Enable (see page 244)
- Autosave Delay (see page 245)
- Connection Restore (see page 245)
- Performance Switch Throttle Enable (see page 245)
- Event Reporting Mode (see page 246)
- Confirm Required (see page 246)
- Default Connection Mode (see page 247)
- Ports Per Row (see page 248)
- PMUs Per Row (see page 248)

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 126 Runtime Options Window



Autosave Enable

The **Autosave Enable** setting governs whether or not user configuration changes will be saved to persistent memory. The frequency of updates to persistent memory is governed by **Delay** parameter (described in the following section).

The Autosave Enable pull-down list provides the following two settings:

Autosave Setting	Description
On (Default)	Configuration changes will be saved to persistent memory at the next interval set by the Autosave Delay value
Off	Configuration changes are not saved and will be lost upon a power cycle of the system.

NOTE: To force an immediate save of configuration changes, see “Save Configuration” on page 216.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Autosave Delay

The **Autosave Delay** parameter works in conjunction with the **Autosave Enable** parameter. If **Autosave Enable** is on, the value configured for **Delay** will determine how frequently changes will be saved to persistent memory. The **Delay** value is in seconds, with a range from 10 to 86400 (24 hours). The default value is 60 seconds.

NOTES:
- Connection persistence is not governed by the Autosave feature.
- Connection persistence is controlled by the Runtime options **Connection Restore** parameter.
- When a power outage occurs, configuration changes between **Delay** periods will be lost. System Maintenance Console and TL1 initiated shut-downs, reboots, and application restarts will save all data prior to the requested action, so no data is lost.

Connection Restore

The **Connection Restore** parameter governs whether or not the existing connection matrix will be restored after a power cycle, reboot, or application restart.

The following table describes the settings in the **Connection Restore** pull-down list.

Connection Restore Setting	Description
Reset (default)	Do not restore the previous connection matrix. On startup after hard reset or power cycle, the system will be reset to have no connections.
Restore	Restore the previous connection matrix (including connection ownership, connection description, and connection lock status).

NOTE: When set to **Restore**, all connections are saved to NVRAM as they are connected or disconnected

Performance Switch Throttle Enable

The **Perf Switch Throttle Enable** parameter enables or disables the requirement for the system to collect and evaluate switch-time data that is presented in the Performance Report.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The following table describes the settings in the **Perf Switch Throttle Enable** pull-down list.

Performance Throttle Setting	Description
On	The system will slow down the connection process to ensure collection of switch time data for presentation in the Performance Report.
Off (default)	Connections will be made without delay.

Event Reporting Mode

The **Event Reporting Mode** parameter specifies how many events will be generated, logged, and reported for configuration requests involving multiple ports (e.g., Import Port Configuration) or connections (e.g., Import Topology).

The following table describes the settings in the **Event Reporting Mode** pull-down list.

Event Reporting Mode Setting	Description
Summary (default)	One event will be generated, logged, and reported for the configuration or provisioning request.
Detail	An event will be generated for each change and a summary record (above) will be generated with the same timestamp to relate each event to the original command.

Confirm Required

The **Confirm Required** parameter allows administrators to establish a system policy that all users must confirm provisioning changes. When the **Confirm** check box on the Connection screen is checked the Provision Connection window will open when making/breaking connections, and a confirmation pop-up will open when changing input port signal thresholds. Changes to this parameter do not affect currently open ClickFlow sessions.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The following table describes the settings in the **Confirm Required** pull-down list.

Confirm Required Setting	Description
User Selected (default)	Users may check or uncheck the **Confirm** check box on the Connection screen, which leaves provisioning confirmation as a user-selectable choice.
Required	The **Confirm** check box on the Connection screen is checked for all users and cannot be unchecked. All provisioning changes require confirmation.

Default Connection Mode

The **Default Connection Mode** parameter allows administrators to establish a system default for the Connection screen **Duplex** check box and **Paired** check box. Changes to this parameter do not affect currently open ClickFlow sessions, and users may still toggle between simplex, duplex, and paired provisioning during each ClickFlow session.

The following table describes the settings in the **Default Connection Mode** pull-down list.

Default Connection Mode Setting	Description
Simplex (default)	The Connection screen **Duplex** and **Paired** check boxes are unchecked when a user initiates a ClickFlow session. Users may change the state of the **Duplex** and **Paired** check boxes during the ClickFlow session.
Duplex	The Connection screen **Duplex** check box is checked when a user initiates a ClickFlow session. Users may change the state of the **Duplex** check box during the ClickFlow session.
Paired	The Connection screen **Paired** check box is checked when a user initiates a ClickFlow session. Users may change the state of the **Paired** check box during the ClickFlow session. **NOTE**: Paired Connection Mode is an optional licensed feature. When enabled an odd-even pair of input ports may be connected to an odd-even pair of output ports in a single connection operation, see ”Configuration Settings” on page 19.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Ports Per Row

The **Ports Per Row** setting controls the number of input and output ports that will be displayed per line in the Connection Screen. When set to "0", the factory default of 32 ports per row will be used.

To change the ports per row display, enter an integer number between 0 and 192 in the provided box and click the **Apply** button. To view the new Connection Screen settings, either logout and login or click the refresh icon for your browser.

The value entered is saved and will be applied for all subsequent ClickFlow user sessions. The value may be set to 0 restore the factory default setting.

NOTE:	This parameter is only supported in the ClickFlow GUI and cannot be set via TL1 or from the Glimmerglass Console.

PMUs Per Row

The **PMUs Per Row** setting controls the number of Photonic Multicast Units that will be displayed on each PMU line. The default for this field is system specific and depends on the number and type of PMUs installed. When set to "0", the factory default display will be used.

To change the number of PMUs displayed per row, enter an integer number between 0 and 16 and click the **Apply** button. To view the new Connection Screen settings, either log out and log in or click the refresh icon for your browser.

The value entered is saved and will be applied for all subsequent ClickFlow user sessions. The value may be set to 0 to restore the factory default setting.

NOTE:	This parameter is only supported in the ClickFlow GUI and cannot be set via TL1 or from the Glimmerglass Console.

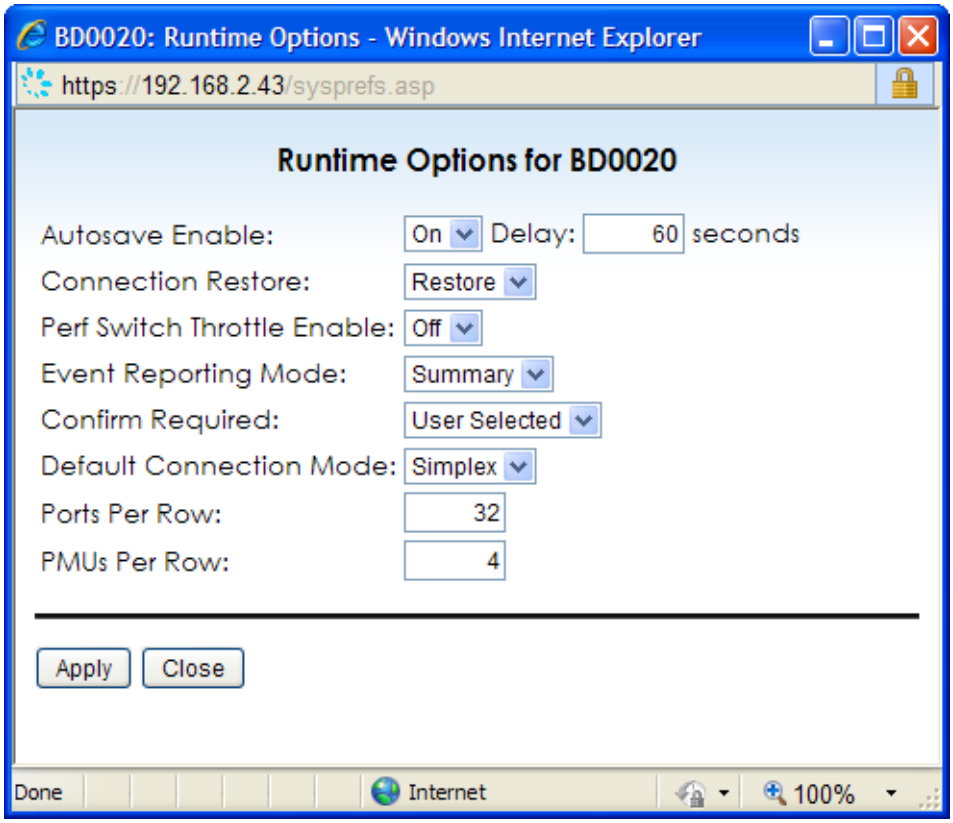
Configuring Runtime Options

Users with the system-level privilege of View or higher may examine the configuration. Only users with the system-level privilege of Manage may modify runtime options. Perform the following steps to configure Runtime options.

1. Select the **System > System Configuration > Runtime Options** menu option from the Connection screen menus. The Runtime Options window (Figure 127) will appear.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 127 Runtime Options Window



2. Use the pull-down lists for each parameter to select the desired value. The values for **Delay**, **Ports Per Row**, and **PMUs Per Row** are changed by placing the cursor in the respective text box and entering the desired values.

3. After all changes are made, click the **Apply** button.

4. A dialogue box will appear confirming the changes have been made. Click **OK**.

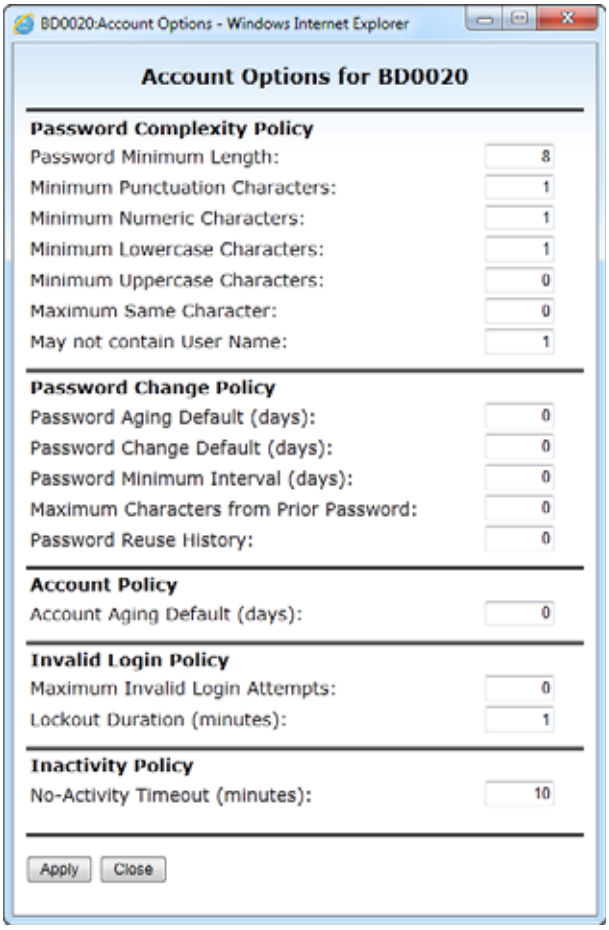
5. Click the **Close** button to close the Runtime Options window

Account Options

Opens the Account Options window (Figure 128), from which the user can configure system parameters supporting password complexity policy and password change policy, as well as system-wide policies for intrusion detection/reporting and no-activity timeout.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 128 Account Options Window



The table below describes the fields in the Account Options window.

Parameter	Description
Password Complexity Policy	
Password Minimum Length	This value establishes the required minimum password length. • Integer: 5-20 (min - max), default 8
Minimum Punctuation Characters	This value establishes the required minimum number of punctuation characters. • Integer: 0-20 (min - max), default 1 The password may not contain the following characters: Space, comma (,), question mark (?), colon (:), single quote (’), double quote (”), and backslash (\).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Parameter	Description
Minimum Numeric Characters	This value establishes the required minimum number of numeric characters (0-9). • Integer: 0-20 (min - max), default 1
Minimum Lowercase Characters	This value establishes the required minimum number of lowercase characters (a-z). Integer: 0-20 (min - max), default 1
Minimum Uppercase Characters	This value establishes the required minimum number of uppercase characters (A-Z). • Integer: 0-20 (min - max), default 0
Maximum Same Character	This value establishes the maximum number of times the same character may be used in a password. For example if the maximum is 2 then "banana.1" would fail because there are three "a" characters. Uppercase and lowercase are considered as different characters, so "bananA.1" would pass. • Integer: 0-20 (min - max), default 0 A value of 0 disables this requirement.
May not contain User Name	The password must not contain the user name spelled forward or backward. This comparison is case insensitive. For example the password for user account "admin" may not include "admin", "nimda", "ADMIN", etc. • Integer: 0 or 1, default 1 A value of 0 disables this requirement.
Password Change Policy	
Password Aging Default	The number of days after a password is changed before the password will expire. After expiration, the user account state will be set to "In Service Expired" and a grace period to change the password (Password Change Interval) will start. • Integer: 0 – 999 (min – max), default 0 Feature is disabled when set to 0 (password change is not required)
Password Change Default	The grace period during which the user is notified to change an expired password. If the password is not changed prior to the end of this period, the account state will be set to out of service. • Integer: 0 – 999 (min – max), default 0 Feature is disabled when set to 0 (account set out of service without notification).
Password Minimum Interval	Number of days required between password changes. • Integer: 0 – 999 (min – max), default 0 Feature is disabled when set to 0 (can change password immediately).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Parameter	Description
Maximum Characters from Prior Password	This value establishes limits on similarity between the current password and the new password. For more information, see “Password Change Policy” on page 179. • Integer: 0-20 (min - max), default 0 Feature is disabled when set to 0 (the passwords can be similar but not identical).
Password Reuse History	This value establishes the depth of comparison in the password history list. The user may not reuse a password that is in the password history list within the comparison depth. For more information, see “Password Change Policy” on page 179. • Integer: 0-24 (min - max), default 0 Feature is disabled when set to 0 (a password in the password history list may be used).
Account Policy	
Account Aging Default	Place user account out of service if the user does not login to the account within the number of days specified. • Integer: 0 – 999 (min – max), default 0 Feature is disabled when set to 0 (no inactivity timeout).
Invalid Login Policy	
Maximum Invalid Login Attempts	Limit for consecutive invalid login attempts by a user. After reached, the lockout duration will start. • Integer: 0 – 9 (min – max), default 0 Feature is disabled when set to 0 (no intrusion detection, no lockout).
Lockout Duration	Duration of the lockout period during which all login attempts by this user will fail. • Integer: 0 – 60 minutes (min – max), default 1.
Inactivity Policy	
No Activity Timeout	The number of minutes after which an idle session will be logged off. • Integer: 0 – 99 minutes (min – max), default 10 Feature is disabled when set to 0 (idle sessions will not timeout).

