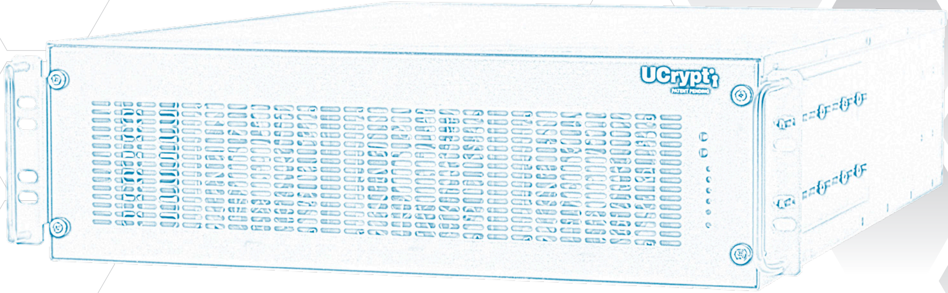
ATX

MDU Solutions®

UCrypt® IP2Agen1
Patent Pending

UCrypt® IP to Analog 1st Generation

Installation & Operation Manual



GENERAL GUIDE NOTES

Firmware Version

Some features described in this manual require the latest firmware to be installed on the UCrypt devices. Check with ATX Networks technical support or the related support web site for your model of UCrypt for the latest release of firmware. The firmware installed on your UCrypt may be found on the ‘System’ tab of the Management Interface. At the time of publication of this manual the most current released firmware version is:

System	**0.56**

Organization of This Manual

This manual is generally organized based on the tabbed Management Interface with an individual chapter dedicated to describing the configurable features of each tab. Further chapters outline activities related to the UCrypt operation such as System Description, Installation, Startup, Emergency Alert System etc.

Cross Reference Hyperlink Usage

Hyperlinks are used liberally throughout the guide to assist the reader in finding related information if the reader is viewing the Adobe PDF file directly. Hyperlinks may be identified by their blue text. Most links are to related pages within the document, but some 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:

⚠ ***NOTE:*** *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.*

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

Although every effort has been taken to ensure the accuracy of this document it may be necessary, without notice, to make amendments or correct omissions. Specifications subject to change without notice.

* Any use of the UCrypt product, directly or indirectly, for the decryption and unauthorized reproduction of content that constitutes or may constitute copyright infringement or otherwise infringes on the proprietary rights of any third party is expressly prohibited. No user of UCrypt shall use UCrypt for any purpose or in any manner which, directly or indirectly, violates the law, violates the proprietary rights of any other party, or aids in any unlawful act or undertaking including, without limitation, laws governing data privacy, international data transmission, and export of technology or data. Any multiple systems operator or other similar party (“**MSO**”) will use the UCrypt product in strict compliance with all applicable laws and in compliance with any agreement in effect between the MSO and a content provider. In no event shall ATX Networks Corp. or any of its affiliates be liable to an MSO, any end user of the UCrypt product, or any other third party, for any claims arising out of or related to any use or misuse of the UCrypt product in contravention of this disclaimer. It is the express obligation of an MSO to convey this disclaimer to any other end user of the UCrypt product.

MDU Solutions®, UCrypt®, DigiVu® and VersAtive®Pro are registered trademarks of ATX in the United States and/or other countries. Products or features contained herein may be covered by one or more U.S. or foreign patents. Verimatrix® and other non-ATX product and company names in this manual are the property of their respective companies.

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 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.

SYSTEM DESCRIPTION

2. System Description

2.1 In This Chapter

- "Applications"
- "Key Features"
- "Simplified Block Diagram"
- "Front Panel"
- "Rear Panel"
- "Available Hardware Models"

2.2 Applications

The UCrypt IP to Analog device is a configurable MPEG digital video signal processor designed to simplify creation of a lineup of up to 20 Cable TV analog channels for any applications where programs are available in IP format. The UCrypt IP to Analog device can help a Service Provider easily and flexibly implement clear analog channel lineups in applications for bulk MDU, small hotels and motels, hospitality, remote conference halls, stadiums, or other commercial accounts where deploying STBs is undesirable or not cost effective.

2.3 Key Features

For full capabilities, see "Specifications" on page 11-1

2.3.1 IP to Analog Signal Processing

The UCrypt IP to A device supports MPEG-2, H.264, HD or SD, SPTS and MPTS multicast streams. Following ingestion, programs are able to be output on up to 20 independent agile analog channel modulators. All modulators are fully agile in the downstream spectrum of 54 MHz - 750 MHz and support multiple PAL and EIA (NTSC) channel plans. For details on channels supported, see "Specifications" on page 11-1. Analog output channel are true analog signals.

2.3.2 Support for Verimatrix Encryption Format

Programs may be ingested whether they are in the clear or encrypted with Verimatrix DRM.

2.3.3 Flexible IPv4 Configuration

IPv4 network addresses are supported and full address configuration may be performed on the PHY interface for deployment on a public or private network. Fixed network addresses are supported along with a DHCP client mode for automatic IP address provisioning. The Gigabit Ethernet physical network port auto senses connection type and is pre-configured with a factory default 192.168.0.23 IP address.

2.3.4 Remotely Accessible Management Interface

An easy to use web based Management Interface is integral and accessible either locally or remotely with your choice of browsers through a 10/100 Base-T network port. Local control is available for the field installation technician and configuration is simple with a Notebook PC connected to the network management port. Remote access from anywhere is easily provided by connecting to a pre-existing Ethernet based network or to a residential or commercial cable modem. The Management Interface allows simple configuration of all operating parameters.

2.3.5 Status Monitoring and Reporting

The UCrypt system is constantly monitored internally and supports sending SNMP traps to an external element management system for remote alarm monitoring if this is part of the operators network. The UCrypt device also supports multiple email address destinations for critical alarm notification. The operator may choose from a list of alerts and either enable or disable them as required. The UCrypt device supports SNMP network monitoring through a built in MIB. The MIB is available from ATX Networks Technical Support for compiling into the external manager.

2.3.6 RF Management

An internal combining network is provided as well as an output test point to simplify troubleshooting and network integration. With a single combined output, the operator is provided with a single wire feed to the distribution network with up to 20 analog channels per UCrypt device.

2.3.7 Power Supply Redundancy

Two power supplies are provided with independent power cords which may be connected to different power sources. For highest reliability, connect one power supply to a UPS system. Switch-over is automatic and transparent and both an audible alarm (which may be silenced with a rear panel switch) and GUI alarms will be activated upon any power supply failure or the supply of power to the outlet. Additionally, an alert may be sent by email or SNMP trap.

2.4 Simplified Block Diagram

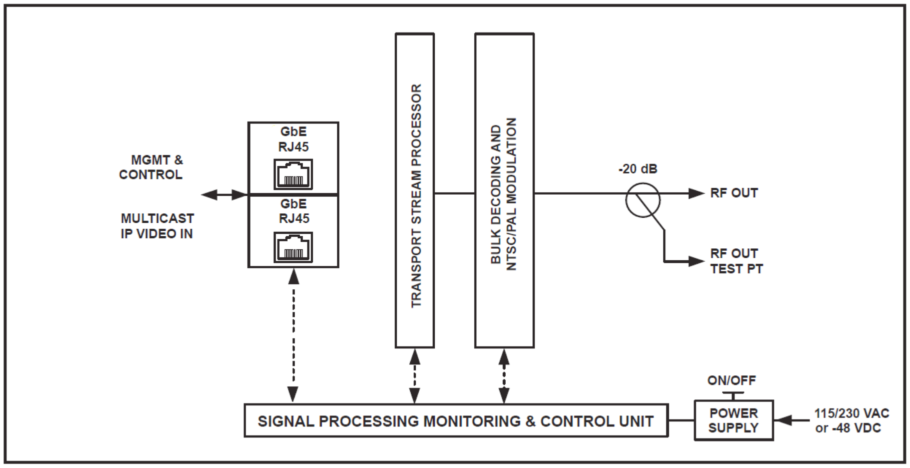


Figure 2-1: Simplified Block Diagram

2.5 Front Panel

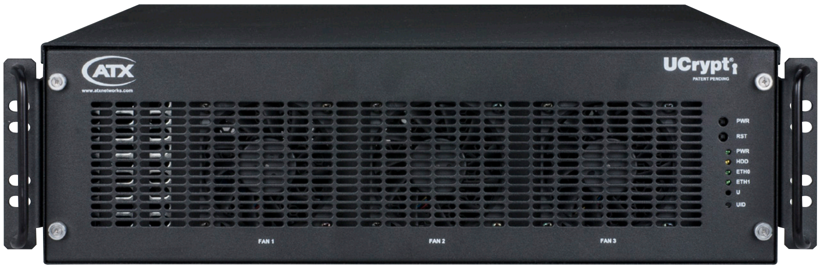


Figure 2-2: Front Panel

2.6 Rear Panel

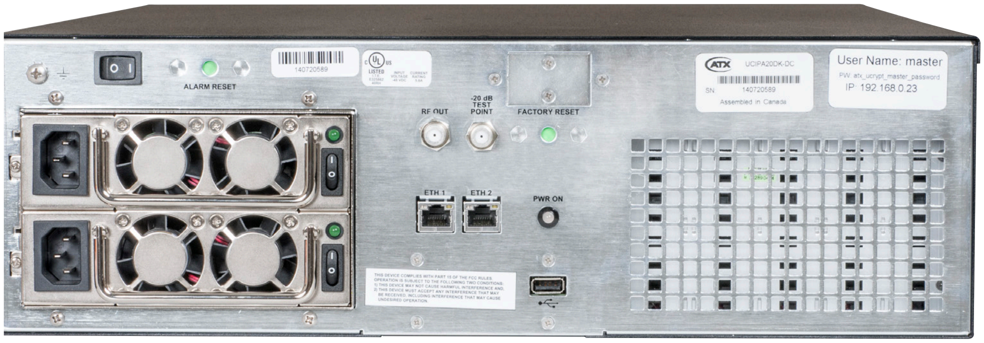


Figure 2-3: Rear Panel - AC Power Supplies

Table 2.6a: Rear Panel Ports and Controls

Port or Control	Type	Description
IP IN	Ethernet Port	Port used to present all multicast IP streams to the UCrypt device, including EAS Alert Message stream and EAS Details Channel stream.
MGMT PORT	Ethernet Port	Port used only to access the Management Interface or GUI. The default IP address of 192.168.0.23 is preset.
Factory Reset	Button	Use to return the UCrypt device to factory default settings, specifically passwords.
Power Supply Alarm Reset	Button	Silences the audible alarm when a single power supply fails or power is interrupted to a single supply.
RF OUT	F Connection	A 75 Ω port for the output of analog channels at a level of 30 dBmV +/- 2 dB per analog carrier.
TEST POINT	F Connection	A 75 Ω port for measuring the output of analog channels at a level -20 dB relative to the RF OUTPUT port.
UCrypt System Power Switch	Toggle Switch	Switch to shut down the UCrypt system. Similar to a computer power switch, this momentary action switch does not remove power from the system. Press once momentarily to cause an orderly shut down; press and hold for an immediate shutdown. When the UCrypt device is shut down, this switch will restart the system.
PWR ON	LED Indicator	LED is lit when the UCrypt system is running. When off, indicates the system is not running but does not necessarily indicate power is removed. See Power Supply Indicators for power-on state.
USB SERVICE	USB Port	USB-2 port used only to present files for firmware upgrades.
Power Supply Switch	Toggle Switch	Each power supply has a power switch and indicator. Turn this switch off before removing the supply. Turn both switches off to remove power entirely from the UCrypt device. Indicators are lit when each power supply is functioning normally.

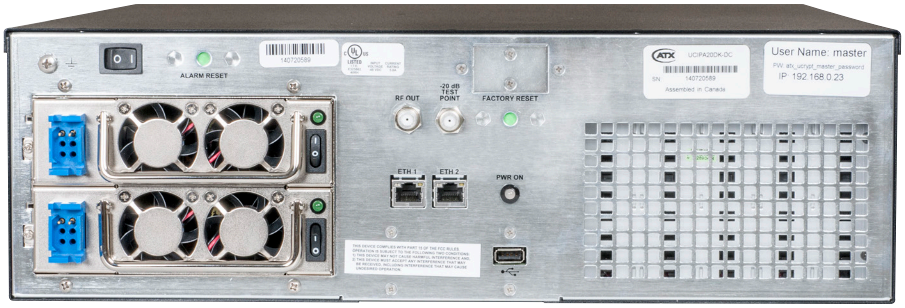


Figure 2-4: Rear Panel - DC Power Supplies

2.7 Available Hardware Models

There are a number of variants of the IP to Analog product available, all of which have similarities in their function. Each variant will be factory configured with hardware options to provide functionality related to the needs of the Cable Service Provider. All options available may also be ordered as upgrades to meet future needs after the product has been in service.

2.7.1 Principal Model Variants

1. Clear IP Channel Input vs. Verimatrix Encrypted IP Channel Input.
2. NTSC Channel Output vs. PAL Channel Output
3. AC Power @115/230 VAC vs. -48 VDC Power Supply

2.7.2 Similarities Among Model Variants

- Common System Features
  - Software Features
  - Management Interface GUI
  - System Configuration
- IP to analog program processing
- 20 Channel capacity

2.7.3 Ordering Information

Part Number	Description
IP to Analog 1st Generation	
UCIPA20N	20-channel IP Input (w/ optional Verimatrix decryption) and NTSC Analog Output (AC power)
UCIPA20N-DC	20-channel IP Input (w/ optional Verimatrix decryption) and NTSC Analog Output (DC power)
UCIPA20BG	20-channel IP Input (w/ optional Verimatrix decryption) and PAL B/G Analog Output (AC power)
UCIPA20BG-DC	20-channel IP Input (w/ optional Verimatrix decryption) and PAL B/G Analog Output (DC power)
UCIPA20DK	20-channel IP Input (w/ optional Verimatrix decryption) and PAL D/K Analog Output (AC power)
UCIPA20DK-DC	20-channel IP Input (w/ optional Verimatrix decryption) and PAL D/K Analog Output (DC power)

INSTALLATION

3. Installation

3.1 In This Chapter

- "Mounting"
- "Equipment Safety Grounding"
- "Environment"
- "Cabling Considerations"
- "Powering up"

3.2 Introduction

This chapter outlines the most important aspects of the installation of the equipment and summarizes the site considerations that the installer must take into account when choosing a location for the unit.

Mounting brackets are provided witch will allow the installer the necessary options to locate the equipment according to site conditions. Both rack mount and backboard brackets are supplied with each unit to allow flexible field mounting. There is no limit on physical orientation; it may be mounted in any position required by site conditions.

