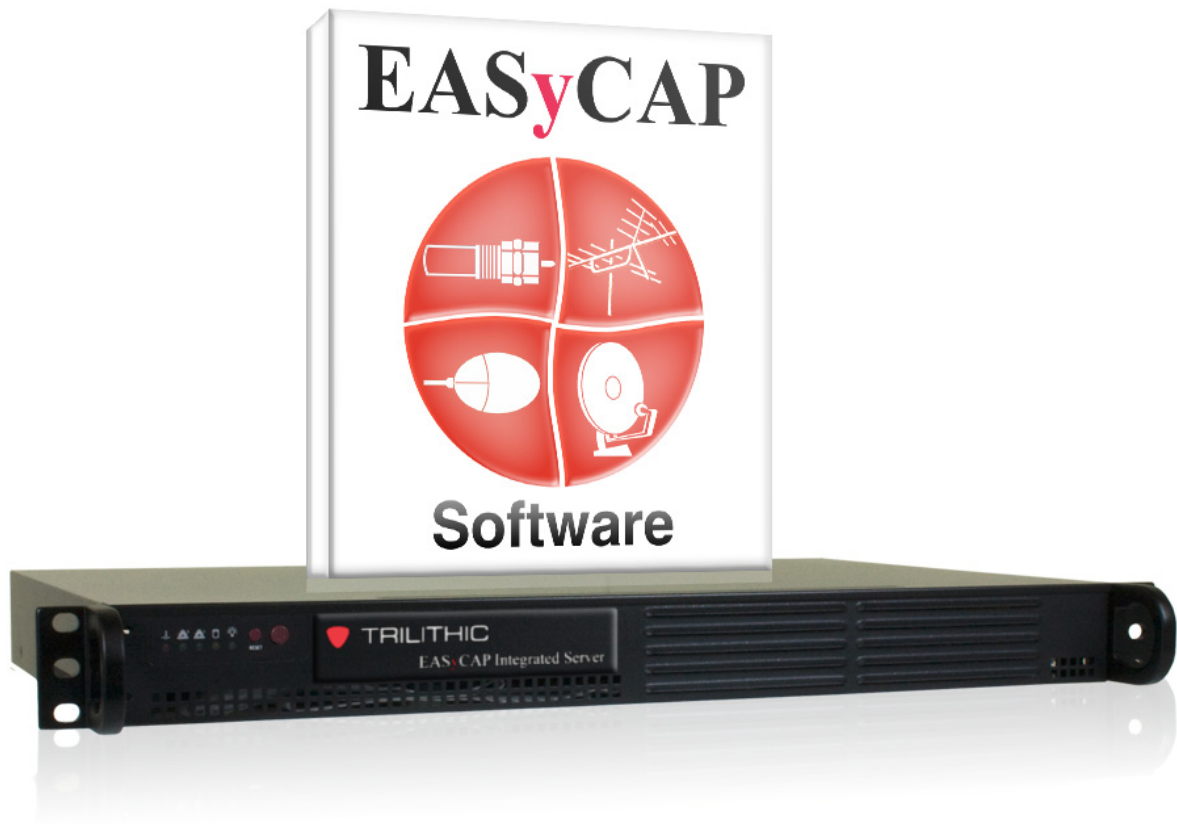


EASyCAP Integrated Server Package Version 1.20

Operation Manual



think ahead.

Trilithic Company Profile

Trilithic is a privately held manufacturer founded in 1986 as an engineering and assembly company that builds and designs customer-directed products for telecommunications, military, and industrial customers. From its modest beginnings as a two-man engineering team, Trilithic has grown over the years and broadened its offerings of RF and microwave components by adding broadband solutions to its product line. This was accomplished with the acquisition of components manufacturer Cir-Q-Tel and instruments manufacturer Texscan.

Today, Trilithic is an industry leader, providing telecommunications solutions for major broadband, RF and microwave markets around the world. As an ISO 9000:2001 certified company with over 40 years of collective expertise in engineering and custom assembly, Trilithic is dedicated to providing quality products, services and communications solutions that exceed customer expectations.

Trilithic is comprised of five major divisions:

- **Broadband Instruments and Systems**
Offers test, analysis, and quality management solutions for the major cable television systems worldwide.
- **RF Microwave Components**
Provides components and custom subsystems for companies specializing in cellular, military, and other wireless applications.
- **Emergency Alert Systems**
Leading supplier of government-mandated emergency alert systems used by broadcast TV, cable TV, IPTV, DBS, and radio stations.
- **XFTP**
Offers a specialty line of field technical products for cable operators and technicians, as well as a line of products for installing electronics in the home of the future.

THIS PAGE LEFT INTENTIONALLY BLANK

Table of Contents

1. General Information	5
Helpful Website	5
Where to Get Technical Support	5
How this Manual is Organized	6
Conventions Used in this Manual	7
2. EASyCAP Server Overview	9
What is the EASyCAP Integrated Server?	9
What Does the EASyCAP Integrated Server Do?	10
Installation Prerequisites	11
Hardware Features	12
Operating System	13
Default IP Configuration	13
Linux Console	13
Secure Shell (SSH) Access	13
Hardware Overview	14
Control Panel	15
I/O Panel	16
3. EASyCAP Server Configuration	17
System Login	17
EASyCAP User Interface Homepage	18
Administration	19
User Accounts	19
Upgrade	21
Reboot	21
CAP Configuration	22
CAP Audio & Text Options	22
Selected States	23
IPAWS Atom Feed	24
TCP Feed	26
Configuration	28
Date/Time	28
Network Configuration	29
IP Message Delivery	34
Logs	36
Alert Log	37
System Log	37

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 1

General Information

Helpful Website

The following website contains general information which may be of interest to you:

<http://www.trilithic.com>

Trilithic's website contains product specifications and information, tips, release information, marketing information, Frequently Asked Questions (FAQs), bulletins, and other technical information. You can also check this website for product updates.

Where to Get Technical Support

Trilithic technical support is available Monday through Friday from 8:00AM to 5:00PM EST. Callers in North America can dial 1-317-895-3600 or 1-800-344-2412 (toll free). International callers should dial 1-317-895-3600 or fax questions to 1-317-895-3613. You can also e-mail technical support at EASysupport@trilithic.com.

For quicker support response when calling or sending e-mail, please provide the following information:

- Your name and your company name.
- The technical point of contact (name, phone number, e-mail address).
- The EASyCAP server software's version number.
- A detailed description of the problem you are having, including any error or information messages.

How this Manual is Organized

This manual is divided into the following chapters:

- Chapter 1, “General Information,” provides Trilithic contact information and describes how this operation manual is structured.
- Chapter 2, “EASyCAP Server Overview” gives an overview of the EASyCAP Server hardware and how it works.
- Chapter 3, “EASyCAP Server Configuration” describes the steps necessary to configure the EASyCAP Server.

Conventions Used in this Manual

This manual has several standard conventions for presenting information.

- Connections, menus, menu options, and user entered text and commands appear in **bold**.
- Section names, web, and e-mail addresses appear in *italics*.



A **NOTE** is information that will be of assistance to you related to the current step or procedure.



A **CAUTION** alerts you to any condition that could cause a mechanical failure or potential loss of data.



A **WARNING** alerts you to any condition that could cause personal injury.

THIS PAGE LEFT INTENTIONALLY BLANK

EASyCAP Server Overview

What is the EASyCAP Integrated Server?

The EASyCAP™ Integrated Server supports IPAWS CAP on EASyPLUS™, EASyCAST™, and EASyIPTV™ systems. The software is used as an intermediary between Trilithic encoder/decoders and Common Alerting Protocol (CAP) sources.

