UCrypt®

Patent Pending

UCrypt® Cable Gateways Monitoring Server

OPERATION MANUAL

General Guide Notes

Document Name	**UCrypt Monitoring Server - Operation Manual**
Document Number	**ANW1175**
Release Date	**July 31 2018**

Firmware Version

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

Version	**1.1**

Organization of This Manual

This manual is generally organized based on the main functions of Encoding and Transcoding with individual chapters dedicated to describing the configurable features and monitoring. Further chapters outline activities related to the GUI operation and configuration.

Cross Reference Usage

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

Symbol Usage

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

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

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

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® 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. Adobe® Flash®, and other non-ATX product and company names mentioned in this document are the property of their respective companies.

TABLE OF CONTENTS

QUICK START

1. Quick Start

The UCrypt Monitoring Server is a software package only and may be installed on a PC or a virtual machine. Access to the GUI (Graphical User Interface) is through a secure web interface using any web browser installed on the Management Computer. The Ethernet port of the Management Computer must have network access to the UCrypt Monitoring Server and the Monitoring Server must have network access to all remote monitored Devices. In this manual and the Monitoring Server GUI the UCrypt, DVIS and DigiVu Devices to be remotely monitored may also be referred to as **Servers**.

1.1 Chapter Contents

This chapter covers the initial log in, a description of some basic features of the GUI and addition of a single emote Device to the Monitoring Server. Further configuration instruction may be found in the other chapters of this manual which are based on the tabs of the Monitoring Server GUI.

1.2 Firewall Open Ports Required

The Monitoring Server uses a number of IP ports to allow communications with a remote management computer's browser. and remotely monitored Devices The following ports will need to be opened in any firewall that could block this communication.

Table 1.2a: Firewall Open IP Ports Required

IP Port Number	Protocol
80, 443	HTTP, HTTPS for GUI
161, 162	SNMP
22	SSH
10514	System logs from UCrypt to Monitor Server
Your currently used port for this service.	TACACS+
Your currently used port for this service.	SMTP Mail server

1.3 Launch the GUI & Log In

1. Open the web browser of your choice or a new browser tab, Figure 1-1.
2. Enter the IP address of the Monitoring Server; factory default is **192.168.0.23**

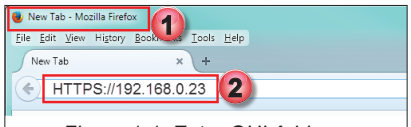

Figure 1-1: Enter GUI Address

3. Upon the first time logging in with a specific browser, you will receive a security warning that the web site's security certificate is unknown, Figure 1-2. This is because the security certificate is self signed and is a normal browser response. This is not a security threat. Accept the security warning. This will be presented in differing ways depending on the specific browser being used.

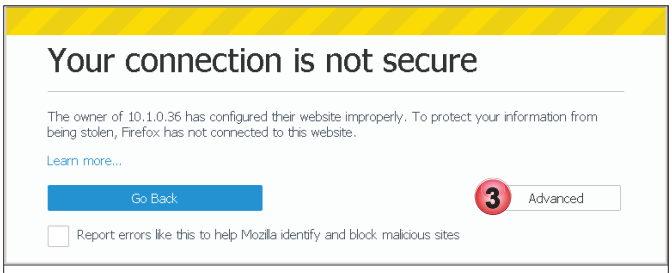

Figure 1-2: Insecure Connection warning

4. Login with credentials, Figure 1-3, (case sensitive): User Name: **admin**
   Password: **atx_monitoring_admin_password**

Figure 1-3: GUI Login

The GUI will open as shown in Figure 1-4.

NOTE: *If you will be enabling TACACS+ authentication, it is possible to disable this local authentication method.*

1.4 The Monitoring Server GUI

The Server GUI is based on the familiar **UCrypt Device Tabbed Interface**, Figure 1-4. The main configuration tabs and some of the Status Page features are:

1. **Status** Tab - The default page showing configured emote Devices and overview of the status of all installed Devices.
2. **Events** Tab - Alarm events for all configured remote Devices.
3. **Profiles** Tab - The profiles which define the parameters being monitored for individual or groups of remote Devices.
4. **System** Tab - Global configuration of the Monitoring Server.
5. **Add Servers** - Button to add new remote monitored Devices.
6. **The List** of added monitored Devices (None configured yet in this example).

Other Status Page features and configuration controls are described in detail in the chapter “STATUS TAB” on page 2-1.

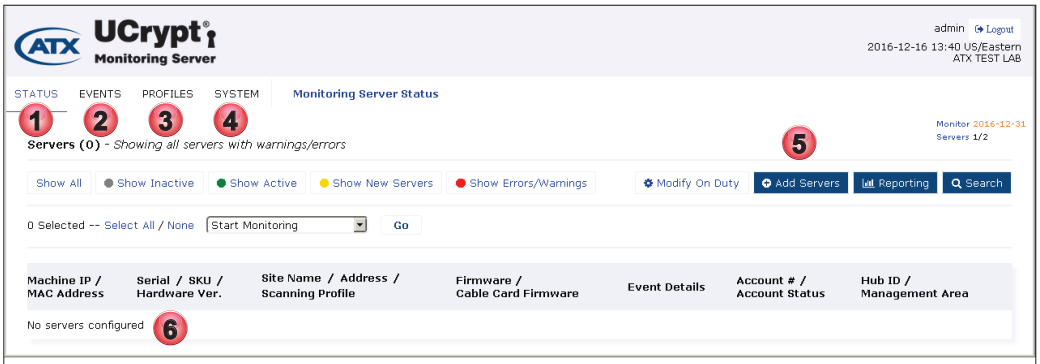

Figure 1-4: The UCrypt Monitoring Server GUI

1.5 Network Configuration

By default, the IP address of the Monitoring Server is 192.168.0.23 so before you are able to connect to emote Devices in your network, the Ethernet Network port configuration must be changed to reside on your network.

Procedure

The procedure to change network settings is described in section “5.2 Network Configuration” on page 5-2.

1.6 Add and Monitor a Remote UCrypt Device

Remote Devices must be added to the Monitoring Server with one of two possible methods. Here we show the quick way to add one or a few Devices from the Status Page. The other method involves importing a CSV file which is intended for importing a large number of remote Devices, see “5.17 Data Management” on page 5-23.

Procedure

This procedure explains how to add a UCrypt Device to the Monitoring Server. The procedure is the same for all Devices.

1. Click the **Status** tab to select it if it isn’t already selected, Figure 1-5.
2. Click the Add Servers **+ Add Servers** button.

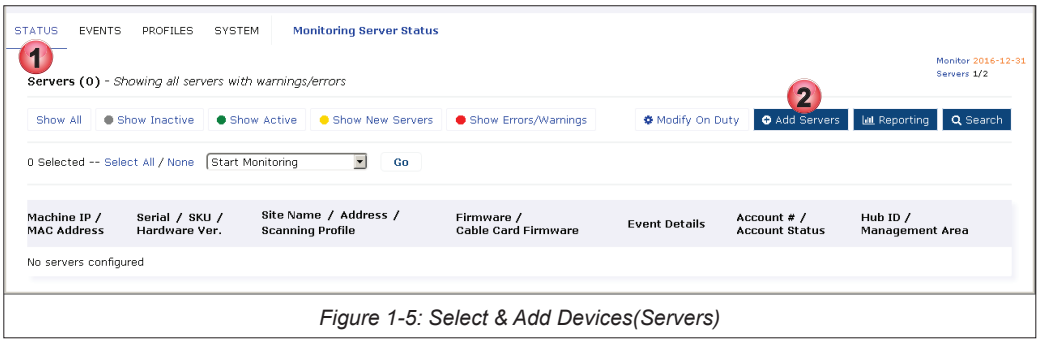

Figure 1-5: Select & Add Devices(Servers)

3. Enter the IP address of the Remote Device, separated with commas if there is more than one, Figure 1-6.
4. Click the **Add Servers** button.

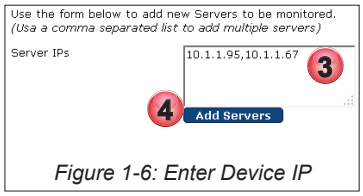

Figure 1-6: Enter Device IP

5. A confirmation dialog is presented, Figure 1-7.
6. Click **Back to Status page**. (You may also add more Devices from this page by clicking **+Add/Import more Servers**.)

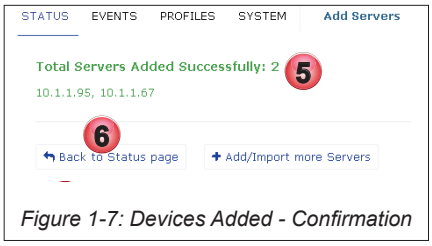

Figure 1-7: Devices Added - Confirmation

7. Upon return to the Status Page, new servers are added to the monitoring list, Figure 1-8. New servers which are added but not configured yet are shown with yellow background for easy identification.

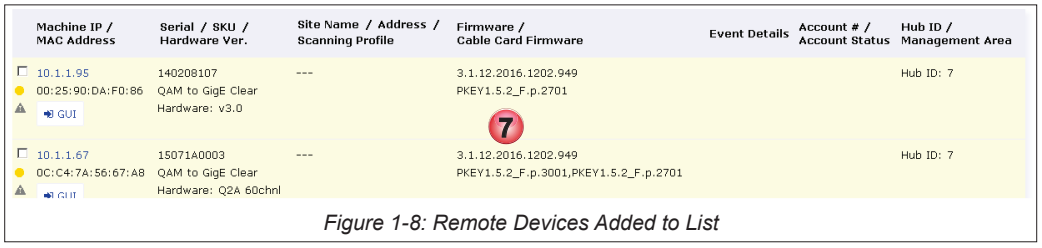

Figure 1-8: Remote Devices Added to List

8. To start to monitor a UCrypt Server that was added, click the tick box for that server, Figure 1-9 If multiple servers have been added, multiple servers may be started at the same time by clicking all applicable tick boxes for those servers.

NOTE: *Before being able to monitor a UCrypt Device, the Master password of the remote Device must match the password for that Device that the Monitoring Server has been set to. By default, the Monitoring Server will use the Device Default Master Password (atx_ucrypt_master_password). It is not good practice to leave default passwords set on remote equipment so it is strongly suggested to change remote access default passwords.*

9. If the remote UCrypt Device has a password different than the default password *(atx_ucrypt_master_password)*,

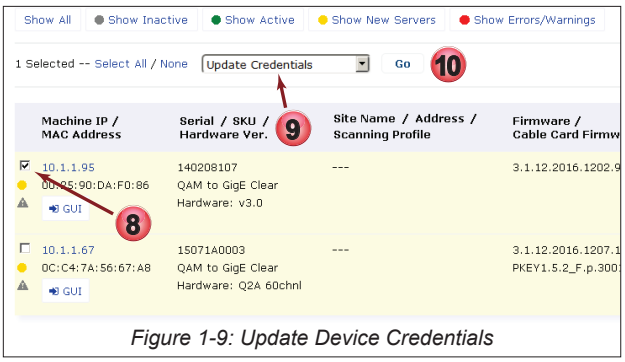

Figure 1-9: Update Device Credentials

select the control instruction **Update Credentials** from the drop down menu.

10. Click the **Go** Go button.
11. In the dialog, enter the correct **Master Password** for this UCrypt Device, Figure 1-10.
12. Click **Save**.

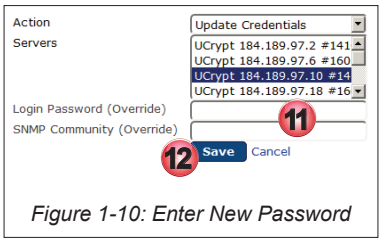

Figure 1-10: Enter New Password

13. Now, ensure that the control instruction **Start Monitoring** is selected from the drop down menu (this is the default setting).
14. Click the **Go** Go button.

