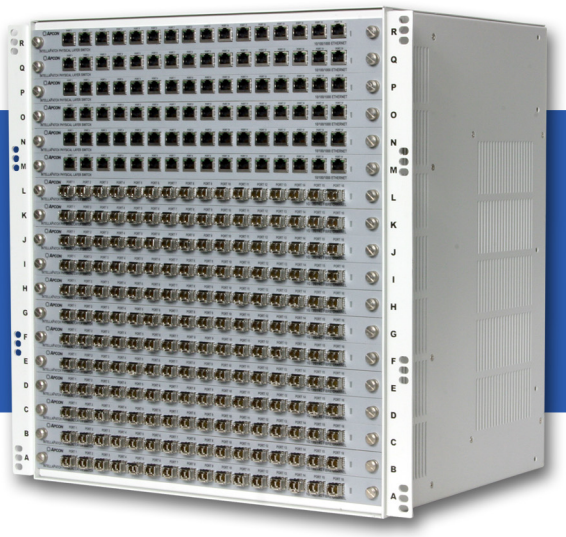
MultiDyne
Video & Fiber Optic Systems

# INTELLAPATCH™

## Physical layer Switch Product Documentation

# ACI-2058 User Manual

### Eighteen Blade Slots • Up to 288 ports



**MultiDyne**
877.MultiDyne | www.multidyne.com
A54-2058-000 | Rev A

# Contents

## Figures



## Tables

# Chapter 1

# Preface

The APCON ACI-2058 INTELLAPATCH™ physical layer switch enables efficient, cost-saving management at the foundation of your enterprise network or interoperability test lab—the physical layer.

With a compact design that saves valuable rack space, the ACI-2058 provides up to 288 ports of any-to-any connectivity at full wire speed. You can populate the 11U chassis with up to eighteen blades to support a wide array of protocols, including 1, 2, and 4Gb/s Fibre Channel, Ethernet from 10 Mb/s to 10 Gb/s,T1/E1/J1, DS3/E3/STS-1, SONET/SDH, and FDDI.

## 1.1. About This Manual

This manual assists those who automate, control, and manage networks using the ACI-2058.

This manual assumes you know how to:

- Connect and disconnect standard types of cables
- Use and configure operating systems and networks.

### 1.1.1. Contents

This manual contains the following:

| Chapter/Appendix | | Description |
|---|---|---|
| 1 | Preface | Explains how to use this manual. |
| 2 | Introduction | Describes features of the ACI-2058. |
| 3 | Install and Set Up the Switch | Explains how to install APCON software, access an APCON switch, and run the software. |
| 4 | Connect to a Host | Explains how to establish an Ethernet connection and connect to a host computer. |
| 5 | Maintaining the Switch | Explains how to remove and re-install blades, tranceivers, and power supplies for repair or upgrade. |
| A | Serial Port Pinout | Lists and describes each pin of the RS-232 serial port. |
| | Index | Lists product topics for quick reference. |

### 1.1.2. Text Conventions

This manual uses the following conventions:

| | |
|---|---|
| > | Indicates the movement through menu options. For example, the sequence for changing the switch name is:<br>Views>Switch Details |
| `MonoText` | Indicates information that displays on the screen. |
| **`MonoBold`** | Indicates information you type. |
| *`ItalicText`* | Variable parameters. |

| | |
|---|---|
| Note | Indicates important information about the product. |
| ESD CAUTION | Indicates situations that may cause damage to hardware via ESD (ElectroStatic Discharge). |
| CAUTION | Indicates potentially hazardous situations which, if not avoided, may result in minor or moderate injury, or damage to data or hardware. It may also alert you about unsafe practices. |
| WARNING | Indicates potentially hazardous situations which, if not avoided, can result in death or serious injury. |
| DANGER | Indicates imminently hazardous situations which, if not avoided, will result in death or serious injury. |

## 1.2. Related Products

APCON provides these software products that you use to access and control your INTELLAPATCH switch(es):

- WEBX, embedded in the ACI-2058, controls the ACI-2058 remotely from a web browser over a network or the Internet. For security, you can enable SSL.
- CONTROLX, included on the CD that comes with your INTELLAPATCH switch, provides an easy-to-use, menu-driven drag-and-drop graphical user interface (GUI) that you use to operate and reconfigure ports from a host computer running Windows NT, 2000, or XP, or the Linux or Solaris operating systems.
- APCONCMDX provides an interactive Telnet and SSH command line interface.
- Firmware Direct Commands, embedded in the ACI-2058, control the ACI-2058 using any scripting language (such as Tcl or Perl) that supports reading from and writing to serial or socket connections.
- C/C++ API provides programmatic access to the switch. To acquire this product, contact APCON as described in the next section.

Additional software can be purchased for application-specific purposes.

## 1.3. Contacting APCON

You can find out more about INTELLAPATCH products from these sources:

- **Release notes**: Lists features and issues that arose too late to include in other documentation.
- **World Wide Web**: APCON maintains an active site on the World Wide Web. The site contains current information about the company and locations of sales offices, new and existing products, contacts for sales, service, and technical support information. You can also send email to APCON using the web site.
  - To access the APCON web site, enter this URL in your web browser:

    http://www.apcon.com
  - To contact APCON technical support, enter this URL in your web browser:

    http://www.apcon.com/support

    **Note**

    When sending email for technical support, please include information about both the hardware and software.
- If you purchased your product from MultiDyne, please contact your MultiDyne sales representative via email or phone.

  Email: sales@multidyne.com

  Telephone: 516.671.7278
  Fax: 516.671.3362

Chapter 2

# Introduction

APCON's ACI-2058 INTELLAPATCH physical layer switch enables intelligent, flexible control of your test lab or enterprise network. The physical layer switch cross-connects copper and optical cables, providing easy-to-use point-to-point, multicast, and loop connectivity across a nonblocking, full line-rate switching matrix.

## 2.1. Features

The ACI-2058 offers the following features:

- Electronic physical layer switch with up to 288 ports and eighteen blades in an 11U height
- Transparent electronic switching
- Compliant with 1, 2, and 4 GB Fibre Channel, 10 Gigabit Fibre Channel, 10/100/1000 and 10 Gigabit Ethernet, SONET OC-3, OC-12 and OC-48, T1/E1/J1, DS3/E3/STS-1, and FDDI (blade-specific)
- Small Form Factor Pluggable (SFP) transceiver module support
- Signal regeneration (blade-dependent)
- 10 Mbit to 10 Gbit/sec port data rate capability
- 1.26 Tb/sec switching capacity per chassis
- Connections from 1 meter to 10 Km (fiber optic) and up to 100 meters for copper Ethernet (blade-specific; fiber optic varies by transceiver)
- Two LAN ports and two serial ports for remote software execution
- Windows†, Linux†, and Solaris† support for APCON CONTROLX GUI software
- Support for multi-user sessions
- Embedded web management software for drag-and-drop patching, SSL included
- Embedded Telnet command-line interface with SSH client support (uses APCONCMDX syntax)
- Embedded ASCII command set interface (backwards-compatible with custom scripts)
- Sixteen user-defined preset patching configurations

Each switch can control up to 288 independent fiber optic or copper ports, with the ability to connect any port to any other port. All ports are fully bi-directional, offering complete flexibility in determining where to connect host computers, targets, switch ports, or other network devices. You can configure fiber optic or copper connections remotely to eliminate manual manipulation of connections.

The ACI-2058 can be externally connected to any AC input voltage between 100 and 240 volts; three hot-swappable AC power supplies provide redundant power to the unit,

auto-ranging input voltages between 90 V AC and 240 V AC. If one power supply fails, operation is not affected.

The ACI-2058 has two LAN ports that support Ethernet connections and two RS-232 ports that support the serial interface. You can connect up to 32 INTELLAPATCH switches at once and control them using one serial port, or any number of INTELLAPATCH switches using one LAN port.

The physical layer switch has a variety of redundant components to ensure uninterrupted operation:

- The switch has three hot-swappable power supplies, only two of which are necessary for operation.
- A wide variety of blades (see *Blades* on page 6) can be installed and removed during operation.

The ACI-2058 increases the distance capability of each fiber optic connection by regenerating the optical signal, thereby improving performance and reliability due to reduced cable and interconnection losses. The ACI-2058 allows standard optical connections to extend up to various distances, depending on the transceiver module — typically from one meter to 300–550 meters using multimode transceivers, and up to 10 Km using single-mode transceivers.

Copper Ethernet connections of 10, 100, or 1000 Mb/second have a signal distance limit of one hundred meters. The ACI-2058 regenerates these signals as well, so that they can reach an additional one hundred meters when patched to another device.

## 2.2. Specifications

**Table 1. Specifications**

| Item | Number | Description |
|---|---|---|
| ACI-2058-C00: 288-port chassis | Number of blade slots | Eighteen |
| | Number of ports | Up to 288 (depending on blade type) |
| | Protocol | Various; see *Blades* on page 6 |
| | Blade data rate | 10 Mbit to 10Gbit/sec |
| Serial interface | Baud Rate | 9600 baud |
| | Mode | No parity, 8 bits, 1 stop bit, software flow control |
| | Maximum cable length | 15 meters (50 feet) |
| | Rear panel connectors | DB-9 |
| LAN port | Protocol | TCP/IP |
| | Interface | 10/100/1000 Base-T Ethernet |
| | Rear panel connector | RJ-45 |
| Physical | Mechanical | 16.75" W x 15.00"D x 18.80"H<br>(42.5 cm W x 38.1 cm D x 47.8 cm H) |
| | Weight | 34 pounds (15.4 kg) without blades or transceiver modules |
| | Power | 100 to 240 V AC 50 / 60 Hz (800 A) |
| | Temperature Operating<br>Storage | 0°C to 50°C (32°F to 123°F)<br>–40°C to 85°C (–40°F to 185°F) |
| | Humidity | 0% to 90% RH (noncondensing) |
| | Rack mount | 19 inches, 11U |
| Agency approvals | UL, FCC Class A, CE | |

## 2.3. Blades

The ACI-2058's modular design enables you to manage multiple protocols and data rates in a single chassis. You can populate the switch with up toeighteendifferent blades, each blade having from four to sixteen ports. In addition to one-to-one, one-to-many, and loop connectivity, blades can provide the following capabilities:

- **Media conversion.** Some blades use optical connectors while others use electrical. Connect a port on a fiber optic blade to a port on a blade using copper connectors and, dependent on the blade model, the ACI-2058 seamlessly converts signals from one medium to the other, assuming that the optical and copper blades use the same protocol.

  Optical signals can also be converted from multimode (shortwave) to single-mode (longwave).

- **Repeater.** Most blades for the ACI-2058 extract the clock from the signal, clean up jitter, and then add the clock back to the signal.

- **Retimed signals.** Certain blades for the ACI-2058 extract the clock from the signal, clean up jitter, and then add a *switch-generated clock* back to the signal.

The specific blades available for the ACI-2058 include:

| Model | Description |
|---|---|
| ACI-2059-B16-1 | Blank cover panel for unused blades |
| ACI-2059-E16-2 | 16-port multi-rate, 10/100/1000 Mb/s, copper (RJ-45) |
| ACI-2059-E16-1M1 | 16-port Fast Ethernet, 100 Mb/s, 1310nm multimode optical (LC) |
| ACI-2059-E16-1M2 | 16-port Gigabit Ethernet, 1.25 Gb/s, 850nm multimode optical (LC) |
| ACI-2059-E16-1M3 | 16-port FDDI, 100 Mb/s, 1300nm, multimode optical (LC) |
| ACI-2059-E16-1M4 | 16-port Gigabit Ethernet, 500 Mb/s-1.25 Gb/s, 850nm multimode optical (LC) |
| ACI-2059-E16-1M6 | 16-port ESCON, 200 Mb/s, 1310nm multimode optical (LC) |
| ACI-2059-E16-1S1 | 16-port Gigabit Ethernet, 1.25 Gb/s, 1310nm single-mode optical (LC) |
| ACI-2059-E04-3M | 4-port Ethernet, 10 Gb/s, 850nm multimode optical (LC) |
| ACI-2059-E04-3S | 4-port Ethernet, 10 Gb/s, 1310nm single-mode optical (LC) |
| ACI-2059-F16-1C | 16-port Fibre Channel, 1 and 2 Gb/s, copper (HSSDC-2) |
| ACI-2059-F16-1M | 16-port Fibre Channel, 1 and 2 Gb/s, 850nm multimode optical (LC) |
| ACI-2059-F16-1S | 16-port Fibre Channel, 1 and 2 Gb/s, 1310nm single-mode optical (LC) |
| ACI-2059-F16-6M | 16-port Fibre Channel, 1, 2 and 4 Gb/s, 850nm multimode optical (LC) |
| ACI-2059-F04-3S | 4-port Fibre Channel, 10 Gb/s, 1310nm single-mode optical (LC) |
| ACI-2059-I16-3S1 | 16-port SONET OC-3, 155 Mb/s, 1310nm single-mode optical (LC) |
| ACI-2059-I16-3M2 | 16-port SONET OC-12, 622 Mb/s, 1310nm multimode optical (LC) |
| ACI-2059-I16-3S2 | 16-port SONET OC-12, 622 Mb/s, 1310nm single-mode optical (LC) |
| ACI-2059-I16-3S3 | 16-port SONET OC-3/OC-12/OC-48, Gigabit Ethernet, 1310nm single-mode optical (LC) |
| ACI-2059-M16-1M | 16-port multirate, Gigabit Ethernet, Fibre Channel 1 and 2 Gb/s, 850nm, multimode optical (LC) |
| ACI-2059-M16-1 | 16-port multirate, 100 Mb/s–3.2 Gb/s (depends on SFPs installed; contact factory) |
| ACI-2059-D08-1 | 8-port DS3/E3/STS-1, 44.7 MHz/34.3 MHz/51.8 MHz copper (mini-BNC) |
| ACI-2059-T08-1 | 8-port T1/E1/J1, 44.7 MHz/34.3 MHz/51.8 MHz copper (mini-BNC) |

## Transceiver Modules

Some blades for the ACI-2058 use Small Form Factor Pluggable (SFP) transceiver modules. SFP modules are available for all supported data rates and protocols, with the following features:

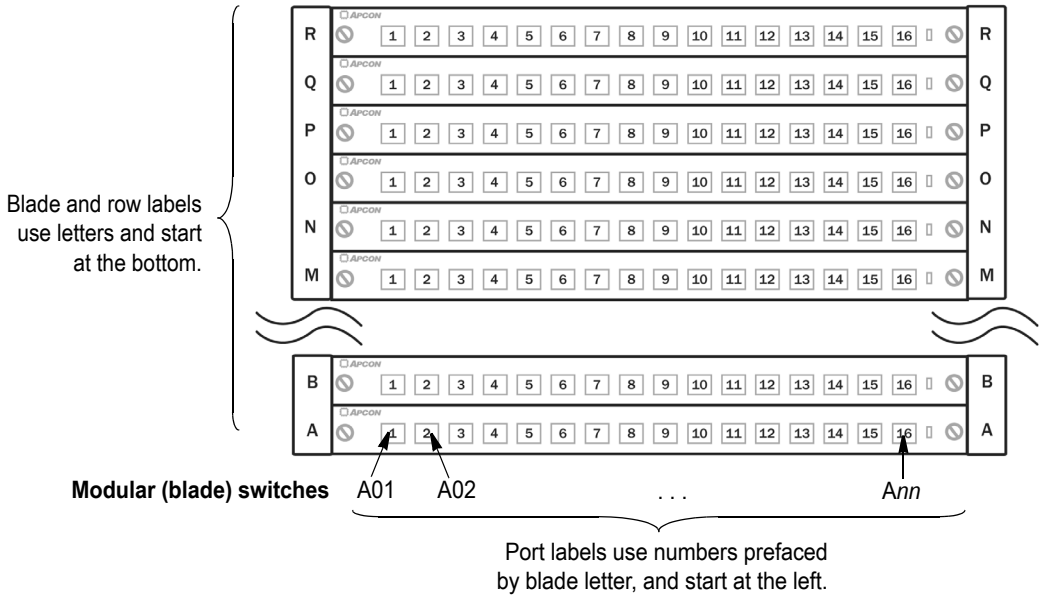
- SFP module types include:
  - **Copper SFP transceivers**, available for Fibre Channel (HSSDC-2) and Gigabit Ethernet (RJ-45).
  - **Multimode (MMF) or single-mode (SMF) fiber optic SFP transceivers**, available for Ethernet, Fibre Channel, SONET OC-3, OC-12, OC-48 and FDDI.
- SFP transceivers have duplex LC fiber optic connections.
- Each transceiver provides built-in Serial ID capabilities. Use APCON's CONTROLX or WEBX to obtain information about the transceiver's manufacturer, part number, serial number, revision, date of manufacture, and other module-specific parameters.

- SFP transceivers used in the ACI-2058 are hot-pluggable, allowing you to change the transceiver while the unit is operating and under power.
- You can view SFP transceivers with digital diagnostic support using APCON's CONTROLX or WEBX.

## 2.4. Switch labeling

To identify each port, modular switches use the following conventions:

**Figure 1. ACI-2058 Port Labeling**




Blades have varying numbers of ports, and a chassis may or may not be fully populated with blades. The greatest number on each blade and the greatest letter in each chassis varies according to the number of ports in a blade and the number of blades installed in a chassis.

The ACI-2058 refers to ports using these labels. You can use the ACI-2058 to assign names to your ports, names that indicate devices they connect to or to provide other meaningful aids to memory.

## 2.5. Software

APCON provides these software products that you can use to access and control your INTELLAPATCH switch(es):

- WEBX, embedded in the ACI-2058, controls the ACI-2058 remotely from a web browser over a network or the Internet. For security, you can enable SSL.
- CONTROLX, included on the CD that comes with your INTELLAPATCH switch, provides an easy-to-use, menu-driven drag-and-drop graphical user interface (GUI) that you use to operate and reconfigure ports from a host computer running Windows NT, 2000, or XP, or the Linux or Solaris operating systems.
- APCONCMDX provides an interactive Telnet and SSH command line interface.

- Firmware Direct Commands, embedded in the ACI-2058, control the ACI-2058 using any scripting language (such as Tcl or Perl) that supports reading from and writing to serial or socket connections.
- C/C++ API provides programmatic access to the switch. To acquire this product, contact APCON as described in the next section.

Additional software can be purchased for application-specific purposes.

All software interfaces provided for the ACI-2058 include these features, as well as many others:

- Patch ports and view port status.
- Store and recall presets.
- View power supply status.
- View the chassis internal temperature, set a temperature threshold for an internal alarm.
- Configure the serial and LAN ports.
- On supported blades, set the data rate and duplex settings.

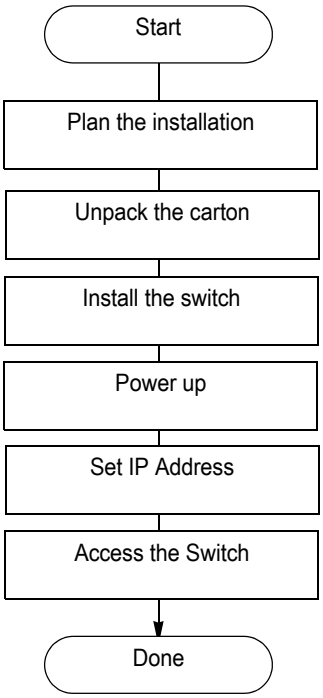
To retain configuration and setup information, the ACI-2058 has internal nonvolatile memory; port settings and control parameters are saved as they are entered.

Chapter 3

# Install and Set Up the Switch

To install the ACI-2058, follow these steps:

**Figure 2. Installing the Switch**




The rest of this chapter details the above steps.

If you experience difficulty during installation, contact your sales office or APCON Technical Support. as described in *Contacting APCON* on page 3.

## 3.1. Plan the Installation

Do this planning before you start installation:

- If you plan to rack-mount the chassis, ensure you have the tools needed to mount the chassis flanges to the rack.
- Ensure there is enough power into the rack to support all units you plan to install. For power requirements, see the Power section in *Table 1, "Specifications,"* on page 6.
- Plan how to route fiber-optic and Ethernet cables to the ACI-2058. Also acquire the cables. The ACI-2058's fiber-optic connectors are of the LC duplex type.
- Plan how to meet the chassis' requirement for air that enters via the left side (as you face the unit) and exits at the right.

- Determine what optional software, if any, to use to communicate between the host computer and the switch. If you plan to use the APCON CONTROLX interface, you will need to install it as described in *Install Optional Software* on page 13.

## 3.2. Unpack the Carton

Unpack the carton(s) and do the following:

- Inspect all components for any sign of damage.

**Note**

- If the shipping carton is damaged or water-stained, please contact the freight carrier for inspection of carton and contents.
- To return a product damaged in shipment, contact APCON to obtain a Return Merchandise Authorization (RMA) number and further instructions.

- Verify you have the items you ordered. A standard ACI-2058 switch kit includes these items:

**Note**

If any modules are in ESD shielding bags, do not yet remove them from the bags.

  - One ACI-2058 INTELLAPATCH physical layer switch chassis
  - Two rack mount brackets (attached to the chassis)
  - Four bottom “feet” (for tabletop, non-rack mount installations)
  - Three AC power cables (110 or 220 V)

**Note**

Unless otherwise specified, the ACI-2058 ships with 110-volt power cords. APCON offers a complete selection of replacement power cords for most countries.

  - One 10 foot RS-232 cable, 9-pin male to 9-pin female
  - One RS-232 adapter, 9-pin male to 25-pin female
  - Blades and transceivers, as ordered
  - One APCON software CD
  - One INTELLAPATCH Product Documentation binder which includes all your INTELLAPATCH documentation, including this guide.

## 3.3. Install the Switch

You can place the ACI-2058 on any stable surface or install it in a standard 19-inch (EIA unit) rack.

**⚠ CAUTION**

- Ensure that the unit remains within the temperature limits detailed in *Specifications* on page 6.
- Place the ACI-2058 in a location that allows adequate airflow to the fans and ventilation slots on the sides of the unit.
- Do not place the ACI-2058 on any device that generates excessive heat.

### 3.3.1. Rack Installation

The ACI-2058 ships with rack mount flanges attached. To install the switch in a rack:

1. Set the unit into position on the rack, aligning the mounting bracket holes with the rack holes.
2. Install the chassis in the rack, securing the chassis with the appropriate screws.

**Note**

If the switch is installed in a rack with other equipment, ensure that you don't overload the wiring circuits. In all cases, make sure power strips and wall sockets are grounded.

### 3.3.2. Table Top Installation

The ACI-2058 ships with "feet" for installation on a flat surface, such as a workbench. To attach the "feet" to the switch:

1. Remove the backing from a "foot".
2. Attach the "foot" to a bottom corner of the switch.

Repeat these steps for each of the four "feet."

### 3.3.3. Install Blades and Transceivers

The ACI-2058 typically ships with all blades and transceivers installed. If they are not installed or if you need to move them, see *Blades* on page 20 or *Transceiver Modules* on page 21.

## 3.4. Power Up

1. Turn on the ACI-2058's three AC power switches, located on the rear panel.
2. Verify each power supply's operation by checking the LEDs:

**Table 2. LED Operation**

| LED state | Description |
|---|---|
| Power LED lit | The power supply is functioning normally. |
| Fault LED lit | The power supply is not functioning. |
| Power and Fault LEDs off | The power supply is not functioning. |

Threehot-swappable AC power supplies provide redundant power to the unit. If one power supply fails, operation is not affected; however, an alarm sounds and that supply's fault LED lights. This alarm can be turned off using any of the software interfaces; for instructions, see the specific software manual.

Figure 3. ACI-2058 Rear Panel

## 3.5. Set the IP Address

For details, see *Setting the IP Address* on page 14.

## 3.6. Access the Switch

### 3.6.1. Use Embedded Software

The following software is embedded in your ACI-2058 switch. These applications are immediately available for use without reconfiguration or installation:

- **WEBX**, an embedded web interface.
- **APCONCMDX**, a command line interface.
- **Firmware Direct Commands**, ASCII programmatic access.

For usage details, see the appropriate software User Manual.

### 3.6.2. Install Optional Software

To communicate with the switch from a host computer, you can use CONTROLX, included on the CD-ROM that comes with the ACI-2058. To use CONTROLX, install it on the host computer you plan to use to control the ACI-2058:

1. Insert the CD into the host computer, or download the latest version from the APCON website:

   `http://www.apcon.com`

2. Follow the onscreen prompts.

You are now ready to connect the ACI-2058 to a host. For details, see *Chapter 4, Connect to a Host*.

Chapter 4

# Connect to a Host

To operate the ACI-2058, you must connect the unit to a host computer running a Windows, Linux, or Solaris operating system. Once connected, you can use one or more of these to control the switch:

- WEBX (using standard HTTP or SSL)
- CONTROLX (requires installation, as described in *Install Optional Software* on page 13)
- APCONCMDX, which you can access via Telnet or SSH.
- Firmware Direct Commands

To use CONTROLX, WEBX, or APCONCMDX, you must establish an Ethernet connection. This chapter explains how.



## 4.1. Overview

You can control the ACI-2058 using one of these methods:

- **Ethernet connection running TCP/IP**: The ACI-2058 includes two 10/100/1000 Ethernet LAN ports.To use this method, you must assign the switch a static IP address appropriate for your network.
- **Serial connection**: Two RS-232 serial ports. To use this method with either custom scripts or CONTROLX, you do not need to set the IP address and other TCP/IP properties.

If desired, you can connect the ACI-2058 to multiple hosts, using any combination of a two serial or two Ethernet ports.

## 4.2. Setting the IP Address

By default, INTELLAPATCH switches are shipped with an IP address of 192.168.0.1, a subnet mask of 255.255.255.0, and no gateway. If it's convenient to configure your host computer with an IP address of the form 192.168.0.*x* (where *x* is any number from 2 to 254, inclusive), then the ACI-2058 is immediately available.

If not, then, to use the Ethernet connection, you must change this default IP address to one appropriate for your network.

You can set the IP address in a variety of ways; these instructions show you how to set the address using WEBX.

**Note**

If you plan to use more than one INTELLAPATCH switch on your network, configure them at the same time. This avoids repeated temporary disconnections of the host computer from your network.

To configure the IP address, subnet mask, and gateway:

1. Ensure that you have the following:
   - A web browser that supports Javascript including, but not limited to:
     - Firefox† browser, version 1.x or later
     - Internet Explorer, version 6.x or later
     - Netscape† browser, version 7.x or later (the WEBX Interface is *not* compatible with version 4.x)
     - Opera
     - Safari† browser

     **Note**

     Ensure that your browser's Javascript is enabled.
   - A host computer that runs one of the above web browsers. The host computer's web browser accesses the interfaces embedded in the ACI-2058.
   - An Ethernet connection between the host computer and the switch.
   - An IP address, subnet mask, and gateway (if required) appropriate for your network to assign to the switch.
2. Connect a host computer to the ACI-2058:
   A. Quit all network client applications currently running on the host computer.
   B. Disconnect from your network the host computer you plan to use to assign the IP address.
   C. Plug the host computer's cable into one of the Ethernet ports on the back of the INTELLAPATCH switch using either a standard patch cable or a crossover cable.

   The host and switch are now physically connected.
3. Enable communication between the host computer and switch.
   A. Access the host computer's current network settings according to the instructions provided with the host's operating system. Note them so that you can restore them at the end of this process.
   B. Temporarily change the host settings to the following:
      - IP address: 192.168.0.$x$
        ($x$ is any number from 2 to 254, inclusive)
      - Subnet mask: `255.255.255.0`
      - Gateway setting: `0.0.0.0` or blank

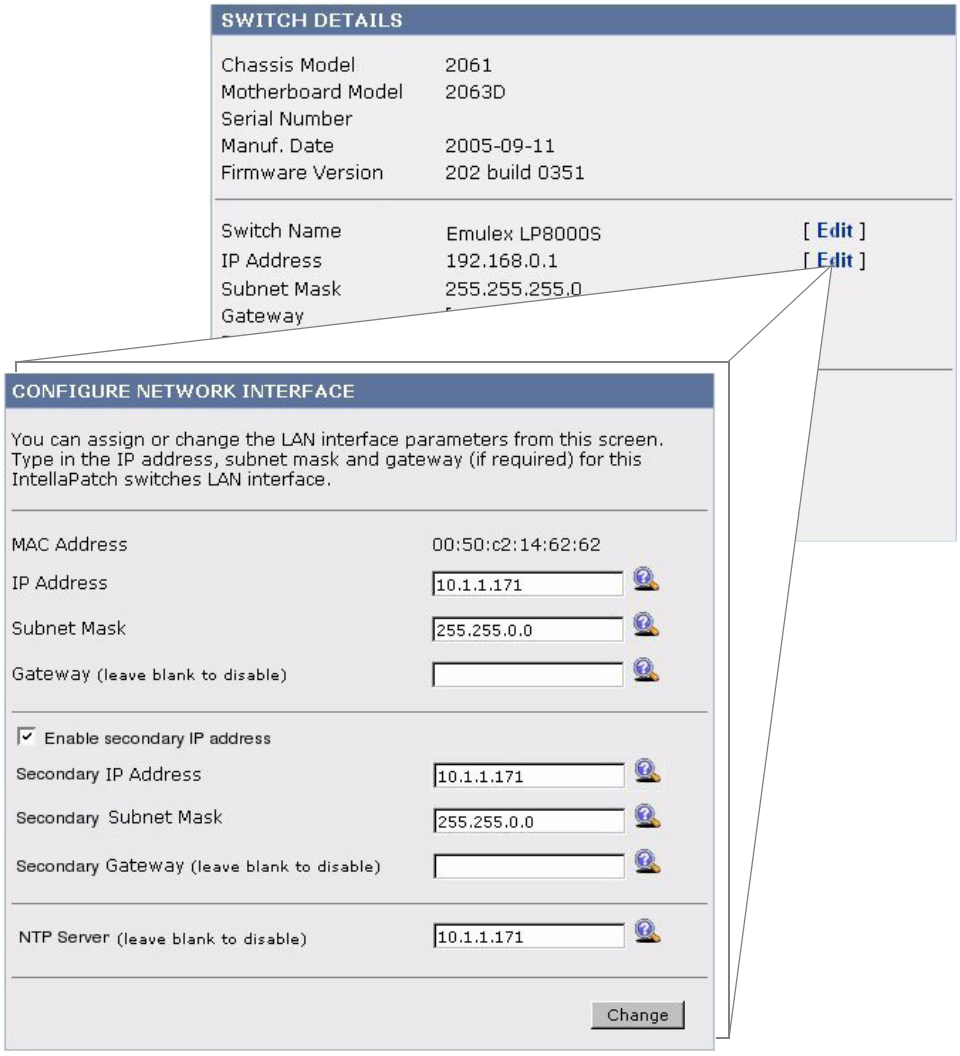
   The host and switch are now on the same network and can communicate.

4. Access the switch's WEBX Interface.
   A. On the host computer, open a web browser.
   B. If the host computer is configured to use a proxy server, disable the proxy setting.
   C. In the browser's address field, enter:

      `http://192.168.0.1`

   D. Click the Edit link, located to the right of the IP Address field. The Configure Network Interface screen displays:

**Figure 4. Configure Network Interface screen**




5. Change the IP address:
   A. Type the new IP address, subnet mask (if required), and gateway (if required) in the fields provided.

| Note |
| --- |
| The subnet mask assigned to the switch must match the host computer's subnet mask. |

B. Click the Change button. The switch reroutes the browser to the new address.

C. Exit the browser.

6. Reconnect the host computer to your network.

A. Reset the host computer's IP address, subnet mask, and gateway settings to their original values.

B. Re-cable the host to the network.

C. Ensure that the switch is cabled to the network with a standard Ethernet patch cable.

You can now configure the ports as desired, using the software interface of your choice, and begin using the switch.

## 4.3. Connecting Multiple Switches

You can configure the serial ports to operate as daisy-chained ports. Daisy-chaining switches allows one computer or terminal to communicate with up to 32 INTELLAPATCH switches.

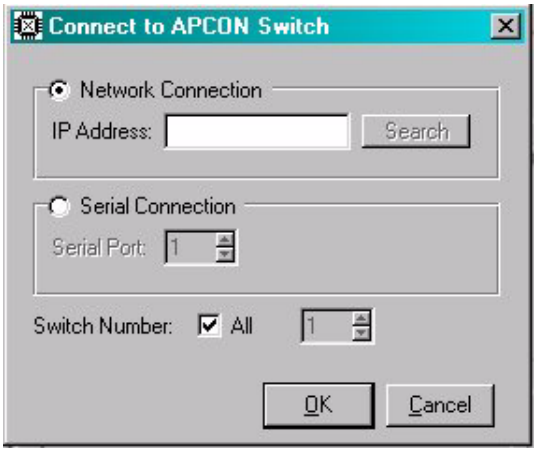
You can use the LAN ports to connect any number of switches without using a hub or wall jack.You cannot, however, mix serial and LAN port connections in a single chain.

### 4.3.1. Connecting Multiple Switches with Serial Ports

CONTROLX recognizes from 1 to 32 INTELLAPATCH switches when daisy-chained. If you plan to use multiple switches daisy-chained together, you must first assign a unique device number to each switch. To do so:

1. Connect the second switch to the host computer using the switch's COM1 port and a standard 9-pin straight-through serial cable. (The first switch already has its device number set to 1 by default.)
2. On the host computer, start CONTROLX.
3. Select File>Connect. The Login dialog displays:

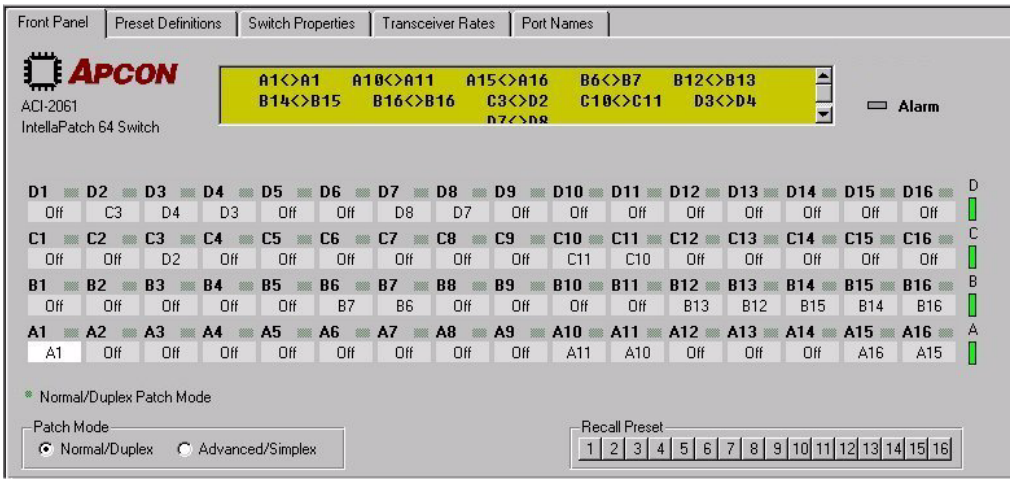
**Figure 5. CONTROLX Login Dialog**




4. Click the Serial Connection radio button. Leave the field set to 1 for the COM1 port (or change to the specific COM port number of your workstation).
5. Click the OK button.

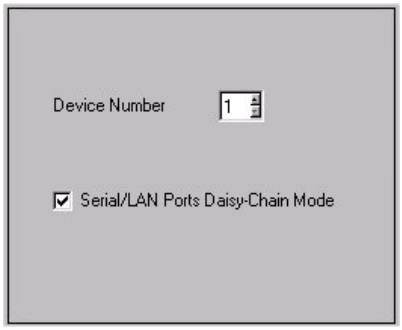
6. Click the Switch Properties tab.

**Figure 6. Switch Properties**




7. Click Communications in the Property List.

**Figure 7. Communications Fields**

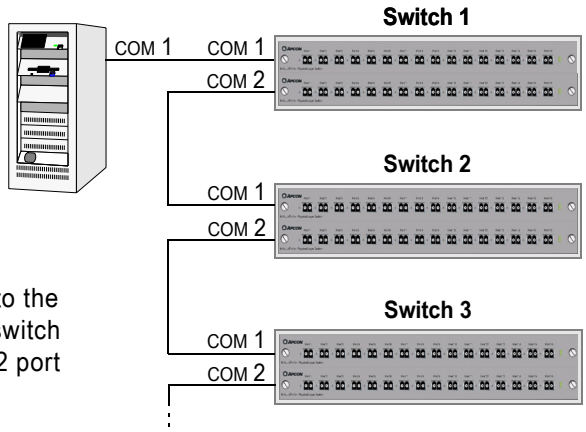



8. Type 2 in the Device Number field.
9. Click the OK button to save the setting.
10. Click the OK button to exit the Switch Properties tab.
11. Exit CONTROLX.
12. Un-cable the switch and cable the host computer to the next switch.
13. Following this procedure, set the next Device Number to 3.

14. Repeat the last two steps until all the switches that you wish to daisy-chain have a unique device number between 1 and 32.

With unique device numbers, you can now daisy-chain the switches:

1. Connect the host computer's COM port to the COM1 port on the first switch (device number 1) using a standard 9-pin straight-through serial cable.
2. Connect the COM2 port on switch 1 to the COM1 port on the switch having the device number 2.
3. Connect the COM2 port on switch 2 to the next switch, and so on until the last switch is connected. The last switch's COM2 port remains unconnected.




## 4.3.2. Connecting Multiple Switches with LAN Ports

To connect more than one switch using LAN ports:

1. Assign each device a unique IP address. (For details on how to do this, see *Setting the IP Address* on page 14.
2. Connect the host computer to one of the first switch's LAN ports (using either an Ethernet crossover cable or a straight Ethernet cable) or connect the first INTELLAPATCH switch to an Ethernet hub or switch connected to your network.
3. Connect the first switch's unused LAN port to either of the next switch's LAN ports with an Ethernet cable (either kind), or connect the next switch to the network hub.
4. Repeat step 3 until all switches are connected.

You can now configure the ports as desired, using the software interface of your choice, and begin using the switch.

Chapter 5

# Maintaining the Switch

Occasionally you will want to perform maintenance or upgrades on the ACI-2058 or its blades. When this occurs, you may need to do one or more of the following:

- **Blades**: Remove a blade from the chassis, repair or install the desired option, then re-install the blade. For details, see page 20.
- **Transceiver Modules**: Remove or re-locate transceivers, disconnect and reconnect the cable. For details, see page 21.
- **Power Supplies**: Remove a power supply from the chassis, repair or install the desired option, then re-install the power supply. For details, see page 22.

## 5.1. Blades

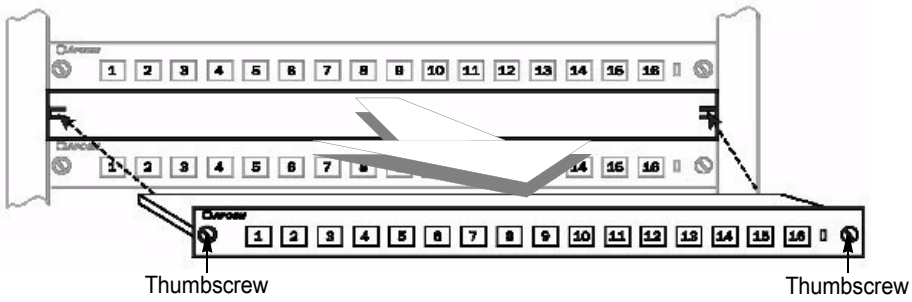
The ACI-2058 allows you to install and remove blades, transceivers, and power supplies without turning the power off to the INTELLAPATCH switch itself, though you must turn power off to the appropriate blade slot before removing or installing a blade.

### 5.1.1. Removing Blades

To remove a blade:

1. Using the software, turn off power to the blade.
2. Unscrew the thumbscrews on either side of the blade.
3. Holding the blade straight, gently pull it towards you.

**Figure 8. Removing a Blade**



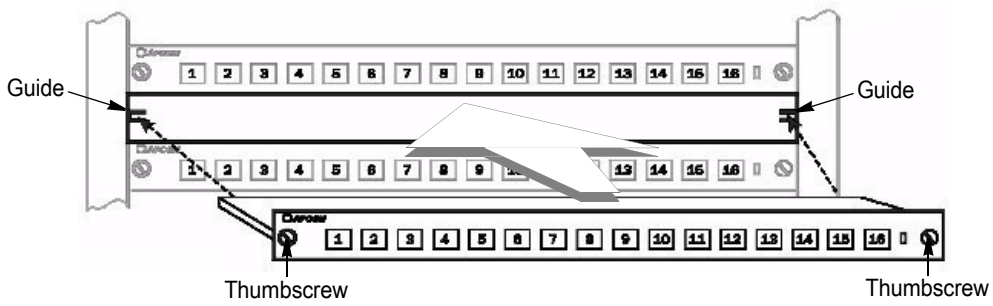

### 5.1.2. Installing Blades

To insert a blade:

1. Using the software, ensure that power is off to the slot in which the blade will be installed.
2. Hold the blade by its outer edges in front of the target slot.

3. Insert the back of the blade into the guides on each side of the slot.
4. Holding the blade straight, slide it into the guides as far as it will go.

**Figure 9. Inserting a Blade**




5. Press the blade into the chassis as you turn the thumbscrews to secure the blade in place.

The ACI-2058 automatically detects that the blade is in place and powers on the blade.

# 5.2. Transceiver Modules

## 5.2.1. Removing SFP Transceiver Modules

To remove a transceiver module:

- **Nonbail type**:
  Carefully push the ejector pin in while pulling out the module.
- **Bail type**:
  Pull the bail down and pull out the module.

## 5.2.2. Installing SFP Transceiver Modules

To insert a transceiver module:

- **Nonbail type**:
  1. Hold the module by the housing, so that the label faces up.
  2. Insert the module into the socket until you hear or feel a slight click.
- **Bail type**:
  1. Close the bail latch if it is currently open.
  2. Hold the module by the housing, so that the label faces up.
  3. Insert the module into the socket until you hear or feel a slight click.