EASyCAP Software is everything you need to be CAP-IPAWS compliant with your EASy Series Encoder/Decoders. With the EASyCAP Software, you can receive CAP alerts from multiple sources.

- Monitors Multiple CAP Sources
- Supports Multiple EASy Series EAS Systems Simultaneously
- Supports CAP Text and Audio
- Complete Network-Based Solution, No Need for Audio Connections

What Does the EASyCAP Integrated Server Do?

The EASyCAP Integrated Server can support multiple EASy Series Encoder/Decoder systems. CAP alerts and audio are delivered to the EASyPLUS, EASyCAST, or EASyIPTV across a network connection (via TCP port), fully supporting CAP text and MP3 audio. CAP alerts are queued by the system until the EASy Series Encoder/Decoders can process the CAP alerts. Additional interfaces will become available for receiving CAP alerts as they are defined and required by FEMA, the FCC, individual states, or individual operators.

The EASyCAP Integrated Server Package is designed for users who need a server. The integrated package consists of a small 1U Linux-based server with EASyCAP Software pre-loaded. An intuitive Web Server is provided to allow for management and configuration of the system and software. (The Linux software is only offered with the integrated server, it is not sold separately). Each Encoder/Decoder must have a Trilithic EASyNIC Ethernet card installed and be licensed to receive EASyCAP alerts.



Installation Prerequisites

The following prerequisites must be met before being able to access the EASyCAP Integrated Server:

- **Network Connection** - The EASyCAP Integrated Server must be on a network where CAP feeds are available and it must also have network connectivity to the EASy Series Encoder/Decoder. Two different network configurations are possible as follows:
 - **Single Network Connection** - If both the EASyCAP Integrated Server and EASy Series Encoder/Decoder are on the same network (or subnet) only a single Ethernet connection to the network should be used. In this configuration **DO NOT** use the second Ethernet port, otherwise TCP/IP communications will be unreliable.
 - **Dual Network Connection** - If the EASyCAP Integrated Server and EASy Series Encoder/Decoder are on two different networks (or subnets) both Ethernet connections to the network must be used. In this configuration each Ethernet port is assigned to a different network (or subnet).
- **Web Browser** - The user interface for the EASyCAP Integrated Server uses a secure web server (HTTPS) over port 443. Trilithic recommends using the Mozilla Firefox (V3.6 or newer) web browser.

Hardware Features

The EASyCAP Integrated Server includes the following standard hardware:

Motherboard - The EASyCAP Integrated Server includes a single processor, low-power motherboard based upon Intel's ATOM D510 + ICH9R chipset.

Processor - Includes one Intel® Atom™ D510 Dual-core 1.66 GHz processor. The processor is embedded into the motherboard.

Memory - Includes two DIMM slots that can support up to 4 GB of non-ECC DDR2-667 SDRAM.

Onboard SATA - A SATA controller is built in to the ICH9R portion of the chipset to provide support for a six port, 3 Gb/sec Serial ATA subsystem.

PCI Expansion Slots - Includes one PCI-Express x4 slot (in a x16 slot).

Onboard Controllers/Ports - Onboard I/O backpanel ports include one COM port, a VGA port, PS/2 mouse and keyboard ports, two Gb Ethernet ports and two USB ports. In addition, an extra COM port and USB ports are included on the motherboard.

Onboard Graphics - A Matrox G200eW graphics/video controller is integrated into the motherboard.

Operating System

The EASyCAP Integrated Server uses Ubuntu Linux as its operating system. A Linux user account is setup for advanced configuration and troubleshooting of the operating system. This account is only used when accessing the Ubuntu Linux operating system. The methods shown in the following sections can be used to access the Ubuntu Linux operating system.

The default username and password are as follows:

Username: eas

Password: eas

Default IP Configuration

The default configuration for **LAN 1 (eth0)** is as follows:

IP Address: 192.168.1.101

Subnet Mask: 255.255.0.0

The default configuration for **LAN 2 (eth1)** is as follows:

IP Address: 10.1.65.101

Subnet Mask: 255.255.0.0

Linux Console

A Linux console can be accessed using the RS-232 serial port at a fixed BAUD rate of 115.2K. Use a null modem cable when connecting the EASyCAP Integrated Server to another computer. The Linux console can be useful for first-time Network setup, but the user will need to be familiar with configuring Network settings using Ubuntu Linux.

Secure Shell (SSH) Access

Secure Shell (SSH) access to the EASyCAP Integrated Server is available. This interface allows a user to login to Linux for lower level configuration or maintenance. Many SSH software clients are available for free, PUTTY is a common client used for SSH sessions using a Windows based computer.

Hardware Overview



Front View



Rear View

1. **Control Panel** - This provides important system monitoring and control information. LEDs indicate power on, network activity, hard disk drive activity and system overheat. The control panel also includes a main power button and a system reset button.
2. **AC Line Input** - This is used to connect the included line cord to an AC input voltage of 100-240 VAC (auto-range) with a maximum current of 3A and rated frequency of 50 to 60 Hz.
3. **I/O Panel** - This provides one COM port, two USB ports, PS/2 mouse and keyboard ports, a graphics port and two Gb Ethernet ports.



NOTE

The EASyCAP Integrated Server is not intended to be operated with a keyboard/mouse and monitor attached.

4. **PCIe Expansion Slot** - This provides the ability to install a one full-height, half-length PCIe expansion card (not included).

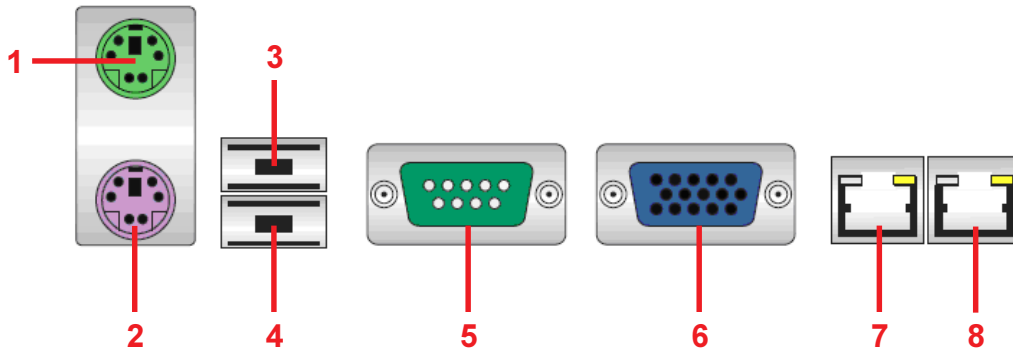
Control Panel

There are several LEDs on the control panel to keep you constantly informed of the overall status of the system as well as the activity and health of specific components. There are also two buttons on the control panel. This section explains the meanings of all LED indicators and the appropriate response you may need to take.



1. **Overheat Indicator** - When this LED is on it indicates an overheat condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. You should also check to make sure that the chassis covers are installed. This LED will remain on as long as the indicated condition exists.
2. **Network 2** - When flashing, this LED Indicates network activity on **LAN 2 (eth1)**.
3. **Network 1** - When flashing, this LED Indicates network activity on **LAN 1 (eth0)**.
4. **Hard Disk Drive** - This LED indicates channel activity for all HDDs. This light indicates IDE or SATA drive activity when flashing.
5. **Power** - This LED Indicates power is being supplied to the system's power supply units. This LED should normally be illuminated when the system is operating.
6. **Reset Button** - This button is used to reboot the server.
7. **Power Button** - This is the main power button, which is used to apply or turn off the main system power. Turning off system power with this button removes the main power but keeps standby power supplied to the system. If you need to service the system you should unplug the AC power cord after shutting down the server.