NOTE: With the exception of Password Aging days, Password Change days, and Account Aging days, the Account Options are system-wide settings governing session security and cannot be configured on a user-by-user basis.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Password Complexity Policy and Password Change Policy

For further information see “Password and Account Policies” on page 178.

Account Aging Default

This parameter sets the default Account Aging Interval when adding new users. When configured, this policy causes dormant user accounts to be placed out of service by the system. A user account is considered dormant when there is no login activity by the user during the time period specified by this parameter. For further information, see “Account Aging Policy” on page 181.

This is a default value only; a different value may be assigned in the user account record when the account is created, or later by editing the user account.

Maximum Invalid Login Attempts and Lockout Duration

The Maximum Invalid Login Attempts and Lockout Duration parameters are used to establish the intrusion detection policy for all users on the system:

- The Maximum Invalid Login Attempts parameter specifies a limit for consecutive failed login attempts by a user.
- The Lockout Duration parameter specifies a time period during which to block all subsequent login attempts (valid or invalid) by this user after the threshold for invalid login attempts is reached.

A valid login attempt after the lockout period expires will be accepted and will clear the invalid login attempt counter. An invalid login attempt after the period expires will restart the lockout period.

When the intrusion is detected and cleared, an event is posted to the system's security log (and the Glimmerglass Console for systems with the Glimmerglass Console feature). Intrusion clear occurs on the first successful login after intrusion.

No Activity Timeout

This parameter is used to set a policy to force a logoff of idle sessions. This parameter applies to all ClickFlow and TL1 sessions.

- For ClickFlow users, the no activity timer is reset by mousing over ports, navigating menus or tool-tips (passive activities). Also, opening a report or configuration window for inspection will disable the no activity timer. If the timer does expire, the user will be sent to the ClickFlow sign-out page.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- For TL1 users, the no activity timer is reset by command entry. If no commands are entered by the user, the session will be dropped and the user will need to reconnect to the switch to login.

Configuring Account Options

Users with the system-level privilege of View or higher may examine the configuration. Only users with the system-level privilege of Manage may modify account options. Perform the following steps to configure Account options.

1. Select the **System > System Configuration > Account Options** menu option from the Connection screen menus. The Account Options window (Figure 128 on page 250) will appear.

2. Place the cursor in the data entry field of the account option to be changed and enter the desired value. Repeat for all account options to be changed.

3. After all changes are made, click the **Apply** button.

4. A dialogue box will appear confirming the changes have been made. Click **OK**.

5. Click the **Close** button to close the Runtime Options window.

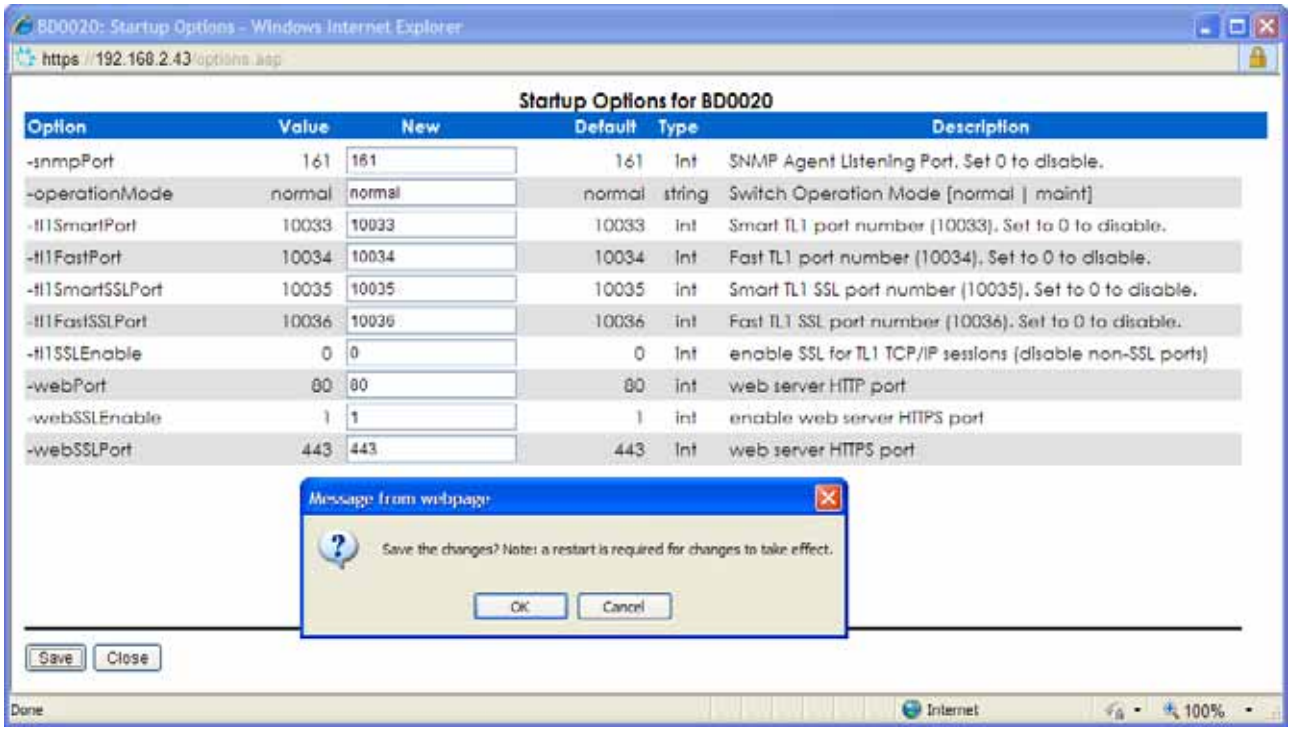
Startup Options

The **System > System Configuration > Startup Options** menu option opens the Startup Options window (Figure 129), from which the system operation mode and TCP port configurations of the system can be configured. The system maintenance operation mode may be used to prevent flooding the Network Operations Center with events (SNMP traps, Glimmerglass Console GGNMSGs, SYSLOG messages) when a system is under maintenance.

Users with the system-level privilege of View or higher may examine the configuration. Only users with the system-level privilege of Manage may modify startup options.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 129 Startup Options Window



The Startup Options window contains the following elements:

Parameter	Default Value	Possible Values	Description
-snmpPort	161	Unassigned registered or private port	SNMP Agent port. Use "0" to disable SNMP.
-operationMode	normal	normal or maint	System Operation Mode. In the maintenance operation mode the switch's SNMP Agent is disabled, the Glimmerglass Console Management interface is disabled, and system-level privilege Manage is required for ClickFlow and TL1 login. Any value other than "maint" will establish normal operation mode.
-tl1SmartPort	10033	Unassigned Registered or Private Port	Interactive TL1 port supporting unencrypted user Telnet access via a terminal emulator such as HyperTerminal.
-tl1FastPort	10034	Unassigned Registered or Private Port	Programmatic TL1 port supporting unencrypted machine-machine TCP socket access.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Parameter	Default Value	Possible Values	Description
-tl1SmartSSLPort	10035	Unassigned Registered or Private Port	Interactive TL1 port supporting encrypted user access via a Terminal Emulator supporting SSL Encryption
-tl1FastSSLPort	10036	Unassigned Registered or Private Port	Programmatic TL1 port supporting encrypted machine-machine SSL access.
-tl1SSLEnable	0	0 or 1	Use to select between unencrypted and encrypted access methods. The default value, 0, enables the unencrypted tl1SmartPort and tl1FastPort ports, and disables the encrypted tl1SmartSSLPort. 0 does not disable the tl1FastSSLPort because the latter port is required for Glimmerglass Console support. Setting the value to 1 enables the encrypted tl1SmartSSLPort and tl1FastSSLPort ports, and disables the unencrypted tl1SmartPort and tl1FastPort ports.
-webPort	80	Unassigned Registered or Private Port	Standard unencrypted http:// webserver port.
-webSSLEnable	1	0 or 1	Use to enable/disable unencrypted web access. The default value, 1, reroutes incoming unencrypted webPort requests to the encrypted webSSLPort. Setting the value to 0 enables unencrypted access via the webPort. The encrypted webSSLPort is disabled.
-webSSLPort	443	Unassigned Registered or Private Port	Standard encrypted https:// webserver port for SSL.
Save Button			Saves the Startup Options values to the permanent configuration file.
Close Button			Closes the Startup Options window.

NOTE: Individual TCP ports may be disabled by setting the port value to 0.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Configuring Startup Options

Users with the system-level privilege of View or higher may examine the configuration. Only users with the system-level privilege of Manage may modify the startup options. Perform the following steps to configure the Startup options:

1. Select **System > System Configuration > Startup Options** from the Connection screen to open the Startup Options window (Figure 129 on page 255).

2. Place the cursor in the **New Value** field of the startup option to be changed and enter the desired value. Repeat for all startup options to be changed.

3. After all changes are made, click on the **Save** button.

4. A dialogue box will appear requesting confirmation to save the changes.

5. Click the **OK** button to save the change. Click the **Cancel** button to abort the change.

6. The dialog box also advises that a system restart is required for the changes to take effect. Until the restart the system will continue to operate with the old startup option values. The restart may be performed by one of the following methods:
   - Application restart via the Maintenance Console or TL1 (init-sys restart)
   - System reboot via the Maintenance Console or TL1 (init-sys softreboot)
   - System power-cycle

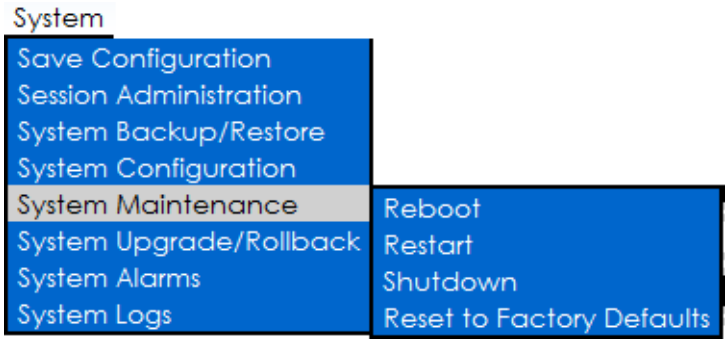
NOTES:
- All of the above restart methods will log off all existing system users (both ClickFlow and TL1). Only power-cycle will interrupt the system connections.
- See the section “Restart Application Services” in the *Glimmerglass System Installation and Maintenance Guide* for information on restarting services using the Maintenance Console.

System Maintenance

The **System > System Maintenance** menu options (Figure 130) allow the administrator to perform maintenance operations to reboot, restart, or shut down the system. Access to these commands is provided only to users with the system-level privilege of Manage.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 130 ***System > System Maintenance*** *Menu Options*



The table below describes the **System > System Maintenance** menu options.

Menu Option	Description
Reboot	Reboots the system without affecting connections. • A reboot is required after changing the systems IP configuration A dialogue box is presented requiring the user to confirm or cancel the request.
Restart	Restarts the Glimmerglass application software only. Does not affect connections. • A restart is required when modifying Startup Options governing TCP port configuration, SSL operation (on/off), or the maintenance mode of the switch. A dialogue box is presented requiring the user to confirm or cancel the request.
Shutdown	Shuts down the system completely; all connections dropped. • Shutdown is for use prior to powering off the Glimmerglass system to ensure that all processes and files are closed prior to power off. A dialogue box is presented requiring the user to confirm or cancel the request.

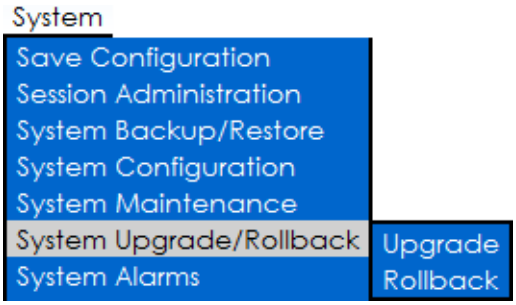
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Menu Option	Description
Reset to Factory Defaults	Break all connections, clear the system configuration database and reboot. A dialog box is presented requiring the user to confirm or cancel the operation. The system's current IP configuration is not defaulted. Therefore, remote network access to the system is not affected by the reset to defaults. The passwords for all default system accounts are reset to default. These passwords will need to be used when accessing the system via the Maintenance Console, ClickFlow/TL1, or SNMP after the system initializes. The Runtime parameter options (see ”Runtime Options” on page 243) will only be defaulted on new systems (Model Numbers GG112-C, GG514-C, GG528-C, or higher). For older systems, these values must be defaulted by the user through ClickFlow, TL1, or SNMP.

System Upgrade/Rollback

The **System > System Upgrade/Rollback** sub-menu options (Figure 131) allow the user to upgrade or rollback the system software. Access to these options is only presented to users with the system-level privilege of Manage.

