UCrypt® IP2Agen2

Patent Pending

UCrypt® Cable Gateways IP to Analog 2nd Generation

INSTALLATION & OPERATION MANUAL

General Guide Notes

Document	**ANW1154 UCrypt IP to Analog - 2nd Generation Installation & Operation Manual**
Release Date	**August 15 2017**

Firmware Version

Some features described in this manual require the latest firmware to be installed on the hardware platform. Check with ATX Networks Technical Support for the latest release of firmware. The firmware version installed on your Device may be found in the UI on the System tab. At the time of publication of this manual the most current released firmware versions are:

Ubuntu OS Release	**12.04**
Firmware Release	**16188**

Organization of This Manual

This manual is generally organized based on the main interface tabs with individual chapters dedicated to describing the configurable features. Further chapters outline activities related to installation and the UI operation and configuration.

Cross Reference Usage

Hyperlinks are used throughout the guide to assist the reader in finding related information if the reader is viewing the PDF file directly. Hyperlinks may be identified by their blue text. Most links are to related pages within the document, but some may reference outside documents if the reader needs that additional information. The Table of Contents is entirely hyperlinked and bookmarks are available but the bookmark feature must be turned on in your Reader application.

Symbol Usage

Throughout the manual, some symbols are used to call the readers attention to an important point. The following symbols are in use:

WARNING: *This symbol usage will call the reader's attention to an important operation feature of the equipment which may be safety related or may cause a service outage.*

NOTE: *This symbol indicates that there is helpful related information available in this note or elsewhere in the guide.*

TABLE OF CONTENTS

SAFETY

1. Safety

WARNING! FAILURE TO FOLLOW THE SAFETY PRECAUTIONS LISTED BELOW MAY RESULT IN PROPERTY DAMAGE OR PERSONAL INJURY. PLEASE READ AND COMPLY WITH THE FOLLOWING:

SAFETY GROUND: The connection to earth of the supplementary grounding conductor shall be in compliance with the appropriate rules for terminating bonding jumpers in Part V of Article 250 of the National Electrical Code, ANSI/NFPA 70, and Section 10 of Part I of the Canadian Electrical Code, Part I, CSA C22.1.

WATER AND MOISTURE: Care should be taken to prevent entry of splashed or dripping water, other liquids, and physical objects through enclosure openings.

DAMAGE: Do not operate the device if damage to any components is suspected.

POWER SOURCES: Only connect the unit to a power supply of the type and capacity specified in the operating instructions or as marked on the device.

NOTE: a) For 115 VAC operation, use the power cord supplied for operation from a 115 VAC source.
b) For 230 VAC operation, use the power cord supplied for operation from a 230 VAC source.

GROUNDING OR POLARIZATION: Electrical grounding and polarization means must not be defeated.

POWER CORD PROTECTION: Care must be taken during installation to route or arrange the power supply cord to prevent and avoid the possibility of damage to the cord by external objects. Pay particular attention to the exit point from the device and plug.

POWER SUPPLY CORD ROUTING: The power supply cord shall not be attached to the building surface, nor run through walls, ceilings, floors and similar openings in the building structure.

SERVICE: Do not attempt to service the device beyond procedures provided in the operating instructions. All other servicing should be referred to qualified service personnel.

MODIFICATIONS: Modifications should not be made to the device or any of its components for applications other than those specified in the operating instructions.

SAFETY CODES AND REGULATIONS: The device should be installed and operated in compliance with all applicable local safety by-laws, codes and regulations.

This page intentionally left blank.

OVERVIEW

2. Overview

The UCrypt IP to Analog Version 2, referred to as **Device** in this manual, is built in either a 1RU chassis for up to 20 analog channels or a 2RU chassis for up to 60 analog channels. Each device can ingest MPEG-2, H.264, SD or HD, SPTS and MPTS IP multicast video streams with redundancy and output in either NTSC or PAL analog formats.

2.2 Chapter Contents

2.3 Front Panels

The front panel of each Device, shown in Figure 2-1 and Figure 2-2, contains a set of controls and indicators to show the status of important operation parameters and allow some control over the device. These control panels are explained further in the next section.

Figure 2-1: UCrypt 1RU Front Panel

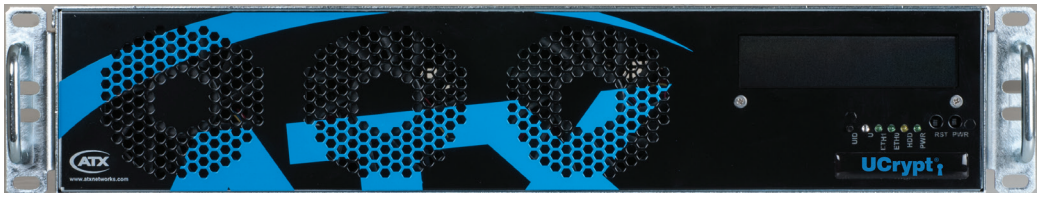

Figure 2-2: UCrypt 2RU Front Panel

2.4 Controls & Indicators

The products are designed to be plug and play and will be in a powered on state when the power cord is plugged in. There may be instances where it is desired to reboot or power down the devices manually and recessed switches to enable that are located on the front panel, a detailed view of which is shown in Figure 2-3 (1RU) and Figure 2-4 (2RU). Indicator lights are provided to allow monitoring of errors and alarms and have a slightly different appearance but the same functionality on 1RU and 2RU devices . See Table 2.4a for functional descriptions of all front panel controls and indicators.

Figure 2-3: 1RU Controls & Indicators

Figure 2-4: 2RU Controls & Indicators

Table 2.4a: Front Panel Controls and Indicators

1RU Symbol	2RU Label	Function	Description
N/A	UID	Recessed Button	Universal Identifier: A switch that will turn on the adjacent "**U**" light. This switch exists only on the 2RU model.

1RU Symbol	2RU Label	Function	Description
	U	Indicator LED Blue	Universal Information LED: The Universal Information BLUE LED is used to indicate fan failure, power failure, overheat condition, or to identify the unit within a large rack installation. This may be activated by the IPMI or front panel button. State Indication: • Fast Blinking Red (1 per sec) - Fan Failure • Solid Red - CPU Overheated • Slow Blinking Red (1 per 4 sec) - Power Failure • Solid Blue - Local UID Button Depressed • Blinking Blue - IPMI Activated UID Note: Deactivating the UID LED must be performed in the same way it was activated. (If the UID LED was activated via IPMI, you can only turn the LED off via IPMI and not with the UID button.)
	ETH1	Indicator LED Green	Indicates network activity on eth1 network port.
	ETH0	Indicator LED Green	Indicates network activity on eth0 network port.
	HDD	Indicator LED Green	Indicates SSD/HDD drive activity when flashing.
	PWR	Indicator LED Green	Indicates power is being supplied to the system's power supply units. This LED should be illuminated when the system is operating.
	RST	Recessed Button	Reset Switch. Used to warm reboot the Device. Functionally equal to a reset button on a computer.
	PWR	Recessed Button	Power Switch. This is the main soft power switch and is used to apply or remove power to the Device. Activating this switch effectively turns the unit off but keeps standby power supplied to the system. You must unplug the system before servicing. Press again to power up.

2.5 Rear Panels

The rear panel connections are shown here. Some ports that are unlabeled are not used in this model of Device.

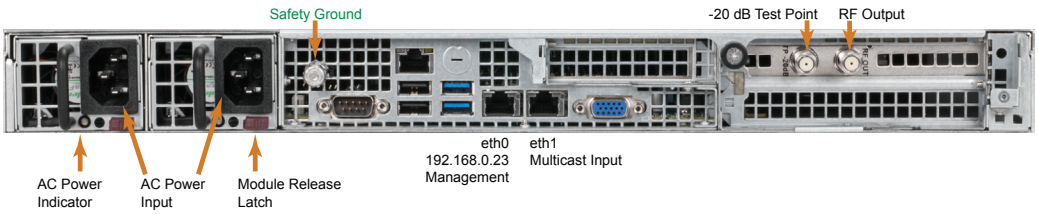

Figure 2-5: 1RU Rear Panel

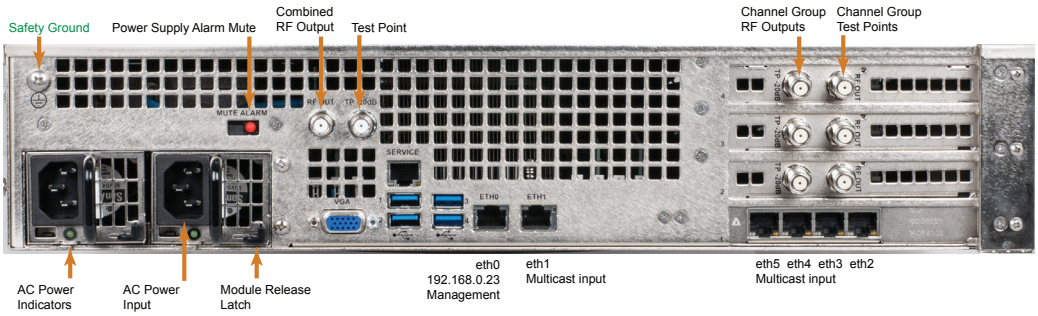

Figure 2-6: 2RU Rear Panel

2.6 Switch & Firewall Port Openings

Any Management Switch used between IP2A Devices and the Management Computer will require the following ports to be opened both Inbound and Outbound.

NOTE: *Failure to open these ports may result in communications problems between the management computer and IP2A Devices.*

Table 2.6a: Ports to Open on Switch

Port Number	Transport	Protocol
80	TCP	HTTP
443	TCP	HTTPS

This page intentionally left blank.

INSTALLATION

3. Installation

This chapter provides a guide to get your Device installed in a rack and connected safely.

3.1 Chapter Contents

3.2 Preparation for Installation

Carefully unpack the equipment from the shipping box. If the box or equipment is damaged, notify the freight company to make a damage claim. If you suspect that there is a problem with the equipment that may preclude safe operation, do not install or operate it. Contact ATX Networks immediately for instructions.

WARNING: *This equipment is intended for installation in a RESTRICTED ACCESS LOCATION only.*

WARNING: *This equipment is NOT for use in a computer room as defined in the Standard for Protection of Electronic Computer/Data Processing Equipment, ANSI/NFPA 75.*

WARNING: *This equipment is intended for use in a fixed position and should be installed securely before operation is initiated.*

3.3 Precautions

3.3.1 Electrical Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the Device chassis from damage:

- Be aware of the locations of the power on/off switch on the chassis as well as the room's emergency power-off switch, disconnection switch or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the system.
- Power should always be disconnected from the system when servicing. When disconnecting power, you should first power down the operating system first and then unplug the power cords. The unit has more than one power supply cord. Disconnect two power supply cords before servicing to avoid electrical shock.
- When working around exposed electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off the power if necessary.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.

- The power supply power cords must include a grounding pin and must be plugged into grounded electrical outlets.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards or areas where power is present.
- This product may be connected to an IT power system. In all cases, make sure that the unit is also reliably connected to Earth (ground).

3.3.2 General Precautions

WARNING: *The RF connections provided with this equipment are not intended for direct connection to any outside telecommunications network or outside cable distribution plant.*

WARNING: *When the equipment is lifted by the front handles, always use both front handles for security. Never lift this equipment using only a single front handle due to the weight of the equipment.*

- The Devices weighs up to approximately 30 lbs (13.5kg). When lifting the system, two people should lift slowly with their feet spread out to distribute the weight. Always keep your back straight and lift with your legs.
- While working on the system, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- After accessing the inside of the Device, close the chassis back up and secure it to the rack unit with the retention screws and ensure that all connections have been made.

3.3.3 Chassis Precautions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest components on the bottom of the rack first, and then work up.
- Use a regulating uninterruptible power supply (UPS) to protect the Device from power surges, voltage spikes and to keep your system operating in case of a power failure.
- Allow any power supply modules to cool before touching them.

3.3.4 Rack Precautions

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In single rack installation, stabilizers should be attached to the rack. In multiple rack installations, the racks should be coupled together.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

3.4 General Mechanical

- The equipment will require 1RU or 2RU of vertical rack space depending on the model being installed and may be mounted directly above or below other equipment without providing space between, however, 1RU space is recommended to be maintained from other equipment which generates significant heat.
- Leave enough clearance in front of the rack to enable you to work on the chassis (~25 inches) and approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease of servicing.

NOTE: *More general information about equipment abient temperature requirements may be found in this document from ATX Networks:* http://www.atxnetworks.com/pdf/ANW1066_MDU_UCrypt_Environment_Temp_Considerations_InfoSheet.pdf

- Rear support of the unit is mandatory and rails for attachment to rear supports are provided. Do not use the unit chassis to support other equipment. Alternately, if rear support rails are unavailable or impractical, install the unit on a well supported shelf.

3.5 General Electrical

- Consideration should be given to the connection of the equipment to the mains power and the effect that any possible overloading of circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings of all connected equipment should be used when addressing this concern.
- Reliable earthing of rack-mounted equipment should be maintained in addition to any grounding conductor provided in the power cord. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

3.6 General Environment

- Be sure to maintain freedom of air movement around equipment to ensure safe operation.
- Installation of the equipment in enclosed racks is not recommended due to possibility of restricted air flow.
- Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- The equipment is designed to operate to specification in an ambient temperature of +0°C to +40°C (+35°F to +104°F), however, normal room temperature is recommended to ensure long term operation of the equipment.
- If equipment is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) of +40°C (+104°F).

3.7 Gigabit Ethernet Ports

The input ports are auto MDI-MDIx and intended to be connected to a network distribution switch using straight through wired Cat5e or better quality cable. The rear panel Management Interface port allows connection to a notebook or desktop PC for managing and configuring the system. The port may be connected to directly, or in the case of a headend with many devices to manage, may be connected to a management network (recommended) or the distribution switch containing the video stream content. It is possible to set up virtual ports for a VLAN. Connections should be made with Cat5e or better network cables. The GigE management port is auto MDI-MDIx and may be connected to a switch or router with a straight through wired cable.

3.8 Install the 1RU Device

This section provides information on installing the 1RU Device chassis in a rack unit with the rails provided. There are a variety of rack units on the market, which may mean that the assembly procedure will differ slightly from the instructions provided. You should also refer to the installation instructions or adapt these instructions to suit the rack unit you are using.

WARNING: *The illustrations in Figure 3-4 and Figure 3-5 are for general guidance purposes only. Always install the Device chassis to the bottom of the rack first to avoid the rack becoming top heavy.*

3.8.1 Identifying the Rack Rail Sections

The 1RU Device chassis includes two rail assemblies in the rack mounting kit. Each assembly consists of two sections: An inner chassis rail secured to the chassis (front part is factory installed, extension is field installed), an outer rail that secures to the rack, and an outer rail extension that secures directly to the rear vertical support, Figure 3-1. Each of these assemblies are designed for mounting universally on the left or right side of the chassis.

NOTE: *This rail will fit a rack between 26" and 33.5" deep.*

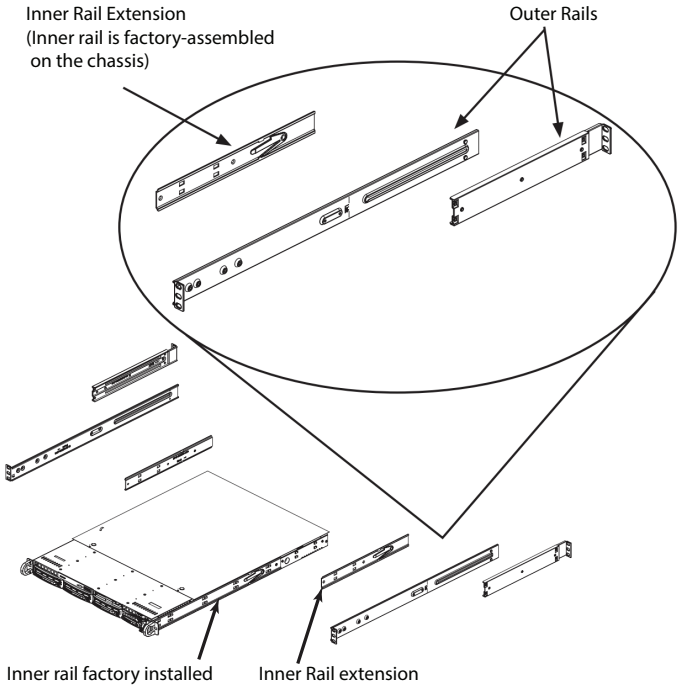

Figure 3-1: Identifying Rack Rail Sections

3.8.2 Install Inner Rail Extensions

The chassis includes a set of inner rails which are in two sections: inner rails and inner rail extensions. The inner rails are pre-attached and do not interfere with normal use of the chassis if you decide not to use a server rack. Attach the inner rail extension to help support the rear of the chassis within the rack.

1. Place the inner rail extensions on the side of the chassis aligning the hooks of the chassis with the inner rail extension holes, Figure 3-2. Make sure the inner rail extension faces “outward” just like the pre-attached inner rail.
2. Slide the extension toward the front of the chassis latching it onto the hooks.
3. Secure the rail extension with 2 screws as illustrated.
4. Repeat steps 1-3 for the other inner rail extension.

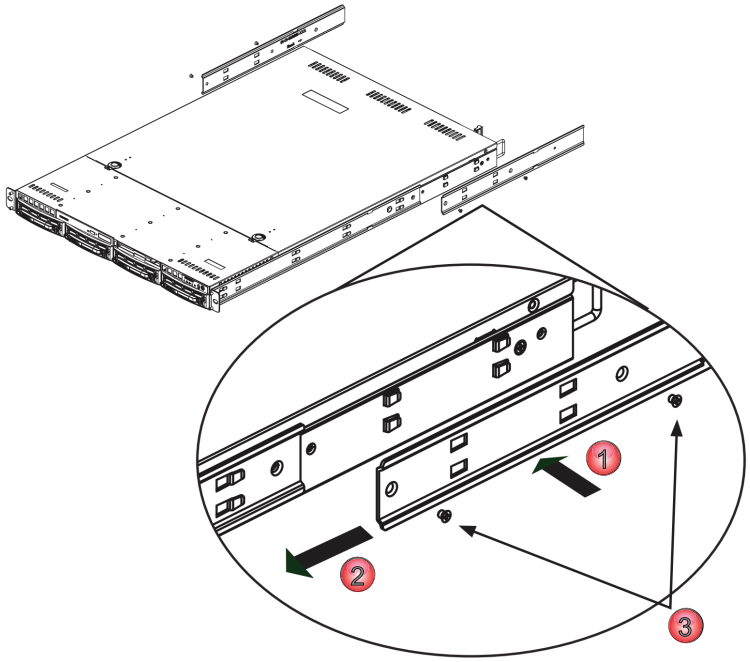

Figure 3-2: Identifying Rack Rail Sections

3.8.3 Install the Outer Rails in the Rack

1. Attach the longer section of the outer rail to the outside of the shorter section of the outer rail, Figure 3-3. You must align the pins with the slides. Both ends of the outer rail must face the same direction in order to be secured to the rack.

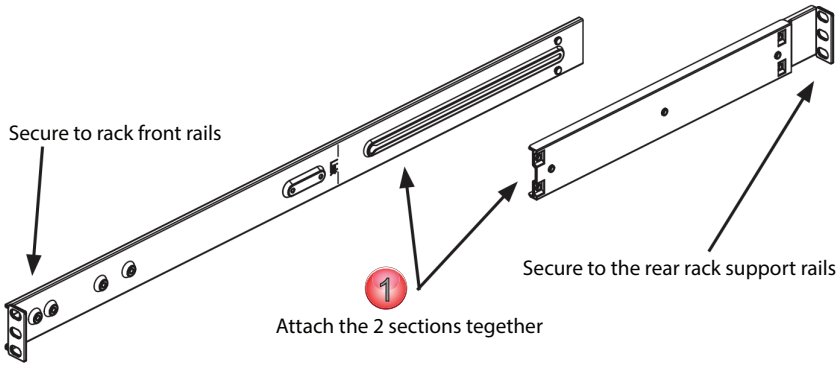

Figure 3-3: Install Rail Sections

2. Adjust both sections of the outer rail to the proper length so that the rail fits snugly within the rack, Figure 3-4.
3. Secure the longer section of the outer rail to the of the front rack rails with two 10-32 rack screws.
4. Secure the shorter section to the rear rack rails with two 10-32 rack screws.
5. Repeat steps 1-4 for the remaining outer rail.

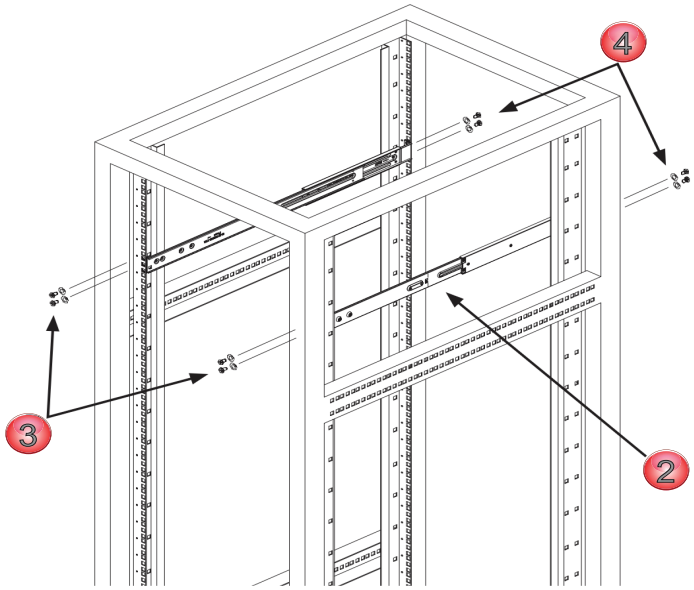

Figure 3-4: Install Outer Rails to Rack

3.8.4 Mount the Chassis

1. Confirm that the inner rails and rail extensions have been installed on the chassis, Figure 3-5.
2. Confirm that the outer rails and extensions are installed on the rack.
3. Line up the chassis rails with the front of the outer rack rails, then slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting). When the Device has been pushed completely into the rack, you should hear the locking tabs “click” into the locked position.
4. Insert and tighten the screws that hold the front of the Device to the rack if desired.