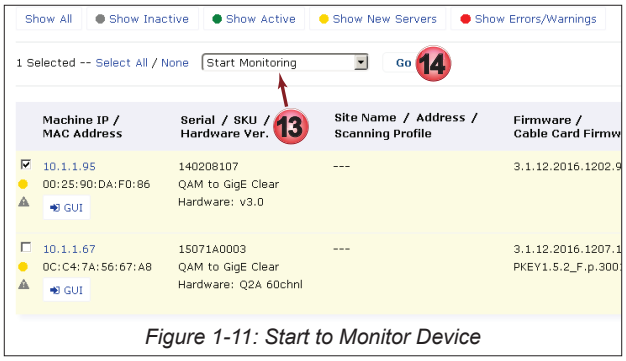

Figure 1-11: Start to Monitor Device

15. In the next dialog, select the **Default Profile**(or other defined profile) from the drop down menu, Figure 1-12. The profile defines the SNMP triggers that are monitored and reported. The default profile includes all possible parameters to be monitored. (See "4.2 Create or Edit a Profile" on page 4-1 to create a new or custom profile).
16. Click **Go**.

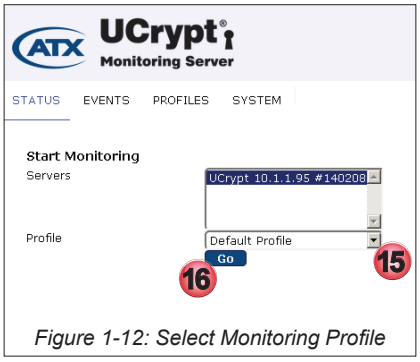

Figure 1-12: Select Monitoring Profile

17. The confirmation of starting the remote Device monitoring process is confirmed, Figure 1-13. Click the link **Back to Status Page** to return to the Status page.

Figure 1-13: Return Back to the Status Page

18. The **Monitoring Status** icons will initially be green on monitored servers, Figure 1-14. They could soon turn to red if alerts are received.
19. This server is being monitored for the parameters listed in the **Default Profile** that was selected. If the monitoring profile is eventually changed, this link will change to reflect the new selection. Clicking on this link allows editing of the profile. If the profile later needs to be changed, the monitoring process must first be stopped for that Device then restarted.

NOTE: *If you make changes to the current profile for any device you will need to re-start the monitoring process for those changes to take effect.*

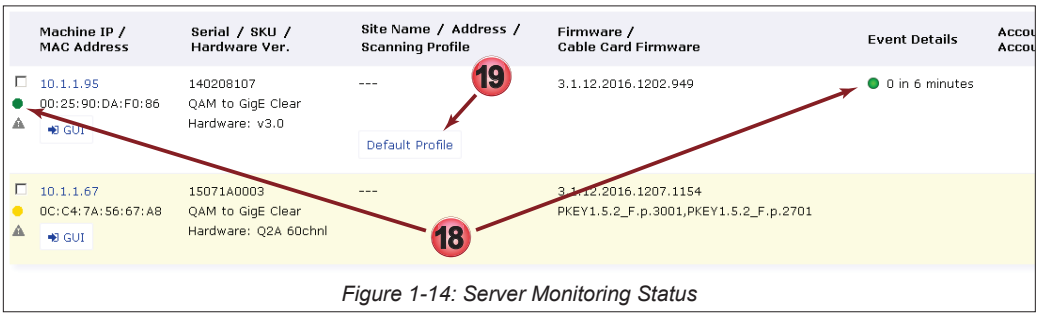

Figure 1-14: Server Monitoring Status

1.7 Delete a Remotely Monitored Device

Remote monitored Devices may be deleted from the Monitoring Server individually or as a group.

Procedure

This procedure explains how to delete Devices from the Monitoring Server.

1. Click the **Status** tab if it isn't already selected, Figure 1-15.
2. Click the **selection tick boxes** for any Devices to be deleted. One or several may be selected for group deletion.
3. From the drop down control menu, select **Delete**.
4. Click the **Go** Go button.

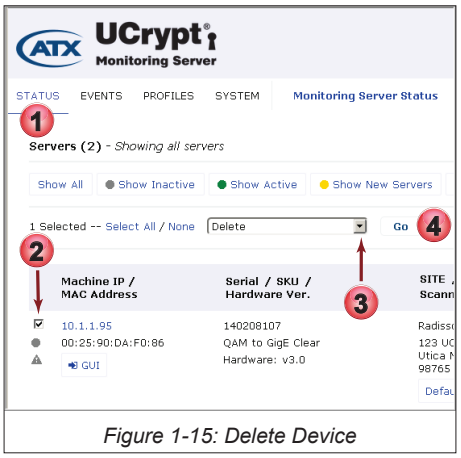

Figure 1-15: Delete Device

5. A confirmation dialog is presented, showing the server IP address and serial number to be deleted, Figure 1-16.
6. Click **Save**.

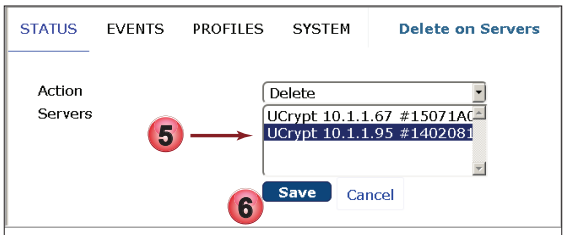

Figure 1-16: Servers for Deletion

7. The Status Page shows a confirmation that the object was deleted, Figure 1-17.

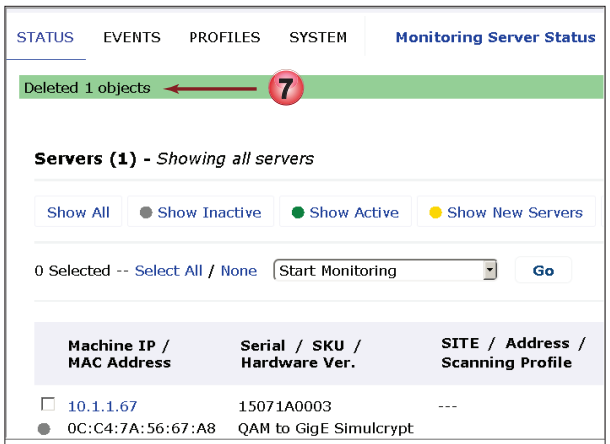

Figure 1-17: Confirmation of Servers Deleted

1.8 Next Steps in Configuration

Further detailed configuration and procedures may be found in the following locations:

Monitoring Server Global settings: "SYSTEM TAB" on page 5-1

Monitored Remote Devices configuration: "STATUS TAB" on page 2-1

Creating and Editing Monitoring Profiles "PROFILES TAB" on page 4-1

This page left intentionally blank.

STATUS TAB

2. Status Tab

The Status Page is the main page of the UCrypt Monitoring Server showing, at a glance, a list of all added Devices and their running status if they are currently being monitored. All management of UCrypt, DVIS and DigiVu Devices is initiated from this page.

***Note** for DVIS Devices only: If an encoder card is installed or removed this change will not be reflected automatically in the Monitoring Server GUI. In order to register this change the affected Device needs to be removed from the Monitoring Server, then re-added. DVIS Devices are not constantly polled for changes in hardware. Re-Identify will not work for this as it does not poll for this type of hardware change.*

2.1 Chapter Contents

This chapter covers the features and functions found on, or initiated from, the Status Page.

2.2 Status Page in Detail

There are our main areas of the Status Page, Figure 2-1.

1. Server(Monitored Device) Display List Filters
   Controls to display the list of monitored UCrypt, DVIS or DigiVu Devices.
2. List of monitored UCrypt Devices.
   The list of added or monitored Devices depending on Display List Filter selection.

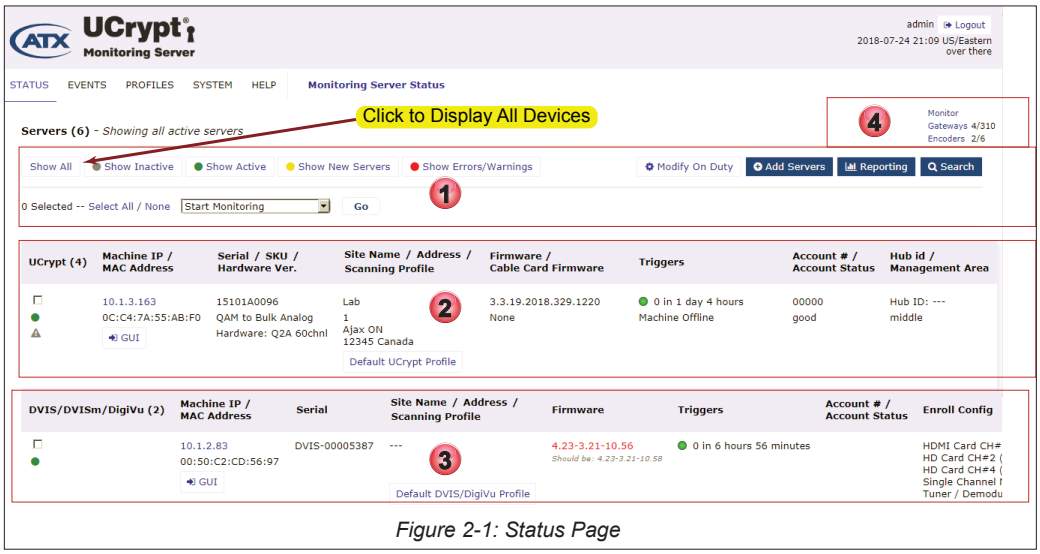

Figure 2-1: Status Page

3. List of monitored DVIS or DigiVu Devices.

The list of added or monitored Devices depending on Display List Filter selection.

4. Monitoring Server licenced number of monitored Devices.

   The number of currently monitored Gateways(UCrypt Cable Gateway) and Encoders is indicated along with the licenced limit.

2.3 Device Filter Panel

The Device Display Filter section, Figure 2-2, allows displaying filtered lists of remote UCrypt, DVIS and DigiVu Devices in different formats based on their current status as well as starting the monitoring process, stopping the monitoring process and other functions related to the monitored Devices.

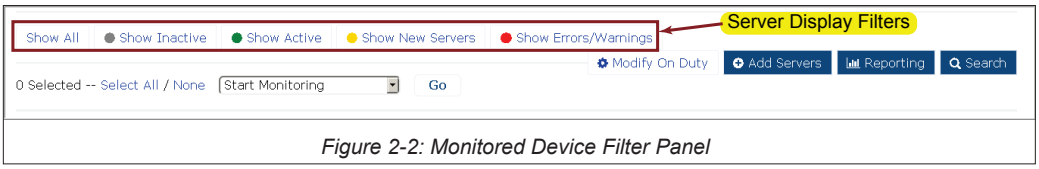

Figure 2-2: Monitored Device Filter Panel

2.3.1 Device List Filters

These buttons control which remote Devices are displayed on the Status Page. These are clickable filters, Figure 2-3, which selectively display in the list, remote Devices based on their monitored status as described below. The colored indicator associated with the filter (Grey, Green, Yellow, Red) indicates that the monitored Device with a corresponding indicator will be displayed by clicking the appropriate filter selection.

Figure 2-3: Show Device Filters

- **Show all**

  Shows all UCrypt Devices that have been added to the Monitoring Server.

- **Show Inactive**

  Shows all remote Devices with a status indicator of **Grey**. These are Devices that have been monitored at least once but are not currently being monitored.

- **Show Active**

  Shows all remote Devices with a status indicator of **Green**. These are Devices that are being actively monitored and have no unacknowledged Alerts.

- **Show New Servers**

  Shows all remote Devices with a status indicator of **Yellow**. These are newly added Devices that have never had monitoring started. These newly added devices will also have a background color of yellow to make them more easily identifiable. Once monitoring has been started then stopped, the indicator for that machine will be grey.

- **Show Errors/Warnings**

  Shows all remote Devices with a status indicator of **Red**. These are Devices that have current Alerts that have not been acknowledged.

2.3.2 Assign the 'On Duty' Technician

It is possible to very easily specify or change which on call technician will receive email notifications of remote Device Alerts from a specific Monitoring Server. The **Modify on Duty** button, Figure 2-4, opens a dialog, Figure 2-5, which allows any user

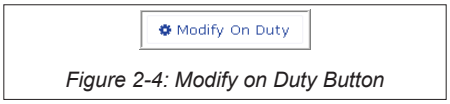

Figure 2-4: Modify on Duty Button

that has been added to the Monitoring Server by LDAP to be specified to receive notification emails if the email feature has been set up (to set up the email alerts, see "5.14 Email Alerts" on page 5-19). The On Duty user's name will also be listed in reports of intervention. Once set up, the 'On Duty' tech will receive emails for triggers with **on_duty** specified for email alerts (to specify the on_duty technician as the email recipient, see "4.4 Configure Email Notifications" on page 4-3).