I/O Panel



1. **Mouse** - This port is used to connect a PS/2 mouse to the server.
2. **Keyboard** - This port is used to connect a PS/2 keyboard to the server.
3. **USB 1** - This port is used to connect a USB device to the server.
4. **USB 2** - This port is used to connect a USB device to the server.
5. **COM 1** - This port is used to connect a Serial RS-232 device to the server.
6. **VGA** - This port is used to connect a VGA monitor to the server.
7. **LAN 1 (eth0)** - This port is used to connect the server to a local area network (LAN).
8. **LAN 2 (eth1)** - This port is used to connect the server to a second local area network (LAN) that is a different network (or subnet) than the network connected to **LAN 1 (eth0)**.



NOTE

The EASyCAP Integrated Server is not intended to be operated with a keyboard/mouse and monitor attached.

EASyCAP Server Configuration

System Login

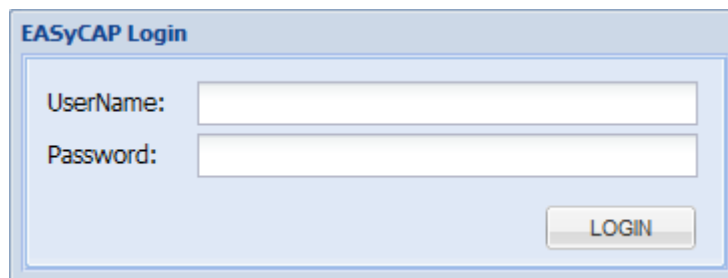
The user interface for the EASyCAP Integrated Server uses a secure web server (HTTPS) over port 443. Trilithic recommends using the Mozilla Firefox (V3.6 or newer) web browser.

The certificate used by the EASyCAP Integrated Server is not signed by a trusted certificate authority (VeriSign, etc) so web browsers will automatically display a security alert about the certificate the first time you connect. At this point, acknowledge the security alert and continue to the site even though the certificate isn't trusted.

When using Mozilla Firefox (V3.6 or newer), the web browser will retain the security setting for the next time you connect to the server. However, if you are using Internet Explorer, the security alert will be displayed every time that you connect to the web server. To disable this, you must install the Trilithic certificate onto your PC. This can be done by clicking on the Certificate Error message (next to the URL), then click "View certificates", and finally press the "Install Certificates" button.

Perform the following steps to login to the EASyCAP Integrated Server:

1. Enter https:// followed by the IP address of the EASyCAP Integrated Server into the URL bar of the web browser and then press **Enter** on your keyboard.
2. The login screen will appear as shown below.

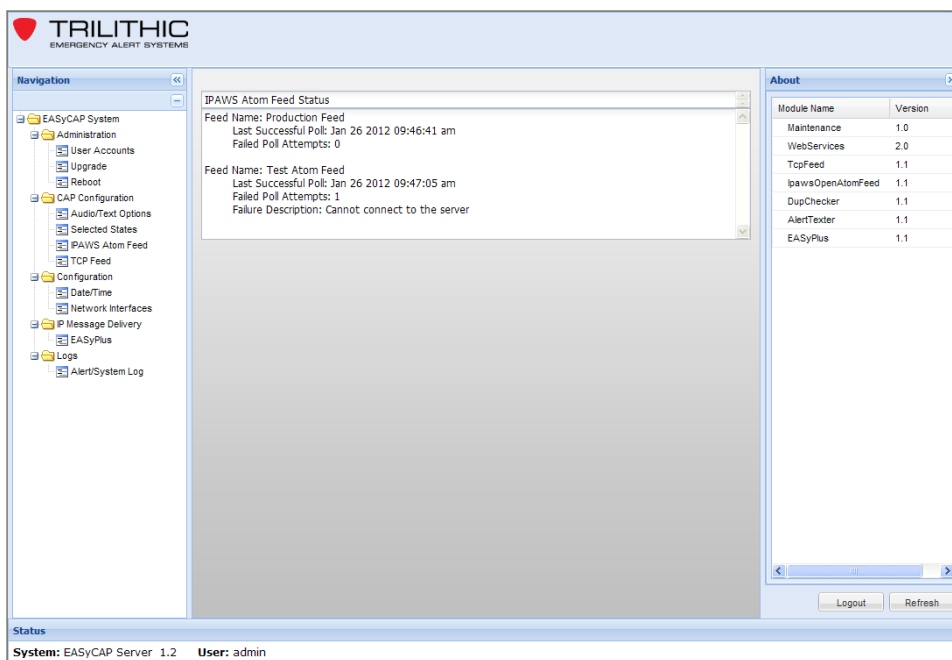


The image shows a screenshot of a web browser window titled "EASyCAP Login". The window has a light blue border and contains two text input fields. The first field is labeled "UserName:" and the second is labeled "Password:". Below the password field is a button labeled "LOGIN".

3. Enter the username and password for the desired user account and then select the **OK** button. The factory default user account has a username and password of **Administrator**.
4. The EASyCAP user interface homepage will appear.

EASyCAP User Interface Homepage

After logging into the system, the homepage will be displayed as shown below.



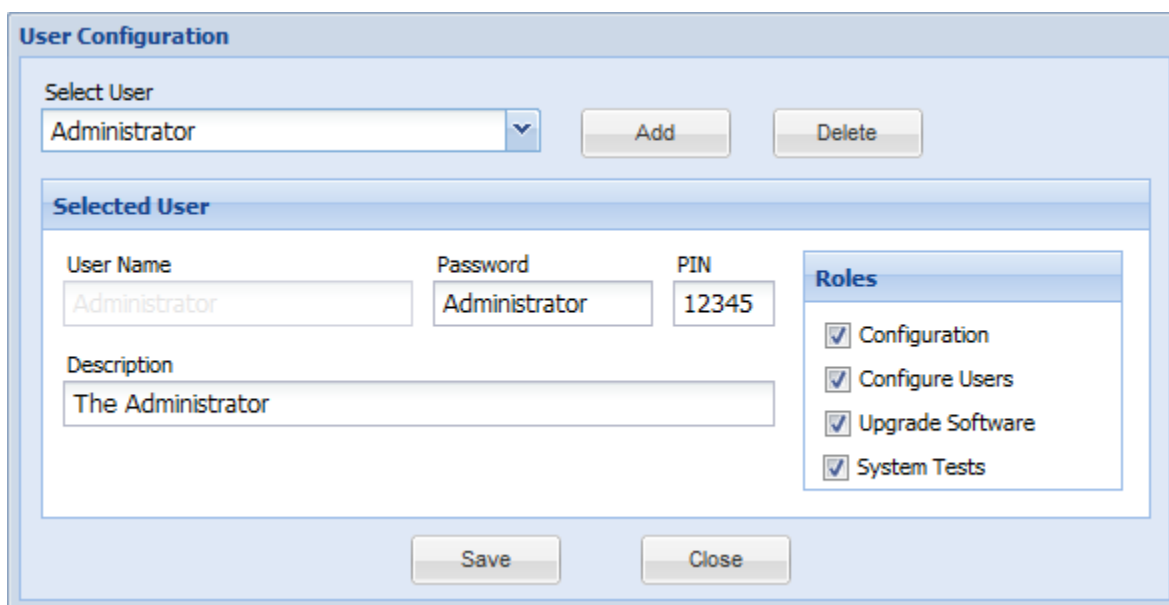
The following items can be viewed from from the homepage:

- **Navigation** - This area is used to navigate to each of the configuration pages. The configuration pages are sorted into categories according to function; **Administration**, **CAP Configuration**, **Configuration**, **IP Message Delivery**, and **Logs**. Select the plus (+) sign to expand a category and select the minus (-) sign to collapse a category. To view a configuration page, select the corresponding link.
- **About** - This area is used to display the name and version of each Module within the EASyCAP server.
- **Status** - This area is used to display the EASyCAP server version number and the user that is currently logged on.
- **Logout** - This button is used to logout of the system.
- **IPAWS Atom Feed Status** - This area shows the status of all configured IPAWS Atom feeds, and can be used to determine if one of the feeds is not operating properly. Press the **Refresh** button to update the status of the IPAWS Atom Feeds.