3.3 Preparation

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, see "Contact ATX Networks" on page 12-1.

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

NOTE: *Not for use in a computer room as defined in the Standard for Protection of Electronic Computer/Data Processing Equipment, ANSI/NFPA 75.*

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

3.4 Mounting

The chassis is designed to enable flexible mounting in a wide variety of locations and environments and brackets are provided to simplify this. The following sections outline rack and panel mounting scenarios, but other mounting arrangements are possible.

NOTE: *If the UCrypt device is to be mounted in a rack, it is essential to attach the rear mounting ears of the unit to rear mounting rails to provide support or alternately install the unit on a well supported shelf.*

3.4.1 Rack Mounting

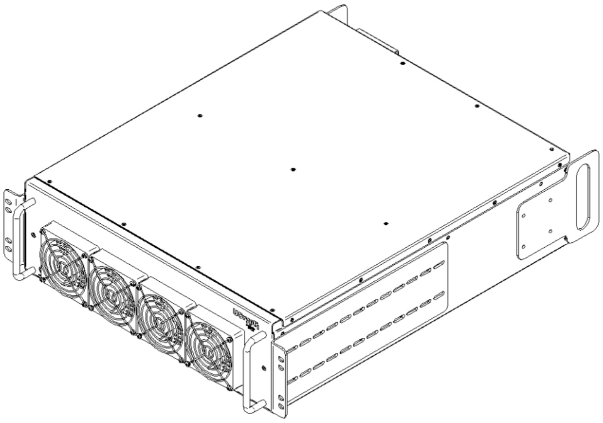


Figure 3-1: Rack Mounting

Rack mount brackets for the front and the rear are provided for mounting in a standard EIA 19" (48.25cm) equipment rack with a depth of at least 24 inches (61cm). The equipment will require 3RU of vertical rack space and may be mounted directly above or below other equipment without providing space between, however, it is recommended that, if possible, 1RU space be maintained from other equipment which generates significant heat. **Rear support is mandatory** and adjustable brackets are provided for that purpose. Do not use the chassis to support other equipment. Fan forced cooling is integral which exhausts to the rear, so be sure to maintain site conditions where freedom of air movement at the front and rear is assured. Installation of the equipment in enclosed racks is not recommended due to the possibility of restricting cooling air flow. Consider also that the site technician will need access to the rear panel for accessing connections, maintenance and configuration when determining the best location for this equipment. Fasteners necessary for mounting in a rack are not supplied.

3.4.2 Panel Mounting

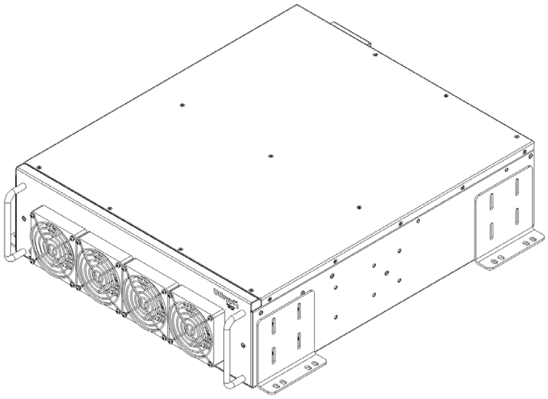


Figure 3-2: Panel Mounting

Brackets are provided for mounting to a vertical backboard for sites where no rack mounting facilities exist. These panel mounting brackets are the same as those provided for supporting the rear of the unit in an equipment rack but are now turned 90º down so the flanges are flat against the backboard and screws may be used hold the unit on the backboard. The brackets will allow the unit to be mounted flat against the backboard only so be sure to provide sufficient area. The dimensions of the unit are 18" x 22.5" but a reasonable amount of space, at least 6", will be required in front of and behind unit. It is recommended to mount the equipment with the long axis in a horizontal orientation. In this manner, the fans will exhaust to one side. The reason for this is to avoid the possibility of screws, other small metal objects, debris or liquids from accidentally falling inside the unit. As there are vent openings on the rear as well, it is also specifically not recommended to install the unit with the rear facing up. Fan forced cooling is integral which exhausts to the rear, so be sure to avoid blocking airflow at the front and rear panels and mount in such a manner to provide a source of ambient cool air at the front air intake of the unit. Consider also that the site technician will need access to the rear panel for accessing connections, maintenance and configuration when determining the best location for this equipment. Fasteners required for mounting to a backboard are not supplied.

3.5 Equipment Safety Grounding

NOTE: It is imperative that the UCrypt device chassis be connected to a permanent building ground to comply with UL, CUL and CB standards.

It is imperative that the UCrypt device housing be connected to a permanent building ground in a manner that will ensure that the exposed metal parts are constantly connected to ground even when the power cord may be disconnected temporarily. A grounding lug is provided on the rear panel to conveniently effect such a connection. 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.

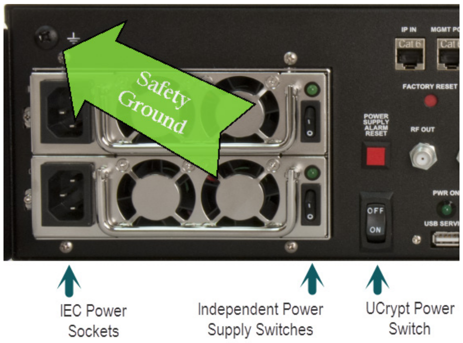


Figure 3-3: Equipment Safety Ground

3.5.1 Connection to Earth

The supplementary equipment grounding conductor is to be installed between the UCrypt device's rear panel ground connector and earth, that is, in addition to the equipment ground conductor in the power supply cord.

3.5.2 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.

3.5.3 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.

3.5.4 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.

3.6 Environment

3.6.1 Airflow and Cooling Considerations

The equipment is designed to operate to specification in an ambient room temperature of 0°C to +40°C (+32°F to +104°F). Normal room temperature is recommended to ensure proper long term operation of the equipment. Sufficient airflow through the unit must be maintained regardless of the mounting location. It is imperative that other equipment or materials of any type do not block free airflow at the front and rear. The product does not contain air filters.

3.7 Power

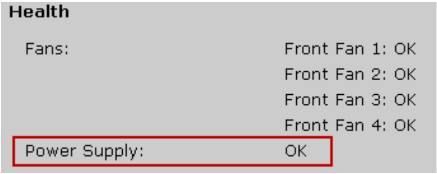
The following points must be taken into account when installing the UCrypt device and connecting power.

3.7.1 Power Supply Input Voltage

The UCrypt device's dual redundant autosensing switching type power supply system can operate on a wide range of input voltages from 115 VAC to 230 VAC. There is no need to configure the power supply to operate on any voltage in this range.

3.7.2 Power Supply Redundancy

Either power supply on its own can provide the required power safely if one fails. To retain the redundancy feature, replace a failed power supply as soon as possible. A power supply failure will be indicated in the Management Interface 'System' tab as shown in Figure 3-4 and will cause an audible alarm within the UCrypt device. Silence the audible alarm with the rear panel **Power Supply Alarm Reset** switch. The GUI alarm will be automatically remitted when the power supply is replaced.



```
Health
  Fans:                               Front Fan 1: OK
                                      Front Fan 2: OK
                                      Front Fan 3: OK
                                      Front Fan 4: OK
  Power Supply:                       OK
```

Figure 3-4: Power Supply Status

3.7.3 Power Cord Protection

Measures must be taken during installation to route or arrange the power supply cord to prevent physical damage to the cord and to avoid the possibility of future damage occurring. The power supply cord 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.

3.7.4 Power Cord Attachment

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

3.7.5 Provision of Electrical Power Outlet

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

3.7.6 IEC Power Input Cord

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

3.7.7 Input Power Requirements

When installing the UCrypt 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. Each UCrypt device model will require power to be supplied from a properly grounded outlet. The installer shall determine that the power outlet, its wiring and receptacle is in compliance with local and/or national electrical codes as applicable. The 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.

3.7.8 Fusing

Over-current protection is built in to the UCrypt product. There is no internal fuse to be replaced or maintained.

3.8 Cabling Considerations

3.8.1 Coaxial

The RF fittings provided are 75 OHM “F” style standard coaxial connectors and are located on the unit’s rear panel. Clear labelling of the output port and test point are provided to simplify installation and maintenance. RF cabling to the unit should be either RG6/u or RG59/u style double or triple shield coaxial cable and connections should be lightly wrench tightened.

The output signal level presented at the port is fixed at a maximum level of +30 dBmV +/- 2 dB per analog carrier depending on the number of carriers activated. Activating more carriers will reduce the per carrier level to maintain a constant total power output. The unit maintains adjacent carriers at an output level equal to one another.

3.8.2 Network

Management Port (MGMT PORT)

The rear panel Management Interface port allows connection to a notebook or desktop PC for managing and configuring the UCrypt 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. Connections should be made with Cat5e or better network cables. The 10/100 Base-T management ports is DTE and should be connected to a switch or router with a straight through wired cable. Direct connection to a PC should be made with the supplied crossover cable.

Ethernet Input Port (IP IN)

The input port is DTE and intended to be connected to a network distribution switch using straight through wired Cat5e or better quality cable. The 10/100/1000 Base-T port negotiate an appropriate connection speed dependant on the type of external port it is connected to.

3.9 Powering up

NOTE: *Before powering, ensure that the RF output connector is disconnected from the distribution network to avoid unintentional service outages if there are overlaps between the analog output channels of the unit and existing services on the cable network. Only when you are sure of the configuration of the UCrypt device channel lineup and output level should you connect the RF output to the building insertion point.*

FYI: *Boot-up of the equipment will take approximately 90 seconds during which there will be no channels output from the RF output port.*

INITIAL STARTUP

4. Initial Startup

4.1 In This Chapter

- “Required Connections”
- “Factory Default IP Address Settings”
- “Computer Requirements”
- “Starting the Management Interface”
- “Account Passwords and Privileges”

4.2 Introduction

In this section we discuss the initial requirements to connect the management computer and configure its IP address to allow communication with the UCrypt device’s Graphical User Interface that we refer to as the Management Interface.

4.3 Required Connections

4.3.1 Management Port (MGMT PORT)

The UCrypt device is provided with an Ethernet port on the rear panel labeled **MGMT PORT** for connecting to the Management Interface for initial configuration and ongoing monitoring and maintenance.

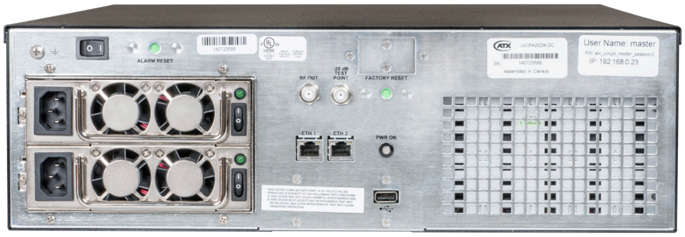


Figure 4-1: Rear Panel AC Ports

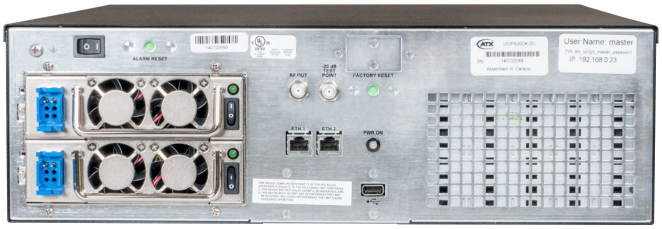


Figure 4-1: Rear Panel DC Ports

The port is of the autosensing type, whereby it can sense the type of connection presented to it whether it is a PC, router, switch or cable modem. Therefore it is possible to use any type of network cable configuration, i.e. crossover or standard straight through to connect the unit to another device. While a crossover cable is provided for your convenience, it is not strictly necessary to use this cable to connect the Management Computer. The MGMT Port will automatically negotiate the speed of the connection depending on the capabilities of the PC network port.

FYI: *If connectivity problems between the PC network port and the UCrypt device occur, check to be sure that you are using a known good network cable.*

If the UCrypt device is to be connected to a local cable modem for remote configuration or monitoring, a standard Cat5e type cable will be required for the connection to the modem and is normally supplied with the modem.

VKS Key Server

If Verimatrix encryption is used, the VKS Key Server must be accessible on the MGMT port.

4.3.2 IP IN Port

The streaming IP programs will need to be presented on the ‘IP IN’ port. In addition, the EAS external message generator and an EAS details channel, if used, will be presented on this port. This port is DTE and requires a straight through wired Cat5e network cable to connect to a switch or router port. There is no access to the Management Interface from here.

4.3.3 RF OUT Port

The RF OUT port connects to the cable TV distribution network with a fixed output level of +30 dBmV +/- 2 dB and an impedance of 75 Ω.

4.4 Factory Default IP Address Settings

The Management Interface is web based and will require a locally connected computer to complete the configuration. The **MGMT PORT** through which access to the web server is available has the following default settings.

Table 4.4a: Factory Default IP Addresses

Address	192.168.0.23
Netmask	255.255.255.0
Gateway	192.168.0.1

4.5 Computer Requirements

It is recommended that the Management Computer meet these minimum requirements. ATX Networks does not endorse the use of any specific operating system software however this combination of software has been thoroughly tested with the product and is known to work without issue. The operator is free to utilize whatever software combination is desired.

4.5.1 Minimum Computer Requirements

- Computer running Windows® or other OS
- Ethernet Network port available
- Web browser for Management Interface: Internet Explorer® Firefox® or other
- Adobe® Reader® for reading this manual
- Text editor for capturing logs

4.5.2 Web Browsers Supported

The UCrypt GUI supports the use of multiple brands of web browser software. ATX Networks does not endorse the use of any specific brand of web browser. Browsers such as Microsoft® Internet Explorer and Mozilla Firefox are commonly used and have been thoroughly tested. It is recommended that the latest version of your choice of browser be used.

4.6 Starting the Management Interface

Set-up of the UCrypt device requires a laptop or desktop PC running Microsoft Windows or other operating system with an available Ethernet network port (called the “Management Computer” in the following procedures). Network parameters of the Management Computer must be set appropriately for access to the Management Interface.

The following procedures are for Microsoft Windows XP and a default IP address setting on the UCrypt device of 192.168.0.23

FYI: *If you are using a different Operating System or the network address on the UCrypt device has been changed from default, adjust the procedures to suit the address or software you are using.*

1. Connect the Management Computer’s Ethernet adapter to the product’s Ethernet port using a Cat5e cable (supplied with the unit). Link lights should illuminate indicating that the cable connection is correct and working.