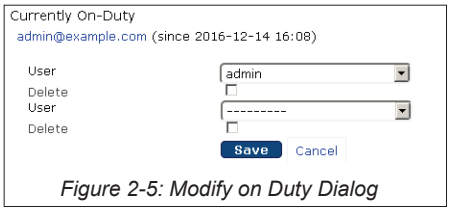

Figure 2-5: Modify on Duty Dialog

2.3.3 Status Page Tools

These clickable controls, Figure 2-6, add new remote Devices and add specific functionality to the Status page.

Figure 2-6: Status Page Tools

Add Servers

Click **+ Add Servers**  to add new remote Devices to the Monitoring Server, Figure 2-7. This is one way to add individual Devices or a small number of Devices but it is possible to import a .csv file to add many Devices at one time (to import a .csv file see "5.17.1 Import/Export Server Records" on page 5-23). Adding individual Devices is described in "1.6 Add and Monitor a Remote UCrypt Device" on page 1-3.

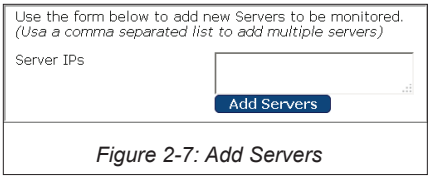

Figure 2-7: Add Servers

Reporting

Click **Reporting**  to add reporting generation controls to the Status page, Figure 2-8, which makes it possible to create a report of remote Device alerts and interventions activity between any two dates.

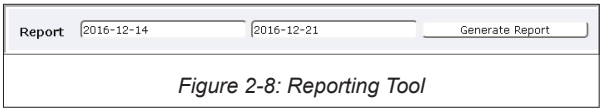

Figure 2-8: Reporting Tool

Search

Click **Search** Search to add search capabilities to the Status page, Figure 2-9, which make it possible to manipulate which remote Devices are displayed based on the chosen search criteria. This search criteria is presented in the form of a filter which may be easily deleted when finished with the search. Multiple search criteria filters may be simultaneously applied.

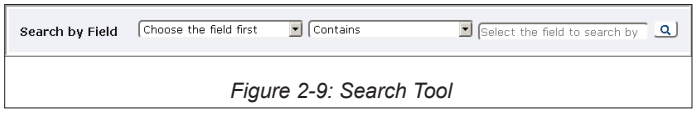

Figure 2-9: Search Tool

2.3.4 Server Monitoring Control

This multifunction control, shown in Figure 2-10, performs a number of manipulations related to the remote Devices. By clicking the down arrow a menu allows selection of Device functions as described below. The user also needs to select the target Device for the action by clicking their individual tick boxes or click **Select All** (or **None** to first deselect all) then click the **Go** button.

Figure 2-10: UCrypt Server Control

- **Start Monitoring**

  Starts the monitoring process for selected remote Devices.
- **Stop Monitoring**

  Stops the monitoring process for selected remote Devices.
- **Re-Identify**

  Queries the selected remote Devices for their identification parameters. This may be necessary if a remote Ucrypt Device for example, has been modified or had functionality added or removed ie. CableCARDs.
- **Delete**

  Deletes the selected remote Devices from the Monitoring Server.
- **Update Credentials**

  Updating Credentials is required for any UCrypt Device when the **Master** password on the physical unit as been changed. This feature allows the automatic login process to complete with the new Master password. This only updates credentials saved in the Monitoring Server, after the actual physical Device credentials have been updated first. Each monitored Device has a **GUI** link GUI which opens a browser page and logs in to the monitored Device to allow that Master password update on the remote Device.

2.3.5 Start Monitoring

After adding remote Devices, the monitoring process must be started for that Device. This process sets up the communications protocols between the remote Devices and the Monitoring Server.

Procedure

This procedure describes the steps required to start the monitoring process for one or more remote Devices.

1. Click the **Status Tab** if it is not already selected, Figure 2-11.
2. Tick the **selection tick box** of any remote Devices that will have monitoring started.
3. Verify the control selector is set to **Start Monitoring** (the default setting).
4. Click the **Go** button.

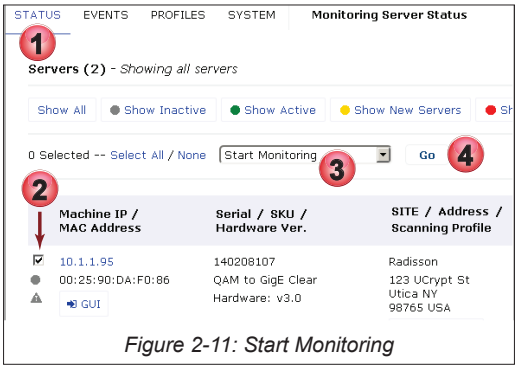

Figure 2-11: Start Monitoring

5. Use the **Profile** dropdown menu, Figure 2-12, to select the **Monitoring Profile** to be applied to this Device (or group of Devices if more than one was selected). There are default Profiles available for each type of Device; UCrypt, DVIS, DigiVu and you may create your own custom profiles for each Device type to select from.
6. Click the **Go** button.

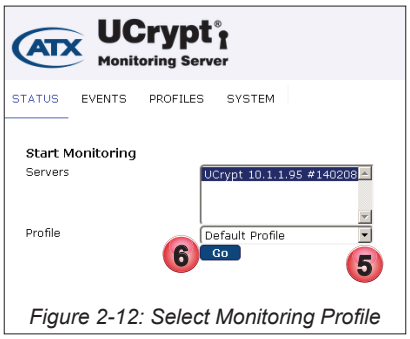

Figure 2-12: Select Monitoring Profile

7. A message indicating success is displayed, Figure 2-13. Click **Back to Status page** to return to the Status page.

Figure 2-13: Back to Status Page

2.3.6 Stop Monitoring

To remove remote Devices from the Monitoring Server, monitoring must be stopped on those Devices. This process shuts down communications between the remote Devices and the Monitoring Server.

Procedure

This procedure describes the steps required to stop the monitoring process for one or more remote Devices.

1. Click the **Status Tab** if it is not already selected, Figure 2-14.
2. Tick the **selection tick box** of any remote Devices that will have monitoring stopped.
3. Select **Stop Monitoring** from the control dropdown menu.
4. Click the **Go** button.

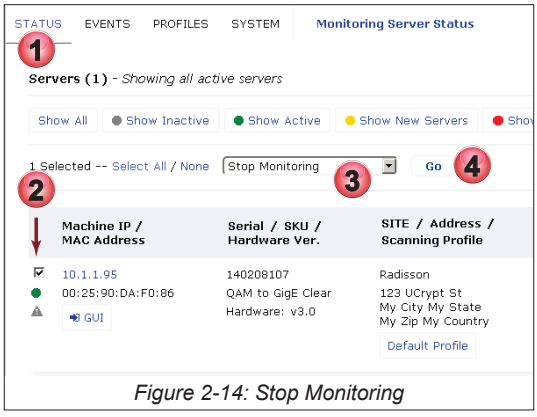

Figure 2-14: Stop Monitoring

5. Verify that the correct remote Device or group of Devices is listed for monitoring to be stopped, Figure 2-15.
6. Click the **Go** button.

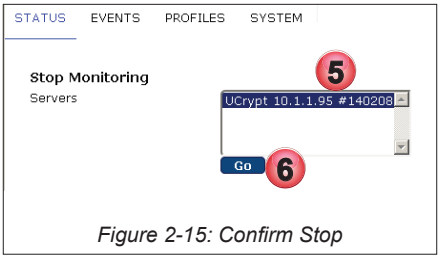

Figure 2-15: Confirm Stop

7. A message indicating success is displayed, Figure 2-16. Click **Back to Status page** to return to the Status page.

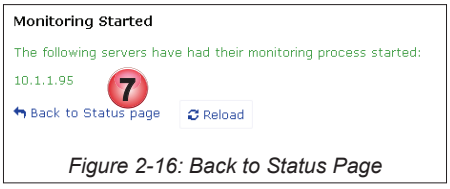

Figure 2-16: Back to Status Page

2.3.7 Re-Identify

This control queries the selected remote Devices for all of their monitored identification parameters such as Firmware, Serial, SKU, capabilities etc. This may be necessary if a UCrypt Device for example, has been modified or had functionality added or removed ie. CableCARDs or firmware updated.

Procedure

This procedure describes the steps required to Re-identify one or more remote Devices.

1. Click the **Status Tab** if it is not already selected, Figure 2-17.
2. Tick the **selection box** of any remote Devices that need to be Re-identified.
3. Use the drop down menu to select **Re-Identify**.
4. Click the **Go** button.

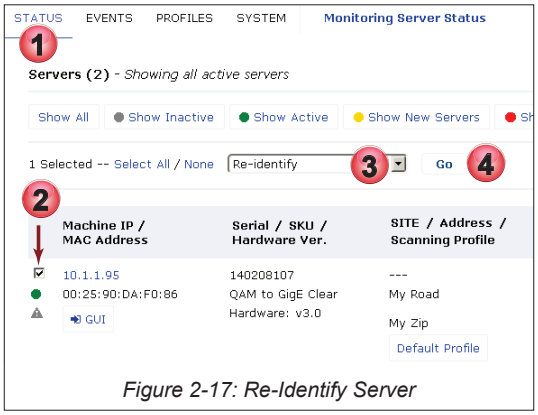

Figure 2-17: Re-Identify Server

5. Verify that the correct Device is being Re-Identified, Figure 2-18.
6. Click the **Go** button.

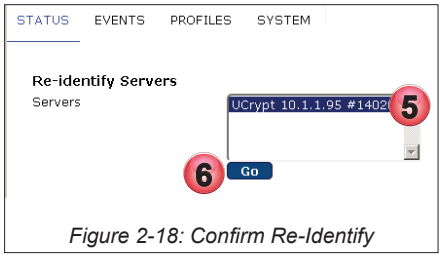

Figure 2-18: Confirm Re-Identify

7. A message indicating success is displayed, Figure 2-19. Click **Back to Status page** to return to the Status page.

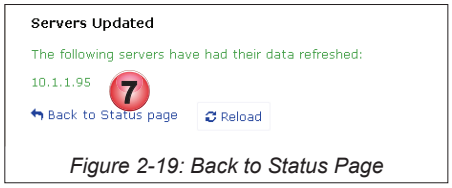

Figure 2-19: Back to Status Page

2.3.8 Delete Monitored Device

Deletes the selected remote Device from the Monitoring Server if it no longer needs to be monitored.

Procedure

This procedure describes the steps required to delete one or more remote Devices.

1. Click the **Status Tab** if it is not already selected, Figure 2-20.
2. Tick the **selection box** of any remote Devices that will be deleted.
3. Use the dropdown menu to select **Delete**.
4. Click the **Go** button.

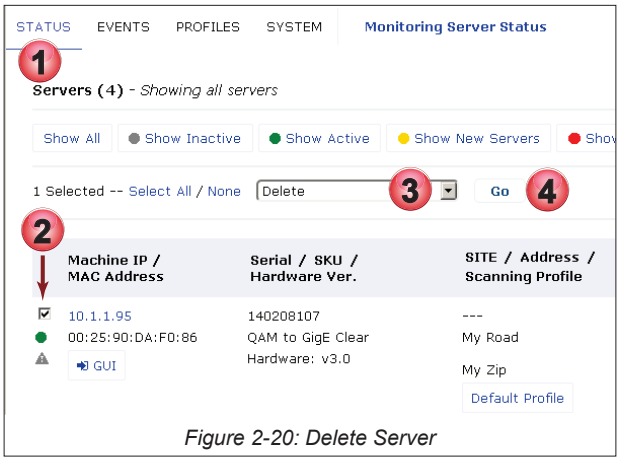

Figure 2-20: Delete Server

5. The Device to be deleted is highlighted but more can be highlighted from this dialog, Figure 2-21
6. Click the **Save** button.