Figure 131 ***System > System Upgrade/Rollback*** *Menu Options*



The system contains two non-volatile Flash RAM partitions (0 and 1), both containing the system software (Linux OS and Intelligent Optical Switch application) and the system configuration data:

- Boot Partition—Contains the current system software release; on a power-cycle or user-initiated reboot the system will boot from the Boot Partition.

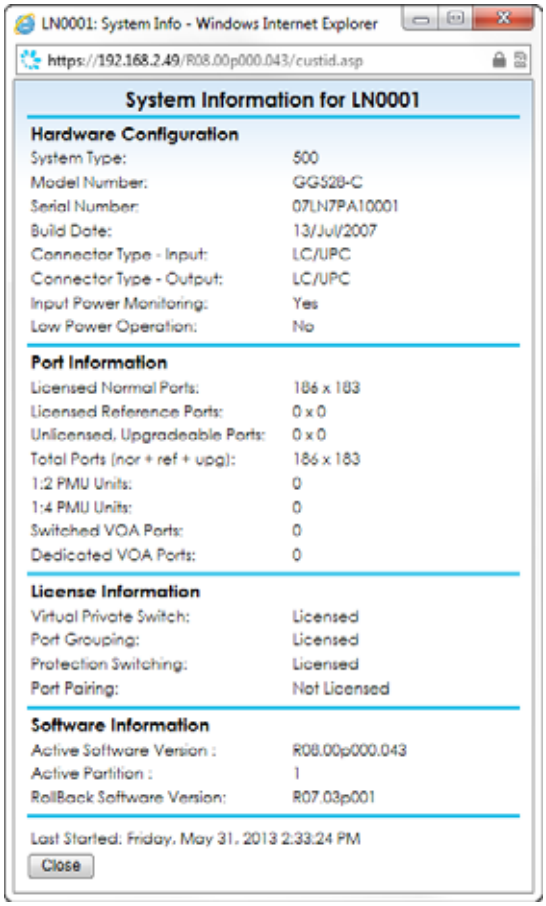
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- Rollback Partition—Contains the previous software release; if software rollback is initiated the roles of the two partitions are reversed and the system is booted from the former rollback partition.

On a software upgrade the rollback partition is upgraded to the new software, then the roles of the two partitions are reversed, and the system is booted from the former rollback partition.

The **Reports > System Info** menu selection opens the System Information window (Figure 132), which displays the boot partition and version, plus the rollback partition and version.

Figure 132 System Information Window



Upgrade

The **System > System Upgrade/Rollback > Upgrade** menu option opens the Upgrade System Software window (Figure 133 on page 263), from which software upgrade may be initiated by a user with system-level privilege of Manage.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE: For system software upgrade from a release prior to R07.01p000, see "Software Upgrade Procedures" in the Glimmerglass *System Installation and Maintenance Guide* for the release being upgraded.

The system software upgrade process consists of three phases:

Upgrade Phase	Description
1: Upload	Upload the software upgrade file to the system's volatile /dnld directory. The upgrade file size is approximately 17MB. The duration of this upgrade phase is a function of the network speed and the latency between the server/PC containing the upgrade file and the system being upgraded.
2: Upgrade	Verify the upgrade file and then upgrade the non-volatile inactive/rollback partition with the new kernel and application files. System availability is unaffected by this upgrade phase; the system continues to operate under the current release. The duration of this upgrade phase is 3 - 7 minutes as a function of the system model.
3: Reboot	Reboot to activate the upgraded partition. If the upgraded partition is booted successfully, then the roles of the boot and rollback partitions are reversed, otherwise the original boot partition is rebooted. The system is unavailable during this reboot phase. The duration of this final upgrade phase is 2 - 3 minutes.

The three software upgrade phases are supported by each of the user interfaces (ClickFlow, TL1, SNMP, and Maintenance Console) as follows:

Interface	Phase	Description
ClickFlow	Upload	Upgrade System Software window - Upgrade phase 1: Upload …
	Upgrade	Upgrade System Software window - Upgrade phase 2: Upgrade …
	Reboot	Upgrade System Software window - Upgrade phase 3: Reboot …
TL1	Upload	COPY-RFILE:::<ctag>:::SRC=<src>,DEST=<dest>;
	Upgrade	APPLY-UPGRADE:::<ctag>;
	Reboot	INIT-SYS:::<ctag>::SOFTREBOOT;
SNMP	Upload	Not supported; upload via SCP/SFTP, ClickFlow (HTTPS), TL1 (FTP), or Maintenance Console (FTP)
	Upgrade	sysProvisionTable.prCommand sysUpgrade
	Reboot	sysProvisionTable.prCommand sysReboot

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Interface	Phase	Description
Maintenance Console	Upload	Main Menu selection "Transfer File to System using FTP"
	Upgrade	Main Menu selection "Upgrade software", optionally includes reboot
	Reboot	Main Menu selection "Reboot"
SCP/SFTP	Upload	Push the upgrade file via SCP/SFTP from a Linux server or Windows PC

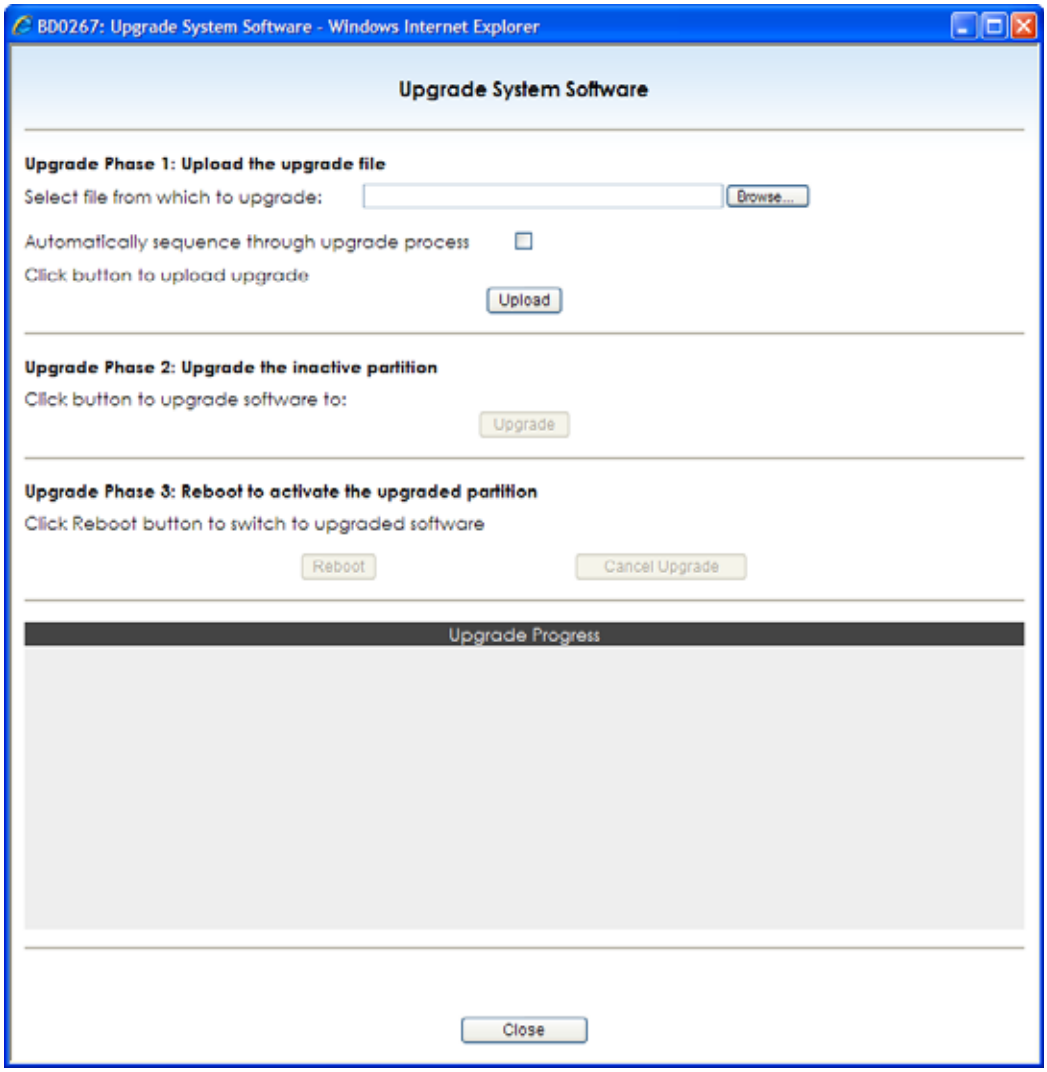
The three software upgrade phases do not have to be directly contiguous. For example, a Linux server with TL1 automation scripts could perform the non-disruptive upload and upgrade phases during the normal system high availability hours and then be scheduled to reboot all of the systems at midnight or during a scheduled maintenance period.

NOTE: Rebooting a system after a system software upgrade phase failure will simply reboot the current release.

In addition, the three software upgrade phases do not have to be performed by the same interface. For example, for the upload phase a Linux server script could push the upgrade files to each system via SCP/SFTP, and then complete the remaining phases by TL1 or SNMP.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 133 Upgrade System Software Window



The table below describes the fields in the Upgrade System Software window.

Element	Description
Browse button	Navigate to the system software upgrade file to be uploaded.
Automatically sequence	Check this checkbox to automatically sequence from the selection of the Upload button though and including rebooting the new software.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Upload button	Upload the selected system software upgrade file. The **Upload** button is disabled if: • The inactive/rollback partition upgrade is already in progress. • The inactive/rollback partition has already been upgraded via any of the interfaces (ClickFlow, SNMP, TL1 or Maintenance Console).
Upgrade button	Upgrade the inactive/rollback partition with the uploaded system software. The **Upgrade** button is disabled if: • A system software upgrade file has not been uploaded. • The uploaded system software file is corrupt or not applicable to this system. • The inactive/rollback partition has already been upgraded by any of the interfaces (ClickFlow, SNMP, TL1, or Maintenance Console).
Reboot button	Reboot the system to complete the upgrade. The **Reboot** button is disabled if: • The inactive/rollback partition has not been successfully upgraded. • Reboot is in progress
Cancel Upgrade button	Cancel the partially completed upgrade procedure and re-enable the **Upload** button. The **Cancel Upgrade** button is disabled if: • The inactive/rollback partition has not been successfully upgraded.
Upgrade Progress pane	Upgrade progress messages are displayed in the upgrade progress pane.
Close button	Close the window; this does not cancel the upgrade.

Upgrading System Software

Users with the system-level privilege of Manage may upgrade the system software. Perform the following steps to upgrade the system software:

1. Select **System > System Upgrade/Rollback > Upgrade** from the Connection screen to open the Upgrade System Software window (Figure 133 on page 263).

NOTE: If upgrade phase 1, or phases 1 and 2, have been previously completed then the upgrade phase section buttons will be appropriately enabled or disabled based on the upgrade phases already successfully completed.

---------- Upgrade Phase 1: Upload the Upgrade File ----------

2. Copy the upgrade file (GGNIOSUPG.tgz) from Glimmerglass Technical Support to a PC/server directory that can be reached from the ClickFlow web browser.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

NOTE: Glimmerglass Technical Support will also have provided a list of system serial numbers for which this upgrade is applicable.

3. In the upgrade phase 1 pane of the Upgrade System Software window, click the **Browse…** button to display the browser-dependent Choose File to Upload window.

4. Browse to and select the system software upgrade file (GGNIOSUPG.TGZ) and click the **Open** button.
   The name and location of the file is displayed in the Upgrade System Software window.

5. By default the upgrade process will stop at the end of the upgrade phase 1 (upload) and upgrade phase 2 (upgrade). To automatically proceed through each upgrade phase including reboot, click (check) the **Automatically sequence** check box.

NOTE: Each upgrade phase displays progress messages in the Upgrade Progress pane; if an upgrade phase fails then the upgrade phase sequencing will stop.

6. Click the **Upload** button.
   The file is uploaded, a basic sanity check is performed, the release information is extracted and displayed above the **Upgrade** button, and the **Upgrade** button is enabled.

NOTES: If "automatically sequence" was checked in step 5 above, no further operator interaction is required.

Due to limitations in the system's embedded web server, service to all ClickFlow web browsers is suspended during file upload, hence if upload takes longer than 10 seconds all of the logged in ClickFlow web browser windows will gray and display "server not responding" until the upload is complete. If the network link between the web browser and the system has low bandwidth and high latency you might choose to upload the file via SCP, see "Software Upgrade Procedures" in the Glimmerglass *System Installation and Maintenance Guide.*

---------- Upgrade Phase 2: Upgrade the Inactive Partition ----------

7. Confirm the displayed release is the one expected, then click the **Upgrade** button.
   Files are extracted from the upgrade file and are copied to the kernel and application sections of the system's non-volatile Flash RAM inactive/rollback partition. Progress messages are displayed in the Update Progress pane. The duration of the phase is 3-7 minutes as a function of the system model. Upon successful completion, the **Reboot** button will be enabled.

---------- Upgrade Phase 3: Reboot to Activate the Upgraded Partition ----------

8. Click the **Reboot** button to complete the upgrade, or click the **Cancel Upgrade** button to cancel the upgrade and remain with the current release.
   The system configuration and log files are saved to non-volatile memory, the application is

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

stopped, the system configuration database is copied to the upgraded partition, and the upgraded partition is booted. If the upgraded kernel and application successfully boot then the roles of the boot and rollback partition are reversed. Any subsequent reboots or power-cycles will automatically boot the upgraded system software. The duration of the reboot phase is 2-3 minutes.

NOTES: The above reboot actions will occur following any method of initiating reboot.