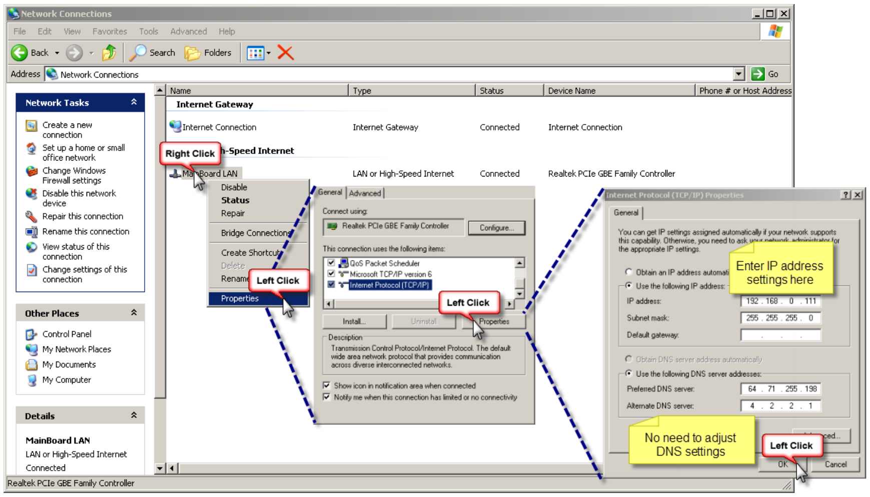
FYI: *See the section above “Connecting to the Management Computer or cable modem” for further information about choice of cables and explanation of link lights.*

2. Set the Management Computer’s Ethernet interface to a static IP address on the 192.168.0.x subnet, as described below:

FYI: *If the Management Computer currently has network settings that will need to be used again after the UCrypt device is configured, this would be a good time to makes note of the current settings if you don't already know them, so the network adapter may be readily returned to these values again.*

a) From the Control Panel, open **Network Connections** and select the connection associated with the Ethernet adapter to be used for connecting to the UCrypt device (e.g., Local Area Connection).

.



Name	Type	Status	Device Name	Phone # or Host Address
Internet Gateway				
Internet Connection	Internet Gateway	Connected	Internet Connection	
LAN or High-Speed Internet				
MainBoard LAN	LAN or High-Speed Internet	Connected	Realtek PCIe GBE Family Controller	

MainBoard LAN
LAN or High-Speed Internet
Connected

Realtek PCIe GBE Family Controller

Connect using:
Realtek PCIe GBE Family Controller

This connection uses the following items:
☑ QoS Packet Scheduler
☑ Microsoft TCP/IP version 6
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automati
● Use the following IP address:
IP address: 192 . 168 . 0 . 111
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 64 . 71 . 255 . 198
Alternate DNS server: 4 . 2 . 2 . 1

Figure 4-2: Management Computer Setup

b) Right click on the connection and select Properties.

c) Select Internet Protocol (TCP/IP) and click Properties.

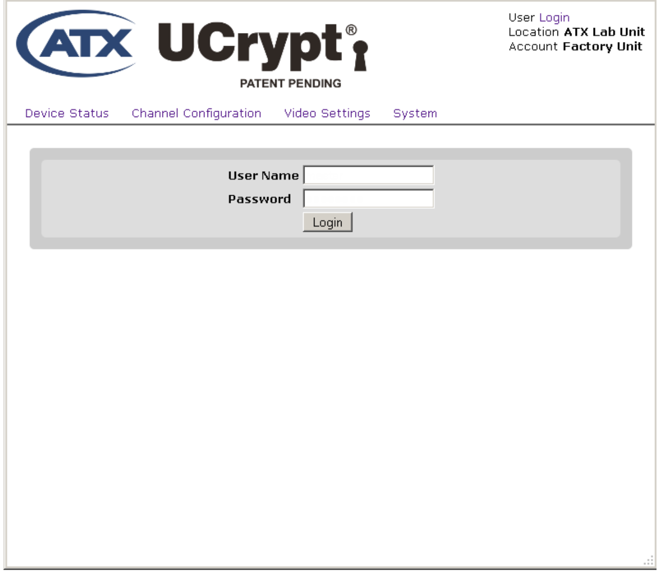
d) Click the selection box beside Use the following IP address to enter a check mark in the box.

e) In the IP address field, enter 192.168.0.x (where x represents any number from 1-253 except 23).

f) In the Subnet mask field enter 255.255.255.0.

g) Click OK and then OK again in the previous window.

3. On the Management Computer, open a web browser and enter **http://192.168.0.23** in the address field. You should be presented with the following screen, prompting you to log in:



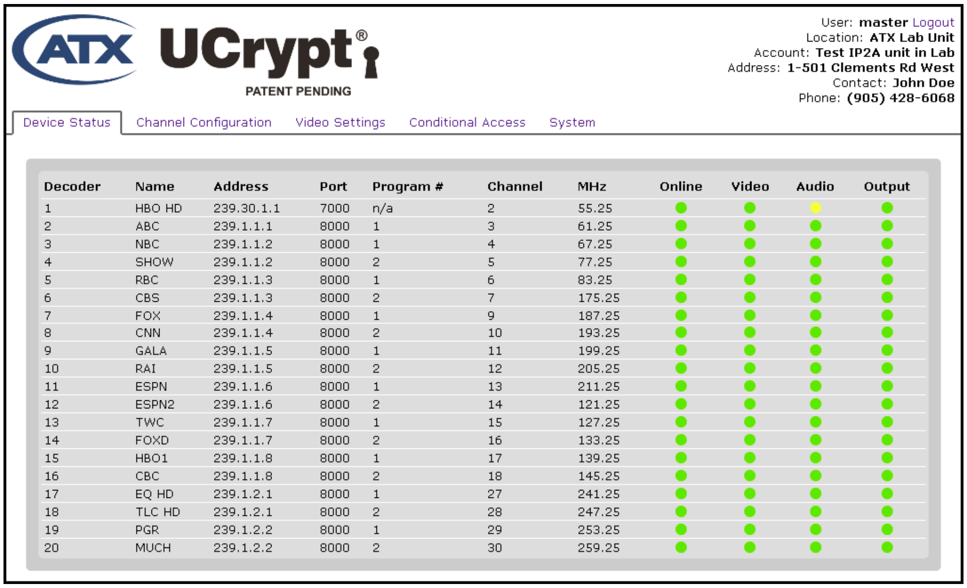
User Login
Location **ATX Lab Unit**
Account **Factory Unit**

User Name
Password

Figure 4-3: System Login Screen

When the login screen appears, enter an appropriate **User Name** and **Password** for the unit from Table 4.7a..

When the login username and password are successfully entered, the page in Figure 4-3 will be presented. Your screen may differ slightly from the illustration depending on whether the unit has previously applied configuration settings or if it is factory new.



User: **master** Logout
Location: **ATX Lab Unit**
Account: **Test IP2A unit in Lab**
Address: **1-501 Clements Rd West**
Contact: **John Doe**
Phone: **(905) 428-6068**

Decoder	Name	Address	Port	Program #	Channel	MHz	Online	Video	Audio	Output
1	HBO HD	239.30.1.1	7000	n/a	2	55.25	🟢	🟢	🟡	🟢
2	ABC	239.1.1.1	8000	1	3	61.25	🟢	🟢	🟢	🟢
3	NBC	239.1.1.2	8000	1	4	67.25	🟢	🟢	🟢	🟢
4	SHOW	239.1.1.2	8000	2	5	77.25	🟢	🟢	🟢	🟢
5	RBC	239.1.1.3	8000	1	6	83.25	🟢	🟢	🟢	🟢
6	CBS	239.1.1.3	8000	2	7	175.25	🟢	🟢	🟢	🟢
7	FOX	239.1.1.4	8000	1	9	187.25	🟢	🟢	🟢	🟢
8	CNN	239.1.1.4	8000	2	10	193.25	🟢	🟢	🟢	🟢
9	GALA	239.1.1.5	8000	1	11	199.25	🟢	🟢	🟢	🟢
10	RAI	239.1.1.5	8000	2	12	205.25	🟢	🟢	🟢	🟢
11	ESPN	239.1.1.6	8000	1	13	211.25	🟢	🟢	🟢	🟢
12	ESPN2	239.1.1.6	8000	2	14	121.25	🟢	🟢	🟢	🟢
13	TWC	239.1.1.7	8000	1	15	127.25	🟢	🟢	🟢	🟢
14	FOXD	239.1.1.7	8000	2	16	133.25	🟢	🟢	🟢	🟢
15	HBO1	239.1.1.8	8000	1	17	139.25	🟢	🟢	🟢	🟢
16	CBC	239.1.1.8	8000	2	18	145.25	🟢	🟢	🟢	🟢
17	EQ HD	239.1.2.1	8000	1	27	241.25	🟢	🟢	🟢	🟢
18	TLC HD	239.1.2.1	8000	2	28	247.25	🟢	🟢	🟢	🟢
19	PGR	239.1.2.2	8000	1	29	253.25	🟢	🟢	🟢	🟢
20	MUCH	239.1.2.2	8000	2	30	259.25	🟢	🟢	🟢	🟢

Figure 4-4: Default Page - Device Status Tab

4.7 Account Passwords and Privileges

There are a choice of three user accounts for managing operators privileges. The default settings for privileges are outlined in the following table. The privilege settings cannot be modified. The passwords may be changed.

Table 4.7a: Default User Account Passwords and Privileges

Username	Default Password	Modify Settings	Install Updates	Set Passwords
master	atx_ucrypt_master_password	Yes	Yes	Yes
admin	atx_ucrypt_admin_password	Yes	No	No
user	atx_ucrypt_user_password	No	No	No

FYI: *If the UCrypt device has previously been configured with a different User Name and Password, use the appropriate values for this unit. When the User Name and Password are changed in the system, the factory default values are lost. There is no “back door” User Name and Password if the master password is forgotten.*

SYSTEM TAB

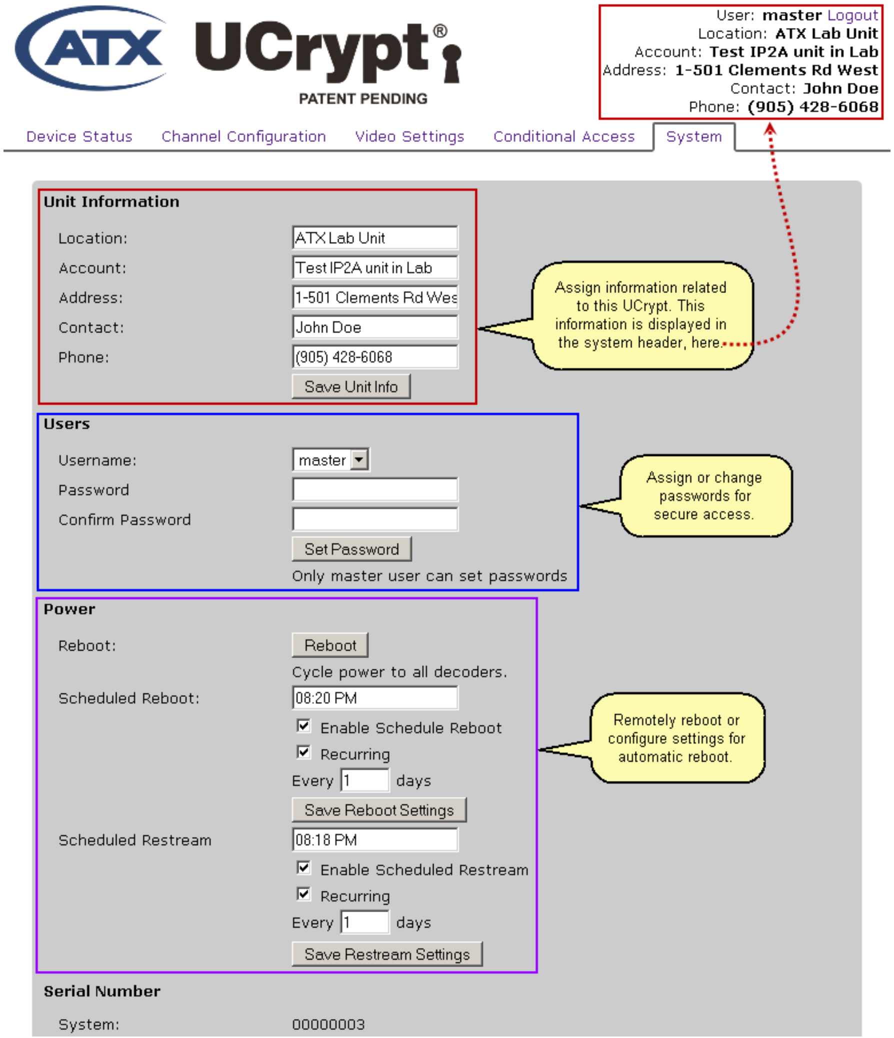
5. SYSTEM Tab - Configuration

5.1 In This Chapter

- "Unit Information"
- "Power"
- "Network"
- "Time"
- "Users"
- "Firmware"
- "Health"
- "Emergency Alert System"

5.2 Introduction

The 'System' tab is the location of the global system settings. The page is arranged in sections, each section dealing with a separate category of settings or information. Down the left side of the page are the section headings which identify the major elements or groups of elements. Headings of these groups of elements are listed below and described in detail.



User: **master** Logout
Location: **ATX Lab Unit**
Account: **Test IP2A unit in Lab**
Address: **1-501 Clements Rd West**
Contact: **John Doe**
Phone: **(905) 428-6068**

Unit Information

Location: ATX Lab Unit
Account: Test IP2A unit in Lab
Address: 1-501 Clements Rd Wes
Contact: John Doe
Phone: (905) 428-6068

Assign information related to this UCrypt. This information is displayed in the system header, here.

Users

Username: master
Password
Confirm Password
Only master user can set passwords

Assign or change passwords for secure access.