Administration

User Accounts

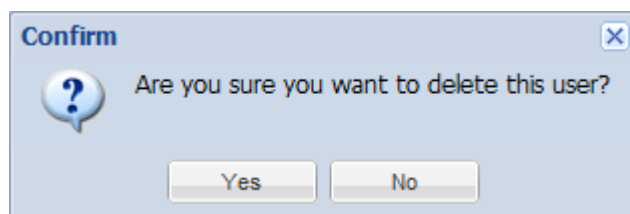
To setup the user accounts for the server, select the **User Accounts** link. The **User Configuration** page will be displayed as shown below.



The **User Configuration** dialog box is shown. It features a 'Select User' dropdown menu with 'Administrator' selected, and 'Add' and 'Delete' buttons. Below this is a 'Selected User' section with input fields for 'User Name' (Administrator), 'Password' (Administrator), 'PIN' (12345), and 'Description' (The Administrator). To the right is a 'Roles' section with four checked checkboxes: 'Configuration', 'Configure Users', 'Upgrade Software', and 'System Tests'. At the bottom are 'Save' and 'Close' buttons.

To view the settings of a user account, use the **Select User** dropdown list to select the desired user.

- Select the **Add** button to create a new user account. Modify the user information as described in the following section and then select the **Save** button to save the user account settings.
- Select the **Delete** button to delete the selected user account. A confirmation page will prompt you before deleting the user account as shown below. Select the **Yes** button to delete the user account or select the **No** button to exit without deleting the user account.



The **Confirm** dialog box is shown with a question mark icon and the text 'Are you sure you want to delete this user?'. It has 'Yes' and 'No' buttons at the bottom.

User Settings

Once the User Account has been selected, any of the following settings can be modified:

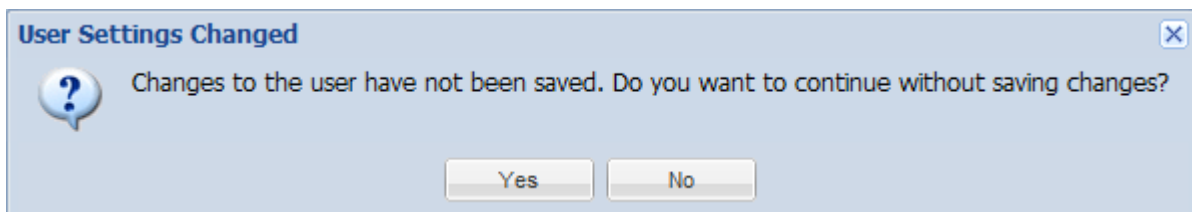
- **User Name** - Enter the user name for the User Account into this field. This field cannot be changed after saving the user account. To change the user name in the future, simply delete the account and create a new account.
- **Password** - Enter the password for the User account into this field.
- **PIN** - Enter the PIN (Personal Identification Number) for the User account into this field. The PIN must be between 4 and 8 digits (numeric digits only) and must be unique.
- **Description** - Enter the description that you wish to display for this user account. This description should be detailed enough to be able to easily discern it within the User Account List.

Roles

To set the role of the User Account select any one of the following checkboxes.

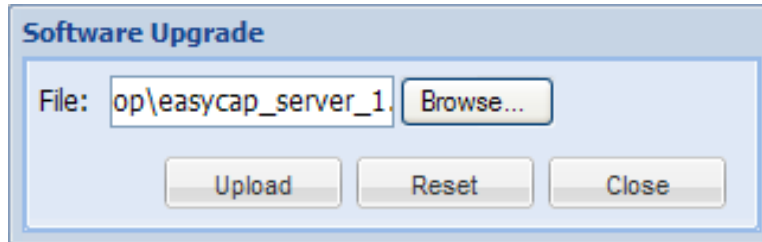
- **Configuration** - This role allows the user to make changes to the configuration of the EASyCAP Server.
- **Configure Users** - This role allows the user to make changes to all user accounts. Note that any user can change their own password and PIN at any time regardless of their own user account role.
- **Upgrade Software** - This role allows the user to upgrade the EASyCAP Server software.
- **System Tests** - This role allows users to perform calibration and system tests.

After making changes, select the **Save** button to save the User Account settings. If you have made changes and have selected the **Close** button, a confirmation page will prompt you before closing. Select the **No** button to return to the **User Configuration** page or select the **Yes** button to exit without saving the changes to the User Account.



Upgrade

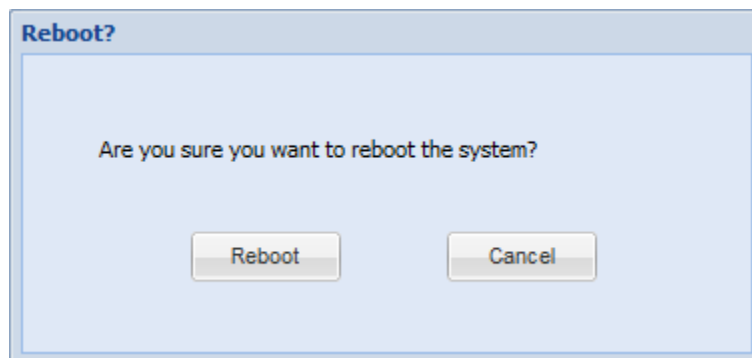
To upgrade the EASyCAP server software, select the **Upgrade** link. The **Software Upgrade** page will be displayed as shown below.



To upgrade the EASyCAP server software, select the **Browse** button. An **Open** dialog box will appear. Choose the upgrade file and then select the **Upload** button to upgrade the software or select the **Close** button to exit without upgrading. The **Reset** button is used to reset the EASyCAP Server after performing an upgrade. Always reset the unit after upgrading the software.

Reboot

To reboot the EASyCAP server, select the **Reboot** link. Select the **Reboot** button to reboot the EASyCAP server or select the **Cancel** button to exit without rebooting the EASyCAP server.



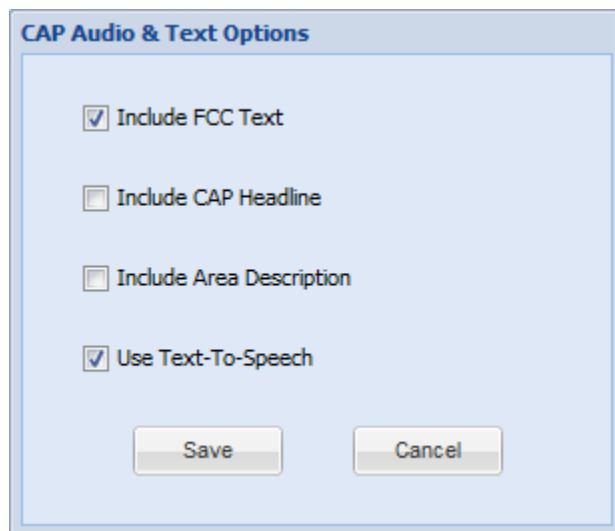
CAP Configuration

CAP Audio & Text Options

To setup the CAP audio and text settings for CAP messages, select the **Audio/Text Options** link. The **CAP Audio & Text Options** setup page will be displayed as shown to the right.