If Cancel Upgrade is selected, then:

- A subsequent reboot or power-cycle will boot the current release.
- The upgrade phase reverts to phase 1 to allow upload of an alternate release
- Selection of Rollback in the Rollback System Software window is disabled, because the rollback partition no longer contains the previous release.

Rollback

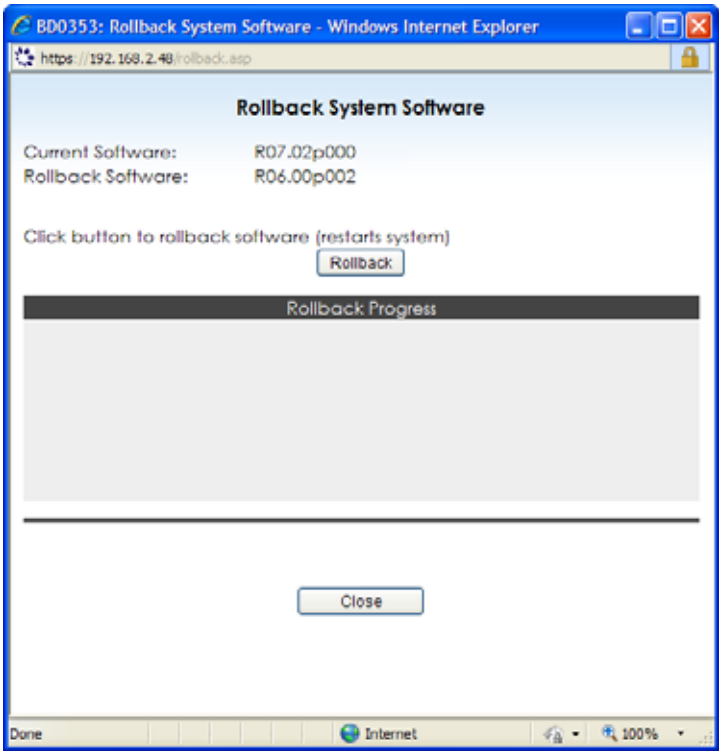
The **System > System Upgrade/Rollback > Rollback** menu option opens the Rollback System Software window (Figure 134), from which software rollback may be initiated by a user with system-level privilege of Manage.

System software rollback is supported by each of the system interfaces as follows:

Interface	Description
ClickFlow	Rollback System Software window (Figure 134).
TL1	APPLY-ROLLBACK:::<ctag>;
SNMP	sysProvisionTable.prCommand sysRollback
Maintenance Console	Main Menu selection "Rollback to other partition"

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 134 Rollback System Software Window



The table below describes the fields in the Rollback System Software window.

Element	Description
Current Software	The system software release number in the boot partition
Rollback Software	The system software release number in the rollback partition
Rollback button	Exchange the roles of the boot and rollback partitions and boot from the former rollback partition. The Rollback button will be disabled if: • The most recent upgrade has already been rolled back (the rollback partition software version is more recent than that in the boot partition). • The most recent upgrade procedure was canceled via Cancel Upgrade (the rollback partition software version is more recent than that in the boot partition).
Rollback Progress pane	Rollback progress messages are displayed in the rollback progress pane.
Close button	Close the window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Rolling Back the System Software

Users with the system-level privilege of Manage may rollback the system software to the previously installed release. Perform the following steps to upgrade the system software:

1. Select **System > System Upgrade/Rollback > Rollback** from the Connection screen to open the Upgrade System Software window (Figure 133 on page 263).
   The current system software release in the boot partition and the system software release in the rollback partition are displayed.

   NOTE: The Rollback button will be disabled if either of the following are true:
   - The most recent software upgrade has already been rolled back
   - The most recent partially completed upgrade was canceled by Cancel Upgrade

2. Click the **Rollback** button to initiate rollback.
   A rollback initiated message is displayed in the rollback progress pane, system reboot is initiated, the ClickFlow browser client window background grays during reboot, and is replaced by the ClickFlow login window on completion of reboot.

System Alarms

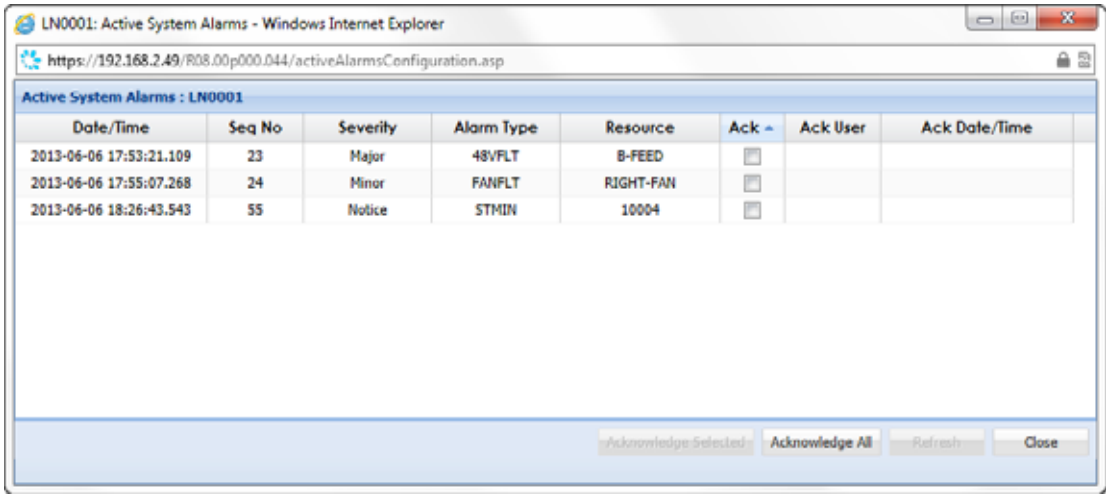
The **System > System Alarms** menu option opens the Active System Alarms window (Figure 135) for viewing the active alarm table. This window also allows users to acknowledge alarms.

All users have access to this menu option but the alarms displayed and actions allowed are tied to the user's privilege levels:

- If an alarm exists for a port for which the user does not have View or higher port privilege, this alarm will not be shown to the user.
- To acknowledge an optical alarm (port/connection alarm), the user must have a port privilege of Modify or higher for the port the alarm is raised against.
- Hardware and software alarms are displayed to all users. To acknowledge a hardware or software alarm, the user must have a system privilege of Modify or higher.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 135 Active System Alarms Window



The alarm table in the window displays active alarms sorted as follows:

- All unacknowledged alarms are displayed first (at the top of the table). Acknowledged alarms will be display after all unacknowledged alarms regardless of severity and date/time of occurrence.
- After the above separation, the alarms are displayed by severity (Critical is highest severity, Notice is lowest severity).
- Lastly, for a given severity, the alarms are presented in date/time order of occurrence (newest to oldest).

See Figure 140 on page 273 for a table view reflecting the above sorting.

The table below describes the elements of the Active System Alarms window.

Element	Description
Date/Time	The date and time at which the alarm was detected, with the time recorded down to milliseconds.
Seq No	The sequence number for the alarm. This information is reflected in the alarm log. When an alarm is cleared, the log will record this sequence number in the field named “ClearSeqNo”.
Severity	The severity of the alarm. For STMIN, STMAX, and CSFLT alarms, the severity may be configured by the user.
Alarm Type	The type of alarm. See ”Alarm Conditions and Alarm Types” on page 274 for an enumeration of all alarm conditions and corresponding alarm codes.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Resource	The resource (hardware device, software issue, switch input or output port) on which the alarm condition was detected
Ack (Check Box)	This check box is used when the user wants to selectively acknowledge alarms in the table. Selectively acknowledging alarms is a two-step process. First, the box is checked for the alarm or alarms. Next, the **Acknowledge Selected** button (below) is clicked to execute the operation. Only users with the required privileges may acknowledge alarms. Once an alarm is acknowledged, it cannot be unacknowledged.
Ack User	When an alarm has been acknowledged, this field will display the name of the user that acknowledged the alarm.
Ack Date/Time	The date and time at which the alarm was acknowledged by the above user, with the time recorded down to milliseconds.
Acknowledge Selected Button Acknowledge Selected Acknowledge Selected	This button is inactive when the Active System Alarms window is opened. The button becomes active only when the user selects the check box in the **Ack** column to acknowledge that specific alarm. After all alarms (rows) to be acknowledged are checked, click this button to execute the acknowledge request for the checked alarms. The display will refresh to show the new alarm conditions.
Acknowledge All Button Acknowledge All	This button may be used to acknowledge all unacknowledged alarms in the alarm table. There is no confirmation for this operation: Once the button is operated, the alarms are acknowledged and the display is refreshed.
Refresh Button Refresh Refresh	When the Active System Alarms window is opened, the **Refresh** button is inactive. If changes are detected in the system, the **Refresh** button automatically activates to notify the user that changes have been detected. In addition, a status message is displayed in the lower right hand corner of the window. Click the **Refresh** button to redisplay the alarm table with current information. The following conditions will trigger a refresh notification: • New alarms are detected • Existing alarms have been cleared • Another user has acknowledged active alarm(s)
Close Button Close	This button closes the window.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Alarm Table Operations

The following cases illustrate alarm table operations and represent sequential changes after the Active System Alarm window is initially opened as seen in Figure 135 on page 269.

Case 1: Alarm condition changes occur after the Active Systems Alarms window has been opened.

The Active Systems Alarms display is a snapshot of the alarm table at the time the window is opened. If alarm changes occur (i.e., new alarms are reported, alarms are cleared, alarms are acknowledged), the user will be given two indications in the window to refresh the display (these are highlighted in Figure 136 below):

- The following status message will appear at the bottom of the right corner of the window: *ALARM CHANGES - 'Refresh' to Display*
- The **Refresh** button will become active, allowing the user to click the button to update the window with the current alarm information.

Figure 136 Active System Alarms Window (Alarm Changes Detected)

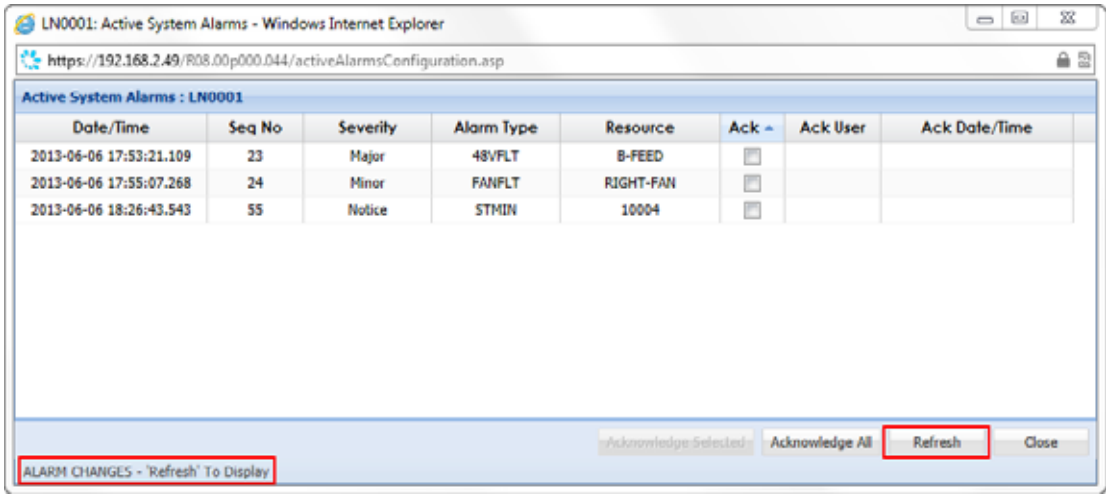
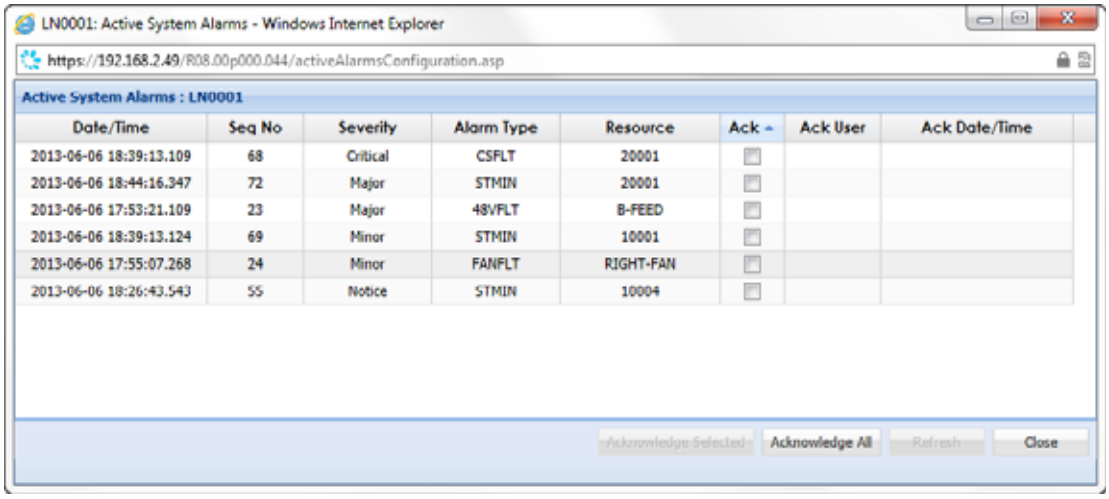


Figure 137 below shows the Active System Alarms window for the above table after the **Refresh** button is clicked.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 137 Active System Alarms Window (After Refresh)



In Figure 137, notice that the cause for the refresh was the detection of new alarm conditions. The ordering of the table is changed to reflect the new severities.

Case 2: Acknowledging an Alarm

Figure 138 shows the window display after the user has selected three alarms to acknowledge. These are indicated both by the check box and the red triangle in the upper corner of the **Ack** cells that are checked. The **Acknowledge Selected** button is highlighted to indicate that the button is now active.