Power

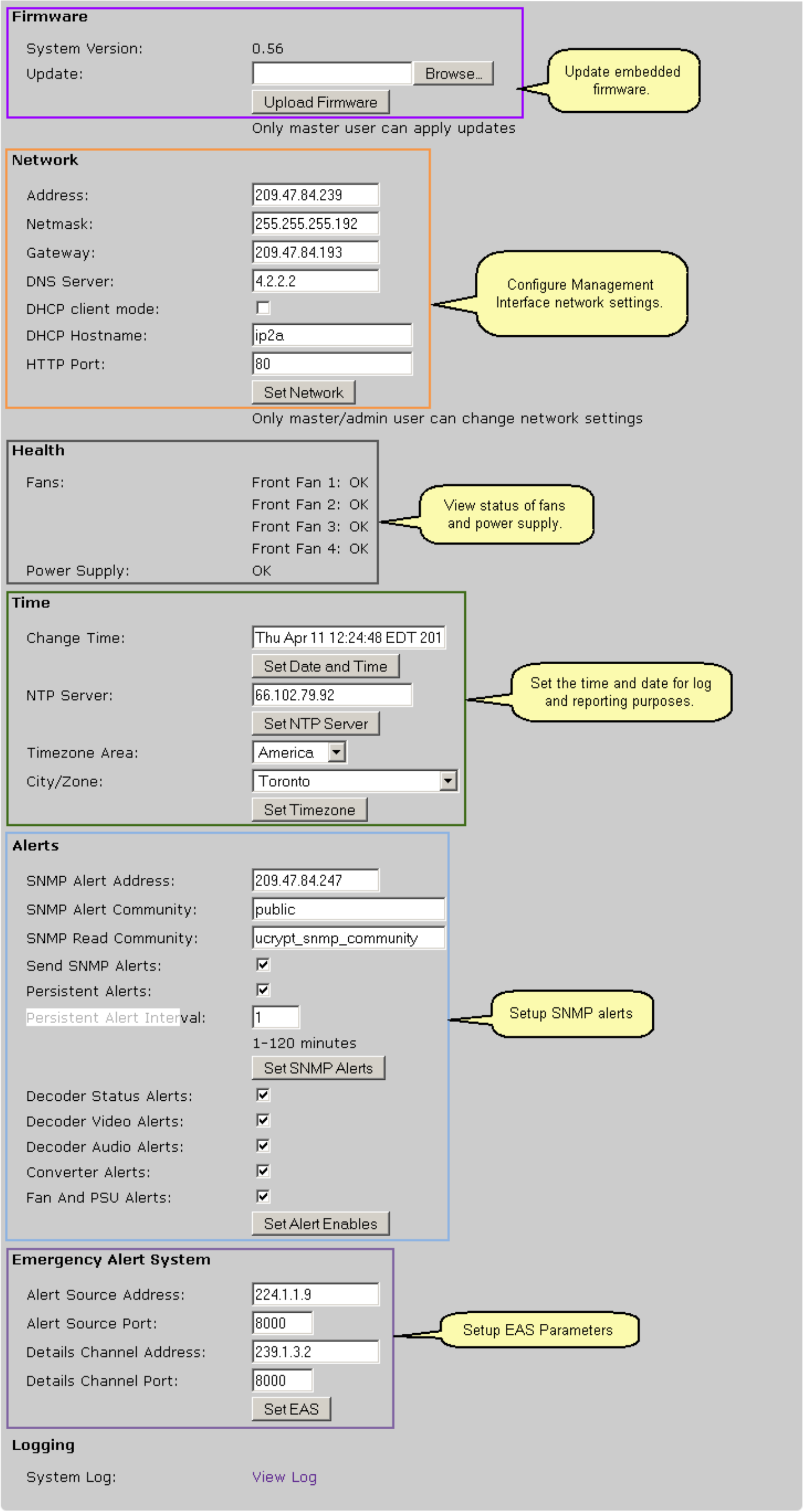
Reboot:
Cycle power to all decoders.
Scheduled Reboot: 08:20 PM
☑ Enable Schedule Reboot
☑ Recurring
Every 1 days
Scheduled Restream 08:18 PM
☑ Enable Scheduled Restream
☑ Recurring
Every 1 days

Remotely reboot or configure settings for automatic reboot.

Serial Number

System: 00000003

Figure 5-1: System Tab - Part 1



Firmware

System Version: 0.56

Update:

Only master user can apply updates

Update embedded firmware.

Network

Address: 209.47.84.239

Netmask: 255.255.255.192

Gateway: 209.47.84.193

DNS Server: 4.2.2.2

DHCP client mode: ☐

DHCP Hostname: ip2a

HTTP Port: 80

Only master/admin user can change network settings

Configure Management Interface network settings.

Health

Fans: Front Fan 1: OK
Front Fan 2: OK
Front Fan 3: OK
Front Fan 4: OK

Power Supply: OK

View status of fans and power supply.

Time

Change Time: Thu Apr 11 12:24:48 EDT 201

NTP Server: 66.102.79.92

Timezone Area: America

City/Zone: Toronto

Set the time and date for log and reporting purposes.

Alerts

SNMP Alert Address: 209.47.84.247

SNMP Alert Community: public

SNMP Read Community: ucrypt_snmp_community

Send SNMP Alerts: ☑

Persistent Alerts: ☑

Persistent Alert Interval: 1

1-120 minutes

Decoder Status Alerts: ☑

Decoder Video Alerts: ☑

Decoder Audio Alerts: ☑

Converter Alerts: ☑

Fan And PSU Alerts: ☑

Setup SNMP alerts

Emergency Alert System

Alert Source Address: 224.1.1.9

Alert Source Port: 8000

Details Channel Address: 239.1.3.2

Details Channel Port: 8000

Setup EAS Parameters

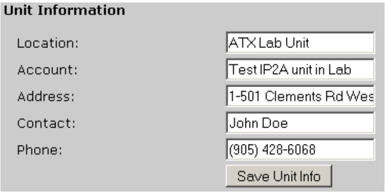
Logging

System Log: View Log

Figure 5-2: System Tab - Part 2

5.3 Unit Information

Information entered here is intended to identify the unit to the user who may be managing many of these devices. This helps the remotely located operator to identify and contact the correct person for any on-site service that may be required. This information is prominently displayed at the top of all configuration pages.



Unit Information

Location:	ATX Lab Unit
Account:	Test IP2A unit in Lab
Address:	1-501 Clements Rd Wes
Contact:	John Doe
Phone:	(905) 428-6068

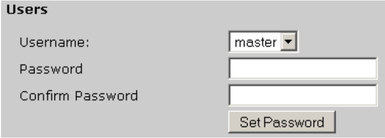
Figure 5-3: Unit Information Section

Table 5.3a: Unit Information Settings

Setting	Value	Description
Location	String	Alphanumeric text string describing the unit's physical location.
Account	String	Alphanumeric text string for an account name or number identifying the unit.
Address	String	Alphanumeric text string for the address of the UCrypt device.
Contact	String	Alphanumeric text string for the name of the contact person for this unit.
Phone	String	A numeric entry for the contact's phone number.

5.4 Users

Three built-in accounts are provided for access to the GUI. Only the Master user may change passwords. The Table 5.4a outlines factory default properties for each user account. The account names and properties may not be changed. It is recommended to reset these passwords to values appropriate to the operator's policy.



Users

Username:	master
Password	
Confirm Password	

Figure 5-4: Users Section

Table 5.4a: Users Settings

Username	Default Password	Modify Settings	Install Updates	Set Passwords
master	atx_ucrypt_master_password	Yes	Yes	Yes
admin	atx_ucrypt_admin_password	Yes	No	No
user	atx_ucrypt_user_password	No	No	No

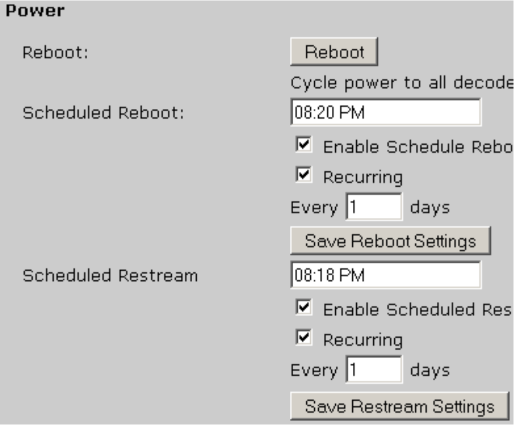
To set the account passwords:

1. Select the username that is to be changed from the drop down menu.
2. Enter the new password.
3. Re-enter the new password.
4. Click the **Set Password** button.

5.5 Power

Power options allow flexible management if it becomes necessary to power cycle or re-boot the device in circumstances when the user is remotely located. Options are available to perform power cycling without the need to physically visit the UCrypt equipment and shutdowns can be scheduled. The control buttons have attached descriptive text which is quite intuitive but an expanded explanation is offered here.

NOTE: *Use of Reboot will result in immediate loss of service for the duration of the process, about 90 seconds.*



Power

Reboot: Reboot

Cycle power to all decode

Scheduled Reboot: 08:20 PM

☑ Enable Schedule Rebo

☑ Recurring

Every 1 days

Save Reboot Settings

Scheduled Restream 08:18 PM

☑ Enable Scheduled Res

☑ Recurring

Every 1 days

Save Restream Settings

Figure 5-5: Power Section

Table 5.5a: Power Settings

Setting	Value	Description
Reboot	Button	Cycle power to all decoders. Will perform an immediate warm reboot of the UCrypt processor but does not cycle the power off.
Scheduled Reboot	String	The time at which a reboot will occur. Time must be entered in AM/PM format such as **03:45 AM.**
Enable Scheduled Reboot	Checkbox	Enable the reboot to occur at the time specified in **Scheduled Reboot**.
Recurring	Checkbox	Causes the reboot to recur in the number of days specified.
Every x days	Integer	The number of days before a reboot will re The number of days before a reboot will recur.
Save Reboot Settings	Button	Saves the settings changes.
Scheduled Restream	String	Time must be entered in AM/PM format such as **03:45 AM.** This enables the UCrypt device to transmit an IGMP **Join-group** command on the IP IN interface for each decoder in the unlikely event that any decoders have lost the subscription to their stream. There will be a very short loss of stream sync when this occurs on a program that has not lost its stream. In an unattended system, it may be an advantage to transmit this Join-group every day to ensure stream continuity and at a time when it is likely that viewership is low such as 2 AM to 3 AM.
Enable Scheduled Restream	String	Enable the restream to occur at the time specified in **Scheduled Restream**.
Recurring	Checkbox	Causes the restream to recur in the number of days specified.
Every x days	Checkbox	The number of days before a restream will recur.
Save Restream settings	Checkbox	Saves the settings changes.

5.6 Serial Number

This section lists the serial number of the UCrypt system itself for record keeping, reference and warranty purposes.

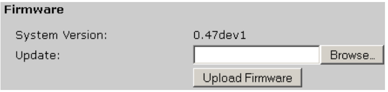
Serial Number

System: 00000003

Figure 5-6: Serial Number Section

5.7 Firmware

This section presents a summary of the installed version of system firmware. This is also the location where the system firmware may be updated when required. Firmware update files are provided by ATX Networks from time to time to improve system performance and/or add new features. Files must first be downloaded to the Management Computer from the ATX Networks support site. The update file must reside on a Management Computer local drive or on a local area network drive which is accessible to the Management Computer. Click the **Browse** button to navigate to the location of the update file. Click the **Upload Firmware** button to start the update procedure.



Firmware

System Version: 0.47dev1

Update:

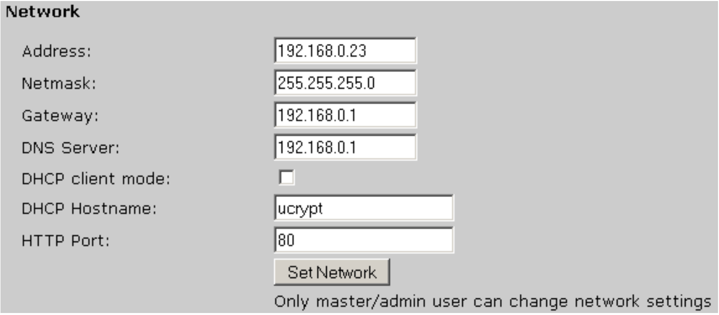
Figure 5-7: Firmware Section

NOTE: *Updating firmware is a service affecting operation and should only be initiated during a maintenance window on any equipment that is in service.*

5.8 Network

The network section allows configuration of all network parameters for installation on a public or private network. The factory default values for the network parameters are listed in Table 5.8a.

After all changes required have been made to network settings, click the **Set Network** button to apply the settings. If the network settings are not saved, navigating away from the System page will discard all changes made. If the network address was changed, you will need to log in again after entering the new address in your browser.



Network

Address: 192.168.0.23

Netmask: 255.255.255.0

Gateway: 192.168.0.1

DNS Server: 192.168.0.1

DHCP client mode: ☐

DHCP Hostname: ucrypt

HTTP Port: 80

Only master/admin user can change network settings

Figure 5-8: Network Section

Table 5.8a: Default Network Configuration

Setting	Default Value	Description
Address	192.168.0.23	The IP address assigned to the rear panel “MGMT PORT” port for the Management Interface. See “Table 5.8b: IP Address Range Supported” on page 5-6 and “IP Address Range Restricted” on page 5-6. If the address is changed, login with the new address.
Netmask	255.255.255.0	The subnet mask associated with the ‘Network Address’ above. Set according to the network requirements.
Gateway	192.168.0.1	The router address that provides network access.
DNS Server	192.168.0.1	Specify a DNS server if e-mail alerts are configured or URLs are used anywhere in this UCrypt device.
DHCP Client Mode	Off	This enables the internal DHCP client to dynamically acquire an IP address from a DHCP server. Commonly used when connected to a cable modem.
DHCP Hostname	UCrypt	Set this if required by your DHCP configuration.
HTTP Port	80	When accessing remotely, the web server needs to be presented on a defined port on the IP address assigned. The default and standard HTTP address is 80. Change this address here if your system design requires. If the port is changed, login again with the new IP port number.

***FYI:** Note on DNS Search Domain Usage.* DNS search domain value is for automatically appending additional domain information to e-mail addresses and may be required for some e-mail servers. Leave this value blank (default value) unless you know that a DNS search domain is required for your e-mail address server.

Table 5.8b: IP Address Range Supported

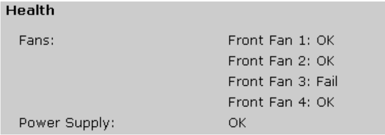
IP Class	Start Address	End Address
A	10.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	192.168.199.255
C	192.169.201.0	223.255.255.255

Table 5.8c: IP Address Range Restricted

192.168.200.0	192.168.200.255

5.9 Health

Basic diagnostic features have been provided which may help to keep the unit in good "Health" by monitoring internal functions and which in turn can be used by the ATX support team in diagnosing internal problems. The UCrypt device also monitors and reports on cooling fans as explained next.