The **CAP Audio & Text Options** setup page is used to configure which additional elements are included in the alert. Select from the following check boxes.

- **Include FCC Text** - When this box is selected, the EAS Header Translation will be included in the alert text. This box should always be selected unless the FCC agrees to drop the requirement for this text to be sent.
- **Include CAP Headline** - When this box is selected, the CAP Headline will be included in the alert text. Trilithic recommends that this box should not be selected.
- **Include Area Description** - When this box is selected, the CAP Area Description will be included in the alert text. Trilithic recommends that this box should not be selected.
- **Use Text-to-Speech** - When this box is selected, the EASyCAP software will generate speech from the text included in the CAP message (and from the EAS Header Translation if enabled). This will only generate audio from text if the CAP message does not include English audio. This option only supports English audio.



NOTE

NOTE: Per the FCC's 5th Report and Order (Jan 2012) this Text to Speech option must be turned off. The option remains in the event that waivers are granted or the decision is reversed.

After making changes, select the **Save** button to save the CAP audio and text settings or select the **Cancel** button to exit without saving the changes to the CAP audio and text settings.

Selected States

To choose the states serviced by your system, select the **Selected States** link. The **Selected States** setup page will be displayed as shown below.

Available States and Areas	
State	FIPS
<input type="checkbox"/>	ALABAMA 001000
<input type="checkbox"/>	ALASKA 002000
<input type="checkbox"/>	ARIZONA 004000
<input type="checkbox"/>	ARKANSAS 005000
<input type="checkbox"/>	CALIFORNIA 006000
<input type="checkbox"/>	COLORADO 008000
<input type="checkbox"/>	CONNECTICUT 009000
<input type="checkbox"/>	DELAWARE 010000
<input type="checkbox"/>	DC 011000
<input type="checkbox"/>	FLORIDA 012000
<input type="checkbox"/>	GEORGIA 013000
<input type="checkbox"/>	HAWAII 015000
<input type="checkbox"/>	IDAHO 016000
<input type="checkbox"/>	ILLINOIS 017000
<input type="checkbox"/>	INDIANA 018000
<input type="checkbox"/>	IOWA 019000

Selected States	
State	FIPS
<input type="checkbox"/>	INDIANA 018000
<input type="checkbox"/>	IDAHO 016000
<input type="checkbox"/>	ARKANSAS 005000

Save Cancel

The **Selected States** setup page is used to configure which CAP messages are processed, based on the areas affected by the alert. The IPAWS Atom Feed includes alerts for the entire United States, the selected States are used to determine which alerts need to be processed. Warning: if no states are selected, no alerts will be processed.

Adding States

From the **Available States and Areas** display area, select the checkbox(s) that corresponds to the state(s) that you wish to add. Add the states to the **Selected States** display area by selecting the right arrow button.

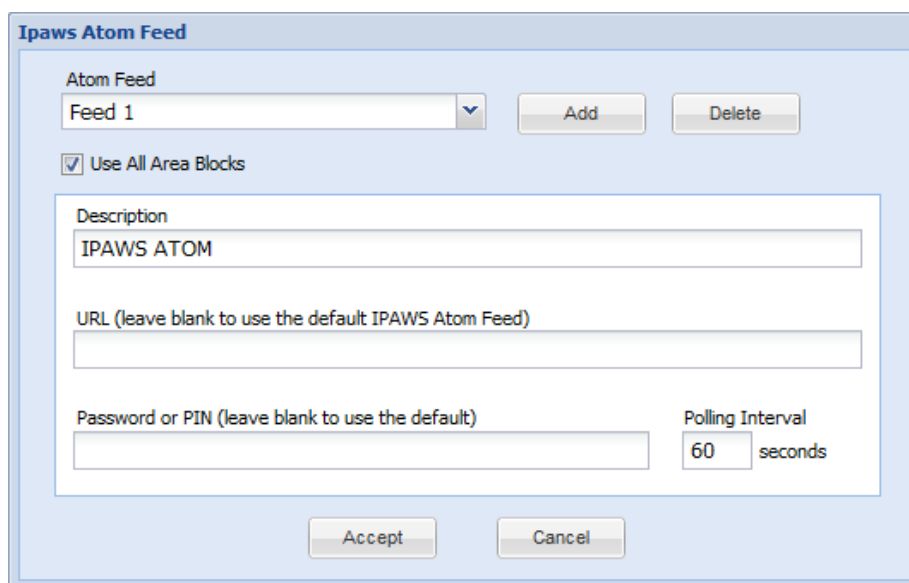
Removing States

From the **Selected States** area, select the checkbox(s) that correspond to the state(s) that you wish to remove. Remove the states from the **Selected States** display area by selecting the left arrow button.

After making changes, select the **Save** button to save the selected states settings or select the **Cancel** button to exit without saving the changes to the selected states settings.

IPAWS Atom Feed

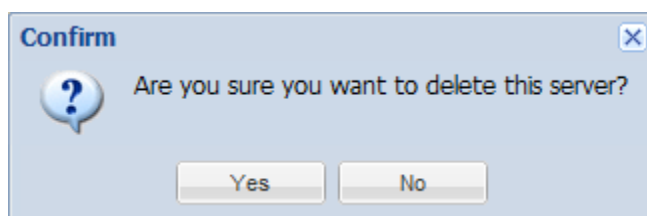
To setup the IPAWS Atom feeds, select the **IPAWS Atom Feed** link. The **IPAWS Atom Feed** setup page will be displayed as shown below.



The screenshot shows a dialog box titled "Ipaws Atom Feed". At the top, there is a dropdown menu labeled "Atom Feed" with "Feed 1" selected. To the right of the dropdown are "Add" and "Delete" buttons. Below the dropdown is a checked checkbox labeled "Use All Area Blocks". The main area contains three input fields: "Description" with the text "IPAWS ATOM", "URL (leave blank to use the default IPAWS Atom Feed)" which is empty, and "Password or PIN (leave blank to use the default)" which is empty. To the right of the password field is a "Polling Interval" section with a text box containing "60" and the label "seconds". At the bottom of the dialog are "Accept" and "Cancel" buttons.

To view the settings of a IPAWS Atom Feed, use the **Atom Feed** dropdown list to select the desired Atom feed.

- Select the **Add** button to add a new Atom feed. Modify the feed settings as described in the following section and then select the **Save** button to save the Atom feed settings.
- Select the **Delete** button to delete the selected Atom Feed. A confirmation page will prompt you before deleting the Atom Feed. Select the **Yes** button to delete the Atom feed or select the **No** button to exit without deleting the Atom feed.



The screenshot shows a small dialog box titled "Confirm" with a close button (X) in the top right corner. On the left is a question mark icon. The text in the center reads "Are you sure you want to delete this server?". At the bottom are two buttons: "Yes" and "No".