Figure 138 Active System Alarms Window (Acknowledge Operation)

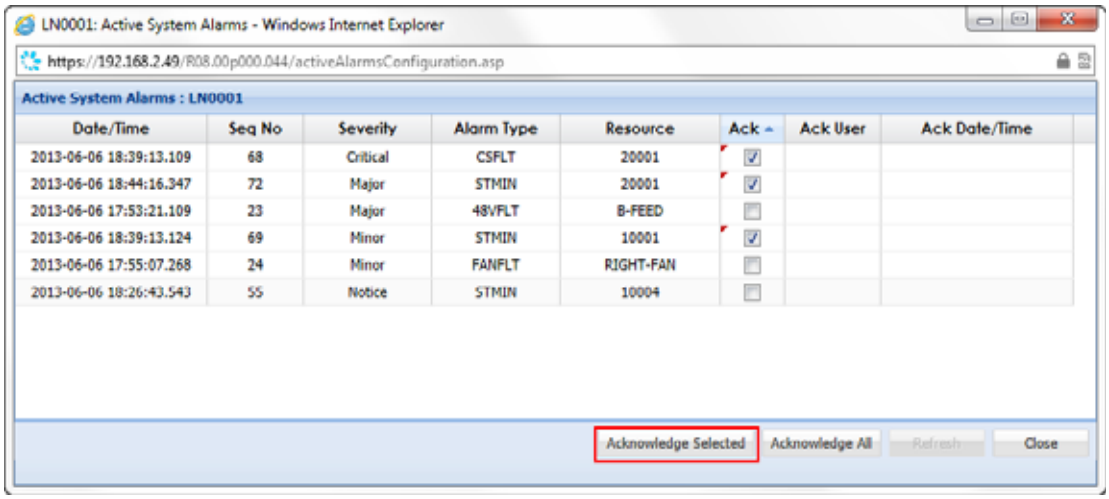
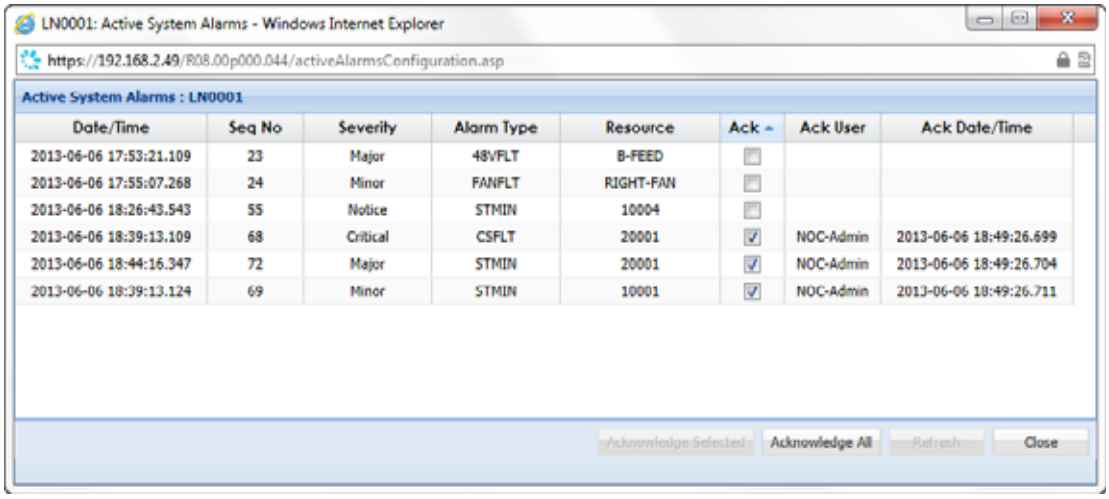


Figure 139 below shows the window after the **Acknowledge Selected** button is clicked.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 139 Active System Alarms Window (After Acknowledging Alarms)



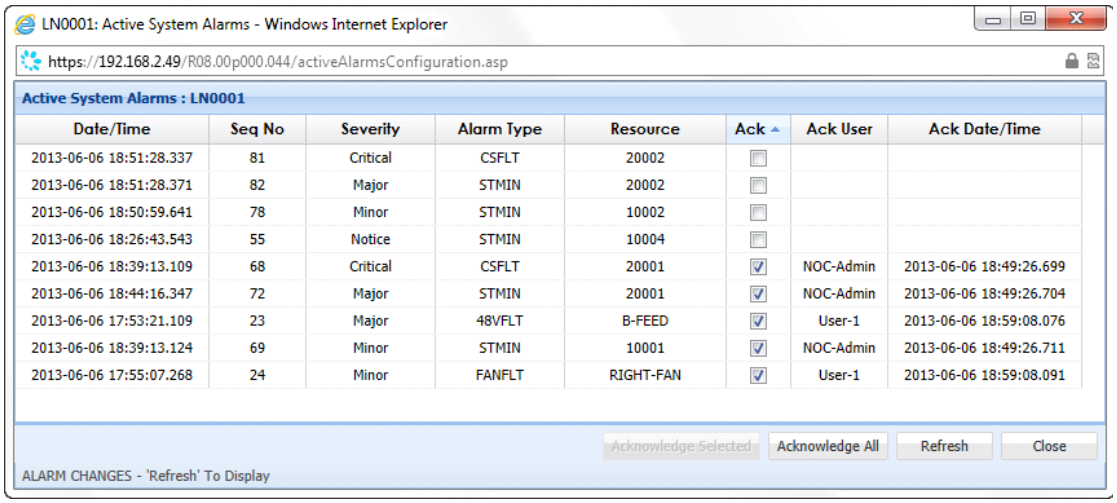
Date/Time	Seq No	Severity	Alarm Type	Resource	Ack	Ack User	Ack Date/Time
2013-06-06 17:53:21.109	23	Major	48VFLT	B-FEED	☐		
2013-06-06 17:55:07.268	24	Minor	FANFLT	RIGHT-FAN	☐		
2013-06-06 18:26:43.543	55	Notice	STMIN	10004	☐		
2013-06-06 18:39:13.109	68	Critical	CSFLT	20001	☑	NOC-Admin	2013-06-06 18:49:26.699
2013-06-06 18:44:16.347	72	Major	STMIN	20001	☑	NOC-Admin	2013-06-06 18:49:26.704
2013-06-06 18:39:13.124	69	Minor	STMIN	10001	☑	NOC-Admin	2013-06-06 18:49:26.711

In Figure 139, notice that the three acknowledged alarms are moved to the bottom of the table and are listed in order of severity. For each of these alarms, the **Ack** box is checked, and the **Ack User** and the **Ack Date/Time** fields are filled in (NOC-Admin is the name of the user who acknowledged the alarm).

Case 3: Alarms Clear

Figure 140 shows the window display after additional alarm changes are reported after the window has been opened. The window displays a refresh notification.

Figure 140 Active System Alarms Window (Alarm Changes Detected)

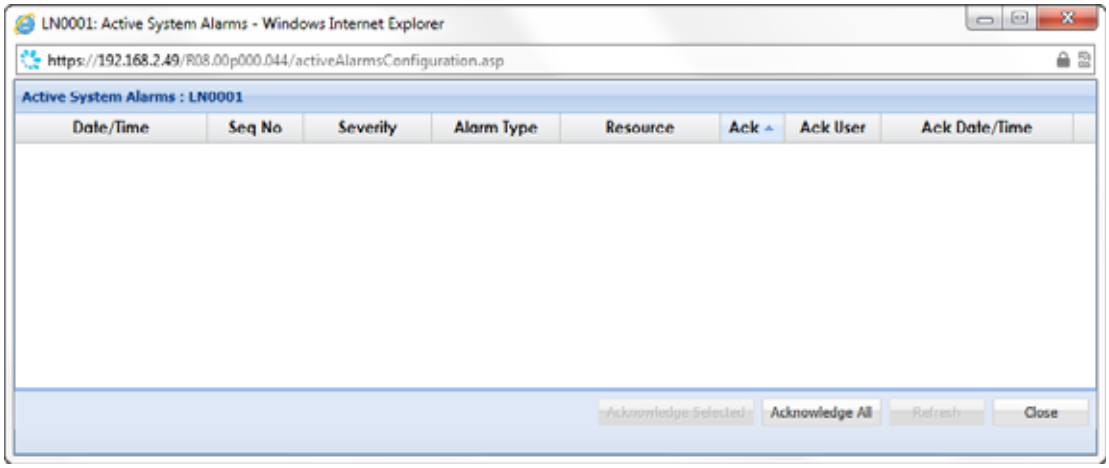


Date/Time	Seq No	Severity	Alarm Type	Resource	Ack	Ack User	Ack Date/Time
2013-06-06 18:51:28.337	81	Critical	CSFLT	20002	☐		
2013-06-06 18:51:28.371	82	Major	STMIN	20002	☐		
2013-06-06 18:50:59.641	78	Minor	STMIN	10002	☐		
2013-06-06 18:26:43.543	55	Notice	STMIN	10004	☐		
2013-06-06 18:39:13.109	68	Critical	CSFLT	20001	☑	NOC-Admin	2013-06-06 18:49:26.699
2013-06-06 18:44:16.347	72	Major	STMIN	20001	☑	NOC-Admin	2013-06-06 18:49:26.704
2013-06-06 17:53:21.109	23	Major	48VFLT	B-FEED	☑	User-1	2013-06-06 18:59:08.076
2013-06-06 18:39:13.124	69	Minor	STMIN	10001	☑	NOC-Admin	2013-06-06 18:49:26.711
2013-06-06 17:55:07.268	24	Minor	FANFLT	RIGHT-FAN	☑	User-1	2013-06-06 18:59:08.091

In this case, all of the existing alarms have cleared. Figure 141 below shows the window after the **Refresh** button is clicked.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 141 Active System Alarms Window (No Alarms)



The table will display as empty when no active alarms are present in the system. With the exception of STMIN, STMAX, CSFLT, and Intrusion alarm types, the alarm condition must be corrected for the alarm to clear.

Intrusion Alarms are cleared when acknowledged. The other alarms (STMIN, STMAX, CSFLT) may be cleared by setting the alarm severity to DISABLE for the port in alarm.

To review the history for cleared alarms, the alarm log (see ”Alarm (ALARM) Log” on page 277) may be used to review the 1000 most recent alarm entries (detection, clear, acknowledge).

Alarm Conditions and Alarm Types

The table below shows the alarms that are supported on the Glimmerglass switch.

- Alarm Condition—The condition which causes the alarm to be detected.
- Alarm Type—The code used to designate the alarm condition.
- Alarm Object—The resource for which the alarm is detected.
- Severity—The severity assigned to the alarm for logging/reporting.

Note that the alarm severity is configurable by the user for the first three optical alarms. The severity may be assigned on a per-port basis. Therefore, an STMIN may be considered critical for one port and minor for another port.

The alarm severities which may be assigned for these conditions are Critical, Major, Minor, Notice, and Disable:

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

- The severity of “Notice” means the alarm will be logged but no external notification for the alarm will be sent.
- The severity of “Disable” means that the alarm condition will be ignored - no alarm will be logged and no notification will be issued.

While the alarm condition is active, a record for the alarm will be present in the active alarm table. When the alarm condition is cleared, the alarm will be removed from the active alarm table. In general, alarms cannot be cleared without fixing the alarm condition. An exception is made for the user-configurable optical alarms. Setting the alarm severity to “Disable” will log a clear event for the alarm and remove the alarm from the active alarm table.

Alarm Condition	Alarm Type	Alarm Object	Severity
Hardware Alarms			
No DC Input Power	48VFLT	A-FEED | B-FEED	Major (MJ)
No DC Fuse	FUSEFLT	A-FEED | B-FEED	Major (MJ)
Single Fan Failure	FANFLT	<Fan Name>	Minor (MI)
Multiple Fan Failure	FANFLT	MULTIPLE-FANS	Major (MJ)
Engine Temperature	TEMPHI	ENGINE	Critical (CR)
MPS – Vbb too low	VBBLO	MPS	Critical (CR)
MPS – Vbb too high	VBBHI	MPS	Critical (CR)
MPS – Vfb too low	VFBLO	MPS	Critical (CR)
MPS – Vfb too high	VFBHI	MPS	Critical (CR)
Software Alarms			
Intrusion Detected	INTRUSION	USER | CHANNEL	Minor (MI)
NTP Sync. Loss	NTPFLT	CLOCK	Critical (CR)
Optical Alarms			
Min. Power Threshold	STMIN	<Port #>	<User Defined>
Max. Power Threshold	STMAX	<Port #>	<User Defined>
Connection Fault	CSFLT	<Output Port#>	<User Defined>
Reverse Light	LGTRVRS	<Output Port#>	Critical (CR)
Max. System Power	PWRMAX	<Port #>	Major (MJ)

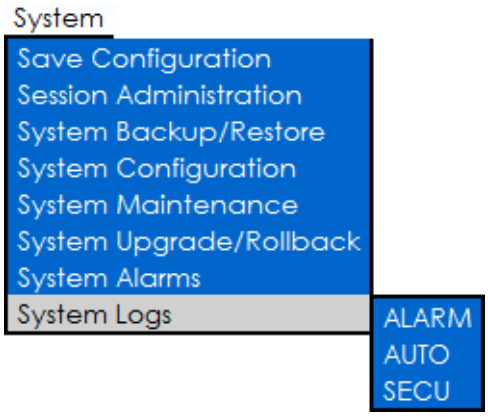
Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

System Logs

The **System > System Logs** sub-menu options (Figure 142) allow the user to view the three log files in the system: Alarm (ALARM) log, Autonomous Message (AUTO) log, and Security (SECU) log.