## 5.2.3. Handling and Installing Fiber Optic Cables

To extend the life of transceiver modules, use caution when handling and installing cables. Do not remove the dust cover until immediately prior to mating the cable. To ensure proper cable mating, complete the steps in the following procedures.

#### 5.2.3.1. Disconnecting the Cable

To disconnect the cable:

1. Grasp the connector while squeezing the connector housing and disconnect the connector from the unit.
2. Cover connector ends and SFP transceivers with clean dust caps when not in use.

#### 5.2.3.2. Connecting the Cable

Clean the cable before connecting it:

1. Thoroughly wipe the side and end of the ferrule using a lint-free, alcohol-dampened cloth.
2. Blow dry the ferrule with compressed air.
3. Visually inspect the ferrule for lint, and blow-dry it again if necessary.
4. Connect the cable.

**Note**

- After every demating cycle, clean and blow-dry the ferrule before remating.
- Do not interchange connectors from one unit to another unit without first cleaning the connector. Doing so can damage the product by transferring small particles to the transceiver.

## 5.3. Power Supplies

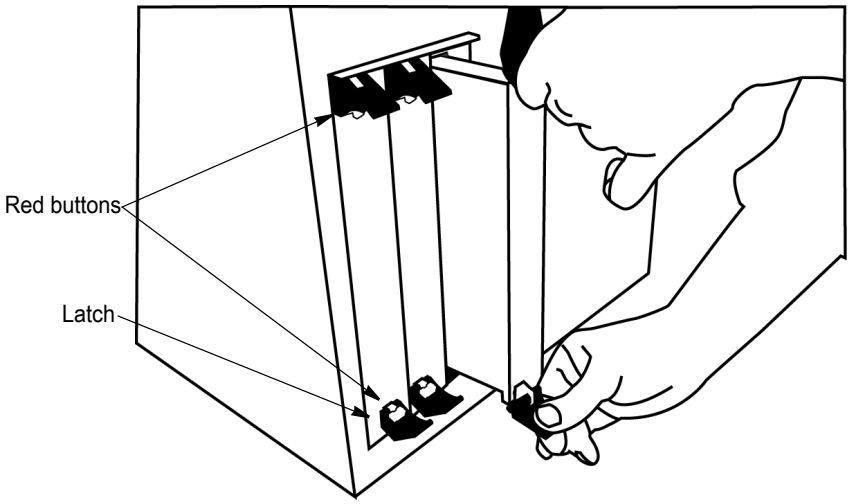
### 5.3.1. Removing a Power Supply

To remove a power supply:

1. Remove the screw from the latch.
2. Remove the two screws — one each from the top and bottom left and right latches.
3. Press the red buttons on the latches in while pushing the latches outward — the upper one upwards and the lower one downwards.
4. Push the latches outward.

5. Pull the supply toward you.

**Figure 10. Removing a ACI-2058 Power Supply**




## 5.3.2. Installing a Power Supply

To insert a power supply:

1. Make sure the latches are is in the outward position — the upper one pushed into the up position and the lower one pushed into the down position.
2. Push the power supply in firmly until you hear the latches click.
3. Secure (turn) the two screws inside the latch areas (one per latch).

## 5.3.3. Switch Defaults

The ACI-2058 default configuration as shipped from the factory is:

**Table 3. Factory Configuration**

| Setting | Default value |
|---|---|
| Ports | All off |
| Serial ports | 9600 baud, 8 data bits, no parity, 1 stop bit, software flow control |
| LAN ports | 10/100/1000 Ethernet, TCP/IP, both enabled |
| Device number | 01 |
| Temperature alarm | 50° Celsius |
| IP address | 192.168.0.1 |
| Subnet mask | 255.255.255.0 |
| Gateway | none |
| Administrator username | `admin` |
| Administrator password | `secret` |

If the switch exceeds the set temperature limit (by default, 50° C), an alarm sounds. This alarm can be turned off using any of the software interfaces; for instructions, see the specific software manual.

# Appendix A

# Serial Port Pinout

The ACI-2058 contains two RS-232 serial ports, each using a DB9 connector. The connectors are compatible with standard RS-232 straight-through serial cables. The next table describes each pin.

**Table 4. Serial Port Pinout**

| Pin | Host computer | COM1 | COM2 |
|---|---|---|---|
| 1 | DCD input | DCD output | No connection |
| 2 | Receive data input | Transmit data output | Receive data input |
| 3 | Transmit data output | Receive data input | Transmit data output |
| 4 | DTR Output | Connected to pin 8 | Connected to pin 8 |
| 5 | Ground | Ground | Ground |
| 6 | DSR input | DSR output | No connection |
| 7 | RTS output | No connection | No connection |
| 8 | CTS input | Connected to pin 4 | Connected to pin 4 |
| 9 | RI input | No connection | No connection |

# Index

## T



## U



## V



## W

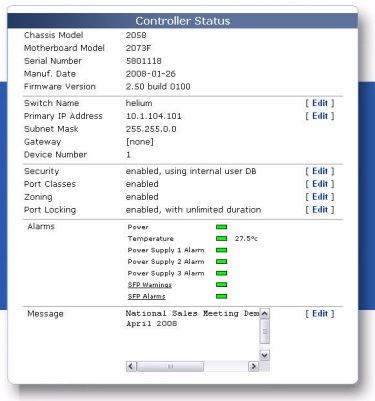
MultiDyne
Video & Fiber Optic Systems

# INTELLAPATCH™

## Physical Layer Switch Product Documentation

# WEBX v2.50 User Manual

## Embedded Web Interface




**MultiDyne**
877.MultiDyne | www.multidyne.com
A54-3000-100 | Rev A

# Contents

## Chapter 9: Maintenance



## Chapter 10: Settings



## Chapter 11: Help

# Figures

# Chapter 1

# Preface

## 1.1. About WEBX

This manual describes APCON's WEBX, an embedded web interface that you use to control your INTELLAPATCH™ switch remotely from a web browser over a network or the Internet. You can operate WEBX with or without security, and you can control user access to various WEBX features.

Since WEBX is embedded on the INTELLAPATCH motherboard, no installation is required. To access the software, you first install your APCON switch, then start a web browser and access WEBX by entering the switch's IP address. For details about accessing the WEBX, see *Chapter 3, Setting Up and Accessing the Switch* on page 16.

### 1.1.1. New in This Release

This version of WEBX includes the following new features:

- **New graphical interface**: WEBX now includes Basic menus that you use to provide detailed information when selecting WEBX features, and Power User menus to use when you are familiar with WEBX features. Customizable menu toolbars provides quick access to frequently used WEBX features, and the new menu structure organizes WEBX features by tasks you routinely perform.
- **TACACS+ support**: WEBX now includes support forTACACS+ servers.
- **SNMP**: WEBX now includes support for SNMP.
- **Logged-in user display**: The new Logged In screen (page 84) displays users currently logged in to the switch.
- Adjustable web session timeouts
- Password strength rules
- TBD syslog

APCON's version 2.5 firmware includes the following features:

- Ability to switch between the following:
  - **CLI version 3 (with CLI v2 for backward compatibility with existing scripts)**. This version provides a more easily parsed mode for new scripts and features and now supports most CLI2 commands.
  - **CLI version 2**. This version provides a different and less-featured command structure that is backwards compatible with previous versions of APCONCMDX.

## 1.2. About This Book

The purpose of this manual is to assist anyone who performs these functions related to the software:

- Patches ports using WEBX. This also requires that you know how to connect and disconnect standard types of cables
- Configures the switch using WEBX. This also requires that you know how to use and configure operating systems and networks.

### 1.2.1. Contents

This manual contains the following chapters and appendices:

| Chapter/Appendix | | Description |
|---|---|---|
| 1 | Preface | Explains how to use this manual. |
| 2 | Introducing WEBX | Describes features of WEBX. |
| 3 | Setting Up and Accessing the Switch | Describes how to connect to, log in, and log off the INTELLAPATCH switch. |
| 4 | Connections | Describes screens available from the Connections menu, where you configure patch settings. |
| 5 | MONITOR | Describes screens available from the MONITOR menu, which you use to connect to and control any INTELLAPATCH switch using the PC's serial port or TCP/IP LAN connection. You use MONITOR for non-intrusive network monitoring and to sharing equipment. |
| 6 | Ports/Blades | Describes screens available from the Ports/Blades menu, where you configure ports and blades in your INTELLAPATCH switch. |
| 7 | View | Describes screens available from the View menu, where you can access switch information and network status. |
| 8 | Tools | Describes screens available from the Tools menu, where you can run diagnostic tests. |
| 9 | Maintenance | Describes screens available from the Maintenance menu, where you can update or restore configuration files. |
| 10 | Settings | Describes screens available from the Settings menu, where you can manage user access and switch security. |
| 11 | Help | Describes screens available from the Help menu, where youcan find information about your INTELLAPATCH switch and contacting APCON. |
| A | Data File Formats | Provides samples for system log files and import/export files. |
| | Index | Lists product topics for quick reference. |

### 1.2.2. Text Conventions

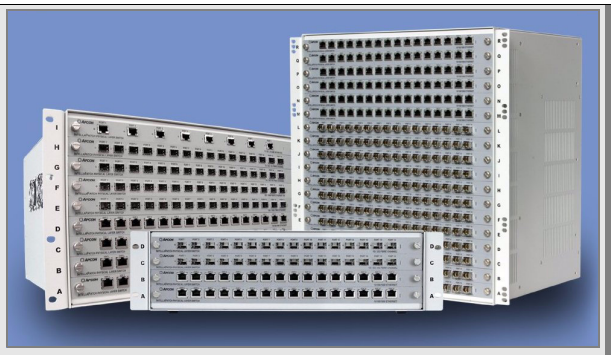
This manual uses the following conventions:

| | |
|---|---|
| > | Indicates the movement through menu options. For example, the sequence for changing the switch name is:<br>View>Chassis>Controller Status |
| **bold** | Indicates a directory or a file. |
| `MonoText` | Indicates information that displays on the screen. |
| **`MonoBold`** | Indicates information you type. |
| *`ItalicText`* | Variable parameters. |

| | |
|---|---|
| Note | Indicates important information about the product. |
| ⚠ CAUTION | Indicates potentially hazardous situations which, if not avoided, may result in minor or moderate injury, or damage to data or hardware. It may also alert you about unsafe practices. |
| ⚠ WARNING | Indicates potentially hazardous situations which, if not avoided, can result in death or serious injury. |
| ⚠ DANGER | Indicates imminently hazardous situations which, if not avoided, will result in death or serious injury. |

## 1.3. Related Products

### INTELLAPATCH Switches



APCON INTELLAPATCH switches employ a modular chassis/blade design that work with a variety of protocols and data rates.

With this modular system, you can populate each switch chassis with different blades, deploying Ethernet, SONET, Fibre Channel and other blades in a single chassis, while running every blade independently and simultaneously. This modular design also provides cost-effective media conversion and scalability.

APCON's WEBX is compatible with high-density (1") INTELLAPATCH switches such as these:

- **INTELLAPATCH ACI-2065**:A 1u[1] switch with one blade slot that supports up to 16 ports.
- **INTELLAPATCH ACI-2069**:A 2u switch with two blade slots that supports up to 32 ports.
- **INTELLAPATCH ACI-2061**: A 3u switch with four blade slots that supports up to 64 ports.
- **INTELLAPATCH ACI-2064**: A 6u switch with nine blade slots that supports up to 144 ports.
- **INTELLAPATCH ACI-2058**: An 11u switch with eighteen blade slots that supports up to 288 ports.

1. A "u" (unit) is 1.75" or 44mm.

APCON also provides these software products that you use to access and control your INTELLAPATCH switch(es):

- **APCONCMDX**, included on the CD that comes with your INTELLAPATCH switch, is a Command Line Utility (CLU) that provides an interactive command line interface.
- **Command Line Utility (CLU)** that provides an interactive command line interface.
- **MONITOR**, included on the CD that comes with your INTELLAPATCH switch, connects to and controls any APCON INTELLAPATCH Physical Layer Switch using the PC's serial port or TCP/IP LAN connection. This software provides non-intrusive network monitoring and for sharing of equipment such as traffic analyzers, network probes and Intrusion Detection System (IDS) equipment.

  Some MONITOR features are available in WEBX. For details, see *Chapter 5, MONITOR*, starting on page 48.
- **Firmware Direct Commands (ASCII)**, embedded in your INTELLAPATCH switch, control the switch using any scripting language (such as Tcl or Perl) that supports reading from and writing to serial or socket connections.
- **C/C++ API**, purchased separately, provides programmatic access to the switch. To acquire this product, contact APCON as described in the next section.

Additional software can be purchased for application-specific purposes.

## 1.4. Contacting APCON

You can find out more about INTELLAPATCH products from these sources:

- **World Wide Web**: APCON maintains an active site on the World Wide Web. The site contains current information about the company and locations of sales offices, new and existing products, contacts for sales, service, and technical support information. You can also send email to APCON using the web site.
  - To access the APCON web site, enter this URL in your web browser:

    http://www.apcon.com
  - To contact APCON technical support, enter this URL in your web browser:

    http://www.apcon.com/support

    **Note**

    When sending email for technical support, please include information about both the hardware and software.
- If you purchased your product from MultiDyne, please contact your MultiDyne sales representative via email or phone.

  Email: sales@multidyne.com

  Telephone: 516.671.7278
  Fax: 516.671.3362

# Chapter 2

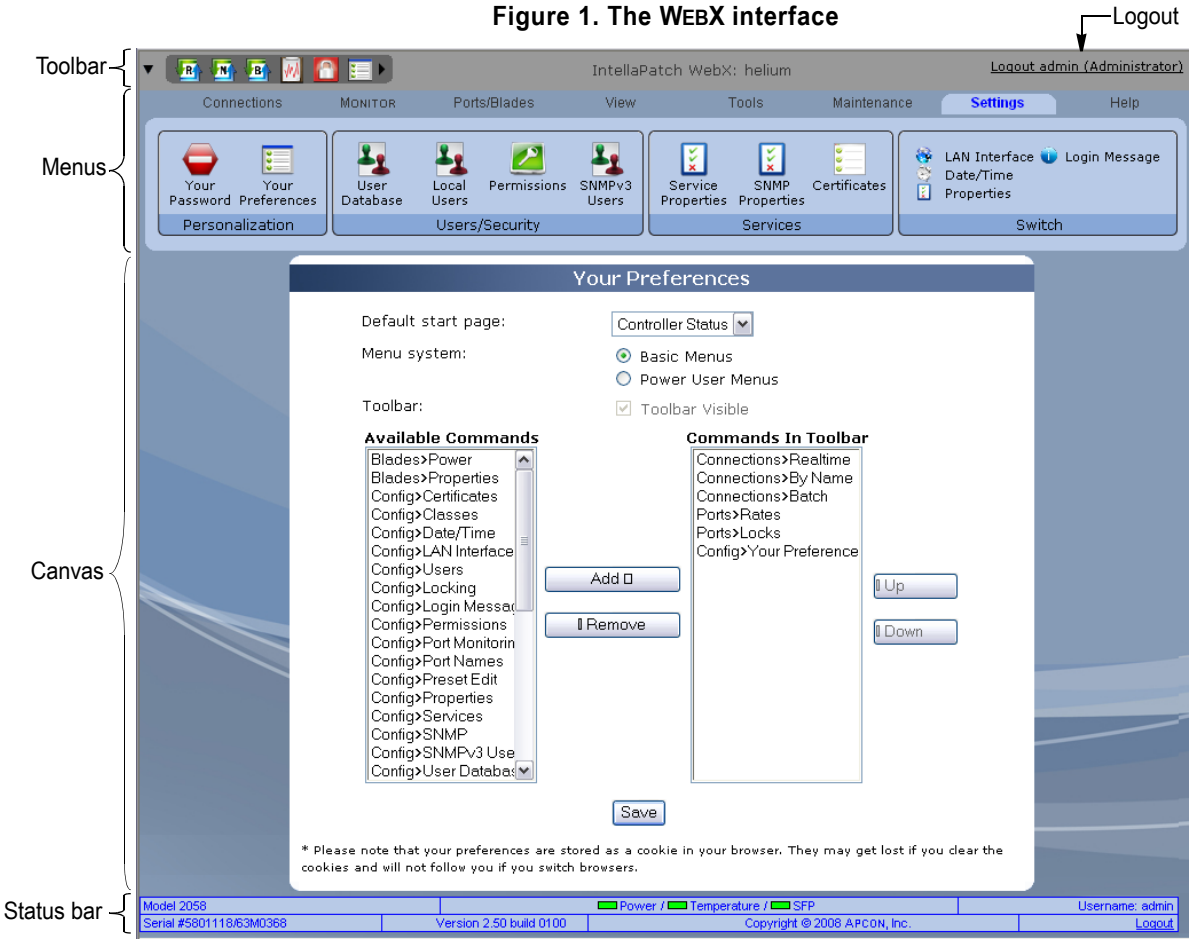
# Introducing WEBX

This chapter describes the following WEBX features:

# 2.1. Screen Layout

WEBX provides access to the INTELLAPATCH switch through your web browser. The interface provides the easy-to-use features described in the following sections:

**Figure 1. The WEBX interface**




## 2.1.1. Toolbar

The toolbar povides quick access to WEBX features you frequently use. The toolbar's appearance varies, depending on the menu you use:

**Basic**:

**Power user**


**Note**: The toolbars above display the default factory configuration.

Clicking the arrow minimizes the Toolbar to provide more room for the Canvas, or maximizes the Toolbar to allow access to its options.

To customize the toolbar, click the arrow at the right side of the menu or select Settings>Personalization>Your Preferences. For information about setting preferences on this screen, see *Your Preferences* on page 105.

## 2.1.2. Logout

**Note**

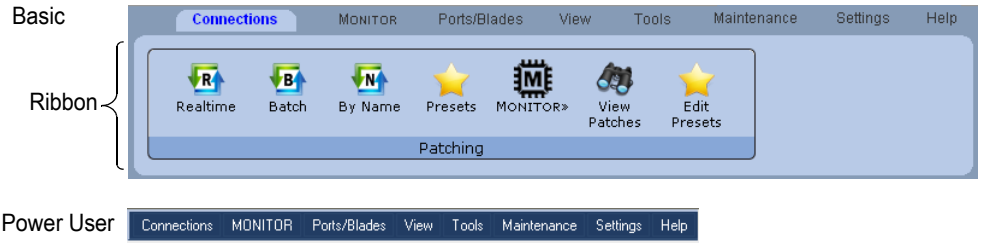
Logout links display only when the User Database (page 107) is not set to None.

The logout link displays at the far right, where you can click to log out and re-display the login screen. Another logout link displays in the Status bar, at the screen's lower right.

The name you specified for the switch also displays to the toolbar's right; you can change this name in View>Chassis>Controller.

## 2.1.3. Menus

WEBX provides these menus to access features:




- **Basic**: Displays available options with icons. After selecting an option, you can minimize the menu by clicking the downward arrow in Switch Info. Use this mode to provide detailed information you can use to select the appropriate WEBX feature.
- **Power User**: Displays available options in a pull-down menu. Use this mode when you are familiar with WEBX features.

Both Menu and Ribbon modes include the following:

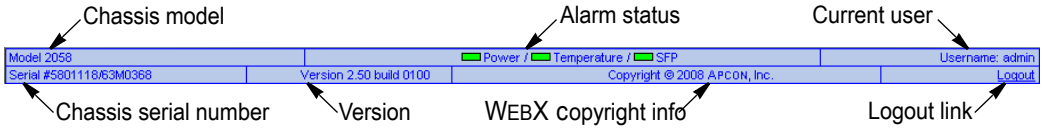
- **Connections**: Display switch status or current settings.
- **MONITOR**: Patch using the WEBX MONITOR interface. Only available (visible) with the proper license key. For information about keys, see *License Key* on page 98.
- **Ports/Blades**: Set and change switch functionality. Most options in this category require that you log in with Advanced Operator privileges. For information about access privileges, see *Permissions* on page 112.
- **View**: Displays switch status or current settings.
- **Tools**: Displays data and runs tests that you can use to troubleshoot connected devices.
- **Maintenance**: Transfer switch settings and store data.
- **Settings**: Manage switch and user options. Options on this menu are largely one-time setup and configuration tasks, and require administrator privileges.
- **Help**: Provides information about the switch and how to contact APCON for more information.

### 2.1.4. Canvas

You use the Canvas to view switch settings or configure switch behavior. The screens and fields that display on the Canvas vary, depending upon the option you select from the menus. The remainder of this book explains the screens and fields that display on the Canvas, and the values you can enter in each field.

### 2.1.5. Status Bar

The status bar, located at the bottom of the screen, displays the following WEBX information:




**Note**

The user name and logout link displays only when the User Database (page 107) is not set to `None`.

## 2.2. Navigation

### 2.2.1. Mouse Techniques

You do much of your work in the WEBX using your mouse:

- You *position* your cursor by moving the mouse until the tip of the cursor touches an object.
- You *hover* by positioning the cursor and keeping the cursor in that location.
- You *click* by positioning the cursor, then pressing and quickly releasing the left mouse button once. In this manual, the words click, highlight, and select all mean the same thing.

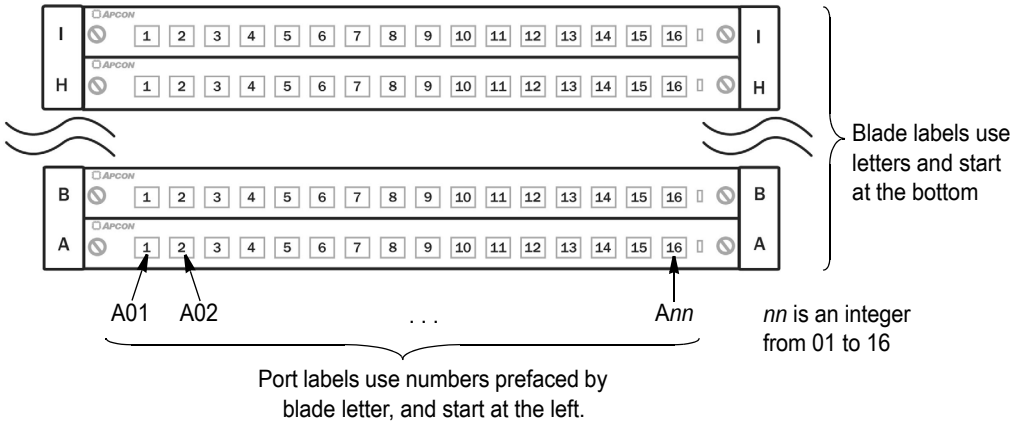
### 2.2.2. Terminology

The instructions in this manual use the terms “enter” and “type” to mean different things. When the instructions tell you to enter something, you press the appropriate keys and press the Enter key. When the instructions tell you to type something, you press the appropriate keys, but do *not* press the Enter key.

## 2.3. Switch Labeling

To identify each port, INTELLAPATCH switches use the following port labeling conventions:

**Figure 2. Switch labeling**




Blades have varying numbers of ports, and a chassis may not be fully populated with blades. The greatest number on each blade and the greatest letter in each chassis varies, therefore, according to the number of ports in a blade and the number of blades installed in a chassis.

WEBX refers to ports using these labels. You can use the WEBX to assign names to your ports, names that indicate devices they connect to or to provide other meaningful aids to memory. For details, see *Port Properties* on page 50.

## 2.4. Patching Ports

APCON's WEBX features the following methods to patch ports:

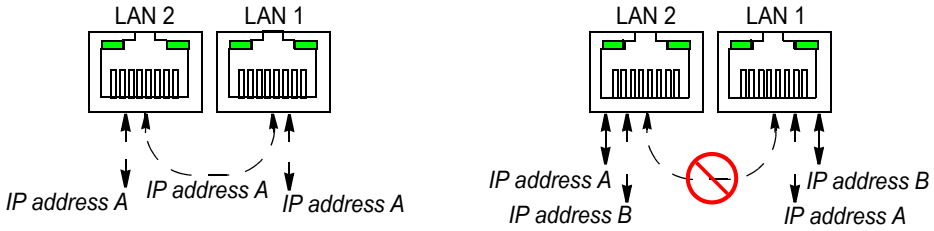
- **Interactive patching**: Patch ports interactively using a graphical, click-and-drop interface. For details, see *Realtime* on page 33.
- **Batch operations**: Create a patching configuration for the entire switch at once and then have this configuration take effect all at the same time. For details, see *Realtime* on page 33.
- **Quick patching**: Type in one or more port names, or select from a dropdown list, to make a few quick patches. For details, see *By Name* on page 42.
- **Preset configurations**: Patch ports according to a preset configuration. For details, see *By Preset (Presets)* on page 45.
- **Import configuration settings**: Patch ports according to settings you exported from another INTELLAPATCH switch. For details, see *Restore Settings* on page 97.

## 2.5. Assigning IP Addresses

When you specify only one IP address, that address is assigned to both ports and traffic flows between the two ports. The ports act like a network switch and you can stack multiple chassis together, plug one into the network, and daisy-chain the rest.

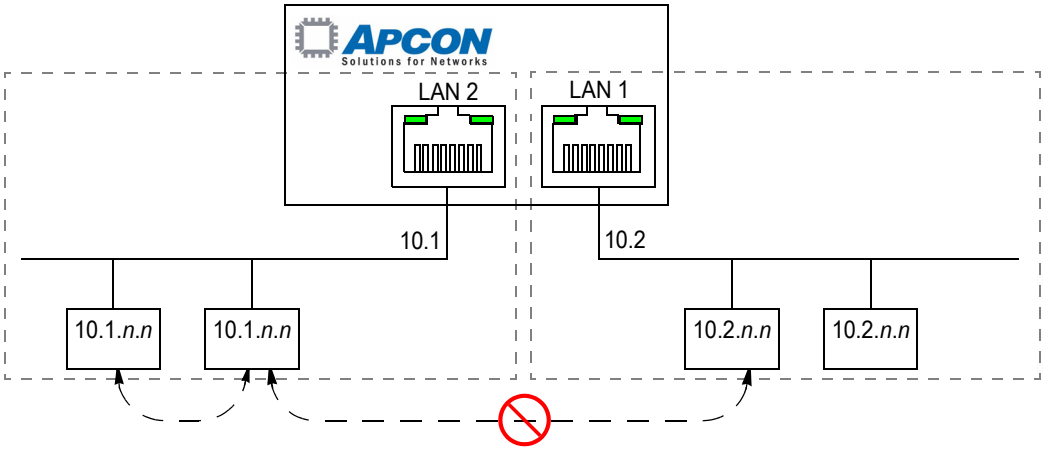
With two IP addresses, each LAN port is multihomed with the two IP addresses. This means you can reach each port by either IP address. The two LAN ports on the back of the unit are split into isolated VLAN segments and cannot pass traffic between each other. You cannot daisy chain.

**Figure 3. Single vs. multiple IP addresses**




In the multiple IP address scenario, typically each address is a different subnet. Each LAN port plugs into the network segment containing that particular subnet. (Since each port listens for both IP addresses, it doesn't matter which port gets plugged into which subnet.) In theory, both IP addresses are available on both LAN ports but, in practice, each LAN port uses only one address.

**Figure 4. Example: multiple IP addresses and subnets**



## 2.6. User Database Concepts

WEBX provides the tools you need to specify the default permission, or access level, for new user accounts. You can configure or modify user accounts for access at any of these levels:

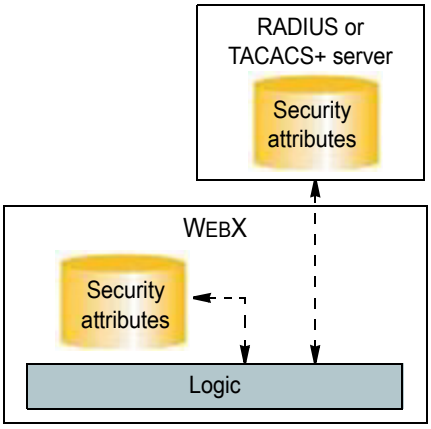
- **Guest**: Users with this permission level have read-only access. This is the lowest permission level.
- **Operator**: Users with this permission level can do all that Guest-level users can do, plus patch ports using only preset configurations.
- **Advanced Operator**: Users with this permission level can do all that Operator-level users can do, plus patch ports on an ad-hoc basis, change rates and port names, plus save configuration settings ("presets").
- **Administrator**: Users with this permission level do everything that the other levels do, plus set switch, blade, port, and other information as well as set and clear user and security information. This is the highest permission level.

WEBX sends user *access information* to the Preferences Security database in your INTELLAPATCH switch.

With the flexible architecture of the user database, you can select any one of these approaches to store user or access *names*:

- **RADIUS or TACACS+ server**: This option points to the user names stored on a RADIUS or TACACS+ server. This option works in conjunction with the local User Database. If a user exists in both databases, the local database takes precedence.
- **Internal user database**: This option stores user names and access information within the switch. This database includes an `admin` account, which acts as a local administrator.

**Figure 5. User Database Architecture**




INTELLAPATCH switches support up to three different RADIUS or TACACS+ servers for user authentication. WEBX consults them in a failover sequence. The first server is always consulted first and is considered the primary server. If no response, the second is consulted, and so on. If the primary is down, this could lead to longer login times.

## 2.7. Network User Authentication

RADIUS and TACACS+ provide centralized user authorization tools. Setting up these services is outside the scope of WEBX documentation. However, you will find brief examples here:

- **RADIUS**: For details, see *Appendix B, Adding APCON Attributes to your RADIUS Server*.
- **TACACS+**: For details, see *Appendix C, Configuring the TACACS+ Server*.

# 2.8. Simplex Patching with SPAN/Monitor Ports

**Note**

APCON's MONITOR feature provides the tools to quickly perform this task. MONITOR requires a license key, available from APCON. For details about acquiring MONITOR, contact your APCON sales representative as described in *Contacting APCON* on page 4 or on the Help>Support menu option. For information about license keys, see *License Key* on page 98..

WEBX accommodates simplex patching from SPAN ports to analyzers for enterprises that require this level of security. When using only simplex patching with SPAN ports, you must set up your INTELLAPATCH switch as described in this section.

**Note**

This method requires an APCON Security blade, such as the ACI-2059-S15-2 or ACI-2059-S15-4. Security blades ensure that ports connected and defined as SPAN ports only transmit information. For information about acquiring such a blade, contact APCON as described in *Contacting APCON* on page 4.

**Figure 6. Security symbol**

(Identifies Security blades)

To configure Security blade ports for simplex patching:

**Note**

If the WEBX MONITOR feature is activated, as described in *License Key* on page 98, the MONITOR Setup wizard automatically performs all these steps. For information about the wizard, see the *MONITOR User Manual.*

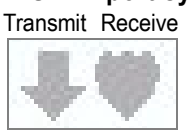
1. Configure the automatic transmitter:
   A. Select Ports/Blades>Ports>Properties. The Properties screen displays.
   B. Select TX on when no RX from the drop-down list.
   C. Click the Update button.
2. Enable port classes:

   To create the port classes needed to implement SPAN security, you must configure the switch to allow port classes.

   A. Select Ports/Blades>Configuration>Classes. The Classes screen displays.
   B. Ensure that the Enforce Port Classes checkbox, located at the top of the screen, is checked. When checked, all available port classes display.
3. Create port classes:
   A. Set up these port classes on the Classes screen:
      - **Analyzers**: Enter any name that consists of up to 31 characters, including letters, numbers, spaces, and most keyboard characters.
      - **SPAN port**s: This class name must begin with the letters "SPAN"; the beginning of the name is not case-sensitive. For example, `SPAN`, `SPAN Ports`, and `SPAN-Lab 1` are valid; `Lab 1 SPAN` is not. WEBX automatically converts entries of `SPAN` or `SPAN PORT` to `SPAN`.

**Note**: The SPAN port symbol, which replaces the port number, identifies ports assigned to the SPAN class. The arrow indicates that the port can transmit signal; the shield indicates that the port cannot receive signal. This prevents accidental network flooding by blocking inbound traffic on the SPAN port.

**Figure 7. SPAN port symbol**




B. Set each class to Exclusive.

C. Save these classes by clicking the Save button.

4. Assign ports to classes:

   A. Click the Class Members link, located at the top of the screen. The Class Members screen displays.

   B. Assign ports to classes as shown in the next table.

| Class | Comments |
|---|---|
| SPAN ports | Assign to this class only ports used as SPAN ports. |
| Analyzers | Assign to this class ports that attach to analyzers. |

5. Set port rates:

**Note**: To ensure proper operation, you must set SPAN and analyzer ports to specific rates.

   A. Select Ports/Blades>Ports>Rates. The Rates screen displays.

   B. Set ports you plan to use as SPAN ports to a specific rate in Analyzer Tap mode.

   C. Set ports you plan to use as analyzer ports to the specific rate in Analyzer Tap mode.

   D. Click the Save button.

6. Set rate options:

   A. Select Ports/Blades>Ports>Properties. The Properties screen displays.

   B. (Optional) Check this box to enable passthrough negotiation on the specified blade:

   ☑ ACI-2052-E16-2 passthrough negotiation

   **Note**: Check only if you set any analyzer ports to `Analyzer Tap: Auto`. APCON recommends using a specific data rate.

   APCON also recommends enabling these options:

   ☑ ACI-2052-E16-2 always negotiate

   ☑ ACI-2052-E16-2 always on

   **Note**: WEBX automatically enables Automatic SPAN Security when you insert a Security blade.

   C. Click the Update button.

You have now set up your SPAN ports, configured the switch for simplex-only connections, and can patch SPAN ports to an analyzer.

### 2.8.1. Disabling Simplex Patching with SPAN/Monitor Ports

Do any of these:

- Remove the APCON Security blade(s) from the INTELLAPATCH switch. For details, see your INTELLAPATCH switch user manual.
- Disable port classes:
  A. Select Ports/Blades>Configuration>Classes. The Classes screen displays.
  B. Uncheck the Enforce Port Classes checkbox, located at the top of the screen.
- Remove ports from the SPAN port class.
  A. Select Ports/Blades>Configuration>Classes. The Classes screen displays.
  B. Click the Class Members link, located at the top of the screen. The Class Members screen displays.
  C. Uncheck SPAN class checkboxes.
  D. Click the Save button.

Chapter 3

# Setting Up and Accessing the Switch

Before running WEBX, you must first set up the switch:



## 3.1. Setting the IP Address

By default, INTELLAPATCH switches ship with an IP address of 192.168.0.1, a subnet mask of 255.255.255.0, and no gateway. If it's convenient to configure your host computer with an IP address of the form 192.168.0.*x* (where *x* is any number from 2 to 254, inclusive), then WEBX is immediately available. If not, to use the Ethernet connection you must change this default IP address to one appropriate for your network, using one of these:

- Serial Console
- Web Browser

**Note**

If you plan to use more than one INTELLAPATCH switch on your network, configure them at the same time. This avoids repeated temporary disconnections of the host computer from your network.

### Before you begin

Ensure that you have an APCON ACI-2073 board in your INTELLAPATCH chassis. This board has adequate memory for the WEBX 2.50 firmware.

**For web configuration,** ensure that you have the following:

- A web browser that supports Javascript including, but not limited to:
  - Firefox† browser, version 2.0 or later
  - Internet Explorer, version 6.x or later

  **Note**

  Ensure that your browser's Javascript is enabled.
- Screen resolution of 1024 x 768 or better.

- A host computer that runs a web browser listed in the previous bullet. The host computer's web browser accesses the embedded WEBX.
- An Ethernet connection between the host computer and the switch.
- An IP address, subnet mask, and gateway (if required) appropriate for your network assigned to the switch.

**For serial configuration,** ensure that you have the following:

- An availabl3e serial port on the host machine.
- A serial cable.

## Changing the IP Address via Serial Console

To use the serial console to change the IP address:

1. Connect a straight-through serial cable to the switch's COM1 port and a host computer's serial port.
2. Start a communications program, such as HyperTerminal.
3. Establish a connection with the following parameters:

   | | |
   |---|---|
   | Port: | COM1 |
   | Bits per second: | 9600 |
   | Data: | 8 bits |
   | Parity: | None |
   | Stop bits: | 1 |
   | Flow Control: | None |

4. Press the ENTER key 3 times. The *console>* prompt displays.

   If the console is configured to answer with the ASCII (slashdot) command set , enter the following to switch to CLI mode:

   `<ENTER>/.|CLI<ENTER>`

5. Set the IP address using one of these methods:

   **CLI2** (default): `configure ip`

   where the program prompts you to enter an IP address, subnet, and gateway, in standard TCP/IP `#.#.#.#` format.

   **APCONCMDX**: `set switch address` *`ip_address subnet_mask optional_gateway`*

   where *`ip_address`*, *`subnet_mask`*, and *`optional_gateway`* are IP addresses, in standard TCP/IP `#.#.#.#` format.

   For example:

   ```
   set switch address 10.1.1.180 255.255.255.0 10.1.1.1
   ```

   The IP address command is issued and the console banner reappears. This process may take several seconds.

## Changing the IP Address via Web Browser

To use APCON's WEBX software to change the IP address:

1. Connect a host computer to the INTELLAPATCH switch:

   A. Disconnect from your network the host computer you plan to use to assign the IP address.

   B. Plug the host computer's serial cable into one of the Ethernet ports on the back of the INTELLAPATCH switch using either a standard patch cable or a crossover cable.

   The host and switch are now physically connected.

2. Enable communication between the host computer and switch:

   A. Access the host computer's current network settings. Note them so that you can restore them at the end of this process.

   B. Temporarily change the host settings to the following:

   - IP address: `192.168.0.x`
     (*x* is a number from 2 to 254)
   - Subnet mask: `255.255.255.0`
   - Gateway setting: `0.0.0.0` or blank

   The host and switch are now on the same network and can communicate.

3. Access WEBX:

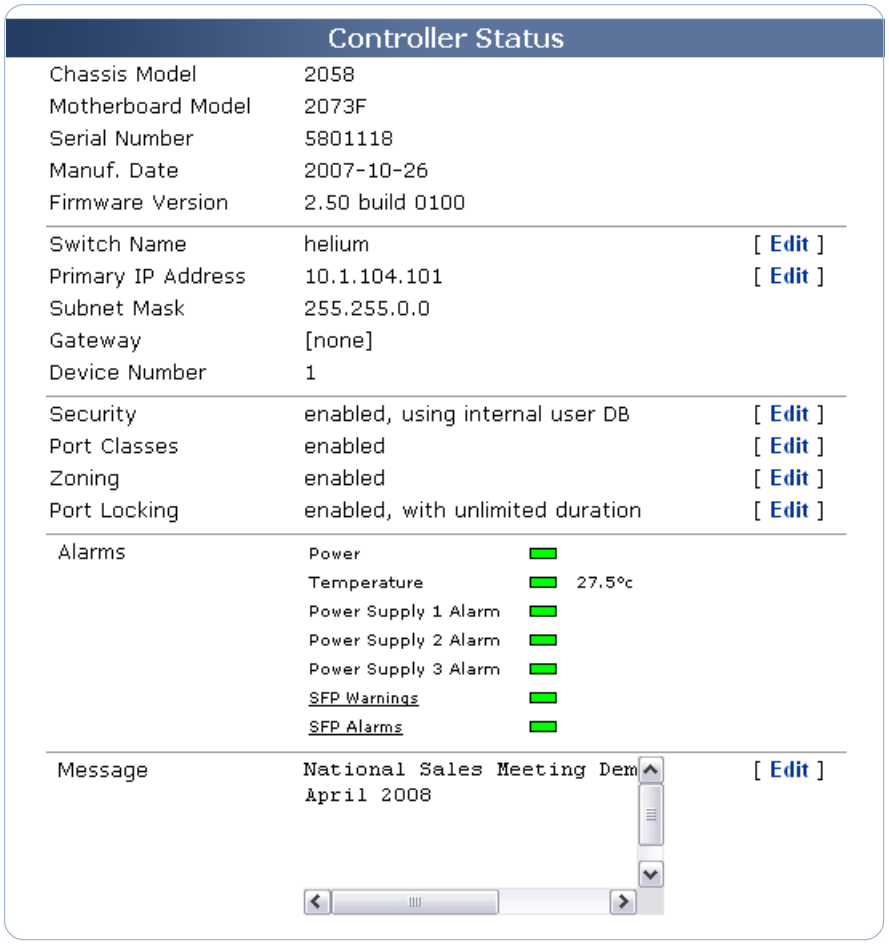
   A. On the host computer, open a web browser.

   B. If the host computer is configured to use a proxy server, disable the proxy setting.

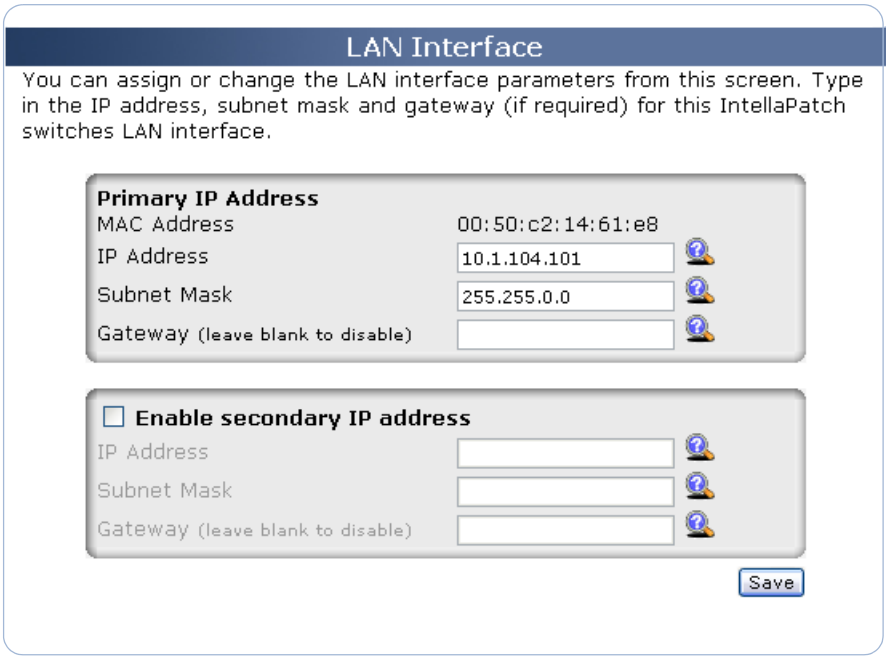
   C. In the browser's address field, enter:

   `http://192.168.0.1`

The Switch Controller Status screen displays.