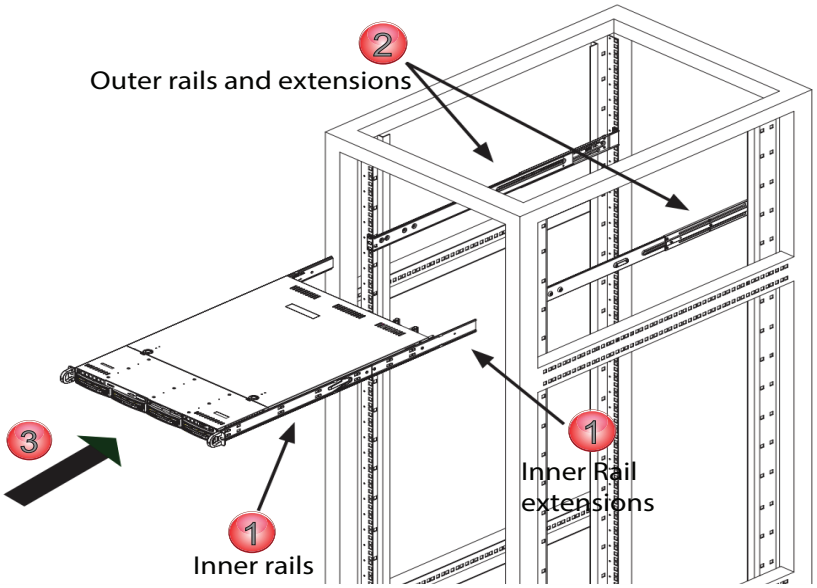

Figure 3-5: Install Chassis to Rack

3.9 Install the 2RU Device

This section provides information on installing the Device chassis in a rack unit with the rails provided. There are a variety of rack units on the market, which may mean that the assembly procedure will differ slightly from the instructions provided. You should also refer to the installation instructions or adapt these instructions to suit the rack unit you are using.

NOTE: *The illustrations in Figure 3-6 and Figure 3-7 are for general guidance purposes only. Always install the Device chassis to the bottom of the rack first to avoid the rack becoming top heavy.*

3.9.1 Mount the Chassis

1. Confirm that you have the four mounting screws required to mount the chassis into a rack.
2. Align the thru holes of the chassis with the thru holes of the rack.
3. Insert the mounting screws into the thru holes in the front of the chassis and through the thru holes in the rack as shown in Figure 3-6 and Figure 3-7.

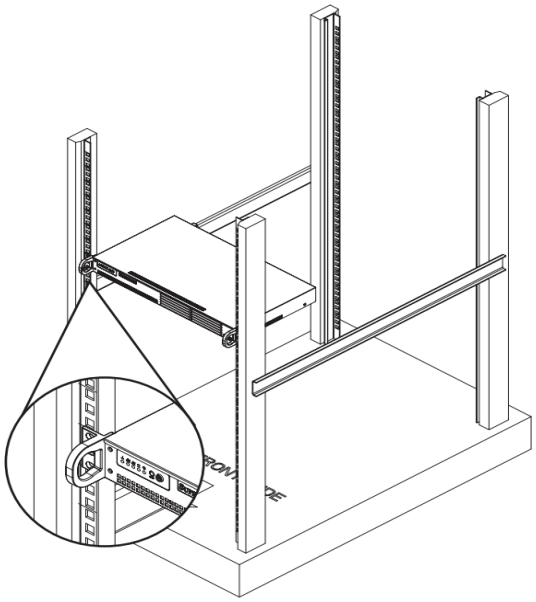

Figure 3-6: Install Chassis to Standard Rack

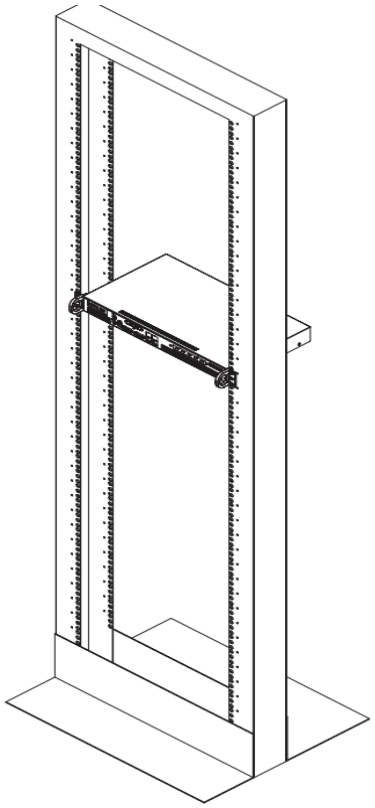

Figure 3-7: Install Chassis to Telco Rack

3.10 Equipment Safety Grounding

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips). The following guidelines are provided to clarify the requirements for the installation to meet UL, CUL and CB standards. The use of the words “Ground” and “Earth” as well as “Grounding” and “Earthing” may be used interchangeably and in this context, have the same meaning.

WARNING: To comply with standards it is imperative that the chassis be connected to a permanent building ground before connecting any power supply conductors due to high leakage currents present in redundant power supply configurations. A warning label, shown in Figure 3-10, is attached to all affected products.

Figure 3-10: Leakage Current Warning Label

The Device housing and power supplies must be connected to a permanent building ground in a manner that will ensure that the exposed metal parts are constantly connected to ground through independent means even when the power supply cord or wires may be disconnected temporarily. A ground connection screw terminal is provided on the rear panel to conveniently effect such a connection.

3.10.1 Ground Connection

The supplementary equipment grounding conductor is to be installed between the rear panel ground screw and earth, that is, in addition to the equipment ground conductor in the power supply cord or wires. The screw terminals provided for this connection are located on the rear panel as illustrated in Figure 3-8 and Figure 3-9.

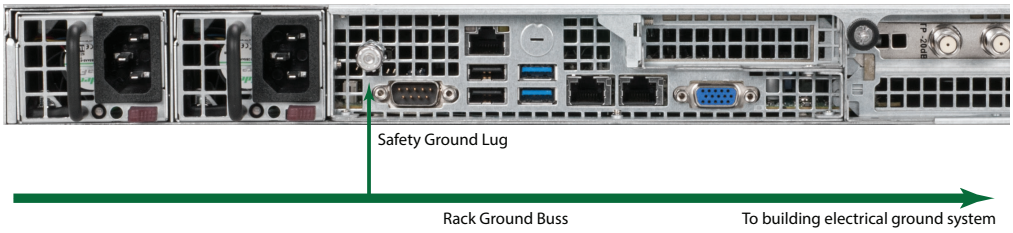

Figure 3-8: 1RU Safety Ground Connection

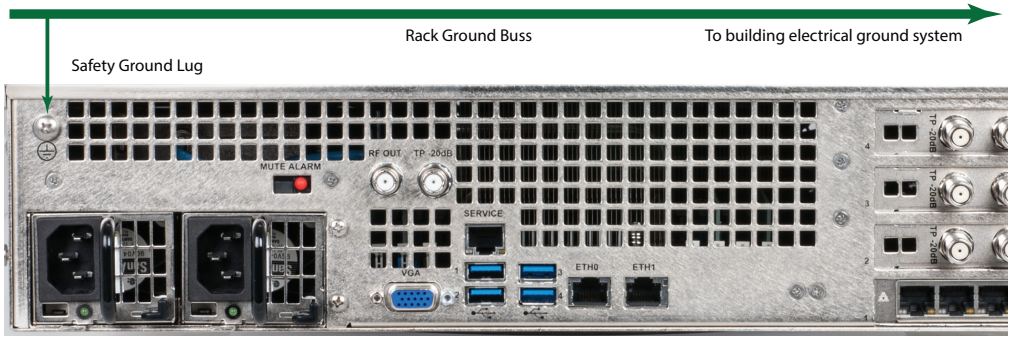

Figure 3-9: 2RU Safety Ground Connection

3.10.2 Ground Conductor Size

The supplementary equipment grounding conductor may not be smaller in size than the branch-circuit supply conductors or a minimum #14 AWG. The supplementary equipment grounding conductor is to be connected at the rear panel terminal provided, and connected to earth in a manner that will retain the earth connection when the power supply cord is unplugged. The connection to earth of the supplementary grounding conductor shall be in compliance with the appropriate rules for

terminating bonding jumpers in Part V of Article 250 of the National Electrical Code, ANSI/NFPA 70, and Section 10 of Part I of the Canadian Electrical Code, Part I, CSA C22.1.

3.10.3 Ground Conductor Termination

Termination of the supplementary equipment grounding conductor may be made to building steel, to a metal electrical raceway system, or to any grounded item that is permanently and reliably connected to the electrical service equipment earth.

3.10.4 Ground Conductor Type

Bare, covered or insulated grounding conductors are acceptable. A covered or insulated grounding conductor shall have a continuous outer finish that is either green, or green with one or more yellow stripes.

3.11 AC Power Supplies

Both the redundant and non-redundant AC power supplies are auto-sensing switching type power supply systems which may be operated on input voltages from 115 VAC to 230 VAC. There is no need to configure the power supplies to operate on any voltage in this range.

3.11.1 AC Power Cord Protection

Measures must be taken during installation to route or arrange the power supply cords or wires to prevent physical damage and to avoid the possibility of future damage occurring. The cords shall be installed and routed such that, throughout it's length, the cord and it's points of connection are not strained in any way.

3.11.2 AC Power Cord Attachment

The unit AC power supply cords shall not be attached to a building surface, bundled with audio, video or RF coaxial cables, nor run through walls, ceilings, floors and similar openings in the building structure.

3.11.3 Provision of Electrical AC Power Outlet

An AC electrical power outlet of appropriate type and rating shall be provided near the location where the unit is installed and easily accessible such that the provided power supply cords may be routed in an appropriate manner, without the use of extension cords, between the receptacle and the chassis. Alternately, the chassis shall be installed in close proximity to an existing AC electrical outlet such that the requirements of this paragraph are achieved.

3.11.4 IEC C13 Power Input Cord for AC

The AC power input receptacle is a standard IEC C14 socket connector similar to that commonly used on computers and monitors. The power cords provided with the IP2A product is a North American configuration with a NEMA 5-15 grounded plug for 115 VAC. If it is necessary to operate the product on 230 VAC, the installer must obtain IEC C13 cords with a NEMA 6-15 grounded plug for use in North America. This may be obtained at time of order from ATX Networks or locally. If shipped outside of North America, the Device will be supplied with an IEC C13 cord set appropriate for the locale to which it is shipped.

3.11.5 AC Input Power Requirements

When installing the equipment, it is the responsibility of the installer to determine that sufficient capacity is available in the electrical circuit feeding the unit to avoid overloading the supply circuit. The AC model will require power to be supplied from a properly grounded AC outlet. The installer shall determine that the AC power outlet, its wiring and receptacle is in compliance with local and/or national electrical codes as applicable. The AC input power requirement is constant over the range of input voltages. At higher input voltages, the current consumption is lower than it is at lower voltages where the input current is higher.

3.12 DC Power Supplies

3.12.1 DC Power Supply Connections

The optional redundant DC switching type power supply system is intended to operate on nominal -48 VDC power systems but functions between -40 and -57.2 VDC. A pair of **insulated #12 AWG** DC power wires must be field installed for each of the two modules using permanent wiring methods. Wire insulation colors must be different for each of the two conductors clearly indicating the polarity of the voltage. It is recommended that stranded conductors be used for DC power and that RED wire be used for the 0V conductor and BLACK for the -48V conductor. Crimped on style Ring or Spade terminals may be used and it is also permissible to strip the wire 8mm, twist the stranded conductors tightly and clamp the wire in the provided wire clamp as illustrated in Figure 3-11.

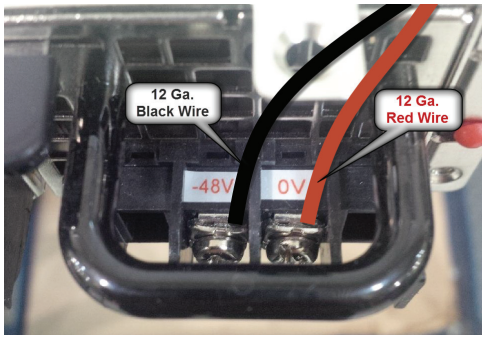

Figure 3-11: DC Power Module Connections

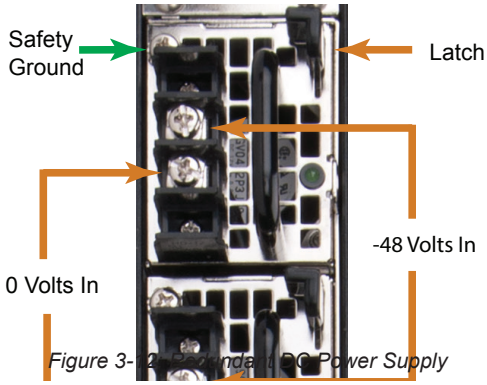

Figure 3-12: Redundant DC Power Supply

3.12.2 DC Disconnect and Fusing

Each DC power module should be externally fused or otherwise adequately protected at no more that 20 Amperes and must be provided with it's own external readily accessible disconnect device. Each disconnect must be prominently labeled indicating the units being powered and with adequate instructions for the removal of all power from the unit being serviced. The disconnect must be turned off for BOTH power modules before removing supply wires from the module terminal blocks when replacing a power supply module or otherwise servicing the unit.

3.13 Power Supply Redundancy

For the redundant power supplies, either power module on its own can provide the required power safely if one fails. To retain the redundancy feature, replace a failed power module as soon as possible. A power module failure or the failure of the supply current or protection fuse will be indicated by an audible alarm within the encoder power modules and the green power status LED on the power module will be extinguished. Silence the audible alarm with the red rear panel **Alarm Reset** switch adjacent to the power supply modules, Figure 3-12.

3.13.1 Redundant Power Module Replacement

AC Version

WARNING: *The power cords for **BOTH** power modules must be disconnected before attempting to remove the power modules or otherwise servicing the unit.*

Power module failure will be indicated by the alarm being sounded and the green status light on the module will no longer be lit. This power module may be replaced by first disconnecting the AC power cord from the IEC input socket of BOTH power modules, then release the module by pressing to the left on the thumb latch at the bottom of each module. Extract the module and replace with an identical replacement module only.

DC Version

WARNING: *The external disconnect for* ***BOTH*** *power modules must be turned off before attempting to disconnect the DC wiring from the power module terminals or otherwise servicing the unit.*

Power module failure will be indicated by the alarm being sounded and the green status light on the module will no longer be lit. This power module may be replaced by first disconnecting the DC power at the external disconnect device for BOTH power modules then use a #2 Phillips screw driver to remove the DC wires from the failed module terminals. Release the module by pressing to the right on the thumb latch on each module and extract the module. Replace with an identical replacement module only.

STARTUP

4. Startup

This chapter will help guide you through initial startup to get your Device operational. Refer to the other chapters of this manual for full configuration guidance.

4.1 Chapter Contents

4.2 Configure Your Computer

Set your computer's wired network IP address and subnet to be on the same subnet as the UCrypt Device. For example use 192.168.0.50/24.

4.3 Device Connections

Each of the UCrypt Device chassis are factory configured identically with the standard ATX Networks default IP address of 192.168.0.23 assigned to port eth0. Before connecting each Device to the management switch or network, the IP addresses must be re-configured for your network.

See Figure 4-1 and Figure 4-2 for the location of the ports.

1. Connect the Management Computer to eth0. The UCrypt Devices have eth0 network ports factory assigned IP address **192.168.0.23**.
2. Connect the headend RF Distribution Network to the RF Output Port. The level may be tested by using the -20 dB test point.
3. Connect the multicast streaming network(s) to eth1 for 1RU Devices and eth1 thru eth5 for 2RU Devices.

4.3.1 Rear Panel Connections for 1RU

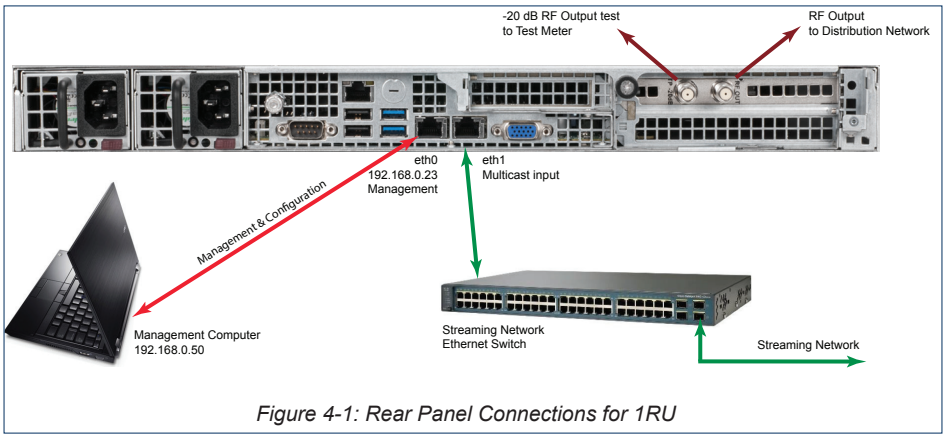

Figure 4-1: Rear Panel Connections for 1RU

4.3.2 Rear Panel Connections for 2RU

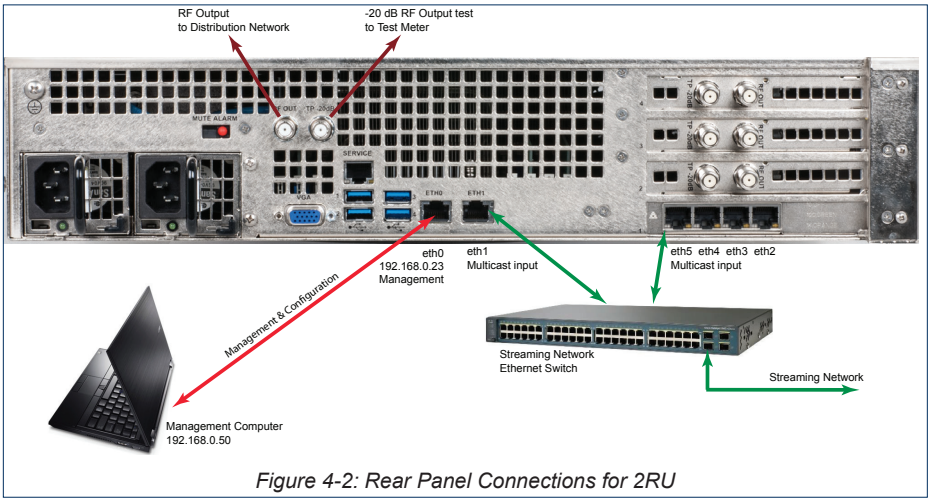

Figure 4-2: Rear Panel Connections for 2RU

4.4 Use a Browser to Login

1. Open any browser and enter the factory default IP address, **192.168.0.23**, see Figure 4-3.

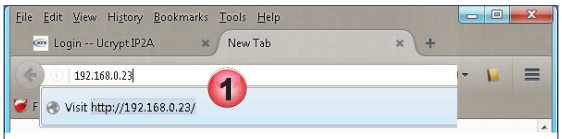

Figure 4-3: Enter Device IP Address

2. The login page is presented, Figure 4-4. Enter the **Master username and password,** see Table 4.4a.

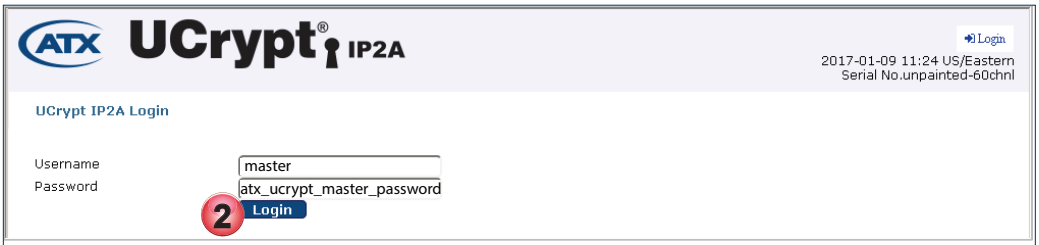

Figure 4-4: Login with Credentials

Table 4.4a: Default Users & Credentials

Username	Password	Authority
master	atx_ucrypt_master_password	Controls Everything
admin	atx_ucrypt_admin_password	Everything except User Configuration
guest	atx_ucrypt_guest_password	No configuration, Just monitoring

PASSWORD WARNING: ATX Networks strongly recommends that the factory default passwords be changed immediately upon Device initialization. The ability to dismiss or disable password warnings in the GUI are intended only for lab test environments with no internet connectivity to the Device.

3. The **Channels** configuration page of the Device is presented, see Figure 4-5. All configuration of the processed channels is initiated from this page.

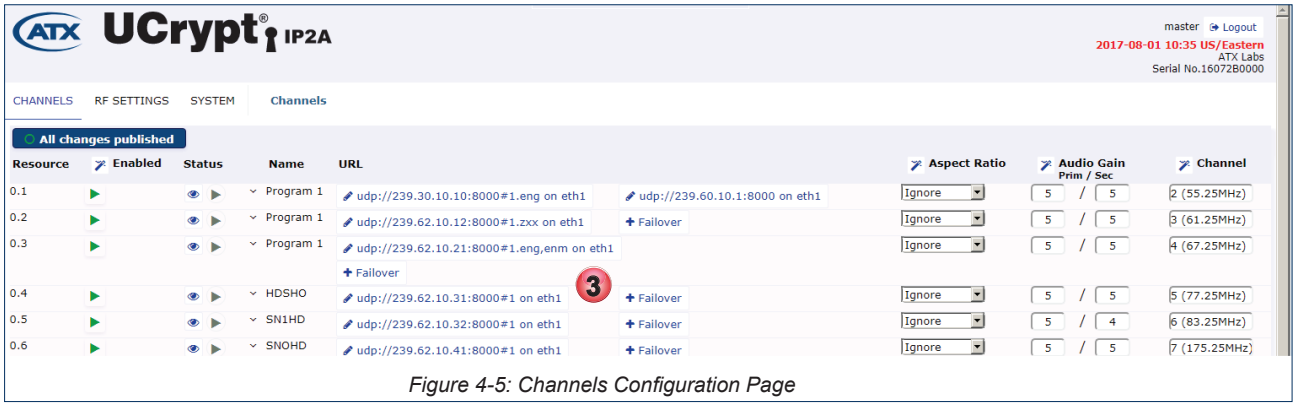

Figure 4-5: Channels Configuration Page

4.5 Principle UI Features

All configuration of the processed channels is done from this page. A few important features, highlighted in Figure 4-6, include:

1. Each line represents a single analog channel referred to as a **Resource**.
2. Each resource or channel may be **individually enabled or disabled**. Disabling turns off RF output on that channel.
3. Output Channels may be changed by clicking the channel then use **search and dropdown menu choices**.
4. Input Multicast may be easily changed. Simply **click the URL and edit** as required.
5. The **Publish Button** is used to apply all changes made on the **Channels and RF Settings** tabs. The System tab and Network configuration pages have their own buttons to apply changes.