Health

Fans: Front Fan 1: OK
Front Fan 2: OK
Front Fan 3: Fail
Front Fan 4: OK

Power Supply: OK

Figure 5-9: Health Section

5.9.1 Fans

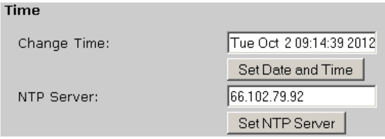
There are four cooling fans located on the front panel numbered from left to right ascending. The status of each fan is indicated here and the assessed condition of the fans will be **OK** or **Fail**. If a fan is reported as **Fail**, the fan should be changed as soon as practical. Replacement fans are available from ATX Networks. Fans may be removed from the front panel simply by removing four Phillips screws and a power plug. When the fan is replaced, the alarm condition is automatically remitted.

5.9.2 Power Supply

This indicator reports on power supply status. If one of the redundant power supplies fails, this will be reported here as 'Fail'.

5.10 Time

If it required that logs and alerts be time stamped correctly for troubleshooting purposes, the local date and local time information may be entered here. An onboard CMOS backup battery saves the settings through power outages. This time may be maintained automatically if a 'NTP Time Server' address is entered.



Time

Change Time: Tue Oct 2 09:14:39 2012

NTP Server: 66.102.79.92

Figure 5-10: Time Section

5.10.1 Change Time:

Click in the white time dialog box to edit the time and date within the existing 24 hour format. The time updates every 10 seconds while you view the page.

Time Setting Format:

Use the 24 hour format **mmm dd HH:MM:SS YYYY** and an example is **Oct 2 12:27:53 2012**. Note the space between month, date and hours as well as between seconds and year. Click the **Set Date and Time** button to save the settings.

Time Setting Guidelines:

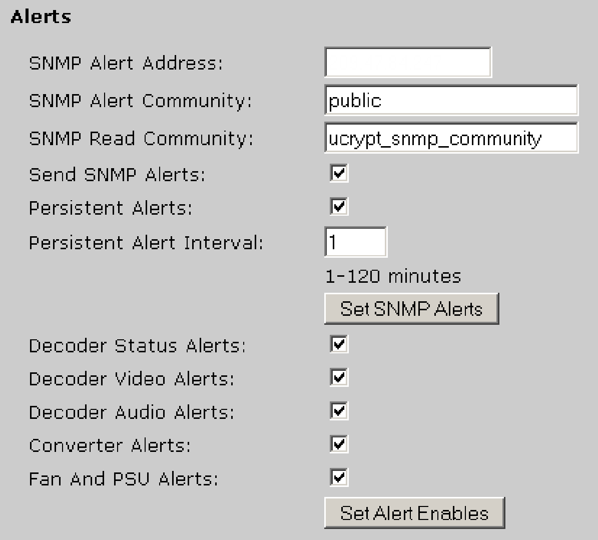
- Do not attempt to edit the day of the week as this in calculated automatically from the entered date.
- Use only the first three letters of the month and case does not matter.
- Deleting the time and date will cause the clock to be set to 00:00:00 on the date stored in the non-volatile memory.
- Do not attempt to change the time format.

5.10.2 NTP Server:

If an NTP server is available on the network or if Internet access is available, an NTP server address or URL may be specified to ensure an accurate time is always set for the UCrypt device's reports and alerts. This server will provide date and time to the UCrypt system. Updates are automatic once a valid address is entered. URL format may be entered only if a DNS server has been defined as well. If changes were made to the NTP server IP address or URL, click the **Set NTP Server** button to save the changes. This is not service affecting.

5.11 Alerts

The UCrypt device can provide alerts about a number of detected error events via SNMP traps. The detected events are designed to assist in field diagnosis of problems that may occur on installed UCrypt systems some of which are related to errors detected on incoming programs and streams. Each alert may be enabled individually by clicking the check box. When all desired alerts are selected, the operator must click the **Set Alert Enables** button. Changes made to the 'SNMP Alert Community' or 'SNMP Alert Address' will require you to click **Set SNMP Alerts** button to save and apply the changes. This action is not service affecting.



Alerts

SNMP Alert Address:

SNMP Alert Community: public

SNMP Read Community: ucrypt_snmp_community

Send SNMP Alerts: ☑

Persistent Alerts: ☑

Persistent Alert Interval: 1

1-120 minutes

Decoder Status Alerts: ☑

Decoder Video Alerts: ☑

Decoder Audio Alerts: ☑

Converter Alerts: ☑

Fan And PSU Alerts: ☑

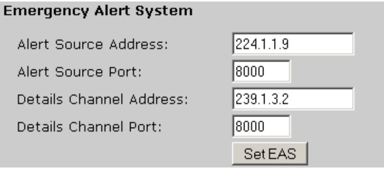
Figure 5-11: Alerts Section

Table 5.11a: Alerts Settings

Setting	Value	Description
SNMP Alert Address	IP Address	Target IP address for the trap. (Address of the external SNMP manager)
SNMP Alert Community	String	The SNMP alert community. This is usually set to **public.**
SNMP Read Community	String	The SNMP read community. By default set to **ucrypt_snmp_community**.
Send SNMP Alerts	Checkbox	Enable the sending of SNMP traps. Default is unticked (off).
Persistent Alerts	Checkbox	Enable Persistent Alerts feature which remembers that an alert has been sent and will not re-send until the specified elapsed time, from 1 to 120 minutes.
Persistent Alert Interval	Integer	Interval for which a sent alert will be remembered if 'Persistent Alerts' box is checked..
Set SNMP Alerts	Button	Click to save and apply SNMP settings changes. Not service affecting.
Decoder Status Alerts	Checkbox	Enable the sending of traps related to the decoding of IP streams.
Decoder Video Alerts	Checkbox	Enable the sending of traps related to the video stream being decoded.
Decoder Audio Alerts	Checkbox	Enable the sending of traps related to audio streams being decoded.
Converter Alerts	Checkbox	Enable the sending of traps related to the analog up converters.
Fan & Power Supply Alerts	Checkbox	Enable the sending of alerts for the power supplies. If one of the two redundant power supplies fails an alert will be sent.
Set Alert Enables	Button	Click to save and apply Alert Settings changes. Not service affecting.

5.12 Emergency Alert System

Mandated by the FCC, the Emergency Alert System (EAS) in the United States disseminates emergency warnings of pressing local, regional, or national importance over a variety of networks and it is a requirement of all associated carrier equipment to support the EAS system to the greatest extent possible. The UCrypt IP to Analog provides support of EAS signaling standards through thoughtful design and implementation. This section describes the support for SCTE 18 allowing the equipment to work effectively with compliant and non-compliant TVs and enabling the Cable Service Provider to comply with FCC mandates. The reception of emergency alert messages by the UCrypt device is done in accordance with ‘Figure 1 Emergency Alert Message Example Processing Flow Diagram’ of the SCTE 18 standard.



Emergency Alert System

Alert Source Address: 224.1.1.9
Alert Source Port: 8000
Details Channel Address: 239.1.3.2
Details Channel Port: 8000

Figure 5-12: EAS Section

5.12.1 EAS Compatibility

The UCrypt IP to Analog system supports EAS text messages on SCTE 18 Compliant and Non Compliant TVs by over-riding the output programs of all processed channels with a program with the EAS alert embedded. Messages are not passed through to be displayed as they are in a STB environment. Full SCTE 18 compatibility requires the creation of a ‘Details Channel’ as outlined in “Creating the EAS Details Channel” on page 5-2 for force tune events. Alternately, any regional broadcaster who is required to carry the SCTE 18 messages may also be used as a source.

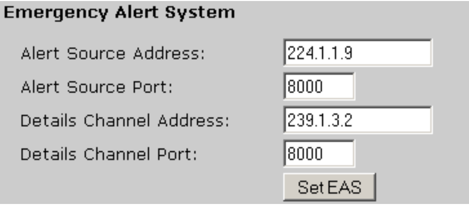
5.12.2 Support for SCTE 18

The UCrypt IP to Analog system achieves compliance with SCTE 18 through the use of an external ‘Details Channel’ which is created for just this application. The UCrypt device monitors and receives EAS messages from an external EAS Message Generator with Ethernet output. The UCrypt device supports text and video alert types. Audio only alerts are not supported.

When an EAS alert is received, the following happens:

- UCrypt device detects the SCTE 18 text message over the external ‘EAS Message Generator’ IP address.
- UCrypt device subscribes to the IP program as defined in the ‘Details Channel Address and Port’ fields which must correspond to the address where the Cable Service Provider will have a program with the EAS text alert already encoded into the program stream available. See “Creating the EAS Details Channel” on page 5-2 for details.
- UCrypt device replicates this program across all active output programs.
- TVs tuned to any output program or channel get the contents of the encoded background plus the EAS text message by default.
- In this scenario, the program being watched by the user is interrupted for the duration of the alert in order to display the text message - i.e. it is not embedded over each individual program like it is in an STB environment.

5.13 EAS Configuration



Emergency Alert System

Alert Source Address: 224.1.1.9
Alert Source Port: 8000
Details Channel Address: 239.1.3.2
Details Channel Port: 8000

Figure 5-13: Emergency Alert System

Table 5.13a: Emergency Alert System Settings

Setting	Value	Description
Alert Source Address	IP Address	The multicast IP address of the message stream from an external EAS generator with IP output which must be presented to the ‘IP IN’ port.
Alert Source Port	Integer	The IP Port number of the multicast IP message stream associated with the ‘Alert Source Address’.
Details Channel Address	IP Address	The IP address of the external ‘Details Channel’ which is created for the purposes of displaying the embedded EAS message which must be available on the ‘IP IN’ port. See “5.14 Creating the EAS Details Channel” on page 5-10.
Details Channel Port	Integer	The IP Port number of the ‘Details Channel’ associated with the ‘Details Channel Address’.
Set EAS	Button	Saves and applies the EAS settings changes.

5.13.1 Details Channel

Video content at the specified **Details Channel Address** location on the input feed to the UCrypt device will be tuned during:

1. A low priority EAS text message event.
2. A high priority EAS force tune event.

Typically this would be the program on the plant at which an encoded output of a ‘crawl capable’ set top box is inserted. The UCrypt equipment will then replicate the program’s contents over all active output programs on all active output channels in order to display an MPEG encoded version of the EAS text message or force tune content on the TVs. This channel needs to be created by the Cable Service Provider and made available on the cable plant at the UCrypt device’s ‘IP IN’ port and specified in the configuration settings.

An alternate to creating a Details Channel is to use a network broadcaster who’s broadcast stream is available on the UCrypt device’s input and who is required to comply with EAS rules and will be broadcasting the alerts. Use the broadcaster’s multicast IP address and port in place of the external Details Channel.

5.14 Creating the EAS Details Channel

5.14.1 The Problem

The Cable Service Provider is required to provide EAS text crawl and force tuning functionality when required to as many end users as possible but many end user TV devices are not SCTE 18 Compliant. Through configuration of the UCrypt IP to Analog EAS features, the service provider can supply EAS Text messages and EAS Force Tune events to these Non compliant TVs with a single setup that may be used across all UCrypt device installations. While the Cable Service Provider may already be carrying the required 'Details Channel' with SCTE 18 EAS messaging in the OOB carrier, the UCrypt IP to Analog equipment does not have any OOB tuners onboard. Normally the Cable System STB receives the SCTE 18 message on it's OOB carrier and internally tunes or creates the text message. A different approach is required to receive the SCTE 18 message and to create the appropriate output program. This involves an external SCTE 18 setup to handle force tuning and text message creation.

5.14.2 The Challenge

The UCrypt device has embedded features to replicate a 'Details Channel' across all programs on all analog outputs when alerts are received but does not have capability to create the Text Crawl on output programs as this requires an MPEG2 encoder. It also has no OOB tuner to receive EAS messages. Further, the only input port is Ethernet and this 'Details Channel' program must be available to all UCrypt devices so the required program must arrive already MPEG2 encoded in an IP multicast. There is an easy and inexpensive workaround to solve this challenge.

5.14.3 The Solution

It is suggested that the following equipment be assembled to create a new 'Details Channel' and the resulting signals be made available on the distribution switch at the headend where the UCrypt device is installed:

- An SCTE 18 compliant cable TV STB.
- An inexpensive MPEG encoder with IP output such as the ATX Networks DigiVu Mini or Nano.

Refer to "Figure 5-14: Creating The EAS Details Channel" on page 5-11 for more details. The "always on" STB will be fed with the cable network signals as usual. Since the set top box would be subject to any EAS alerts, it would display, at its video output, any 'EAS Text Alert' or 'EAS Force Tune' content when EAS alerts are received on it's OOB carrier. The STB video output would feed the MPEG2 video encoder which would be configured to have an IP multicast as its output. With the MPEG2 encoder's output available to the UCrypt device "IP IN" Ethernet port, the UCrypt device could subscribe to the set top box multicast when required, during EAS alert events. The UCrypt device configuration allows specifying the 'Details Channel Address' IP multicast address and port number of the source.

5.14.4 Receiving the SCTE 18 Messages

The UCrypt device would be configured to receive the SCTE 18 messages through its "IP IN" Ethernet port that is connected to an EAS Encoder/Decoder with Ethernet output capability. This setup is shown in Figure 5-13 which gives sufficient detail to allow adapting to the specific conditions at the Cable Service Provider headend.

5.14.5 The Way it Works

When an EAS alert is received, the following happens:

- UCrypt device detects the SCTE 18 text message by monitoring the external 'EAS Message Generator' IP multicast address.
- The STB used to create the new 'Details Channel' will simultaneously receive the EAS message and display the appropriate text crawl or will force tune to the 'Cable System Details Channel' as appropriate and according to the EAS message received.
- UCrypt device subscribes to the IP multicast program as defined in the 'Details Channel Address and Port' fields which must correspond to the address where the Cable Service Provider will have a program with the EAS text alert already encoded into the program stream available.
- UCrypt device replicates this program across all active output programs.
- TVs tuned to any output program or channel get the contents of the encoded background plus the EAS text message or force tune content by default.

See “5.14 Creating the EAS Details Channel” on page 5-10 for more details.