4. Click the Edit link, located to the right of the Primary IP Address field. The LAN Interface screen displays:




5. Change the IP address:

   A. Type the new IP address, subnet mask and gateway (if required) you previously received from your network administrator into the fields provided.

   B. Click the Save button. The switch reroutes the browser to the new address.

      If the new IP address no longer exists on the same subnet as the host computer, this may fail. Reset the host computer to its original settings as described in step 6A.

   C. Exit the browser.

6. Reconnect the host computer to your network.

   A. Reset the host computer's IP address, subnet mask and gateway settings to their original values.

   B. Re-cable the host computer to the network.

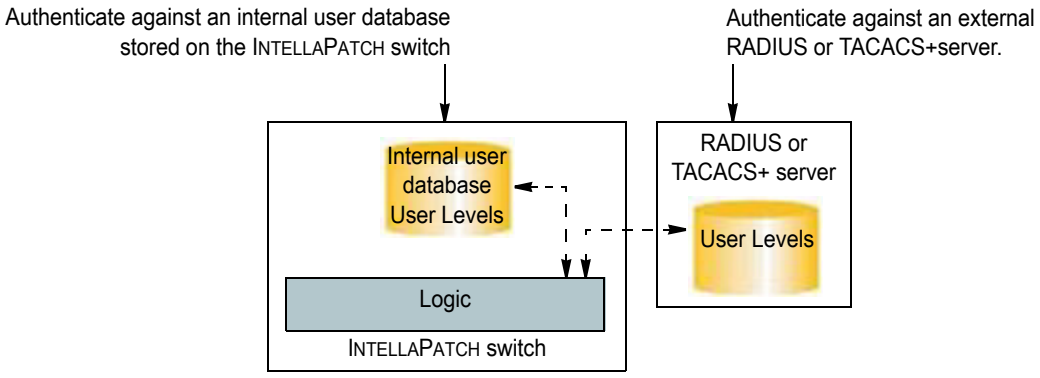
   C. Ensure that the switch is cabled to the network with a standard Ethernet patch cable.

## 3.2. Setting Up User Authentication

When you need authentication, WEBX provides the tools required to specify the default permission, or access level, for new user accounts. With authentication enabled, you can:

- Restrict who can access general functionality and administrator-level configuration.
- Use port locking.
- Enable zoning.
- Use APCON's Security blades to share SPAN/Monitor ports.

Before setting up user accounts, however, you must decide which authentication method, if any, you want to use:



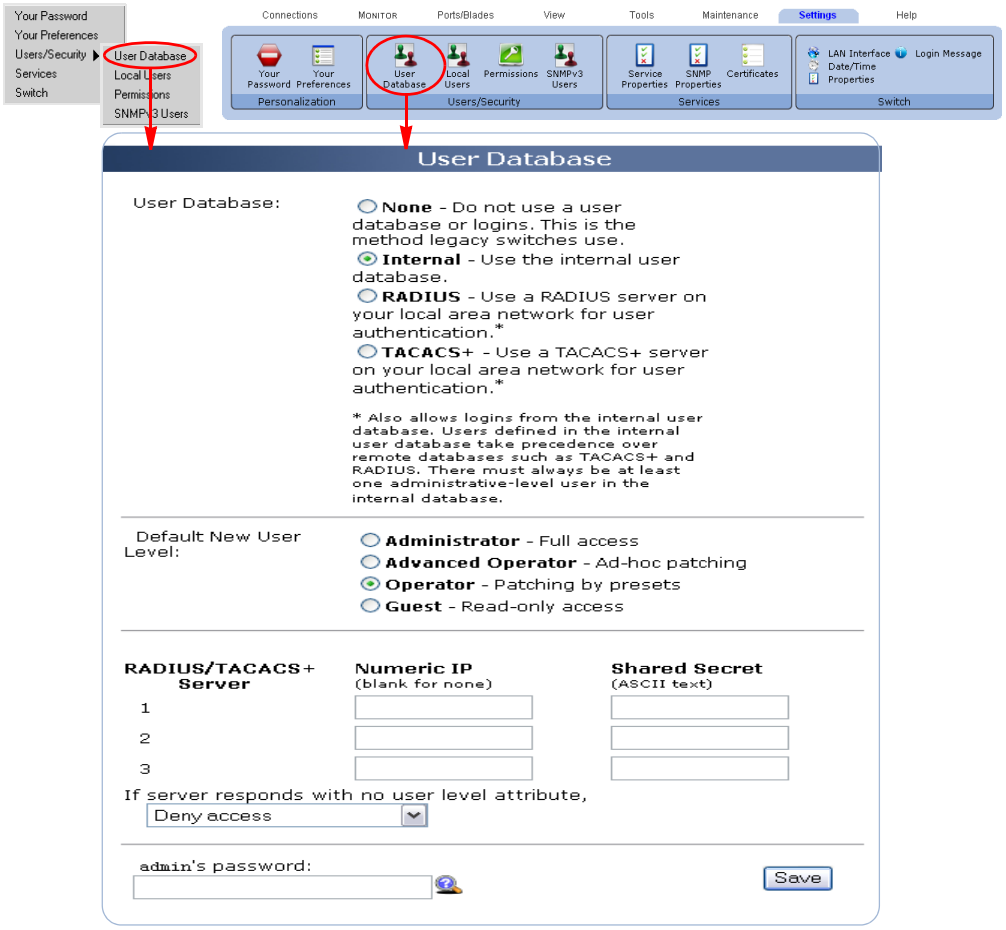

To set up a user database:

1. Ensure that an IP address is set up, as described in *Setting the IP Address* starting on page 16.
2. Access WEBX:
   A. On the host computer, open a web browser.
   B. If the host computer is configured to use a proxy server, disable the proxy setting.
   C. In the browser's address field, enter the switch's IP address, in standard TCP/IP `#.#.#.#` format. For example:

      `http://192.168.0.1`

   The WEBX main screen displays.

3. Select **Settings>Users/Security>User Database** in the Navigation pane. The User Database screen displays:




**Note**: For details about options on the User Database screen, see *User Database* on page 107.

4. Set the User Database to one of these:

   - **Internal**: Select this option if you plan to use the internal user database.
   - **RADIUS**: Select this option if you plan to use a RADIUS server on your local area network for user authentication.
   - **TACACS+**: Select this option if you plan to use a TACACS+ server on your local area network for user authentication.

   Set any additional options that display.

5. Click the Update button. The switch automatically exits and displays the WEBX login screen.

# 3.3. Logging In

**Note**

You can log in only if User Database is set to Internal, RADIUS, or TACACS+, as described in the previous section.

After you assign the switch an IP address and add it to your network, you can log in to the switch over the web using either an ordinary (HTTP) or a secure (HTTPS) connection. (The first time you log in to the switch to add it to your network, a secure connection is not available.)

**Note**

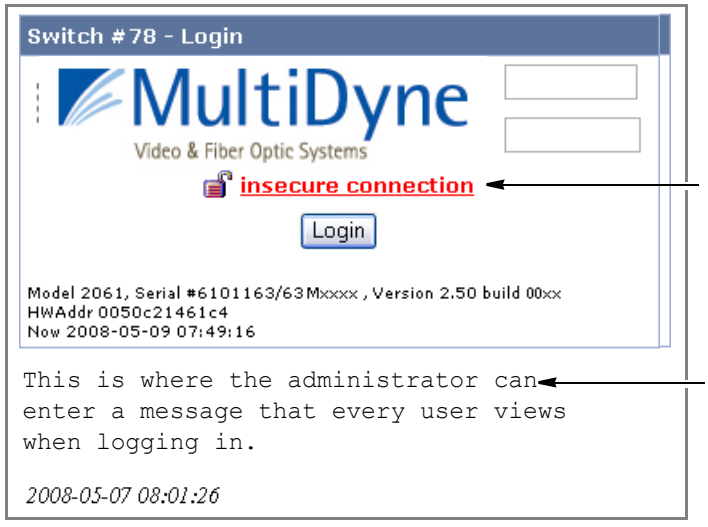
If you plan to use secure logins, you need an SSL certificate. For details, see *Certificates* on page 125.

To log in to the switch:

1. Ensure that the following is done:
   - An IP address is set up, as described in *Setting the IP Address* starting on page 16.
   - The User Database is set to Internal, RADIUS, or TACACS+, as described in *Setting Up User Authentication* starting on page 21.
2. In the browser's address field, enter one of these:
   - For an insecure connection (default): `http://x.x.x.x`
   - For a secure connection: `https://x.x.x.x`

   where each *x* is a value from 1 to 254, and the total four-part number is the IP address assigned to the switch.

   The WEBX login screen displays:




3. Enter your User name and Password. The factory defaults are shown below:

   **User**: `admin`
   **Password**: `secret`

4. Press either the Login button or the Enter key.

   The switch's main screen displays.

You can now view your switch's settings. If you have administrator permission privileges, you can also modify switch settings. For details about permissions, see *Permissions* on page 112.

## 3.4. Setting Up Security

Set up WEBX to perform the switch security tasks you desire:

- Enable secure web (HTTPS) connections, requiring users to log in using a secure SSL connection. You can also generate the SSL certificate required to enable secure SSL logins.
- Enable secure command line (APCONCMDX) connections, allowing users to log in using an SSH connection. You can also generate the SSH key required to enable SSH.
- Enable one or more users to issue ASCII commands or run ASCII-command scripts over the network.
- Change the default serial port console mode to the ASCII scripting mode.
- Enable access to APCON software products such as APCONCMDX, CONTROLX, and MONITOR.

You set up these tasks on the Security/Services screen. For details about other options on this screen, see *Service Properties* on page 117.

### 3.4.1. Establishing Secure (SSL) Connections

When you require all management functions—including user authentication—to run over a secure connection, you can enable SSL as described in the following steps.

**Note**

SSL is slower than non-secure HTTP.

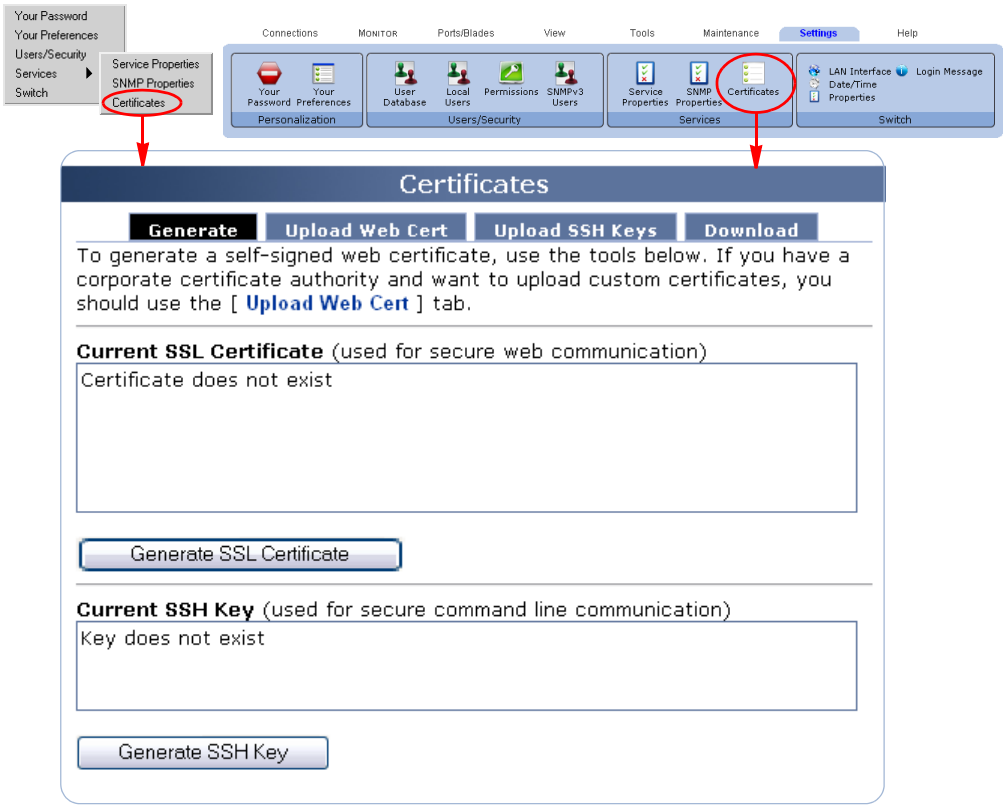
To require all users to log in using a secure SSL connection:

1. Ensure that an IP address is set up, as described in *Setting the IP Address* starting on page 16. APCON recommends that you also set the User Database to Internal, RADIUS or TACACS+, as described in *Setting Up User Authentication* on page 21.
2. Log in as described in *Logging In* on page 23.

**Note**

If authentication is enabled, you must log in with Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

3. Select **Settings>Services>Certificates**. The Certificates screen displays:




4. Click the Generate SSL certificate button.

   WEBX generates the SSL certificate. This may take up to three minutes to complete; do not cancel or change screens during generation. When the certificate is generated, this message displays:

   ```
   Keys generated...
   Service restarting...SUCCESS
   ```

5. Select **Settings>Services>Certificates** to refresh and re-display the screen.
6. Check the Force secure (HTTPS) logins checkbox, then click the Update button.

   You are prompted to verify your actions. WEBX enables secure logins, then displays the **View>Controller Status** screen.

When users log on, it will be via a secure connection.

## 3.4.2. Establishing SSH Connections

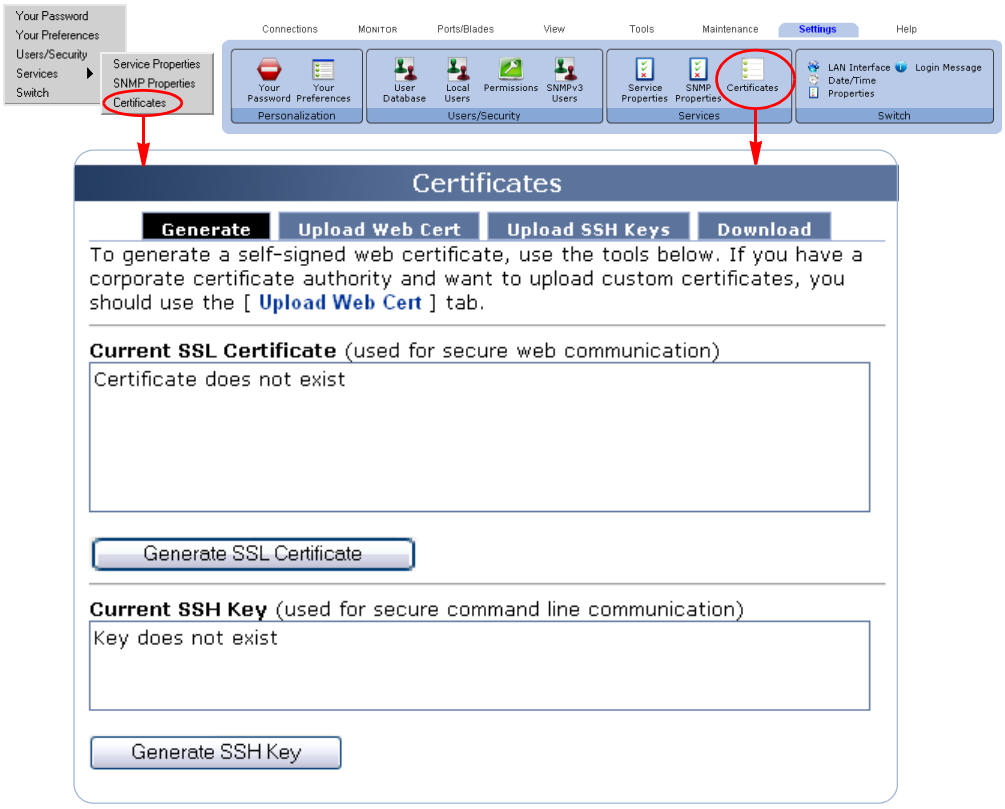
When you require command line communication to run over a secure connection, you can enable SSH as described in the following steps.

To require all users to log in using an SSH connection:

1. Ensure that an IP address is set up, as described in *Setting the IP Address* starting on page 16.
2. Log in as described in *Logging In* on page 23.

> **Note**
> If authentication is enabled, you must log in with Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

3. Select **Settings>Services>Certificates**. The Certificates screen displays:




4. Click the Generate SSH key button.

   WEBX generates the SSH key. This may take up to three minutes to complete; do not cancel or change screens during generation. When the key is generated, this message displays:

```
Keys generated...
Service restarting...SUCCESS
```

5. Select **Settings>Services>Certificates** to refresh and re-display the screen.
6. Check the Enable SSH checkbox, then click the Update button.

You are prompted to accept the certificate. WEBX enables SSH, then displays the **Settings>Services>Certificates** screen.

7. Uncheck the Enable Telnet checkbox, then click the Update button.

   **Note**: This prevents both secure SSH and non-secure telnet from being simultaneously available.

When users use telnet, it will be via a secure connection.

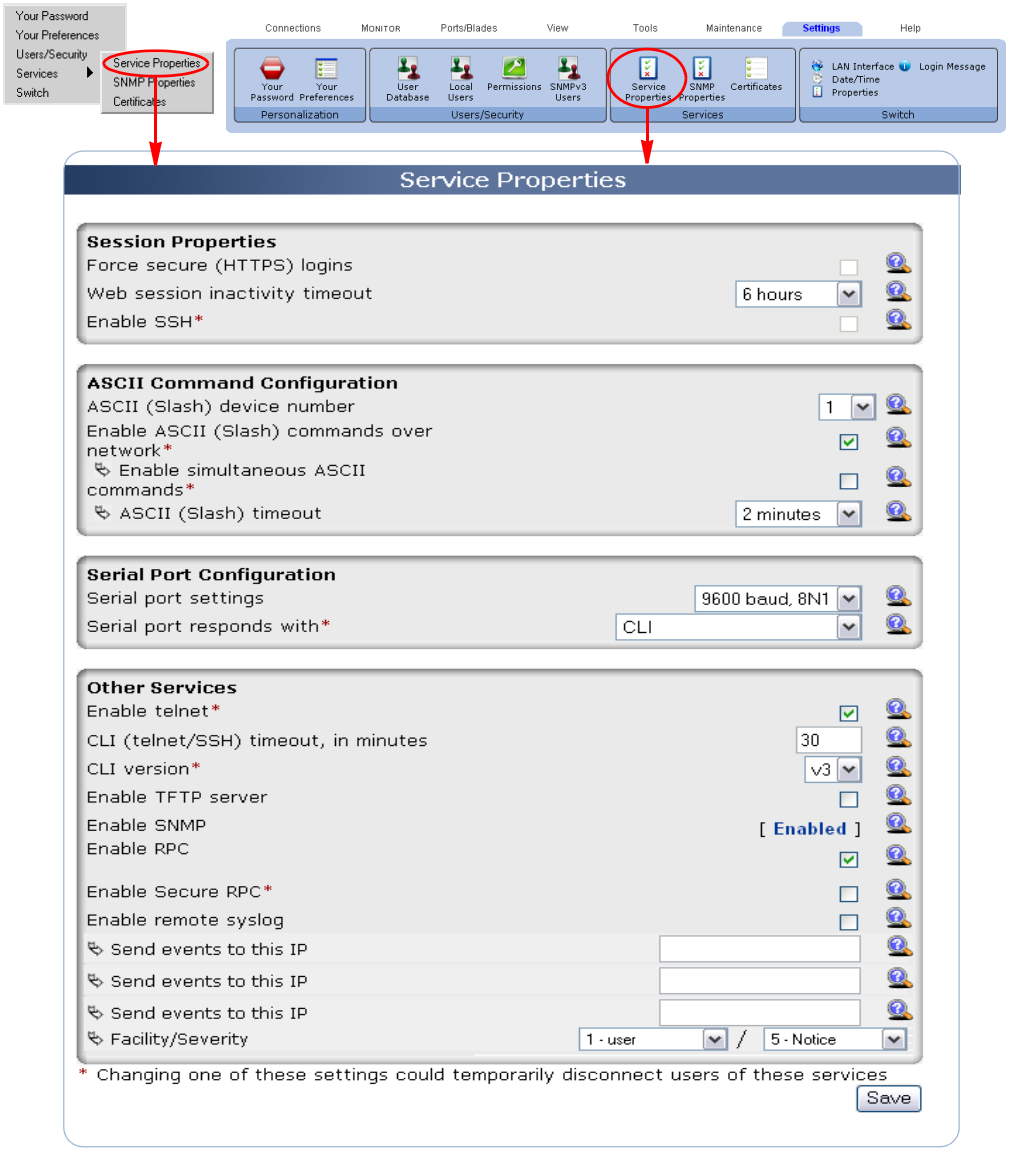
## 3.4.3. Running ASCII Command Scripts Over the LAN Ethernet Interface

To Enable one or more users to issue ASCII commands or run ASCII-command scripts over the network:

1. Ensure that an IP address is set up, as described in *Setting the IP Address* starting on page 16.
2. Log in as described in *Logging In* on page 23.

| Note |
| --- |
| If authentication is enabled, you must log in with Administrator permission privileges. For details about permissions, see *Permissions* on page 112. |

3. Select **Settings>Services>Service Properties**. The Service Properties screen displays:




4. Check the Enable ASCII (Slash) commands over network checkbox. The Enable simultaneous ASCII commands field displays.
5. (Optional) If you want more than one user to send ASCII commands over the network at the same time, check the Enable simultaneous ASCII commands checkbox.
6. Click the Update button.

   You can now run ASCII commands over the network. If you selected both checkboxes, multiple users or scripts can concurrently run ASCII commands over the network.

## 3.4.4. Enabling Access to APCON Software

WEBX is set, by default, to enable network use of these APCON software products:

- TITAN
- APCONCMDX
- CONTROLX
- MONITOR

**Note**

These products must be installed on a computer connected to your network. For a description of these products, see *Related Products* on page 3.

If you plan to use any of these APCON products, ensure that WEBX enables their use.

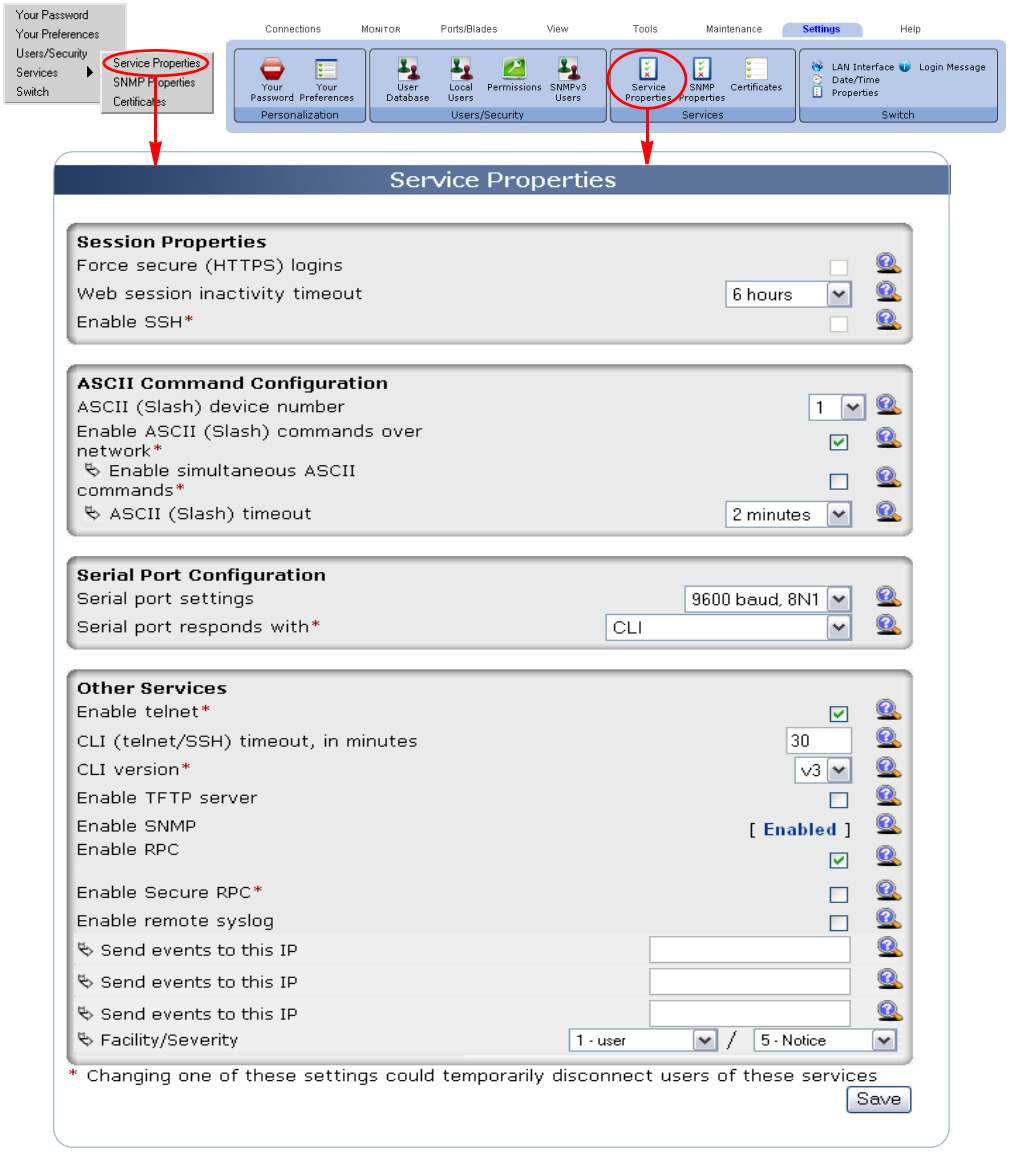
To enable network use of APCON software products:

1. Ensure that the following has occurred:
   - An IP address is set up, as described in *Setting the IP Address* starting on page 16.
   - The User Database is set to Internal, RADIUS, or TACACS+, as described in *Setting Up User Authentication* starting on page 21.
2. Log in as described in *Logging In* on page 23.

**Note**

If authentication is enabled, you must log in with Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

3. Select **Settings>Services>Service Properties**. The Service Properties screen displays:




4. Check the Enable RPC checkbox.
5. Click the Update button.

You can now access installed APCON software products.

# 3.5. What's Next

## 3.5.1. Configuring Ports and Port Access

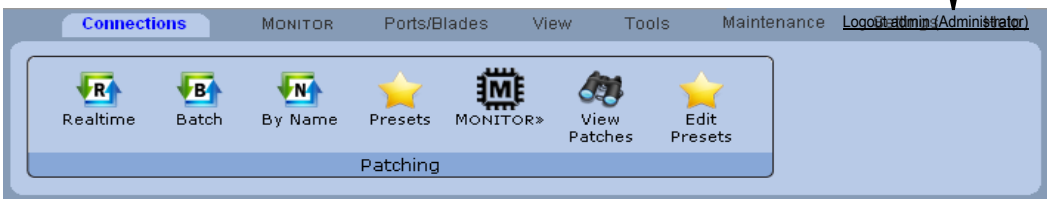
Although you can complete these tasks at any time, you may now want to set up the following:

- **Data Rate Selection**. For information about data rates, see *Rates* on page 52.
- **Port names**. For information about naming ports, see *Names* on page 63.
- **Zones**. For information about zoning, see *Zoning* on page 70.
- **Classes**. For information about classes, see *Classes* on page 65.

## 3.5.2. Logging Out

To log out of the switch, click the Logout prompt, located on the upper right side of the screen:

**Logout prompt** includes the current user's login name




**Note**

The switch automatically logs out users who have left the switch idle for over six hours.

# Chapter 4

# Connections

This chapter details the screens available from the Connections menu:

# 4.1. Realtime

Configuring your switch's patches in Batch mode means the patch settings immediately take effect. Select this option when you have few changes to make or when you need to immediately implement your changes.

**Note**

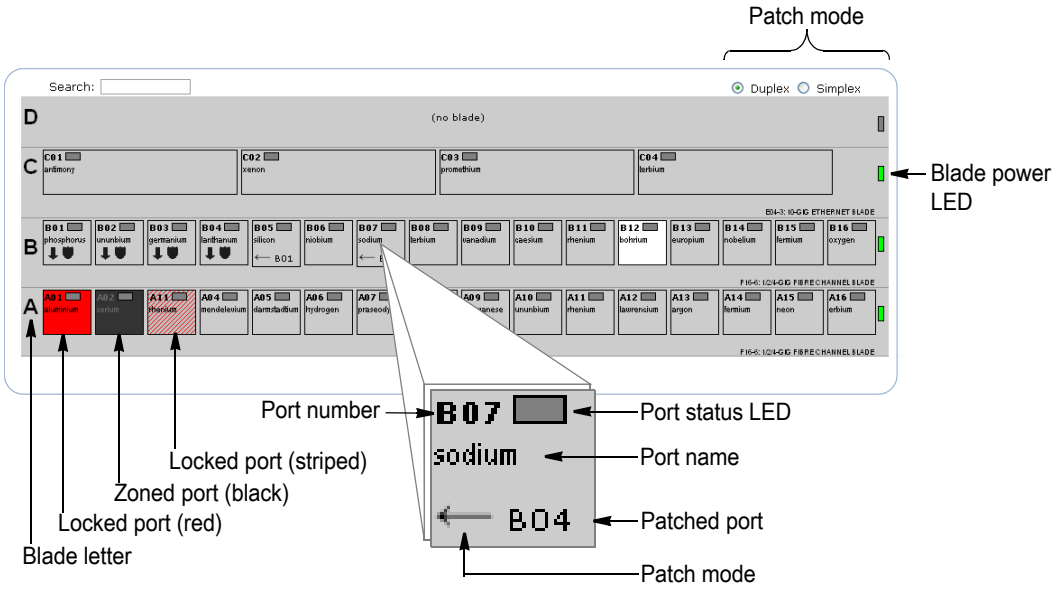
After setting up classes and assigning ports to those classes, you can quickly view and modify settings for SPAN and Analyzer ports by accessing the Monitor screen. For information about setting up classes, see *Classes* on page 65. For information about modifying settings, see *Chapter 5, MONITOR*, starting on page 48.

To view and configure your switch's current patches, select:

**Connections>Patching>Realtime**

This screen displays on the Canvas (this figure is truncated to more easily identify parts):

**Figure 8. Patch Ports: Realtime and Batch screens**




The screen includes these options:

**Note**

To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Patch mode | Clicking these radio buttons determines the direction of data flow:<br>• **Duplex (normal)**: All patching occurs in duplex, or bidirectional, mode.<br>• **Simplex (advanced)**: All patching occurs in simplex, or single direction, mode.<br>This option also displays at the bottom of the screen. |
| TRASH | Disconnects the selected port. |

| Field | Description |
|---|---|
| Cancel Drag | Discards, without saving changes, an in-process patch. |
| Lock/Unlock | Locks or unlocks the “picked up” port. |
| Search... | Displays a Search screen where you type the port name (a string) you want to locate:<br>Backspace key Clears characters. Use to correct entries.<br>Clear Clears an entry. Use to make new entries.<br>Up/down arrows Highlights the previous or next match, when more than one match displays.<br>Enter key Selects the highlighted item. |
| Refresh button | (Displays only on the Batch screen) Clicking this button retrieves current information from the switch and displays it on the screen.<br>When data changes (or might have changed), click the Refresh button to update the view. |
| Save button | (Displays only on the Batch screen) Clicking this button saves and implements your changes.<br>This button displays only on the **Connections>Patch ing>Batch** screen. It also displays at the bottom of the screen. |
| Locked port (red and striped) | Ports highlighted in red are not available for your use. They are reserved for the exclusive use of a specified user. Ports highlighted in red stripes are locked by you. Although they are reserved, you can unlock them.<br>For information about locked (reserved) ports, see *Locks* on page 54.<br>Note: If locked ports are not red, clear your internet cache:<br>1. Close the web browser.<br>2. Select Start>Settings>Control Panel>Internet Options.<br>3. In Temporary Internet Files, click the Delete Files button, then click the OK button.<br>4. Restart your web browser and access the switch. |
| Zoned port (black) | Ports highlighted in black are not available for your use. These ports belong to a zone that you do not have permission to access.<br>For information about zones, see *Zoning* on page 70 |

| Field | Description |
|---|---|
| Port number | Identifies the port and serves as a link location when patching port to one another. To patch a port:<br>1. Ensure that Data flow is set to the value you want: Duplex or Simplex.<br>**Note**: For details about how Patch Mode affects your patching, see *Patch Mode*, following this table.<br>2. Place the cursor over a port label or patched port textbox, then click. The following actions occur:<br>• A status message at the bottom of the screen identifies the port you selected.<br>• The action popup— which includes Trash, Lock Port, and Cancel links—displays at the top of the screen.<br>3. Do one of these:<br>• Click the label of a port—the port you want the selected port to patch to. Labels of the selected port(s) display in the Patched Port field of one or both ports, depending on the Data Flow you selected.<br>• Click the action link that produces the action you desire:<br>• **Trash**: Disconnects one or both ports, depending on the Data Flow you selected.<br>• **Cancel drag**: Terminates the current patch operation.<br>• **Lock Port**: Locks the port for the number of minutes you specify. You can optionally add a message regarding the lock. For details about locked (reserved) ports, see *Locks* on page 54.<br>**Note**: To verify a port's status and connections, hover the cursor over the port. Port status displays in a popup. |
| Port Status LED | The LED color indicates port status:<br>• **Green**: A signal is present. The letters indicate the rate: 10, 100, or GIGE (Gigabit Ethernet).<br>• **Gray**: No signal is present. |
| Patched port | Identifies the blade and port number this port is linked to. Also serves as a link location when patching port to one another. To patch a port, see Port number (at top of page).<br>The background color indicates port status:<br>• **White**: An SFP transceiver is inserted in the port, or the port is copper—which doesn't use an SFP transceiver.<br>• **Green**: An SFP transceiver is inserted in the port and the port is receiving signal, or the port is copper and it is receiving signal.<br>• **Gray**: No transceiver is installed, and the port is not copper. |
| Patch mode | Identifies the patch mode:<br>← Simplex<br>↔ Duplex<br>For details, see *Patch Mode* on page 36. |

| Field | Description |
|---|---|
| Blade letter | Displays the blade position within the chassis.<br>Blade labels use letters and start at the bottom. Port labels use numbers prefaced by blade letter, and start at the left. For more information, see *Switch Labeling* on page 9. |
| Blade power LED | The LED color indicates blade status:<br>• **Green**: This blade's power is on.<br>• **Gray**: This blade's power is off.<br>The LED is also a link which, when clicked, displays the Blade Power screen. For details about this screen, see *Power* on page 59. |

### 4.1.1. Patch Mode

The Patch mode you select results in the following:

- **Duplex (normal):** Connected ports each transmit and receive.

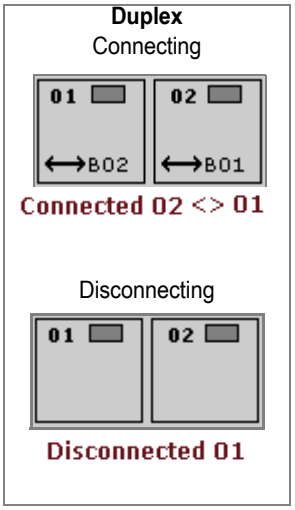
  When you select port A01, then select port A02, the ports connect and each port transmits or receives simultaneously.

  The label of the first selected port displays in the Patched Port field of the second selected port, and the label of the second selected port displays in the Patched Port field of the first selected port

  This bi-directional connection is indicated at the bottom of the screen with the "⟷" symbol.

  When you select either port, then click Trash, both ports disconnect.

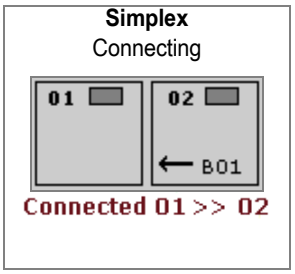
  If you change to Simplex mode, then select a port and click Trash, the port you selected disconnects.




- **Simplex (advanced)**: Connected ports either transmit or receive.

  When you select port A01, then select port A02, port A01 sends data to port A02. The label of the first selected port displays in the Patched Port field of the second selected port. This single-direction connection is indicated at the bottom of the screen with the "⟵" symbol.

  When you select port A01, then click Trash, the connection between A01 and A02 remains unchanged. When you select port A02, then click TRASH, the ports disconnect.



# 4.2. Batch

Configuring your switch's patches in Batch mode means the patch settings take effect only after you click the Save button. Select this option when you have multiple patches to make in a single transaction, or for complex changes.

**Note**

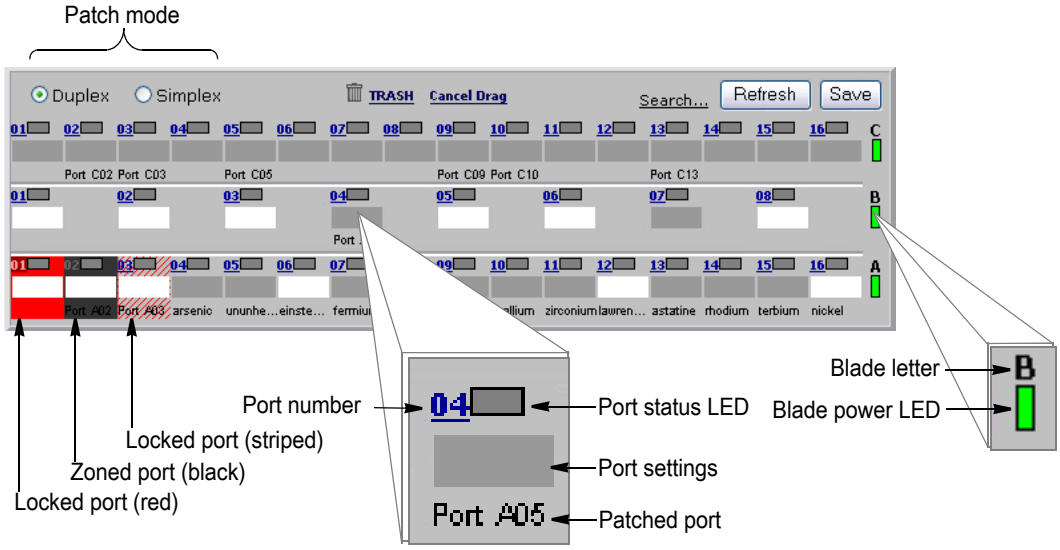
After setting up classes and assigning ports to those classes, you can quickly view and modify settings for SPAN and Analyzer ports by accessing the Monitor screen. For information about setting up classes, see *Classes* on page 65. For information about modifying settings, see *Chapter 5, MONITOR*, starting on page 48.

To view and configure your switch's current patches, select:

**Connections>Patching>Batch**

This screen displays on the Canvas (this figure is truncated to more easily identify parts):

**Figure 9. Patch Ports: Realtime and Batch screens**




The screen includes these options:

**Note**

To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Patch mode | Clicking these radio buttons determines the direction of data flow:<br>• **Duplex (normal)**: All patching occurs in duplex, or bidirectional, mode.<br>• **Simplex (advanced)**: All patching occurs in simplex, or single direction, mode.<br>This option also displays at the bottom of the screen. |
| TRASH | Disconnects the selected port. |
| Cancel Drag | Discards, without saving changes, an in-process patch. |

| Field | Description |
|---|---|
| Search... | Displays a Search screen where you type the port name (a string) you want to locate:<br>Backspace key — Clears characters. Use to correct entries.<br>Clear — Clears an entry. Use to make new entries.<br>Up/down arrows — Highlights the previous or next match, when more than one match displays.<br>Enter key — Selects the highlighted item. |
| Refresh button | (Displays only on the Batch screen) Clicking this button retrieves current information from the switch and displays it on the screen.<br>When data changes (or might have changed), click the Refresh button to update the view. |
| Save button | (Displays only on the Batch screen) Clicking this button saves and implements your changes.<br>This button displays only on the **Connections>Patch ing>Batch** screen. It also displays at the bottom of the screen. |
| Locked port (red and striped) | Ports highlighted in red are not available for your use. They are reserved for the exclusive use of a specified user. Ports highlighted in red stripes are locked by you. Although they are reserved, you can unlock them.<br>For information about locked (reserved) ports, see *Locks* on page 54.<br>Note: If locked ports are not red, clear your internet cache:<br>1. Close the web browser.<br>2. Select Start>Settings>Control Panel>Internet Options.<br>3. In Temporary Internet Files, click the Delete Files button, then click the OK button.<br>4. Restart your web browser and access the switch. |
| Zoned port (black) | Ports highlighted in black are not available for your use. These ports belong to a zone that you do not have permission to access.<br>For information about zones, see *Zoning* on page 70 |

| Field | Description |
|---|---|
| Search... | Displays a Search screen where you type the port name (a string) you want to locate:<br>Backspace key — Clears characters. Use to correct entries.<br>Clear — Clears an entry. Use to make new entries.<br>Up/down arrows — Highlights the previous or next match, when more than one match displays.<br>Enter key — Selects the highlighted item. |
| Refresh button | (Displays only on the Batch screen) Clicking this button retrieves current information from the switch and displays it on the screen.<br>When data changes (or might have changed), click the Refresh button to update the view. |
| Save button | (Displays only on the Batch screen) Clicking this button saves and implements your changes.<br>This button displays only on the **Connections>Patch ing>Batch** screen. It also displays at the bottom of the screen. |
| Locked port (red and striped) | Ports highlighted in red are not available for your use. They are reserved for the exclusive use of a specified user. Ports highlighted in red stripes are locked by you. Although they are reserved, you can unlock them.<br>For information about locked (reserved) ports, see *Locks* on page 54.<br>Note: If locked ports are not red, clear your internet cache:<br>1. Close the web browser.<br>2. Select Start>Settings>Control Panel>Internet Options.<br>3. In Temporary Internet Files, click the Delete Files button, then click the OK button.<br>4. Restart your web browser and access the switch. |
| Zoned port (black) | Ports highlighted in black are not available for your use. These ports belong to a zone that you do not have permission to access.<br>For information about zones, see *Zoning* on page 70 |

| Field | Description |
|---|---|
| Port number | Identifies the port and serves as a link location when patching port to one another. To patch a port:<br>1. Ensure that Data flow is set to the value you want: Duplex or Simplex.<br>**Note**: For details about how Patch Mode affects your patching, see *Patch Mode*, following this table.<br>2. Place the cursor over a port label or patched port textbox, then click. The following actions occur:<br>• A status message at the bottom of the screen identifies the port you selected.<br>• Action links—Trash and Cancel drag—display at the top and bottom of the screen.<br>3. Do one of these:<br>• Click the label of a port—the port you want the selected port to patch to. Labels of the selected port(s) display in the Patched Port field of one or both ports, depending on the Data Flow you selected.<br>• Click the action link that produces the action you desire:<br>• **Trash**: Disconnects one or both ports, depending on the Data Flow you selected.<br>• **Cancel drag**: Terminates the current patch operation. |
| Port Status LED | The LED color indicates port status:<br>• **Green**: A signal is present. The letters indicate the rate: 10, 100, or GIGE (Gigabit Ethernet).<br>• **Gray**: No signal is present. |
| Port settings<br>[R P C] | Each letter within the braces is a separate option. Selecting an option produces these results:<br>R (Rate Select) Displays the port's Set Rate Selection screen. For information about the options on this screen, see *Rates* on page 52.<br>P (Port Properties) Displays the port's Port Properties screen. For information about the options on this screen, see *Port Properties* on page 50.<br>C (Connections) Highlights all ports connected to this port. Select this option to quickly identify ports patched to the source. |
| Patched port | Identifies the blade and port number this port is linked to. Also serves as a link location when patching port to one another. To patch a port, see Port number (at top of page).<br>The background color indicates port status:<br>• **White**: An SFP transceiver is inserted in the port, or the port is copper—which doesn't use an SFP transceiver.<br>• **Green**: An SFP transceiver is inserted in the port and the port is receiving signal, or the port is copper and it is receiving signal.<br>• **Gray**: No transceiver is installed, and the port is not copper. |

| Field | Description |
|---|---|
| Blade letter | Displays the blade position within the chassis.<br>Blade labels use letters and start at the bottom. Port labels use numbers prefaced by blade letter, and start at the left. For more information, see *Switch Labeling* on page 9. |
| Blade power LED | The LED color indicates blade status:<br>• **Green**: This blade's power is on.<br>• **Gray**: This blade's power is off.<br>The LED is also a link which, when clicked, displays the Blade Power screen. For details about this screen, see *Power* on page 59. |

## 4.2.1. Patch Mode

The Patch mode you select results in the following:

- **Duplex (normal):** Connected ports each transmit and receive.