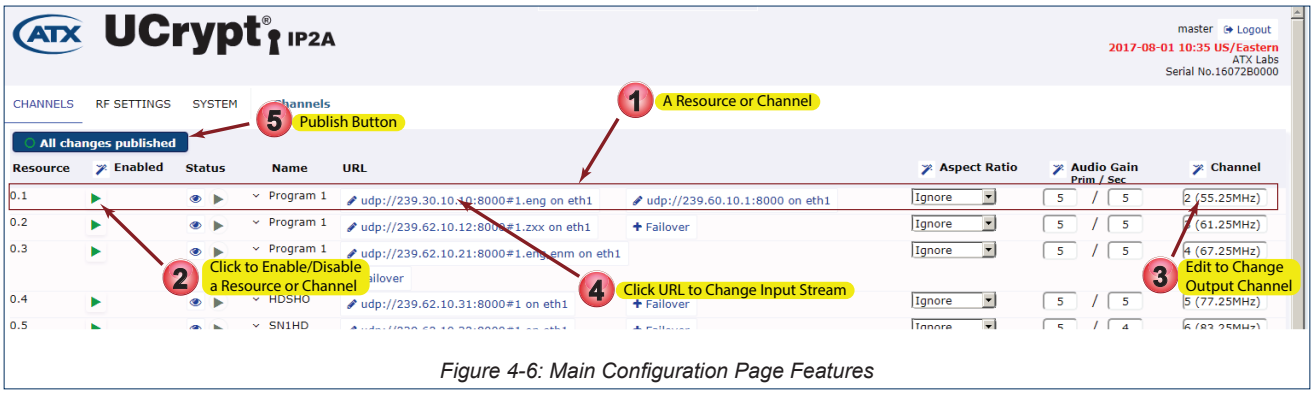

Figure 4-6: Main Configuration Page Features

6. A control to **bulk enable** a selected group of resources, Figure 4-7.
7. A group of controls to **bulk configure** a selected group of resources.
8. Click the **Eye** icon to enable a **streaming monitor window** with audio for any configured and streaming resource.
9. Configure a **backup stream** for each resource from the **+Failover** link.

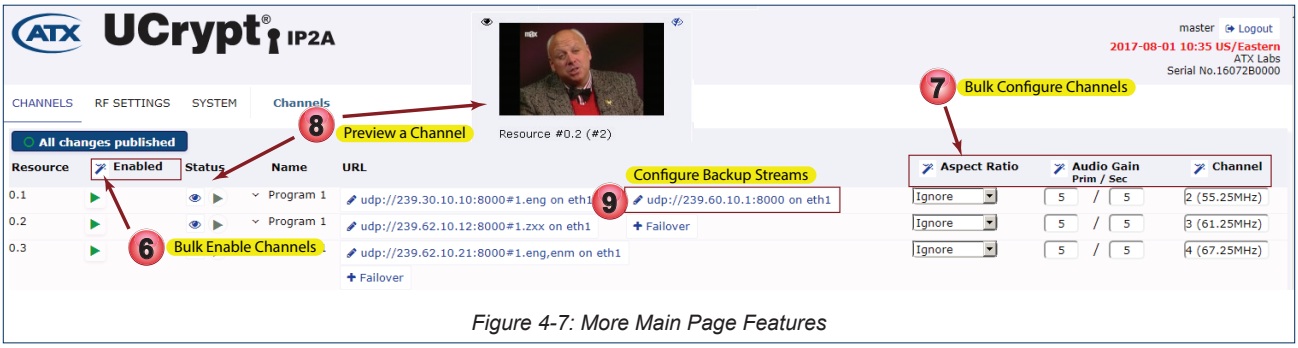

Figure 4-7: More Main Page Features

4.6 Configure Network Settings

Refer to “6.2 Network Configuration” on page 6-2 for configuration information.

4.7 Select Analog Channel Plan

Refer to “7.3 Select Active Channel Plan” on page 7-2 for configuration information.

4.8 Setup Analog Channels

Refer to “5.10 Setup the Output Analog Channels” on page 5-10 for configuration information.

4.9 Add an Input Stream

Refer to “5.7 Add an Input Stream” on page 5-4 for configuration information.

CHANNELS TAB

5. Channels Tab

The Channels tab is the page used to configure input streams, RF output channels, monitoring Resources and Status.

5.1 Chapter Contents

5.2 Publishing Changes

All changes that are made on this page must be published before they take effect. The number of changes to be published are noted inside the **Publish Button** just below the header, Figure 5-1, just click the button to apply the changes. Changes to all channels or groups of channels such as starting, stopping, enabling and disabling may be made simultaneously with the **Mass Configuration Button**, see Figure 5-1.

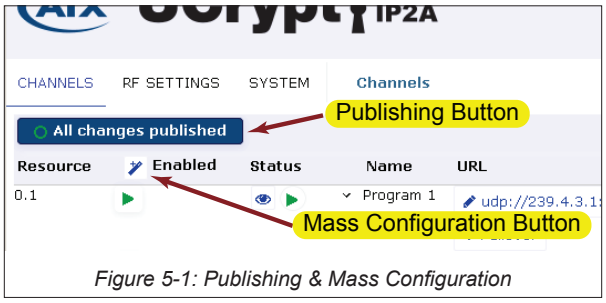

Figure 5-1: Publishing & Mass Configuration

5.3 Status Icons Explained

There are several types of Status Icons used on the Channels page to help interpret the resource states, see Figure 5-2.

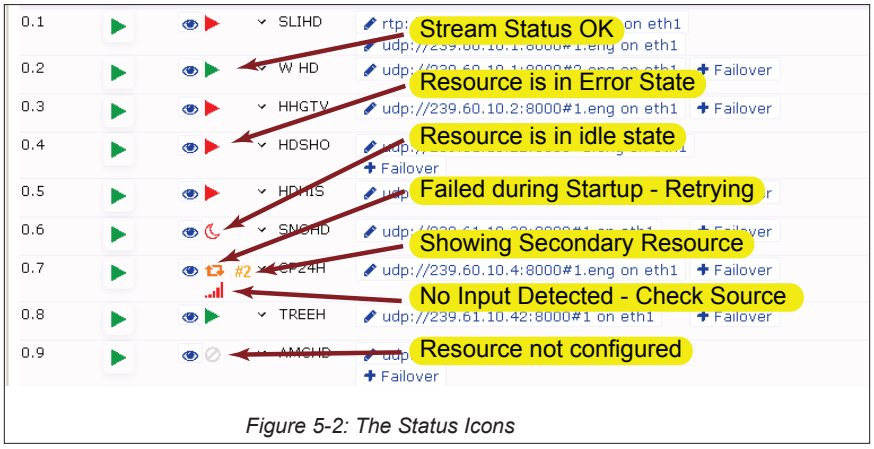

Figure 5-2: The Status Icons

5.4 Reset Configuration

The Device may be reset to factory configuration by using the **Reset Configuration** button at the bottom of the Channels page and you will need to scroll to the very bottom of this page to see it, Figure 5-3. Saving the form that opens when clicking the button will erase the content configuration for this machine, resetting all multicast resources and analog card outputs.

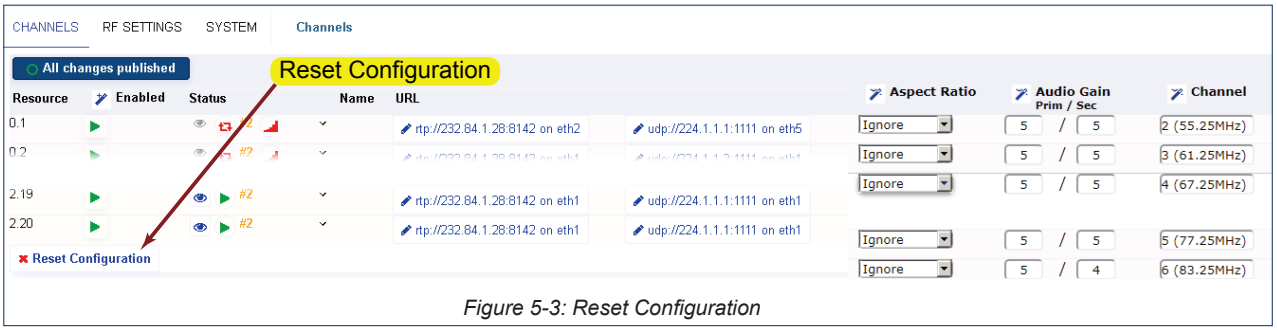

Figure 5-3: Reset Configuration

5.5 Expand and Enable Resources

Resources must be enabled before use. Enabling turns on the RF output for each resource and may be done individually by clicking the small grey square icon for each resource which then changes into a small green triangle icon , see Figure 5-4.

To enable a group of channels at once, click the **Wand** icon nearest the Enabled header and refer to "5.6 Mass Configuration" on page 5-3.

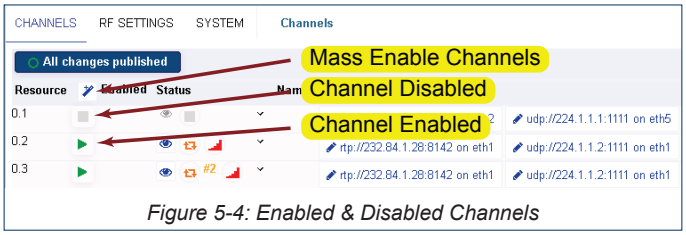

Figure 5-4: Enabled & Disabled Channels

To reveal expanded information about the resources, click the small **Down Arrow** under the Name heading. Collapse this display by clicking again.

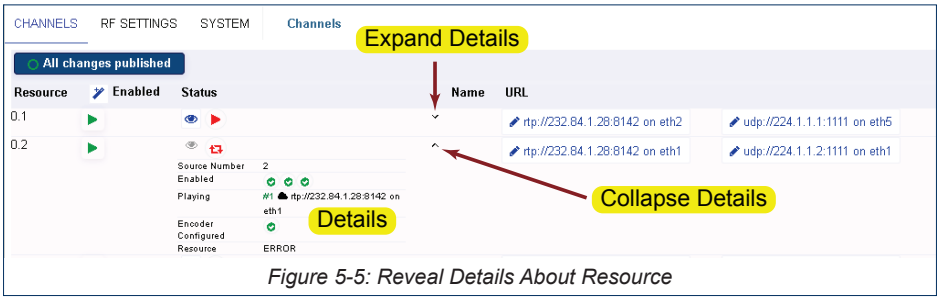

Figure 5-5: Reveal Details About Resource

5.6 Mass Configuration

Tools to allow mass configuration of all or groups of resources at one time speeds configuration when many resources need to have the same operation performed. These tools are found within the **Resources List Headers** highlighted in Figure 5-6. Each tool operates in the same manner in that you may select a single resource to act upon or any range of resources. The resources or ranges do not need to be contiguous. Click the **Wand** icon beside the appropriate labels to access the tools.

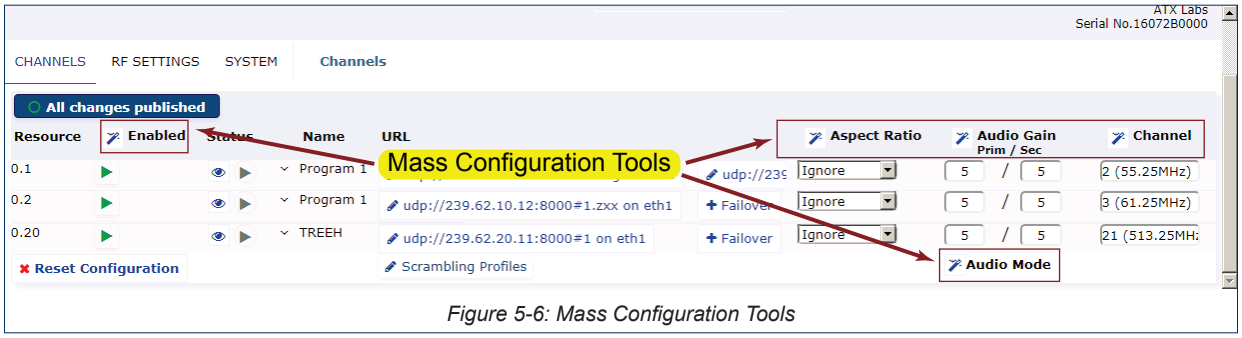

Figure 5-6: Mass Configuration Tools

5.6.1 Enabled Tool

Enabled

- Starting and stopping of streaming of multiple resources.
- Used for enabling or disabling multiple resources.

5.6.2 Aspect Ratio Tool

Aspect Ratio

- Used for changing Aspect Ratio of multiple resources.

5.6.3 Audio Mode Tool

Audio Mode

- The Audio Mode tool is at the bottom of the page below the Audio Gain column.
- Used for changing audio mode between Stereo & Mono of multiple resources.

5.6.4 Audio Gain Tool

Audio Gain

- Used for adjusting audio gain of multiple resources.
- Allows setting the primary and secondary audio levels.

5.6.5 Channel Tool

Channel

- Used for assigning RF output channels to multiple resources.

Procedure

This procedure shows how to use the mass configuration tools. We show one tool example, all tools function similarly.

1. From the Channels tab, click the **Wand** of any Mass Configuration tool, Figure 5-7.

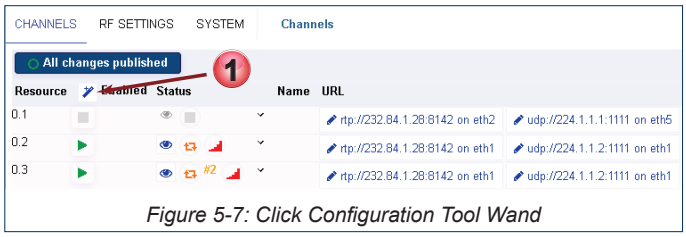

Figure 5-7: Click Configuration Tool Wand

2. Select the desired function that the tool is intended for as some have more than one possible function, Figure 5-8. In this example case it is enabling the selected sources (channels).
3. Click the first (left) Sources selector and choose the first channel of the range to be affected. This is either the single channel you want to affect or the first in a range of channels.
4. Click the second Sources selector and choose the second Source of the range to be affected. For a single channel, select the same channel as the first channel or select the end channel of the range of channels.
5. For selecting more ranges, click the **+** icon then repeat steps 3 and 4. A running total of the remaining items that may be chosen is shown beside the **+**.
6. Click **Save**.

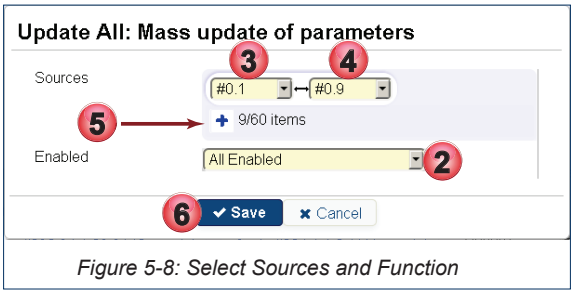

Figure 5-8: Select Sources and Function

You are returned to the Channels tab where the publish button announces that '**x Changes are waiting to be published**'. Click the 2 changes are waiting to be published **Publish** button.

5.7 Add an Input Stream

The Channels tab presents the input streams, streaming status of each resource and provides access to configuration pages. If any channels are to be decrypted, that will be specified as the channel is added or edited so the Decryption Profile must be defined beforehand, see "5.11.1 Decryption Profiles" on page 5-12.

Procedure

This procedure explains how to add an input stream to any resource.

1. Click the **Channels** tab if it is not already selected, Figure 5-9.
2. Chose any resource in the list. In this example we modify **Resource 0.2**.
3. Click the channel's **URL** which is the input multicast stream to which the channel will subscribe. There may already be a factory default stream or one that has been previously defined.

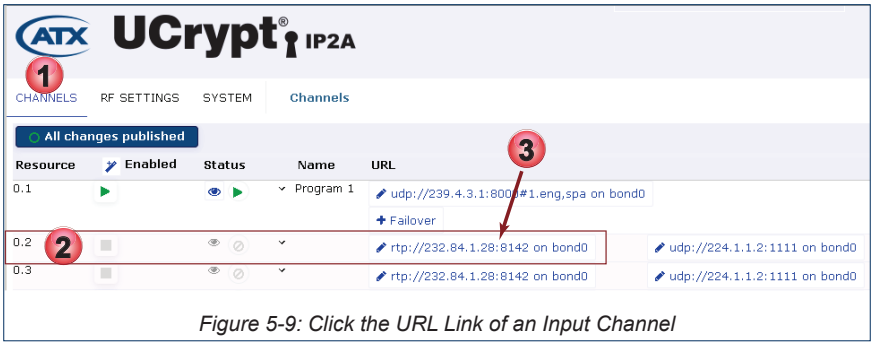

Figure 5-9: Click the URL Link of an Input Channel

4. Edit or fill in the Input Channel form, Figure 5-10 and Table 5.7a.
5. If this program should be decrypted on the output, select the pre-defined **Decryption Profile** from the drop down menu choices. The profiles must be configured before any decryption selection may be made. The default is no decryption. (If profiles are not ready you may return here to select decryption later, saving the change.)
6. Click **Detect**. This action causes the input stream to be read to determine any existing programs.

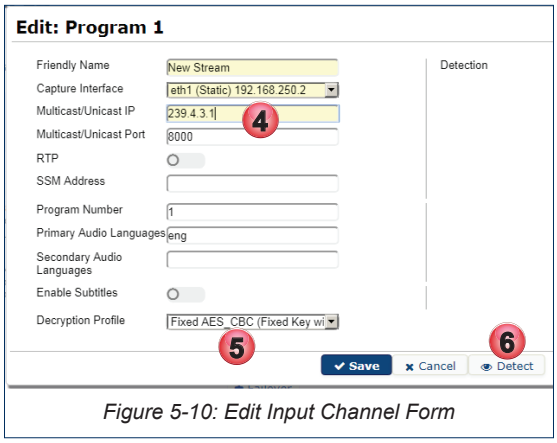

Figure 5-10: Edit Input Channel Form

Table 5.7a: Input Channel Form Settings (See Figure 5-10)

Field	Configurable	Value
Friendly Name	String	A name for identification of this stream in this UI.
Capture Interface	Dropdown Menu	Interface from which to pull the stream (defaults to the Input or Primary Interface).
Multicast/Unicast IP	IP Address	(Multicast) IP Address from which to pull the stream.
Multicast/Unicast Port	IP Address port	(Multicast) IP Port from which to pull the stream.
RTP	Tick Box/Switch	Whether the source uses RTP or regular UDP.
SSM Address	IP Address	Source Specific Multicast (IP address), when specified, only content sent by this IP is processed.
Program Number	Scroll Control	MPEG program #, usually detected by the system.
Primary Audio Language	String, string	If specified, the comma separated set of languages to match/select when choosing PIDs. If not specified the first audio PID will be used. If multiple, the Device will try each one in order of listing until it can sync to one language and will then use that one language. If none are listed it will default to the first Audio PID found regardless of the language. Normally three character language specs such as eng, spa.
Secondary Audio Language	String, string	If specified, the comma separated set of languages to match/select when choosing PIDs. If not specified the first audio PID will be used. If multiple, the Device will try each one in order of listing until it can sync to one language and will then use that one language. If none are listed it will default to the first Audio PID found regardless of the language. Normally three character language specs such as eng, spa.
Enable Subtitles	Tick Box/Switch	Click to select subtitles PIDs for processing and inclusion.
Decryption Profile	Dropdown Menu	Only pre-defined profiles will be listed. Select the required profile for this channel.
Detection	Title	A list of the programs detected in the stream (if any) after the Detect button is clicked.
Save	Button	Saves all changes on this form.
Cancel	Button	Cancels changes on this form.
Detect	Button	Detects streams on the Multicast group address entered above.
Swap	Button	Swap the primary and secondary failover roles.

7. The programs detected within the stream, if any, are listed along with languages available, Figure 5-11.
8. Click the **desired program** from the choices to add it to the form (in a multi-program or multi language transport stream there may be more than one but only one program may be selected).
9. By default all available languages will be selected and added. Alternately, click only the language you want.
10. The selected program and language are added to the form.
11. Click **Save**.

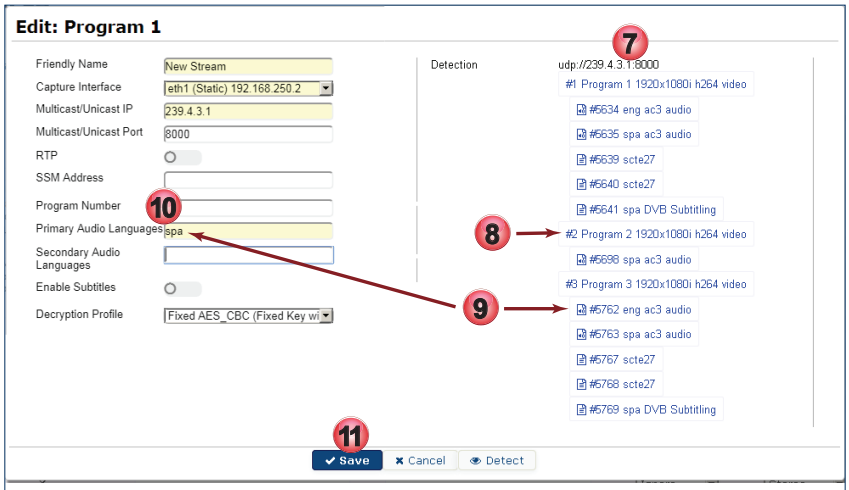

Figure 5-11: Select Detected MPTS Program

12. The Resource needs enabling, click the **Enable Button** icon to turn it to a **green triangle** , see Figure 5-12.

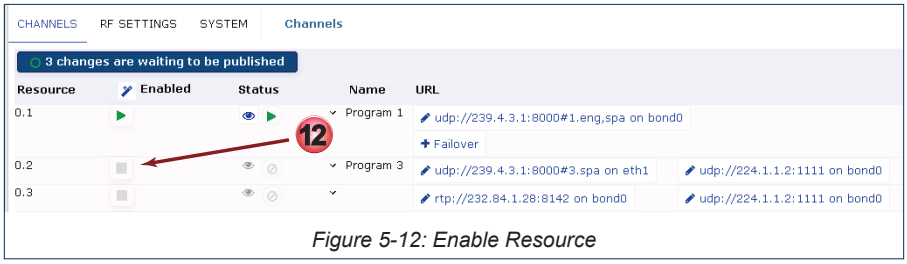

Figure 5-12: Enable Resource

13. The new stream URL values added to the resource are not yet live, Figure 5-13, and the publish button announces that '**3 Changes are waiting to be published**'. The new stream or changes to the stream (could be one or more) are waiting to be published (taken live).
14. Click the **Publish** button.