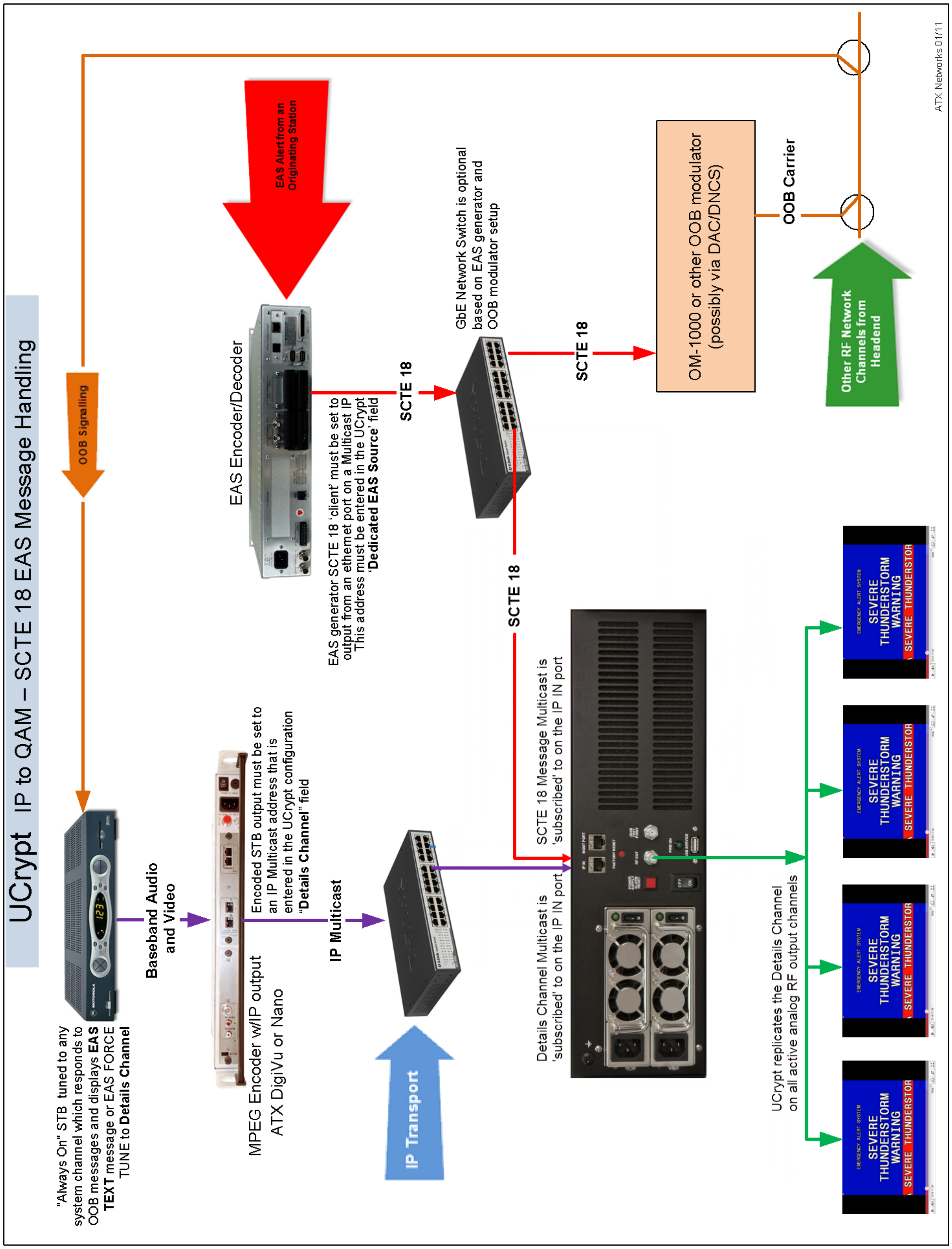

UCrypt IP to QAM – SCTE 18 EAS Message Handling
OOB Signalling
EAS Alert from an Originating Station
EAS Encoder/Decoder
EAS generator SCTE 18 'client' must be set to output from an ethernet port on a Multicast IP This address must be entered in the UCrypt 'Dedicated EAS Source' field
SCTE 18
GbE Network Switch is optional based on EAS generator and OOB modulator setup
SCTE 18
OM-1000 or other OOB modulator (possibly via DAC/DNCS)
OOB Carrier
Other RF Network Channels from Headend
ATX Networks 01/11
"Always On" STB tuned to any system channel which responds to OOB messages and displays EAS TEXT message or EAS FORCE TUNE to Details Channel
Baseband Audio and Video
MPEG Encoder w/IP output ATX DigiVu or Nano
Encoded STB output must be set to an IP Multicast address that is entered in the UCrypt configuration "Details Channel" field
IP Multicast
IP Transport
SCTE 18
Details Channel Multicast is 'subscribed' to on the IP IN port
SCTE 18 Message Multicast is 'subscribed' to on the IP IN port
UCrypt replicates the Details Channel on all active analog RF output channels
EMERGENCY ALERT SYSTEM
SEVERE THUNDERSTORM WARNING
SEVERE THUNDERSTOR

Figure 5-14: Creating The EAS Details Channel

5.15 More Information on SCTE18 and EAS

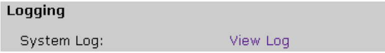
SCTE18

Download the SCTE 18 document for details on the standard.

EAS

More information about EAS in general may be found in the Electronic Code of Federal Regulations (e-CFR) Title 47 Part 11 at www.gpo.gov/fdsys/pkg/CFR-2009-title47-vol1/pdf/CFR-2009-title47-vol1-part11.pdf.

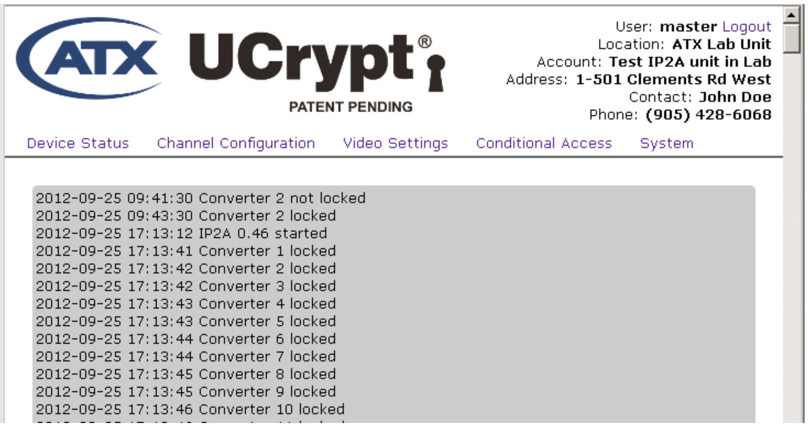
5.16 Logging


Logging

System Log: View Log

Figure 5-15: Logging Section

Logging of all critical and informational processes is automatically performed that may be important for troubleshooting. A time stamp is added to each entry to help understand the timing of the events. The time stamp derives its clock reference from 'Time' setting on the 'System' page. The format of the log is designed to be friendly and informative to the field personnel responsible for reading it. A sample of a log is shown in Figure 5-16.



User: **master**
Location: **ATX Lab Unit**
Account: **Test IP2A unit in Lab**
Address: **1-501 Clements Rd West**
Contact: **John Doe**
Phone: **(905) 428-6068**

```
2012-09-25 09:41:30 Converter 2 not locked
2012-09-25 09:43:30 Converter 2 locked
2012-09-25 17:13:12 IP2A 0.46 started
2012-09-25 17:13:41 Converter 1 locked
2012-09-25 17:13:42 Converter 2 locked
2012-09-25 17:13:42 Converter 3 locked
2012-09-25 17:13:43 Converter 4 locked
2012-09-25 17:13:43 Converter 5 locked
2012-09-25 17:13:44 Converter 6 locked
2012-09-25 17:13:44 Converter 7 locked
2012-09-25 17:13:45 Converter 8 locked
2012-09-25 17:13:45 Converter 9 locked
2012-09-25 17:13:46 Converter 10 locked
```

Figure 5-16: Sample Log Output

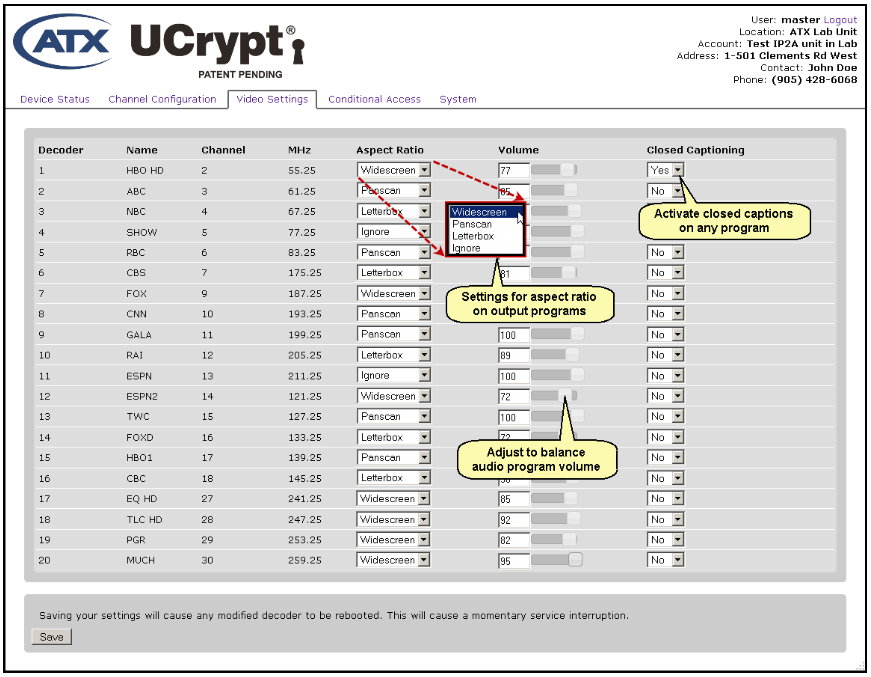
The log file display will vary depending on what processes have taken place since the last time the log was cleared. Usually the log will be referred to when a problem has arisen and support personnel are troubleshooting. A copy of the file may be taken by simply left clicking on the text at the top of the page and holding the left mouse button down while dragging to the bottom. Right click and chose **copy** from the mouse menu to copy the text to the Windows clipboard. Open Notepad or another text editor and paste the text. Save as a .txt file. If requesting support from ATX Networks Support Engineers, you may be asked to send a copy of this log to the support engineer.

VIDEO SETTINGS TAB

6. Video Settings Tab - Configuration

6.1 Introduction

The ‘Video Settings’ tab in the Management Interface is a page that presents dialogs and controls related to the configuration of video properties of the output channels. The controls available are related to setting aspect ratio of the output video program and balancing volume of the accompanying audio program.


ATX UCrypt®
PATENT PENDING
Activate closed captions on any program
Settings for aspect ratio on output programs
Adjust to balance audio program volume
Widescreen
Panscan
Letterbox
Ignore

User: master Logout
Location: ATX Lab Unit
Account: Test IP2A unit in Lab
Address: 1-501 Clements Rd West
Contact: John Doe
Phone: (905) 428-6068

Device Status | Channel Configuration | Video Settings | Conditional Access | System

Decoder	Name	Channel	MHz	Aspect Ratio	Volume	Closed Captioning
1	HBO HD	2	55.25	Widescreen	77	Yes
2	ABC	3	61.25	Panscan	85	No
3	NBC	4	67.25	Letterbox		
4	SHOW	5	77.25	Ignore		
5	RBC	6	83.25	Panscan		No
6	CBS	7	175.25	Letterbox	81	No
7	FOX	9	187.25	Widescreen		No
8	CNN	10	193.25	Panscan		No
9	GALA	11	199.25	Panscan	100	No
10	RAI	12	205.25	Letterbox	89	No
11	ESPN	13	211.25	Ignore	100	No
12	ESPN2	14	121.25	Widescreen	72	No
13	TWC	15	127.25	Panscan	100	No
14	FOXD	16	133.25	Letterbox	72	No
15	HBO1	17	139.25	Panscan		No
16	CBC	18	145.25	Letterbox	[illegible]	No
17	EQ HD	27	241.25	Widescreen	85	No
18	TLC HD	28	247.25	Widescreen	92	No
19	PGR	29	253.25	Widescreen	82	No
20	MUCH	30	259.25	Widescreen	95	No

Saving your settings will cause any modified decoder to be rebooted. This will cause a momentary service interruption.

Save

Figure 6-1: Video Settings Tab

Table 6.1a: Video Settings

Setting	Value	Description
Decoder		The decoder number for reference within the UCrypt device. It is not transmitted or used outside the Management Interface.
Name		A name for each program assigned for easier identification of the program in the Management Interface not used or transmitted outside the UCrypt device and is not seen by the end used/viewer. Name is fixed on this tab but may be defined on the “Channel Configuration Tab” on page 7-1.
Channel		The RF channel assigned to each decoder output. Depending on the model ordered, this channel is either EIA/NTSC for North America or CCIR B/G for Europe. Channel is fixed on this screen but may be defined on the “Channel Configuration Tab” on page 7-1.
MHz		For information only; lists the video carrier frequency of the channel modulator. MHz is linked to the assigned output channel which is defined on the “Channel Configuration Tab” on page 7-1.
Aspect Ratio	Drop down menu	The aspect ratio for each program, independently defined with the drop down menu. Default is ‘Widescreen’. See “6.1.2 Aspect Ratio Settings”.
Volume	Integer or slider	Each program may be adjusted independently for its audio output volume with this slider control. See “6.1.1 Adjusting the Program Volume”

Closed Captioning	Drop down menu	If closed captions are available on a program, they may be turned on for each individual program by selecting **Yes** from the drop down menu and the caption will be displayed on the analog channel after clicking the **Save** button.
Save	Button	All changes made to the Video Settings page must be manually saved before navigating to another page or closing the browser. If changes are made but not saved, the changes are not applied and are discarded when leaving the page.

⚠ ***NOTE:*** *Clicking the* ***Save*** *button is service affecting. Services on this UCrypt device will be interrupted momentarily while the configuration is saved and applied.*

6.1.1 Adjusting the Program Volume

Adjustments to the program volume could be necessary due to differing source program audio levels. Adjust this control while listening to the audio level on a TV connected to the UCrypt device's RF output. Each time the level is adjusted up or down, click the **Save** button to save the setting and apply it to the decoder before the difference will be heard on the TV. The number is relative (a percentage of full volume) and does not relate to an absolute output level. Settings between 0 (muted) and 99 (full volume) are possible. Use this only to balance the audio levels between programs, reducing only the programs that are louder than the average volume of the majority of other programs.

6.1.2 Aspect Ratio Settings

Widescreen

- 16:9 aspect ratio presentation

Select 'Widescreen' for televisions which have automatic ratio switching. In this mode, the television switches between 4:3 and 16:9 depending on the video content, and full content is displayed for both. The widescreen setting will always display all of the picture regardless of the source ratio and is therefore the default setting.