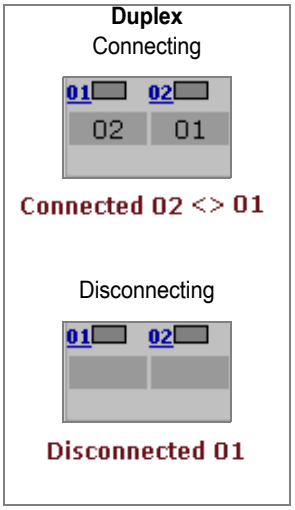
  When you select port A01, then select port A02, the ports connect and each port transmits or receives simultaneously.

  The label of the first selected port displays in the Patched Port field of the second selected port, and the label of the second selected port displays in the Patched Port field of the first selected port

  This bi-directional connection is indicated at the bottom of the screen with the "< >" symbol.

  When you select either port, then click Trash, both ports disconnect.

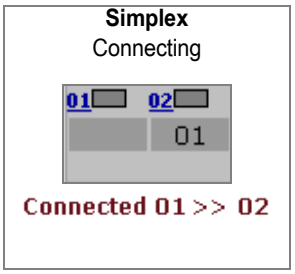
  If you change to Simplex mode, then select a port and click Trash, the port you selected disconnects.




- **Simplex (advanced)**: Connected ports either transmit or receive.

  When you select port A01, then select port A02, port A01 sends data to port A02. The label of the first selected port displays in the Patched Port field of the second selected port. This single-direction connection is indicated at the bottom of the screen with the ">> " symbol.

  When you select port A01, then click Trash, the connection between A01 and A02 remains unchanged. When you select port A02, then click TRASH, the ports disconnect.



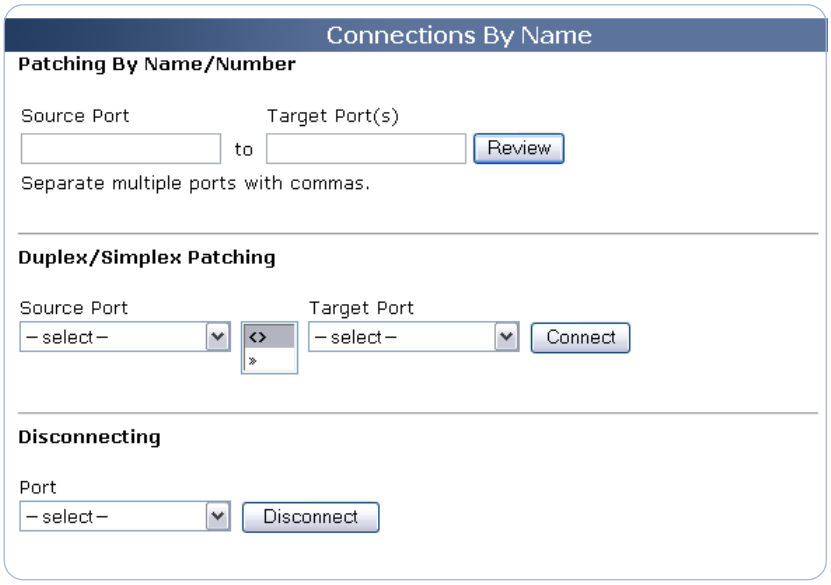
# 4.3. By Name

To quickly configure patch settings, select:

**Connections>Patching>By Name**

This screen displays on the Canvas:

**Figure 10. By Name screen**




The screen includes these options:

**Note**

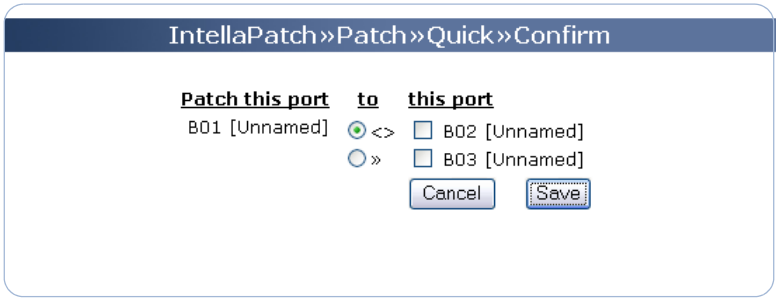
To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Patching By Name/Number | Use the top section of the screen when you know the name and/or number of the ports you want to connect, or to enter many target ports in a single entry.<br>• **Source Port**: Enter the source port name or number—the port you want to patch from—in the text box on the left.<br>• **Target Ports**: Enter the target port or ports—the port(s) you want the selected port to patch to—in the text box on the right. You can enter either the name or number.<br>Entering A00 turns the port off; A99 leaves the port unchanged.<br>By default, all patching occurs in duplex, or bidirectional, mode. To change the mode, click the Review button.<br>• **Review button**: Click this button to display the Quick Patch Review dialog box where you can customize your entry. For information about this dialog box, see *By Name: Review* on page 43. |

| Field | Description |
|---|---|
| Duplex/Simplex Patching | Use the middle section of the screen to display a list of ports from which you can select:<br>• **Source Port**: Select the source port—the port you want to patch from—from the drop-down list on the left.<br>• **Target Port**: Select the target port—the port(s) you want the selected port to patch to—in the drop-down list on the right.<br>• **Direction**: Indicates the direction of data:<br>**>> (Simplex)**: Data flows from the Source to the Target.<br>**<> (Duplex)**: Data flows both directions.<br>• **Connect button**: Click this button to save and implement your settings. |
| Disconnecting | To disconnect a port:<br>• **Port**: Select the port you want to disconnect from the drop-down list.<br>• **Disconnect button**: Click this button to disconnect the port.<br>**Note**: If the port you disconnect is bi-directionally patched to another port, the other port also disconnects. |

## 4.3.1. By Name: Review

**Figure 11. By Name: Review dialog box**




The dialog box includes these options:

**Note**

To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Patch this port | Displays the source port—the port you want to patch from—in the left column. |
| to | Indicates the direction of data:<br>**>> (Simplex)**: Data flows in only one direction.<br>**<> (Duplex)**: Data flows both directions.<br>**Note**: By default, all patching occurs in duplex, or bidirectional, mode. You can change the mode on this screen. |

| Field | Description |
|---|---|
| this port | Displays the target port or ports—the port(s) you want the selected port to patch to—in the right column. |
| Save button | Click this button to save and implement your settings. |

# 4.4. By Preset (Presets)

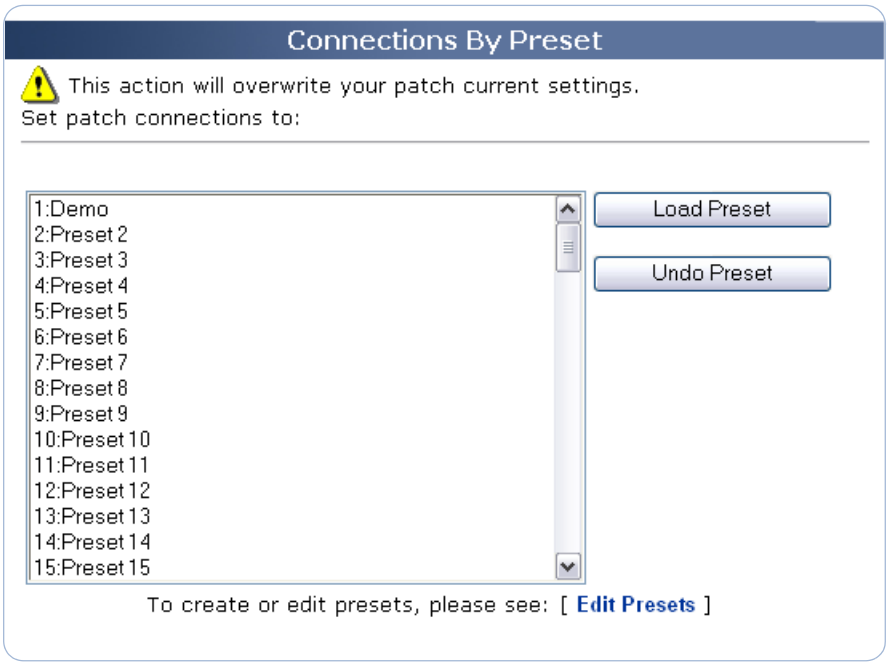
Saves, changes, or clears configuration settings, referred to as “presets.” You can save up to ninety nine different switch configurations as a preset. Once you reach ninety nine saved configurations, you must clear an existing preset configuration to make room for a new one.

To create, change, and delete switch settings, select:

**Connections>Patching>Presets**

These screens display simultaneously on the Canvas:

**Figure 12. By Preset (Presets) screens**




The screen includes these options:

**Note**

To make changes on this screen, your account must have a minimum of Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Preset 1–99 | A configuration assigned to this preset number and name.<br>A configuration includes only patch connections.<br>For information about assigning a configuration to a Preset, see *Edit Presets* on page 75. |
| Load Preset button | Sets the switch to the configuration to the preset name or number selected in the list at left.<br>**CAUTION**: This action overwrites current patch settings. |
| Undo Preset button | |
| To create or edit presets, please see: [Edit Presets] | Displays the Edit Presets screen where you can set switches to a saved configuration. For more information about this screen, see page 75. |

## 4.5. With MONITOR (MONITOR)

To access APCON's MONITOR software which non-intrusively connects to and controls any INTELLAPATCH switch using the PC's serial port or TCP/IP LAN connection and shares equipment, select:

**Connections>Patching>MONITOR**

The MONITOR screen displays. For more information about MONITOR, see chapter *Chapter 5, MONITOR*, starting on page 48.

**Note**

To use the MONITOR feature, you must fbtain a license key from APCON. For information about license keys, see *License Key* on page 98. To find out how to contact APCON, see *Contacting APCON* on page 4.

**Note**

You can also acess this tool by selecting:

**Connections>MONITOR**

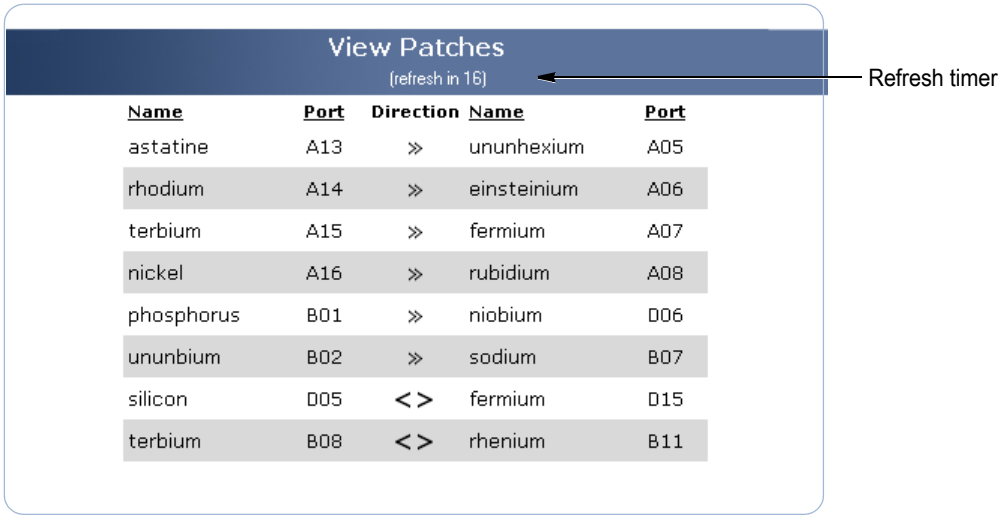
# 4.6. View Patches

To view your switch's current patch connections, select:

**Connections>*Patching*>View Patches**

This screen displays on the Canvas:

**Figure 13. View Patches screen**




The screen includes these options:

**Note**

To view this screen, your account needs only Guest permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Name | The port name you specify. For information about naming ports, see *Names* on page 63. |
| Port | The port number. Blade labels use letters and start at the bottom. Port labels use numbers prefaced by blade letter, and start at the left. For details, see *Switch Labeling* on page 9. |
| Direction | Indicates the direction of data:<br>**>> (Simplex)**: Data flows in only one direction.<br>**<> (Duplex)**: Data flows both directions. |
| Refresh timer | Displays the number of seconds remaining before the data refreshes. A refresh occurs every thirty seconds. |

# Chapter 5

# MONITOR

MONITOR software connects to and controls any APCON INTELLAPATCH Physical Layer Switch using the PC's serial port or TCP/IP LAN connection. The software is specifically tailored for non-intrusive network monitoring and for sharing equipment such as traffic analyzers, network probes and Intrusion Detection System (IDS) equipment.

A powerful addition to your network administration toolset, you use APCON MONITOR software to:

- Electronically move and share monitoring equipment to increase utilization of existing equipment.
- Increase network visibility, getting a quick snapshot of network connections to monitoring devices.
- Gather information at-a-glance about ports, connections, data rates and more.
- Employ digital diagnostics and INTELLAPATCH switch monitoring.
- Control user permissions for modifying system status and software options.

**Note**

MONITOR software is not intended for in-line monitoring/electronic tapping, wherein data is passed through the switch, with traffic in both directions mirrored non-intrusively by the analyzer device. To implement this functionality, consider the WEBX Realtime or Batch interfaces.

Accessing MONITOR software through WEBX requires a license key from APCON. To find out how to contact APCON, see *Contacting APCON* on page 4. After obtaining the key, you must activate the MONITOR feature as described in *License Key* on page 98.

To find out more about operating MONITOR software, see the *MONITOR User Manual.*

# Chapter 6

# Ports/Blades

This chapter details the screens available from the Ports/Blades menu:

# 6.1. Ports

## 6.1.1. Port Properties

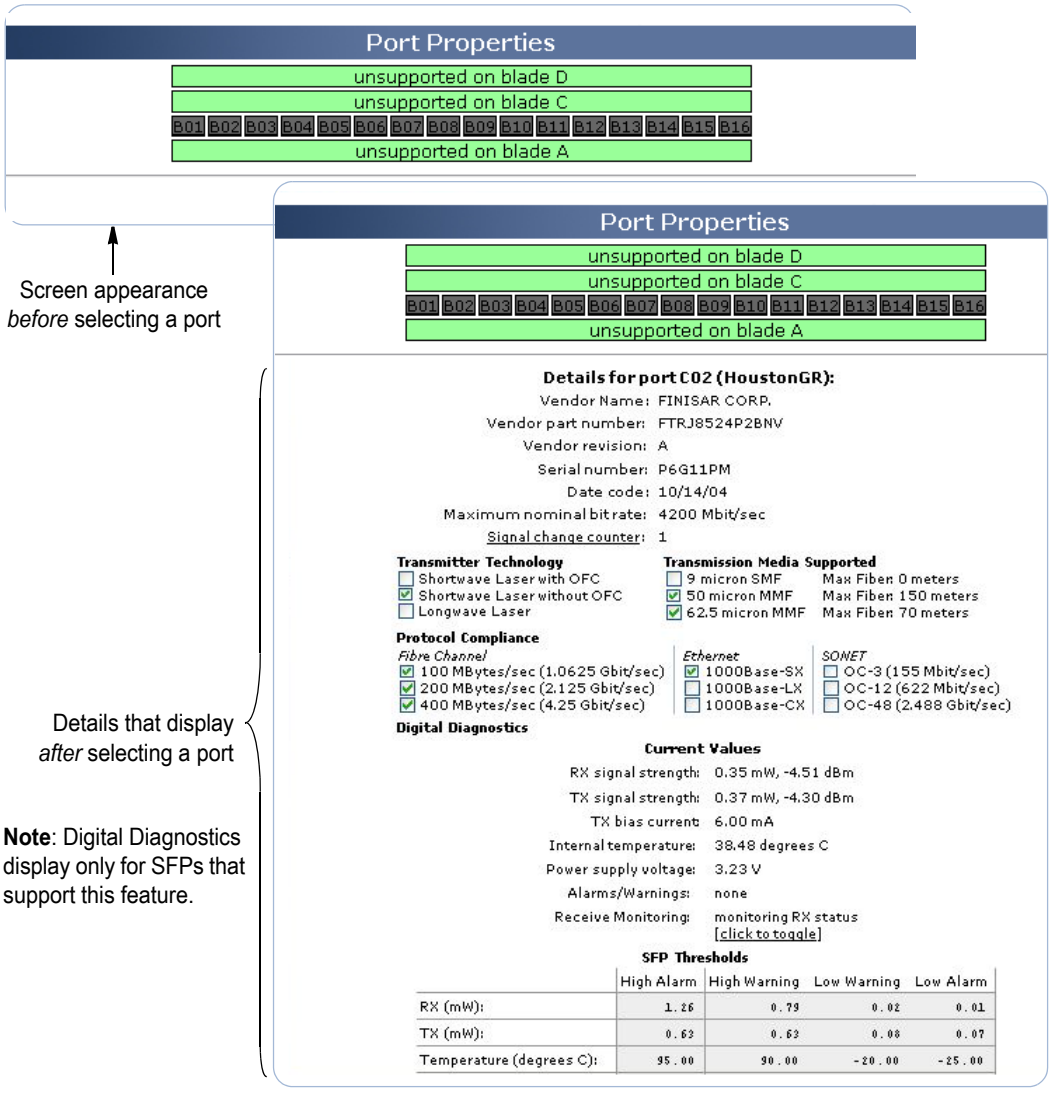
Many transceiver modules have manufacturer-provided identification capabilities, allowing you to determine part numbers, serial numbers, supported transmission media, protocol compliance, maximum data rate, digital diagnostics, or other vendor-specific parameters.

To view transceiver details, select:

**Ports/Blades>Ports>Properties**

This screen displays on the Canvas:

**Figure 14. Port Properties screen**




The screen includes these options:

**Note**

To make changes on this screen, your account needs only Guest permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Port numbers | Identifies ports. The background color indicates port status:<br>• **White**: An SFP transceiver is inserted in the port, but is not receiving signal.<br>• **Green**: An SFP transceiver is inserted in the port and the port is receiving signal.<br>• **Gray**: No transceiver is installed.<br>To select the port whose transceiver information you want to view, place the cursor over port number and click. The screen enlarges to display vendor information. You can display only one port's vendor information at a time.<br>Blades that do not support SFP transceivers (for example, copper blades) display this message:<br>`unsupported on Blade n` |
| Vendor information | Displays the vendor name, part number and revision, serial number, date, maximum data rate, and any other information the vendor makes available. |
| Transmitter Technology | Displays the transmitter capabilities of this SFP transceiver:<br>☐ **Unchecked**: The SFP transceiver does not support the specified item.<br>☑ **Checked**: The SFP transceiver supports the specified item. To determine whether the blade supports the item, see *Rates* (page 52) and the blade's data sheet. |
| Protocol Compliance | Displays the protocols this device complies with:<br>☐ **Unchecked**: The SFP transceiver does not support the specified item.<br>☑ **Checked**: The SFP transceiver supports the specified item. To determine whether the blade supports the item, see *Rates* (page 52) and the blade's data sheet. |
| Digital Diagnostics | Displays real-time digital diagnostics for SFPs that support this feature.<br>Real-time parameters include transceiver temperature, laser bias current, transmitted and received optical power, transceiver supply voltage, and alarm status. |
| Transmission Media Supported | Displays the supported transmission media supported by the device:<br>☐ **Unchecked**: The SFP transceiver does not support the specified item.<br>☑ **Checked**: The SFP transceiver supports the specified item. To determine whether the blade supports the item, see *Rates* (page 52) and the blade's data sheet. |

## 6.1.2. Rates

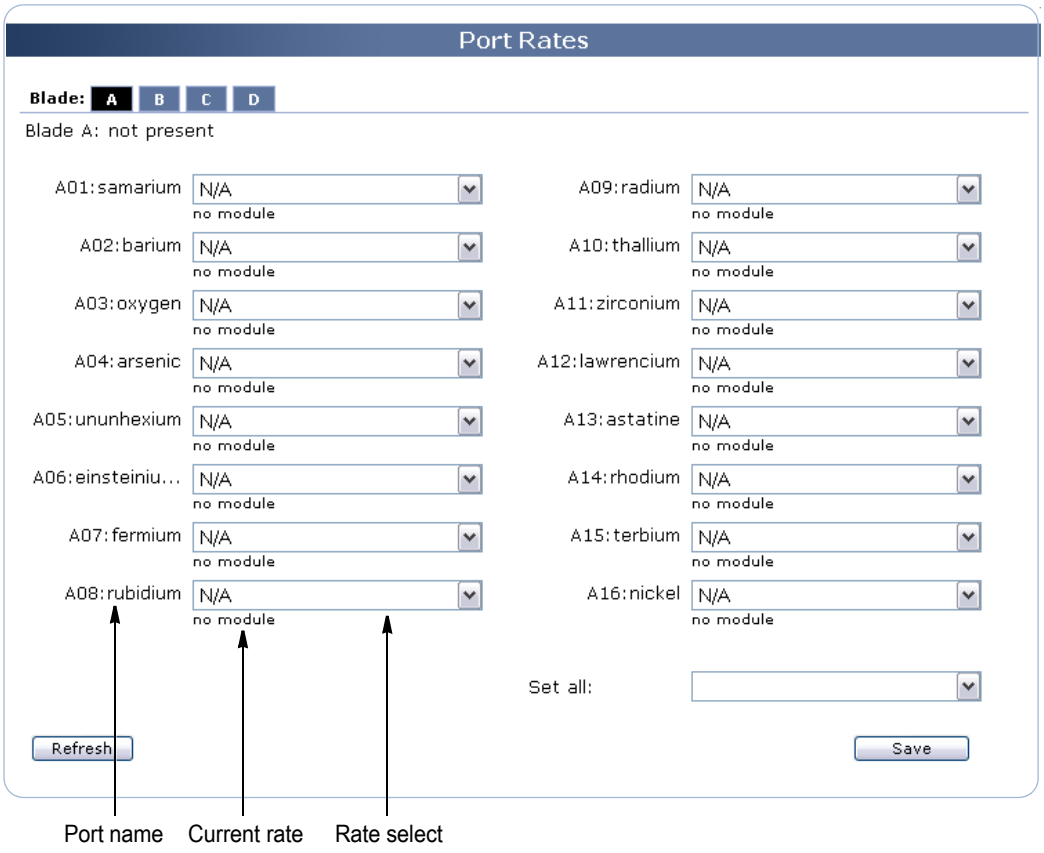
Depending on the capabilities of a given port, you can change the data rate and other transmission characteristics.

To set your switch's data transmission rate, select:

**Ports/Blades>Ports>Rates**

This screen displays on the Canvas:

**Figure 15. Rates screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Blades<br>(Tabs A, B, C ...) | Clicking a tab displays the rate settings for the specified blade.<br>Tab letters match the blade numbers on your INETELLAPATCH chassis. Blade labels use letters and start at the bottom. Port labels use numbers prefaced by blade letter, and start at the left. For details, see *Switch Labeling* on page 9. |

| Field | Description |
|---|---|
| Port name | Identifies the port assignment. The port name consists of:<br>*PortNumber*:*PortName*<br>Where *PortNumber* is the number assigned to the port and *PortName* is the name you specify. If you do not specify a port name, Unnamed displays.<br>For information about naming ports, *Names* on page 63. |
| Current rate | Displays the rate at which the port currently transmits data and the duplex setting, either full or half. Blades that do not have a rate select option display N/A. |
| Rate select | The rate at which the port transmits data. Each blade model supports different options; some values include:<br>• **Auto**: The switch negotiates the fastest possible rate to transmit data, and accommodates changing devices with maximum flexibility.<br>• **Full/half**: Allows the port to transmit and receive in full duplex mode when connected to a duplex device, but negotiate down to half duplex automatically when necessary.<br>• **N/A**: Not applicable |
| Set all | Selecting a value sets all the ports on this blade to the specified rate when you click the Save button. |
| Refresh button | Clicking this button retrieves current information from the switch and displays it on the tab. |
| Save button | Clicking this button saves and implements your changes. |

## 6.1.3. Locks

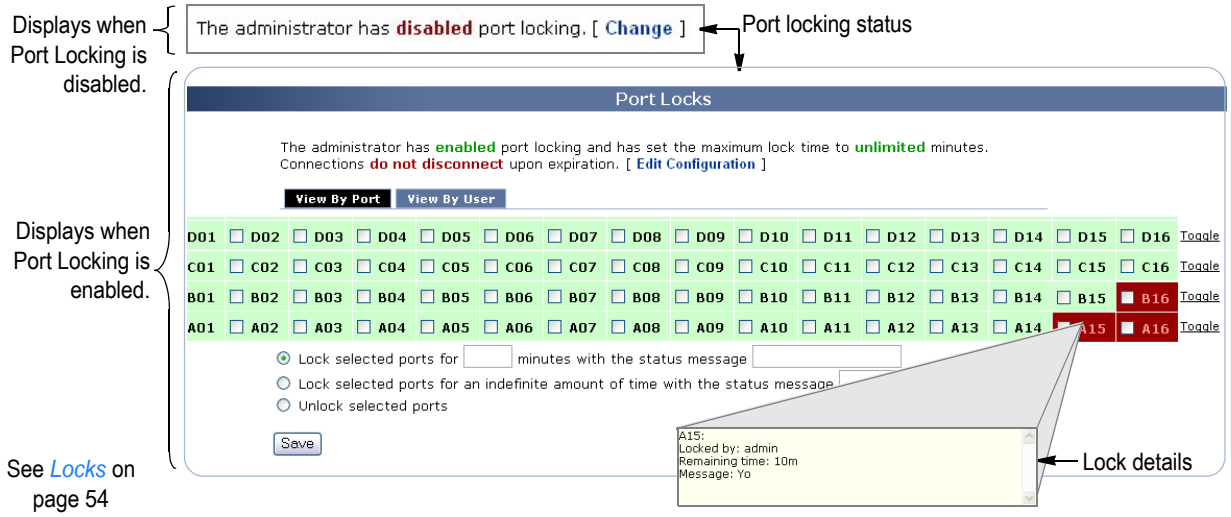
Reserves the specified port(s) for your exclusive use.

To access port locking options, select:

**Ports/Blades>Ports>Locks**

This screen displays on the Canvas:

**Figure 16. Locks screen**




The screen includes these options:

**Note**

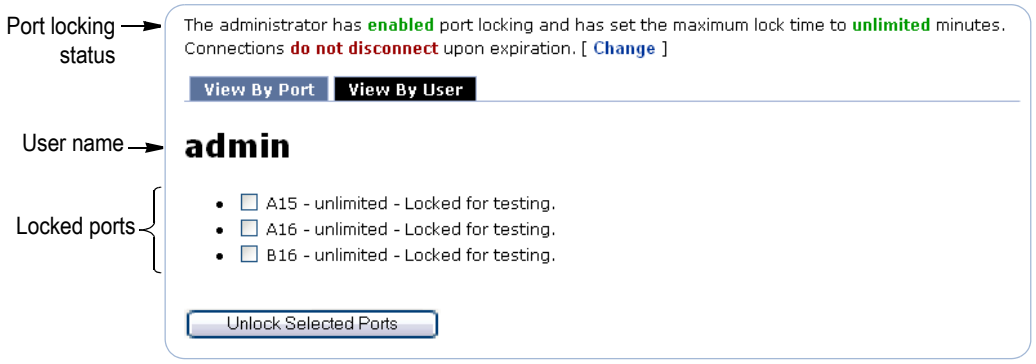
To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Port locking status | Located at the top of the screen, this message indicates:<br>• Port locking status, either enabled or disabled.<br>• Maximum lock duration, either a fixed or unlimited number of minutes.<br>• Disposition of connections when lock duration expires. |
| Change | Clicking this link displays the *Port Locking* screen where you can specify the port lock settings to allow. For details about this screen, see page 69. |
| Tabs | Clicking a tab displays the the following<br>• **View By Port tab**, shown in the above figure, that you use to lock and unlock ports. Ports display by blade.<br>• **View By User tab**, shown on page 55, that you use to view ports locks set by each user, and to unlock ports. |

| Field | Description |
|---|---|
| Ports | Identifies the port and serves as the link location when locking ports. To lock a port:<br>1. Select the port(s) you want to lock using one of these methods:<br>• Place the cursor over the port's checkbox and click.<br>• Click the Toggle link, located on the right side of the screen, for the blade whose ports you want to lock.<br>2. Specify the port lock settings, located at bottom of the screen.<br>3. Click the Save Changes button.<br>Locked ports display as red, while unlocked ports remain green. |
| Lock details | Hovering your cursor over a port displays the following lock information for that port:<br>• ***Port number: Port name**:* Identifies the port assignment. *PortNumber* is the number assigned to the port and *PortName* is the name you specify. If you do not specify a port name, `Unnamed` displays.<br>For information about naming ports, *Names* on page 63.<br>• **Locked by**: The login name of the user that set the lock.<br>• **Remaining time**: The number of minutes the lock remains in effect.<br>• **Message (optional)**: A message from the user that set the lock. |
| Toggle | Checks or unchecks all ports on the selected blade. |
| Port lock settings | Specifies the settings for this lock operation:<br>• **Lock selected ports for *n* minutes with the status message *abc***: Specifies the duration of the lock and the message that displays when users try to access a port while locked.<br>**Note**: To change the number of minutes, you must cancel the lock, then lock the port again with a different duration.<br>• **Unlock selected ports**: Releases the lock |
| Save button | Clicking this button saves and implements your changes. |

### 6.1.3.1. Locks: View By User tab

**Figure 17. Locks: View By User tab**




The screen includes these options:

**Note**

To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Port locking status | Located at the top of the screen, this message indicates:<br>• Port locking status, either enabled or disabled.<br>• Maximum lock duration, either a fixed or unlimited number of minutes. |
| Tabs | Clicking a tab displays the the following<br>• **View By User tab**, shown in the above figure, that you use to view ports locks set by each user, and to unlock ports.<br>• **View By Port tab**, shown on page 54, that you use to lock and unlock ports. Ports display by blade. |
| User name | Displays the user's login name. |
| Locked ports | Displays the ports locked by each user. You can also unlock a ports from this screen:<br>**Note**: Users with Administrator permission privileges can unlock any port. Users with Advanced Operator Other permission privileges can unlock only the ports they locked.<br>1. Select the port or ports you want to unlock using one of these methods by placing the cursor over the port's checkbox and clicking.<br>2. Click the Unlock Selected Ports button. The View By Port tab displays. |
| Unlock Selected Ports button | Unlocks the specified ports and displays the View By Port tab. |

# 6.2. Blades

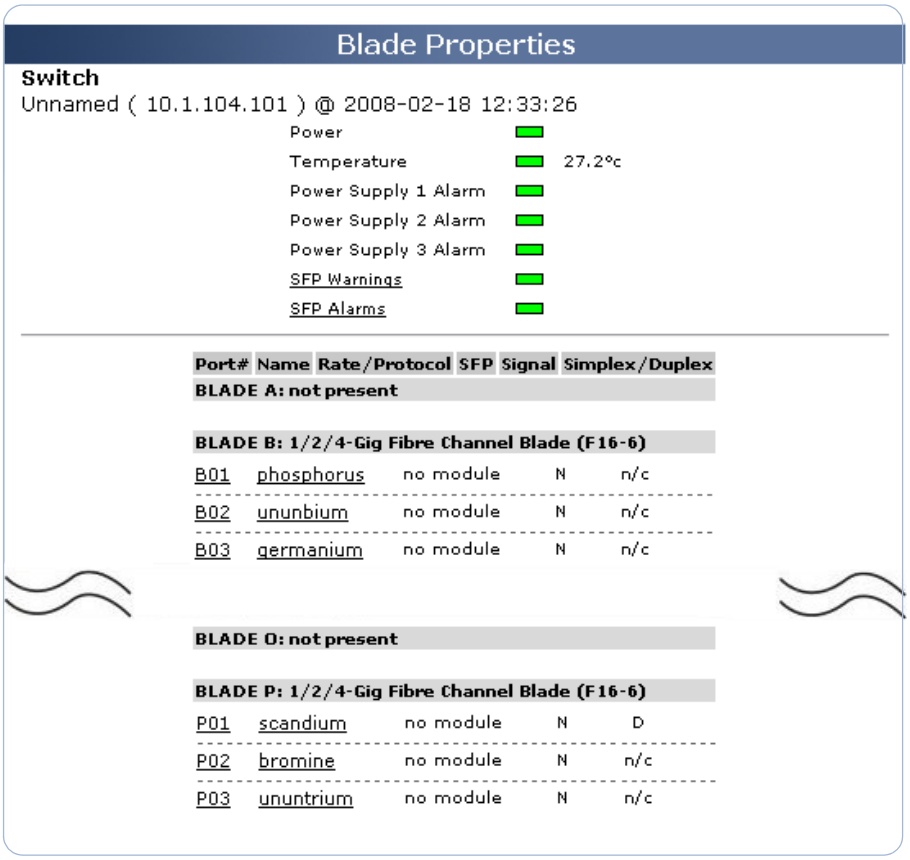
## 6.2.1. Properties

To view your switch's current patches, settings, and port properties, select:

**Ports/Blades>Blades>Properties**

This screen displays on the Canvas:

**Figure 18. Properties screen**




The screen includes these options:

**Note**

To view this screen, your accountneeds only Guest permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Switch | The screen's top section displays information about the switch:<br>• **Switch name**: The name and IP address you specified for the switch.<br>To change the switch name, see *Properties* on page 57. To change the IP address, see *LAN Interface* on page 129.<br>• **Power**: Indicates whether power is supplied to the switch. |

| Field | Description |
|---|---|
| Switch | • **Temperature**: Indicates temperature and status:<br>  • **Green**: Internal temperature is within specified limits.<br>  • **Flashing red**: Internal temperature exceeds the specified maximum temperature threshold. If this occurs, the switch also emits an audible alarm, provided the audible alarm is enabled. For information about audible alarms, see *Properties* on page 133.<br>The default temperature threshold is 50° C. To change the default, see *Properties* on page 133.<br>• **Power Supply *n* Alarm**: Indicates operational status of the specified power supply.<br>  • **Green**: The power supply is functioning normally.<br>  • **Flashing red**: The power supply failed. If this occurs, the switch also emits an audible alarm, provided the audible alarm is enabled. For information about audible alarms, see *Properties* on page 133.<br>• **SFP Warnings and SFP alarms**: Indicates whether any SFP warnings or alarms exist<br>  • **Gray**: Monitoring is disabled.<br>  • **Green**: No alarms exist; SFPs are functioning normally.<br>  • **Flashing red**: At least one SFP warning or alarm exists.<br>Clicking the links to the left of the LED displays the Alarms screen where you can view warning and alarm details. For more information about this screen, see *Alarms* on page 61. |
| Port# | The port number. |
| Name | The port name. |
| Rate/Protocol | Specifies the data rate and protocol the port is currently negotiated at or hard set to. Fiber optic blades that don't support auto-negotiation display only `signal` or `no signal`. |
| SFP | Indicates transceiver status:<br>• **Y (Yes)**: An SFP transceiver is inserted in the port, or the port is copper.<br>• **N (No)**: No SFP transceiver exists. |
| Signal | Indicates signal status:<br>(Green) The port currently has signal.<br>(Gray) The port does not have a signal. |
| Simplex/Duplex | Displays the direction of data flow:<br>D (Duplex) The port is configred in duplex, or bidirectional, mode.<br>S (Simplex) The port is configured in simplex, or single direction, mode.<br>n/c No connection. |

## 6.2.2. Power

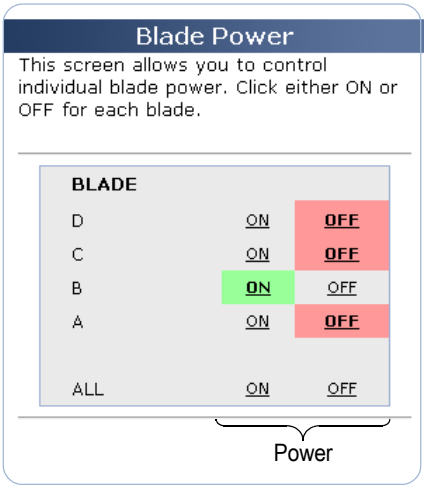
Before inserting or removing a blade, power to its slot must be turned off.

To turn a blade slot's power off or on, select:

**Ports/Blades>Blades>Power**

This screen displays on the Canvas:

**Figure 19. Power screen**




**Note**

To make changes on this screen, your account must have a minimum of Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

The screen includes these options:

| Field | Description |
|---|---|
| Blade | Identifies the blade, and therefore slot, whose power status you want to change.<br>Blade labels use letters and start at the bottom. For details, see *Switch Labeling* on page 9. |
| Power | Determines the blade slot power status:<br>• **ON**: Turns blade power on. When you select this option, the background changes to green.<br>• **OFF**: Turns blade power off. When you select this option, the background changes to red. |
| ALL | Sets the blade slot power status for all blades in the chassis:<br>• **ON**: Turns power on for all blades. When you select this option, the background changes to green.<br>• **OFF**: Turns power off for all blades. When you select this option, the background changes to red. |

# 6.3. SFP/XFP

## 6.3.1. Properties

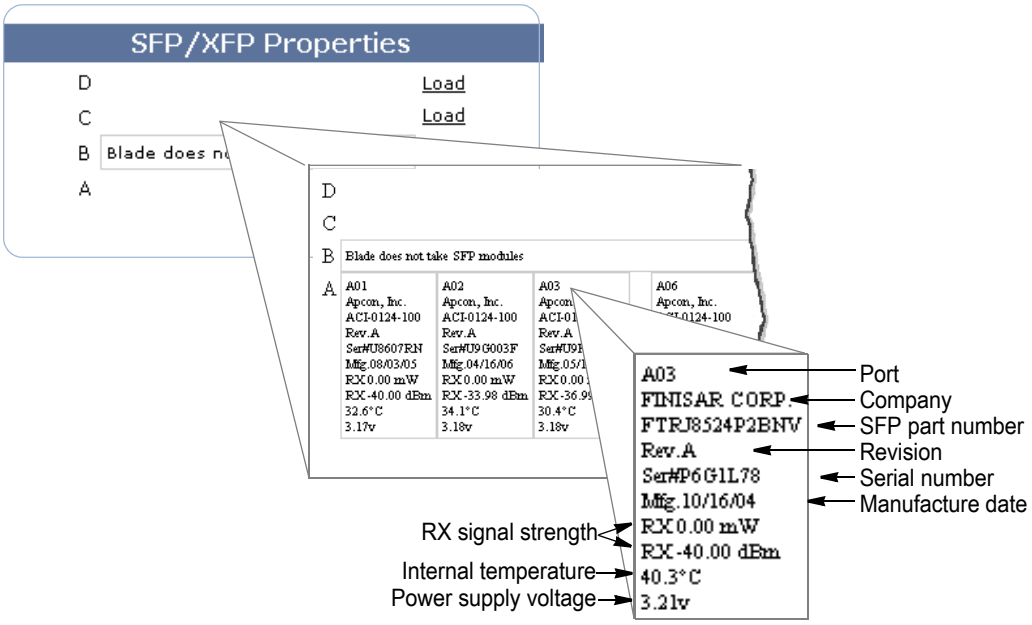
Displays SFP transceiver information in a format you can quickly view and copy.