To view the full contents of the ALARM and AUTO logs, the user must have View system-level and port-level privileges. To view the contents of the SECU log, the user must have Manage system-level privileges. The SECU option will not appear in the sub-menu if the user does not have Manage system-level privileges.

Figure 142 ***System > System Logs*** *Menu Options*



Each log maintains the last 1000 messages written to the log. The log information is automatically saved every 24 hours or when a reboot, restart or, shutdown is initiated. Log data will be lost if the system is powered off without first shutting down the system.

NOTE:	Log data will be lost if the system is powered off without first shutting down the system.:

The following sections describe each of the three logs:

- “Alarm (ALARM) Log” (below)
- ”Autonomous Message (AUTO) Log” on page 279
- ”Security (SECU) Log” on page 282

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Alarm (ALARM) Log

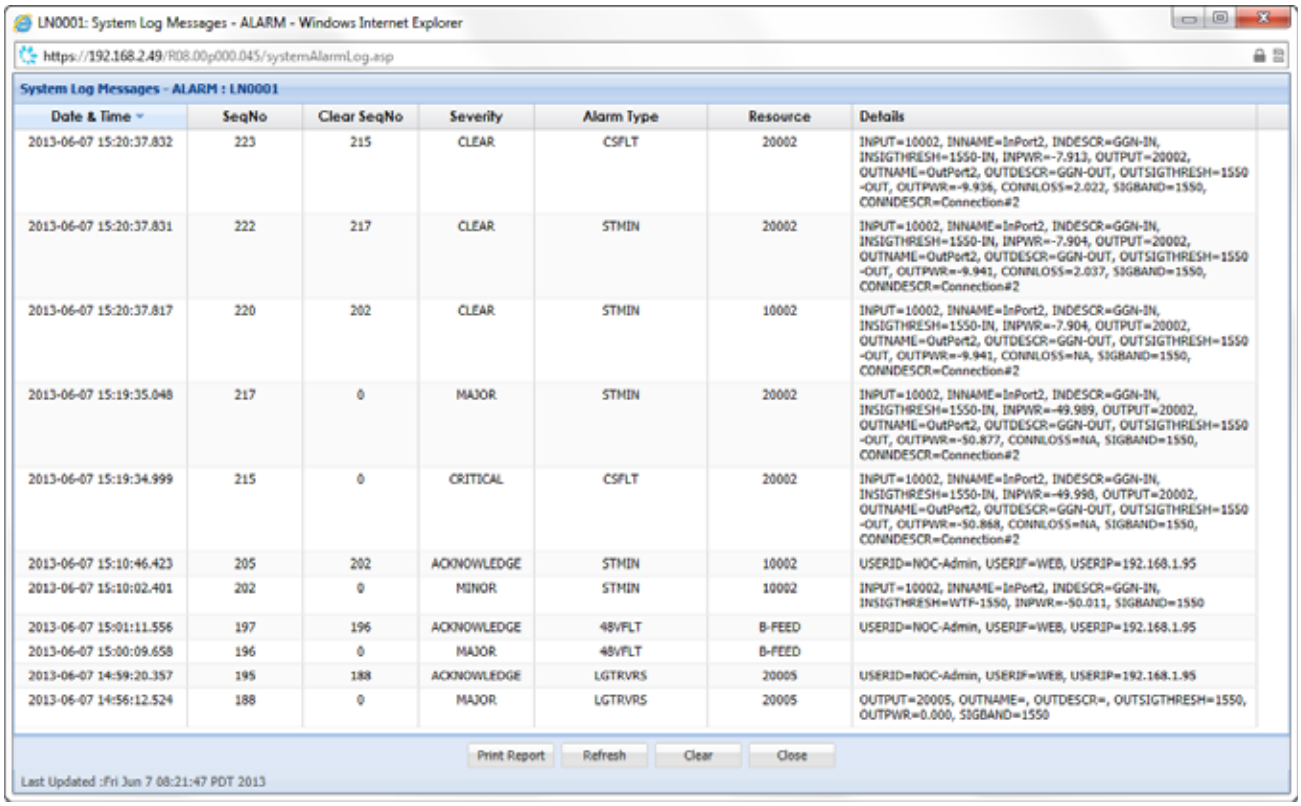
The **System > System Logs > ALARM** sub-menu option opens the Alarm log (Figure 143), which contains entries for the following system activities:

- Log entry for alarm when detected
- Log entry for alarm when cleared
- Log entry for alarm acknowledgment

The **System > System Logs** option will not be presented if the user's port privilege is less than View.

- To update the data to current, press the **Refresh** button at the bottom of the window.
- To clear the log file, press the **Clear** button at the bottom of the window. A system-level privilege of Manage is required to clear either the ALARM log file.
- To print the log file, press the **Print Report** button at the bottom of the window. Follow the browser instructions to specify the printer. The browser will display the image of the log file that will be printed.

Figure 143 Alarm Log Window



Date & Time	SeqNo	Clear SeqNo	Severity	Alarm Type	Resource	Details
2013-06-07 15:20:37.832	223	215	CLEAR	CSFLT	20002	INPUT=10002, INNAME=InPort2, INDESCR=GGN-IN, INSIGTHRESH=1550-IN, INPWR=-7.913, OUTPUT=20002, OUTNAME=OutPort2, OUTDESCR=GGN-OUT, OUTSIGTHRESH=1550-OUT, OUTPWR=-9.936, CONNLOSS=2.022, SIGBAND=1550, CONNDESCR=Connection#2
2013-06-07 15:20:37.831	222	217	CLEAR	STMIN	20002	INPUT=10002, INNAME=InPort2, INDESCR=GGN-IN, INSIGTHRESH=1550-IN, INPWR=-7.904, OUTPUT=20002, OUTNAME=OutPort2, OUTDESCR=GGN-OUT, OUTSIGTHRESH=1550-OUT, OUTPWR=-9.941, CONNLOSS=2.037, SIGBAND=1550, CONNDESCR=Connection#2
2013-06-07 15:20:37.817	220	202	CLEAR	STMIN	10002	INPUT=10002, INNAME=InPort2, INDESCR=GGN-IN, INSIGTHRESH=1550-IN, INPWR=-7.904, OUTPUT=20002, OUTNAME=OutPort2, OUTDESCR=GGN-OUT, OUTSIGTHRESH=1550-OUT, OUTPWR=-9.941, CONNLOSS=NA, SIGBAND=1550, CONNDESCR=Connection#2
2013-06-07 15:19:35.048	217	0	MAJOR	STMIN	20002	INPUT=10002, INNAME=InPort2, INDESCR=GGN-IN, INSIGTHRESH=1550-IN, INPWR=-49.989, OUTPUT=20002, OUTNAME=OutPort2, OUTDESCR=GGN-OUT, OUTSIGTHRESH=1550-OUT, OUTPWR=-50.877, CONNLOSS=NA, SIGBAND=1550, CONNDESCR=Connection#2
2013-06-07 15:19:34.999	215	0	CRITICAL	CSFLT	20002	INPUT=10002, INNAME=InPort2, INDESCR=GGN-IN, INSIGTHRESH=1550-IN, INPWR=-49.998, OUTPUT=20002, OUTNAME=OutPort2, OUTDESCR=GGN-OUT, OUTSIGTHRESH=1550-OUT, OUTPWR=-50.868, CONNLOSS=NA, SIGBAND=1550, CONNDESCR=Connection#2
2013-06-07 15:10:46.423	205	202	ACKNOWLEDGE	STMIN	10002	USERID=NOC-Admin, USERIF=WEB, USERIP=192.168.1.95
2013-06-07 15:10:02.401	202	0	MINOR	STMIN	10002	INPUT=10002, INNAME=InPort2, INDESCR=GGN-IN, INSIGTHRESH=WTF-1550, INPWR=-50.011, SIGBAND=1550
2013-06-07 15:01:11.556	197	196	ACKNOWLEDGE	48VFLT	B-FEED	USERID=NOC-Admin, USERIF=WEB, USERIP=192.168.1.95
2013-06-07 15:00:09.658	196	0	MAJOR	48VFLT	B-FEED	
2013-06-07 14:59:20.357	195	188	ACKNOWLEDGE	LGTRVRS	20005	USERID=NOC-Admin, USERIF=WEB, USERIP=192.168.1.95
2013-06-07 14:56:12.524	188	0	MAJOR	LGTRVRS	20005	OUTPUT=20005, OUTNAME=, OUTDESCR=, OUTSIGTHRESH=1550, OUTPWR=0.000, SIGBAND=1550

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The table below describes the elements of the Alarm Log window.

Element	Description
Date/Time	The date and time at which the alarm was detected, with the time recorded down to milliseconds.
SeqNo	The sequence number for the log entry. The system automatically assigns and tracks sequence numbers. These sequences numbers are shared by the three logs. Therefore, all events can be identified by sequence number order as well as date/time when comparing among the logs.
Clear SeqNo	This field is only used when the Severity for the alarm record is CLEAR. The field contains the sequence number for the record reporting the alarm condition. This allows correlation between the clear record and the original alarm record. This field will contain the value of 0 (zero) in all other cases.
Severity	The severity associated with the alarm event. The severity values are: • CRITICAL • MAJOR • MINOR • NOTICE • CLEAR (used when the active alarm clears) • ACKNOWLEDGE (used when logging alarm acknowledgment)
Alarm Type	The code describing the Alarm Condition that is detected, cleared, or acknowledged. See ”Alarm Conditions and Alarm Types” on page 274 for a description of all alarm conditions and corresponding alarm codes.
Resource	The resource (hardware device, software issue, switch input or output port) on which the alarm condition was detected
Details	This field may contain a series of comma separated KEYWORD=VALUE pairs. This data provides additional information regarding the configuration of the resource in alarm (e.g., port or connection configuration) as well as the relevant data concerning the alarm itself (e.g., optical power values). Alarm acknowledgments will include the information about the user that cleared the alarm, such as: • USERID—user name • USERIF—interface used (e.g., WEB or TL1) • USERIP—IP address of the user host machine
Print Report Button Print Report	This button will open a browser window displaying the log contents in a format for printing, with an options to send the view to a printer.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Refresh Button Refresh	This button is used to refresh the log window display to include any events which occurred after the window was opened or last refreshed. The Last Updated time stamp at the bottom of the window indicates the time at which the window was opened or last refreshed.
Clear Button Clear Clear	This button may be used to clear the alarm log. When cleared, a message will be posted in the AUTO log indicating the ALARM log was cleared as well as the user who cleared the log. This button is dimmed unless the user has Manage system-level privileges.
Close Button Close	This button closes the window.
Last Updated:	The date and time at which the data in the window was last updated (refreshed).

Autonomous Message (AUTO) Log

The **System > System Logs > AUTO** sub-menu option opens the Autonomous Message log (Figure 144), which contains entries for the following user and system activities:

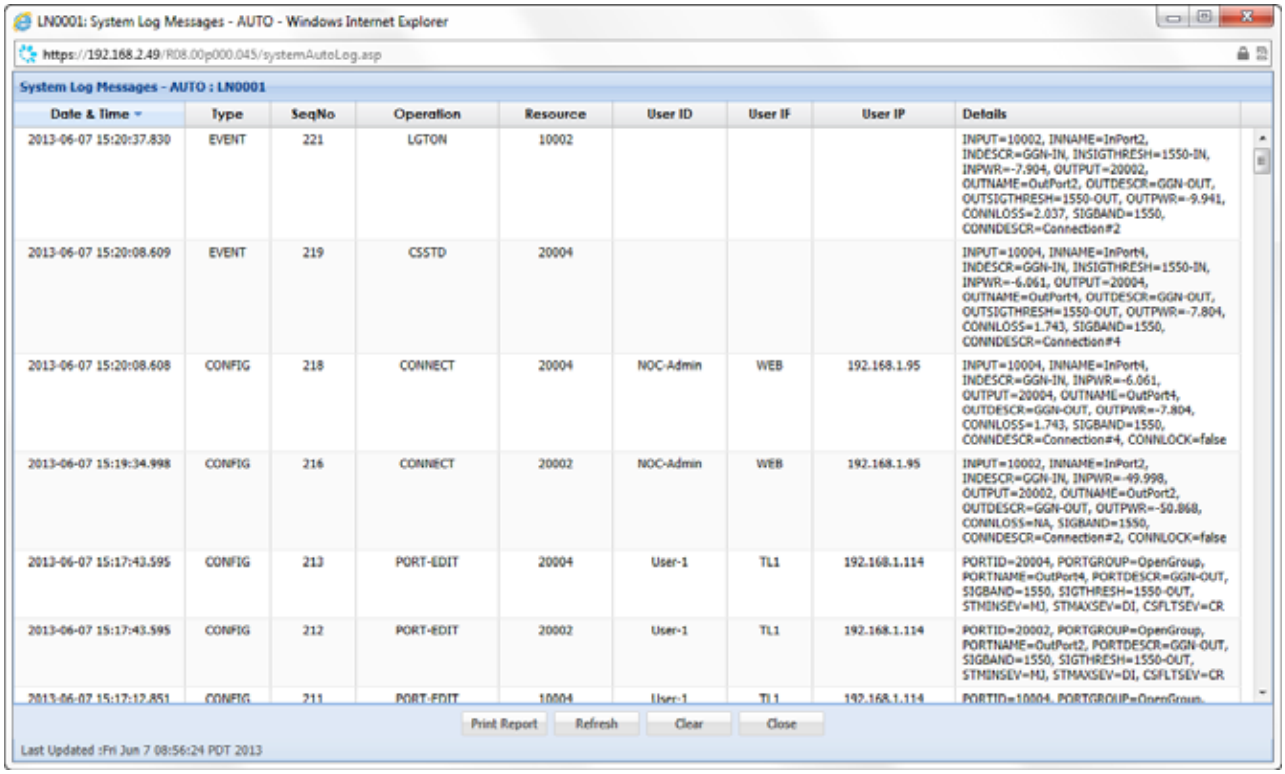
- System configuration (e.g., name/IP, date/time, SNMP, Syslog, runtime/startup options)
- All port and/or connection configuration
- Maintenance operations
- Non-alarm system and port power and connection events

The **System > System Logs** option will not be presented if the user's port privilege is less than View.