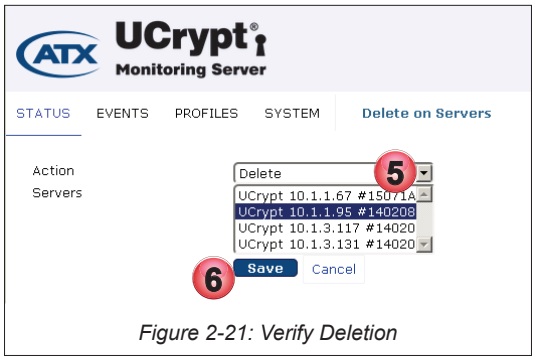

Figure 2-21: Verify Deletion

7. A message indicating success is displayed, Figure 2-22.

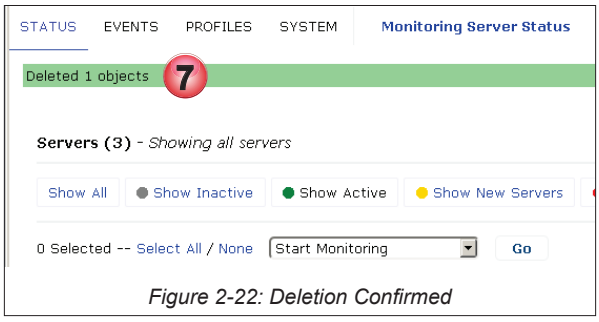

Figure 2-22: Deletion Confirmed

2.3.9 Update UCrypt Login Credentials

Updating Credentials is required for any UCrypt Device if the monitored Device **Master** user password is changed. Each monitored Device has a GUI link which automatically opens a browser page and logs in to the monitored UCrypt Device. Updating Credentials allows the automatic login process to complete after a password change. The Master password for the actual UCrypt Device must be done within the UCrypt Device GUI as always. The Monitoring Server does not itself update the remote UCrypt Device passwords.

Procedure

This procedure describes the steps required to Update Credentials on one or more UCrypt Devices.

1. Click the **Status Tab** if it is not already selected, Figure 2-23.
2. Click one of the **Server Filter** selections as appropriate to show the Device that you are working with.
3. Tick the **selection box** of any UCrypt Devices that will have its credentials updated.
4. Use the dropdown menu to select **Update Credentials**.
5. Click the **Go** button.

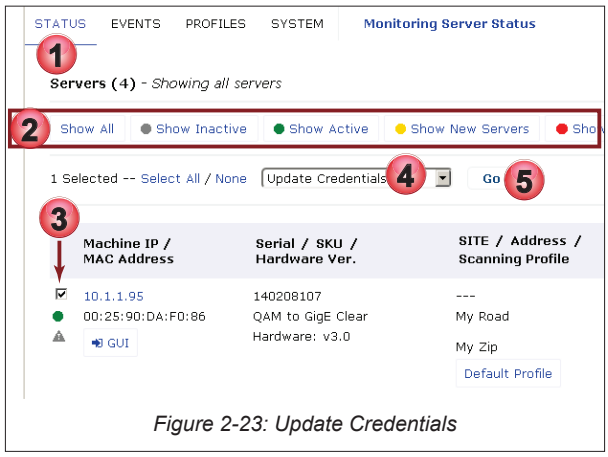

Figure 2-23: Update Credentials

6. The appropriate Device will be highlighted. Enter the new **Master account** password and, only if the SNMP community changed, enter it as well, Figure 2-24.
7. Click the **Save** button.

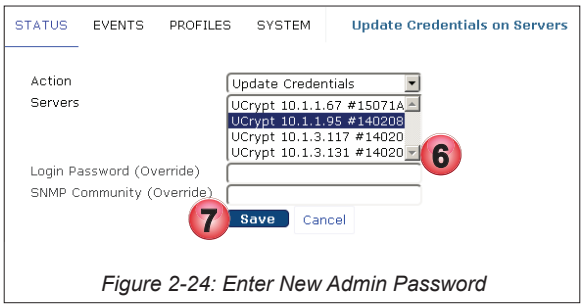

Figure 2-24: Enter New Admin Password

8. A message indicating success is displayed on the Status Page, Figure 2-25.

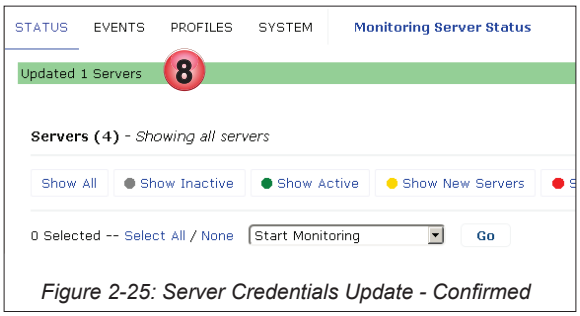

Figure 2-25: Server Credentials Update - Confirmed

2.4 Device Identification and Events (Alerts)

The column headings fields above the monitored remote Devices, Figure 2-26, are sortable identification parameters. Headings are clickable and each click sorts the column ascending then descending. The first click turns on the sorting icon as shown here using Event Details Event Details as an example. Some fields related to **Location and Identity** are definable by the MSO based on their specific requirements and terminology. For an explanation of fields, see Table 2.4a. To edit MSO Fields, see "5.15.2 Customize MSO Fields" on page 5-21.

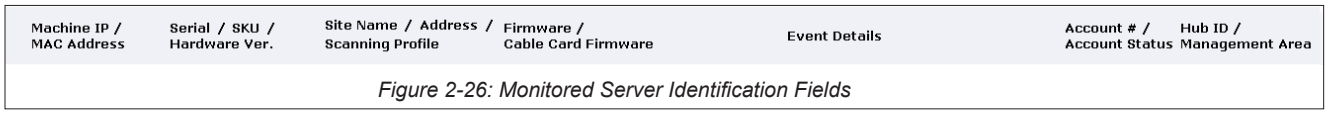

Figure 2-26: Monitored Server Identification Fields

Table 2.4a: Monitored Device Identification Fields (See Figure 2-26)

Field	MSO Definable Field	Description
Machine IP	No	The IP Address assigned to the monitored remote Device and used to connect to the GUI.
MAC Address	No	The MAC Address of the monitored Device.
Serial	No	The serial number of the monitored Device.
SKU	No	The SKU of the monitored Device. This is factory assigned and relates to the capabilities of the device, ie. QAM to GigE Clear.
Hardware Version	No	The factory assigned version of the Device hardware.
MSO_Site_Name	Yes	A name assigned by an MSO to identify the site where the monitored Device is installed. This parameter title is flexible and may be edited by the MSO to specify any required data.
Address	Yes	An address assigned by an MSO to identify the site where the monitored Device is installed. This parameter title is flexible and may be edited by the MSO to specify any required data.
Scanning Profile	No	The profile which contains the monitoring parameters that will be reported upon in the Monitoring Server. Profiles may be changed and any number of customized profiles may be created.
Firmware	No	The version of firmware installed on the monitored Device.
CableCARD Firmware	No	The version of firmware installed on the CableCARDs of the monitored Device.
Event Details	N/A	A summary of events recorded by the Monitoring Server for a specific remote monitored Device.
MSO_Account_Number	Yes	A number assigned by an MSO to identify the site where the monitored Device is installed. This parameter title is flexible and may be edited by the MSO to specify any required data.
MSO_Account_Status	Yes	An account status assigned by an MSO to identify the account where the monitored Device is installed. This parameter title is flexible and may be edited by the MSO to specify any required data.
MSO_HubID	Yes	An ID number assigned by the remote Device to identify the site where the monitored Device is fed from. This parameter title is flexible and may be edited by the MSO to specify any required data.
MSO_Management_ Area	Yes	An identifier assigned by an MSO to identify the site where the monitored Device is installed. This parameter title is flexible and may be edited by the MSO to specify any required data.

2.5 Added or Monitored Remote Devices(Servers)

This section of the Status Page, shown in Figure 2-27, is a list of all remote Devices that have been added to the Monitoring Server. This list may be displayed with variations based on the Devices Filter panel, (see “2.3 Device Filter Panel” on page 2-2) and search criteria filters (see “3.3 Search by Field” on page 3-2).

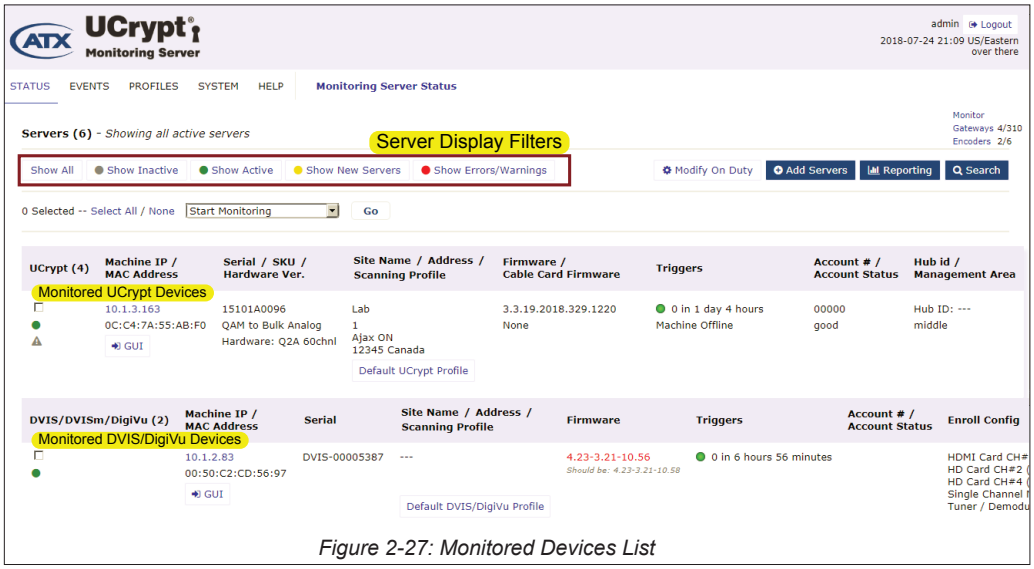

Figure 2-27: Monitored Devices List

There are a few notable features described below and highlighted in Figure 2-28:

1. The **IP Address** of the remote Devices are clickable and lead to a details page with configurable elements for identifying the specific remote Device (for details see “2.6.2 Device Site Identification” on page 2-13).
2. The **Monitoring Status Indicator** shows its overall status:
   - Grey for inactive.
   - Green for actively being monitored.
   - Yellow for new and never monitored as yet.
   - Red for actively being monitored but with unacknowledged alerts.
3. The monitored **Remote Device GUI** may be directly accessed by clicking the **GUI Icon**. If login credentials have been entered, an automatic login to the remote Device account results(Master for UCrypt, admin for DVIS and DigiVu). The Monitoring Server knows the default Master or admin password so this does not need to be entered but if the password was changed this will need updating in a process called **Update Credentials** (described in section “2.3.9 Update UCrypt Login Credentials” on page 2-9).
4. A **Warning Icon** is displayed If the remote Device runs the factory default password for the Admin or Master account.
5. The remote Device **Monitoring Profile** is presented with direct access by clicking the link to edit the profile.

Figure 2-28: Device Access and Configuration

2.6 Site Identification for Devices

Each listed UCrypt Device may have **site specific identification information** added to aid in identifying its location and MSO status. This identity information appears in the fields of the Devices List and to further customize the information, the fields may be changed to suit the MSO (To customize fields see “2.6.1 Customize MSO Fields” on page 2-12). As an example we show a Device before adding identification info in Figure 2-29. (To add Device identification information see “2.6.2 Device Site Identification” on page 2-13).