Panscan

- 4:3 aspect ratio presentation

Select 'Panscan' for televisions with no automatic aspect ratio switching, where the video image is required to fill the full 4:3 screen. In this mode, 4:3 content fits the screen correctly, and any 16:9 video content is cropped on the left and right sides.

Letterbox

- 4:3 aspect ratio in Letterbox presentation

Select 'Letterbox' for televisions with no automatic aspect ratio switching, where the full 16:9 screen is required. In this mode, 4:3 content fits the screen correctly, and any 16:9 content is displayed in full, with black bars above and below.

Ignore

- 4:3 aspect ratio stretched to 16:9
- 16:9 aspect ratio compressed to 4:3

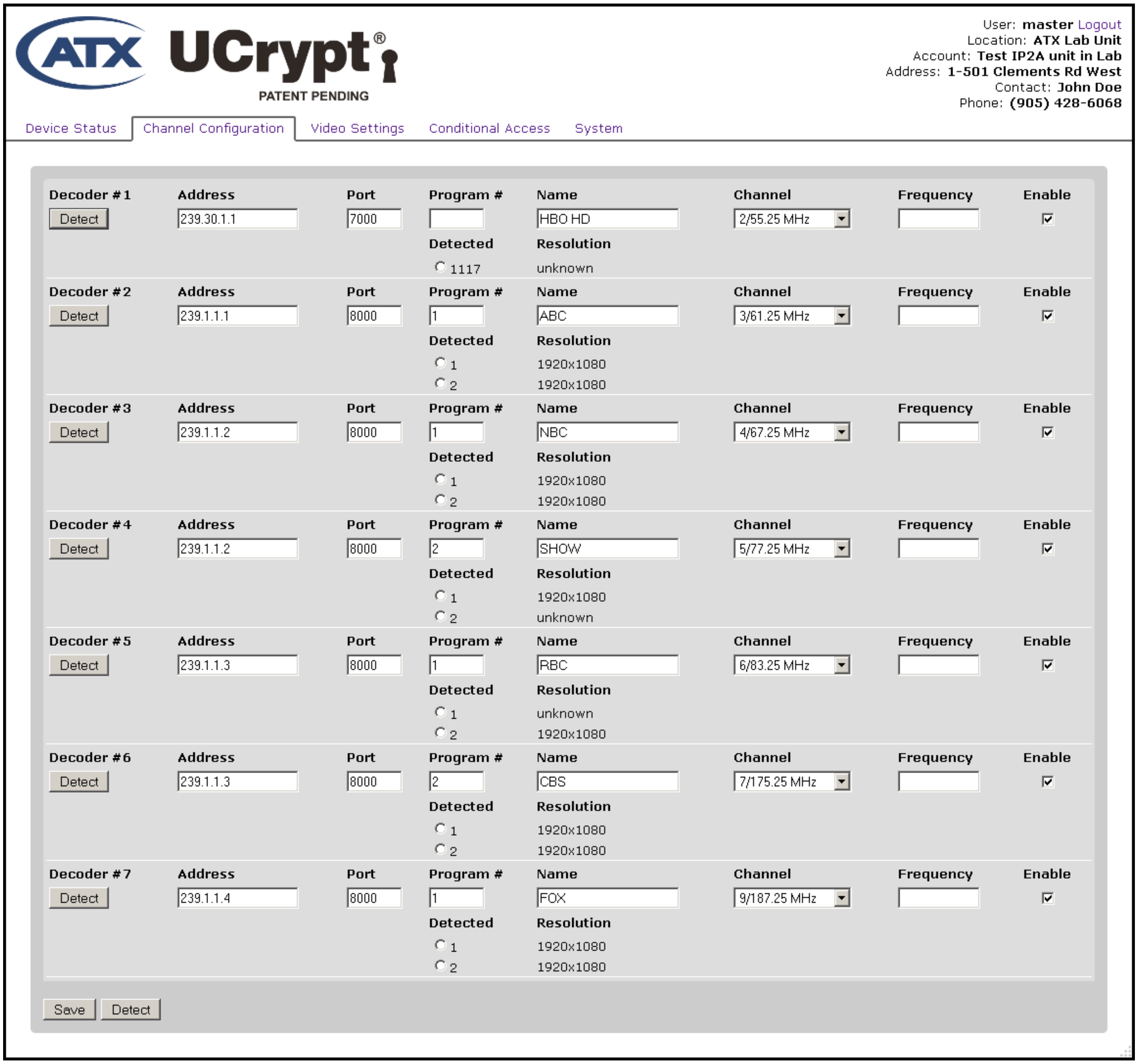
Select 'Ignore' to ignore the aspect ratio of the video, and assume that it is the same as the ratio of the output. On 16:9 display, a 4:3 image will appear vertically distorted. On a 4:3 display, a 16:9 image will appear vertically distorted.

CHANNEL CONFIGURATION TAB

7. Channel Configuration Tab

7.1 Introduction

The Channel Configuration tab, shown in Figure 7-1, allows the operator to specify the incoming multicast SPTS or MPTS IP streams that contain the programs that will be processed as well as the RF channel that the program will be output on. The channel may be named with alpha-numeric characters for identification in the UCrypt Management Interface. The decoder and RF output may be disabled if less that 20 channels are to be configured for the device.



User: **master** Logout
Location: **ATX Lab Unit**
Account: **Test IP2A unit in Lab**
Address: **1-501 Clements Rd West**
Contact: **John Doe**
Phone: **(905) 428-6068**

Decoder	Address	Port	Program #	Name	Channel	Frequency	Enable	Detected	Resolution
Decoder #1	239.30.1.1	7000		HBO HD	2/55.25 MHz		☑	○ 1117	unknown
Decoder #2	239.1.1.1	8000	1	ABC	3/61.25 MHz		☑	○ 1 ○ 2	1920x1080 1920x1080
Decoder #3	239.1.1.2	8000	1	NBC	4/67.25 MHz		☑	○ 1 ○ 2	1920x1080 1920x1080
Decoder #4	239.1.1.2	8000	2	SHOW	5/77.25 MHz		☑	○ 1 ○ 2	1920x1080 unknown
Decoder #5	239.1.1.3	8000	1	RBC	6/83.25 MHz		☑	○ 1 ○ 2	unknown 1920x1080
Decoder #6	239.1.1.3	8000	2	CBS	7/175.25 MHz		☑	○ 1 ○ 2	1920x1080 1920x1080
Decoder #7	239.1.1.4	8000	1	FOX	9/187.25 MHz		☑	○ 1 ○ 2	1920x1080 1920x1080

Figure 7-1: Channel Configuration Tab

7.2 Channel Configuration Settings

The programs to be decoded may be on a Single Program Transport Stream (SPTS) or Multi Program Transport Stream (MPTS). The IP and must be known to the operator and present on the Ethernet input port. There is no mechanism to detect the programs or IP streams that may be present. The Stream must be a multicast stream. If the stream is MPTS, the IP address and port must be entered, then the Detect button clicked. Any programs present will be found and displayed. Click the Radio Button for the desired program.

Table 7.2a: Channel Configuration Settings

Setting	Value	Description
Detect	Button (under decoder Number)	Use to read the PAT and PMT table of the entered multicast IP address and detect the SPTS or MPTS programs. First enter an IP address and port.
Address	IP Address	Specify the IP address of the multicast SPTS or MPTS which contains the program that is to be decoded.
Port	Integer	The IP port number associated with the multicast IP address above.
Program #	Integer	The MPEG number for the desired program in the multiplex. Can be filled manually or tick the radio button for a detected program in an MPTS.
Name	String	A name assigned for easier identification in the GUI. This name is not used or transmitted outside the UCrypt device and is not seen by the end user/viewer.
Channel	Drop down menu	Used to assign the RF frequency to each channel modulator. Depending on the model ordered, is either EIA/NTSC or one of several PAL plans.
Frequency	Integer	The UCrypt device may also be configured with a custom channel lineup by entering the video carrier frequency in this dialog box. The frequency is entered in MHz and may be specified to +/- 1 kHz, i.e. 175.251 MHz. Entering a number over-rides the **Channel** drop down menu.
Enable	Checkbox	Used to enable the RF output for the channel. Un-tick this box for each channel that is not required on the UCrypt device channel lineup, which disables the RF output for that channel.
Save	Button	Saves all changes made to this page before navigating to another page or closing the browser. If changes are made but not saved, the changes are not applied.
Detect	Button (Page Bottom)	Use to read the PAT and PMT table of all of the entered multicast IP addresses and detect the programs. First enter all the desired IP addresses. This action may take a lengthy time to conclude.

⚠ ***NOTE:*** *Clicking the **Save** button is service affecting. Services will be interrupted momentarily while the configuration is saved and applied.*

DEVICE STATUS TAB

8. Device Status Tab

8.1 Introduction

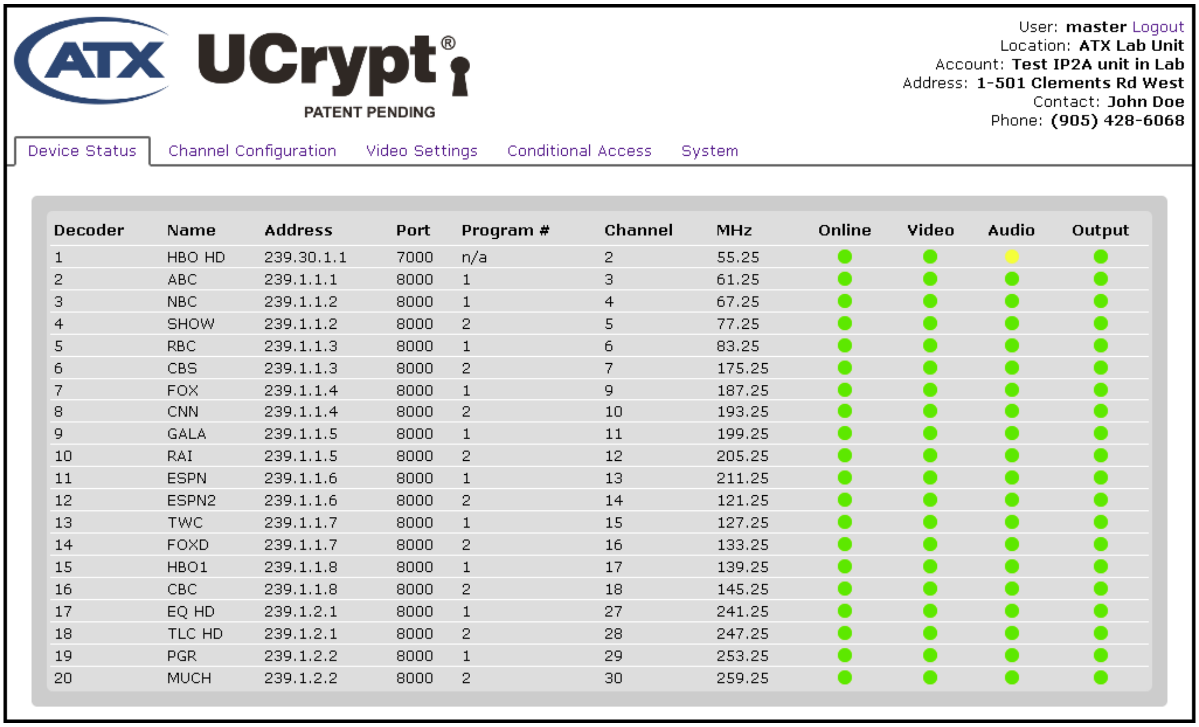
The ‘Device Status’ tab reports on the current UCrypt device configuration and the operational status of the 20 channel decoders. This page lists the IP address each decoder is subscribed to, the RF output channel of each and reports if the decoder is detecting video and audio programs on the IP address.

8.1.1 Status Indicator Lights

There are two possible states for the indicators:

- Green indicates that the channel is working or the program is detected.
- Yellow indicates that the channel is not working as expected or that there is no program detected.

If the channel is disabled on the Channel Configuration page, the entire line for that channel will be greyed out.



User: **master** Logout
Location: **ATX Lab Unit**
Account: **Test IP2A unit in Lab**
Address: **1-501 Clements Rd West**
Contact: **John Doe**
Phone: **(905) 428-6068**

Decoder	Name	Address	Port	Program #	Channel	MHz	Online	Video	Audio	Output
1	HBO HD	239.30.1.1	7000	n/a	2	55.25	🟢	🟢	🟡	🟢
2	ABC	239.1.1.1	8000	1	3	61.25	🟢	🟢	🟢	🟢
3	NBC	239.1.1.2	8000	1	4	67.25	🟢	🟢	🟢	🟢
4	SHOW	239.1.1.2	8000	2	5	77.25	🟢	🟢	🟢	🟢
5	RBC	239.1.1.3	8000	1	6	83.25	🟢	🟢	🟢	🟢
6	CBS	239.1.1.3	8000	2	7	175.25	🟢	🟢	🟢	🟢
7	FOX	239.1.1.4	8000	1	9	187.25	🟢	🟢	🟢	🟢
8	CNN	239.1.1.4	8000	2	10	193.25	🟢	🟢	🟢	🟢
9	GALA	239.1.1.5	8000	1	11	199.25	🟢	🟢	🟢	🟢
10	RAI	239.1.1.5	8000	2	12	205.25	🟢	🟢	🟢	🟢
11	ESPN	239.1.1.6	8000	1	13	211.25	🟢	🟢	🟢	🟢
12	ESPN2	239.1.1.6	8000	2	14	121.25	🟢	🟢	🟢	🟢
13	TWC	239.1.1.7	8000	1	15	127.25	🟢	🟢	🟢	🟢
14	FOXD	239.1.1.7	8000	2	16	133.25	🟢	🟢	🟢	🟢
15	HBO1	239.1.1.8	8000	1	17	139.25	🟢	🟢	🟢	🟢
16	CBC	239.1.1.8	8000	2	18	145.25	🟢	🟢	🟢	🟢
17	EQ HD	239.1.2.1	8000	1	27	241.25	🟢	🟢	🟢	🟢
18	TLC HD	239.1.2.1	8000	2	28	247.25	🟢	🟢	🟢	🟢
19	PGR	239.1.2.2	8000	1	29	253.25	🟢	🟢	🟢	🟢
20	MUCH	239.1.2.2	8000	2	30	259.25	🟢	🟢	🟢	🟢

Figure 8-1: Device Status Tab

Table 8.1a: Device Status

Setting	Value	Description
Decoder		The number identifying the decoder in the GUI.
Name		The name entered to identify the program in the GUI.
Address		The IP address of the multicast SPTS or MPTS which contains the program that is to be decoded.
Port		The IP port number associated with the multicast IP address above.
Program #		The MPEG number for the desired program in the multiplex.
Channel		The channel within the channel plan for this program which is either EIA/NTSC or one of several PAL plans.