- To update the data to current, press the **Refresh** button at the bottom of the window.
- To clear the log file, press the **Clear** button at the bottom of the window. A system-level privilege of Manage is required to clear the AUTO log file.
- To print the log file, press the **Print Report** button at the bottom of the window. Follow the browser instructions to specify the printer. The browser will display the image of the log file that will be printed.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 144 Autonomous Message (AUTO) Log Window



The table below describes the elements of the Autonomous Message Log window.

Element	Description
Date/Time	The date and time at which the event was detected, with the time recorded down to milliseconds.
Type	This column identifies the operational category for the log entry. These values are: • CONFIG - Any change to system, port, connection settings • EVENT - Non-alarm state changes in the system. • MAINT - Maintenance operations
SeqNo	The sequence number for the log entry. The system automatically assigns and tracks sequence numbers. These sequences numbers are shared by the three logs. Therefore, all events can be identified by sequence number order as well as date/time when comparing among the logs.
Operation	The operation is the activity performed by the user or the event detected by the system. The values are related to the message type (above).
Resource	The resource (hardware device, software issue, switch input or output port) on which the alarm condition was detected

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
User ID	For CONFIG and MAINT type messages, the USER ID field will contain the user name for the user that performed the operation. This allows the log viewer to track the activity back to the person that performed the activity.
User IF	For CONFIG and MAINT type messages, the USER IF field will display the user interface from which the above USER ID performed the requested operation (e.g., WEB, TL1, SNMP).
User IP	For CONFIG and MAINT type messages, the USER IP field will display the IP address of the machine the above user used to open the session to the switch. This allows the view to discriminate between the two users logged in from different machines using the same user ID.
Details	This field may contain a series of comma separated KEYWORD=VALUE pairs. The data displayed provides additional information regarding the operation performed by the user. For example, if port attributes are changed, the full port configuration is reported.
Print Report Button Print Report	This button will open a browser window displaying the log contents in a format for printing, with an options to send the view to a printer.
Refresh Button Refresh	This button is used to refresh the log window display to include any events which occurred after the window was opened or last refreshed. The Last Updated time stamp at the bottom of the window indicates the time at which the window was opened or last refreshed.
Clear Button Clear Clear	This button may be used to clear the log. When cleared, a message will be posted in the log indicating the log was cleared as well as the user who cleared the log. This button is dimmed unless the user has Manage system-level privileges.
Close Button Close	This button closes the window.
Last Updated:	The date and time at which the data in the window was last updated (refreshed).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Security (SECU) Log

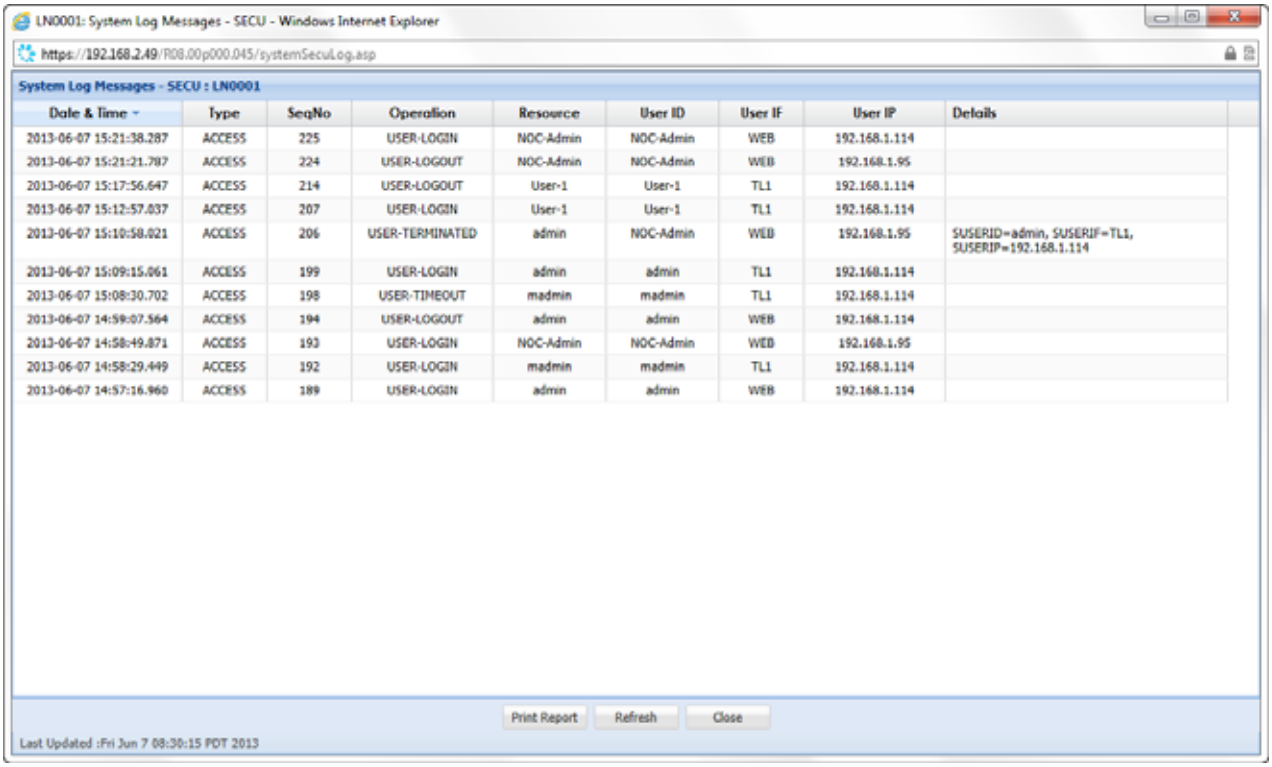
The **System > System Logs > SECU** sub-menu option opens the Security log (Figure 145), which contains entries of the following user and system activities:

- System access activity (e.g., login and logout)
- User configuration (e.g., add/edit/delete)
- System security policy configuration (e.g., account options)

The SECU option will not be available if the user does not have the system-level privilege of Manage. The **System > System Logs** option will not be presented if the user's port privilege is less than View.

- To update the data to current, press the **Refresh** button at the bottom of the window.
- To print the log file, press the **Print Report** button at the bottom of the window. Follow the browser instructions to specify the printer. The browser will display the image of the log file that will be printed.

Figure 145 Security (SECU) Log Window



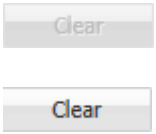
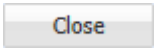
Date & Time	Type	SeqNo	Operation	Resource	User ID	User IF	User IP	Details
2013-06-07 15:21:38.287	ACCESS	225	USER-LOGIN	NOC-Admin	NOC-Admin	WEB	192.168.1.114	
2013-06-07 15:21:21.787	ACCESS	224	USER-LOGOUT	NOC-Admin	NOC-Admin	WEB	192.168.1.95	
2013-06-07 15:17:56.647	ACCESS	214	USER-LOGOUT	User-1	User-1	TL1	192.168.1.114	
2013-06-07 15:12:57.037	ACCESS	207	USER-LOGIN	User-1	User-1	TL1	192.168.1.114	
2013-06-07 15:10:58.021	ACCESS	206	USER-TERMINATED	admin	NOC-Admin	WEB	192.168.1.95	SUSERID=admin, SUSERIF=TL1, SUSERIP=192.168.1.114
2013-06-07 15:09:15.061	ACCESS	199	USER-LOGIN	admin	admin	TL1	192.168.1.114	
2013-06-07 15:08:30.702	ACCESS	198	USER-TIMEOUT	madmin	madmin	TL1	192.168.1.114	
2013-06-07 14:59:07.564	ACCESS	194	USER-LOGOUT	admin	admin	WEB	192.168.1.114	
2013-06-07 14:58:49.871	ACCESS	193	USER-LOGIN	NOC-Admin	NOC-Admin	WEB	192.168.1.95	
2013-06-07 14:58:29.449	ACCESS	192	USER-LOGIN	madmin	madmin	TL1	192.168.1.114	
2013-06-07 14:57:16.960	ACCESS	189	USER-LOGIN	admin	admin	WEB	192.168.1.114	

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

The table below describes the elements of the Security Log window.

Element	Description
Date/Time	The date and time at which the event was detected, with the time recorded down to milliseconds.
Type	This column identifies the operational category for the log entry. These values are: • ACCESS - Login/logout activity • CONFIG - Any change to system, port, connection settings • EVENT - Non-alarm state changes in the system.
SeqNo	The sequence number for the log entry. The system automatically assigns and tracks sequence numbers. These sequences numbers are shared by the three logs. Therefore, all events can be identified by sequence number order as well as date/time when comparing among the logs.
Operation	The operation is the activity performed by the user or the event detected by the system. The values are related to the message type (above).
Resource	The resource (hardware device, software issue, switch input or output port) on which the alarm condition was detected
User ID	For CONFIG type messages, the USER ID field will contain the user name for the user that performed the operation. This allows the log viewer to track the activity back to the person that performed the activity.
User IF	For CONFIG type messages, the USER IF field will display the user interface from which the above USER ID performed the requested operation (e.g., WEB, TL1, SNMP).
User IP	For CONFIG type messages, the USER IP field will display the IP address of the machine the above user used to open the session to the switch. This allows the view to discriminate between the two users logged in from different machines using the same user ID.
Details	This field may contain a series of comma separated KEYWORD=VALUE pairs. The data displayed provides additional information regarding the operation performed by the user. For example, if port attributes are changed, the full port configuration is reported.
Print Report Button Print Report	This button will open a browser window displaying the log contents in a format for printing, with an options to send the view to a printer.
Refresh Button Refresh	This button is used to refresh the log window display to include any events which occurred after the window was opened or last refreshed. The Last Updated time stamp at the bottom of the window indicates the time at which the window was opened or last refreshed.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Element	Description
Clear Button  	This button may be used to clear the log. When cleared, a message will be posted in the log indicating the log was cleared as well as the user who cleared the log. This button is dimmed unless the user has Manage system-level privileges.
Close Button  	This button closes the window.
Last Updated:	The date and time at which the data in the window was last updated (refreshed).

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Web Browser SSL Certificate Warnings

A

For SSL (https), the Intelligent Optical System web server uses self-signed certificates containing the system's default host name (which is derived from the system serial number). If the certificate has not been installed on the web browser PC, a certificate warning message will be displayed by the browser. The following sections define the procedures to install the certificates on Internet Explorer and Mozilla Firefox.

- “Eliminating Security Certificate Warnings in Internet Explorer 7-9”
- “Eliminating Security Certificate Warnings in Firefox 7-13” on page 288

Eliminating Security Certificate Warnings in Internet Explorer 7-9

Follow these steps to eliminate the security certificate warnings in Internet Explorer 7 through 9:

1. Launch Internet Explorer and open a browser window.

2. From the Internet Explorer menu panel, select **Tools > Internet Options...**

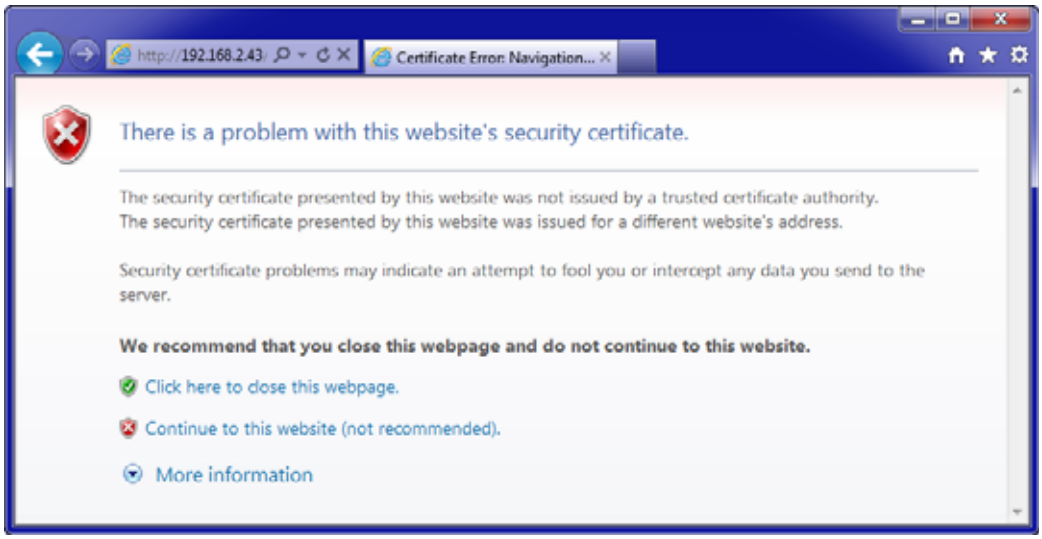
3. Set the Advanced options to disable the certificate address mismatch warning for installed certificates by doing the following:
   a. In the Internet Options window, click on the **Advanced** tab.
   b. In the Advanced tab, scroll to the **Security** section.
   c. Uncheck the option **Warn about certificate address mismatch**.
   d. Click the **Apply** button.
   e. Click **OK** to close the Internet Options window.
   f. Close all Internet Explorer windows.