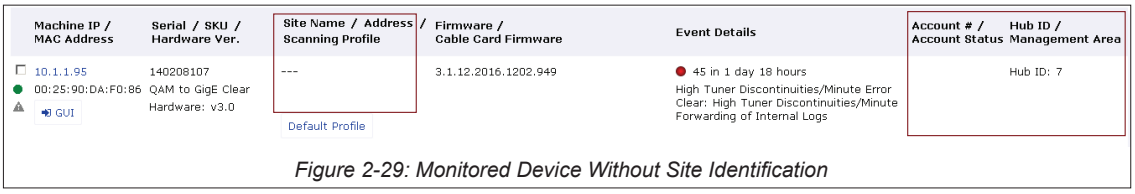

Figure 2-29: Monitored Device Without Site Identification

After adding the identity information and changing MSO Fields the new format is shown in Figure 2-30. (To customize fields see “2.6.1 Customize MSO Fields” on page 2-12).

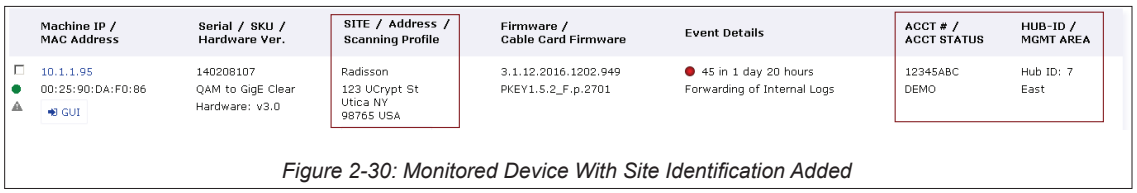

Figure 2-30: Monitored Device With Site Identification Added

2.6.1 Customize MSO Fields

MSO fields are part of the UCrypt Device Site Identification fields and may be changed from default to suit specific MSO needs and terminology. Access the link to make these changes from the **System** page.

Procedure

This procedure explains how to change the MSO fields.

1. Click the **System** tab if it isn’t already selected, Figure 2-31.

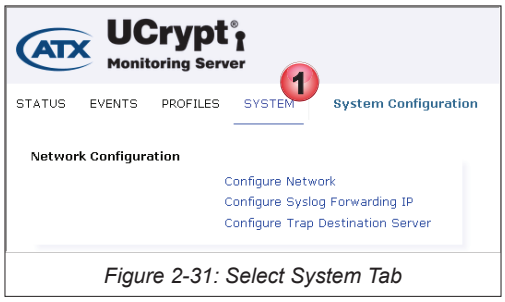

Figure 2-31: Select System Tab

2. Under the **Monitoring Server Details** section, click **Customize MSO Fields**, Figure 2-32.

Figure 2-32: Select Customize MSO Fields

3. Modify any of the six **Display Name** fields to reflect your desired content by directly editing the fields, Figure 2-33.
4. All fields are displayed by default. Choose whether the fields are not displayed by un-checking tick boxes.
5. Click **Save**.
6. Click **Back to System page** after saving.

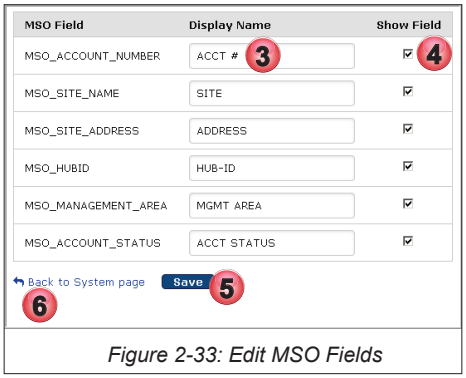

Figure 2-33: Edit MSO Fields

7. The updated fields, if they were changed, are displayed in the Server List header fields, Figure 2-34, or, if boxes were un-checked are not displayed at all.

Figure 2-34: Customized MSO Fields Displayed

2.6.2 Device Site Identification

Device Site Identification Information, highlighted in Figure 2-35, will make it easier for technical staff to know which equipment and location requires attention. This information will be displayed with the Device status but must be entered for each individual Device when added.

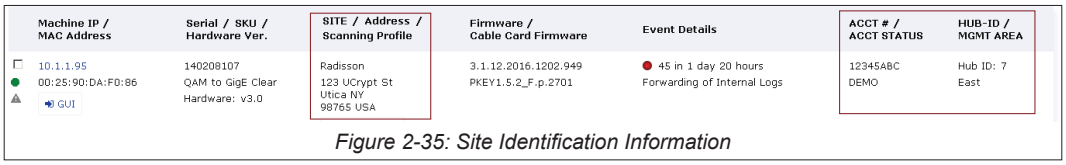

Figure 2-35: Site Identification Information

Procedure

This procedure explains how to enter site specific identification to the monitored Devices.

1. Click the **Status** tab if it isn't already selected, Figure 2-36.
2. Click the **IP Address** of the Device to have the Site Identification information updated.

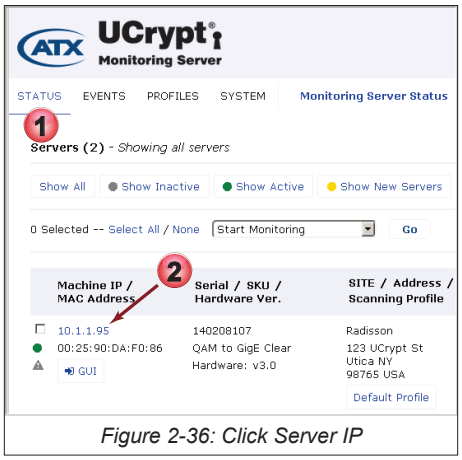

Figure 2-36: Click Server IP

3. Enter the information for this Device, Figure 2-37. General information about this Device such as the product name, SKU, Hardware, Serial, etc, which appears on the Status page also appears here for convenience as well as a link to modify the Monitor Profile and Acknowledge Alerts (see “2.7 Acknowledge Alerts” on page 2-14).
4. Some of the titles (outlined in green in Figure 2-37) are referred to as MSO Fields and are themselves editable from a dialog accessible from the System page (see section “2.6.1 Customize MSO Fields” on page 2-12).
5. The identity info dialog, Figure 2-37, also contains a **Field Notes** section where technicians may enter site specific info or leave notes for team-mates to be able to track and record site related issues, etc. Click the **Field Notes edit** link to access this feature. Notes that are entered are displayed below the link.
6. This reminder that there is a default factory password on the admin account of this Device will be active until the admin password is changed. Change the password on the remote Device GUI then **Update Credentials**, see “2.3.9 Update UCrypt Login Credentials” on page 2-9.
7. Click **Save Changes** when site information has been changed.

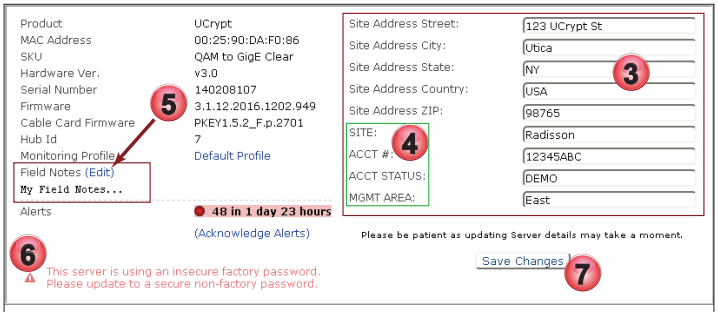

Figure 2-37: Edit Site Identification Info

2.7 Acknowledge Alerts

Alerts received from monitored Devices will cause that Device to have a red indicator in the list. Alerts need to be acknowledged to confirm that the reported problem has been investigated and corrected or has corrected itself. The process of acknowledging alerts will cause an **Intervention** to be recorded against that Device along with the user that applied the intervention. If alerts are not acknowledged, when 2001 alerts have occurred, the Monitoring Server will automatically stop monitoring and reporting until such time as this is done. Once alerts are acknowledged, the Device will be returned to its normal ‘green’ state. The goal should be to have all monitored Devices green at all times.

Procedure

This procedure explains how to acknowledge Alerts on the monitored Device.

1. Select the **Status** tab if it is not already selected, Figure 2-38.
2. A Device with Alerts will have a red indicator along with the Alerts listed in the Event Details column. A monitored Device with over 2001 unacknowledged alerts will have a red background as in our example.
3. Rectifying the problem may require accessing the remote GUI. Click the **GUI icon** to check out the machine directly.
4. After confirming remote Device operation, click the **IP Address** to acknowledge alerts.

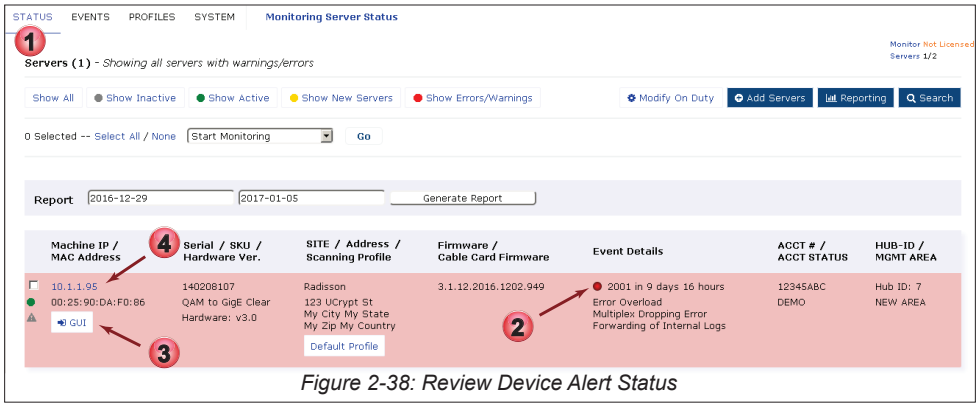

Figure 2-38: Review Device Alert Status

5. Alerts count is summarized on this page, Figure 2-39.
6. Click the link (Acknowledge Alerts) **Acknowledge Alerts**.

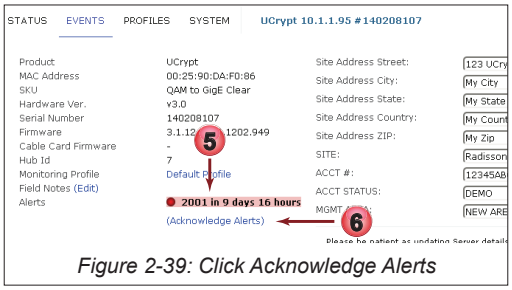

Figure 2-39: Click Acknowledge Alerts

7. The specific Alerts are listed for reference, Figure 2-40.
8. Select from the dropdown menu the most appropriate intervention description for the Alert problem resolution.
9. Click **Save**.
10. To record details not part of the intervention description, click the link Edit the Field Notes **Edit the Field Notes**.

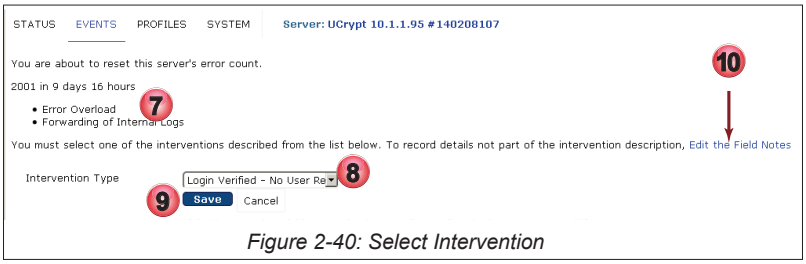

Figure 2-40: Select Intervention

11. In the field notes dialog, enter any information that will help others understand what happened, Figure 2-41.
12. Click **Save**.

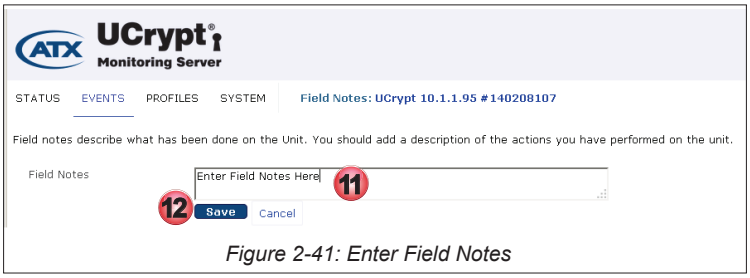

Figure 2-41: Enter Field Notes

13. Field Notes are saved on the Events Details page for the specific remote Device. Click the machine **IP Address** to see them, Figure 2-42.