Feed Settings

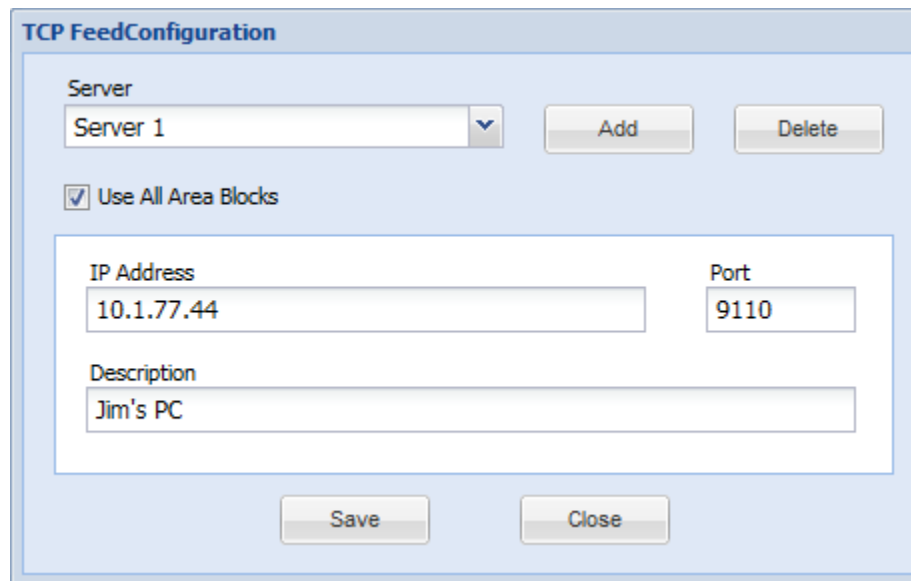
Once the Atom feed has been selected, any of the following settings can be modified:

- **Description** - Enter a description for this feed.
- **Use All Area Blocks** - When this box is selected, this allows processing of all the <area> blocks within a CAP message. If off (unchecked), only the first <area> block will be processed. This option should be left off (unchecked) in order to comply with current CAP to EAS implementation guidelines.
- **URL** - Enter the URL of the IPAWS Atom Feed into this field. Leave blank to use the default IPAWS Atom Feed URL.
- **Password or PIN** - Enter the password or PIN assigned by the CAP source administrator. Leave blank to use the default IPAWS Atom feed.
- **Polling Interval** - Enter the amount of time in seconds between each request for new CAP messages.

You can change the settings for multiple Atom feeds before accepting (and saving) the changes. Once your done configuring the Atom feeds, press the **Accept** button to save all of the changes made or select the **Cancel** button to exit without saving the changes to the Atom feed settings.

TCP Feed

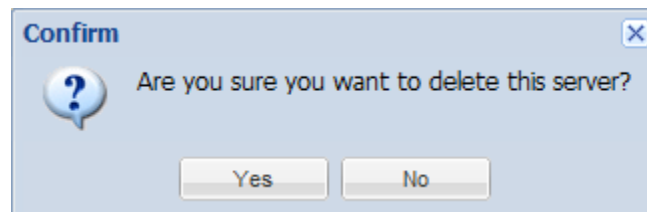
To setup the TCP feeds for the server, select the **TCP Feed** link. The **TCP Feed Configuration** setup page will be displayed as shown below.



The screenshot shows a dialog box titled "TCP FeedConfiguration". It features a "Server" dropdown menu with "Server 1" selected, and "Add" and "Delete" buttons. A checked checkbox labeled "Use All Area Blocks" is present. Below this is a form with three fields: "IP Address" containing "10.1.77.44", "Port" containing "9110", and "Description" containing "Jim's PC". At the bottom are "Save" and "Close" buttons.

To view the settings of a TCP Feed, use the **Server** dropdown list to select the desired server.

- Select the **Add** button to add a new TCP Feed. Modify the feed settings as described in the following section and then select the **Save** button to save the TCP feed settings.
- Select the **Delete** button to delete the selected TCP Feed. A confirmation page will prompt you before deleting the TCP feed. Select the **Yes** button to delete the TCP feed or select the **No** button to exit without deleting the TCP feed.



The screenshot shows a "Confirm" dialog box with a question mark icon. The text reads "Are you sure you want to delete this server?". At the bottom are "Yes" and "No" buttons.

Feed Settings

Once the TCP feed has been selected, any of the following settings can be modified:

- **Use All Area Blocks** - When this box is selected, this allows processing of all the <area> blocks within a CAP message. If off (unchecked), only the first <area> block will be processed. This option should be left off (unchecked) in order to comply with current CAP to EAS implementation guidelines.
- **IP Address** - Enter the IP Address of the TCP feed into this field.
- **Port** - Enter the TCP port number.
- **Description** - Enter the description that you wish to display for this feed. This description should be detailed enough to be able to easily discern it from other configured feeds.

After making changes, select the **Save** button to save the TCP feed settings or select the **Cancel** button to exit without saving the changes to the TCP feed settings.

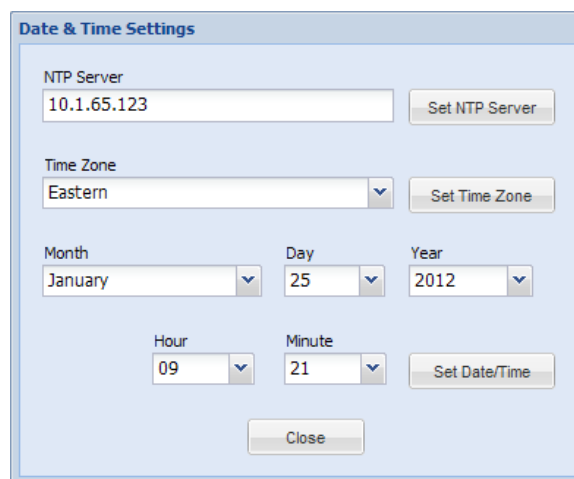
Configuration

Date/Time

To adjust the date and time settings of the server, select the **Date/Time** link. The **Date/Time** setup page will be displayed as shown to the right.

The following settings can be adjusted:

- **NTP Server** - Enter the URL or IP address of the Network Time Protocol connection to the server. Select the **Set NTP Server** button to save the changes to the NTP Server.
- **Time Zone** - Select the time zone from the dropdown list. Select the **Set Time Zone** button to save the changes to the time zone.
- **Month** - Select the current month from the dropdown list.
- **Day** - Select the current day from the dropdown list.
- **Year** - Select the current year from the dropdown list.
- **Hour** - Select the current hour from the dropdown list.
- **Minute** - Select the current minute from the dropdown list.



After making changes, select the **Set Date/Time** button to save the date and time settings. Select the **Close** button to close this window.



During initial configuration time and date should be set manually. Afterwards, if an NTP server is configured the date and time will automatically synchronize with the NTP server.

Network Configuration



CAUTION

Regardless of the network settings of the EASyCAP Integrated Server, a properly firewalled connection to the Internet is critical for the safe operation of this equipment. In addition, use of a reputable Internet provider and DNS Service may minimize risks associated with Internet access.

To setup the network interfaces of the server, select the **Network Interfaces** link. The **Network Configuration** page will be displayed as shown to the right.

The EASyCAP Integrated Server must be configured for network connectivity that allows Internet access to retrieve CAP messages and TCP access to each EAS Encoder/Decoder served. In addition the EASyCAP server provides an HTTPS server for configuration, so an inbound connection on port 443 will be necessary at least part of the time. Two basic network configurations are possible as follows:

- **Single Network Connection** - The EASyCAP Integrated Server may be configured with one of it's Ethernet ports disabled, relying on the system/station network for all connections to the Internet, EAS Encoder/Decoders, and the web client (for configuration). In this configuration, the internal network is responsible for any necessary routing and security. In a very simple network of this kind, a router/gateway would allow outbound connectivity to the Internet while the Encoder/Decoder(s) and a Web Client PC would be on the same IP subnet as the EASyCAP Integrated Server and therefore directly accessible.
- **Dual Network Connection** - The EASyCAP Integrated Server may be configured with both Ethernet interfaces enabled allowing (typically) one interface to be used to access the Internet, while the other interface is used to access EAS Encoder/Decoder(s) and a web client (for configuration). In this configuration one interface may be configured with a default gateway pointing to an Internet router, while the other interface is either on the same subnet with the EAS Encoder/Decoder(s), or is configured with a (narrow) gateway to the EAS Encoder/Decoder(s).