To display transceiver properties, select:

**Ports/Blades>SFP/XFP>Properties**

This screen displays on the Canvas:

**Figure 20. Properties screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *User Levels* on page 95.

| Field | Description |
|---|---|
| Load | Clicking this link loads and displays SFP information for the blade or blades you select. |
| Port | Identifies the port. |
| Company | Displays APCON as the INTELLAPATCH switch manufacturer. |
| SFP part # | The SFP's part number. |
| Revision | The switch's revision number. |
| Serial number | The switch's serial number. |
| Manufacture date | The switch's manufacture date. |
| RX signal strength | Displays the SFP's Receive signal strength. |
| Internal temperature | Indicates SFP temperature. |
| Power supply voltage | Indicates SFP voltage. |

## 6.3.2. Alarms

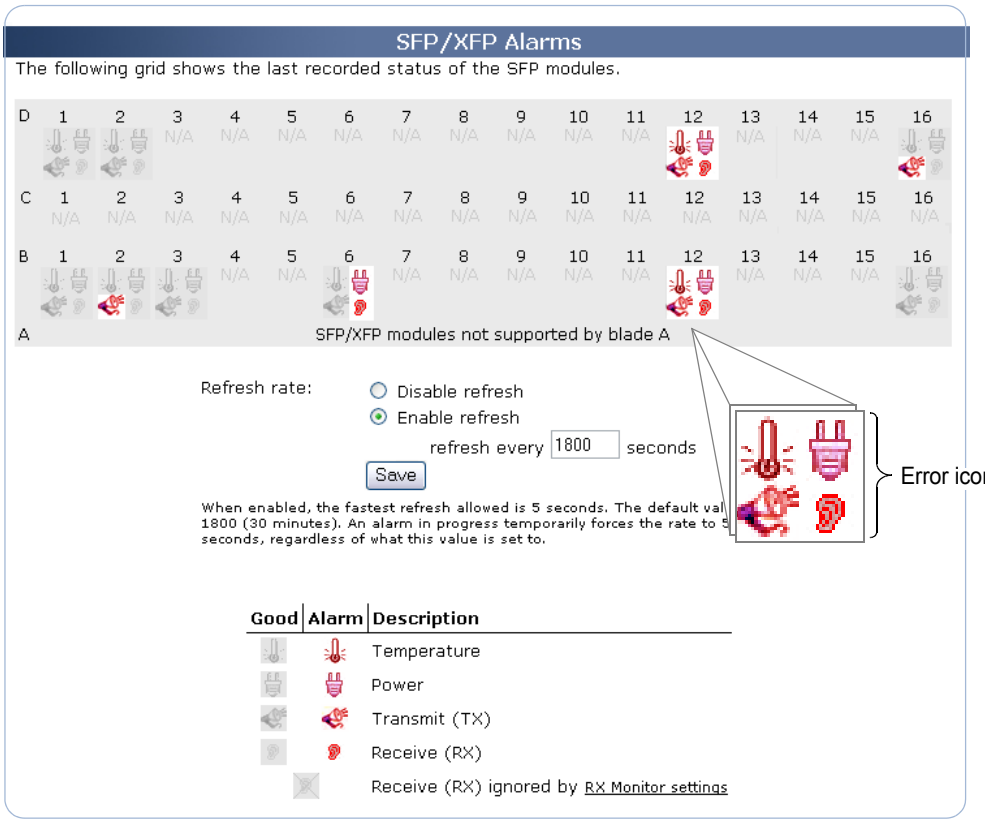
Indicates warning and error conditions for the SFP transceivers.

To monitor transceiver status, select:

**Ports/Blades>SFP/XFP>Alarms**

This screen displays on the Canvas:

**Figure 21. Alarms screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Error icons | When red, each icon alerts you to an error in any of these areas:<br>  Power<br>  Receive[1]<br>  Transmit<br>  Temperature<br>For details about an error, hover over or click the red icon. The Port Properties screen, with error detail, displays. For information about this screen, see *Port Properties* on page 50.<br>[1] You can specify which ports to monitor and which to ignore. For details, see Receive rate ignored by RX Monitor settings (below).<br>Ignored ports display an inactive (gray) icon with an "X" (  ) |
| Refresh rate | Determines whether and how data on the screen refreshes:<br>• **Disable refresh**: Data does not refresh.<br>• **Enable refresh**: Refreshes data at the interval specified in "refresh every *n* seconds." The default is 1800 seconds (30 minutes).<br>While an alarm condition exists, data refreshes every 10 seconds (overriding the specified Refresh rate) until the alarm/warning is resolved. |
| Save button | Clicking this button saves and implements your changes. |
| Receive rate ignored by RX Monitor settings | Clicking the RX Monitor settings link displays the Monitoring screen where you specify which port signals to monitor and which to ignore. For details about this screen, see *Receive Monitoring* on page 74. |

# 6.4. Configuration

## 6.4.1. Names

Although port numbers are automatically designated, you can assign names to your ports, names that indicate devices they connect to or to provide other meaningful aids to memory.

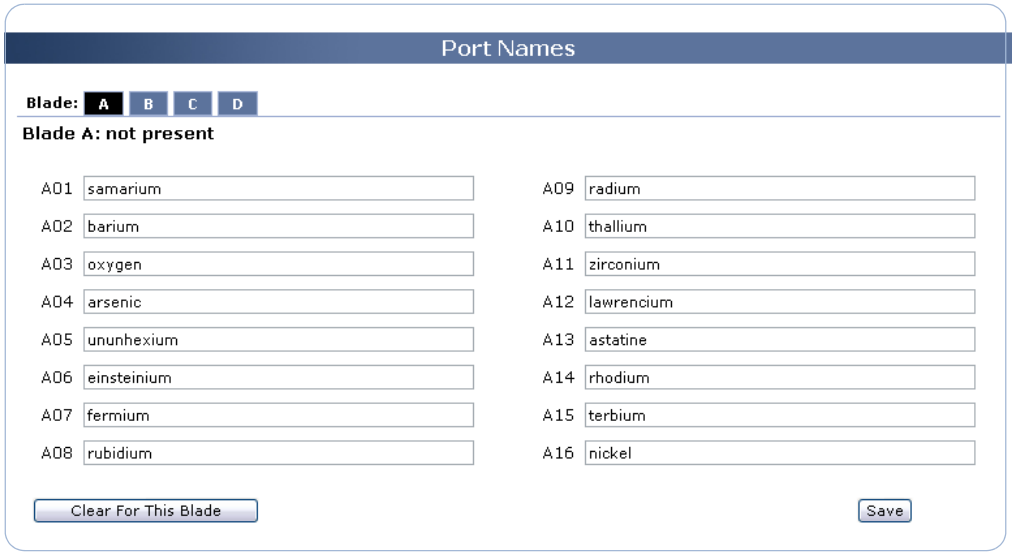
INTELLAPATCH blade labels use letters and start at the bottom. Port labels use numbers prefaced by blade letter, and start at the left. For details, see *Switch Labeling* on page 9.

To name ports, select:

**Ports/Blades>Configuration>Names**

This screen displays on the Canvas:

**Figure 22. Names screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Blade:<br>(Tabs A, B, C...) | Clicking a tab displays port names for the specified blade.<br>Tab letters match the blade numbers on your INETELLAPATCH chassis. Blade labels use letters and start at the bottom. Port labels use numbers prefaced by blade letter, and start at the left. For details, see *Switch Labeling* on page 9. |
| Port Number | Identifies the port whose name you want to change:<br>• To assign a name, type the name in the text box to the right of the port number, then click the Update button.<br>• To clear a name, delete the name in the text box to the right of the port number, then click the Update button. |

| Field | Description |
|---|---|
| Clear For This Blade button | Deletes assigned names for all ports on this blade. |
| Save button | Saves and implements your changes. |

## 6.4.2. Classes

Sets up port classes and defines the properties of each port class.

**Note**

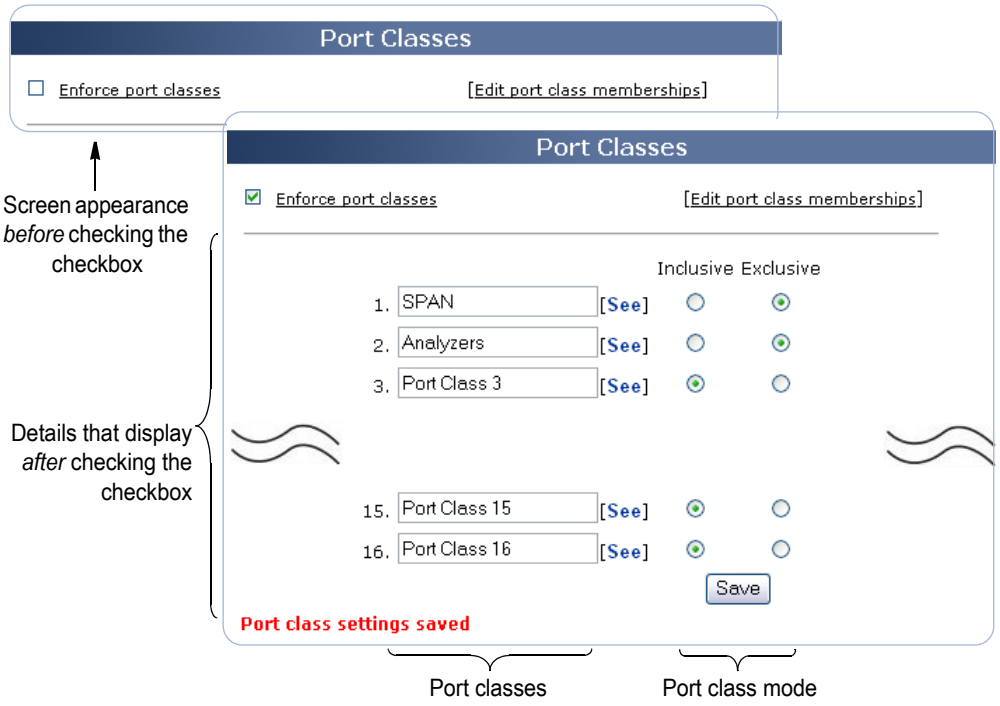
After setting up classes and assigning ports to those classes, you can quickly view and modify settings for SPAN and Analyzer ports by accessing the Monitor screen. For more information, see *Chapter 5, MONITOR*, starting on page 48.

To set up or change port classes and their properties, select:

**Ports/Blades>Configuration>Classes**

This screen displays on the Canvas:

**Figure 23. Classes screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Enforce port classes | Determines how classes are used:<br>☑ **Checked**: Enforce classes.<br>☐ **Unchecked (default)**: Do not enforce classes. |
| Edit port class memberships | Displays the port *Class Members* window. For details about this window, see page 67. |

| Field | Description |
|---|---|
| Port Class 1–16<br>—or—<br>Names you specify | A name that both creates and identifies the port class. The default name is `Port Class n`. Port class names consist of up to 31 characters and can include letters, numbers, spaces, and most keyboard characters. Port class names cannot include these characters:<br>< (Less-than symbol) " (Quote marks)<br>> (Greater-than symbol) ' (Apostrophe)<br>\ (Backslash)<br>Fields that retain the name `Port Class n` or are blank are not classes.<br>**Note**: If the first four letters of a class are `SPAN`, the INTELLAPATCH switch assumes that ports assigned to the class are SPAN ports. For details about setting up classes for SPAN ports, see *Simplex Patching with SPAN/Monitor Ports* on page 13. |
| See | Lists all ports by class. When you click this link, the window displays the class to the left of the link. You can scroll to display all ports. Use this window to quickly view all ports included in this class. |
| Port class mode | Restricts connections as follows:<br>• **Inclusive classes (default)**: Allows ports to connect only when they belong to the same class. When all port classes are inclusive, ports not assigned a port class cannot connect to any other port.<br>• **Exclusive classes**: Prevents ports of the same class from connecting. When all port classes are exclusive, ports not assigned a port class may patch to any other port. |
| Save button | Saves and implements your changes. |

## 6.4.3. Class Members

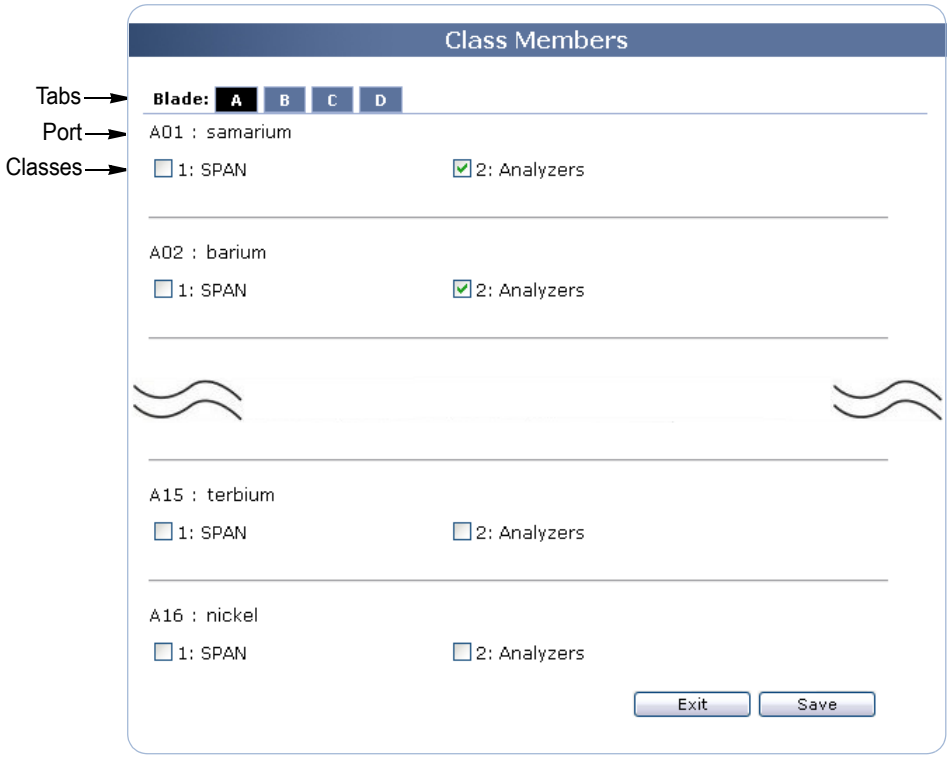
Assigns a port to a class.

To assign a port to a class, select:

**Ports/Blades>Configuration>Class Members**

This screen displays on the Canvas:

**Figure 24. Class Members window**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Blade:<br>Tabs A, B, C ...) | Clicking a tab displays the class settings for the specified blade.<br>Tab letters match the blade numbers on your INETELLAPATCH chassis. Blade labels use letters and start at the bottom. Port labels use numbers prefaced by blade letter, and start at the left. For details, see *Switch Labeling* on page 9. |
| Port | Identifies the port assignment. The port name consists of:<br>*PortNumber*:*PortName*<br>Where *PortNumber* is the number assigned to the port and *PortName* is the name you specify. If you do not specify a port name, `Unnamed` displays.<br>For information about naming ports, *Port Properties* on page 50. |

| Field | Description |
|---|---|
| Classes | Assigns the port to a class or classes. This screen displays the classes you specified on the *Classes* screen. Only the classes display; fields named `Port Class n` or are blank are not classes and therefore do not display.<br>To assign a port to a class:<br>1. Click the checkbox of the class you want to assign the port to.<br>2. Click the Save button. |
| Exit button | Exits the Class Members screen without saving changes. |
| Save button | Saves and implements your changes. |

## 6.4.4. Port Locking

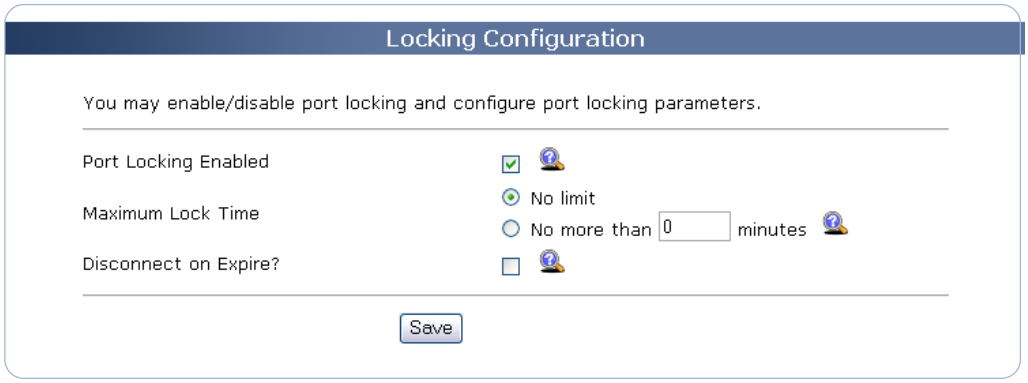
Reserves the specified port(s) for your exclusive use.

To access port locking options, select:

**Ports/Blades>Configuration>Locking**

This screen displays on the Canvas:

**Figure 25. Port Locking screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Port Locking Enabled | Specifies port locking capabilities:<br>☑ (Enabled) Allows users to lock ports.<br>☐ (Disabled) Users cannot lock ports. |
| Maximum Lock Time | Specifies the lock duration:<br>• **No Limit**: The lock remains in effect until manually cleared.<br>• **No more than *n* minutes**: The lock remains in effect for only the number of minutes specified. |
| Disconnect on Expire? | Determines port behavior when the lock period expires:<br>☑ (Checked) Locked ports disconnect.<br>☐ (Unchecked) Locked ports remain connected. |
| Help | Hovering your cursor over this icon displays Help information about the associated field. |
| Save button | Clicking this button saves and implements your changes, then displays the Port Locking screen. |

## 6.4.5. Zoning

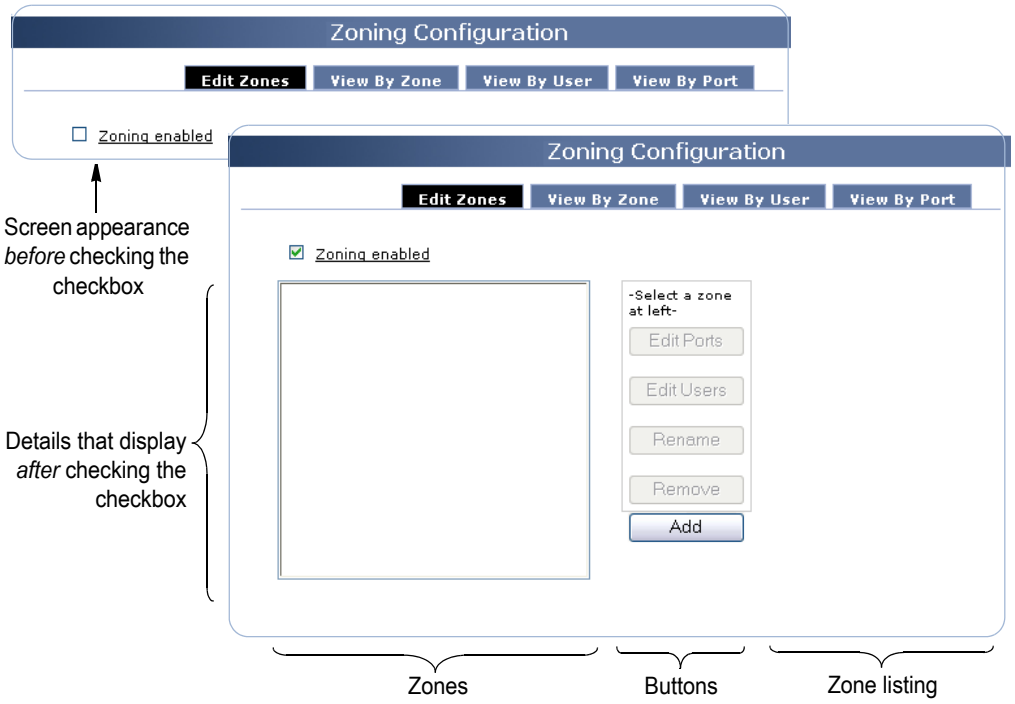
Sets up zones and defines the properties of each zone.

To access zoning options, select:

**Ports/Blades>Configuration>Zoning**

This screen displays on the Canvas:

**Figure 26. Zoning screen**




The screen includes these options:

**Note**

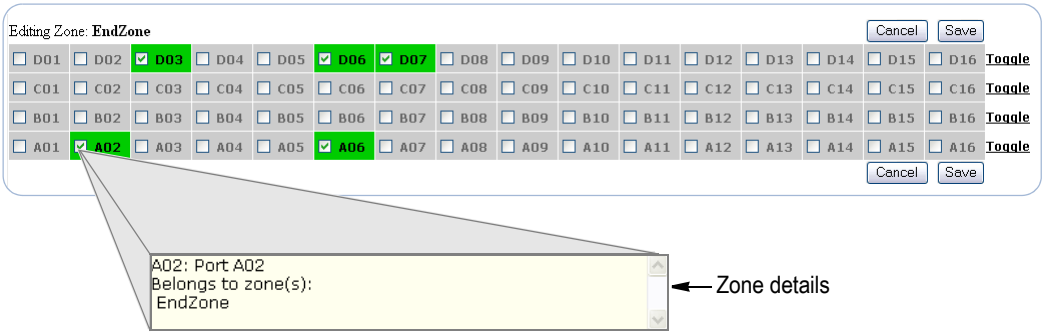
To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Zoning enabled | Determines how zones are used:<br>☐ **Unchecked (default)**: Disables zoning.<br>☑ **Checked**: Enables zoning. |
| Zones | Displays zones available on this switch. To create a zone:<br>1. Click the Add button. The Explorer User Prompt dialog box displays.<br>2. Type a zone name, then click the OK button. The *Edit Ports dialog screen* displays. For details about this screen, see *Zoning: Edit Ports Screen* on page 71.<br>3. Select the ports you want to include in this zone, then click the save button. The Zoning screen displays. |

| Field | Description |
|---|---|
| Buttons | The buttons on this screen perform the following actions:<br>• **Edit Ports**: Displays the *Edit Ports dialog screen* screen where you can add or delete ports included in this zone. For details about this screen, see *Zoning: Edit Ports Screen* on page 71.<br>• **Edit Users**: Displays the *Edit User dialog box* dialog box where you can add or delete users included in this zone. For details about this dialog box, see *Zoning: Edit User Dialog Box* on page 72.<br>• **Add**: Creates a new zone.<br>• **Rename**: Changes the name of a zone.<br>• **Remove**: Deletes a zone. |
| Zone listing | Displays the ports and users included in the specified zone. |
| Tabs | Displays zone ports in the order you specify:<br>• **View By Zone**: Displays zones in alphabetical order and indicates the ports, if any, assigned to each zone.<br>• **View By User**: Displays users in alphabetical order and indicates the zone, if any, to which each is assigned.<br>• **View By Port**: Displays ports in ascending order and indicates the zone, if any, to which each is assigned. |

### 6.4.5.1. Zoning: Edit Ports Screen

**Figure 27. Zoning: Edit Ports Screen**



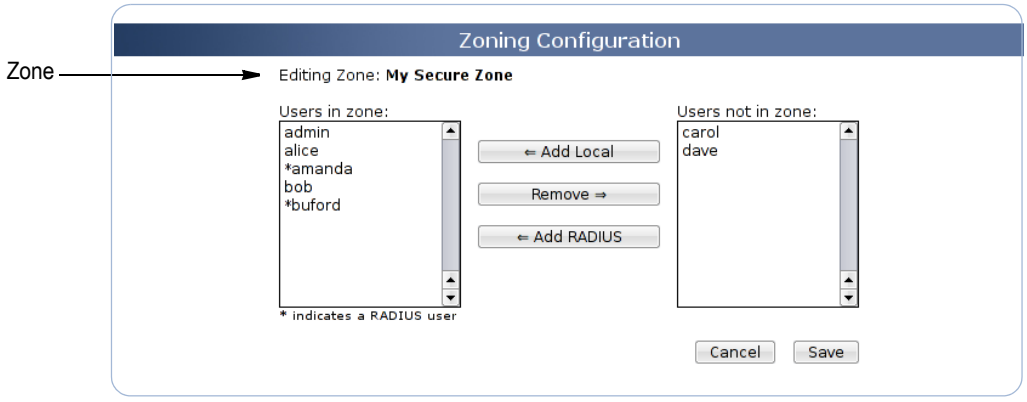

The screen includes these options:

| Field | Description |
|---|---|
| Editing Zone: | Identifies the zone and serves as the link location when adding ports to a zone. To add a port to a zone:<br>1. Select the port(s) you want to add using one of these methods:<br>• To add a port to a zone, place the cursor over the port's checkbox and click.<br>• To add a blade to a zone, click the Toggle link, located on the right side of the screen.<br>2. Click the Save button.<br>Locked ports display as green, while unlocked ports remain gray. |

| Field | Description |
|---|---|
| Zone details | Hovering your cursor over a port displays the following lock information for that port:<br>• ***Port number: Port name**:* Identifies the port assignment. *PortNumber* is the number assigned to the port and *PortName* is the name you specify. If you do not specify a port name, `Unnamed` displays.<br>For information about naming ports, *Names* on page 63.<br>• **Belongs to zone(s)**: The zone to which this port is assigned. If no name is specified a port name, `(none)` displays. |
| Toggle | Checks or unchecks all ports on the selected blade. |
| Cancel button | Exits the Edit Ports screen without saving changes. |
| Save button | Clicking this button saves and implements your changes. |

### 6.4.5.2. Zoning: Edit User Dialog Box

**Figure 28. Zoning: Edit User Dialog Box**




The dialog box includes these options:

| Field | Description |
|---|---|
| Zone | The zone you selected on the *Zoning* screen. |
| Users in zone: | Lists users assigned to the specified zone. RADIUS and TACACS+ users are identified with an asterisk.<br>To add a user to this zone:<br>1. Select user(s) in the Users not in zone list. You can click to select a single user, hold down the Alt button while clicking to add multiple users, or hold down the Shift button while clicking to add a range of users.<br>2. Click the <== Add button. The selected user names move to the Users in zone list.<br>**Note**: The `admin` user is automatically added to all zones. |

| Field | Description |
|---|---|
| Users in zone: (cont'd) | To remove a user from this zone:<br>1. Select user(s) in the Users in zone list. You can click to select a single user, hold down the Alt button while clicking to add multiple users, or hold down the Shift button while clicking to add a range of users.<br>2. Click the Remove ==> button. The selected user names move to the Users not in zone list. |
| Users not in zone: | Lists users not assigned to the specified zone. |
| <== Add button | Adds the user(s) selected from the Users not in zone list. |
| Remove ==> button | Removes the user(s) selected from the Users in zone list. |
| <== Add RADIUS button | Adds all RADIUS user(s) in the Users not in zone list. |
| Cancel button | Clicking this button exits the dialog box without saving your changes. |
| Save button | Clicking this button saves and implements your changes. |

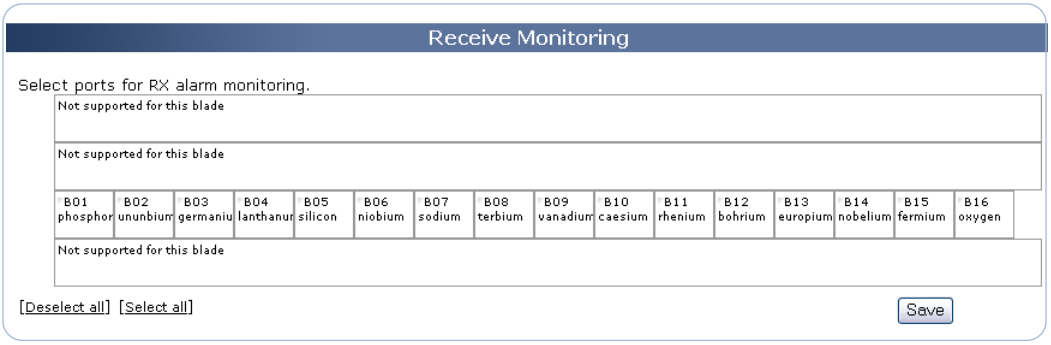
## 6.4.6. Receive Monitoring

To select ports you want to monitor for loss of signal, select:

**Ports/Blades>Configuration>Receive Monitoring**

This screen displays on the Canvas:

**Figure 29. Receive Monitoring screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Ports | Clicking a port's checkbox means that port is continuously monitored for loss of signal. Ports not selected are not monitored.<br>To view monitor results, see the Alarms screen (Ports/Blades>Configuration>Alarms>, described on page 61. |
| Deselect all | Un-selects all ports on the switch. |
| Select all | Selects all ports on the switch. |
| Save button | Clicking this button saves and implements your changes. |

## 6.4.7. Edit Presets

To set switches to a saved configuration, select:

**Connections>*Patching*>Edit Presets**

This screen displays on the Canvas:

**Figure 30. Edit Presets screen**


The screen includes these options.

**Note**

To make changes on this screen, your account must have a minimum of Advanced Operator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Save Current Patches As a Preset | Saves or changes configuration settings to the preset name or number you specify. |
| Preset | The Preset number whose configuration settings you want to save or change. You can select a name or number from 1 to 99.<br>**CAUTION**: Selecting a position that already has configuration settings assigned overwrites those settings without warning. |
| New Preset Name | A name you specify for the Preset. You can enter a name of up to 255 characters. Select names that provide meaningful aids to memory, so that you can recall later how it configures the switch, and so that others can understand its purpose. |
| Store Current button | Saves the configuration settings to the Preset position you specified. |
| Edit/Clear Preset | Clears (deletes) configuration settings for the preset name or number you specify. |
| Preset drop-down menu | The Preset number you want to change. You can select a name or number from 1 to 99. |

| Field | Description |
|---|---|
| Clear button | Clears the configuration settings of the Preset position you specified.<br>**Note**: Clearing a preset is equivalent to changing all its settings to `n/c`, or no change. |
| Edit button | Displays a screen similar to the *Realtime* patching screen where you can specify new configuration settings. For information about this screen, see page 33.<br>Unique to the Edit Presets screen are the All ports options:<br>`n/c` Instructs WEBX to leave the current patch settings unchanged when this preset configuration is invoked.<br>`off` Unpatches all ports.<br>`loopback` Patches each port to itself, except SPAN ports.<br>**Note**: SPAN ports do not change when you select any of these options. |

# Chapter 7

# View

This chapter details the screens available from the View menu:

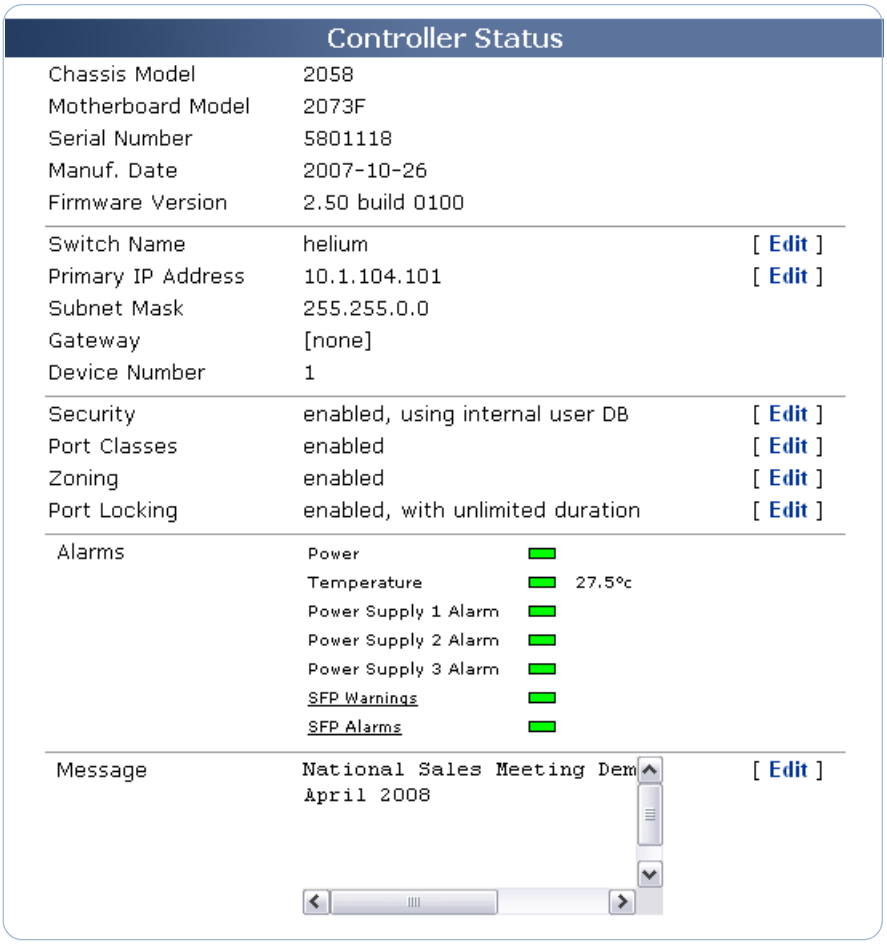
# 7.1. Controller

To see switch details such as name, model number, serial number, manufacture date, firmware version, device number, network properties, and alarm status, selecte:

**View>Chassis>Controller**

This screen displays on the Canvas:

**Figure 31. Controller screen**




The screen includes these options:

**Note**

To view this screen, your account needs only Guest permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Chassis Model | The switch's model number. This is a display-only field; you cannot change its value. |
| Motherboard Model | The switch motherboard's model number. This is a display-only field; you cannot change its value. |
| Serial Number | The switch's serial number. This is a display-only field; you cannot change its value. |

| Field | Description |
|---|---|
| Manuf. Date | The switch's manufacture date. This is a display-only field; you cannot change its value. |
| Firmware Version | The version number of firmware embedded in the switch. This is a display-only field; you cannot change its value. |
| Switch Name | The name you specify for the switch. The default is `Unnamed`.<br>Clicking the Edit link, viewable only by users with Administrator permission privileges, displays the *Properties* screen where you can change the switch name. For details about this screen, see page 133.<br>**Note**: You can also access this screen by selecting **Configuration>Switch Properties**. |
| Primary IP Address | The IP address you specify for the switch. The default is 192.168.0.1.<br>Clicking the Edit link, viewable only by users with Administrator permission privileges, displays the *LAN Interface* screen where you can change the IP address. For details about this screen, see page 129.<br>**Note**: You can also access this screen by selecting **Configuration>LAN Interface**. |
| Subnet Mask | The subnet mask address you specify for the switch. The default is 255.255.255.0. |
| Gateway | The network gateway address you specify for the switch. The default is to not use a gateway. |
| Device Number | The device number you specify for the switch. The default is 1.<br>To change the device number, go to the ASCII (Slash) device number option on the Service Properties screen. For details about this screen, see page 117. |
| Security | Indicates whether user authentication is required, and specifies the type.<br>Clicking the Edit link, viewable only by users with Administrator permission privileges, displays the *User Database* screen where you can change the IP address. For details about this screen, see page 107.<br>**Note**: You can also access this screen by selecting **Configuration>User Database**. |
| Port Classes | Indicates whether you can specify or use port classes.<br>Clicking the Edit link, viewable only by users with Administrator permission privileges, displays the *Classes* screen where you can change the IP address. For details about this screen, see page 65.<br>**Note**: You can also access this screen by selecting **Configuration>Port Classes**. |

| Field | Description |
|---|---|
| Zoning | Indicates whether you can specify or use zones.<br>Clicking the Edit link, viewable only by users with Administrator permission privileges, displays the *Zoning* screen where you can change the IP address. For details about this screen, see page 70.<br>**Note**: You can also access this screen by selecting **Configuration>Zoning**. |
| Port Locking | Indicates whether you can reserve specified ports exclusive use.<br>Clicking the Edit link, viewable only by users with Administrator permission privileges, displays the *Locks* screen where you can change the IP address. For details about this screen, see page 54.<br>**Note**: You can also access this screen by selecting **Configuration>Port Locking**. |
| Power | Indicates whether power is supplied to the switch.<br>The ACI-2058, 288-port switch, includes three power supplies. One is required to power on the motherboard. At least two must function to fully power the unit, including the blades.<br>Other switches, such as the 144- and 64-port switches, include two power supplies. Only one is required to power on the motherboard and to fully power the unit. |
| Temperature | Indicates temperature and status:<br>• **Green**: Internal temperature is within specified limits.<br>• **Flashing red**: Internal temperature exceeds the specified limit. If this occurs, the switch also emits an audible alarm, if enabled. For details, see *Properties* on page 133.<br>The default temperature's maximum threshold is 50º C. To change the default, click the Edit link, viewable only by users with Administrator permission privileges and located to the right of Switch Name, to display the *Properties* screen. For details about this screen, see page 133.<br>**Note**: You can also access this screen by selecting **Configuration>Switch Properties**. |
| Power Supply *n* Alarm | Indicates operational status of the specified power supply.<br>• **Green**: The power supply is functioning normally.<br>• **Flashing red/amber**: The power supply failed. If this occurs, the switch also emits an audible alarm if enabled. For details, see *Audible alarms enabled* on page 138. |
| SFP Warnings | Indicates operational status of SFP temperature, power, and received signal. Checks the transmit signal only if Automatic Transmitter Disable is set to `TX on when no RX`. For details about this option, see *Properties* on page 133.<br>• **Green**: The SFP is functioning within normal thresholds.<br>• **Flashing red**: One or more SFPs have exceeded the warning threshhold defined by the SFP manufacturer. To determine which SFP(s) failed, click the field label to display the *Alarms* screen. For details about this screen, see page 61. |

| Field | Description |
|---|---|
| SFP Alarms | Indicates operational status of SFP temperature, power, and received signal. Checks the transmit signal only if Automatic Transmitter Disable is set to `TX on when no RX`. For details about this option, see *Properties* on page 133.<br>• **Green**: The SFP is functioning within normal thresholds.<br>• **Flashing red**: One or more SFPs have exceeded the alarm threshhold defined by the SFP manufacturer. If this occurs, the switch also emits an audible alarm. To determine which SFP(s) and what alarm s encountered problems, click the field label to display the *Alarms* screen. For details about this screen, see page 61. |
| Message | The system message, a message supplied by the administrator.<br>Clicking the Edit link, viewable only by users with Administrator permission privileges and located to the right of Switch Name, displays the *Login Message* screen where you can change the system message. For details about this screen, see page 140.<br>**Note**: You can also access this screen by selecting **Data>Message**. |

# 7.2. Event Log

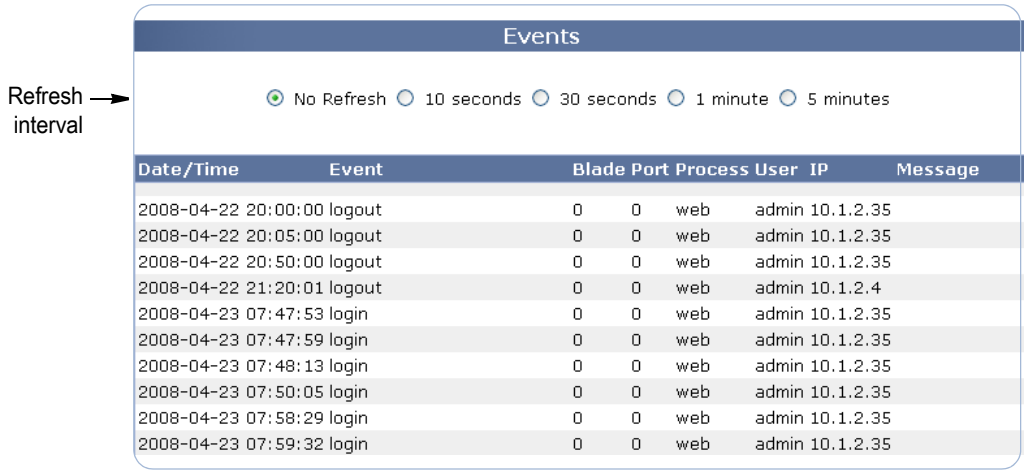
Displays the 500 most recent system events that occurred since the most recent boot. This log mirrors the *remote syslog*, described on page 120.

To view system events, select:

**View>Chassis>Event Log**

This screen displays on the Canvas:

**Figure 32. Events screen**




The screen includes these options:

**Note**

To view this screen, your account needs only Guest permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Refresh interval | Specifies the amount of time that elapses before WEBX refreshes the data. Valid values include<br>• **No refresh (default)**: WEBX does not refresh the data.<br>• **10 seconds**: Data automatically refreshes every ten seconds.<br>• **30 seconds**: Data automatically refreshes every thirty seconds.<br>• **1 minute**: Data automatically refreshes every minute.<br>• **5 minutes**: Data automatically refreshes every five minutes. |
| Date/Time | Displays the date and time the event occurred. |
| Event | Lists the event type. |
| Blade | Displays the letter of the blade on which the event occurred. If 0 (zero) displays, a blade was not involved in the event. |
| Port | Displays the number of the port on which the event occurred. If 0 (zero) displays, no port was involved in the event. |
| Process | Lists the program that caused the event to occur. |
| User | Displays the login name of the user associated with the event. Includes an IP address only if the User is at a different address than the process. |

| Field | Description |
|---|---|
| IP | Lists the IP address, in standard TCP/IP #.#.#.# format, where the process that caused the event runs. 127.0.0.1 indicates that the process was running within the APCON switch. For example, accessing APCONCMDX via Telnet versus the APCONCMDX application running on a workstation. |
| Message | Displays additional information about the event. |

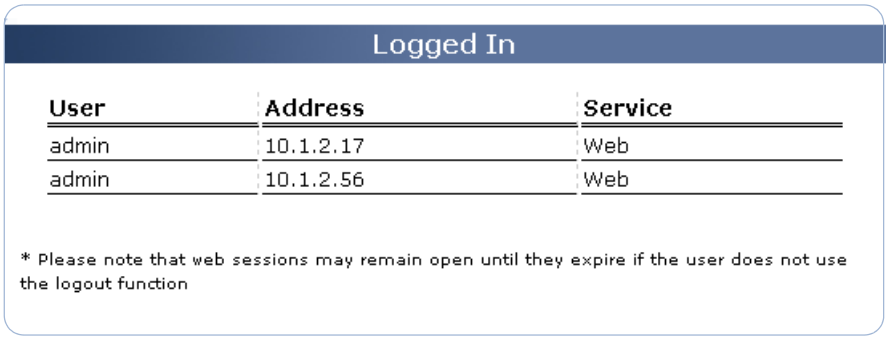
# 7.3. Logged In

To view users currently logged in to the switch, select:

**View>Chassis>Logged In**

This screen displays on the Canvas:

**Figure 33. Logged In screen**




The screen includes these options:

**Note**

To view this screen, your account needs only Guest permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| User | The user's login name. |
| Address | The IP address from which the user logged in. |
| Service | The interface from which the user logged in. For example, Web or CLI (including telnet and SSH). |

# 7.4. Display Options

## 7.4.1. Show Toolbar

To toggle the toolbar display, select:

**View>Chassis>Show Toolbar**

You can choose one of these:

- ☑ **Checked (default)**: The Toolbar displays.
- ☐ **Unchecked**: The Toolbar does not display.