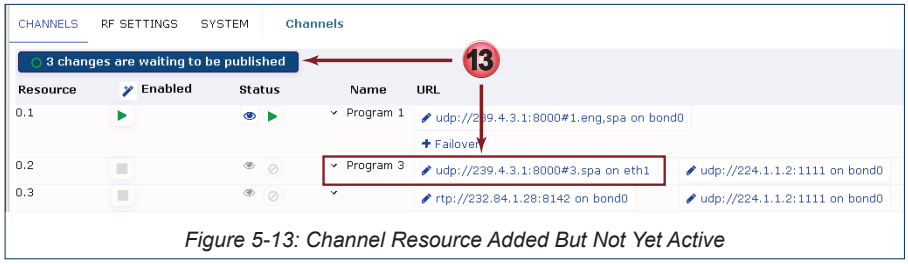

Figure 5-13: Channel Resource Added But Not Yet Active

15. The new stream settings become active as indicated by the **green status triangle** icon. The publish button now announces '**All changes published**', Figure 5-14.

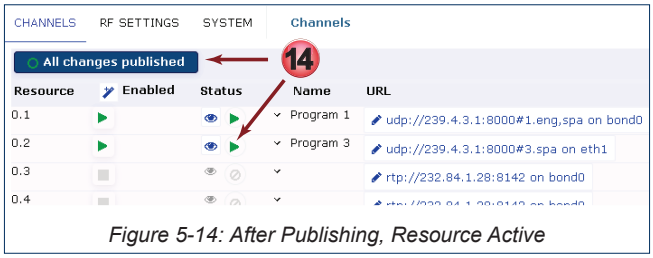

Figure 5-14: After Publishing, Resource Active

16. A preview of this channel is available. Click the **Eye** icon, Figure 5-15
17. A low resolution stream with Primary Audio Channel is presented.
18. To close this stream click the **No Eye** icon beside the preview window.

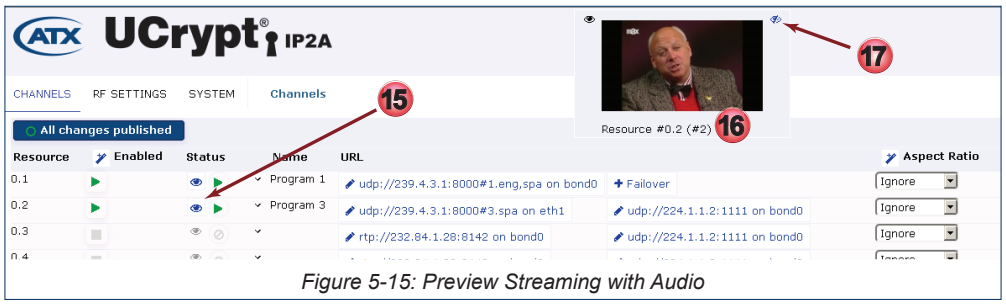

Figure 5-15: Preview Streaming with Audio

5.8 Configure Redundancy Failover

Input streams may have a redundant stream defined. Failover to the backup will automatically occur when the primary feed is unavailable. The return to primary can be defined as automatic '**return to primary**' or '**stay on secondary**'. Feeds may also be manually swapped. If any channels are to be decrypted on the output, that will be specified as the channel is added or edited so the Decryption Profile must be defined beforehand, see "Decryption Profiles" on page 5-12.

Procedure

This procedure explains how to configure redundancy.

1. Click the **Channels Tab** if it is not already selected, Figure 5-16.
2. Click the **+Failover** Failover link for the resource for which redundancy will be defined.

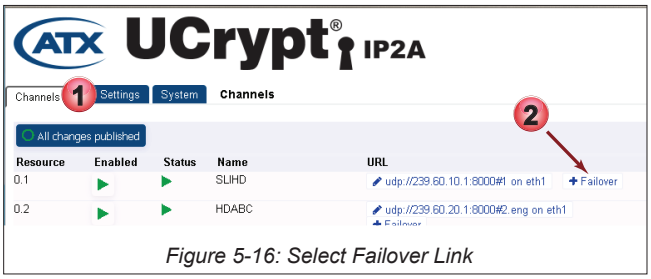

Figure 5-16: Select Failover Link

3. Edit the Failover form settings according to your system requirements, Figure 5-17, and use Table 5.8a for guidance. By default the system assumes that the IP address and port as well as program number and language matches the primary feed.
4. If this program should be decrypted on the output, select the pre-defined **Decryption Profile** from the drop down menu choices. The profiles must be configured before any decryption selection may be made. The default is no decryption. (If profiles are not ready you may return here to select decryption later, saving the change.)
5. Click **Detect**. Note that 'Detecting' the programs is only technically necessary if the failover feed **is not the same** IP address, port, program number and language as the primary as would be the case for a redundant stream which is an exact copy of the main stream on a different interface. Detecting the programs allows a **different** program to be used as failover. If the failover and main IP address, port, program number and language match, go to step 9.

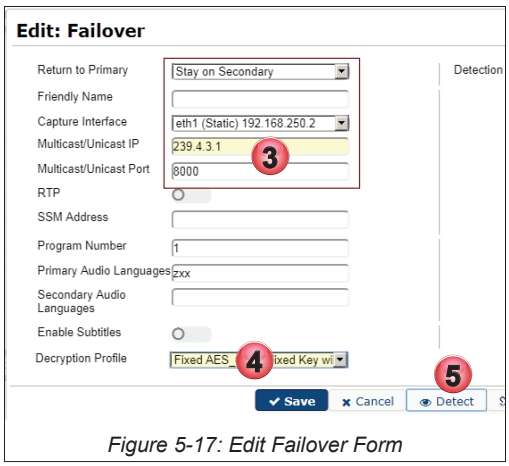

Figure 5-17: Edit Failover Form

Table 5.8a: Failover Form Settings (See Figure 5-17)

Field	Configurable	Value
Return to Primary	Dropdown Menu	Strategy to apply: **return to primary** or **stay on secondary**.
Friendly Name	String	User-friendly description of the stream content in this UI.
Capture Interface	Dropdown Menu	Interface from which to pull the stream (defaults to the Primary Interface). If there have been VLANs or Bonds created, those choices appear also.
Multicast Group	IP Address	The backup stream Multicast IP Address from which to pull the stream.
Multicast Port	Integer	The backup stream IP Port from which to pull the stream.
RTP	Tick box/Switch	Tick/select if the source uses RTP, leave unticked/unselected for regular UDP.
SSM	IP Address	Source Specific Multicast IP. When specified, only content sent by this IP is processed.
Program Number	Integer	Program # of backup stream.
Primary Audio Language	String, string	If specified, the comma separated set of languages to match/select when choosing PIDs. If not specified the first audio PID will be used. If multiple, the Device will try each one in order of listing until it can sync to one language and will then use that one language. If none are listed it will default to the first Audio PID found regardless of the language. Normally three character language specs such as eng, spa.
Secondary Audio Language	String, string	If specified, the comma separated set of languages to match/select when choosing PIDs. If not specified the first audio PID will be used. If multiple, the Device will try each one in order of listing until it can sync to one language and will then use that one language. If none are listed it will default to the first Audio PID found regardless of the language. Normally three character language specs such as eng, spa.
Enable Subtitles	Tick Box/Switch	Click to select subtitles PIDs for processing and inclusion.
Decryption Profile	Dropdown Menu	Only pre-defined profiles will be listed. Select the required profile for this channel.
Detection	Title	A list of the programs detected in the stream (if any) after the Detect button is clicked.
Save	Button	Saves all changes on this form.
Cancel	Button	Cancels changes on this form.
Detect	Button	Detects streams on the Multicast group address entered above.
Break	Button	Break the failover pair, delete this secondary resource.
Swap	Button	Swap the primary and secondary failover roles.

6. The programs will be detected on the Multicast Group stream and displayed, Figure 5-18. Each program line listed is a link to add that program as the backup. An SPTS will only display one stream, and an MPTS will display all streams.
7. Click the desired program for backup. The selected program is added to the form.
8. Click the desired language (if multiple languages are present, all are selected by default but you can manually select a single language). The selected languages are added to the form.
9. Click **Save** when finished.

NOTE: *Mousing over the configuration fields shows tool tips for help in configuration.*

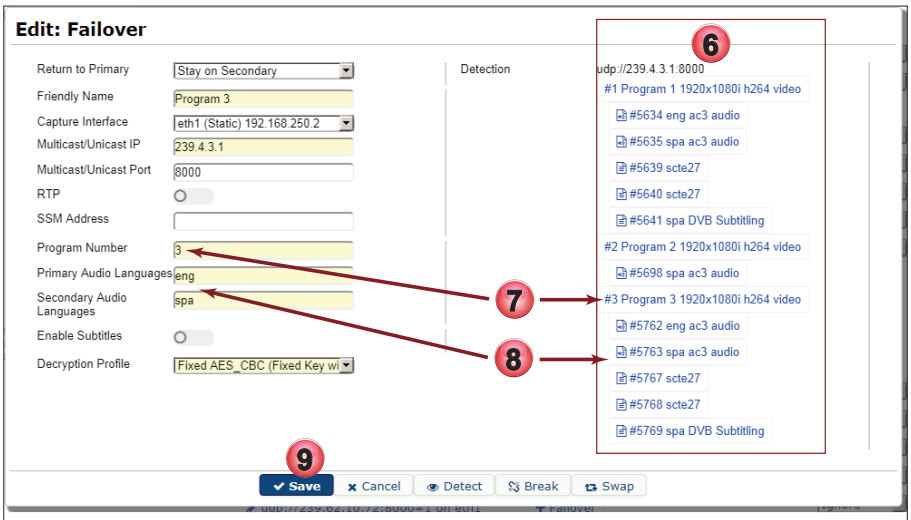

Figure 5-18: Save Failover Form

10. The backup stream is added to the resource line, but is not yet active as the publish button announces **'1 Change is waiting to be published'**, Figure 5-19.
11. Click the **Publish** button.

The stream is now ready to perform as backup to the primary stream.

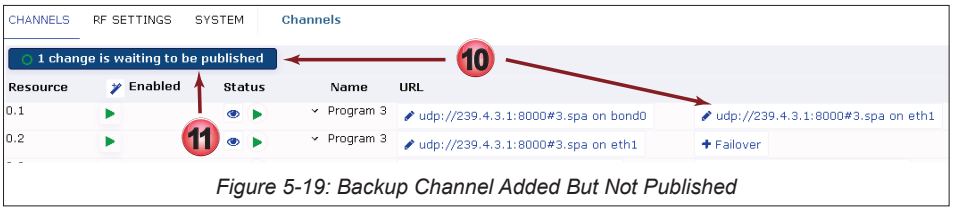

Figure 5-19: Backup Channel Added But Not Published

5.9 Manually Activate the Backup Stream

The primary and secondary streams may be swapped manually.

Procedure

This procedure explains how to manually activate the backup feed.

1. Select the **Channels** tab if it isn't already selected, Figure 5-20.
2. Click the resource's backup feed **URL**.

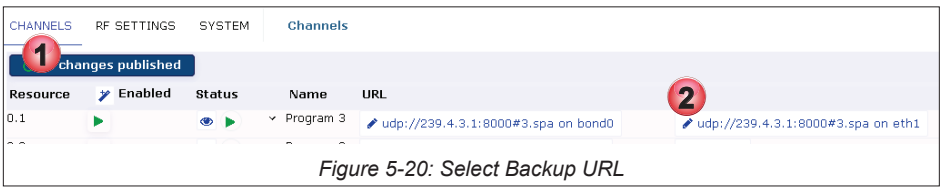

Figure 5-20: Select Backup URL

3. Click **Swap**, Figure 5-21.

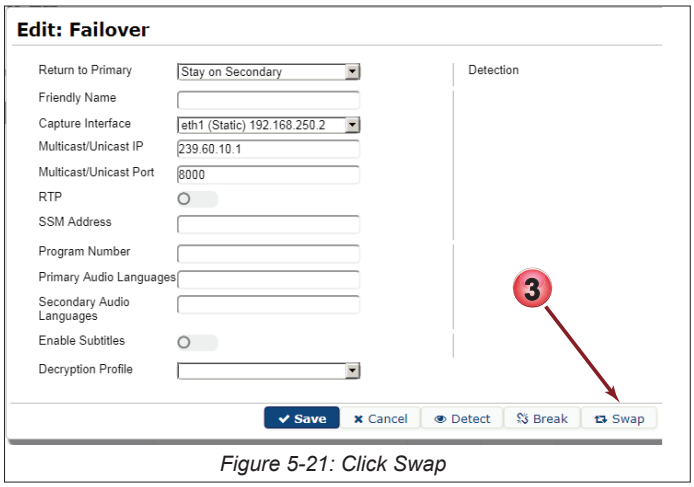

Figure 5-21: Click Swap

4. The backup feed name is now in the list of channels and the main channel URL has shifted to the left column but the swap is not yet active as the publish button announces **1 Change is waiting to be published**, Figure 5-22.
5. Click the **Publish** button.

The backup stream is now the main stream for this channel and will stay the main stream due to the choice of '**stay on secondary**'. See the new feed in the **Name** column. The stream that was formerly the main stream is now not in use and must be manually switched back if desired.

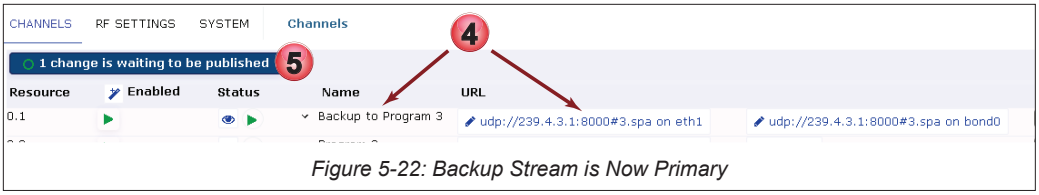

Figure 5-22: Backup Stream is Now Primary

5.10 Setup the Output Analog Channels

The UCrypt Device comes pre-configured with all channels defined but any channel may be re-assigned easily by typing in the new channel number. Duplicates are not allowed so first delete any channels to be moved to avoid duplication.

1. Click the **Channels** tab if it is not already selected, Figure 5-23.
2. The channel assignments within the chosen plan are pre-defined in text boxes which are both dropdown menus of available choices and searchable by typing a number.
3. Clicking the box presents the current assignment highlighted and allows other choices. Typing any number will activate the search menu which lists all candidates that meet the criteria both in frequency and channel number.

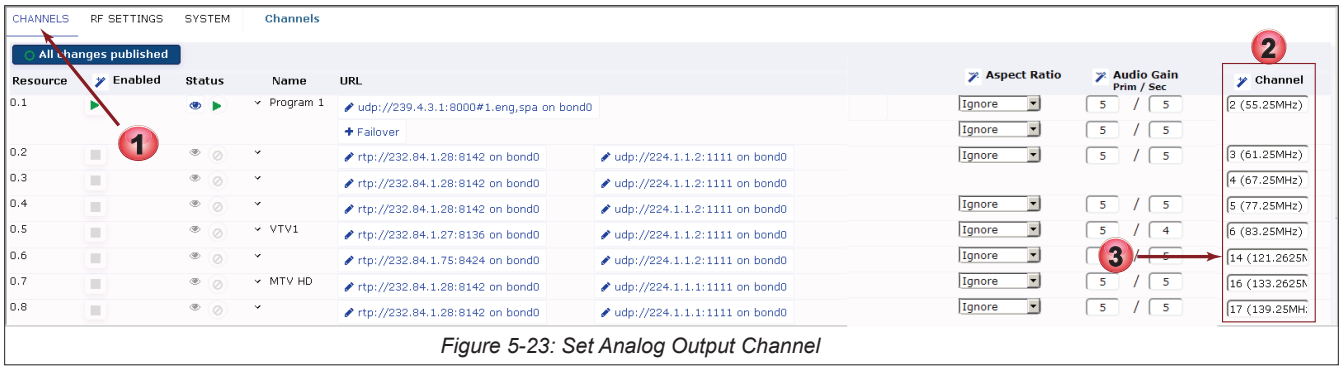

Figure 5-23: Set Analog Output Channel

4. Select your desired channel assignment from the dropdown menu of choices, Figure 5-24.

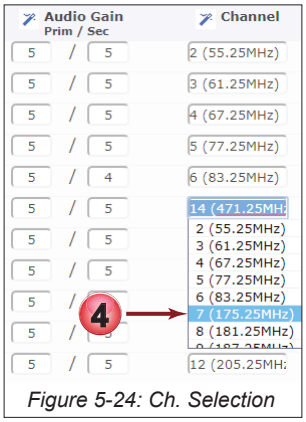

Figure 5-24: Ch. Selection

5. The new channel is assigned and the frequency is displayed with the channel for your convenience, Figure 5-25.

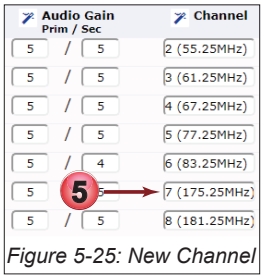

Figure 5-25: New Channel

6. The changes need to be published as the publish button announces **4 changes waiting to be published**. Click the **Publish** button, Figure 5-26.

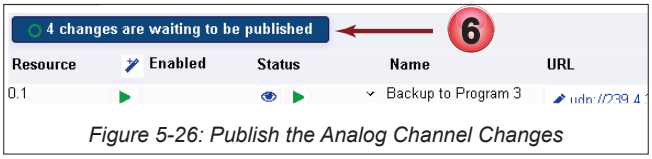

Figure 5-26: Publish the Analog Channel Changes

5.11 Decryption

The QAM to Analog UCrypt is capable of Fixed Key Decryption. Multiple profiles may be setup and saved for simple activation. Decryption Profiles may be applied on any or all of the resources on a channel by channel basis. The types of decryption include ECB (Electronic Codebook) and CBC (Cypher Block Chaining) whereas the decryption profiles describe the parameters to be used for decryption. Decryption Profiles are created or accessed from the bottom of the Channels page, see Figure 5-27, and decryption is activated per channel by clicking the channel URL, opening the channel edit form.

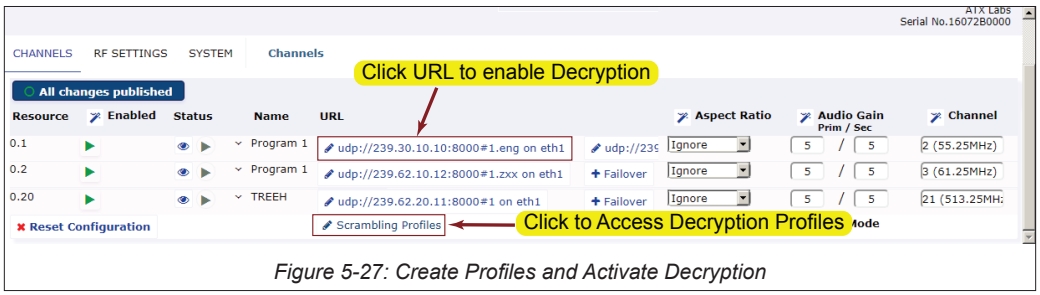

Figure 5-27: Create Profiles and Activate Decryption

5.11.1 Decryption Profiles

Decryption profiles allow the decryption configurable values to be saved and applied to each channel that requires decryption. The created profiles appear on each channels configuration form. Profiles may be imported from files, see “5.11.2 Decryption Profile Import/Export” on page 5-13.

Procedure

This procedure explains how to create a Decryption Profile and assign it to a channel.

1. Click the **Channels** tab if it is not already selected, Figure 5-28.
2. At the page bottom, click **Scrambling Profiles**.

Figure 5-28: Click Scrambling Profiles

3. Click **+Fixed Key**, Figure 5-29, to create a new Fixed Key Decryption Profile.

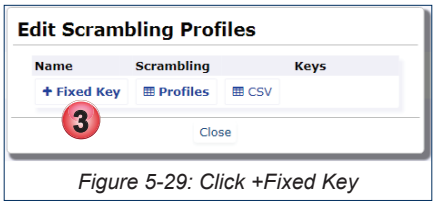

Figure 5-29: Click +Fixed Key

4. Enter a name for the new profile. This will be used to identify it within the GUI.
5. Select Decryption type from the drop down menu: Fixed Key with AES CBC or Fixed Key with AES ECB. In the following example we show creation of the CBC key but ECB keys are created in the exact same way, less the Initialization Vector.
6. Click **Save**.

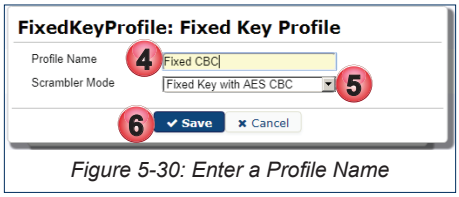

Figure 5-30: Enter a Profile Name

7. In the Key configuration form that opens, Figure 5-31 configure the Even Key by typing or pasting the key value.

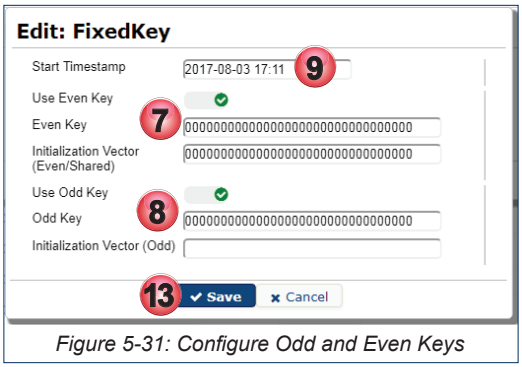

Figure 5-31: Configure Odd and Even Keys

8. Configure the Odd Key by typing or pasting the key value, Figure 5-31. If this is the CBC type decryption, type or paste the Initialization Vector.

Table 5.11a: Decryption Profile Form Settings (See Figure 5-30)

Field	Configurable	Value
Start Timestamp	Clickable Config.	The future time to start decryption.
Use Even Key	Tick Box/Switch	Click to activate use of Even Key Decryption. Requires defining the Even Key.
Even Key	String	32 Hexadecimal Digits defining the even 128-bit decryption key for the TS encoding.
Initialization Vector (Even/Shared)	String	32 Hexadecimal Digits defining the initialization vector (IV) for fixed-key TS encoding used with Even key, or both if no Odd IV is specified.
Use Odd Key	Tick Box/Switch	Click to activate use of Odd Key Decryption. Requires defining the Odd Key.
Odd Key	String	32 Hexadecimal Digits defining the odd 128-bit decryption key for the TS encoding.
Initialization Vector (Odd)	String	32 Hexadecimal Digits defining the initialization vector (IV) for fixed-key TS encoding used with Odd key. If left blank (the default setting), the Odd Key IV will use the Even Key IV value specified above.
Save	Button	Saves the changes made on this form.
Cancel	Button	Cancels changes made and returns to the previous window.