Two Ethernet Interfaces are provided. Ethernet 1 in the Web GUI configures eth0 in the Operating System. Ethernet 2 in the Web GUI configures eth1.

Global Network Settings

The following Global Network Settings can be adjusted:

- **Host Name** - Enter the host name of the EASyCAP server in this field.
- **DNS Server 1** - Enter the primary DNS server address in this field.
- **DNS Server 2** - Enter the secondary DNS server address in this field.

Network Interface Settings

The following settings can be adjusted for each network interface:

- **Disable Interface** - Select this checkbox to disable this port when only using one Ethernet connection. When this check box is selected configuration fields will be grayed out, and cannot be manually adjusted.
- **Use DHCP** - Select this checkbox to enable DHCP to automatically assign the IP Address, Subnet, and Gateway of the server. When this check box is selected these fields will be grayed out and cannot be manually adjusted.



Use of DHCP on either interface may result in IP and gateway conflicts with the other interface, DNS conflicts, and other conflicts and ambiguities resulting in unreliable communication on both interfaces. In addition, use of DHCP will enable the configuration HTTPS interface on both interfaces, regardless of the Allow Web Server settings for the interfaces.

- **IP Address** - Enter the IP address that the Interface should use. IP Addresses should be unique on any given network. The IP address and subnet mask together specify the interfaces subnet.
- **Subnet Mask** - Enter the subnet mask for the interface. Together with the IP address, this determines the subnet of the interface. Typical values for subnet mask include 255.255.255.0 (255 addresses are directly accessible) and 255.255.0.0 (65025 addresses are directly accessible). IP Addresses that are not directly accessible to an interface will be routed through the narrowest gateway available.
- **MAC Address** - This displays the MAC address of the network interface.
- **Disable Gateway** - Selecting this option disables the Gateway on the interface, allowing only peer to peer connections on the same subnet.
- **Default Gateway** - Selecting this option enables this interfaces gateway to be used for communications that do not match the other interfaces subnet or masked gateway. Selecting this option on both interfaces will result in unreliable communications.
- **Gateway** - This setting is used to specify the address of a router used to communicate to IP addresses that are not part of the local subnet(s). In conjunction with the Default Gateway and Network Mask settings, any IP address that does not match either interfaces subnet will be directed to the narrowest matching gateway address. The Gateway IP address must be within the subnet defined using the IP Address and Subnet Mask settings.

- **Network Mask** - This setting, in conjunction with the Gateway address determines what IP Address range will be sent through the gateway. This is used in dual-gateway configurations. Generally, the interface facing the Internet will have the Default Gateway option enabled, and the interface facing the EAS Encoder/Decoders will either have the gateway disabled, or have a narrow Network Mask allowing use of an internal gateway for a limited number of IP addresses. For example:

Ethernet 1 - used to access the Internet

IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Gateway 192.168.1.1
Default Gateway Enabled

Ethernet 2 - used to access 2 separate Encoder/Decoders

IP Address 10.1.20.10
Subnet Mask 255.255.255.0
Gateway 10.1.20.1
Network Mask 255.255.0.0 (allows all 10.1.x.x addresses)

EAS Encoder 1

IP Address 10.1.20.100
Is on the same subnet as Ethernet 2
EASyCAP Server talks directly to EAS Encoder 1

EAS Encoder 2

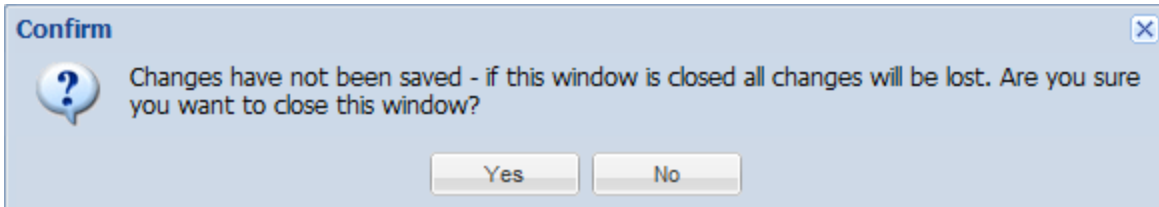
IP Address 10.1.1.27
Is not on the same subnet as the EASyCAP Server
Is connected on the other side of the router
EASyCAP Server sends traffic through the router at 10.1.20.1, which forwards the traffic to Encoder 2.

- **Default Multicast Interface** - Selecting this option causes multicast traffic to use this interface. The built-in software on the EASyCAP Integrated Server does not currently use multicast communications, so this option is generally not turned on.
- **No Special Configuration** - Selecting this option allows the operating system to choose the multicast traffic route. This is the recommended setting.
- **Multicast Start Address** - In conjunction with the Multicast Mask setting, determines which multicast addresses will be sent using the interface. This address must be the lowest address of the address range specified.

- **Multicast Mask** - In conjunction with the Multicast Start Address, determines which multicast addresses will be sent through the interface.
- **Custom IF-UP Script** - This script provides a means for experienced users to hand-edit routes when a given interface is brought online. The \$IFACE variable identifies the interface (eth0 or eth1). For example:


```
# : if [ "$IFACE" = eth0 ]; then
#   do something
# fi
```
- **Custom IF-DOWN Script** - This script allows re-routing or removal of routes when an interface is going offline. The \$IFACE variable identifies the interface going offline.

After making changes, select the **Accept** button to save the network configuration settings. If you have made changes and have selected the **Close** button, a confirmation page will prompt you before closing. Select the **No** button to return to the **Network Configuration** page or select the **Yes** button to exit without saving the changes to the network configuration.



If the IP address of the server has changed, you will need to close the browser window and reopen to login to the server at the new IP Address.

IP Message Delivery

To setup the outgoing delivery settings from the server to EASy Series Encoder/Decoders, select the **EASyPLUS** link. The **EASyPLUS Configuration** setup page will be displayed as shown below.

The screenshot shows the 'EASyPlus Configuration' dialog box. It features a 'Unit Name' dropdown menu set to 'Unit 1', with 'Add' and 'Delete' buttons. The main configuration area includes fields for 'IP Address' (10.1.77.160), 'Command Port' (59911), 'Audio Port' (59919), 'Password' (5555), 'Call Sign' (nope), and a 'No EAN Audio' checkbox. A 'Description' field contains 'Lab EASyPLUS'. 'Accept' and 'Cancel' buttons are at the bottom.

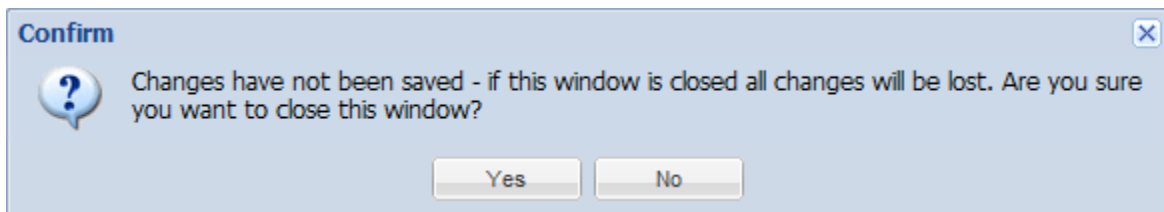
To view the settings of a EASyPLUS configuration, use the **Unit Name** dropdown list to select the desired EASyPLUS unit.

- Select the **Add** button to add a new EASyPLUS unit. Modify the unit settings as described in the following section and then select the **Save** button to save the EASyPLUS unit settings.
- Select the **Delete** button to delete the selected EASyPLUS unit. A confirmation page will prompt you before deleting the EASyPLUS unit. Select the **Yes** button to delete the EASyPLUS unit or select the **No** button to exit without deleting the EASyPLUS unit.