For more information about the WEBX toolbar, see *Toolbar* on page 6.

## 7.4.2. Toolbar Text Labels

To display menu option labels, select:

**View>Chassis>Toolbar Text Labels**

You can choose one of these:

- ☑ **Checked (default)**: Menu labels display.
- ☐ **Unchecked**: Menu labels do not display.

For more information about WEBX menus, see *Menus* on page 7.

# Chapter 8

# Tools

This chapter details the screens available from the Tools menu:

# 8.1. Cable Test

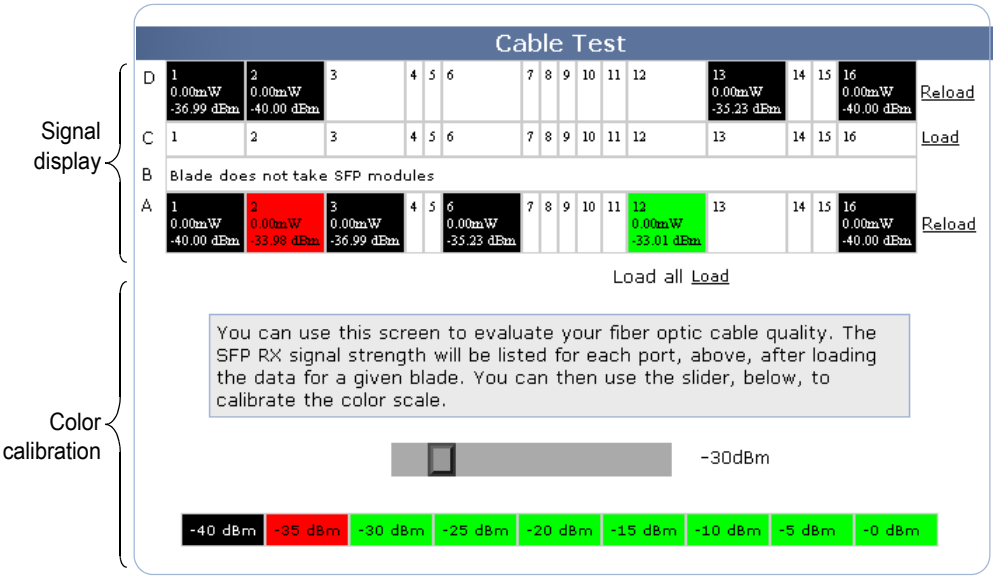
Displays signal strength, in dBm and by color. You can use this screen to monitor cable health.

To view or calibrate signal strength, select:

**Tools>Diagnostics>Cable Test**

This screen displays on the Canvas:

**Figure 34. Cable Test screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Signal display | Displays the SFP's RX signal strength in dBm and by color, rounded to the nearest 0.05 mW, for each port on the INTELLAPATCH switch.<br>Signal information does not display for the following:<br>• Transceivers that do not support signal display.<br>• Ports that do not have SFP modules installed.<br>• Blades that do not support SFP modules. |
| Load/Reload links | Selectively loads and updates signal data on a per-blade basis. Select this option to quickly access signal data. |
| Load All link | Loads and updates signal data for all blades on the switch. Select this option when you need to see the data for all blades and time is not an issue. |

| Field | Description |
|---|---|
| Color calibration | Specifies the color that displays for various signal strengths.<br>Set the slider to the minimum signal strength required for transmission. Check your transceiver manufacturer specifications for acceptable signal strengths.<br>After you set the slider, signals display as follows:<br>• **Green**: The transceiver is receiving enough signal to properly transmit.<br>• **Red gradient**: The transceiver is not receving enough signal to properly transmit. The darker the color, the lower the signal.<br>• **Black**: The transceiver either does not receive signal or no transceiver exists. |

# 8.2. Flapping

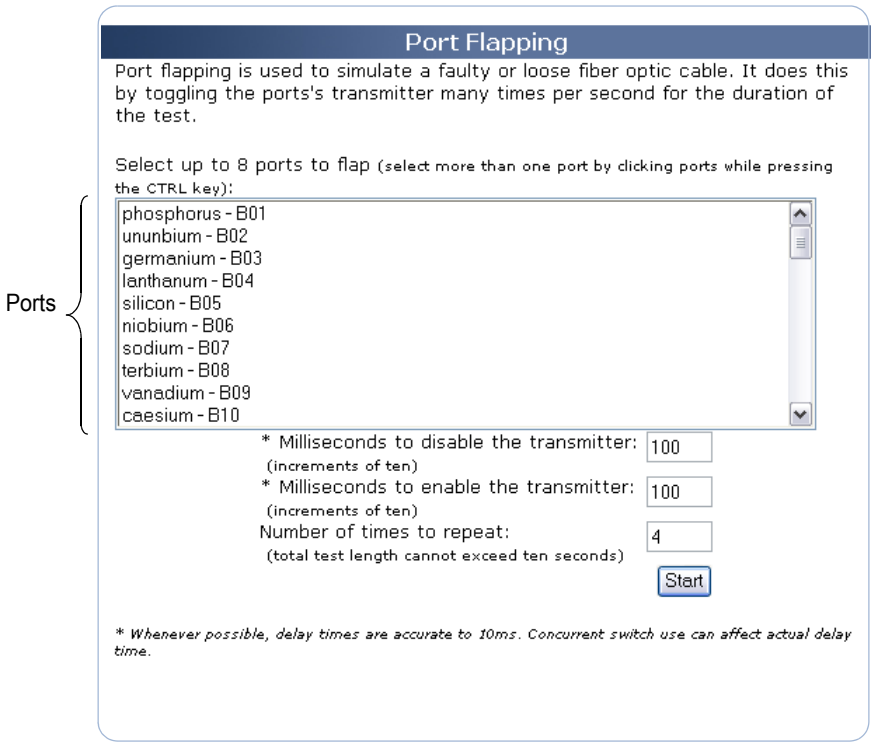
Specifies the ports whose signal you want to toggle to test for faulty or loose cable connections.

To set up ports for signal flapping, select:

**Tools>Diagnostics>Flapping**

This screen displays on the Canvas:

**Figure 35. Flapping screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Ports | Specifies the ports you want to test using port flapping. Locking and zoning permissions apply. |
| Milliseconds to disable the transmitter: | The duration, in milliseconds, the transmitter is disabled. The default is 100. |
| Milliseconds to enable the transmitter: | The duration, in milliseconds, the transmitter is enabled. The default is 100. |

| Field | Description |
|---|---|
| Number of times to repeat: | The number of times the disable/enable cycle repeats. The default is x.<br>**Note**: The duration of the total test period cannot exceed 10 seconds. |
| Start button | Pressing the Start button saves your test settings and starts the test. |

# 8.3. Signal Counters

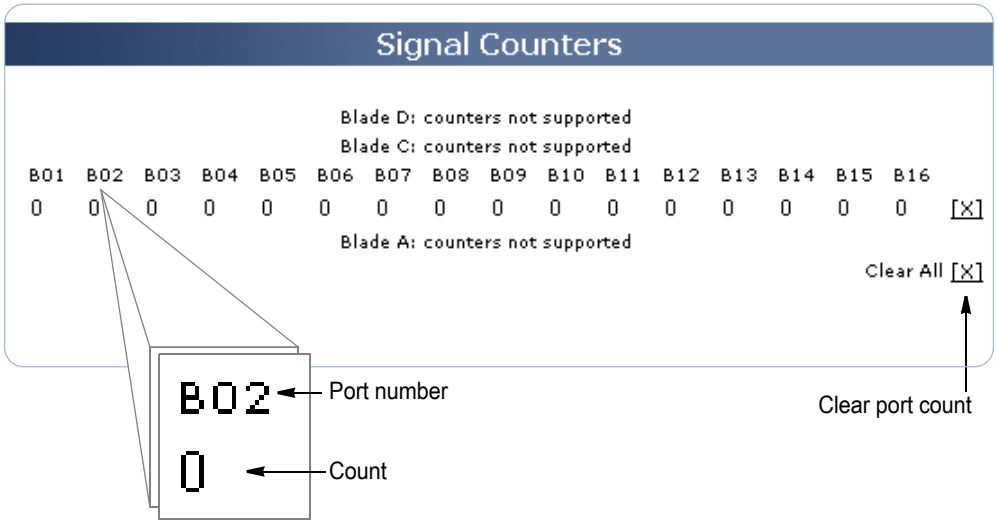
Counts how many times the port's signal starts and stops. WEBX updates the count every five seconds, displaying a `Loading...` message in the upper left corner during updates. Use this screen to troubleshoot cable integrity.

To count signal transitions, select:

**Tools>Diagnostics>Signal Counters**

This screen displays on the Canvas:

**Figure 36. Signal Counters screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Port number | Identifies the port whose transitions you want to count. |
| Count | Displays the number of times signal has transitioned from on to off or from off to on. The counter can record up to 16 million transitions. |
| Clear port count | Resets the counter to 0 (zero) and restarts the count. |
| Clear All | Resets all counters to 0 (zero) and restarts the count. |

# Chapter 9

# Maintenance

This chapter details the screens available from the Maintenance menu:

# 9.1. Backup/Restore

## 9.1.1. Backup Settings

Exports switch configuration settings for use in another switch.

Once you export data, you can modify file content, provided you leave the formatting intact. For information about this format, see *Import/Export Settings File Format* on page 146. You should use only a text editor or scripts to make changes. A word processor adds additional formatting which renders XML files invalid for importing.

**Note**

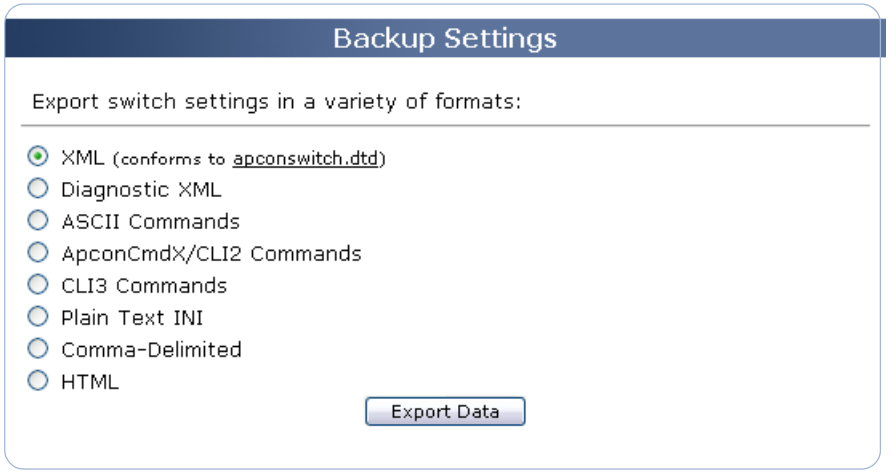
To import configuration settings, see *Restore Settings* on page 97.

To export switch configuration data, select:

**Maintenance>Backup/Restore>Backup Settings**

This screen displays on the Canvas:

**Figure 37. Export screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| XML (conforms to apconswitch.dtd) | Instructs the switch to export the specified data in XML format. For information about this format, see *Import/Export File Formats* on page 147.<br>**Note**: If you plan to import this data to an INTELLAPATCH switch, you must select this option. INTELLAPATCH switches accept imported configuration data only in XML format. |
| Diagnostic XML | Instructs the switch to export the specified data in Diagnostic XML format. For information about this format, see *Import/Export File Formats* on page 147.<br>Diagnostic XML is the same as XML, but includes SFP digital diagnostic information, such as SFP serial and model number, in the export. You can use this additional information to take inventory of the SFPs in your INTELLAPATCH switch, and when contacting APCON Technical Support.<br>**Notes**:<br>• Because this format takes significantly longer to export on large switches with a great number of SFPs, use regular XML unless you specifically need the digital diagnostic information.<br>• The extra fields in the Diagnostic XML format do not affect the import. You can import settings with either a regular XML file or a Diagnostic XML file; the extra diagnostic fields are simply ignored. |
| ASCII Commands | Instructs the switch to export the specified data in plain text (ASCII) format. For information about this format, see *Import/Export File Formats* on page 147.<br>These commands can then be used directly in any custom scripts that use the APCON Firmware Direct command set, also known as ASCII. |
| APCONCMDX / CLI2 Commands | Instructs the switch to export the specified data in APCONCMDX format. For information about this format, see *Import/Export File Formats* on page 147.<br>Once exported to APCONCMDX format, you can use the command strings from within the telnet or SSH CLI or the APCONCMDX command line utility.<br>**Note**: Use the exported file as a template when developing your own scripts. Running the exported file without scrutiny may alter settings, such as network your IP address, that may cause your connection to drop. |
| CLI3 Commands | Instructs the switch to export the specified data in APCON CLI3 format. For information about this format, see *Import/Export File Formats* on page 147.<br>Once exported to APCON CLI3 format, you can use the command strings from within the telnet or SSH CLI or the APCON CLI3 command line utility.<br>**Note**: Use the exported file as a template when developing your own scripts. Running the exported file without scrutiny may alter settings, such as network your IP address, that may cause your connection to drop. |

| Field | Description |
|---|---|
| Plain Text INI | Instructs the switch to export the specified data in plain text INI (Legacy ApconControl) format. For information about this format, see *Import/Export File Formats* on page 147.<br>This format follows the popular Windows style for configuration files. This format is easier to review, but harder to use in a scripting environment. |
| Comma-Delimited | Instructs the switch to export the specified data in a comma-delimited, spreadsheet-style format. For information about this format, see *Import/Export File Formats* on page 147. |
| HTML | Instructs the switch to export the specified data in HTML table format. For information about this format, see *Import/Export File Formats* on page 147. |
| Export Data button | Implements the instructions. The switch writes the specified data in the selected format to an output file or directly to the screen where it can be saved or copied for pasting. You are prompted to supply a filename and destination folder or directory into which to write the file. |

## 9.1.2. Backup Users

To export the user database, select:

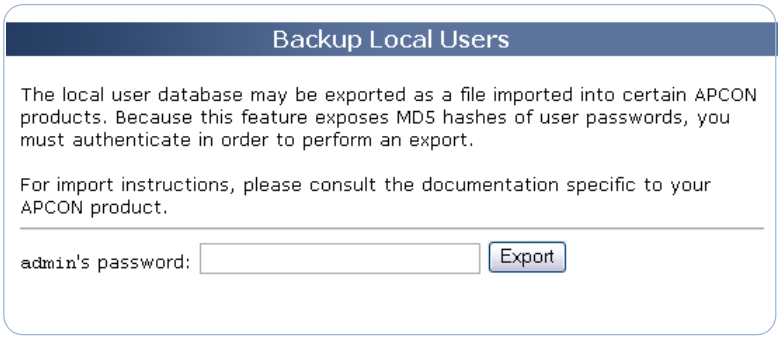
**Maintenance>Backup/Restore>Backup Users**

**Note**

Before *importing* user data, contact APCON as described in *Contacting APCON* on page 4 or on the Help>About menu option.

This screen displays on the Canvas:

**Figure 38. Backup Users screen**




The screen includes these options:

**Note**

To view this screen, your account needs only Guest permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| *user* password | Specifies the password for the currently logged in user. Unless the *User Database* (see page 107) is set to None, you must provide a valid password. |
| Export button | Prompts you for a destination, then exports the user database to that destination. |

## 9.1.3. Restore Settings

Imports part or all of another switch's configuration settings for use in your switch. Importing switch settings quickly configures a switch in a manner the same as, or similar to, another.

**Note**

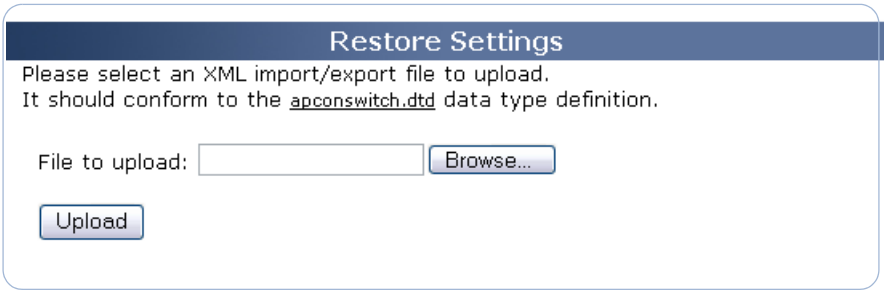
To export configuration settings, see *Backup Settings* on page 93.

To import switch configuration data, select:

**Maintenance>Backup/Restore>Restore Settings**

This screen displays on the Canvas:

**Figure 39. Restore Settings screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| File to upload: | Specifies the switch configuration file you want to upload.<br>You can do one of these:<br>• Enter the update file's full directory path and filename.<br>• Click the Browse button to navigate to and select the file.<br>**Note**: Ensure that the file you plan to import is in XML format and was previously exported using APCON WEBX or, if manually created, the file strictly adheres to XML syntax. INTELLAPATCH switches accept imported configuration data only in XML format. For information about file format, see *Import/Export File Formats* on page 147. |
| Upload button | Clicking this button copies the specified file to the switch. |

# 9.2. Switch

## 9.2.1. License Key

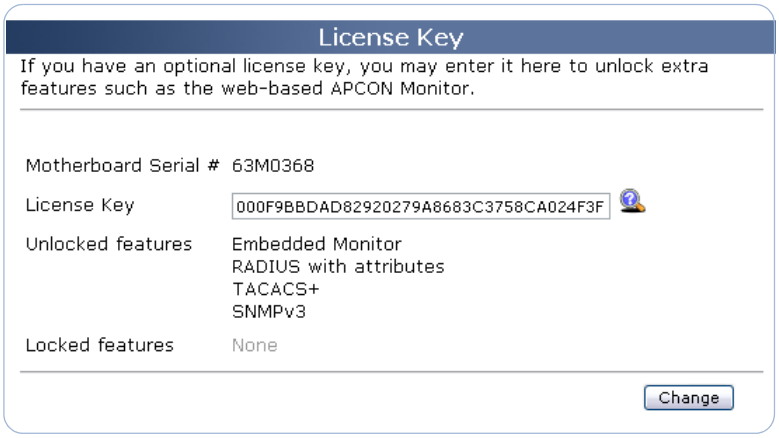
Activates additional features available from APCON. For details about available features, contact your APCON sales representative as described in *Contacting APCON* on page 4 or on the Help>Support menu option.

To configure features, select:

**Maintenance>Switch>License Key**

This screen displays on the Canvas:

**Figure 40. License Key screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Motherboard Serial # | The serial number of the INTELLAPATCH chassis. This is a display-only field; you cannot change its value. |
| Unlocked features | Lists currently unlocked features. This is a display-only field; you cannot change its value. |
| Locked features | Lists locked features. This is a display-only field; you cannot change its value.<br>For information about accessing locked features, contact APCON as described in *Contacting APCON* on page 4 or on the Help>Support menu option. |
| Change button | Saves and implements the changes you specified. |

## 9.2.2. Reset

For troubleshooting or other purposes, you can use the options on this screen to:

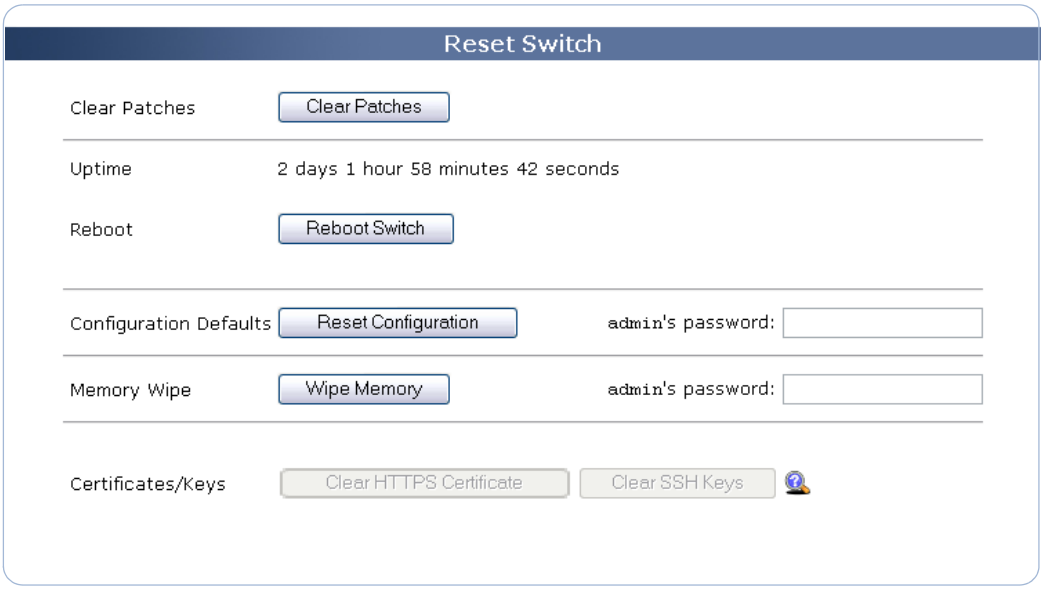
- Reset the switch to its factory default configuration.
- Reboot the switch.

To access reset options, select:

**Maintenance>Switch>Reset**

This screen displays on the Canvas:

**Figure 41. Reset screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Clear Patches | Disconnects all ports (unpatches all connections). |
| Uptime | Displays the elapsed time, in days, hours, minutes, and seconds, since the last boot. |
| Reboot Switch button | Clicking this button reboots the switch without cycling power. Port names, patches, and other details of the current configuration remain unchanged.<br>APCON recommends that you avoid rebooting a switch. Reboot only after firmware updates or if you experience software or connectivity issues.<br>**WARNING**: Rebooting the switch disconnects all patch ports until the switch fully reboots. |

| Field | Description |
|---|---|
| Reset Configuration button | Clicking this button resets the switch to the factory default configuration.<br>You must enter the password for the currently logged in user. Unless the *User Database* (see page 107) is set to `None`, you must provide a valid password.<br>**Note**: The switch's IP address and and system message remain unchanged. |
| Wipe Memory button | Clicking this button wipes (deletes) everything, including the IP address and internal user database.<br>You must enter the password for the currently logged in user. Unless the *User Database* (see page 107) is set to `None`, you must provide a valid password.<br>Customers in high-security environments may find this useful before passing the APCON switch (or the motherboard) to another department or to the factory (e.g. for an RMA return, trade, or upgrade.) |
| Clear HTTPS Certificate button | Clicking this button deletes the SSL certificate required for secure (HTTPS) logins. For information about creating this certificate, see *Certificates* on page 125. |
| Clear SSH Keys button | Clicking this button deletes the SSH key required for secure command line communication. For information about creating this certificate, see *Certificates* on page 125. |

## 9.2.3. Upgrade Firmware

Activates the service necessary to update switch firmware, and uploads the new firmware file to complete the update.

To update the switch's firmware, select:

**⚠ CAUTION**

Before updating firmware, make a backup copy of your current firmware. Most firmware updates preserve user-settable parameters such as IP address and patch configurations, but firmware updates can sometimes overwrite some of these.

**Maintenance>Switch>Upgrade Firmware**

This screen displays on the Canvas:

**Figure 42. Update Firmware screen**


The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Upload service | Does the following:<br>• Displays firmware upload status, either running or not running.<br>• Toggles the service between a running and not-running state. To change the state, click the underlined link. |
| File | Specifies the file you want to upload.<br>You can do one of these:<br>• Enter the update file's full directory path and filename.<br>• Click the Browse button to navigate to and select the file. |
| Upload button | Clicking this button copies the specified file to the switch.<br>**Note**: Uploading and processing new firmware can take several minutes. Check the browser's progress bar at the bottom of the screen to check update progress. |

After the firmware successfully updates, a message similar to this displays:

```
Upload accepted. About to process file...
File size is 3976389
Running system command: /apcon/flashinstaller '/tmp/upload.dat' 2
Verifying integrity of file
Found control block data
File looks okay
Tagging factory firmware as bootable (transaction start)
Writing kernel data
Erasing device /dev/mtd/1
Writing 653936 bytes to /dev/mtd/1
10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Verifying data was written successfully
Verify completed successfully
Writing root filesystem data
Erasing device /dev/mtd/2
Writing 3322197 bytes to /dev/mtd/2
10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Verifying data was written successfully
Verify completed successfully
Tagging new firmware as bootable (transaction complete)
Program complete, returning code 0
NOTE: You must now reboot the switch
EOF from child process
```

If you supplied an inappropriate or corrupted firmware file or if the upgrade does not succeed for other reasons, a message similar to this displays:

```
Upload accepted. About to process file...
File size is 815473
Running system command: /apcon/flashinstaller '/tmp/upload.dat' 2
Verifying integrity of file
Bad control block (ApconROM not found)
EOF from child process
```

# Chapter 10

# Settings

This chapter details the screens available from the Settings menu:

# 10.1. Personalization

## 10.1.1. Your Password

**Note**

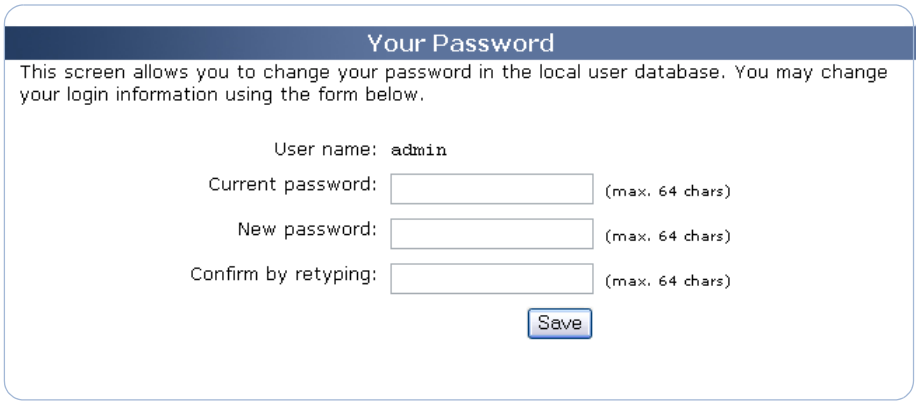
This screen is available only if User Database is set to Internal. For details about User Database options, see *User Database* on page 107.

To change your password, select:

**Settings>Personalization>Your Password**

This screen displays on the Canvas:

**Figure 43. Your Password screen**




The screen includes these options:

**Note**

Accounts at all permission privilege levels can access this screen. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| User name | Displays the name you used at login. This is a display-only field; you cannot change its value. |
| Current password | The password you want to change. |
| New password | A password comprised of up to 64 characters. Passwords are case sensitive. |
| Confirm by retyping | The same password typed in the New password field. The switch ensures that the passwords match before accepting the change. |
| Save button | Clicking this button saves and implements your changes. |

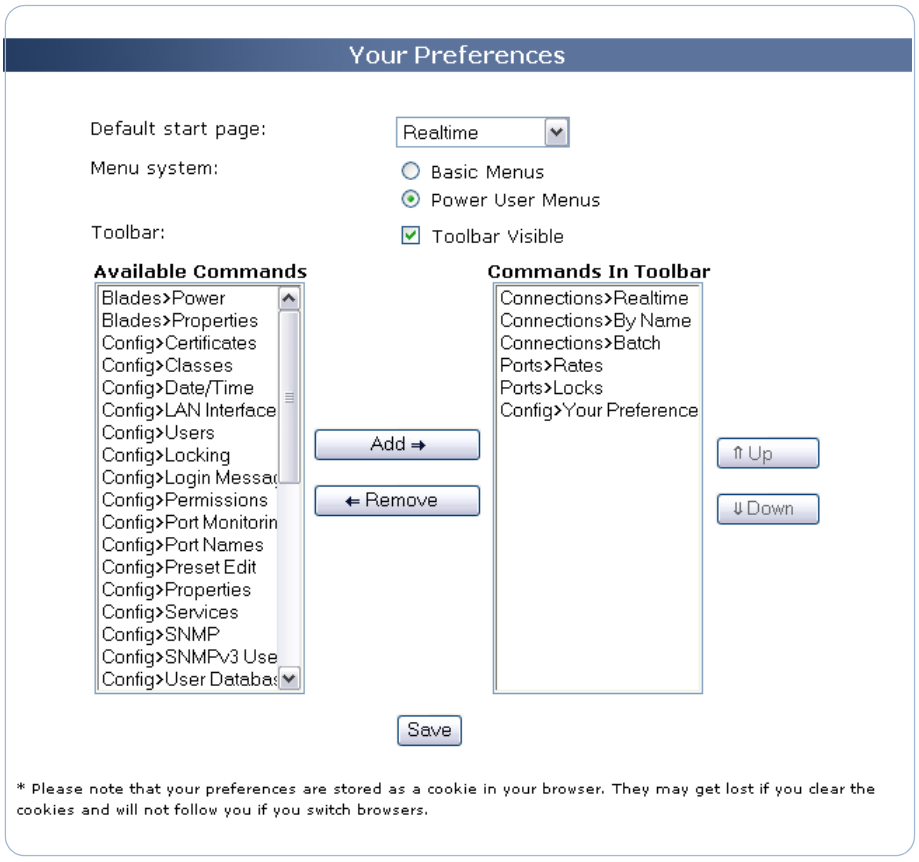
## 10.1.2. Your Preferences

To change your preferences, select:

**Settings>Personalization>Your Preferences**

This screen displays on the Canvas:

**Figure 44. Your Preferences screen**




The screen includes these options:

**Note**

Accounts at all permission privilege levels can access this screen. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Default start page: | Specifies the first screen that displays when you log in to WEBX. |
| Menu system: | Specifies the menus you want to use:<br>• **Basic**:Displays available options with icons.<br>• **Power user**: Displays available options in a pull-down menu.<br>For details about the menus, see *Menus* on page 7. |

| Field | Description |
|---|---|
| Toolbar: | Determines whether the Toolbar displays:<br>☑ **Checked (default)**: The toolbar displays.<br>☐ **Unchecked**: The toolbar does not display.<br>For more information about the WEBX toolbar, see *Toolbar* on page 6. |
| Available Commands | Lists all commands available to include in the toolbar. To select a command, highlight it, then click the Add => button. |
| Commands in Toolbar | Lists all commands you selected for inclusion in the toolbar. You can put up to ten commands in this toolbar.<br>To remove a command, highlight it, then click the <= Remove button. To change the display order, highlight a command, then click the Up or Down buttons to move the command to the location you desire. |
| Save button | Clicking this button saves and implements your changes. |

# 10.2. Users/Security

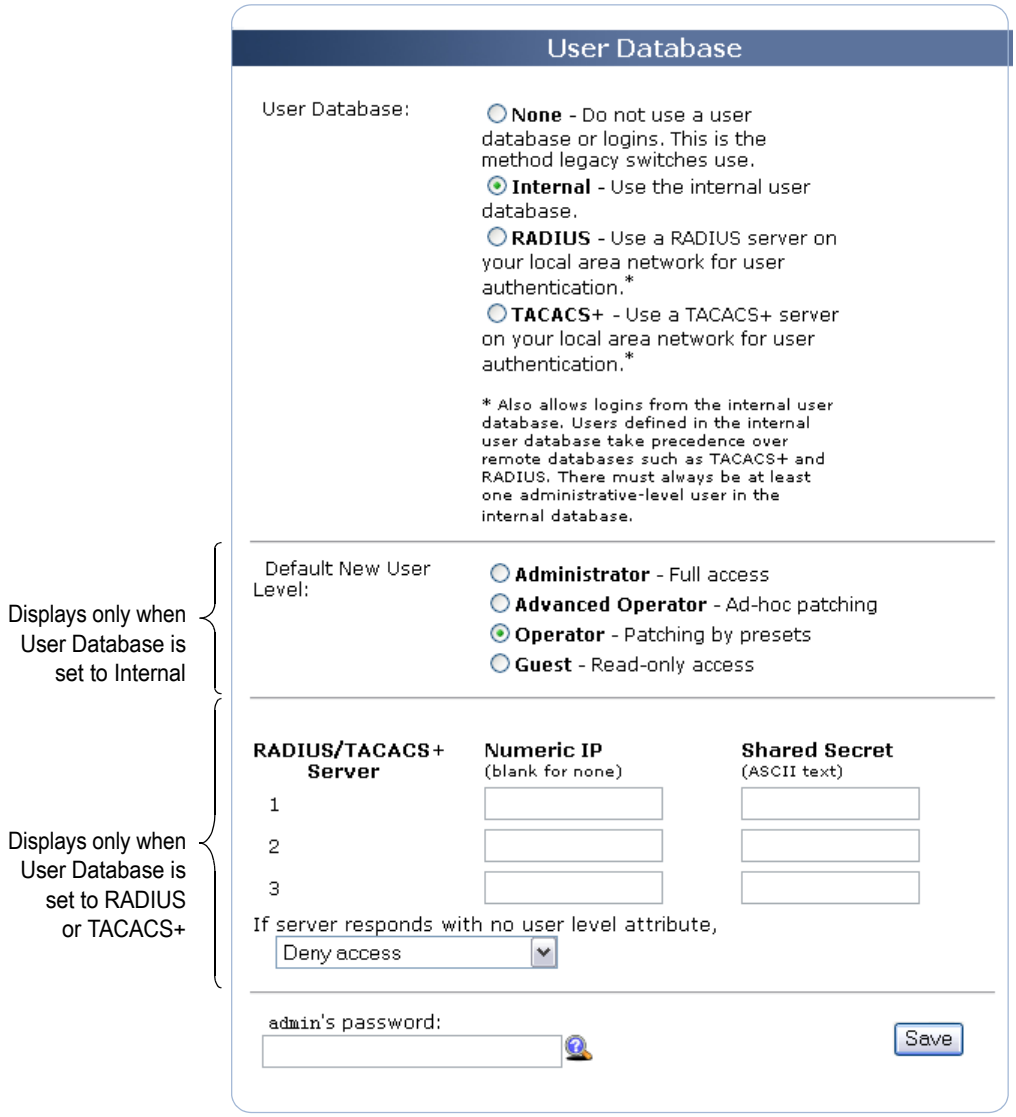
## 10.2.1. User Database

To manage the user database, select:

**Settings>Users/Security>User Database**

This screen displays on the Canvas:

**Figure 45. User Database screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| User Database | Specifies which user database to use:<br>• **None**: (Default) Does not use a user database or logins. Legacy switches use this method.<br>• **Internal**: Uses the internal user database.<br>• **RADIUS**: Uses a RADIUS server on your local area network for user authentication.<br>• **TACACS+**: Uses a TACACS+ server on your local area network for user authentication.<br>**Note**: If your RADIUS or TACACS+ server goes down, you can still access the switch through the `admin` account, which acts as a local administrator. For more information, see *User Database Concepts* on page 11. |
| Default New User Level | Specifies the default permission, or access level, for new user accounts:<br>• **Guest**: Users with this permission level have read-only access. This is the lowest permission level.<br>• **Operator**: Users with this permission level can do all that Guest-level users can do, plus patch ports using only preset configurations.<br>• **Advanced Operator**: Users with this permission level can do all that Operator-level users can do, plus patch ports on an ad-hoc basis, change rates and port names, plus save configuration settings (“presets”).<br>• **Administrator**: Users with this permission level do everything that the other levels do, plus set switch, blade, port, and other information as well as set and clear user and security information. This is the highest permission level.<br>These options are available only if User Database is set to Internal, RADIUS, or TACACS+. |
| Numeric IP (blank for none): | Specifies the IP address for the specified RADIUS or TACACS+ server on your local area network that contains the user database.<br>**Notes**:<br>• INTELLAPATCH switches support up to three RADIUS or TACACS+ servers. For details, see *User Database Concepts* on page 11.<br>• This option displays only if User Database is set to RADIUS or TACACS+. |
| Shared secret (ASCII text) | Specifies the password or phrase shared between the switch and the specified RADIUS or TACACS+ server. This value must match the value set for the INTELLAPATCH switch on your RADIUS or TACACS+ server.<br>**Notes**:<br>• INTELLAPATCH switches support up to three RADIUS or TACACS+ servers. For details, see *User Database Concepts* on page 11.<br>• This option displays only if User Database is set to RADIUS or TACACS+. |

| Field | Description |
|---|---|
| *user*'s password | Confirms the password of the currently logged in user. Unless the *User Database* (see page 107) is set to None, you must provide a valid password. |
| Save button | Saves and implements your changes. |

## 10.2.2. Local Users

To manage user accounts, select:

**Settings>Users/Security>Local Users**

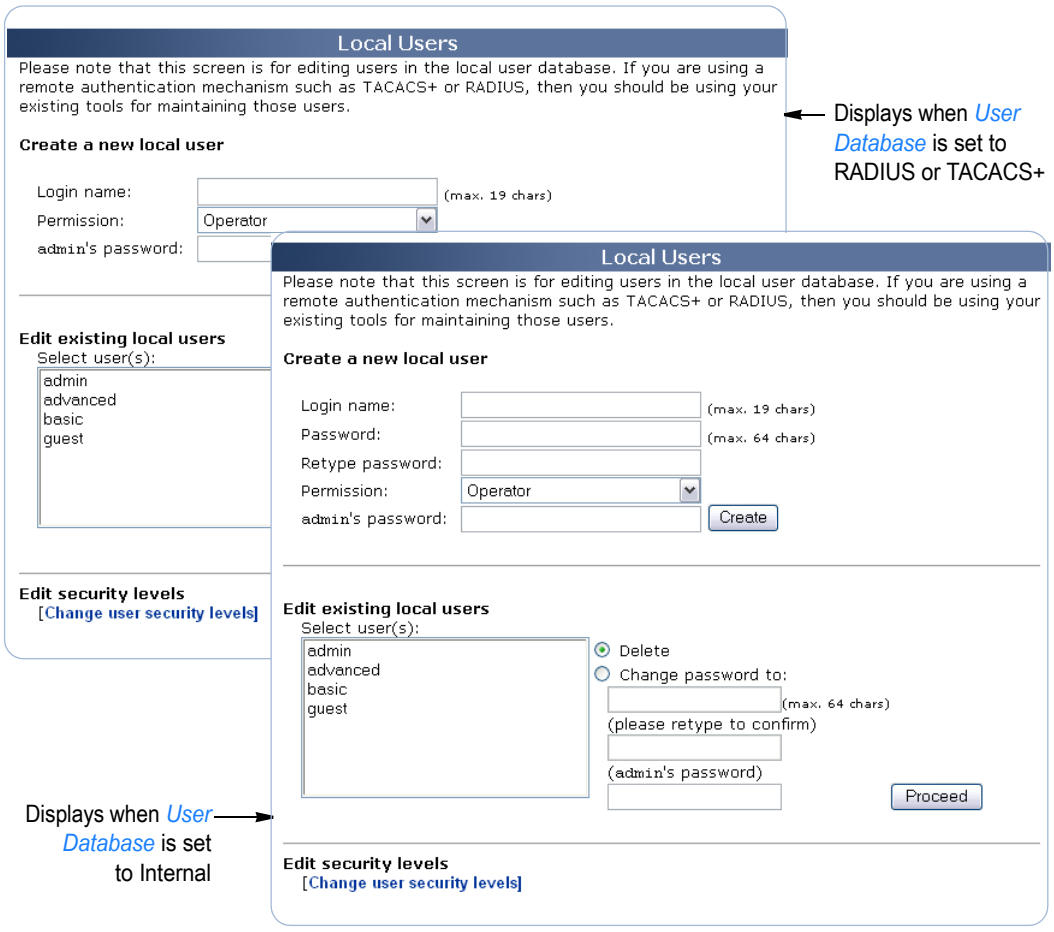
You can also access this pane by selecting **Configuration>User Levels**, then clicking the **User Management** option.

**Note**

This screen is available only if User Database is set to RADIUS, TACACS+, or Internal. For details about specifying a user database, see *User Database* on page 107.

One of these screens display on the Canvas:

**Figure 46. Local Users screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Login name | Specifies the new account name. Account names are not case-sensitive. Account names can include underscores or hyphens, but cannot include spaces or special characters. |
| Password | Specifies the password required for the user of this account to log in. A password can consist of up to 64 characters, and can include any keyboard character, including special characters. Passwords are case sensitive.<br>This option displays only if *User Database* is set to Internal. |
| Retype password: | Type the password again in this box for confirmation. The switch ensures that the passwords match before accepting the password.<br>This option displays only if *User Database* is set to Internal. |
| Permission | Specifies the permission, or access level, for each user:<br>• **Guest**: Users with this permission level have read-only access. This is the lowest permission level.<br>• **Operator**: Users with this permission level can do all that Guest-level users can do, plus patch ports using only preset configurations.<br>• **Advanced Operator**: Users with this permission level can do all that Basic Operator-level users can do, plus patch ports on an ad-hoc basis, change rates and port names, plus save configuration settings (“presets”).<br>• **Administrator**: Users with this permission level do everything that the other levels do, plus set switch, blade, port, and other information as well as set and clear user and security information. This is the highest permission level. |
| *user*’s password | Specifies the password for the currently logged in user. Unless the *User Database* (see page 107) is set to `None`, you must provide a valid password. |
| Create button | Creates a new user with the login name and permission level you specified. |
| Edit existing users | Specifies, by Login name, the user you whose account profile you want to change. You can either change the password or delete the account.<br>Clicking the Proceed button to the right of this text box saves your changes. |
| Edit Security Levels [Change user security levels] | Displays the User Levels screen where you can quickly change the permission level of one or many users. For more information about this screen, see *Permissions* on page 112. |

## 10.2.3. Permissions

**Note**

These permissions are only for Internal users. If using RADIUS or TACACS+, you must set permissions in your Authentication server. For information about user types, see *User Database* on page 107.