9. If the decryption is to start at a future time, click the **Start Timestamp** dialog, see Figure 5-31, which opens a clickable Time/Date configuration window, Figure 5-32.
10. In the Time/Date dialog, configure the start date by clicking the **day of the week** and use the forward and backward arrows to **choose a month and year**.
11. Click the **Time** tab then use the sliders to set minutes and seconds as necessary.
12. Click **Save** when done.

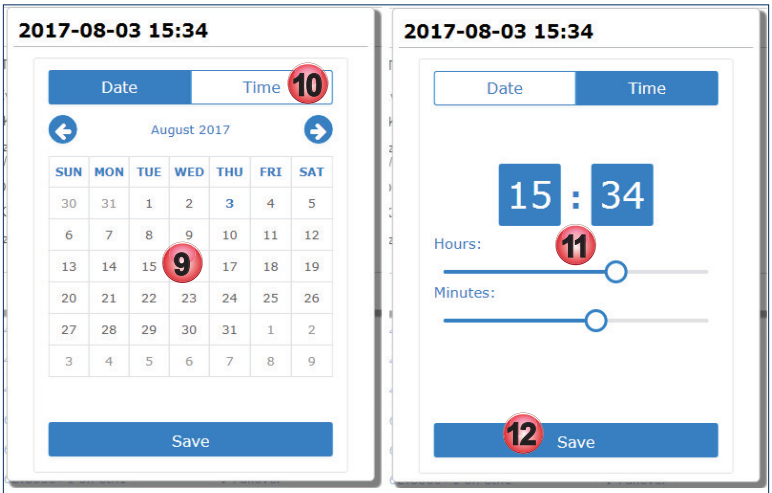

Figure 5-32: Configure Clock/Calendar

13. Click **Save** when returned to the original Fixed Key Edit dialog, see Figure 5-31.

Return to the Channels tab then click the **Publish** button to take these decryption profile changes live.

5.11.2 Decryption Profile Import/Export

Two file types are supported for import or export of Decryption Profiles to make setting up decryption faster, easier and less prone to error. Choose the file format best suited to your application or file formats available to you.

- JSON File Format
- CSV File Format

Decryption Profiles may be imported to the Device if a profile file exists (perhaps exported from another machine) saving time to create each profile repeatedly while mass deploying UCrypt Devices. It is also possible to download to your computer the currently defined profiles in both file formats. If a new profile has been created it may be exported to be used on other UCrypt Devices.

Procedure

This procedure explains how to upload new Decryption Profiles or download current Decryption Profiles in either JSON (JavaScript Object Notation) or CSV (comma separated values) format. Working with JSON or CSV files is similar so we show both examples together for clarity.

1. Click the **Channels** tab if it is not already selected, Figure 5-33.
2. At the page bottom, click **Scrambling Profiles**.

Figure 5-33: Click Scrambling Profiles

3. Click **Profiles**, to work with Decryption Profiles in **JSON** format, or click **CSV** to work with Decryption Profiles in **CSV** format, Figure 5-34.

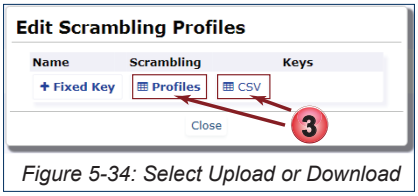

Figure 5-34: Select Upload or Download

4. To save current Decryption Profiles to your computer in whatever format you have selected, click the **Download** link, Figure 5-35. The profile is downloaded to your usual browser downloads folder.
5. To import or upload an existing Decryption Profiles file in either format to the Device click the **Choose File** button to browse to the file using the file explorer window that opens.
6. For CSV files only, click the **Ignore Unknown** switch to instruct the Device to ignore any unknown values within the imported CSV file. This is due to the differences between CBC and ECB decryption Key requirements.
7. Click **Save** to save any uploaded files to the Device.

Return to the **Channels** page and click the **Publish Button** to take these changes live.

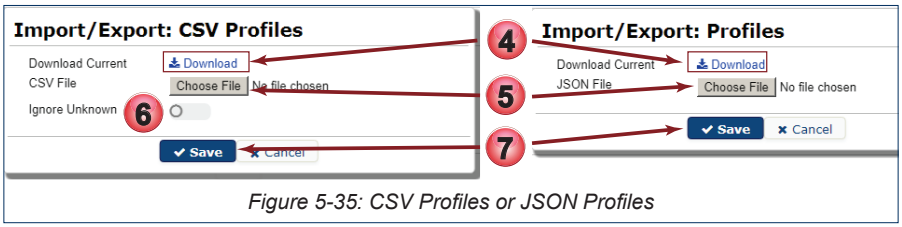

Figure 5-35: CSV Profiles or JSON Profiles

The CSV file format opened in a spreadsheet program is shown in Figure 5-36. This form may be manually filled then imported.

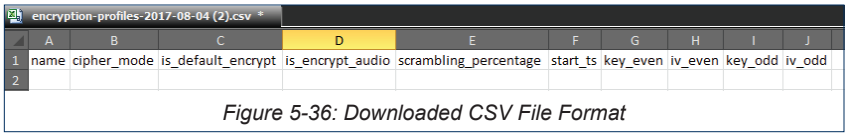

Figure 5-36: Downloaded CSV File Format

SYSTEM TAB

6. System Tab

This tab contains the platform Global settings and includes the categories of Network Configuration, User Configuration, Firmware Upgrades, System Time, SNMP and more.

6.1 Chapter Contents

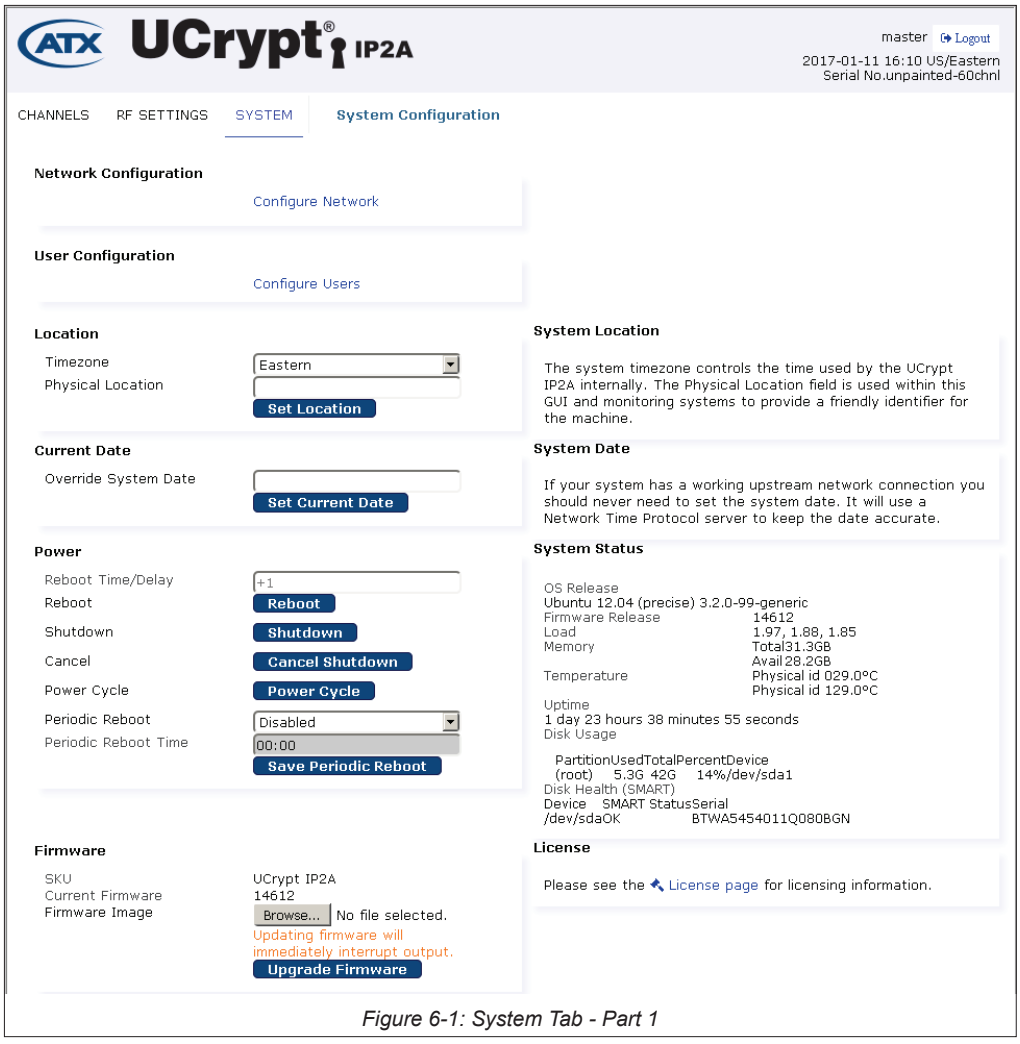

Figure 6-1: System Tab - Part 1

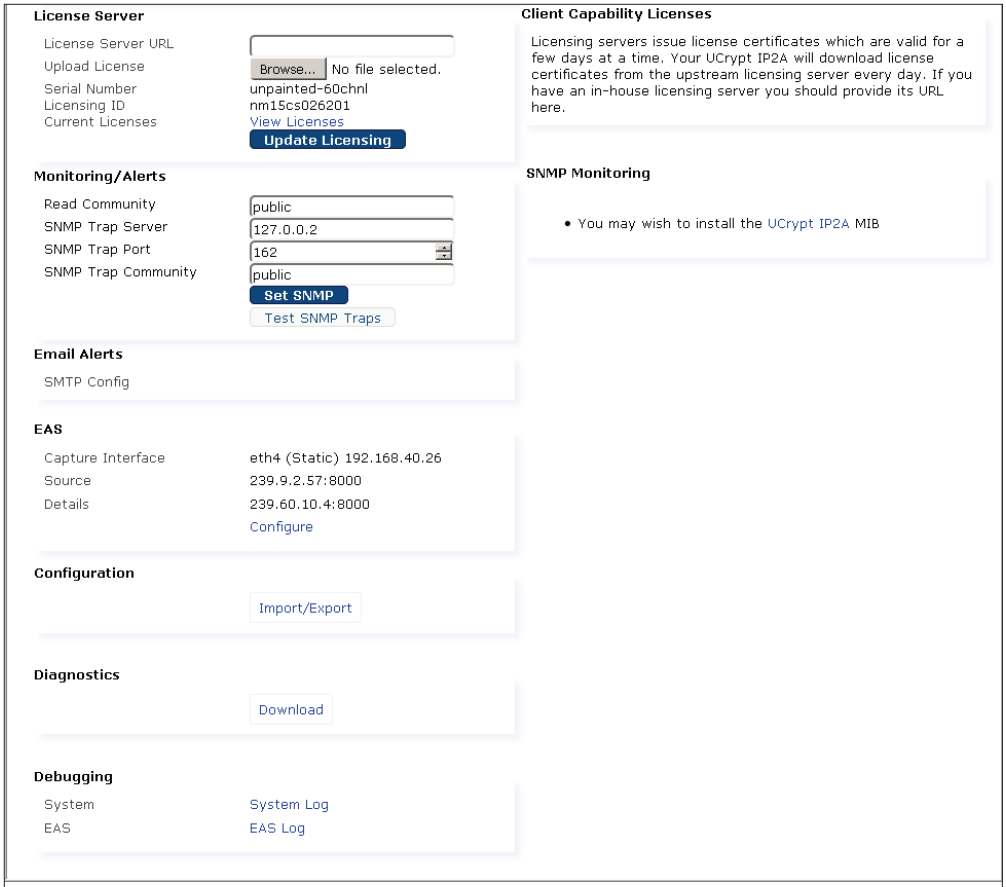

Figure 6-2: System Tab - Part 2

6.2 Network Configuration

From this page, Figure 6-3, you may edit the physical Ethernet port IP addresses and create VLANs.

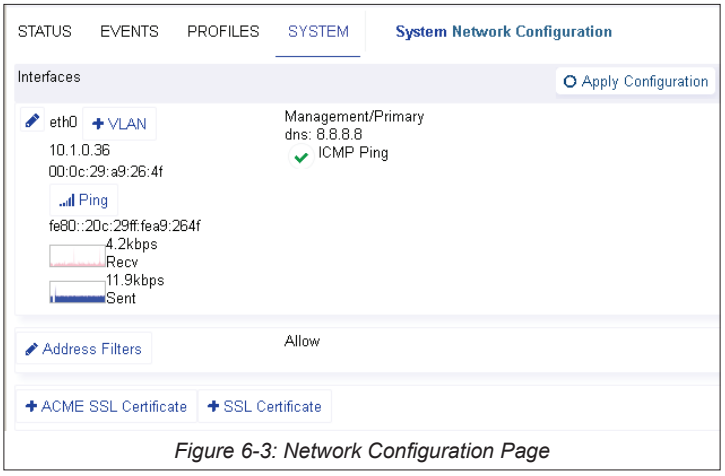

Figure 6-3: Network Configuration Page

NOTE: *Mousing over the page fields shows tool tips for help in configuration.*

6.2.1 Interface Role

All Ethernet network interfaces may have their role defined in their respective Edit Forms, see Figure 6-4, as one of the following interface types with the conditions and limitations listed below (to access this feature see “6.2.2 Edit a Network Interface” on page 6-3).

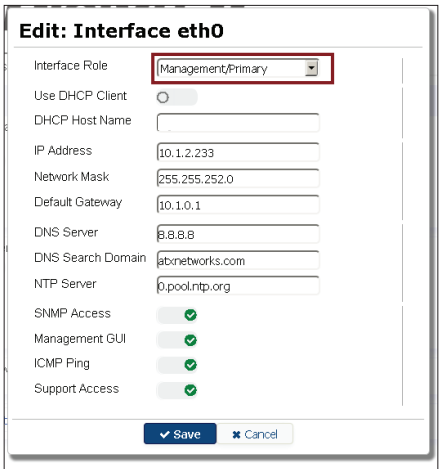

Figure 6-4: Defining Interface Role

Management Role

- By factory default eth0 will be defined with this role.
- Only one interface can be given Management/Primary role and there **must always** be one interface with this role.
- This is the only role which allows assignment of Gateway, DNS server, DNS search domain and NTP server.

External IP In

- The interface which will be used for IP input if a specific interface is not set when defining the source (This role is only useful for Device models which accept IP input).
- An interface defined as ‘External IP In’ may have the Management GUI, SNMP Access & Support Access ports enabled if desired via the respective toggle switches.

6.2.2 Edit a Network Interface

Your application of the Server will likely require the factory default network settings to be configured. The factory default address of 192.168.0.23 is only provided to allow you to access this configuration.

Procedure

This procedure describes editing of the network port eth0 to change IP addresses to suit your network requirements.

1. Click the **System** tab if it isn’t already selected, Figure 6-5.
2. Click **Configure Network** under Network Configuration section.

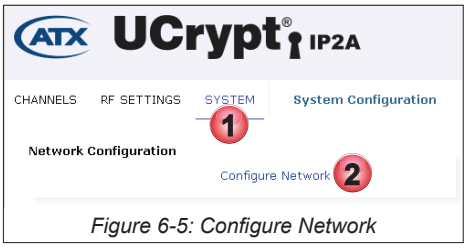

Figure 6-5: Configure Network

3. To edit the eth0 management network settings click the **Edit Icon** on eth0 interface, Figure 6-6.

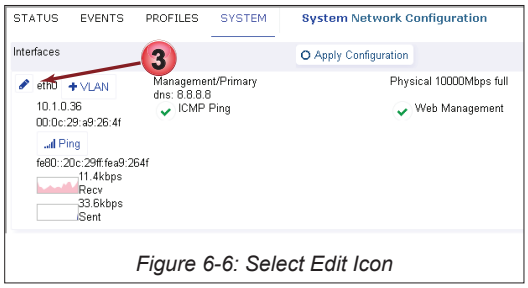

Figure 6-6: Select Edit Icon

4. Edit default values or fill in the Interface Settings form, Figure 6-7 per Table 6.2a and/or your requirements.
5. Click **Save** when finished with edits.

NOTE: *The Interface Role for Management Port eth0 should not be changed from the default value Management/Primary.*

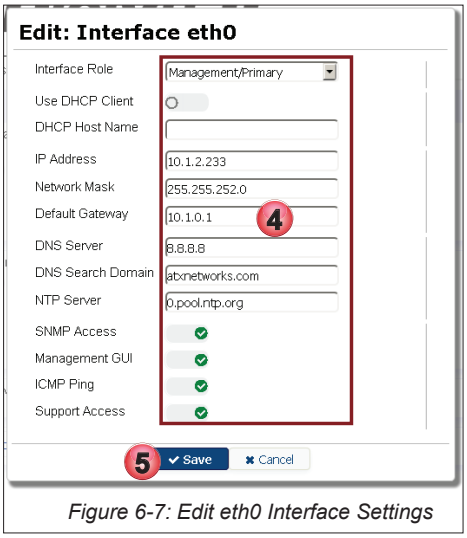

Figure 6-7: Edit eth0 Interface Settings

Table 6.2a: Ethernet Interface Form Values (See Figure 6-7)

Field	Configurable	Value
Interface Role	Dropdown Menu	Management/Primary. Do not change this value for eth0.
Use DHCP Client	Tick Box/Switch	Un-Ticked (Grayed out) for static IP address, tick (checked) for DHCP.
DHCP Host Name	String	Host name used in DHCP requests.
IP Address	IP Address	IP Address v4 or v6
Network Mask	IP Subnet Mask	Network Mask, (ffff:ffff:ffff:: or 255.255.255.0 format).
Default Gateway	IP Address	Routing Gateway for the Interface.
DNS Server	IP Address	DNS Server, only used if specified here.
DNS Search Domain	URL	As required by your network.
NTP Server	IP Address/URL	Network Time Protocol server to which to synchronize this Device.
SNMP Access	Tick Box/Switch	Tick to allow SNMP messages on this interface then the SNMP port will be exposed on this interface.
Management GUI	Tick Box/Switch	Ticked to expose UI ports on this interface. Must be active on at least one interface.
ICMP Ping	Tick Box/Switch	Tick to enable ping response on this interface.
Support Access	Tick Box/Switch	If enabled, the support (ssh) port will be exposed on this interface; note it is strongly encouraged to leave this enabled on at least one interface.

6. When saved, eth0 values are changed but not yet activated on the Server, Figure 6-8.
7. Click **Apply Configuration** to activate the changes.

You will need to log in again using the new IP address in your browser if the Monitoring Server IP address was changed.

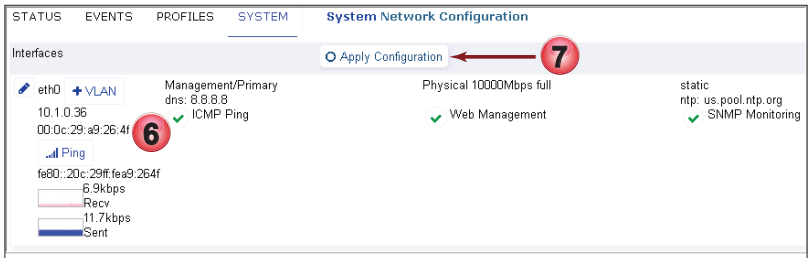

Figure 6-8: Changed Values Applied to eth0

6.2.3 Monitor Network Performance

It is possible to view the aggregate network traffic Histogram on any Ethernet interface occurring over a period of time.

Procedure

This procedure describes monitoring of the network performance histogram.

1. Click the **System** tab if it isn't already selected, Figure 6-9.
2. Click **Configure Network** under Network Configuration section.

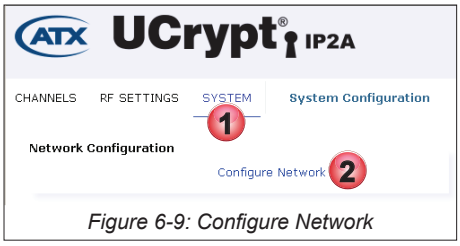

Figure 6-9: Configure Network

3. A Histogram of network data sent and received over each individual interface is updated every 10 seconds and shows continuous history for as long as the window is open, Figure 6-10. The current data rate is also shown in Mbps or kbps. The data rate histogram is for comparative purposes only and is not calibrated.

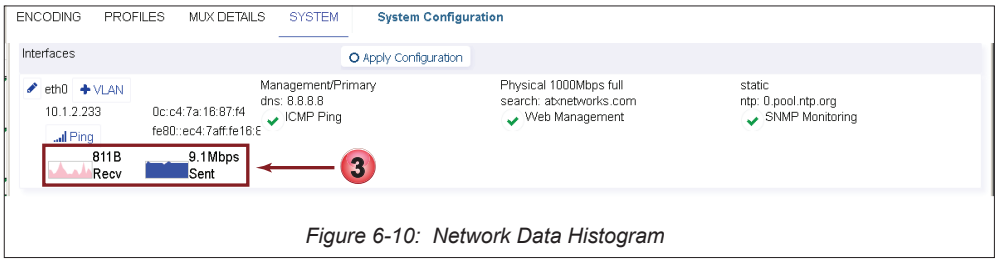

Figure 6-10: Network Data Histogram

6.2.4 Ping Target

Use PING functionality to troubleshoot network connectivity from any Ethernet Interface.

Procedure

This procedure details how to use the ping feature.

1. Click the **System** Tab if it isn't already selected, Figure 6-11.
2. Click **Configure Network** under Network Configuration section.

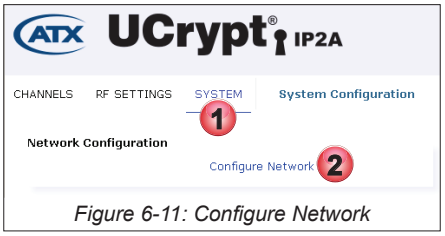

Figure 6-11: Configure Network

3. Click the **Ping** Ping button on any Ethernet port to initiate the Ping function on that interface, Figure 6-12.

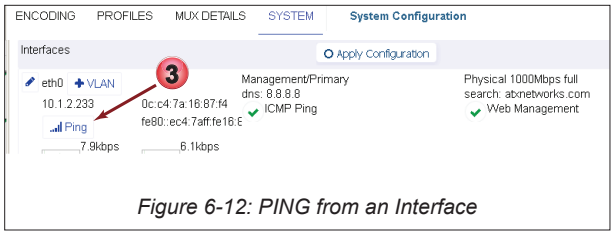

Figure 6-12: PING from an Interface

4. Enter the Target IP address of the device to be pinged, Figure 6-13.
5. Click the **Ping** button.

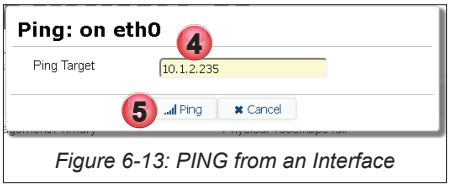

Figure 6-13: PING from an Interface

6. The ping results are shown, Figure 6-14. To continue with another ping to this address, click **Ping** again.
7. Alternately try another target by entering its IP address then click **Ping**.