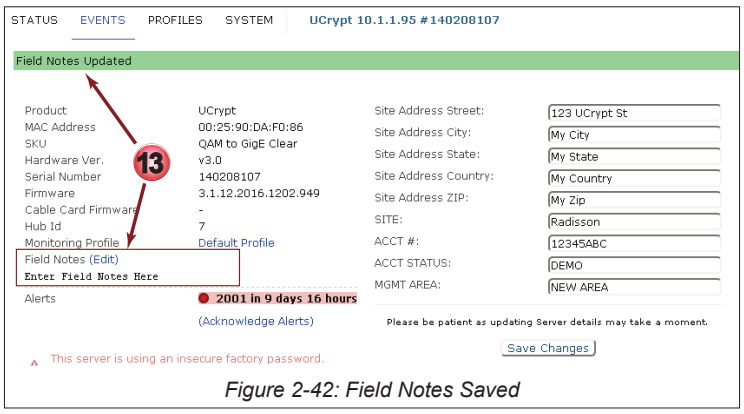

Figure 2-42: Field Notes Saved

This page left intentionally blank.

EVENTS TAB

3. Events Tab

Events are Alerts and other issues that currently exist or existed at one time with the remote monitored Devices.

3.1 Chapter Contents

This chapter covers the features and functions found on the Events Tab.

3.2 Events Page

This page displays all reported events for all monitored servers and can potentially contain a very long list of issues, refer to Figure 3-1. Several **Search & Sort** tools as well as **Report Generation** allow the events to be presented in a meaningful and useful way.

Key Features

1. **Search by Field** - A field by field search based on selected **event types**, **causes** and **remote Device identification** parameters. This creates a filter which reduces the list to only items of interest. Several search filters may be in play at one time and filters may be easily deleted. Available search fields are explained in Table 3.2e.
2. **Report Generation** - Create a report based on selected calendar dates. Reports include received Alerts and their Interventions, if any exist.
3. **Sortable Event List** - Heading Fields are sortable for **Ascending/Descending** presentation. Mousing over remote Devices before or after application of search filters provide pop up sort controls **Greater-than/Less-than** sorting and **Equal/Not Equal** sorting, see Figure 3-1.
4. **Web GUI Direct Link** - Direct access and automatic login to the monitored emote Device GUI can expedite troubleshooting and service.

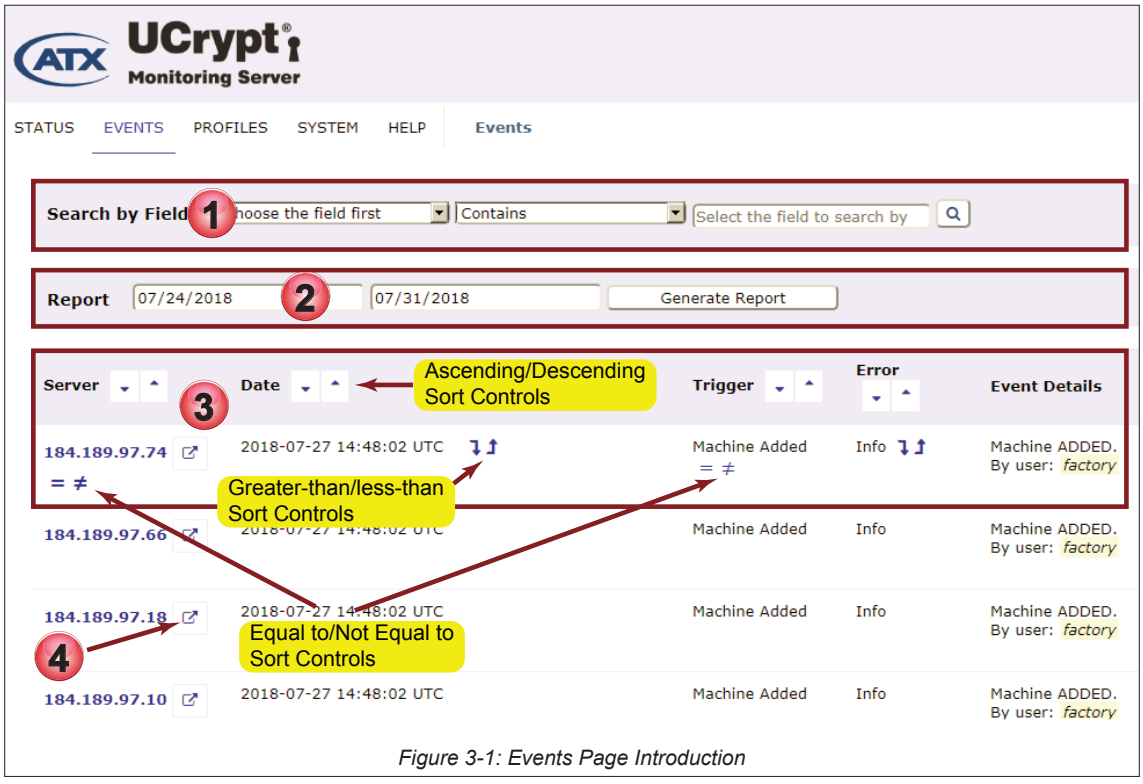

Figure 3-1: Events Page Introduction

Table 3.2e: Search Fields (See Figure 3-1)

Field	MSO Configurable Field	Search Parameter
Message	No	Each remote monitored Device will provide a **message describing the symptom**. This message is displayed on the Events page in a list. This is the message to search.
Trigger	No	Numerous triggers within each remote monitored Device will cause an Event to be recorded. This trigger is displayed on the Events page in the list as **Sender**.
IP	No	This is the IP Address for each remote monitored Device.
Firmware	No	This is the firmware version of the remote monitored Device.
CableCARD Firmware	No	This is the firmware version installed on the CableCARDs.
Serial	No	This is the serial number of the remote monitored Device.
MAC Address	No	This is the MAC address of the remote monitored Device.
Sku	No	This is the SKU (Stock Keeping Unit) of the remote monitored Device assigned as the product name i.e. QAM to GigE Clear, QAM to QAM ProI, etc
Scanning profile	No	The monitoring profile assigned for monitoring parameters of each monitored Device.
ACCT #	YES	An MSO assignable field of any alpha-numeric string. ACCT # is a value for example.
SITE	YES	An MSO assignable field of any alpha-numeric string. SITE is a value for example.
HUB-ID	YES	An MSO assignable field of any alpha-numeric string. HUB-ID is a value for example.
MGMT AREA	YES	An MSO assignable field of any alpha-numeric string. MGMT AREA is a value for example.
ACCT STATUS	YES	An MSO assignable field of any alpha-numeric string. ACCT STATUS is a value for example.

3.3 Search by Field

This feature allows searching the list of reported faults based on header fields of the list. The initial field selection is a fixed list of fields based on Monitoring Server field headings as well as the MSO defined fields, see Figure 3-2 and also Table 3.2e for explanations of the search fields. These are presented in a dropdown menu as the first item to select.

Procedure

This procedure explains how to search the remote monitored Device list for Devices that meet specific criteria.

1. Select the **Events** tab if it isn't already selected, Figure 3-2.
2. Click the **down arrow** of the first search field. The field text prompts you to choose it first.
3. From the dropdown menu, select the desired field to search. This is a fixed list but contains MSO definable fields (see Table 3.2e and "5.15.2 Customize MSO Fields" on page 5-21). In this example we select Firmware.

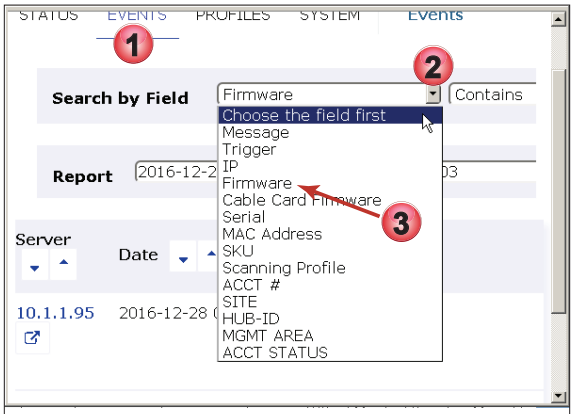

Figure 3-2: Initial Search Field Selection

4. Select the **down arrow** of the next search criteria, Figure 3-3. Choices are always only **Contains** to include & **Does Not Contain** to exclude the next search criteria.
5. We select **Contains** for this demo to search for and obtain a list of servers **with** the specified firmware version. Selecting **Does Not Contain** would produce a list of Devices that **do not** have the firmware.

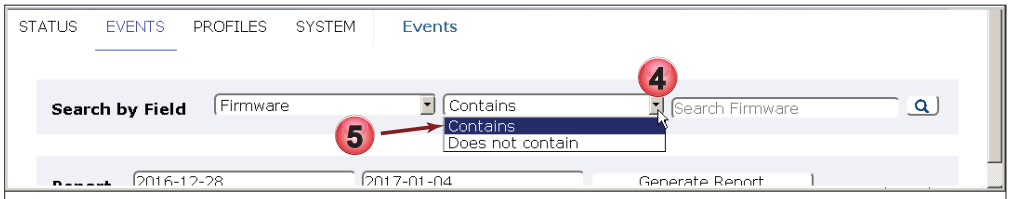

Figure 3-3: Contains or Not, Field Selection

6. Click **inside** the third search box and make a selection, Figure 3-4 . Regardless of the first search criteria selected, the dropdown list of choices will be just entries that exist in the monitored Devices, therefore only valid searches will result. If there are no items in the third dropdown list then there are no servers that match this particular search criteria.
7. With all three criteria selected, click the **Search** Icon.

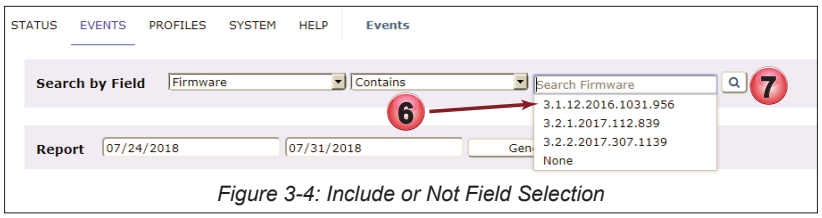

Figure 3-4: Include or Not Field Selection

8. An **Active Filter** is created, Figure 3-5, and multiple filters may be created in the same way to further refine the selection. Filters may be deleted by clicking anywhere on the filter. A **Trash Can** icon is on the filter to remind you of this.
9. The list of Devices with the specified criteria is presented. In this demo case only one Device exists with this specified firmware but this could also be a long list. Refine the list further with more filters.
10. Sort the resulting list fields with **Ascending/Descending** controls on each field heading.
11. Mouse over the Server list and further refine the list by creating more filters. Mouse over the icons for tool tips or click the **Include/Exclude** = ≠ Icons & **Greater-Than/Less-Than** Icons.