Once the EASyPLUS unit has been selected, any of the following settings can be modified:

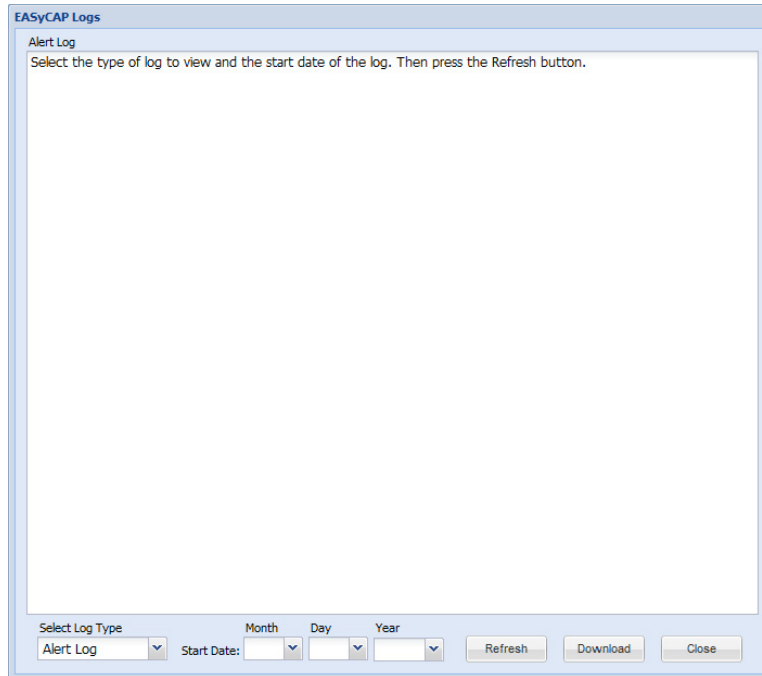
- **Description** - Enter the name that you wish to display for this encoder/decoder.
- **IP Address** - Enter the IP address used to connect to the selected encoder/decoder.
- **Command Port** - Enter the TCP command port used to communicate with the selected encoder/decoder. The default value is 59911.
- **Audio Port** - Enter the TCP port used to transfer audio from the server to the encoder/decoder. The default value is 59919.
- **Password** - Enter the password used to login to the configured Encoder/Decoder. This should be a special CAP account added to the user accounts of the Encoder/Decoder, and given EAS Alert and Ethernet permissions in the user account.
- **Call Sign** - Enter the station identification that will be included in the Encoder/Decoder log.
- **No EAN audio** - When this box is selected the EAN audio stream will not be used, Encoder/Decoders will receive EAN audio from a local audio input.

After making changes, select the **Accept** button to save the EASyPLUS unit settings. If you have made changes and have selected the **Cancel** button, a confirmation page will prompt you before cancelling. Select the **No** button to return to the **EASyPLUS Configuration** setup page or select the **Yes** button to exit without submitting the changes to the EASyPLUS unit.



Logs

To view the alert and system logs of the EASyCAP Server, select the **Alert/System Log** link. The **EASyPLUS Configuration** setup page will be displayed as shown below.



The screenshot shows a window titled "EASyCAP Logs" with a sub-header "Alert Log". Below the sub-header is a text box containing the instruction: "Select the type of log to view and the start date of the log. Then press the Refresh button." The main area of the window is empty. At the bottom, there is a control panel with a "Select Log Type" dropdown menu set to "Alert Log", a "Start Date:" label, and three dropdown menus for "Month", "Day", and "Year". To the right of these are three buttons: "Refresh", "Download", and "Close".

To view the logs, perform the following steps:

- Use the **Select Log Type** dropdown list to select the desired log type.
- Select the **Start Date** dropdown lists for **Month**, **Day** and **Year** to set the start date of the desired logs.
- Select the **Refresh** button to view the specified logs.

Alert Log

Select **Alert Log** from the **Select Log Type** dropdown list to view the CAP Alert information.

The **Alert Log** page will be displayed as shown to the right. To download a copy of the alert log in ASCII text file format, select the **Download** button.

EASyCAP Logs

Alert Log

Alert Reference: TestFacility,Avalanche_Warning_1/20/2012_1:58:02_PM-2:29:46_PM_5ACC0D9E,2012-01-20T18:58:02-00:00
At 01/20/2012 13:58:02 EST: Received Alert
Received from Jim's PC
Originator: EAS Participant
Event: Avalanche Warning
Sent: 2012-01-20T18:58:02-00:00
Expires: 2012-01-20T19:29:46-00:00
FSK Received: CZCC-EAS-AVVW-018059+0045-0201858-EASyCAP -
Languages:
en-us with voice file resource
Alert Text: 'An EAS Participant has issued an Avalanche Warning for the following counties: Hancock IN. Effective until 02:43 PM EST. An Avalanche Warning has been issued for the following areas: Hancock, IN. This Avalanche Warning is effective until 2:29 pm, Friday, January 20.'

Alert Reference: TestFacility,Avalanche_Warning_1/20/2012_2:03:53_PM-2:29:46_PM_F90FFB9,2012-01-20T19:03:53-00:00
At 01/20/2012 14:03:54 EST: Received Alert
Received from Jim's PC
Originator: EAS Participant
Event: Avalanche Warning
Sent: 2012-01-20T19:03:53-00:00
Expires: 2012-01-20T19:29:46-00:00
FSK Received: CZCC-EAS-AVVW-018059+0030-0201903-EASyCAP -
Languages:
en-us with voice file resource
Alert Text: 'An EAS Participant has issued an Avalanche Warning for the following counties: Hancock IN. Effective until 02:33 PM EST. An Avalanche Warning has been issued for the following areas: Hancock, IN. This Avalanche Warning is effective until 2:29 pm, Friday, January 20.'

Select Log Type: Alert Log | Month: 01 | Day: 01 | Year: 2012 | Refresh | Download | Close

System Log

Select **System Log** from the **Select Log Type** dropdown list to view the general system and application information.

The **System Log** page will be displayed as shown to the right. To download a copy of the system log in ASCII text file format, select the **Download** button.

EASyCAP Logs

System Log

At 01/23/2012 11:07:10 EST: Plugin Manager Information daemon Maintenance started

At 01/23/2012 11:07:10 EST: Plugin Manager Information daemon WebServices started

At 01/23/2012 11:07:10 EST: Plugin Manager Information plugin TpcFeed started

At 01/23/2012 11:07:10 EST: Plugin Manager Information plugin IpawsOpenAtomFeed started

At 01/23/2012 11:07:10 EST: Plugin Manager Information plugin DupChecker started

At 01/23/2012 11:07:10 EST: Plugin Manager Information plugin AlertTexter started

At 01/23/2012 11:07:10 EST: Plugin Manager Information plugin EASyPlus started

At 01/23/2012 12:55:05 EST: Plugin Manager Information Configuration file /home/eas/cfg/AcceptedStates.cfg changed by WebServices. Dependent executables will be restarted.

At 01/23/2012 12:55:05 EST: Plugin Manager Information plugin TpcFeed killed because configuration file /home/eas/cfg/AcceptedStates.cfa changed.

Select Log Type: System Log | Month: 01 | Day: 01 | Year: 2012 | Refresh | Download | Close

THIS PAGE LEFT INTENTIONALLY BLANK



TRILITHIC
INNOVATIVE ENGINEERING

9710 Park Davis Drive
Indianapolis, IN 46235
(317) 895-3600
www.trilithic.com