Click **Cancel** to exit the Ping function.

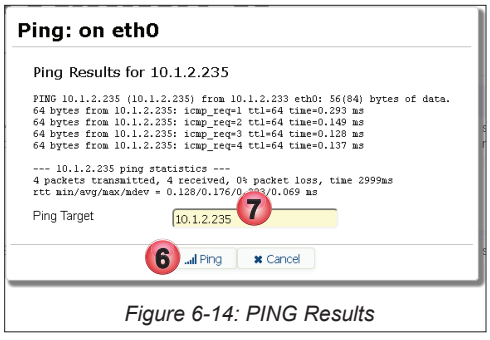

Figure 6-14: PING Results

6.2.5 Configure IP Address Filter

Security concerns may dictate that only certain IP addresses may connect to this Server. You may set up IP addresses that are specifically allowed or specifically excluded from logging into the Device.

Procedure

This procedure explains how to configure IP Address filters.

1. Click the **System** Tab if it isn't already selected, Figure 6-15.
2. Click **Configure Network** under Network Configuration section.

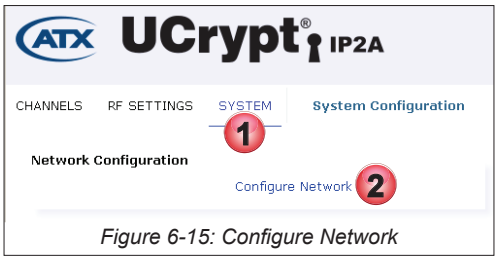

Figure 6-15: Configure Network

3. Click the **Edit Address Filters** Address Filters button, Figure 6-16.

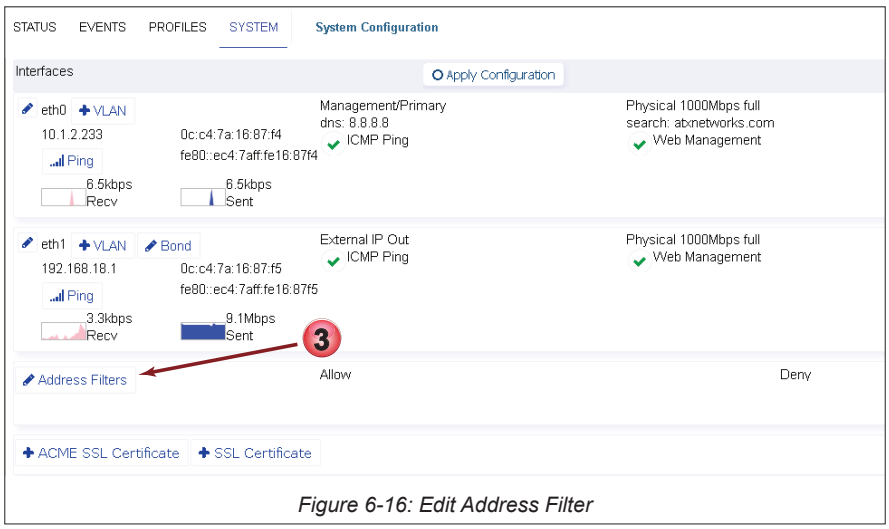

Figure 6-16: Edit Address Filter

4. In the window that opens, enter the IPv4 addresses or networks in CIDR notation that will be allowed or denied access to this machine GUI in the corresponding dialog box, Figure 6-17.
   - CIDR Notation examples: CIDR 192.168.100.0/32 is the same as 192.168.100.1 / 255.255.255.255
     CIDR 192.168.100.0/24 is the same as 192.168.100.0 / 255.255.255.0
     CIDR 192.168.100.0/16 is the same as 192.168.100.0 / 255.255.0.0
5. Click **Save**.

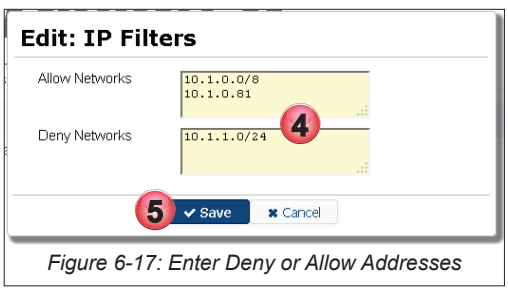

Figure 6-17: Enter Deny or Allow Addresses

6. The entered addresses are displayed adjacent the Edit Address Filters button, Figure 6-18

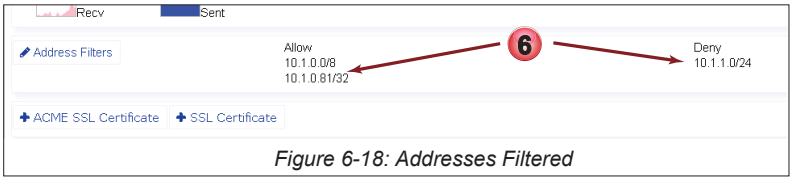

Figure 6-18: Addresses Filtered

6.2.6 Create ACME SSL Certificate

The Automated Certificate Management Environment (ACME) protocol is a communications protocol allowing the automated deployment of public key infrastructure. It was designed by the Internet Security Research Group (ISRG) for their free **Let's Encrypt** service. An ACME certificate may be easily installed in the device through an automated process but it will be necessary to have a registered domain name for the Device. Detailed information about obtaining a certificate is available at https://letsencrypt.org/.

Procedure

This procedure explains how to add an Acme SSL Certificate to the Device.

1. Click the **System** Tab if it isn't already selected, Figure 6-19.
2. Click **Configure Network** under Network Configuration section.

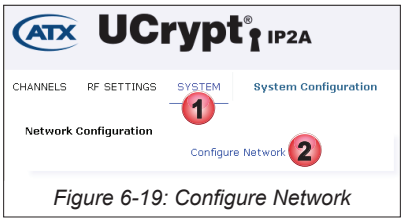

Figure 6-19: Configure Network

3. Click the **+ ACME SSL Certificate** + ACME SSL Certificate button, Figure 6-20.

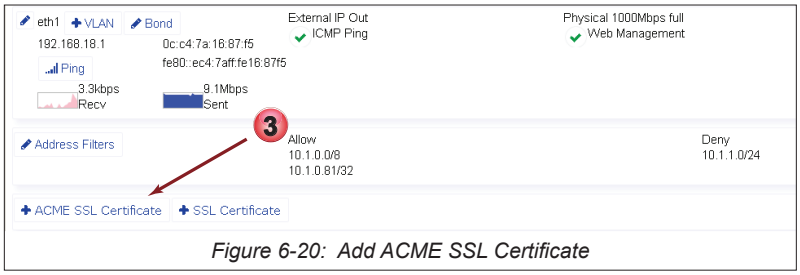

Figure 6-20: Add ACME SSL Certificate

4. Update the form with **Domain Names**, Figure 6-21.
5. Read the TOS (Terms of Service) Subscriber Agreement, then click **TOS Presented**.
6. Accept the Subscriber Agreement by clicking **TOS Accepted**.
7. Click **Save**.

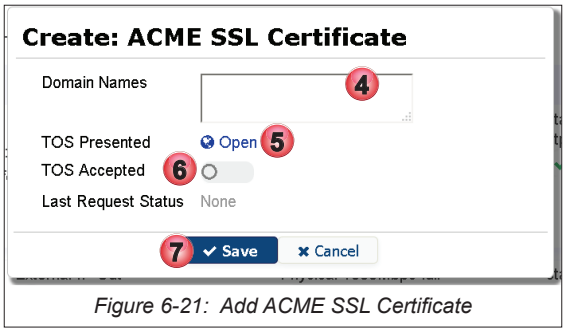

Figure 6-21: Add ACME SSL Certificate

6.2.7 Install SSL Certificate

SSL (Secure Sockets Layer) Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server such as the one within this device, it activates the padlock and the https protocol and allows secure connections from the Device to a browser. Once a secure connection is established, all traffic between the server and the web browser will be secure. This tool allows the installation of your own self signed SSL certificates. This is useful if you already have an internally trusted self signing authority.

Procedure

This procedure explains how to install an SSL Certificate to this device.

1. Click the **System** Tab if it isn't already selected, Figure 6-22.
2. Click **Configure Network** under Network Configuration section.

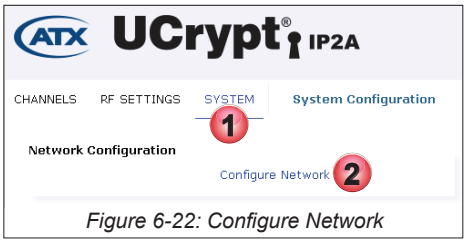

Figure 6-22: Configure Network

3. Click the **+ SSL Certificate** button, Figure 6-23.

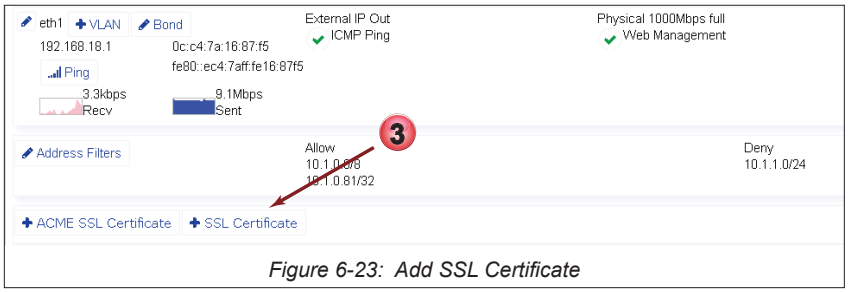

Figure 6-23: Add SSL Certificate

4. To upload an SSL Private Key, click the Private Key **Browse** button then browse for and select the previously saved certificate file, Figure 6-24.
5. To upload an SSL Public Certificate, click the Public Certificate **Browse** button then browse for and select the previously saved certificate file.
6. Click **Save**.

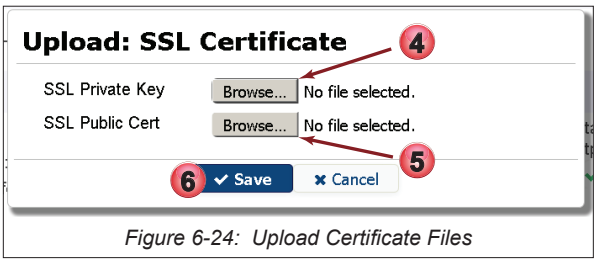

Figure 6-24: Upload Certificate Files

6.2.8 Create or Edit VLAN

Your application may require a management VLAN to allow remote Device management over one of the network interfaces. We will show here how to create a management VLAN on the interface eth1 on the Device. We do not explain all the steps required to set up a VLAN system on your equipment.

1. Click the **System** tab if it isn't already selected, Figure 6-25.
2. Click **Configure Network** under Network Configuration section.

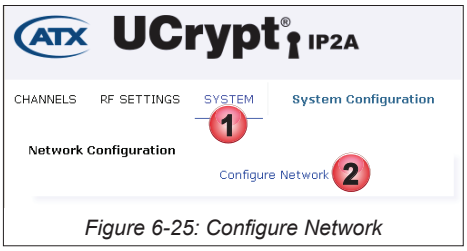

Figure 6-25: Configure Network

3. Click **+VLAN** on the eth1 (or other) interface to add a VLAN for remote Device management over the network interface.

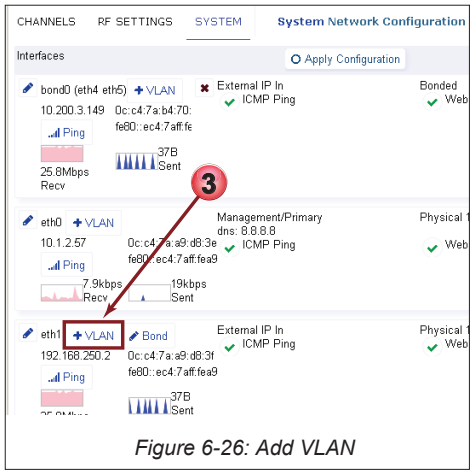

Figure 6-26: Add VLAN

4. Edit or fill in the VLAN settings form, Figure 6-27, according to Table 6.2a and your system requirements.
5. Click **Save** when finished.

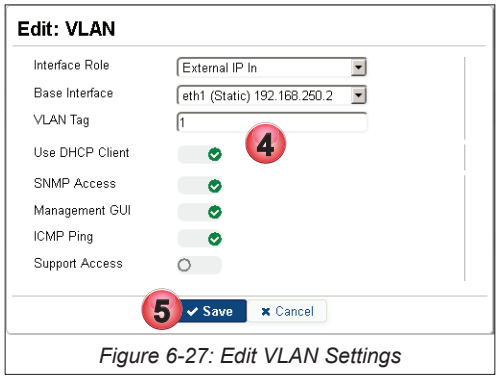

Figure 6-27: Edit VLAN Settings

NOTE: *Mousing over the configuration fields shows tool tips for help in configuration.*

Table 6.2a: VLAN Form Settings (See Figure 6-27)

Field	Configurable	Value
Interface Role	Dropdown Menu	Management/Primary if this is what you want to set up. Alternately, select
Base Interface	Dropdown Menu	Base address on which VLAN will operate.
VLAN Tag	Integer	802.1Q VLAN Tag identifier to apply to the connection
Use DHCP Client	Tick Box/Switch	Un-Ticked (Grayed out) for static IP address, tick (checked) for DHCP
DNS Server	IP Address/URL	DNS Server, only used if specified.
DNS Search Domain	String	DNS Search Domain only if required by your network.
NTP Server	IP Address/URL	Network Time Protocol Server to which to synchronize.
SNMP Access	Tick Box/Switch	Tick to allow SNMP messages on this interface then the SNMP port will be exposed on this interface.
Management GUI	Tick Box/Switch	Ticked to expose UI ports on this interface. Must be active on at least one interface.
ICMP Ping	Tick Box/Switch	Tick to enable ping response on this interface.
Support Access	Tick Box/Switch	If enabled, the support (ssh) port will be exposed on this interface; note it is strongly encouraged to leave this enabled on at least one interface.

6. VLAN is added to Interfaces but is not yet activated, Figure 6-28.
7. Click **Apply Configuration** to activate changes.
8. If it is required to edit an existing interface, click the **Pencil** icon for each interface to be edited. Always click the **Apply Configuration** button after all changes have been made.

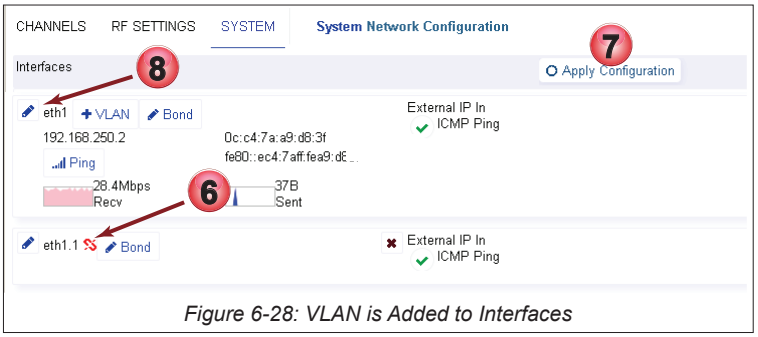

Figure 6-28: VLAN is Added to Interfaces

6.3 Ethernet Interface Bonding

A feature enabling bonding may be configured on the Ethernet interfaces. Bonding, also called port trunking or link aggregation, means combining network interfaces (NICs) to form a single link, providing either high-availability, load-balancing, maximum throughput, or a combination of these. The available modes of bonding are summarized in Table 6.3a.

NOTE: *For more detailed information on NIC bonding, see* https://help.ubuntu.com/community/UbuntuBonding.

NOTE: *NIC bonding is not allowed on the Management Interface port eth0*

Table 6.3a: Bonding Modes & Description

Mode	Description
802.3ad	IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification. Prerequisite: A switch that supports IEEE 802.3ad Dynamic link aggregation. Most switches will require some type of configuration to enable 802.3ad mode.

Mode	Description
Active Backup	Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.

6.3.1 Add a Bond

Once a bond is added to an interface it is dedicated to this function and it may not be used for another purpose.

Procedure

This procedure explains how to create a bond between two Ethernet ports for redundancy or aggregation.

1. Click the **System** tab if it is not already selected, Figure 6-29.
2. Click **Configure Network** under Network Configuration section.

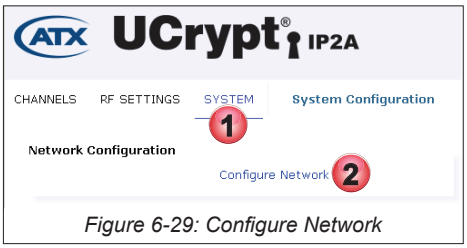

Figure 6-29: Configure Network

3. Click the **Edit Bond** Bond icon on the eth1 interface to add a Bond for this NIC, Figure 6-30.

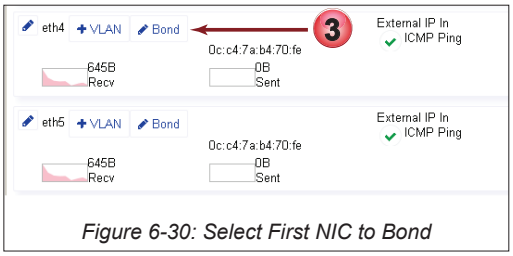

Figure 6-30: Select First NIC to Bond

4. Select **Active Backup** as the Bonding Method and the **Secondary NIC** to bond with from the choices available in the drop down menus, Figure 6-31. See "Table 6.3a: Bonding Modes & Description" on page 6-11 for guidance on the 802.3ad bonding method.
5. When finished, click **Save**.

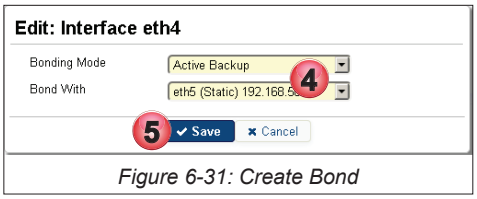

Figure 6-31: Create Bond

6. After creation, Figure 6-32, you may edit the Bond as there are more configuration option default settings that you may be changed as required or to suit your evolving requirements. Click the **Edit Bond** Bond icon next to the interface to be edited.

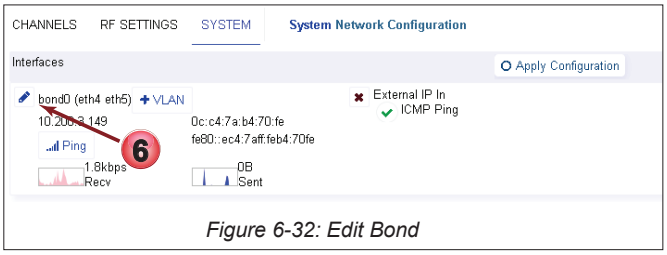

Figure 6-32: Edit Bond

7. Modify settings to your requirements, Figure 6-33. Use Table 6.3a for guidance.
8. Click **Save** when finished with this form.

The changes are saved but not applied. Click the **Apply Configuration** Apply Configuration button on the System Network Configuration page to apply the changes to the Device.

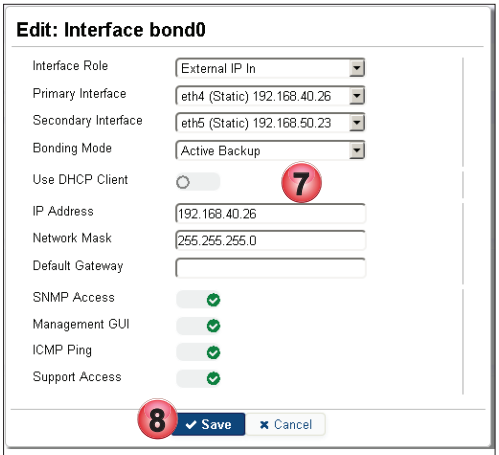

Figure 6-33: Edit Bond Form Settings

Table 6.3a: Bond Interface Settings (See Figure 6-33)

Field	Configurable	Value
Interface Role	Dropdown Menu	The role of the interface. This would have been set to External IP In by default for Active Backup during initial configuration but may be changed here.
Primary Interface	Dropdown Menu	Primary interface for the bond in Active Backup mode, member in other modes.
Secondary Interface	Dropdown Menu	Secondary interface for the bond in Active Backup mode, member in other modes.
Bonding Mode	Dropdown Menu	Bonding mode used to aggregate the interfaces. See “Table 6.3a: Bonding Modes & Description” on page 6-11
Use DHCP Client	Tick Box/Switch	Un-Ticked (Grayed out) for static IP address, tick (checked) for DHCP
IP Address	IP Address	IP Address IPv6 or IPv6
Network Mask	Integer	Network Mask, (ffff:ffff:ffff:: or 255.255.255.0 format).
Default Gateway	IP Address	The default routing gateway.
SNMP Access	Tick Box/Switch	Tick to allow SNMP messages on this interface then the SNMP port will be exposed on this interface.
Management GUI	Tick Box/Switch	Ticked to expose UI ports on this interface. Must be active on at least one interface.
ICMP Ping	Tick Box/Switch	Tick to enable ping response on this interface.
Support Access	Tick Box/Switch	If enabled, the support (ssh) port will be exposed on this interface; this must be enabled on at least one interface.

6.3.2 Delete a Bond

Deleting a Bond frees the interface to use for another purpose.

Procedure

This procedure explains how to delete a bond between two Ethernet ports.

1. Click the **System** Tab if it is not already selected, Figure 6-34.
2. Click **Configure** under Network Configuration section.

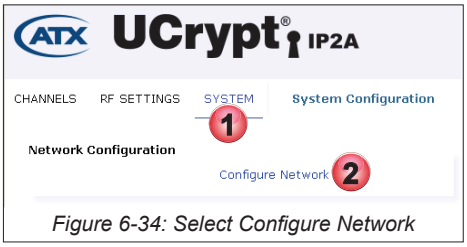

Figure 6-34: Select Configure Network

3. Click the red **X** ✖ in the bond you wish to delete, Figure 6-35.
4. Click the **Apply Configuration** O Apply Configuration button.