4. Install each system's ClickFlow SSL certificate by doing the following:
   a. Log into the system using IE; a warning window is displayed (Figure 146 below).
   b. Select **Continue to this website** in the Certificate Error window; the ClickFlow Login window opens (Figure 147 for IE 7 and 8; Figure 148 for IE 9).
   c. Select the **Security Report** icon in the Login window heading.
   d. Select **View Certificates**, a Certificate window opens.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

e. Verify the system hostname is as expected in the Certificate Information **Issued to: system-hostname** line, where *system-hostname* is the system's installation default hostname based on the system serial number.
f. (Optional) Select the **Details** tab and verify the certificate issuer is Glimmerglass Networks.
g. Select **Install Certificate…** in the Certificate window, and then click **Next**.
h. Select the radio button **Place all certificates in the following store** in the Certificate Store window, and then click **Browse**.
i. Select **Trusted Root Certificate Authorities** in the Select Certificate Store window, and then click **OK**.
j. Follow the prompts to complete the installation (select **Next**, **Finish**, **Yes**, **OK**, and **OK)**.

Figure 146 Security Certificate Warning Page



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 147 ClickFlow Login Window after a Certificate Warning (Internet Explorer 7 and 8)

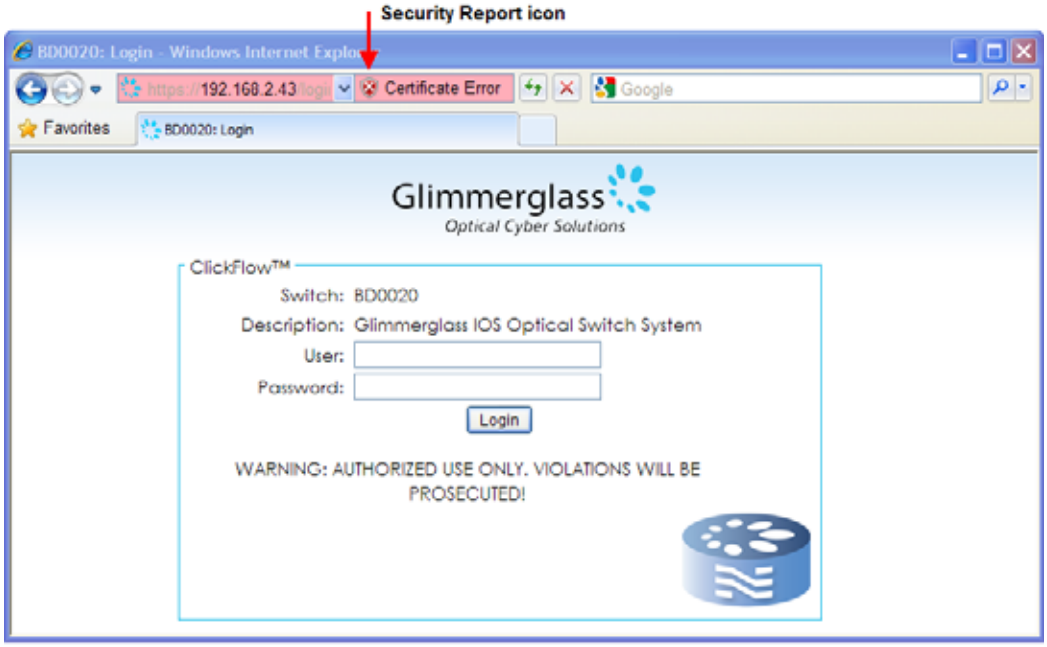


Figure 148 ClickFlow Login Window after a Certificate Warning (Internet Explorer 9)

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

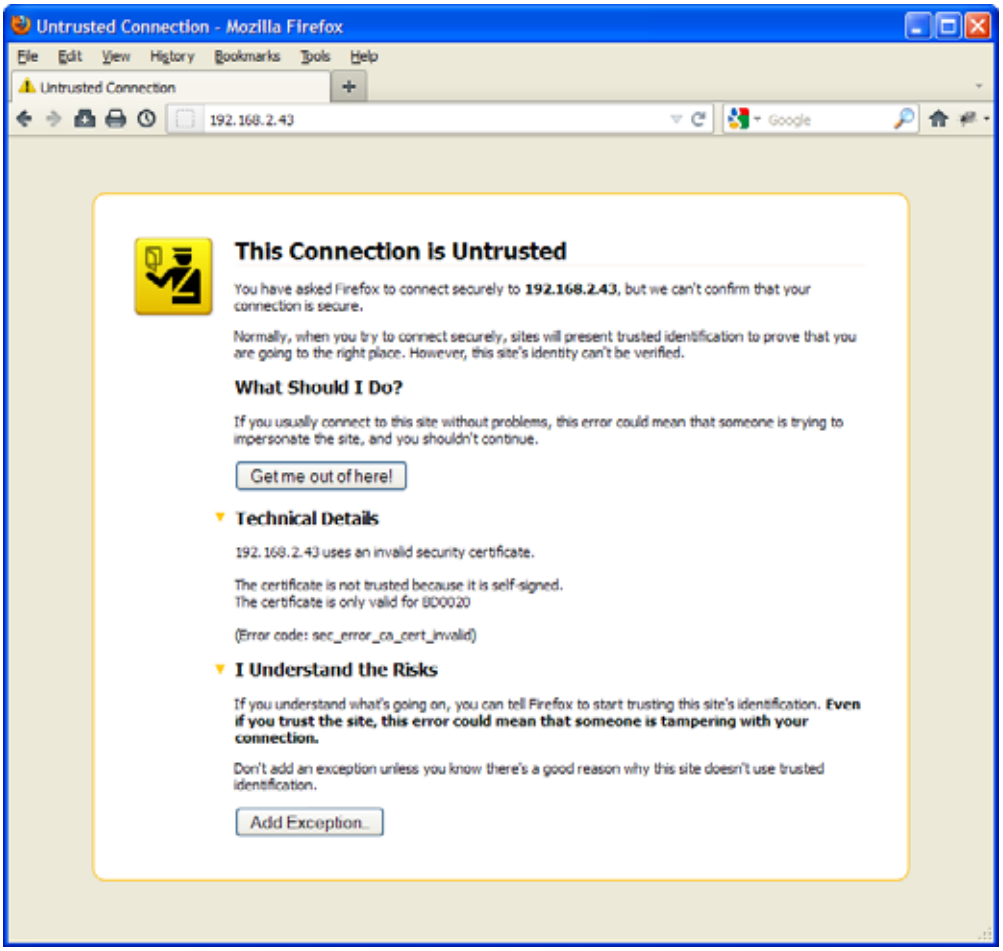
Eliminating Security Certificate Warnings in Firefox 7-13

Follow these steps to eliminate the certificate warnings in Mozilla Firefox:

1. Launch Firefox and open a browser window.
2. Initiate login for the system using Firefox; an “Untrusted Connection” warning window is displayed (see Figure 149 on page 289, in the figure “Technical Details” and “I understand the Risks” have been expanded).
3. Click **Technical Details** and verify that the certificate for this IP address indicates the host name of the system for which you are adding the exception (e.g., "The certificate is only valid for <system's hostname>"), where <system's hostname> is the installation default hostname based on the system's serial number.
4. Click **I understand the Risks**, then click **Add Exception**.
5. (Optional) Click **View** and verify the certificate issuer is Glimmerglass Networks.
6. Click **Confirm Security Exception**.

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Figure 149 Untrusted Connection Window (Firefox 9)



Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

THIS PAGE INTENTIONALLY LEFT BLANK

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

Index

A

account options 249
admin user 172
aging default 253
aging policy 181
alarm severity
    changing 135
alarms 268
    conditions 274
alarms panel 14
arming modes (protection) 155
Attenuate Power mode (for VOA) 165
autosave 244
    delay 245
    description 244

B

build date 95

C

color codes
    legend window 19, 96
configuration settings 19
Configure Port window 45
configure ports
    description 111
configuring connections 143
confirm operation check box 31
confirmation windows 20
connection report
    printing 86
    saving 87
connection restore 245
Connection screen 8
    alarms panel 14
    configuration settings 19
    connection status 18
    I/O matrix 16
    menus 15
    overview 8
    Photonic Multicasting Units 22
    port information 11
    port number 13, 18
    port state 78
    Switched VOA display 29
    system information 21
    VOA displays 25
connections
    breaking 35, 56
    connect all ports 59
    creating 58
    deleting 58
    disconnect all ports 60
    duplex 20
    duration 78
    insertion loss 78, 85
    locked/unlocked 37
    locking 21
    making 33, 53, 54
    names
        changing 144
        clearing 146
    paired 20
    port state 78
    protection rule state 154
    provisioning 31
    provisioning methods 32
    simplex 20
    state 85
    status 18
    status color codes 19
    switch time 78
    updating 36
connections report 83

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

D

date and time 231
Dedicated VOA
    default port names 25
    description 24
    displays 25
default connection mode 247
delay (autosave) 245
duplex
    protection type 153
duplex connections 20
duplex protection 153

E

event reporting mode 246
exporting
    port names/descriptions 119
    protection rules 162
    topology file 70
    user accounts 197, 198

F

file format
    port names/descriptions 114
    protection rules 161
    topology 62

G

group assignment
    changing 130
GUI
    browser requirements 3
    connecting to 4

I

I/O matrix 16
importing
    port names/descriptions 117, 118
    protection rules 160
    topology 69
    topology file 68
        Quick Load list 71
    user accounts 197
    users 196
insertion loss 85

L

lock check box 21
logs 276

M

madmin user 172
menus 15
    Configure 99
    Fiber menu 57
    Port Box context menu 43
    Reports 75
    System 213
    Topology 62
    User Management 182
model number 95

N

no activity timeout 253

P

paired connections 20
passwords
    change policy 179, 180
    changing 185
    complexity policy 178
    default admin password 5
    expiration 179
peer port 13
performance report 77
    printing 79
    saving to file 79
    viewing 79

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

performance switch throttle enable 245
permanent configuration file 244, 245
persistent memory 245
Photonic Multicasting Units (PMUs)
default port names 23
description 22
port box
breaking connection 56
making connection 53, 54
Port Box context menu 43
configure 45
deselect 44
provision 49
port report 80
printing 82
saving to file 83
ports
alarm severity
changing 135
configure attributes 39
configuring 119
connecting 58
connecting all 59
connection 13
description 13
creating import file 116, 117
exporting file 119
importing file 118
disconnecting 58
disconnecting all 60
group 81
group assignment
changing 130
health 81
import file format 114
information 11
name 13
number 13, 18
parameters
clearing 122
peer 13
port group 13
port threshold 13
power 14, 81
signal threshold
changing 126
signal thresholds 41
state 78
user 14
waveband 13
changing 123
wavebands 40
ports per row 248
power
port 81
printing
connection report 86
port report 82
privilege levels
overview 173
privileges 172, 173

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

protection
- description 151
- duplex 153
- simplex 153

protection rules 151
- adding 157
- arming modes 155
- connection type 153
- default settings 156
- deleting 159
- deleting all 160
- duplex 158
- exporting file 162
- file format 161
- importing 160
- printing 163
- protection rule state 154
- symmetric 158
- triggering 156

protection type 153
Provision Connection window 49

Q

Quick Load list 71
- applying a topology 72
- clearing 73

R

reboot 258
reports
- connections 83
- performance 77
- port 80

resize screen size 22
restart 258
runtime options 243
- configuring 248
- connection restore 245
- event reporting mode 246
- performance switch throttle enable 245

S

save configuration 216
Secure Sockets Layer (SSL) 7
serial number 95
session admin 218
set power mode (for VOA) 165
shutdown 258
sign out link 22
signal threshold
- adding 106
- changing 126
- deleting 109
- description 41
- modifying 107

signing out 22
simplex 153
simplex connections 20
simplex protection 153
SNMP 237
snmpuser 172
software version info 21
SSL 7
startup options 254
- configuring 257

state
- connection 85

status report 77
switch time 78
Switched VOA
- default port names 30
- description 26
- display 29

syslog 240

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

system
- account options 249
- date and time 231
- hardware 93
- information 21, 93
- IP 226
- maintenance 257
- name 226
- reboot 258
- restart 258
- rollback 266
- rolling back software 268
- runtime options 243
- save configuration 216
- session 21
- session admin 218
- shutdown 258
- SNMP 237
- startup options 254
- syslog 240
- system alarms 268
- system backup/restore 219
- system logs 276
- upgrade 260
- upgrade/rollback 259
- upgrading software 264

system alarms 268
system backup 219
system information 93
- build date 95
- model number 95
- serial number 95

system log 240
system logs 276
System menu 213
system ports
- default port numbers 255

system preferences 231, 243
system restore 219

T

topology
- connection mode 68
- export 70
- export file format 70
- exporting 71
- import 68
- import file format 62
- import/export 62
- importing file 69

triggering (protection) 156

U

user accounts
- adding a user 186
- aging default 253
- aging policy 181
- configuring account options 254
- default accounts 172, 182
- default admin user 5
- deleting a user 194
- editing a user 190
- editing password 183
- editing the XML file 211
- exporting 198
- importing file 197
- importing users 196
- lockout duration 253
- max invalid logins 253
- no activity timeout 253
- XML file 203
- XML file considerations 209

user management
- delete user 194
- edit user 190
- export users 197
- set password 185

user privileges 172, 173
user session
- logged in user 21
- logging in 5
- signing out 22
- status 21

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved

V

Variable Optical Attenuation (VOA) ... 164
configuring ... 166
description ... 24
guidelines for operation ... 170
guidelines for use ... 168
hardware implementations
Dedicated VOA ... 24
Switched VOA ... 26
modes of operation ... 165
Attenuate Power ... 165
set power ... 165
performance specifications ... 165
Virtual Private Switch (VPS)
description ... 177

W

waveband
changing ... 123
description ... 40
windows
Configure Port ... 45
Provision Connection ... 49

X

XML users file ... 203
considerations ... 209
editing ... 211

Copyright 2013 Glimmerglass Networks, Inc.
All rights reserved