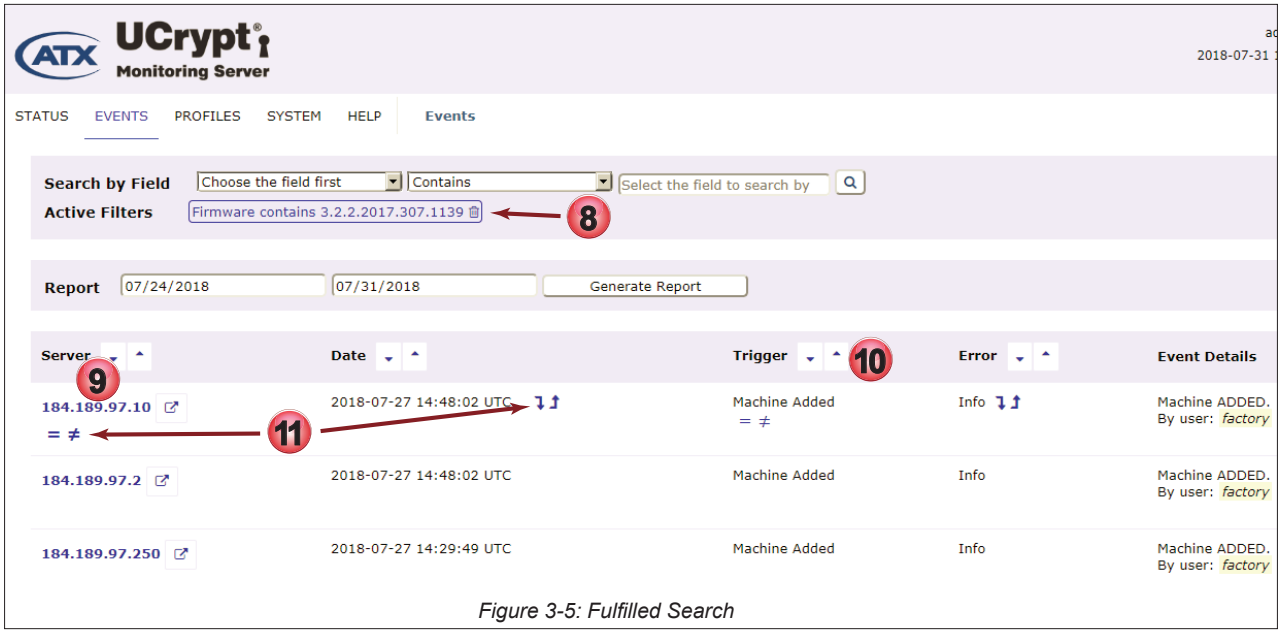

Figure 3-5: Fulfilled Search

3.4 Report Generation

Reports are a summary of Alerts and the Interventions recorded that have occurred between two dates. The report will be summarized by Server and Event Time Line.

Procedure

This procedure explains how to create a server Intervention Report.

1. Select the **Events** tab if it isn't selected already, Figure 3-6.
2. Enter the **start date** for the report in the format YYYY-MM-DD. This date will be included in the report.
3. Enter the **end date** for the report in the format YYYY-MM-DD. This date will be included in the report.
4. Click **Generate Report**.

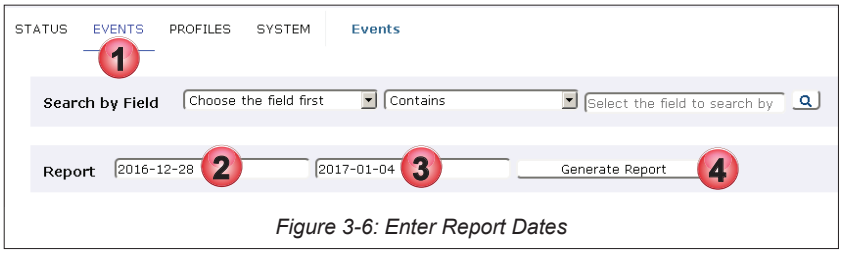

Figure 3-6: Enter Report Dates

5. An **Intervention Report** containing all events will be presented, Figure 3-7, and summarized the following ways:
6. Summary based on **Devices** affected.
7. Summary based on **TimeLine.**
8. Summary of **Interventions** if any (in the case of this demo there were no interventions).
9. Summary of **Alert Messages** from remote Devices.

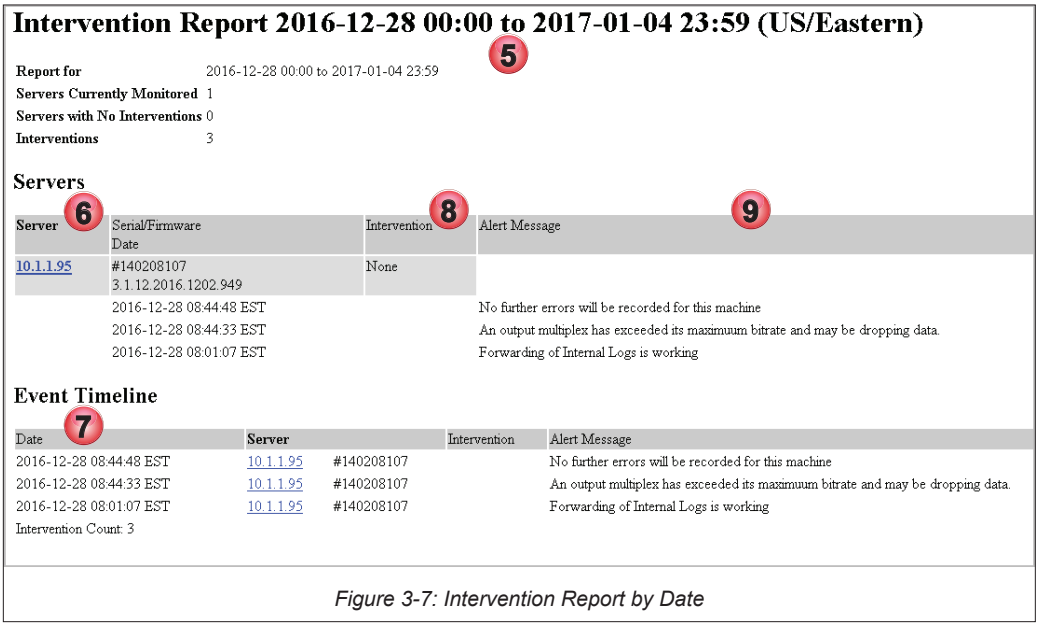

Figure 3-7: Intervention Report by Date

PROFILES TAB

4. Profiles Tab

Monitoring Profiles are the subsets of monitored Alerts of the monitored Devices that the Monitoring Server will watch over and report on. The factory default profile includes all functions available to monitor all manufactured compatible models. If an Alert is included in a profile that is applied to a monitored Device, when that Device sends such an Alert, the Monitoring Server will log that Alert and send an email to configured recipients if it has been set up to do so.

4.1 Chapter Contents

This chapter covers creation and management of a Monitoring Profile.

4.2 Create or Edit a Profile

Creating a new profile and editing an existing profile share most of the same steps so we combine these two procedures to avoid needless repetition.

It is worthy of note that while UCrypt monitoring profiles default to all triggers enabled, the DVIS/DigiVu profiles default to only one trigger, (SNMP Online Transition). When building DVIS/DigiVu profiles, all required triggers must be manually selected.

Procedure

This procedure explains how to create a new Monitoring Profile or edit an existing Profile.

1. Select the **Profiles** tab if it isn't already selected, Figure 4-1.
2. To create a new profile click the **+New** (+ New) link or to edit a profile just click the profile **Name,** in this case the Default Profile **Default Profile** for the Device being added. In our example we add a UCrypt but you may select DVIS or DigiVu depending on the equipment being monitored.

***Note** that there is no error generated if you chose the wrong profile for the equipment being monitored so be sure to choose a UCrypt profile for UCrypt Devices and the correct DVIS profile for the DVIS/DigiVu equipment being monitored.*

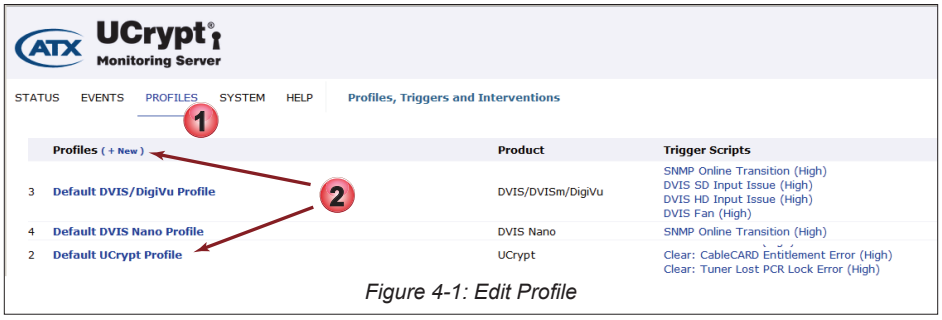

Figure 4-1: Edit Profile

3. Enter the new profile name if you are creating or you may edit the existing name if you are editing, Figure 4-2.
4. Select **UCrypt** as the product (for this example).

***Note** that there is no error generated if you chose the wrong profile for the equipment being monitored so be sure to choose a UCrypt profile for UCrypt Devices and the correct DVIS profile for the DVIS/DigiVu equipment being monitored.*

5. Select the **Triggers** that will be monitored within this profile. Hold the **Control** key while clicking to select all applicable Triggers or hold the Shift key to select a block of Triggers. The triggers may be added or subtracted from existing profiles in the same way.
6. Click **Save** when done.

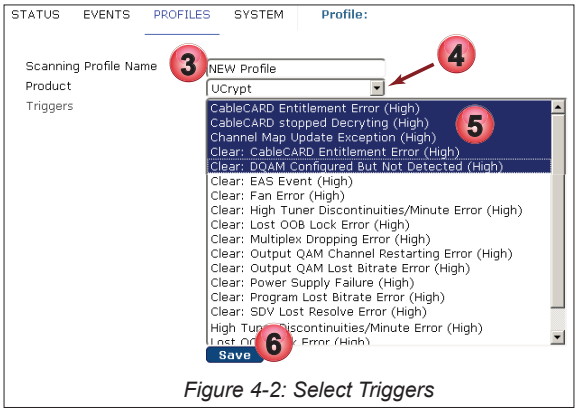

Figure 4-2: Select Triggers

Click the **Profiles** tab to continue work on Profiles or any tab to continue configuration or monitoring.

4.3 Delete a Profile

Profiles that are no longer required may be deleted from the Profiles tab.

Procedure

This procedure explains how to delete a Monitoring Profile.

1. Select the **Profiles** tab if it isn't already selected, Figure 4-3.
2. Click the **name of the profile** to be deleted.

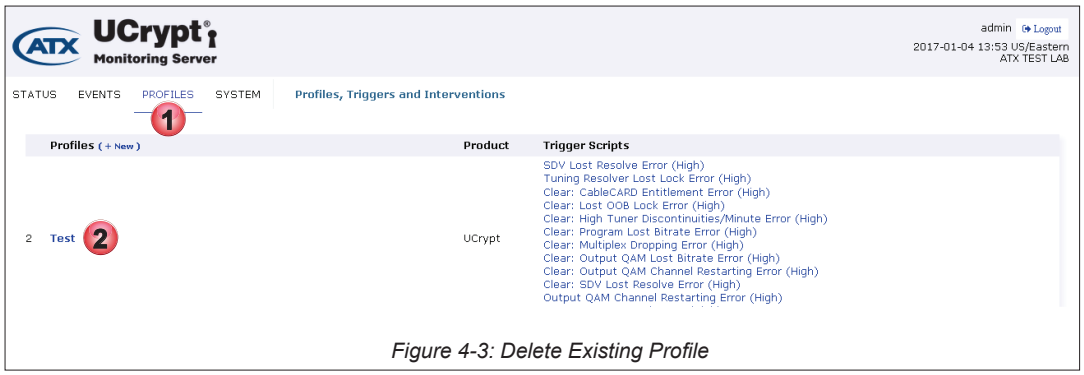

Figure 4-3: Delete Existing Profile

3. Click **Delete**, Figure 4-4.

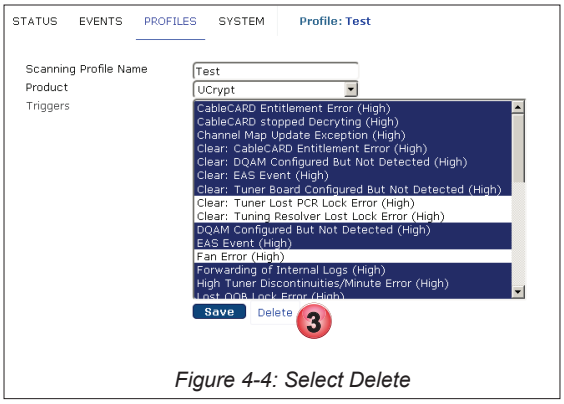

Figure 4-4: Select Delete

4. A dialog prompts you to consider that there is no way to undo this operation, Figure 4-5.
5. Click **Confirm and Delete**.