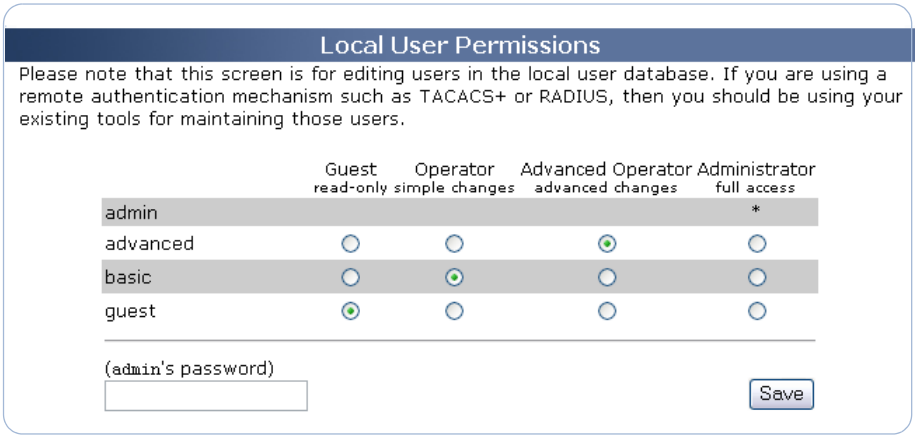
To manage user accounts, select:

**Settings>Users/Security>Persmissions**

You can also access this pane by selecting **Configuration>User Management**, then clicking the **change user security levels** option.

This screen displays on the Canvas:

**Figure 47. Permissions screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see the next table.

| Field | Description |
|---|---|
| Login name | Identifies the user by Login name. This is a display only field; you cannot change its value. |
| Permission level | Specifies the permission, or access level, for each user:<br>• **Guest**: Users with this permission level have read-only access. This is the lowest permission level.<br>• **Operator**: Users with this permission level can do all that Guest-level users can do, plus patch ports using only preset configurations.<br>• **Advanced Operator**: Users with this permission level can do all that Basic Operator-level users can do, plus patch ports on an ad-hoc basis, change rates and port names, plus save configuration settings ("presets").<br>• **Administrator**: Users with this permission level do everything that the other levels do, plus set switch, blade, port, and other information as well as set and clear user and security information. This is the highest permission level. |
| *user*'s password | Specifies the password for the currently logged in user. Unless the *User Database* (see page 107) is set to `None`, you must provide a valid password. |
| Save button | Saves and implements your changes. |

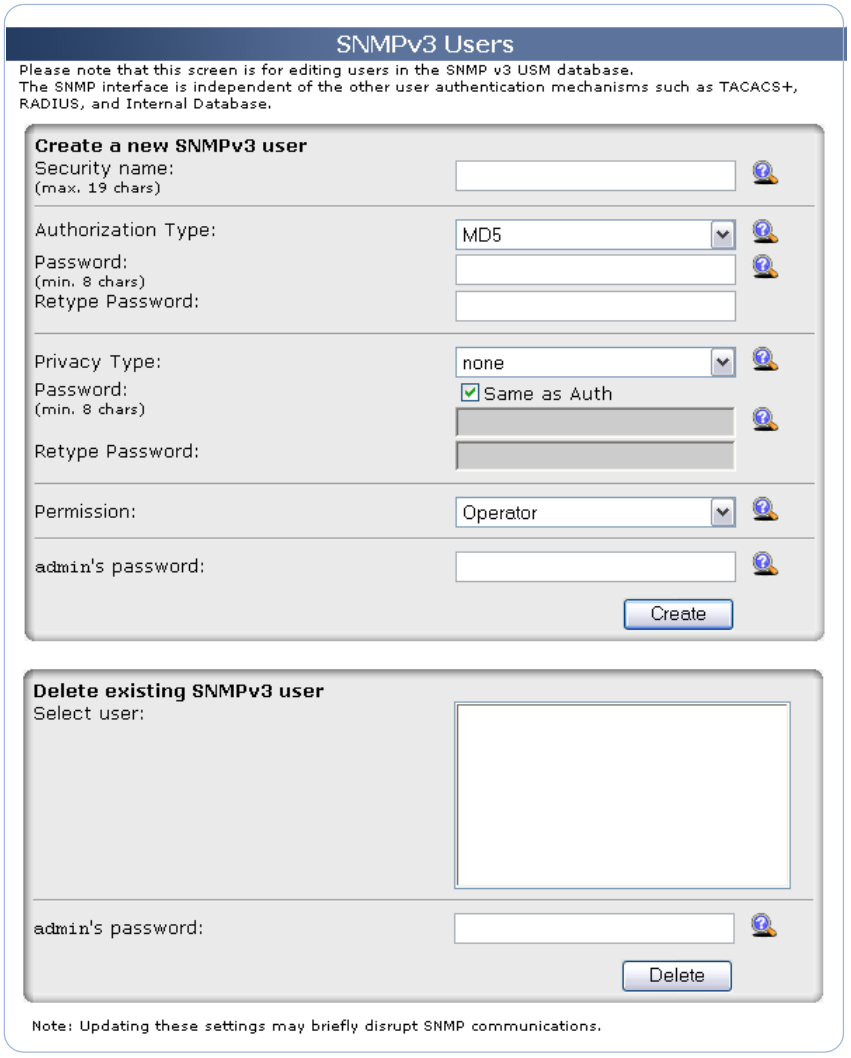
## 10.2.4. SNMP v3 Users

To xyz select:

**Settings>Users/Security>SNMP v3 Users**

This screen displays on the Canvas:

**Figure 48. SNMP v3 Users screen**




The screen includes these options:

**Note**

Accounts at all permission privilege levels can access this screen. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| **Create a new SNMPv3 user** | |
| Security name: | Specifies the SNMP USM user name. |

| Field | Description |
|---|---|
| Authorization Type: | Specifies the encryption method used for authorization. Values include:<br>• MD5<br>• SHA |
| Password: | Specifies the SNMP auhorization passphrase. |
| Privacy Type: | Specifies the encryption method used for communication. Values include:<br>• None<br>• AES<br>• DES |
| Password: | Specifies the SNMP privacy passphrase. |
| Retype Password: | Type the password again in this box for confirmation. The switch ensures that the passwords match before accepting the password. |
| Permission: | Specifies the default permission, or access level, for new user accounts:<br>• **Guest**: Users with this permission level have read-only access. This is the lowest permission level.<br>• **Operator**: Users with this permission level can do all that Guest-level users can do, plus patch ports using only preset configurations.<br>• **Advanced Operator**: Users with this permission level can do all that Operator-level users can do, plus patch ports on an ad-hoc basis, change rates and port names, plus save configuration settings (“presets”).<br>• **Administrator**: Users with this permission level do everything that the other levels do, plus set switch, blade, port, and other information as well as set and clear user and security information. This is the highest permission level.<br>These options are available only if User Database is set to Internal, RADIUS, or TACACS+. |
| *user* password: | Specifies the password for the currently logged in user. Unless the *User Database* (see page 107) is set to `None`, you must provide a valid password.<br>This field is required only for changes to the SNMP user database. |
| Create button | Adds a user account to the SNMP user database. |
| **Delete existing SNMPv3 user** | |
| Select user: | Lists all users in the SNMP user database. To select a user for deletion, highlight that user, enter your password, then click the Delete button. To select more than one user, press the Ctrl key as you select users. To select a block of users, press the Shift key, then select the first and last user in the block. |
| *user* password: | Specifies the password for the currently logged in user. Unless the *User Database* (see page 107) is set to `None`, you must provide a valid password.<br>This field is required only for changes to the SNMP user database. |
| Delete button | Deletes selected users from the SNMP user database. |

## 10.3. Services

With WEBX, you can perform the following switch security tasks:

- Enable secure web (HTTPS) connections, requiring users to log in using a secure SSL connection. You can also generate the SSL certificate required to enable secure SSL logins.
- Enable secure command line (CLI) connections, allowing users to log in using an SSH connection. You can also generate the SSH key required to enable SSH.
- Enable one or more users to issue ASCII commands or run ASCII-command scripts over the network.
- Enable network use of TITAN.
- Enable network use of CLI, APCON's Telnet interface, as a secure Telnet (SSH) connection. You can also generate an SSH key to run CLI in secure mode.
- Enable the use of telnet, TFTP, RPC, Secure RPC, SNMP, and remote syslog.

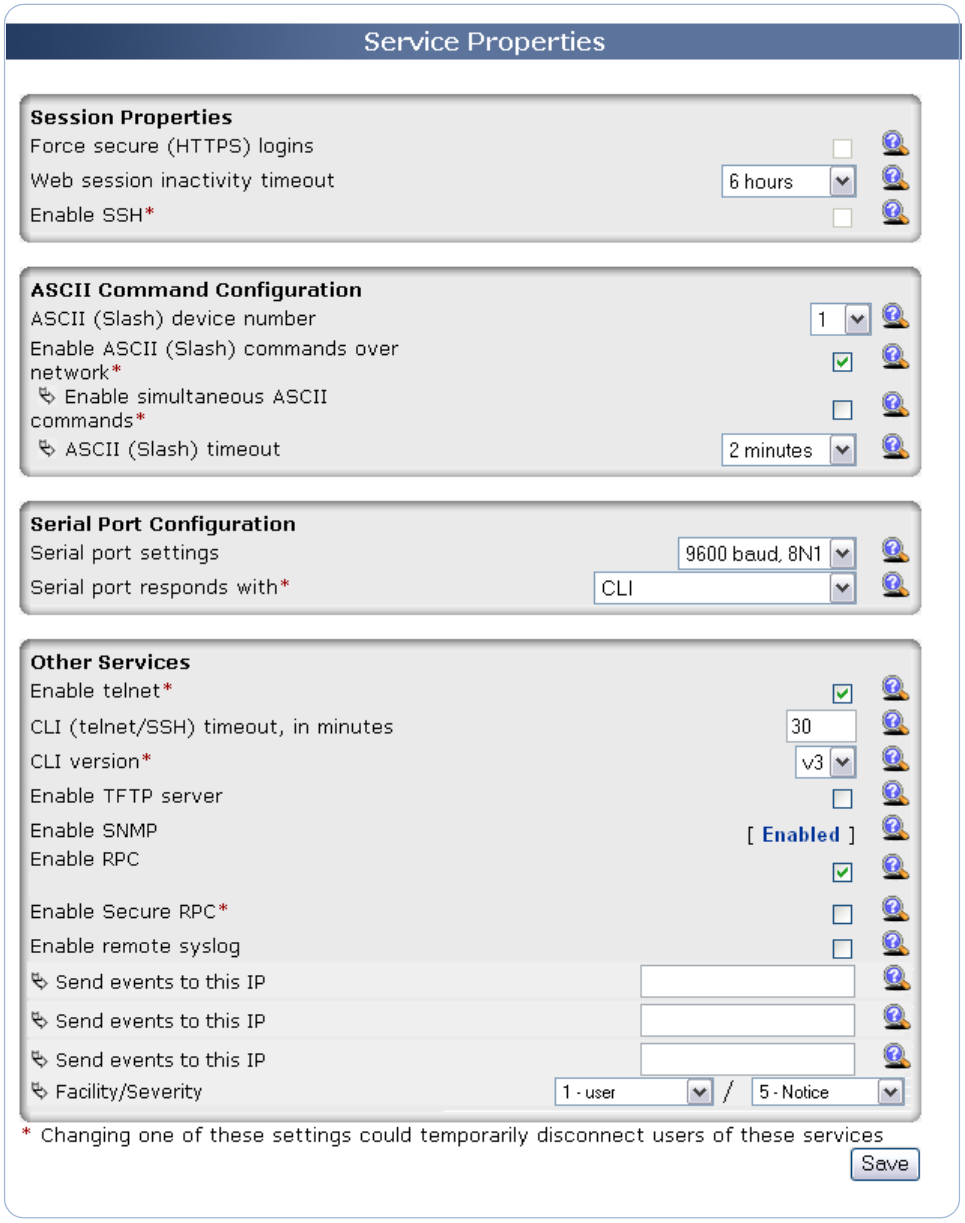
## 10.3.1. Service Properties

To manage switch security, select:

**Settings>Services>Service Properties**

This screen displays on the Canvas:

**Figure 49. Service Properties screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Force secure (HTTPS) logins | Specifies the types of logins allowed:<br>☐ **Unchecked (default)**: Allows both HTTP (insecure) and HTTPS (secure) logins.<br>☑ **Checked**: Allows only HTTPS (secure) logins.<br>**Note**: Valid only if an SSL certificate exists and the certificate is linked to the correct IP address. |
| Web session inactivity timeout | Specifies the number of minutes or hours of inactivity that elapse before WEBX automatically logs out a user. |
| Enable SSH | Specifies the types of logins allowed:<br>☐ **Unchecked (default)**: Does not allow SSH (secure) logins.<br>☑ **Checked**: Allows SSH (secure) logins.<br>**Note**: SSH provides a channel you can use to communicate with the switch and encryption. If you do not require the security of encryption, you can also consider using insecure telnet connections. |
| ASCII Command Configuration | Configures ASCII command behavior and their network availability. |
| ASCII (Slash) device number | Enter a number from 1 to 32 that indicates the ASCII device number. The factory default is 1 (one). Do not change this number unless you plan to daisy chain the switch or use it with INTELLAZONE. |
| Enable ASCII (Slash) commands over network | Determines ASCII (slash) command availability:<br>☐ **Unchecked (default)**: The ASCII (Slash) commands are not enabled or available over the network.<br>☑ **Checked**: Users can use the ASCII (Slash) commands over the network.<br>ASCII (Slash) commands are used to run scripts or issue commands that use the ASCII command set. To get ASCII (Slash) command documentation, contact APCON as described in *Contacting* APCON on page 7. |
| Enable simultaneous ASCII commands | Determines ASCII (slash) command availability:<br>☐ **Unchecked (default)**: Only one user at a time can access the ASCII (Slash) commands over the network.<br>☑ **Checked**: Multiple users can simultaneously access the ASCII (Slash) commands over the network.<br>**Note**: This option displays only when the Enable ASCII (Slash) commands over network option is checked. |
| ASCII (Slash) timeout | Specifies the number of minutes with no activity that elapse before ASCII commands are no longer available over the network. Select the number of minutes, from 1 to 10, from the drop-down list. |
| Serial Port Configuration | Configures serial port behavior. |
| Serial port settings | Specifies the number of stop bits used by the switch's serial port. The default is 1 stop bit. All other serial port settings are fixed: 9600 baud, 8 data bits, no parity, no flow control. |

| Field | Description |
|---|---|
| Serial port responds with | Specifies the software that runs on the serial port. Valid values include:<br>• **CLI [default]**: To access the switch, users must enter CLI commands.<br>• **ASCII (Slash) commands**: To access the switch, users must enter ASCII commands. |
| Other Services | Configures the behavior of network services. |
| Enable telnet | Determines telnet availability:<br>☐ **Unchecked (default)**: CLI, APCON's embedded telnet interface, is not available over the network. Users must use other methods to access the switch.<br>☑ **Checked**: Users can now access the switch over the network using CLI, APCON's telnet interface.<br>**Note**: Telnet provides a channel you can use to communicate with the switch, but does not provide encryption. If you require the security of encryption, use SSH. |
| CLI (telnet/SSH timeout, in minutes) | Specifies the number of minutes of inactivity that must elapse before automatically terminating a telnet or SSI session. The default is 5 (five) minutes. The maximum is 1440 minutes. |
| CLI version | Specifies the CLI version you want to use:<br>• **v2**: Supports version 2 of the embedded CLI. Select this option if you are running firmware version 2.11 or earlier, or if your existing scripts were developed using this version.<br>Previous firmware that shipped with a CLI (most, if not all of the existing "200 series" of firmware) shipped with this version, which uses the same inputs and outputs as CLI.<br>• **v3 (default; recommended)**: Supports version 3 of the embedded CLI. Select this option if you are running firmware version 2.12 or later.<br>WEBX 2.12 introduces this version, which includes features such as user maintenance, zoning, locking, and port classes. Although it tries to be backward compatible with v2, it may not perfectly emulate all commands, which is why v2 is also provided.<br>**Note**: Upgraded switches default to v2 to maintain compatibility until the administrator explicitly switches to v3. |

| Field | Description |
|---|---|
| Enable TFTP server | Determines TFTP availability:<br>☐ **Unchecked (default)**: Users cannot import and export switch settings.<br>☑ **Checked**: Users can now import and export switch settings.<br>**Note**: For security reasons, APCON recommends that you enable the service only during short windows such as installing a new switch with predefined parameters or backing up an existing switch configuration as the TFTP protocol itself does not support authentication.<br>When you select this option, you can access these files:<br>/tmp/export.xml (READ-ONLY)<br>Contains the current switch settings<br>/tmp/import.xml (WRITE-ONLY)<br>Upon successful upload, the switch is reconfigured using the contents of this file. Depending on what parameters are defined in the XML, the configuration can take up to two minutes, during which time the switch may beep or flash (e.g. when a blade is being configured, powered on/off, or port rates are set.)<br>Because this batch process runs in the background, you cannot check status or completion (except to view switch settings and verify that they change). |
| Enable SNMP | Clicking the Enabled or Disabled link to the right displays the *SNMP Properties* screen where you set SNMP criteria. For details about this screen, see page 122. |
| Enable RPC | Determines RPC status:<br>☑ **Checked (default)**: RPC is enabled and available over the network. You can now access and control the switch over the network using standalone software applications such as APCON's TITAN software.<br>☐ **Unchecked**: RPC is not available over the network. Users must use other methods to access the switch.<br>**Note**: Use the default value unless directed otherwise by APCON support personnel. |
| Enable Secure RPC | Determines Secure RPC status:<br>☑ **Checked (default)**: Secure RPC (SSL) is enabled and available over the network.<br>☐ **Unchecked**: Secure RPC is not available over the network. Users must use other methods to access the switch.<br>**Note**: Use the default value unless directed otherwise by APCON support personnel. |
| Enable remote syslog | Determines whether log events are sent to a central log server:<br>☑ **Checked (default)**: Send remote system log events.<br>☐ **Unchecked**: Do not send remote system log events. |

| Field | Description |
|---|---|
| Send events to this IP | Specifies the IP address you want to send remote system log events to, in standard TCP/IP #.#.#.# format.<br>**Note**: This option displays only when the Enable remote syslog option is checked. |
| Facility/Severity | Specifies the event type and importance. You can select from the following:<br>**Facility**<br>*Core*<br>0 kernel<br>1 user<br>2 mail<br>3 system<br>4 security<br>*Services*<br>5 syslogd<br>6 lp<br>7 news<br>8 UUCP<br>9 clock<br>10 security<br>11 FTP<br>12 NTP<br>13 log audit<br>14 log alert<br>15 clock<br>*Local*<br>16 local0<br>17 local1<br>18 local2<br>19 local3<br>20 local4<br>21 local5<br>22 local6<br>23 local7<br>**Severity**<br>0 Emergency<br>1 Alert<br>2 Critical<br>3 Error<br>4 Warning<br>5 Notice<br>6 Informational<br>7 Debug<br>**Note**: This option displays only when the Enable remote syslog option is checked. |
| Help | Hovering your cursor over this icon displays Help information about the associated field. |
| Save button | Saves and implements your changes. |

## 10.3.2. SNMP Properties

APCON provides a Management Information Base (MIB) you can use in conjunction with an SNMP management tools (such as OpenView) to manage INTELLAPATCH switches via Simple Network Management Protocol (SNMP). WEBX supports only SNMP versions 1 and 2.

To use the MIB, you set the options in this screen and point your SNMP management application to the INTELLAPATCH switch. You can then use your SNMP management application to monitor and manage your INTELLAPATCH switch(es).

**Note**

These tools provide read-only access. Write permission requires SNMP v3, which requires a license key from APCON. For more information about SNMP v3, see *SNMP v3 Users* on page 114. For information about license keys, see *License Key* on page 98.

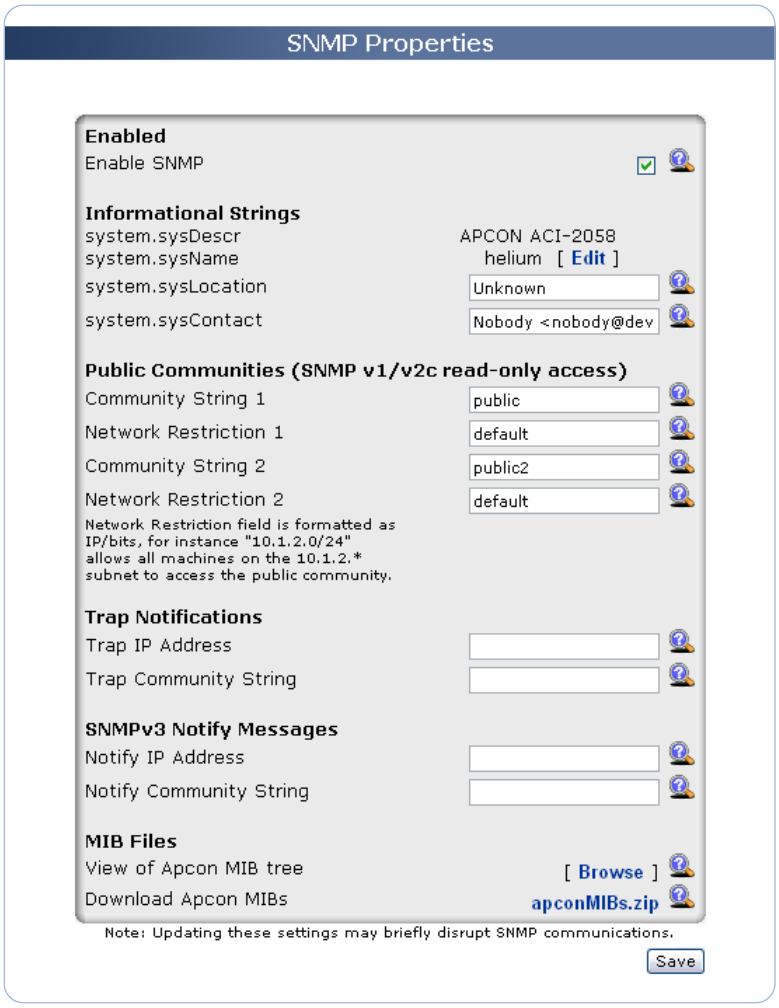
For more information about SNMP and APCON's MIB files, see *Appendix B, Adding APCON Attributes to your RADIUS Server*.

To configure WEBX SNMP settings, select:

**Settings>Services>SNMP Properties**

This screen displays on the Canvas:

**Figure 50. SNMP Configuration screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Enable SNMP | Checking this box enables Simple Network Monitoring Protocol (SNMP). |
| Informational Strings | These fields specify how the switch identifies itself. |
| system.sysDescr | The switch's model number. This is a display-only field; you cannot change its value. |
| system.sysName | The name you specify for the switch. Clicking the Edit link displays the *Properties* screen where you can change the switch name. For details about this screen, see page 133.<br>**Note**: You can also access this screen by selecting **Configuration>Switch Properties**. |

| Field | Description |
|---|---|
| system.sysLocation | A name you specify for the switch location. Select names that provide meaningful aids to memory, so that you and others can identify later the switch location. |
| system.sysContact | Information you specify as a contact for the switch. You can include names, phone numbers (including extenstions), email addresses, or any other useful contact information. |
| Public Communities (SNMP v1/v2c read-only access) | The community with read-only access. Use this community to monitor switch events. |
| Community Strings 1 & 2 | The string required for community access. The switch includes this string in outgoing public messages. |
| Network Restriction 1 & 2 | The subnet of machines allowed to access the corresponding SNMP community. Valid values include:<br>• A subnet in IP/numbits format (`#.#.#.#/n`)<br>Examples:<br>`10.1.1.1/32`<br>Only the specified host can access the community.<br>`10.1.1.0/24`<br>Any host in the 10.1.1.* Class C subnet can access the community.<br>• `default`. Selecting this value opens access to all. |
| Trap Notifications | These fields specify how to handle event report messages, also known as *traps*. Traps include only alarm events. |
| Trap IP Address | The IP address, in standard TCP/IP `#.#.#.#` format, of the SNMP management application. |
| Trap Community String | The string required for trap community access. The switch includes this string in outgoing trap messages. |
| MIB Files | Provides access to APCON's MIB file. |
| View of APCON MIB tree | Displays APCON's MIB tree in a formatted, human-readable format. |
| Download APCON MIBs | Downloads the APCON's MIB file in archived text format. You can then feed this file to your SNMP management application. |

## 10.3.3. Certificates

To change your preferences, select:

**Settings>Services>Certificates**

This screen's Generate tab displays on the Canvas.

### 10.3.3.1. Certificates screen: Generate tab

Generates self-signed SSL certificates and SSH keys.

**Figure 51. Certificates screen**


The screen includes these options:

**Note**

Accounts at all permission privilege levels can access this screen. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Current SSL Certificate | Displays the current SSL certificate. The contents of the SSL certificate change each time you generate a new SSL certificate. |
| Generate SSL Certificate button | Creates a self-signed SSL certificate.<br>SSL certificates are based in part on the switch's IP address. Each time you change the switch's IP address, you must generate a new SSL certificate.<br>SSL certificates are required to log in to the switch using a secure (HTTPS) connection. For information about secure logins, see *Logging In* on page 23. For information about deleting this certificate, see *Reset* on page 99.<br>**Note**: The switch may not respond until the new certificate is generated. This process can take up to several minutes. |

| Field | Description |
|---|---|
| Current SSH Key | Displays the current SSH key. The contents of the SSH key change each time you generate a new SSH key. |
| Generate SSH Key button | Creates an SSH key.<br>SSH key are based in part on the switch's IP address. Each time you change the switch's IP address, you must regenerate a new SSH key.<br>SSH key are required to log in to the switch using a secure telnet (SSH) connection. For information about deleting this key, see *Reset* on page 99.<br>**Note**: The switch may not respond until the new key is generated. This process can take up to several minutes. |

### 10.3.3.2. Certificates screen: Upload Web Cert tab

Generates custom certificates. To use these options, you must have corporate certificate authority.

**Figure 52. Certificates screen**


The screen includes these options:

**Note**

Accounts at all permission privilege levels can access this screen. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| CA public certificate, *.PEM format: | A text box where you paste the copied CA public certificate. |
| Apcon switch public certificate, *.PEM format: | A text box where you paste the copied APCON switch public certificate. |
| Apcon switch private certificate, *.PEM format: | A text box where you paste the copied APCON switch private certificate. |
| Upload button | Uploads the custom certificate(s) you specified.<br>**Note**: The switch may not respond until the new key is generated. This process can take up to several minutes. |

### 10.3.3.3. Certificates screen: Upload SSH Keys tab

Uploads a premade host key.

**Figure 53. Certificates screen**


The screen includes these options:

**Note**

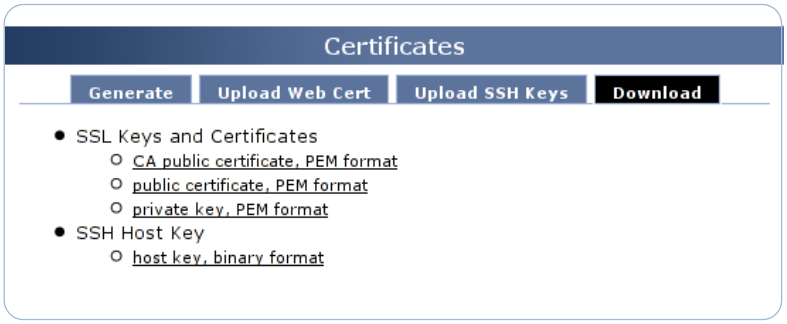
Accounts at all permission privilege levels can access this screen. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| The SSH keyfile upload server is: | Specifies the host key file you want to upload.<br>You can do one of these:<br>• Enter the update file's full directory path and filename.<br>• Click the Browse button to navigate to and select the file. |
| Upload button | Clicking this button copies the specified file to the switch. |
| Text box | Displays the host key file after upload. |

### 10.3.3.4. Certificates screen: Download tab

Downloads certificates and keys from WEBX.

**Figure 54. Certificates screen**




The screen includes these options:

**Note**

Accounts at all permission privilege levels can access this screen. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| SSL Keys and Certificates | |
| CA public certificate, PEM format | Displays a dialog where you can download the CA public certificate from WEBX to the workstation you specify. |
| public certificate, PEM format | Displays a dialog where you can download the public certificate from WEBX to the workstation you specify. |
| private key, PEM format | Displays a dialog where you can download the private certificate from WEBX to the workstation you specify. |
| SSH Host Key | |
| host key, binary format | Displays a dialog where you can download the host key from WEBX to the workstation you specify. |

# 10.4. Switch

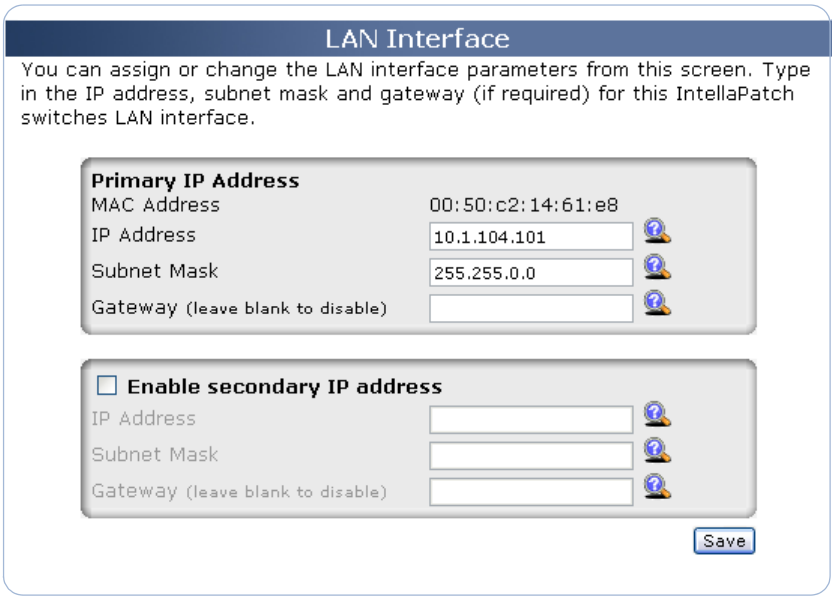
## 10.4.1. LAN Interface

To configure network parameters, select:

**Settings>Switch>LAN Interface**

This screen displays on the Canvas:

**Figure 55. LAN Interface screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Primary IP Address | Provides network information related to the primary IP address. |
| MAC Address | The switch's MAC address. This is a display-only field; you cannot change its content. |
| IP Address | The switch's IP address. The default is:<br>`192.168.0.1`<br>Set this value to an available static IP address on your network. |
| Subnet Mask | The switch's subnet mask. The default is:<br>`255.255.255.0`<br>Your INTELLAPATCH switch requires a static IP address; DHCP is not supported. |
| Gateway | (Optional) The switch's gateway address. To disable the network gateway, leave this field blank, which means "none". The default is blank. |

| Field | Description |
|---|---|
| Enable secondary IP address | Determines how many IP addresses the switch uses:<br>☑ **(Checked)**: The switch uses two IP addresses. Each LAN port is multihomed with the two IP addresses. The two LAN ports on the back of the unit are split into isolated VLAN segments and cannot pass traffic between each other. You can reach each port by either IP address, but cannot daisy chain.<br>☐ **(Unchecked)**: The switch uses one IP address. You can stack multiple chassis together, plug one into the network, and daisy-chain the rest.<br>For more information about single vs. dual IP addresses, see *Assigning IP Addresses* on page 10. |
| IP Address | The switch's second IP address. The default is:<br>`192.168.0.1`<br>Set this value to an available static IP address on your network. |
| Subnet Mask | The switch's second subnet mask. The default is:<br>`255.255.255.0`<br>Your INTELLAPATCH switch requires a static IP address; DHCP is not supported. |
| Gateway | (Optional) The switch's second gateway address. To disable the network gateway, leave this field blank, which means "none". The default is blank. |
| Save button | Saves the changes you specified. |
| Help | Hovering your cursor over this icon displays Help information about the associated field. |

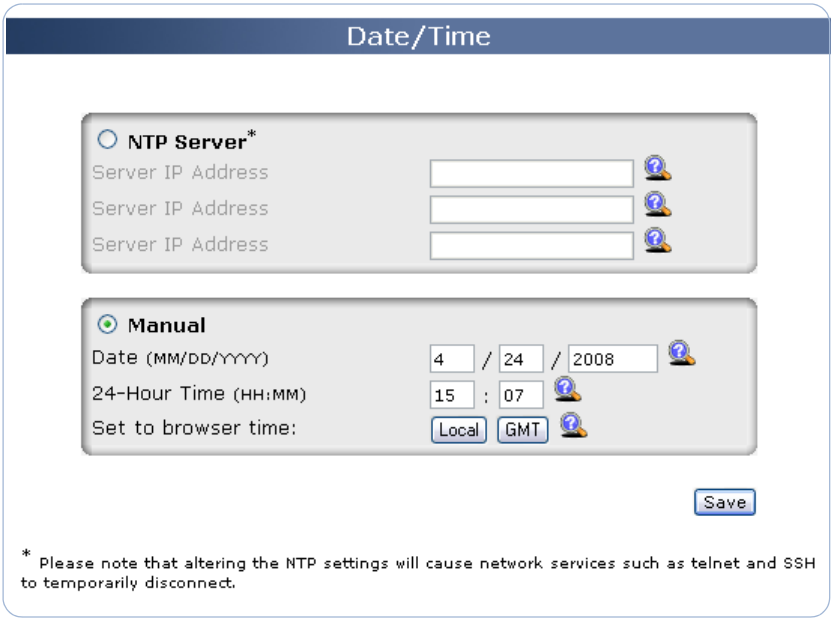
## 10.4.2. Date/Time

To configure switch date and time, select:

**Settings>Switch>Date/Time**

This screen displays on the Canvas:

**Figure 56. Date/Time screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| NTP Server | Obtains the date and time from the NTP server, re-synchronizing every hour. If you select this option, you cannot manually set the time.<br>**Note**: Changing the NTP settings temporarily disconnects network services such as telnet and SSH. |
| Server IP Address | The IP address of your network NTP server, in standard TCP/IP #.#.#.# format. |
| Manual | Obtains the date and time from the source you specify. If you select this option, you cannot obtain the date and time from the NTP server. |
| Date (MM/DD/YYYY) | Sets the switch date. Enter the time in the following format:<br>*MM/DD/YYYY*<br>*MM* Two digits that indicate the month.<br>*DD* Two digits that indicate the day.<br>*YYYY*Four digits that indicate the year. |

| Field | Description |
|---|---|
| 24-Hour Time (HH:MM) | Sets the switch time. Enter the time in 24-hour format:<br>*HH:MM*<br>*HH* Two digits that indicate the hour.<br>*MM* Two digits that indicate the minute. |
| Set To Browser Time | Sets the time to one of these:<br>• **Local**: Uses the date and time reported by your web browser in the Date and 24-Hour Time fields.<br>• **GMT**: Uses Greenwich Mean Time in the Date and 24-Hour Time fields. |
| Save button | Saves the changes you specified. |
|  Help | Hovering your cursor over this icon displays Help information about the associated field. |

## 10.4.3. Properties

To configure switch characteristics, select:

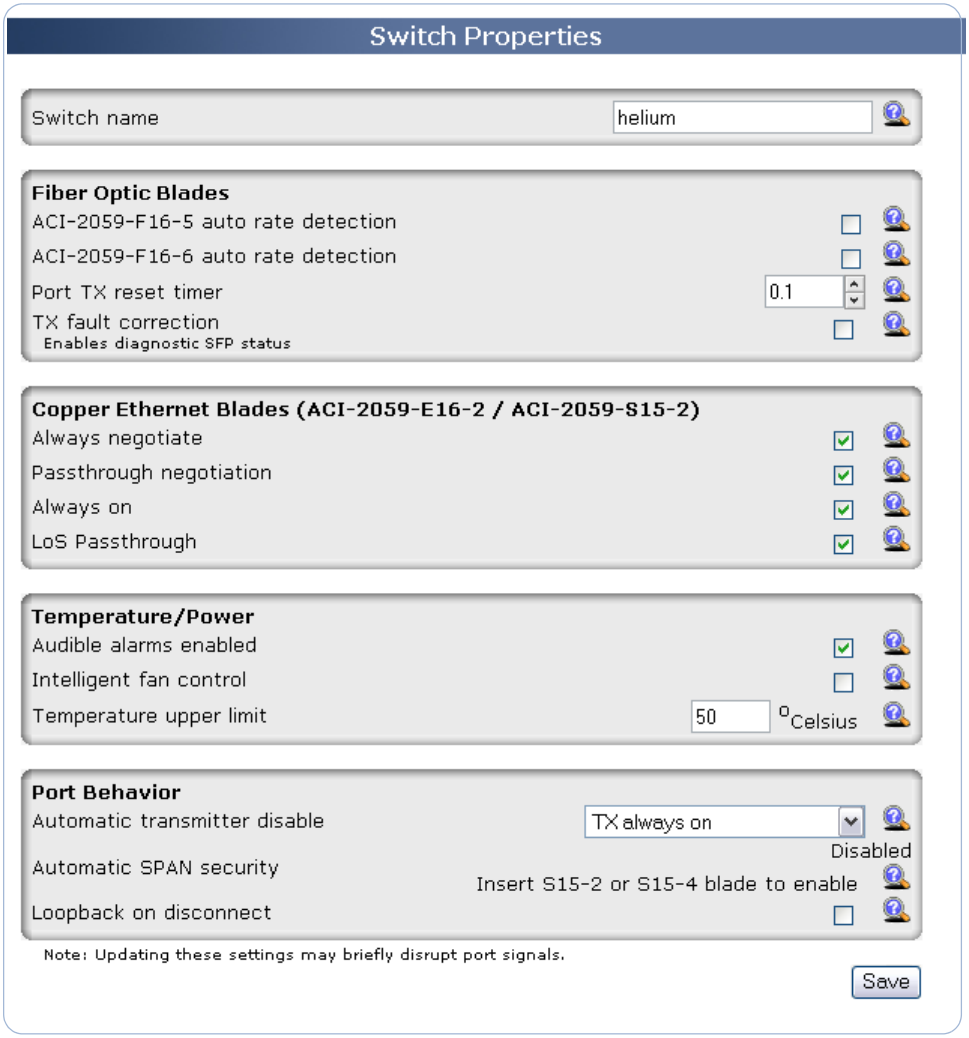
**Settings>Switch>Properties**

**Note**

You can also access this screen from the Switch Details screen, as described on page 18.