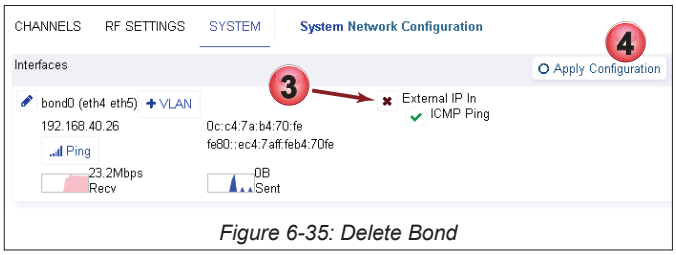

Figure 6-35: Delete Bond

6.4 User Configuration

Here you may manage users; adding new, deleting, setting permissions.

PASSWORD WARNING: ATX Networks strongly recommends that the factory default passwords be changed immediately upon Device initialization. The ability to dismiss or disable password warnings in the GUI are intended only for lab test environments with no internet connectivity to the Device.

Procedure

This procedure explains how to add or delete users.

1. Click the **System** tab if it is not already selected, Figure 6-36.
2. Click **Configure Users** in the User Configuration section.

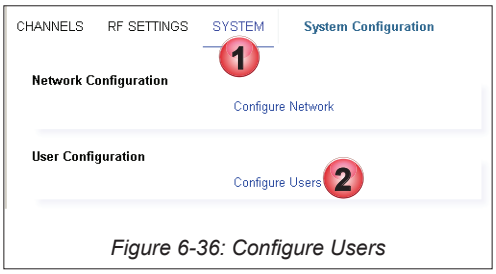

Figure 6-36: Configure Users

3. The User Accounts page opens, see Figure 6-37.
4. Click **New** to create a new user (or click the name of an existing user to edit or delete it).

Figure 6-37: Create New or Edit Existing User

5. When creating a new user, enter the username, first and last names and email address, all mandatory, Figure 6-38 or edit the existing fields. See Table 6.4a for help with these fields.
6. Highlight the group for this user's permission level. Only one group is necessary but multiple may be selected.
7. Enter a password, no restrictions.
8. If deleting a user, click **Delete**. You will need to confirm this deletion in the next step.
9. If creating or editing a user, click **Save**.

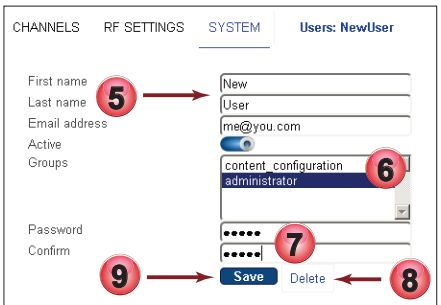

Figure 6-38: Edit & Save Changes

Table 6.4a: Add/Edit User Settings (See Figure 6-38)

Field	Configurable	Value
First Name	String	The first name of the user. This is mandatory.
Last Name	String	The last name of the user. This is mandatory.
Email Address	String	The email address of the user. This is mandatory.
Active	Tick Box/Switch	A switch to deactivate the user while retaining the user in the database for later reactivation.
Groups	Selection dialog	The user may be assigned permissions as a Monitor, Administrator or Content Configuration. Administrator can do everything. Highlight the applicable permissions, select one or more.
Password	String	A password is mandatory, there are no restrictions on what may be entered.
Save	Button	Click to save settings.
Delete	Button	Click to delete the user.

6.5 Location

This section, Figure 6-39, allows setting the time zone for the machine as well as a friendly name for positive identification while logged in.

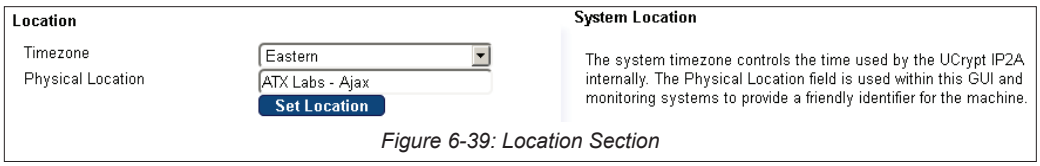

Figure 6-39: Location Section

6.5.1 Timezone

Setting the Timezone will result in accurate time being displayed in logs and in the UI. Time will be taken from an NTP (Network Time Protocol) server. The NTP server is internally predefined but may also be changed by entering a new URL on any of the network interfaces that have access to an NTP server. Access that by editing each/any interface that has access to an NTP server, see “6.2.2 Edit a Network Interface” on page 6-3.

6.5.2 Physical Location

Enter a friendly name for location which will be displayed in the header when logged in. This name will help to positively identify the unit being worked on.

Procedure

This procedure explains how to set the friendly location name for display in the machine header when logged in.

1. Click the **System** tab if it isn’t already selected, Figure 6-40.
2. Under the Location section, enter a **Name** for the **Physical Location** to identify the unit to the user when logged in. There is no limit to the number of characters as the line extends across the header to accommodate the text string.
3. Click **Set Location**.
4. The name will be displayed in the header when logged into the Device.

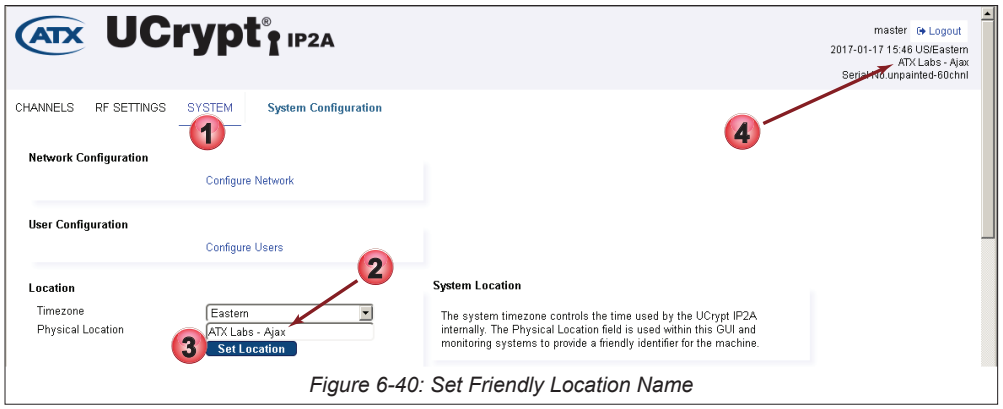

Figure 6-40: Set Friendly Location Name

6.6 Current Date

The date is kept current by integrated use of network time protocol but you may override that here if there is no time server accessible. Access to the Internet NTP server will be required for this automatic feature to work.

NOTE: *Mousing over the configuration fields shows tool tips for help in configuration.*

Procedure

This procedure explains how to override the built-in NTP time keeping feature.

1. If it is necessary to change the time, refer to Figure 6-41 and use the format YYYY-mm-dd HH:MM:SS
2. Click **Set Current Time.**

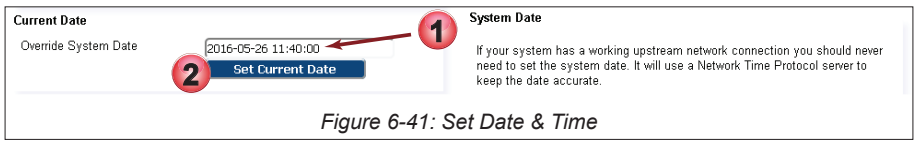

Figure 6-41: Set Date & Time

3. If an incorrect time and date is entered, there may be a discrepancy reported in the entered time against the time and date on your management PC, Figure 6-42. In this case adjust the entered date to the correct date and time.

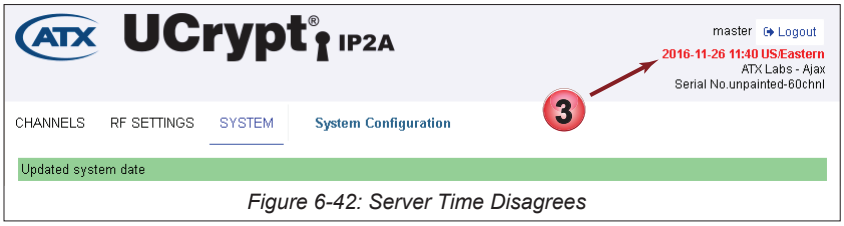

Figure 6-42: Server Time Disagrees

6.7 Power

Power management features such as reboot, shutdown, Auto power cycle may be accessed here, Figure 6-43. Table 6.7a summarizes the controls and settings configuration.

NOTE: *Mousing over the configuration fields and buttons shows tool tips for help in configuration.*

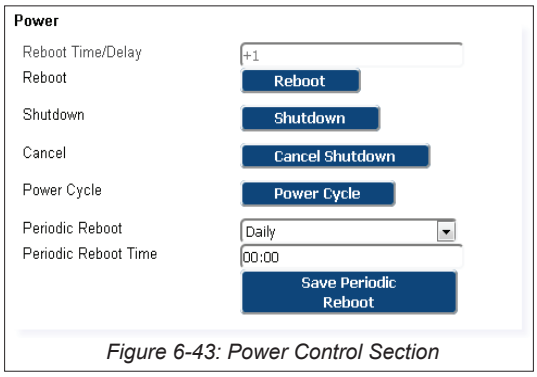

Figure 6-43: Power Control Section

Table 6.7a: Power Section Configuration (See Figure 6-43)

Field	Value	Description
Reboot Time Delay	Integer	If specified the reboot will occur at this time specified in local server time as HH:MM (24Hr) or +MM (minutes in the future). Default is **1 minute** in the future.
Reboot	Button	Resets Video Streaming Processes with a warm boot. May be used to attempt to restart the streaming if it has stopped.
Shutdown	Button	Schedule a shutdown to occur in **1 minute.** Power off the system until it is manually power cycled. This takes a unit out of service until field personnel arrive for a power recycle. May be used if an errant system configuration is causing unintended channel outages and must be removed from service.
Cancel Shutdown	Button	Cancel pending shutdown or reboot if a shutdown was scheduled and it is decided to not to allow follow through. This button immediately cancels the pending action.
Power Cycle	Button	Powercycles immediately. System will remain off for 30 seconds before rebooting, performing a cold power off reboot. Total outage of about 2 minutes.
Periodic Reboot	Dropdown	Enables periodic reboot of system at frequency chosen: Disabled, Daily or Weekly (Sunday).
Periodic Reboot Time	Integer	The system may be configured to perform a reboot at the time specified in the dialog box. Time must be entered in 24 hour format i.e. **13:45**.
Save Periodic Reboot	Button	It is necessary to save the changes to the **Periodic Reboot Settings** that were made. Failing to save the settings will result in changes being discarded when navigating away from the System page.

6.8 Firmware

The firmware version installed is reported here, Figure 6-44.

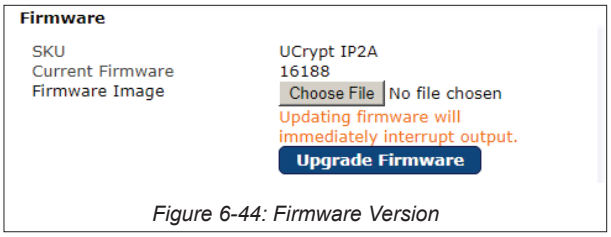

Figure 6-44: Firmware Version

Firmware upgrades, when available, are obtained from ATX Networks Technical Support group. Obtain the file and save it to your Management Computer before beginning the upgrade.

6.9 Monitoring/Alerts

The platform may be configured to sent SNMP traps to a remote SNMP manager, Figure 6-45. The default Port is **162** which is the well known port for SNMP and read only community is **Public**.

NOTE: *Mousing over the configuration fields shows tool tips for help in configuration.*

6.9.1 Configure SNMP

1. Download the SNMP MIB to compile into the remote manager system, click **UCrypt IP2A** MIB link.
2. Enter the SNMP parameters in the form.
3. Click the **Set SNMP** button.
4. To test that the settings are correct, send a test message to the remote manager, click **Test SNMP Traps**.

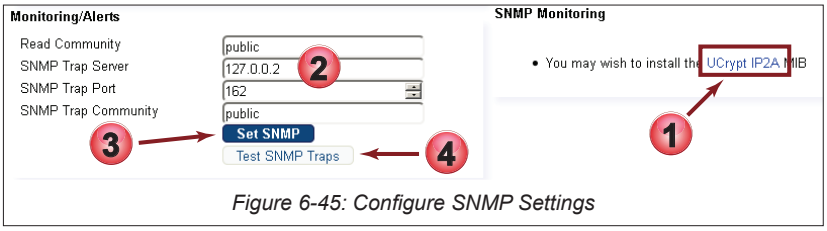

Figure 6-45: Configure SNMP Settings

6.10 EAS

The EAS section, Figure 6-46, allows EAS (Emergency Alert System) configuration for messaging and program substitution but there needs to be a **Details Channel** streaming source and a source of **J-STD-42-B EAS Alerts** available on one of the Ethernet interfaces. Only a full channel substitution is supported, no text crawls. This is accomplished by way of mass force tune of all resources to the multicast address specified as the Details Channel. EAS Alerts are received on the **Source** multicast address. This would be the IP address of your EAS encoder/Generator.

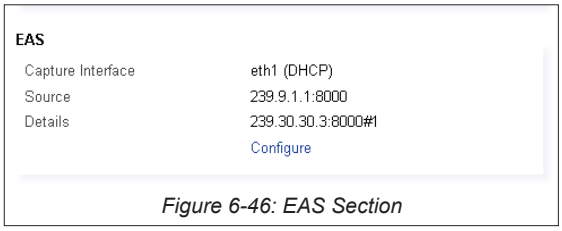

Figure 6-46: EAS Section

The configuration form is shown in Figure 6-47 and Table 6.10a summarizes the form and settings.

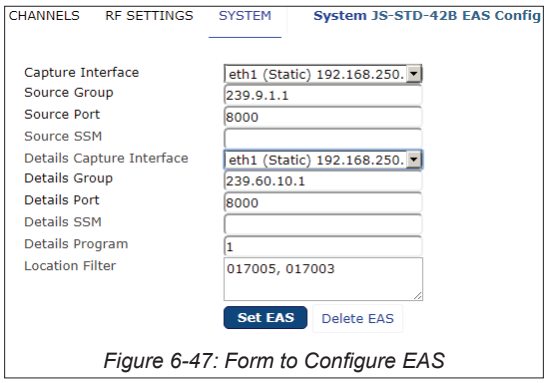

Figure 6-47: Form to Configure EAS

Table 6.10a: EAS Configuration Form Settings (See Figure 6-47)

Field	Configurable	Value Entered
Capture Interface	Dropdown Menu	The Ethernet port that the J-STD-42-B EAS Signalling appears on. Default is Primary Interface.
Source Group	IP Address	Multicast IP Address from which to pull the J-STD-42-B EAS Alerts.
Source Port	Integer	Multicast IP Port from which to pull the J-STD-42-B EAS Alerts.
Source SSM	IP Address	Alerts Source Specific Multicast. When specified, only alerts sent by this IP are processed.
Details Capture Interface	Dropdown Menu	The Ethernet port that the Details Channel appears on. Default is Primary Interface.
Details Group	IP Address	Multicast IP Address from which to pull the Details Channel stream during force tune.
Details Port	Integer	Multicast IP Port from which to pull the Details Channel stream during force tune.
Details SSM	IP Address	Details Source Specific Multicast. When specified, only content sent by this IP is processed.
Details Program	Integer	Program number to use for the Details Channel stream during force tune.
Location Filter	Integer,Integer,etc,	Use the location filter to ensure the alert is activated only when appropriate for your county or state. FIPS codes for location are in numeric format SSCCC or XSSCCC where SS is the FIPS state ID (integer), CCC is the FIPS county ID (integer) and X is the FIPS county subdivision (integer) separate locations with, and use county ID 000 to indicate all counties within a state. Separate multiple FIPS codes with a comma.
Set EAS	Button	Click to save this form data.
Delete EAS	Button	Click to delete this form data.

6.11 Configuration Backup

It is possible to back up the Device settings in a file and even use the file to replicate the device for mass deployment to other units with mostly similar settings. If a file is exported from a configured machine and it is to be deployed to other similar machines, be sure the firmware versions are the same.

6.11.1 Download or Backup the Device

Procedure

This procedure explains how to download a backup file to your management PC.

1. Click the **System** tab if it is not already selected, Figure 6-48.
2. Click the **Import/Export** link in the Configuration section.

Figure 6-48: Click Import/Export Link

3. In the **Download/Upload Configuration** page that opens, click the **Pack/Download** link, Figure 6-49.

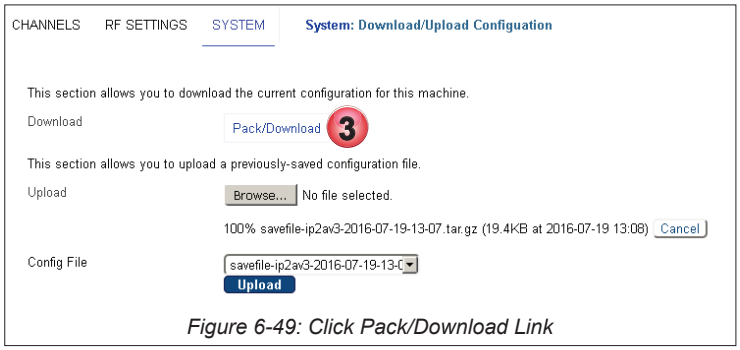

Figure 6-49: Click Pack/Download Link

4. In the new window that opens, Figure 6-50, click the **Save File** selection. Your browser may present this in a slightly different way.
5. Click **OK** to proceed to save the date stamped file in the folder usually used by your browser downloaded files. Your browser may present this in a slightly different way.

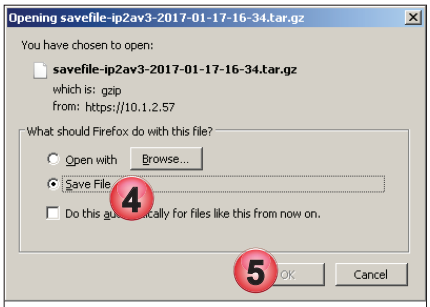

Figure 6-50: Save the Backup File

6.11.2 Upload or Restore a Backup

Procedure

This procedure explains how to restore a previously saved backup file to the Device.

1. Click the **System** tab if it isn't already selected, Figure 6-51.
2. In the Configuration section, click the **Import/Export** link.

Figure 6-51: Click Import/Export Link

3. On the **Download/Upload** page that opens, click the **Browse** button, Figure 6-52.

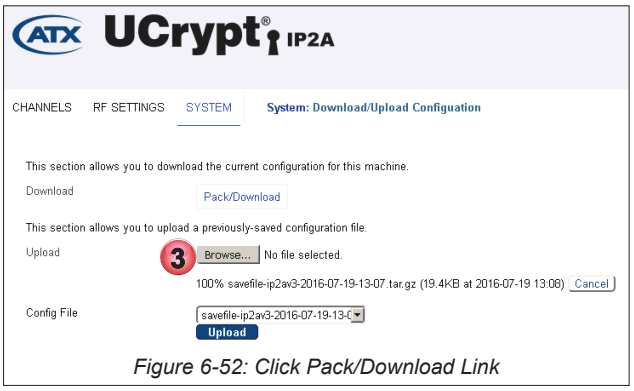

Figure 6-52: Click Pack/Download Link

4. Find the configuration file that was saved earlier and select it from the file explorer window, Figure 6-53.
5. Click **Open**. The configuration defined by the uploaded file is loaded to the Device but not yet applied.

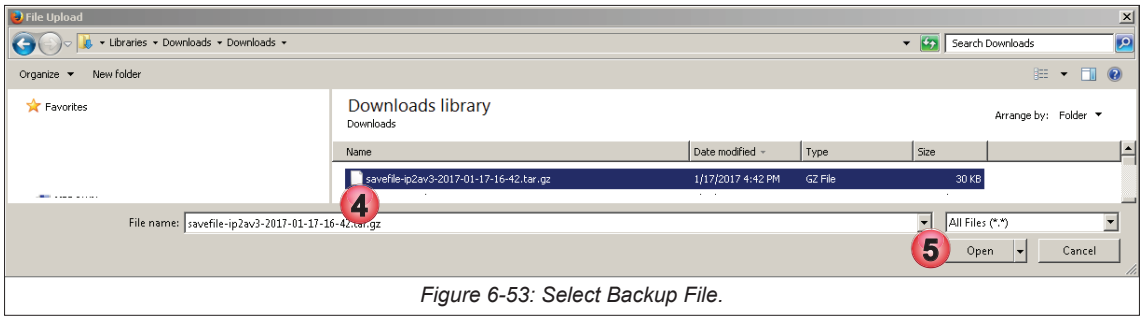

Figure 6-53: Select Backup File.

6. Click the **Channels** tab, Figure 6-54.
7. The Publish button announces ' **1 change is waiting to be published**'. Click the **Publish** button.

The uploaded configuration is taken live.

Figure 6-54: Click the Publish Button

6.12 Diagnostics

The Device can download a diagnostics file for troubleshooting purposes, Figure 6-55. This is not a human readable file. Use this feature only under the guidance of ATX Networks Technical Support Group.

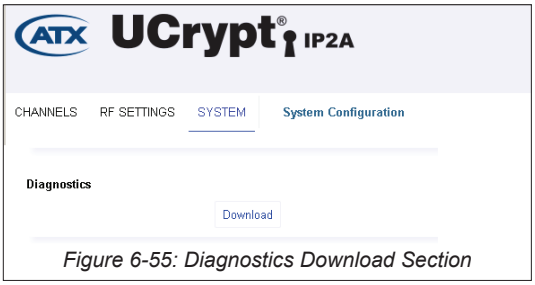

Figure 6-55: Diagnostics Download Section

6.13 Debugging

There are two features to help in diagnosing problems or understanding better what is happening with your Device, Figure 6-56. Click the links to access the features.

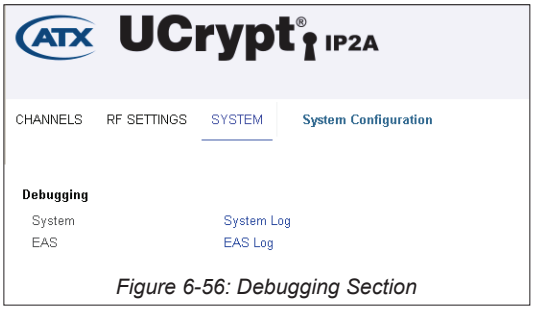

Figure 6-56: Debugging Section

6.13.1 System Log

The Device produces a System Log of many of the internal functions, Figure 6-57. It can be long and cryptic but may also help to understand issues that can arise. It is on by default showing the switch turned on (blue) but may be disabled by clicking to turn it off like this (grey).

To access this feature from the System page click **System Log** under the Debugging section, Figure 6-56. The log is displayed in the browser and may be copied by dragging across the text and copying to a text editor.