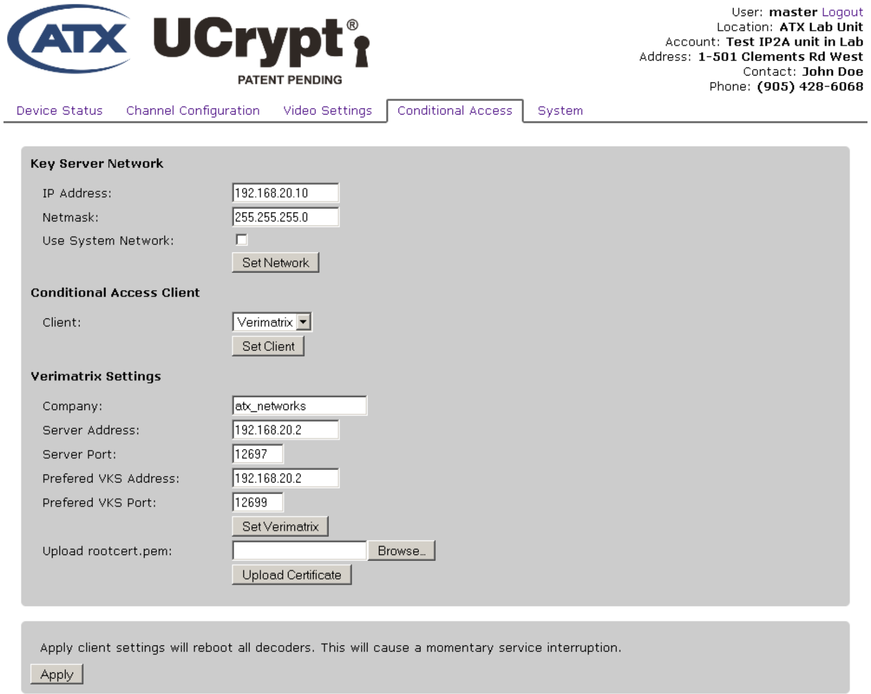
MHz		The frequency within the channel plan for this program.
Online	Green or Yellow	Reports on the health of the decoder. Green = Decoder is working normally. Yellow = Decoder is not working normally.
Video	Green or Yellow	Reports on whether a video signal is detected by the decoder. Green = Decoder detects video. Yellow = Decoder does not detect video. (This condition would be normal for an audio only program)
Audio	Green or Yellow	Reports on whether an audio signal is detected by the decoder. Green = Decoder detects audio. Yellow = Decoder does not detect video. (This condition would be normal for a video only program)
Output	Green or Yellow	Reports on the health of the Output Upconverter. Green = Output Upconverter is working normally. Yellow = Output Upconverter is not working normally.

CONDITIONAL ACCESS TAB

9. Conditional Access Tab - Configuration

9.1 Introduction

The UCrypt IP to Analog system is capable of decoding VeriMatrix DRM encrypted content. After the Verimatrix parameters are configured on this page, there is no further configuration for the content programs; if the program content is encrypted, it will automatically be decrypted.



User: **master**
Location: **ATX Lab Unit**
Account: **Test IP2A unit in Lab**
Address: **1-501 Clements Rd West**
Contact: **John Doe**
Phone: **(905) 428-6068**

Key Server Network

IP Address: 192.168.20.10
Netmask: 255.255.255.0
Use System Network: □

Conditional Access Client

Client: Verimatrix

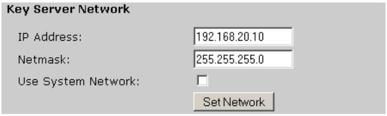
Verimatrix Settings

Company: atx_networks
Server Address: 192.168.20.2
Server Port: 12697
Prefered VKS Address: 192.168.20.2
Prefered VKS Port: 12699
Upload rootcert.pem:

Apply client settings will reboot all decoders. This will cause a momentary service interruption.

Figure 9-1: Conditional Access Page

9.2 Key Server Network



Key Server Network

IP Address: 192.168.20.10
Netmask: 255.255.255.0
Use System Network: □

Figure 9-2: Key Server Network Section

The UCrypt device rear panel physical 'MGMT Port' is shared between the Management Interface and the Verimatrix Key Server (VKS) network. Although a single physical port, each network (Management Interface and VKS) may have IP addresses assigned on differing subnets, each address being a virtual address on a virtual network. The tick box 'Use System Network' in this section determines if the two networks reside on the same or differing subnets. There are two scenarios:

- Tick the **Use System Network**

  If the VKS resides on the same subnet as the Management Interface such as a private network, then there is no need to specify a distinct network for VKS.

- Un-tick the **Use System Network**

  If the VKS resides on a different subnet as the Management Interface, i.e. the VKS is on a private network and the Management Interface is public, then specify a distinct network for VKS.

9.2.1 IP Address:

This is the virtual IP address assigned to the Verimatrix DRM Key Server access network port. This address needs to be in the same subnet as the VKS.

9.2.2 Netmask:

This is the associated subnet mask for the Key Server Network virtual IP address assigned above.

9.2.3 Use System Network:

- Tick the **Use System Network** box

If the VKS resides on the same subnet as the Management Interface, such as a private network, then there is no need to specify a distinct network for VKS and this will cause both virtual interfaces to use the Management Interface subnet. This subnet was set on "5.8 Network" on page 5-5.

- Un-tick the **Use System Network** box

If the VKS resides on a different subnet as the Management Interface, i.e. the VKS is on a private network and the Management Interface is public, then specify a distinct IP Address for the VKS virtual interface in "9.2.1 IP Address:".

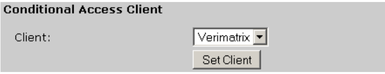
9.2.4 Set Network Button

See Figure 9-2 for button location. Any changes made to the network settings above require clicking the **Set Network** button to save and apply changes. Navigating away from this page before saving the settings will result in changes being discarded.

9.3 Conditional Access Client

9.3.1 Client:

This drop down menu is used to select multiple encryption clients. Currently, select Verimatrix as the encryption client. If a change is made, click **Set Client** to save this change. Navigating away from this page before saving the settings will result in changes being discarded.



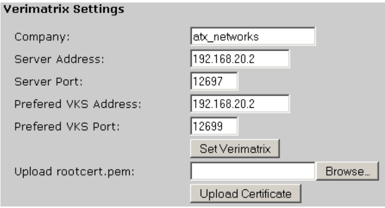
Conditional Access Client

Client: Verimatrix

Figure 9-3: Conditional Access Client Section

9.4 Verimatrix® Settings

These settings need to correspond to the values assigned by Verimatrix.



Verimatrix Settings

Company: atx_networks

Server Address: 192.168.20.2

Server Port: 12697

Prefered VKS Address: 192.168.20.2

Prefered VKS Port: 12699

Upload rootcert.pem:

Figure 9-4: Verimatrix Settings Section

Table 9.4a: Verimatrix Settings

Setting	Value	Description
Company	String	Enter the company name assigned by Verimatrix here.
Server Address	IP Address	The IP address of the Verimatrix DRM server.
Server Port	Integer	The IP port of the Verimatrix DRM server associated with the 'Server Address' above.
Preferred VKS Address	IP Address	The IP address of the preferred Verimatrix Key Server.
Preferred VKS Port	Integer	The IP port of the Verimatrix Key server associated with the 'Preferred VKS Address' above.
Set Verimatrix	Button	Click to apply the above settings
Upload rootcert.pem	Folder	This dialog is populated with the folder location of the rootcert.pem file.
Browse	Button	Click to browse to the location of the rootcert.pem file on your computer or network. The dialog is filled with the location after selection.
Upload Certificate	Button	Click to upload the rootcert.pem file after pointing to it with the dialog above.

9.5 Apply Button

See Figure 9-1 for button location. If changes are made to this page, click the **Apply** button to save and apply all the changes.

⚠ ***NOTE:*** *Clicking the **Save** button is service affecting. Services will be interrupted momentarily while the configuration is saved and applied.*

UPDATING FIRMWARE

10. Updating Firmware

10.1 Introduction

New system software for the UCrypt device is provided in a compressed Zip file format. It is not necessary for an operator to un-compress the package. The unit has built-in facilities to accept the file in exactly the format that is downloaded. Get the file from the ATX support web site.

Problems that are encountered during an update should be referred to ATX support. See ”Contact ATX Networks” on page 12-1 for ways to contact a technical support specialist.

A brief summary of a firmware update is shown here. As firmware releases may vary over time and the exact procedure may also vary, it is best to refer to the ATX support web site for up to date information on updating firmware. A written instruction sheet may be downloaded from the same web page where the firmware update file is found.

10.2 Installing Updated System Software

Coming Soon

This page intentionally left blank

SPECIFICATIONS

11. Specifications

SPECIFICATIONS		
INPUT		
ETHERNET		IEEE 802.3-2002,1000BASE-T (GbE)
CONNECTORS		2x RJ45; Chassis Rear
TRANSPORT STREAM/LAYER PROTOCOL		SPTS, MPTS over UDP
MULTICAST PROTOCOL SUPPORT		IPv4 Multicast, IGMP v1, 2
SUPPORTED VIDEO FORMATS		MPEG-2 MP@HL. MPEG-4 pt10 AVC/H.264 HP@L4
SUPPORTED VIDEO RESOLUTIONS		Up to 720p & 1080i
SUPPORTED AUDIO FORMATS		Dolby® Digital (AC-3), MPEG-1 L1/2/3, AAC, AAC (HE)
REDUNDANCY		Dual input multicasts per program
TS PROCESSING		
DECODING		Supports Decoding of up to 20 Streams per Chassis
DECRYPTION		Supports Decryption of up to 20 Verimatrix Encrypted Programs
ADDITIONAL PROCESSING CAPABILITIES		Closed Captioning, VBI Insertion, Teletext, DVB® Subtitles
SUPPORTED ASPECT RATIOS		4:3, 16:9
OUTPUT		
RF		Up to 20 Modulated Channels
SUPPORTED MODES		NTSC, PAL B/G, PAL D/K
FREQUENCY RANGE		54-750 MHz (EIA ch2-116)[1]
FREQUENCY PLANS		STD, HRC, IRC & Custom Offsets
OUTPUT LEVEL & FLATNESS		35 dBmV +/- 2 dB per Analog Carrier
SIGNAL-TO-NOISE RATIO (SNR)		54 dB (min)
CARRIER-TO-NOISE RATIO (CNR)		54 dB (min)
COMP. TR. BT. (CTB)		-65 dBc
COMP. 2nd ORD. (CSO)		-65 dBc
OUTPUT RETURN LOSS		18 dB (min)
VIDEO CARRIER FREQUENCY STABILITY		± 3ppm
AUDIO CARRIER FREQUENCY STABILITY		± 5ppm
DEMODULATED VIDEO	DIFFERENTIAL GAIN	≤ 5%
	GROUP DELAY VARIATIONS	≤ 100nS
	2TK FACTOR	≤ 2%
OUTPUT VIDEO ASPECT RATIOS		4:3, 16:9
AUDIO OUTPUT FORMAT		Mono
CONNECTOR		F Connector; Chassis Rear
RF OUTPUT TEST		-20 dB Relative to Output; F Connector, Chassis Rear
DEVICE MANAGEMENT		
MANAGEMENT INTERFACE		Local or Remote Management via Integrated Secure Web Server or Central Management Server
MANAGEMENT INTERFACE PORT		1000BASE-T(GbE), Static IP or DHCP, RJ45, Chassis Rear
MANAGEMENT SECURITY		3 Password Protected Tiered User Accounts
MASS DEPLOYMENT & BACKUP		Importable/Exportable Device Configuration Files
REMOTE MONITORING		Integrated SNMP Agent & MIB
ALARMS		SNMP Traps, GUI LED Indication
EAS		
EAS SUPPORT		Supports Processing IP Mulitcast-based SCTE 18 Standard Messages
PHYSICAL & ENVIRONMENTAL		
FORM FACTOR		3RU, 19” Rack Mount
DIMENSIONS		5.25”H x 19.0”W x 22.8”D (13.34H x 48.26W x 57.91D cm)
WEIGHT (Max)		52.0 lbs (23.6 kg)
POWERING		Redundant 110/220 VAC or -48 VDC Options, 400W (max)
SAFETY APPROVALS		cULus & FCC Title 47 Part 15 (class A)
POWER CONTROL		Rear Panel ON/OFF Switch & Software-based Power Control
OPERATING TEMPERATURE		0ºC to +40ºC[2] (+32ºF to +104ºF)
HUMIDITY		0-95% Non-condensing

NOTES:

(1) Supports output frequencies up to 750 MHz, however specs above may only apply up to 650 MHz.

(2) For details on exceeding +30ºC, please refer to the UCrypt Environment & Temperature Considerations Info Sheet (#ANW1066).

Dolby is a registered trademark of Dolby Laboratories. Manufactured under license from Dolby Laboratories.

This page intentionally left blank.

SERVICE & SUPPORT

12. Service & Support

12.1 Contact ATX Networks

Please contact ATX Technical Support for assistance with any ATX products. Please contact ATX Customer Service 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 the factory.

Digital Video Products
(DVIS, DigiVu, UCrypt, VersAtivePro)

TECHNICAL SUPPORT

Tel:	(905) 428-6068 – press *3 then press 1
Toll Free:	(800) 565-7488 – press *3 then press 1 (USA & Canada only)
Email:	digitalvideosupport@atxnetworks.com

CUSTOMER SERVICE
ATX Networks
1-501 Clements Road West
Ajax, ON L1S 7H4 Canada

Tel:	(905) 428-6068
Toll Free:	(800) 565-7488 (USA & Canada only)

► Press *1 for **Customer Service**

Fax:	(905) 427-1964
Toll Free Fax:	(866) 427-1964 (USA & Canada only)
Email:	support@atxnetworks.com
Web:	www.atxnetworks.com

12.2 Warranty Information

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

1-501 Clements Road West, Ajax, ON L1S 7H4 Canada
Tel +1 (905) 428-6068   Toll Free +1 (800) 565-7488
Fax +1 (905) 427-1964   Toll Free Fax +1 (866) 427-1964
www.atxnetworks.com   support@atxnetworks.com