This screen displays on the Canvas:

**Figure 57. Properties screen**




The screen includes these options:

**Note**

- To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.
- Changing the settings on this screen may temporarily disrupt port signals.

| Field | Description |
|---|---|
| Switch name | A name that identifies the switch. The default name is `Unnamed`. Switch names are up to 31 characters and can include letters, numbers, spaces, and most keyboard characters. Switch names cannot include these characters:<br>< (Less-than symbol)<br>> (Greater-than symbol)<br>\ (Backslash) |
| Fiber Optic Blades | Options in this section specify behavior for Fiber Optic blades.<br>**Note**: INTELLAPATCH products do not negotiate links in the way a Layer 2/3 switch does. The ACI-2059-E16-2/S15-2 and ACI-2059-E16-4/S15-4 blades are the only exception, as they each have a PHY chip and do negotiate a link with the end device. |
| ACI-2059-F16-5 auto rate negotiation | Specifies rate negotiation for the F16-5 blades on the switch:<br>☐ **Unchecked**: Transmission rates are set as specified on the *Rates* screen, as described on page 52. Under most conditions, this option is preferred.<br>☑ **Checked**: Each port tries to lock onto the negotiated data rate of the peripherals, HBAs, and switches physically cabled to the INTELLAPATCH switch. Check the box only when this feature is needed as it may decrease system performance.<br>**Note**: Selecting this option requires that you also set the port's data rate to Auto. For details, see *Rates* on page 52. Failure to use this rate may result in incorrect data rates displaying for some ports on the Patch Ports, Realtime screen. For information about this screen, see *Realtime* on page 33. |
| ACI-2059-F16-6 auto rate negotiation | Specifies rate negotiation for the F16-6 blades on the switch:<br>☐ **Unchecked**: Transmission rates are set as specified on the *Rates* screen, as described on page 52. Under most conditions, this option is preferred.<br>☑ **Checked**: Each port tries to lock onto the negotiated data rate of the peripherals, HBAs, and switches physically cabled to the INTELLAPATCH switch. Select this option only when this feature is needed as it may decrease system performance.<br>**Note**: Selecting this option requires that you also set the port's data rate to Auto. For details, see *Rates* on page 52. |

| Field | Description |
|---|---|
| Switch name | A name that identifies the switch. The default name is `Unnamed`. Switch names are up to 31 characters and can include letters, numbers, spaces, and most keyboard characters. Switch names cannot include these characters:<br>< (Less-than symbol)<br>> (Greater-than symbol)<br>\ (Backslash) |
| Fiber Optic Blades | Options in this section specify behavior for Fiber Optic blades.<br>**Note**: INTELLAPATCH products do not negotiate links in the way a Layer 2/3 switch does. The ACI-2059-E16-2/S15-2 and ACI-2059-E16-4/S15-4 blades are the only exception, as they each have a PHY chip and do negotiate a link with the end device. |
| ACI-2059-F16-5 auto rate negotiation | Specifies rate negotiation for the F16-5 blades on the switch:<br>☐ **Unchecked**: Transmission rates are set as specified on the *Rates* screen, as described on page 52. Under most conditions, this option is preferred.<br>☑ **Checked**: Each port tries to lock onto the negotiated data rate of the peripherals, HBAs, and switches physically cabled to the INTELLAPATCH switch. Check the box only when this feature is needed as it may decrease system performance.<br>**Note**: Selecting this option requires that you also set the port's data rate to Auto. For details, see *Rates* on page 52. Failure to use this rate may result in incorrect data rates displaying for some ports on the Patch Ports, Realtime screen. For information about this screen, see *Realtime* on page 33. |
| ACI-2059-F16-6 auto rate negotiation | Specifies rate negotiation for the F16-6 blades on the switch:<br>☐ **Unchecked**: Transmission rates are set as specified on the *Rates* screen, as described on page 52. Under most conditions, this option is preferred.<br>☑ **Checked**: Each port tries to lock onto the negotiated data rate of the peripherals, HBAs, and switches physically cabled to the INTELLAPATCH switch. Select this option only when this feature is needed as it may decrease system performance.<br>**Note**: Selecting this option requires that you also set the port's data rate to Auto. For details, see *Rates* on page 52. |

| Field | Description |
|---|---|
| Switch name | A name that identifies the switch. The default name is `Unnamed`. Switch names are up to 31 characters and can include letters, numbers, spaces, and most keyboard characters. Switch names cannot include these characters:<br>< (Less-than symbol)<br>> (Greater-than symbol)<br>\ (Backslash) |
| Fiber Optic Blades | Options in this section specify behavior for Fiber Optic blades.<br>**Note**: INTELLAPATCH products do not negotiate links in the way a Layer 2/3 switch does. The ACI-2059-E16-2/S15-2 and ACI-2059-E16-4/S15-4 blades are the only exception, as they each have a PHY chip and do negotiate a link with the end device. |
| ACI-2059-F16-5 auto rate negotiation | Specifies rate negotiation for the F16-5 blades on the switch:<br>☐ **Unchecked**: Transmission rates are set as specified on the *Rates* screen, as described on page 52. Under most conditions, this option is preferred.<br>☑ **Checked**: Each port tries to lock onto the negotiated data rate of the peripherals, HBAs, and switches physically cabled to the INTELLAPATCH switch. Check the box only when this feature is needed as it may decrease system performance.<br>**Note**: Selecting this option requires that you also set the port's data rate to Auto. For details, see *Rates* on page 52. Failure to use this rate may result in incorrect data rates displaying for some ports on the Patch Ports, Realtime screen. For information about this screen, see *Realtime* on page 33. |
| ACI-2059-F16-6 auto rate negotiation | Specifies rate negotiation for the F16-6 blades on the switch:<br>☐ **Unchecked**: Transmission rates are set as specified on the *Rates* screen, as described on page 52. Under most conditions, this option is preferred.<br>☑ **Checked**: Each port tries to lock onto the negotiated data rate of the peripherals, HBAs, and switches physically cabled to the INTELLAPATCH switch. Select this option only when this feature is needed as it may decrease system performance.<br>**Note**: Selecting this option requires that you also set the port's data rate to Auto. For details, see *Rates* on page 52. |

| Field | Description |
|---|---|
| Port TX reset timer | Specifies the duration, in tenths of seconds, a port's transmitter is turned off when re-patching a port without first un-patching it. The port repatches with its transmitter off. Then, after the specified time elapses, the transmitter turns back on.<br>This setting is required in environments where ports are not always unpatched before repatching. It primarily affects end devices that require a certain amount of time for the transmitter to turn off before the link is forced to renegotiate which in turn guarantees that new devices will be recognized.<br>INTELLAPATCH switches can patch ports as quickly as 100µs, often resulting in devices not recognizing that a change in the physical layer occurred, and therefore not renegotiating new devices. Instead, the old devices are still recognized even though they are no longer physically attached.<br>`0.0` (Default) Transmitter is always on during port patching and un-patching.<br>`0.1–4.0` Specifies the duration, in tenths of seconds, that the transmitter is turned off when re-patching previously connected ports. Select a value long enough to satisfy the protocol specification for forcing a link to renegotiate. |
| TX fault correction | Determines action taken when transceiver faults are detected:<br>Some SFP transceivers support the MSA laser eye safety circuit specification. Many conditions can trigger the laser eye safety circuit, including high laser power, high laser bias current, high or low voltage, and high or low temperature.<br>☐ **Unchecked (default)**: If the laser eye safety circuit is triggered, the transmitter turns off.<br>If you select this option, turning a transmitter back on requires manual intervention: physically unplugging the fiber optic cable, re-seating it, re-seating the SFP transceiver, and then power-cycling the blade or chassis.<br>☑ **Checked**: The INTELLAPATCH switch actively monitors the transceivers, checking SFPs for a fault every five seconds. If a fault is detected, the laser eye safety circuit is reset which turns the transmitter back on. If the condition that caused the failure is still present, the fault is triggered again and the transmitter may potentially stay off until the condition is corrected. |
| Copper Ethernet Blades (ACI-2059-E16-2 / ACI-2059-S15-2) | Options in this section specify behavior for Copper Ethernet blades. |
| Always negotiate | Specifies rate negotiation with other copper Ethernet devices:<br>☑ **Checked (default)**: The switch automatically negotiates with other copper Ethernet devices. APCON recommends that you do not change this setting without first contacting support. For contact information, see *Contacting APCON* on page 4.<br>☐ **Unchecked**: The switch does not negotiate with other copper Ethernet devices. |

| Field | Description |
|---|---|
| Passthrough negotiation | Specifies rate matching:<br>☐ **Unchecked (default)**: The switch does not match rates.<br>☑ **Checked**: The switch automatically matches the rate at both ends of the connection.<br>**Note**: Rate matching may get "stuck" if performing switch-to-switch hopping. For example, when multiple APCON switches are arranged in a matrix configuration. |
| Always on | Specifies non-patched behavior:<br>☐ **Unchecked (default)**: Ports receive power only when patched. This matches the operation of older INTELLAPATCH switches and can be used to simulate a cable break.<br>☑ **Checked**: Ports always receive power, whether patched or unpatched. This matches the operation of most contemporary hubs, switches and routers. Although the port indicates a linked status, it does not indicate whether the port receives data.<br>When you select this option, you must also set Automatic Transmitter disable to one of the TX off when no RX options. For details, see *Automatic Transmitter disable* on page 139. |
| LoS Passthrough | Determines how to handle Loss of Signal (LoS) on one side of a pair of duplex-patched ports:<br>☐ **Unchecked**: The continuity light on the INTELLAPATCH port the device is patched remains lit. The device the port is patched to may be dead, alive, or simply unpatched, but the port is still "up" (powered and lit).<br>☑ **Checked**: The INTELLAPATCH switch forces the other side of that pair to go offline.<br>**Note**: This option available only when transmitter disable is set to one of the "TX off" states. |
| Temperature/Power | Options in this section specify temperature and power behavior. |
| Audible alarms enabled | Specifies the operation mode of the audible alarm.<br>☑ **Checked (default)**: The switch emits an audible alarm upon reaching and/or exceeding the alarm threshold, or when a power supply fails.<br>☐ **Unchecked**: The switch does not emit an audible alarm during an alarm condition. Other alarm notifications, such as LEDs changing color, continue to operate.<br>For information about what comprises an alarm condition, see the Temperature and Power options in *Controller* on page 78. |
| Intelligent fan control | Determines the operation of fans inside the switch:<br>☐ **Unchecked (default)**: Fans operate at full speed all the time.<br>☑ **Checked**: Fans operate at a rate appropriate for the blades that populate the switch. |
| Temperature upper limit | Specifies the temperature at or beyond which the switch triggers an alarm. The default is 50° C.<br>**WARNING**: Enter a value of 55° or less. Temperatures above 55° C can damage the switch. |

| Field | Description |
|---|---|
| Port Behavior | Options in this section specify port behavior. |
| Automatic Transmitter disable | Specifies the behavior of the transmitter on a port that does not receive a signal:<br>• **TX off when no RX (Default)**: The transmitter on a port is turned off when the opposing port's receiver does not have signal.<br>• **TX on always on**: The transceiver's transmitter is turned on at all times, regardless of whether the opposing port receives signal. |
| Automatic SPAN security | Determines SPAN port support:<br>• **Disabled (Insert S15-2 or S15-4 blade to enable)**: This switch supports SPAN ports.<br>• **Enabled**: This switch does not support SPAN ports. Selecting this option ensures that SPAN ports do not receive any traffic.<br>**Notes**:<br>• This is a display-only field; you cannot change its value.<br>• SPAN security requires additional configuration. For details about setting up SPAN security, see *Simplex Patching with SPAN/Monitor Ports* on page 13. |
| Loopback on disconnect | Determines port behavior when the patch is disconnected:<br>☐ **Unchecked (default)**: Turns ports off upon disconnect.<br>☑ **Checked**: Loops ports back to themselves upon disconnect. |
| Help | Hovering your cursor over this icon displays Help information about the associated field. |
| Save button | Saves and implements the changes you specify. |

## 10.4.4. Login Message

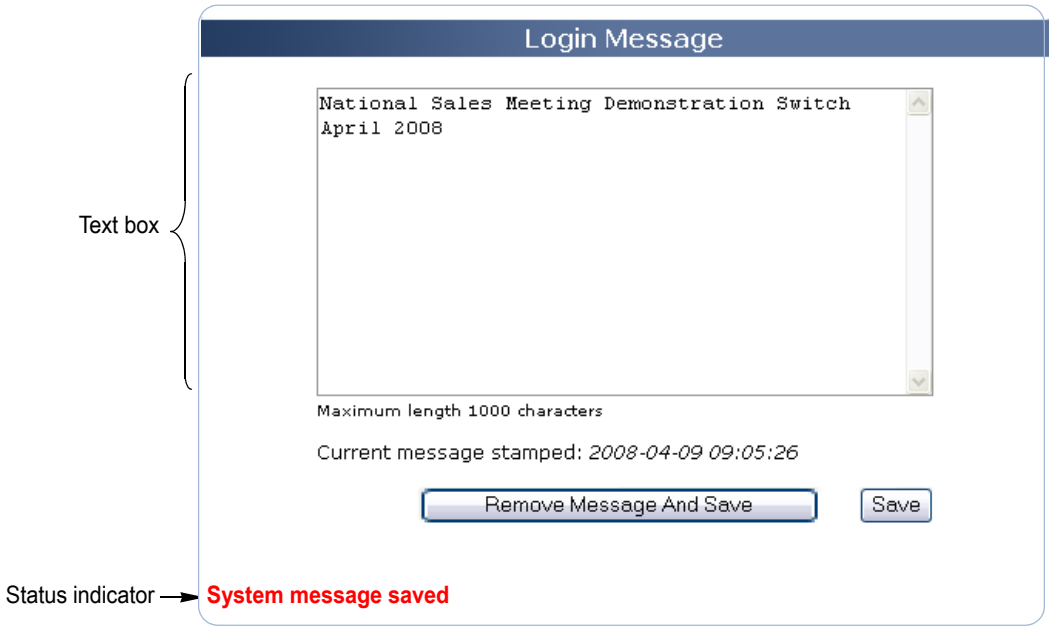
Specifies the message of the day that displays on the The WEBX login screen and the Controller screen.

To change the message of the day, select:

**Settings>Switch>Login Message**

This screen displays on the Canvas:

**Figure 58. Message screen**




The screen includes these options:

**Note**

To make changes on this screen, your account must have Administrator permission privileges. For details about permissions, see *Permissions* on page 112.

| Field | Description |
|---|---|
| Text box | Displays the message of the day. You use this box to change or delete the system message. |
| Current message stamped: | Displays the time and date the system message was last changed. |
| Remove Message And Save button | Deletes the current message, then saves the change. Clicking this button means no system message displays. |
| Save button | Saves your changes. Clicking this button means the updated system message displays. |
| Status indicator | Indicates the action taken by WEBX. Displays only after you click one of the buttons at the bottom of the screen. |

# Chapter 11

# Help

This chapter details the screens available from the Help menu:

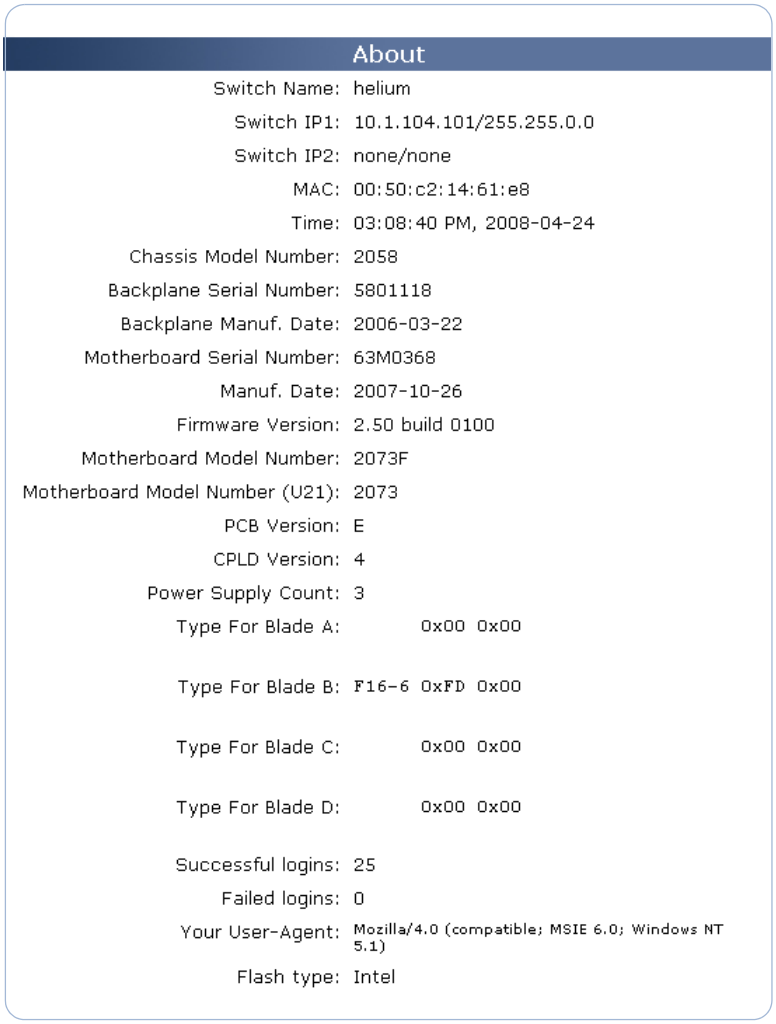
# 11.1. About

To view information about your INTELLAPATCH chassis, its blades, and login activity, select:

**Help>About**

This screen displays on the Canvas:

**Figure 59. About screen**




The screen includes information you can use when contacting APCON technical support.

For information about contacting technical support, see *Contacting APCON* on page 4 or the Help>Support menu option.

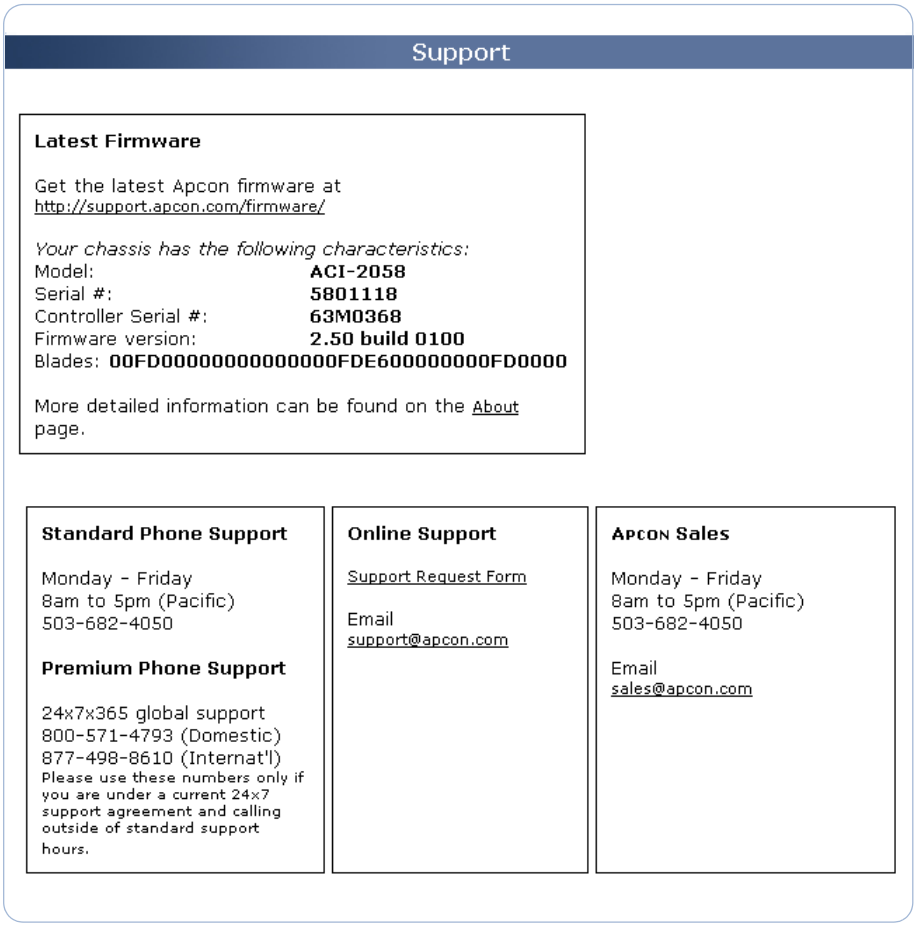
# 11.2. Support

To quickly access contact information for APCON support, select:

**Help>Support**

This screen displays on the Canvas:

**Figure 60. Support screen**




The screen includes these options:

| Field | Description |
|---|---|
| Latest Firmware | Lists pertinent information about your INTELLAPATCH chassis and provides a link where you can obtain firmward upgrades. |
| Standard Phone Support | Provides phone contact information for APCON technical support. |
| Online Support | Provides links to a troubleshooting questionnaire and email address for APCON support |
| APCON Sales | Lists hours of operation and contact information for APCON's Sales department. |

# Appendix A

# Data File Formats



## A.1. Sample SysLog File

For information about setting up your switch to write events to a SysLog, see the Enable Remote Syslog option in *Service Properties* on page 117.

Events written to a logfile include:

- Powering on or off a blade.
- Patching or unpatching a port.
- Naming a port.
- Storing, recalling, naming, or getting the name of a preset configuration.
- Setting the data rate, duplex setting, or MDI/MDIX status of a port.
- Setting the TCP/IP parameters of the INTELLAPATCH switch.
- Setting the device number of the INTELLAPATCH switch.
- Enabling or disabling the Telnet interface, or its secure (SSH) variant.
- Enabling a remote SysLog file, or getting or setting the IP address of the computer to which to write it.
- Requiring secure logins.
- Resetting the INTELLAPATCH switch to its factory defaults.
- Specifying an event type(Facility) and importance (Severity). For details about available choices, see the Facility/Severity option on the Event Log screen. For details about this screen, see page 82.

### A.1.1. Format

The messages consist of:

```
[date] [serverIP] [switchname] apcond/[service]: [action]|b:[blade]
p:[port] u:[user]@[IP] [string]
```

— OR —

```
[date] [serverIP] [switchname] apcond/[service]: [action]|b:[blade]
p:[port] u:[user]/[remoteIP]@[IP] [string]
```

## Parameters

`[date]` The date in standard RFC 3164 format.

`[serverIP` The IP address of the APCON switch.

`[switchname]`
The name of the APCON switch.

`[service]` The service that this action came from .

`[action]` An action string. Current action strings include:

Info
- Core service startup/shutdown
- System reboot requested

Security
- Login/logout
- Bad login
- Zoning
- RPC connection
- RPC disconnect

Configuration change
- Patch
- Blade powerup/powerdown
- Port flapping
- Port rate change
- Preset recall
- Preset name change
- Preset definition change
- Port name change
- Switch name change
- Port class enable
- Port class name change
- Port class definition change
- Port locking enable
- Port lock
- Port unlock

Alarm
- Power supply *n* failure/all-clear
- Chassis temperature failure/all-clear
- SFP alarm/alarm all-clear
- SFP temperature failure/all-clear
- SFP transmit failure/all-clear
- SFP receive failure/all-clear
- SFP power failure

SFP power failure
- TX fault corrected

`[blade]` A single-character blade letter or 0 (zero).

`[port]` The three-character port number or 0 (zero).

`[user` The user that caused the action.

`[remoteIP]`
(If present) The IP address from which the user is connected (see example).

`[IP]` The IP address from which the call was made (see example).

**Note**

If the service resides inside the APCON switch, such as the web, telnet, or SSH service, the IP address may be 127.0.0.1.

`[string]` An optional string related to the command.

## A.1.2. Import/Export Settings File Format

```
Jun 15 17:04:51 10.1.104.2 ununquadium apcond/apcond: core service startup|b:0 p:0
u:nobody@127.0.0.0
Jun 15 17:05:17 10.1.104.2 ununquadium apcond/web: login|b:0 p:0
u:admin/10.1.2.56@127.0.0.0
Jun 15 17:21:28 10.1.104.2 ununquadium apcond/web: configuration change|b:0 p:0
u:admin/10.1.2.56@127.0.0.0 Set name of preset 16 to "Preset 16"
Jun 15 17:22:15 10.1.104.2 ununquadium apcond/web: patch|b:0 p:0
u:admin/10.1.2.56@127.0.0.0
Q:A06A05A07A08A08A07A09A10A10A09A11A12A12A11A13A14A14A13A15A16
B01B02B02B01B03A00B04A00B05B01B06B01B07B02B08B02B09A00B10A00B11A00B12A00B13A00B14A0
0B15A00C01C02C02C01C03A00C04A00C05A00C06A00C07A00C08A00C09A00C10A00C11A00C12A00C13
A00C14A00C15A00C16A00D01D02
Jun 15 17:22:16 10.1.104.2 ununquadium apcond/web: patch|b:0 p:0
u:admin/10.1.2.56@127.0.0.0
Q:D02D01D03D04D04D03D05D06D06D05D07D08D08D07D09D10D10D09D11D12
D12D11D13A00D14A00D15A00D16A00
```

# A.2. Import/Export File Formats

Examples of some of the export file formats, provided below, are truncated for brevity:

**Figure 61. Sample file formats**

**Plain Text INI**

```
[PortNames]
A01=ATTO 3300
A02=Emulex LP10000DC
A03=Emulex LP8000
A04=Emulex LP8000S
A05=JNI Z210
A06=JNI FCE-6410
A07=LSI 7207XP-LC
A08=LSI 449290
```
*—lines deleted for brevity—*
```
[PortAssignments]
A01=OFF
A02=D02
A03=OFF
A04=OFF
A05=D05
A06=OFF
A07=OFF
A08=D07
```
*—lines deleted for brevity—*
```
Name=Preset 1
A01=NC
A02=NC
A03=NC
A04=NC
A05=NC
A06=NC
A07=NC
A08=NC
```
*—lines deleted for brevity—*

**HTML**

| port number | port name |
|---|---|
| A01 | ATT0 3300 |
| A02 | Emulex LP 10000DC |
| A03 | Emulex LP8000 |
| A04 | Emulex LP8000S |
| A05 | JNI Z210 |
| A06 | JNI FCE-6410 |
| A07 | LSI 7207XP-LC |
| A08 | LSI 449290 |

**Comma Delimited**

"port number","port name"
"A01","ATTO 3300"
"A02","Emulex LP10000DC"
"A03","Emulex LP8000"
"A04","Emulex LP8000S"
"A05","JNI Z210"
"A06","JNI FCE-6410"
"A07","LSI 7207XP-LC
"A08","LSI 449290"

"porta","portb"
"A01","A12"
"A02","B05"
"A03","C01"
"A04","A05"
"A05","A04"
"A06","B11"
"A07","B12"
"A08","C02"

"preset","preset name","porta","portb"
1,"Preset 1","A01,"A99"
1,"Preset 1","A02,"A99"
1,"Preset 1","A03,"A99"
1,"Preset 1","A04,"A99"
1,"Preset 1","A05,"A99"
1,"Preset 1","A06,"A99"
1,"Preset 1","A07,"A99"
1,"Preset 1","A08,"A99"

**XML and Diagnostic XML**

```
<allsettings>
<portnames>
<port number="A01" name="ATTO 3300"/>
<port number="A02" name="Emulex LP100DC"/>
<port number="A03" name="Emulex LP8000"/>
<port number="A04" name="Emulex LP8000S"/>
<port number="A05" name="JNI Z210"/>
<port number="A06" name="JNI FCE-6410"/>
<port number="A07" name="LSI 7207XP-LC"/>
<port number="A08" name="LSI 449290"/>
```
*—lines deleted for brevity—*
```
</portnames>
<patches>
<patch porta="A01" portb="A00"/>
<patch porta="A02" portb="D02"/>
<patch porta="A03" portb="A00"/>
<patch porta="A04" portb="A00"/>
<patch porta="A05" portb="D05"/>
<patch porta="A06" portb="A00"/>
<patch porta="A07" portb="A00"/>
<patch porta="A08" portb="D07"/>
```
*—lines deleted for brevity—*
```
</patches>
<presets>
<preset number="1" name="Preset 1">
<patch porta="A01" portb="A99"/>
<patch porta="A02" portb="A99"/>
<patch porta="A03" portb="A99"/>
<patch porta="A04" portb="A99"/>
<patch porta="A05" portb="A99"/>
<patch porta="A06" portb="A99"/>
<patch porta="A07" portb="A99"/>
<patch porta="A08" portb="A99"/>
```
*—lines deleted for brevity—*
```
</preset>
```
*—lines deleted for brevity—*
```
</presets>
</allsettings>
```

# A.3. Export Users File Format

```
# User list export of 10.1.104.2 on 2007-12-06 20:33:09 UTC
# Format: <username>:<level>:<MD5 password hash>
# User level is: 1=guest, 2=basic, 3=advanced, 4=admin
drevil:4:A94FA805F98ECA6FE686930C7C8B0403
number2:3:27BF0058AF50FD43E46419D6324F0B88
minime:1:1A242DA32316B0F62E406A95E7DB2DE9
scott:2:21F63C6E971CD913A9C147E8652CA659
basil:3:6862EFB4028E93AC23A6F90A9055BAE8
bigglesworth:1:CC7F3896E15C5628A175484C088C5D24
```

The `# Format:` line includes these fields:

| Field | Description |
|---|---|
| `username` | Specifies the new account name. Account names are not case-sensitive. Account names can include underscores or hyphens, but cannot include spaces or special characters. |
| `level` | Specifies the permission, or access level, for each user:<br>`1` **Guest**: Users with this permission level have read-only access. This is the lowest permission level.<br>`2` **Operator**: Users with this permission level can do all that Guest-level users can do, plus patch ports using only preset configurations.<br>`3` **Advanced Operator**: Users with this permission level can do all that Basic Operator-level users can do, plus patch ports on an ad-hoc basis, change rates and port names, plus save configuration settings (“presets”).<br>`4` **Administrator**: Users with this permission level do everything that the other levels do, plus set switch, blade, port, and other information as well as set and clear user and security information. This is the highest permission level. |
| `MD5 password hash` | The MD5 hash of the user password. |

# Appendix B

# Adding APCON Attributes to your RADIUS Server

After you finish the initial setup, verify that it works. You can then add attributes, which are available to the APCON firmware that supports them.

**Note**

Examples of the of the RADIUS attributes are based on the FreeRADIUS server. The exact syntax depends upon your RADIUS server.

To add attributes:

1. Get the `dictionary.apcon` file from support (Professional Services).
2. Copy `dictionary.apcon` to this location:

   `/usr/share/freeradius/`
3. Edit `/etc/raddb/dictionary`, adding this line:

   `$INCLUDE /usr/share/freeradius/dictionary.apcon`

   This adds an `Apcon-User-Level` attribute with these possible values:

   | | | |
   |---|---|---|
   | 0 | Default | User inherits the switch's default new user level. |
   | 1 | Guest | User has read-only access. |
   | 2 | Operator | User has some pre-canned write functionality (for example, recalling presets). |
   | 3 | Advanced | User can perform ad-hoc patching. |
   | 4 | Admin | User can administer the switch. |
4. Alter the user lines /etc/raddb/users to include the user level. For example:

   ```
   user1  Auth-Type := Local, User-Password == "pass1"
          Apcon-User-Level == Admin
   ```
5. Restart your RADIUS server by entering this command:

   `sudo /etc/rc.d/init.d/radiusd restart`

# Appendix C

# ConfiguringtheTACACS+Server



## C.1. Overview

The APCON switch supports up to three TACACS+ servers. The APCON switch does not allowing the server to redirect the switch to a different server, possibly using a different protocol.

TACACS+ provides authentication (user identity verification) and authorization (switch access levels ). Accounting provides an audit trail of who logged in, who logged out and who made configuration changes to the switch, and is provided though the syslog.

TACACS+ can provide authorization on a per-switch basis. (Zoning provides authorization on a per-port basis.)

The APCON switch requests password authentication while the server handles user authentication. It can use the system password file or store the user's password in any form it desires. If the TACACS+ sever doesn't recognize a user or the user's login has expired, access is denied to that user. If the server recognizes a user but doesn't have an explicit APCON user level, the user receives the system default.

## C.2. Configuring The Server

**Note**

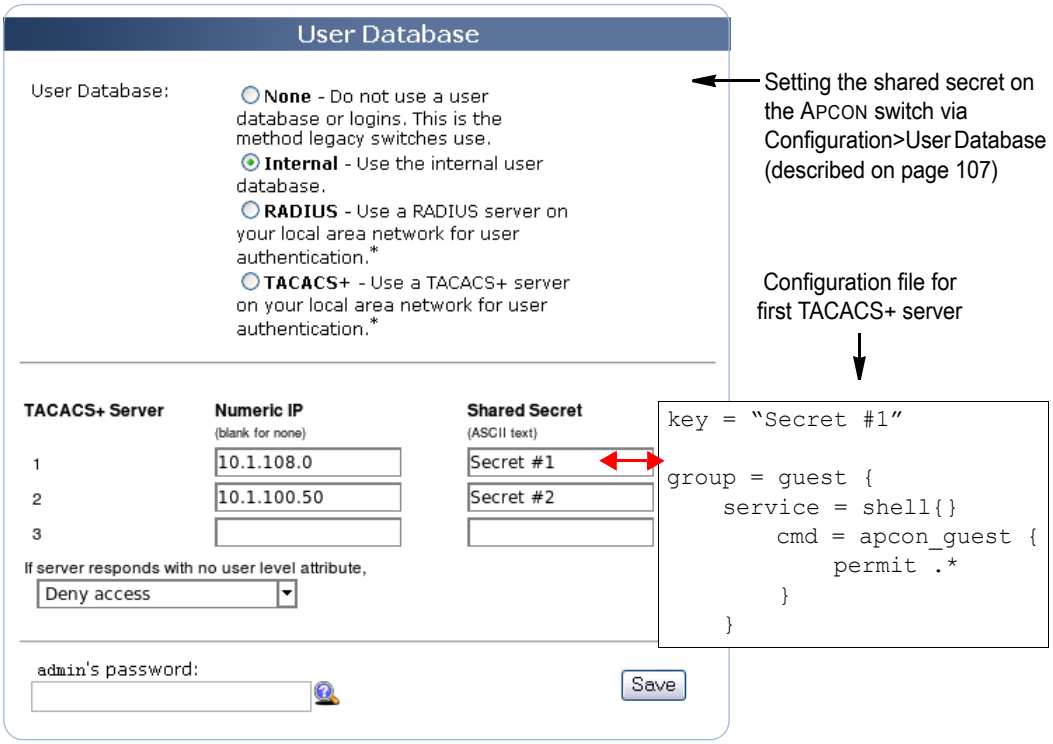
Examples of the of the TACACS+ server configuration file are based on the references server in the TAC_PLUS Developer's Kit from Sysco Systems, Inc. The exact syntax depends upon your TACACS+ server.

### C.2.1. Setting the Shared Secret

The shared secret is identified by the line `"key = "`. The value inside of quotes appears on the shared secret line of the input file for tacpluslogin. This can be any value, but it must match exactly in case and white space.

The next figure shows how to set the shared secret on the APCON switch on the left. On the right, is a snippet of the server's configuration file. The second TACACS+ server would have a similar file.

**Figure 62. Setting up the shared secret**




In the Server Configuration file example below, the APCON switch is set via the console, but any user with administrator rights can use any connection. If the change is from a connection other than the console, the user will likely need to log in after changing to the TACACS+ database.

**Note**

Although double quotes aren't used around the shared secret on the APCON switch, the double quotes may be needed in the configuration file.

```
console>> configure userauthentication
Authentication Method? [N]one, [I]nternal, [R]ADIUS, [T]ACACS+ [n/i/r/T/?]: T
TACACS+ servers:
Server 1
IP Address? [10.1.108.0]:
Shared Secret? [old]: Secret #1                <-> key = "Secret #1"
Enable a second server? [Y/n] Y
Server 2
IP Address? [10.1.100.50]:
Shared Secret? [old]: Secret #2
Enable a third server? [y/N] N
If server responds with no level? [D]eny access, [G]uest, [O]perator,
ad[V]anced, [A]dministrator [D/g/o/v/a]: D
```

## C.2.2. Apcon Access Levels and Service

You can assign these access levels to a user or group of users:

- `apcon_admin`
- `apcon_adv`
- `apcon_basic`
- `apcon_guest`

The server is configured to allow authorization for the user for the service `shell` and one of the APCON levels as a `cmd`.

## C.2.3. Assigning Authorization

| For information about... | Go to this page... |
|---|---|


### 11.2.0.1. User Authorization

The most basic configuration is assigning access levels directly to a user. This snippet of the TACACS+ Server Configuration file assigns advanced access to the user `clark` for all APCON switches:

```
user = clark {
  service = shell {}
  login = cleartext "clark-pw"
  cmd = apcon_adv {
    permit .*
  }
}
```

### 11.2.0.2. Group Authorization

The server likely supports users and groups belonging to groups. If a right isn't specified for a user or group, the server looks in groups that user or group belongs to.

This snippet of the TACACS+ Server Configuration file includes `apcon` permission in the group description:

```
group = user {
  service = shell {}
  cmd = apcon_basic {
    permit .*
  }
}
user = lois {
  login = des 5EFj8xcpfXY8U
  member = user
}
user = jimmy {
  login = cleartext "jimmy-pw"
  member = user
}
```

### 11.2.0.3. APCON Switch Authorization

You can use the `permit` and `deny` attributes to assign different authorization levels on different switches.

This snippet of TACACS+ Server Configuration file defines access for the user `phineas`:

```
group = user {
  service = shell {}
  cmd = apcon_basic {
    permit .*
  }
}
user = phineas {
  service = shell {}
  login = cleartext "phineas-pw"
  cmd = apcon_admin {
    permit 10\.1\.108\.0
  }
  cmd = apcon_adv {
    permit 10\.1\.108\.[0-9]*
  }
  member = user
}
```

The code defines the following access for `phineas`:

- Administrator access on the APCON switch with a primary IP address of 10.1.108.0.
- Advanced access on any other APCON switch with a 10.1.108.* primary IP address.
- Basic access on any other APCON switch, as a member of the `user` group.

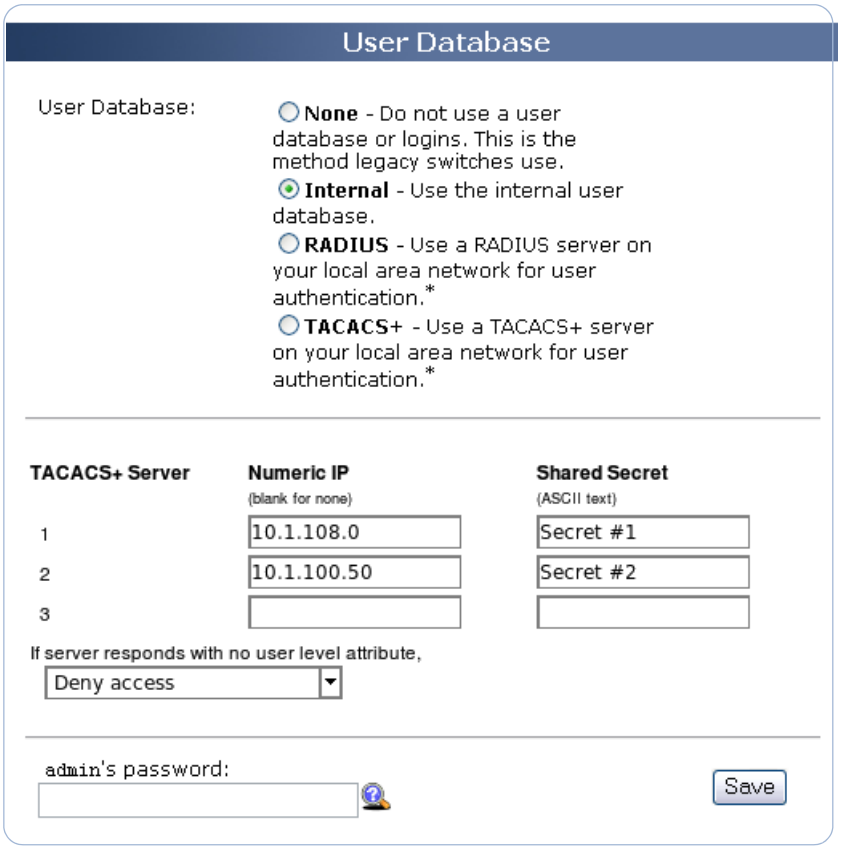
### 11.2.0.4. Unspecified Authorization

If a user is in the TACACS+ database but doesn't have an assigned APCON authorization level, that user receives the switch default. The default can deny access or assign the user a level, from guest to demonstrators.

You can set default action set to deny access using either of these:

- **WEBX**

**Figure 62. Setting up the shared secret**




- **Command line interface**

```
Six Corners>> configure userauthentication
Authentication Method? [N]one, [I]nternal, [R]ADIUS, [T]ACACS+ [n/I/r/t/?]: T
TACACS+ servers:
Server 1
IP Address? [10.1.108.0]:
Shared Secret? [Secret #1]:
Enable a second server? [Y/n] N
If server responds with no level? [D]eny access, [G]uest,
[O]perator,ad[V]anced, [A]dministrator [D/g/o/v/a]: D
```

# C.3. Accounting

The syslog handles the accounting or audit trail. You can configure the APCON switch to send audit event to up to three syslog servers.

By default, the messages from APCON switches are placed into /var/log/messages on the server(s). You can then redirect these messages either to a file specific to APCON switches or the file used by the TACACS+ server.

## C.3.1. Example: Routing Messages To TACACS+ Log

The next example redirects the messages to the TACACS+ server file. It assumes the TACACS+ server is configured to send its messages to /var/log/tacacs.

The syslog log redirects messages by service. All messages for a given service that exceed the specified threshold are rerouted to the file. The `local6` service was chosen because it unused on the local network. Your choice depends on services used by your network and supported by your syslog server.

**Note**

The syslog configuration syntax and location of files depends on the operating system and syslog on your servers. The server used in this example is the default syslog server running on Fedora 6 Linux.

Add the following two lines to /etc/syslog.conf on your servers.

```
# Route messages from Apcon switch
local6.=notice          /var/log/tacacs
```

This causes the message from service `local6` and a severity exactly matching notice to be sent to /var/log/tacacs. You must send a HUP signal to the syslog server so it will reread its configuration file.

You must configure the APCON switches to match the servers.You can configure APCON switches using either of these:

- **Command line**: The next example shows the syslog being configured from the command line interface. Typing a "?" for facility and severity displays the possible values.

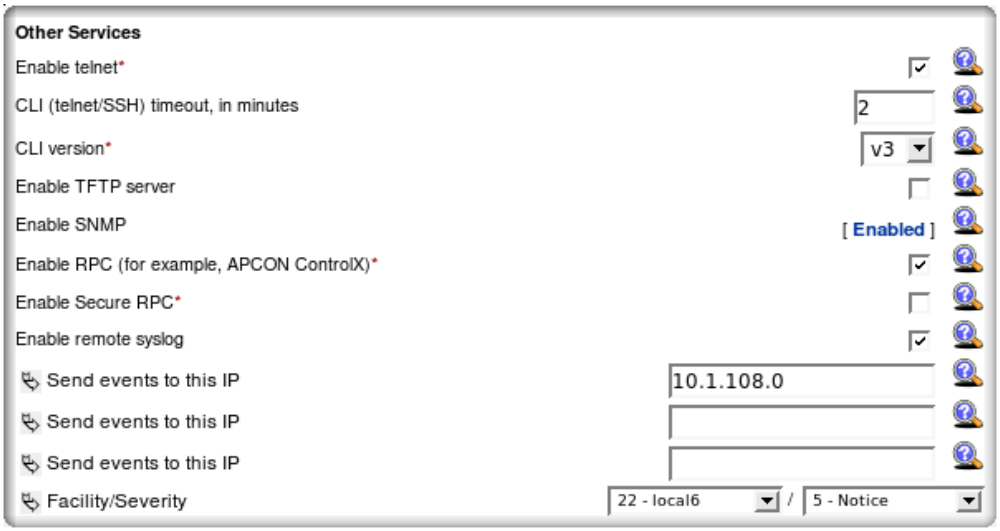
  **Note**

  The exact command syntax and file location depends on the version of syslog your server is running.

  ```
  Six Corners>> configure service syslog
  syslog servers:
  Server 1
  IP Address? [10.1.108.0]:
  Enable a second server? [Y/n] Y
  Server 2
  IP Address? [10.1.100.50]:
  Enable a third server? [y/N] N
  Facility? [22] (? for help): 22
  Severity? [5] (? for help): 5
  ```

- **WEBX**: This shows syslog on the APCON switch being configured to match the server above. The facility and severity are set to match the server. You access this screen by selecting Configure>Services.

**Figure 63. Configuring the syslog to match syslog server**



# Index

## R



## S

## T



## U