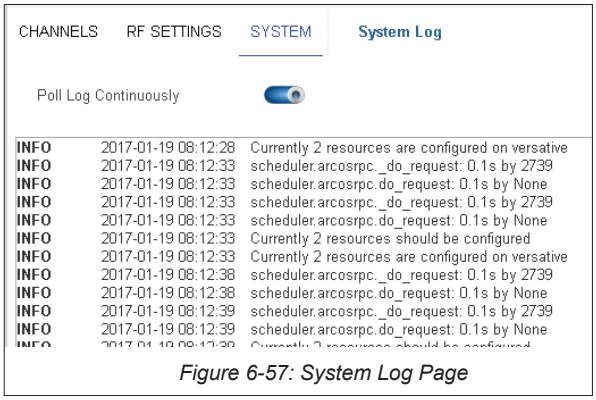

Figure 6-57: System Log Page

6.13.2 EAS Log

The Device produces an EAS log of the internal functions, Figure 6-58. It can be long but may also help to understand issues that can arise with EAS. It is on by default showing the switch turned on (blue) but may be disabled by clicking to turn it off like this (grey).

To access this feature from the System page, click **EAS Log** under the Debugging section, Figure 6-56. The log is displayed in the browser and may be copied by dragging across the text and copying to a text editor. In our example below, there are no EAS logs to display.

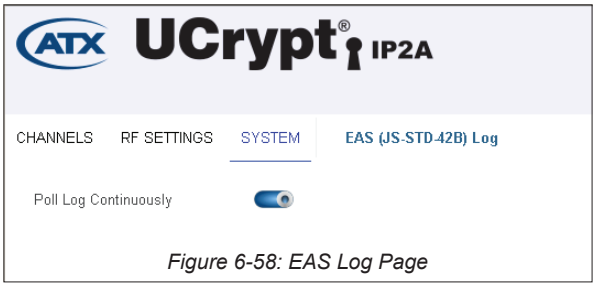

Figure 6-58: EAS Log Page

RF SETTINGS TAB

7. RF Settings Tab

7.1 Chapter Contents

7.2 About RF Settings Page

Use the RF Settings page, Figure 7-1, to manage channel plans and select the current active plan as described below.

1. Find this configuration page by clicking the RF Settings Tab.
2. A new or modified channel plan may be uploaded. Click **New** to name the new plan and initiate an upload.
3. The **Plan Number** is assigned based on the order in which the plan is uploaded and has no further relevance.
4. The plan **Friendly Name** identifies the plan in this UI.
5. The green **Dot** indicator identifies the active plan.
6. The **Channel Plan** and **Video Standard** is changed with a menu. Select from available plans and standards.
7. The **Channel Count** (for information only) is the number of channels available for each plan.
8. You can **Delete** a Channel Plan by clicking the '**x**' adjacent the relevant plan.
9. The **Analog Output Mode** control link controls modulation (Can transmit CW) for test purposes.
10. The **Enable VITS** switch (Blue = ON, Grey = OFF) and **VITS Mode** menu enable Vertical Interval Test Signals to be inserted in analog channels. Chose **Automatic** mode to have them inserted if none already exist in the channel or **Manual** mode to insert them even if they already exist**.**
11. Any changes to this page must be saved, click **Save** after all changes to apply the new settings.

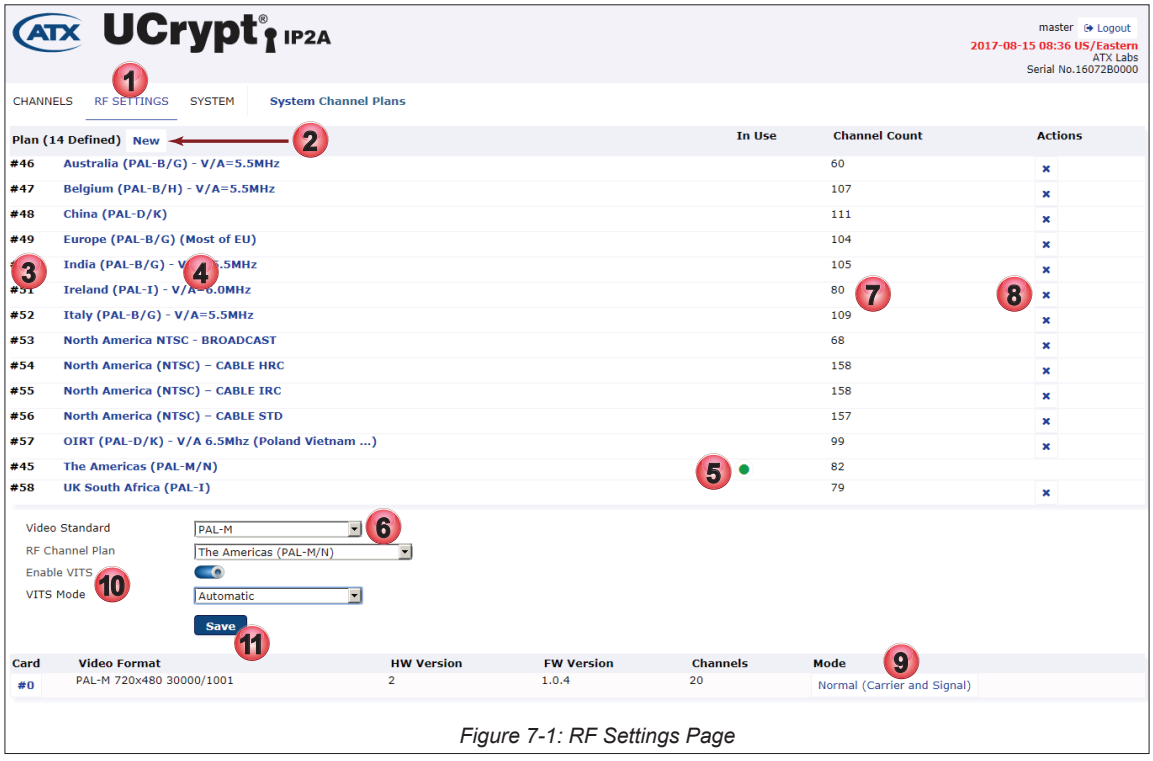

Figure 7-1: RF Settings Page

7.3 Select Active Channel Plan

An analog output RF Channel Plan must be selected from the choices available on the RF Settings tab.

Procedure

This procedure explains how to select the active Channel Plan and Video Standard.

1. Click **RF Settings** tab if it isn't already selected, Figure 7-2.
2. Select the appropriate **Video Standard** from the drop down list.
3. Select the corresponding **RF Channel Plan** from the drop down list.
4. Click the **Enable VITS** switch if you wish to have Vertical Interval Test Signals inserted on these analog channels.
5. Click **Save**.
6. The active plan is indicated by a green indicator adjacent the plan.

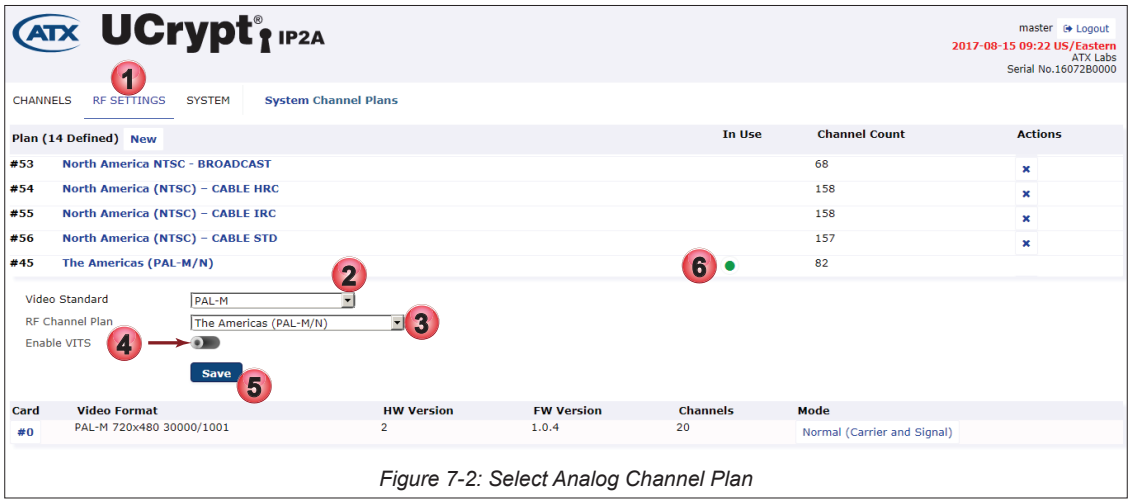

Figure 7-2: Select Analog Channel Plan

7. It is necessary to **Publish** changes made to the Plan on the Channels page. Click the **Channels** tab, Figure 7-3.
8. The Publish button shows '**1 change is waiting to be published**'. Click the **Publish Button**. This applies the change to the Device.
9. After publishing, a reboot may be required and a prompt is presented if it is required. Click the link **Reboot Required**.

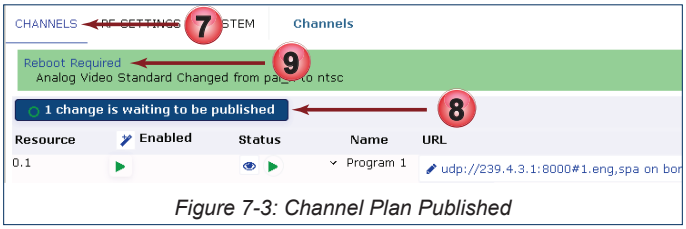

Figure 7-3: Channel Plan Published

10. You will be taken to the **System** page for a reboot. In the Power section, click **Reboot**, Figure 7-4.

After reboot, the new RF Channel Plan will be in effect.

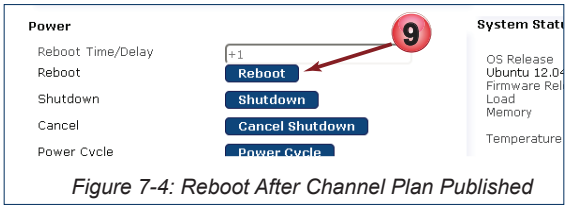

Figure 7-4: Reboot After Channel Plan Published

7.4 Download a Channel Plan

There are a good number of pre-installed channel plans, however you may want a variation of one of those plans. An existing plan may be downloaded in a comma separated values(CSV) format and modified to reflect your custom channel plan then later uploaded. It is likely that a plan that is close to what you need will be pre-installed; use it as a template for your custom plan.

7.4.1 Procedure

This procedure explains how to download a channel plan in a comma delimited spreadsheet format to your PC.

1. Click the **RF Settings** Tab if it isn't already selected, Figure 7-5.
2. Click the name of the existing plan to be downloaded from the choices presented.

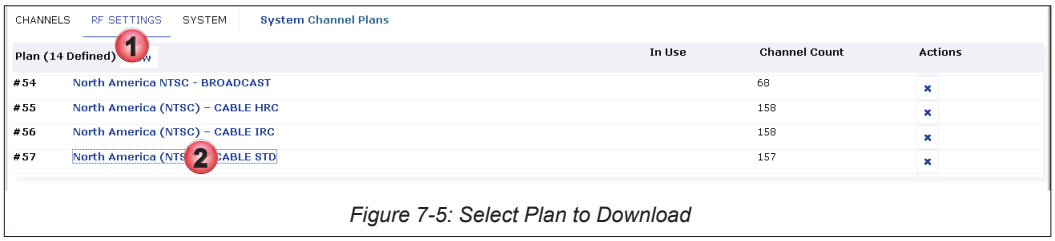

Figure 7-5: Select Plan to Download

3. A summary of channels included in this plan are listed, Figure 7-6.
4. Click the **Download** button.

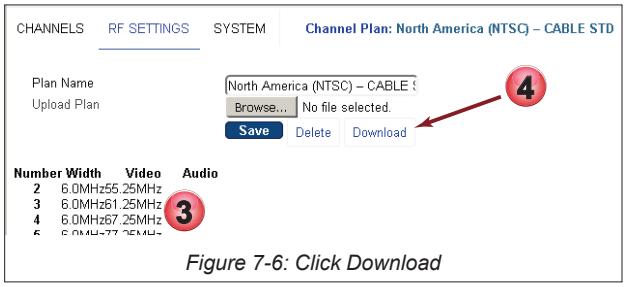

Figure 7-6: Click Download

5. Select "Save File", Figure 7-7, to download the file via your browser. Alternately select the compatible program to open the file with. This dialog may appear differently in the browser you are using.
6. Click **OK**.

The plan is saved to your browser downloads directory or opened in your spreadsheet program.

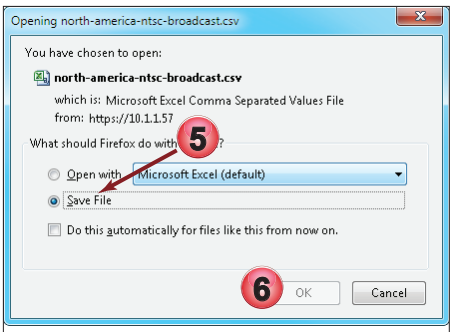

Figure 7-7: Save File

7.5 Upload a Custom Channel Plan

An existing plan may be downloaded as described above and modified to reflect your custom channel plan then uploaded. The method described next will create a new plan using your custom channel plan file or one you receive from ATX Networks that will be available in the list of Channel Plans on the RF Settings page.

7.5.1 Procedure

This procedure explains how to create a new plan by uploading a modified channel plan from your PC.

1. Click the **RF Settings** Tab if it isn't already selected, Figure 7-8.
2. Click **New**.

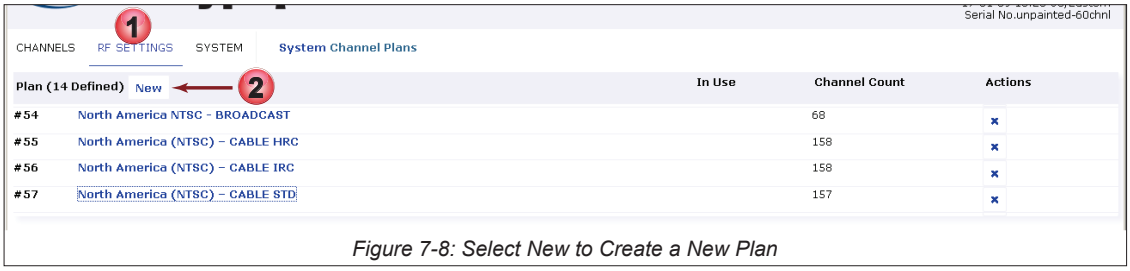

Figure 7-8: Select New to Create a New Plan

3. Enter the **Plan Name** for the new plan, Figure 7-9. This name identifies the plan in the UI only.
4. Click **Browse**.

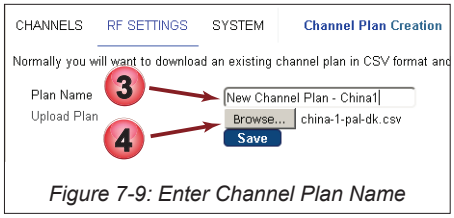

Figure 7-9: Enter Channel Plan Name

5. Browse to your custom Channel Plan file with the file manager window that opens, Figure 7-10 (the appearance of which depends upon the browser you are using).
6. Click **Open** (this may also differ depending on your browser).

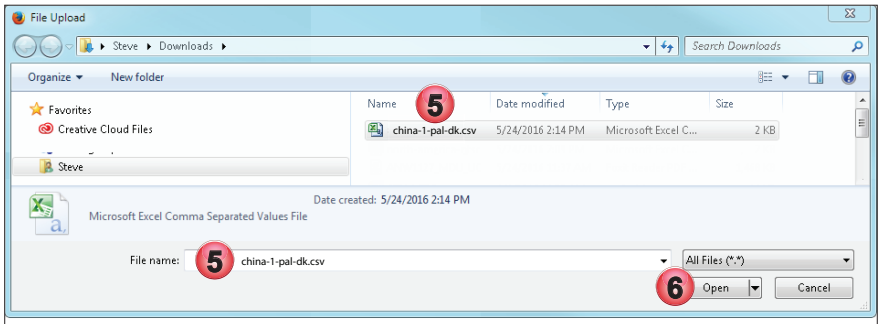

Figure 7-10: Select Channel Plan File

7. The Channel Plan file name appears in the display, Figure 7-11.
8. Click **Save** to start the upload.

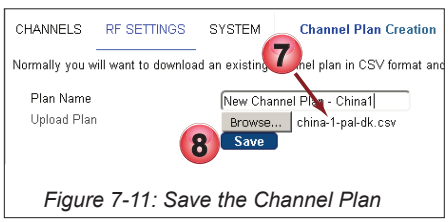

Figure 7-11: Save the Channel Plan

9. The new Channel Plan is added to the available channel plans but not yet published or available, Figure 7-12.

Figure 7-12: New Channel Plan Now Available

10. Click the **Channels** tab, Figure 7-13.
11. The Publish button announces **1 change is waiting to be published**. Click the **Publish** button to make this plan available. Once available, it won't be live on your machine until you make it the default channel plan, see "7.3 Select Active Channel Plan" on page 7-2.

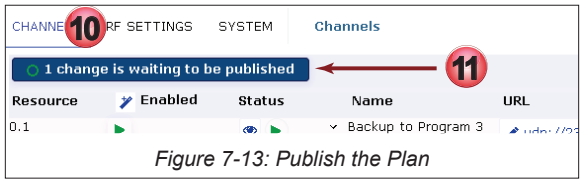

Figure 7-13: Publish the Plan

7.6 Set Carriers to CW Mode

The carriers of all output channels can be set to CW for test purposes. They are controlled in groups of 20 channels so if there are 60 channels in your device, this must be done to all 3 cards to get all channels set to CW.

Procedure

This procedure outline how to set the RF output carriers to CW mode.

1. Click the **RF Settings** Tab if it isn't already selected, Figure 7-14.
2. At the page bottom, for the RF Output card (There may be up to 3 cards. In this example we select 'Card 0'), click the **Mode** link for the card. The current mode setting is stated in the link, in this case **Normal (Carrier and Signal)**.

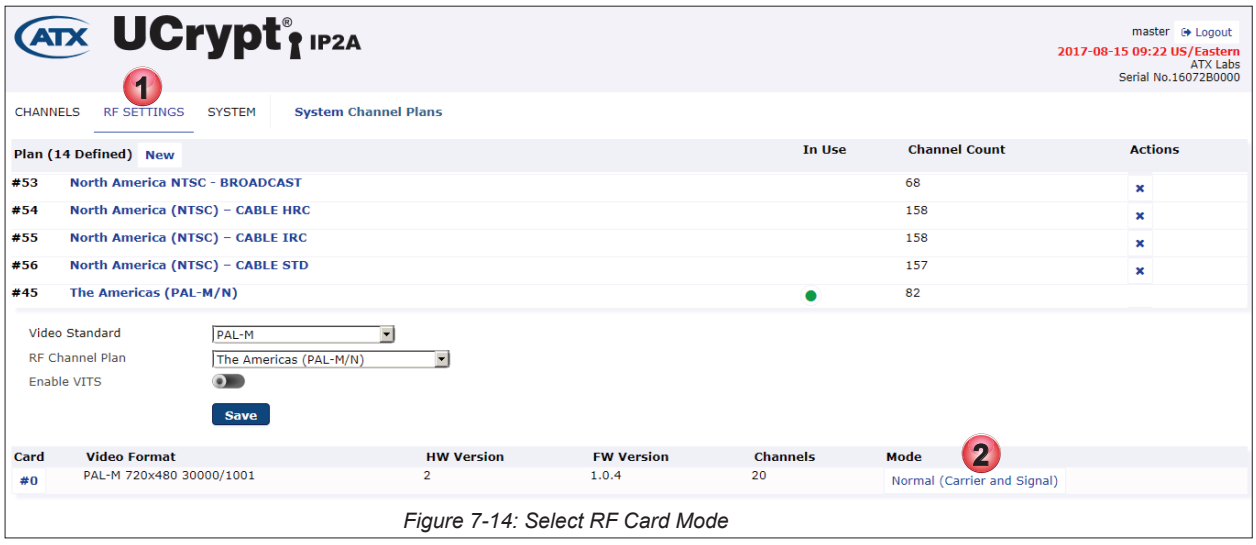

Figure 7-14: Select RF Card Mode

3. Select from the drop down menu '**Continuous Wave(Carrier Only)**', Figure 7-15.

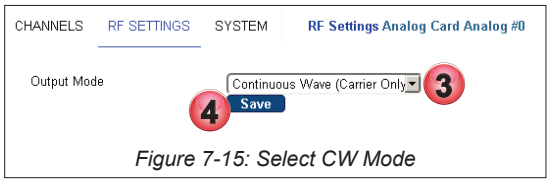

Figure 7-15: Select CW Mode

4. Click **Save**. If more RF Output cards need to be set to CW Mode, return to step 2 and repeat for all cards.
5. The changes need to be published. Click the **Channels** tab, Figure 7-16.
6. The Publish button announces **X change is waiting to be published**. Click the **Publish** button to make this plan live.

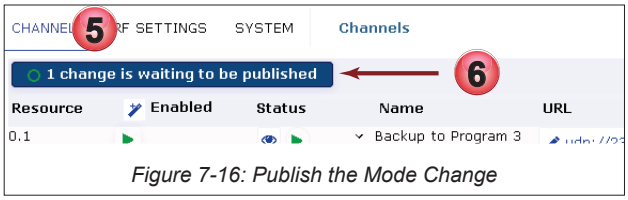

Figure 7-16: Publish the Mode Change

SERVICE & SUPPORT

8. Service & Support

8.1 Contact ATX Networks

Please contact ATX Technical Support for assistance with any ATX products. Please contact ATX to obtain a valid RMA number for any ATX products that require service and are in or out-of-warranty before returning a failed module to ATX.

TECHNICAL SUPPORT

Tel: 289.204.7800 – press 1
Toll-Free: 866.YOUR.ATX (866.968.7289) USA & Canada only
Email: support@atx.com

SALES ASSISTANCE

Tel: 289.204.7800 – press 2
Toll-Free: 866.YOUR.ATX (866.968.7289) USA & Canada only
Email: insidesales@atx.com

FOR HELP WITH AN EXISTING ORDER

Tel: 289.204.7800 – press 3
Toll-Free: 866.YOUR.ATX (866.968.7289) USA & Canada only
Email: orders@atx.com
Web: www.atx.com

8.2 Warranty Information

All of ATX Networks' products have a 1-year warranty that covers manufacturer's defects or failures.

ISO
9001:15
REGISTERED

Rev. 11/19 (ANW1154)

ATX Networks
Tel: 289.204.7800 | Toll-Free: 866.YOUR.ATX (866.968.7289) | support@atx.com