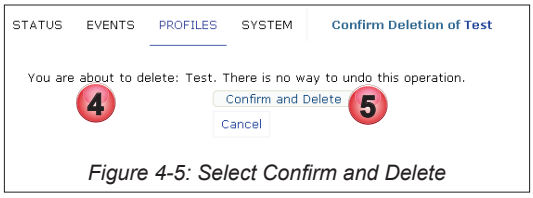

Figure 4-5: Select Confirm and Delete

6. A confirmation of deletion operation completed.

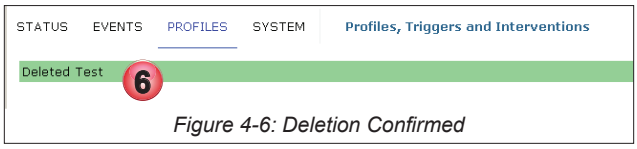

Figure 4-6: Deletion Confirmed

4.4 Configure Email Notifications

Any alert received from a monitored Device may be programmed to send an email to one or more destination addresses by setting a configuration called a **Trigger Script**. Before email notifications can be sent, the SMTP account and mail server parameters need to be defined on the **System** tab, see "5.14 Email Alerts" on page 5-19 for the required configuration.

4.4.1 Configure Trigger Scripts

Triggers occur when a monitored Device detects a reportable problem, the **Alert**, and forwards its syslog report to the Monitoring Server. If that alert has been defined as **active**, then the Monitoring Server responds by sending an email message to defined recipients. For any given Monitoring Server there can be only **one configuration** for email alerts **per alert trigger**. This means that all monitored Devices sending an identical alert and configured with the same profile alert item will generate an email to all defined recipients. All monitored Devices use the same fundamental trigger configuration even though they may be monitored with different profiles, so if the alert trigger appears in more than one Monitoring Profile both profiles use the same trigger configuration.

A few terms defined:

- Alert

  A detected condition within a monitored Device that can be monitored and generate a report to external recipients. Recipients could be an SNMP trap, an email alert programmed directly in the Device or a syslog report which is an internal mechanism. This is the Alert that is familiar to any user of this equipment and descriptions of the Alerts is provided in Table 4.4a. See also "6. Remote Device Alerts" on page 6-1.

- Trigger

  A condition where a received Alert from a monitored Device matches an active programmed Alert monitor in the

monitoring Server. When the Monitoring Server detects this condition, it triggers an email message to defined recipients and as well, an SNMP trap Northbound (traps sent to an SNMP Manager), if set to do so.

- Sender

  This is the Alert Message displayed in the Events list which is usually the same as the Alert message from the monitored Device itself though it may be modified by the Monitoring Server if necessary.

- Email Alert

  The email message that is sent to recipients that have been defined for each trigger. An email address of **on_duty** will specify that an email message is to be sent to whatever technician is defined as being on call or 'On Duty'.

Procedure

This procedure outlines enabling trigger scripts, adding email recipients to the script and forwarding SNMP Northbound traps.

1. Click the **Profiles** tab if it is not already selected, Figure 4-7.
2. The upper section lists the profiles and their included scripts. These elements are also hyperlinks but do not use these links for configuration.
3. Configuration is done in the second lower section titled **Trigger Scripts**. They relate directly to the familiar Device Alerts as there is one for each Alert that you are familiar with and a few new ones that relate to the interaction with the Monitor Server and the remitting of specific Alerts.
4. Click the **Trigger** to be configured. There is only one set of triggers per Monitoring Server. All monitored Devices whose profile includes a trigger will use the same set of Trigger Scripts.

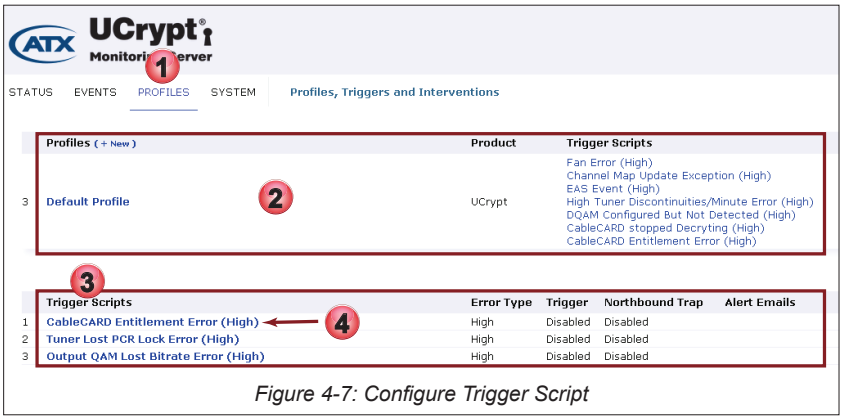

Figure 4-7: Configure Trigger Script

5. Tick the box to enable this trigger, Figure 4-8.
6. Select the Error Level from the dropdown menu choices of High, Medium, Low or Info. **Info** does not generate an email but all levels above do result in an email being sent.
7. Enter the email addresses of each recipient that should receive an email alert when this alert is triggered. Multiple addresses may be entered with comma separation. Entering **on_duty** will link to the designated on call technician defined with the Modify On Duty **Modify On Duty** button on the Status Page, (see "2.3.2 Assign the 'On Duty' Technician" on page 2-3 for this procedure).
8. If Northbound SNMP traps (traps sent to an SNMP Manager) are required, tick the box to enable. Be sure to configure the SNMP trap target, see "5.4 Configure SNMP" on page 5-12.
9. Click **Save** when finished.

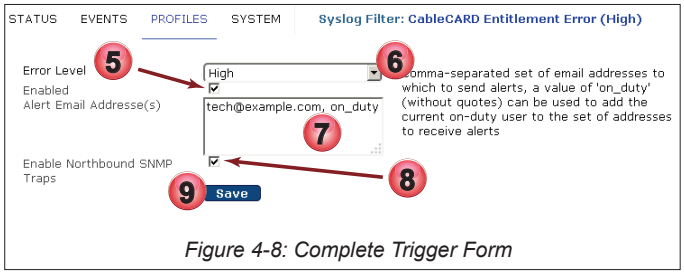

Figure 4-8: Complete Trigger Form

Click the **Profiles** tab to return for more configuration of Trigger Scripts.

10. The Trigger is configured and enabled. Email recipients are listed for this Alert.

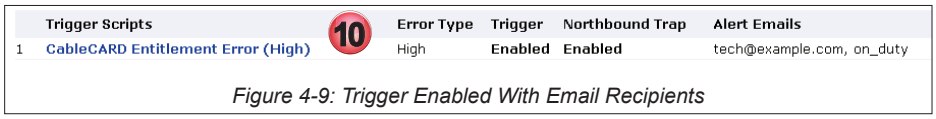

Figure 4-9: Trigger Enabled With Email Recipients

4.4.2 DVIS Trigger Descriptions

A summary of DVIS/DigiVu Device Triggers and descriptions is provided here for reference and convenience. Refer to the operating manual for your specific Device model for expanded information on Alerts.

***Note** for DVIS Devices only: If an encoder card is installed or removed this change will not be reflected automatically in the Monitoring Server GUI. In order to register this change the affected Device needs to be removed from the Monitoring Server, then re-added. DVIS Devices are not constantly polled for changes in hardware. Re-Identify will not work for this as it does not poll for this type of hardware change.*

Table 4.4a: DVIS Trigger Descriptions Summary (Provided For Reference)

Field	Trigger Description Summary
DVIS SD Input Issue	SD Encoder Card has no input.
DVIS HD Input Issue	SD Encoder Card has no input.
DVIS Fan	Fan failure detected.
SNMP Online Transition	Monitors that the device is actually online via SNMP (if not specified in the profile you will not know if the server is online/offline)

4.4.3 UCrypt Trigger Descriptions

A summary of UCrypt Device Triggers and descriptions is provided here for reference and convenience. Refer to the operating manual for your specific Device model for expanded information on Alerts. Also see “Remote DEvice Alerts” on page 6-1 for further details of UCrypt Alerts messages.

Table 4.4a: UCrypt Trigger Descriptions Summary (Provided For Reference)

Field	Trigger Description Summary
CableCARD Entitlement Error	Refers to a specific program on a specific CableCARD module does not possess an entitlement enabling it to be decrypted.
Tuner Lost PCR Lock Error	Refers to the loss of Program Clock Reference on a specific multiplex or QAM channel.
Output QAM Lost Bitrate Error	Refers to QAM Modulator stops modulating at 38.8 Mb/s. The bit stream from the internal multiplexer to the QAM modulator has failed. This error indicates that the modulator has failed to acquire the bit stream properly.
SDV Lost Resolve Error	Refers to a Tuning Adapter tried to determine the frequency of the channel but it received an error message.
Tuning Resolver Lost Lock Error	Refers to Tuning Adapter lost lock to the Data Carousel.
Temperature Error	Refers to the internal operating temperature of the UCrypt CPU Cores.
Forwarding of Internal Logs	Refers to syslogs are not being received from the UCrypt Server. This could occur if there are more than 2001 unacknowledged alerts on the Monitoring Server from a single UCrypt Server.
Channel Map Update Exception	Refers to The inability of the UCrypt to accommodate a program move as required by a channel map update.
Lost OOB Lock Error	The UCrypt has lost reception on the specified OOB carrier.
High Tuner Discontinuities/Minute Error	Refers to MPEG level packet loss at a specific QAM tuner (Tuner #0 to #5) on a specific Host card (Card #0 to #9).
Multiplex Dropping Error	Refers to the aggregate bit rate of the specific QAM is exceeding 38.8 Mb/s or the internal multiplexer is failing to properly process all packets as it should.
Output QAM Channel Restarting Error	Refers to PCR accuracy abnormal at the output of the UCrypt program multiplexer.
Power Supply Failure	Refers to failure of one of the two redundant power supply modules. This failure could be caused also by the lack of AC input to one power supply if they are fed from redundant power sources.
EAS Event	Refers to reception of an event related to the Emergency Alert System (EAS). An official test of the EAS system will be reported with the same alert as a real EAS event.
Fan Error	Refers to the failure of cooling fans of the UCrypt.
Plant Maintenance Exception	Refers to the scheduled check of programs that are either missing or are not decrypting. On the System page under the ‘Power’ section, the device may be configured to do a “Scheduled Outage Check”.
Clear: Temperature Error	Refers to the remitting or clearing of the temperature alert.
Clear: Fan Error	Refers to the remitting or clearing of the Fan Error alert.

Field	Trigger Description Summary
Clear: EAS Event	Refers to the remitting or clearing of the EAS alert.
Clear: CableCARD Entitlement Error	Refers to the remitting or clearing of the CableCARD Entitlement Error alert.
Clear: Tuner Lost PCR Lock Error	Refers to the remitting or clearing of the Tuner Lost PCR Lock Error alert.
Clear: Lost OOB Lock Error	Refers to the remitting or clearing of the Lost OOB Lock Error alert.
Clear: High Tuner Discontinuities/Minute Error	Refers to the remitting or clearing of the High Tuner Discontinuities/Minute Error alert.
Clear: Program Lost Bitrate Error	Refers to the remitting or clearing of the Program Lost Bitrate Error alert.
Clear: Multiplex Dropping Error	Refers to the remitting or clearing of the Multiplex Dropping Error alert.
Clear: Output QAM Lost Bitrate Error	Refers to the remitting or clearing of the Output QAM Lost Bitrate Error alert.
Clear: Output QAM Channel Restarting Error	Refers to the remitting or clearing of the Output QAM Channel Restarting Error alert.
Clear: SDV Lost Resolve Error	Refers to the remitting or clearing of the SDV Lost Resolve Error alert.
Clear: Tuning Resolver Lost Lock Error	Refers to the remitting or clearing of the Tuning Resolver Lost Lock Error alert.
Clear: Power Supply Failure	Refers to the remitting or clearing of the Power Supply Failure alert.
Clear: DQAM Configured But Not Detected	Refers to the remitting or clearing of the DQAM Configured But Not Detected alert.
Clear: Tuner Board Configured But Not Detected	Refers to the remitting or clearing of the Tuner Board Configured But Not Detected alert.
Tuner Board Configured but not Detected	Refers to programs known to be assigned to tuner boards will be missing from the output.
Restarting DQAM Channel	Refers to a DQAM Channel continuously restarting.
DQAM Configured But Not Detected	Refers to UCrypt device configuration has programs assigned to a DQAM but the DQAM has not been detected.
System Booted	Refers to the UCrypt Server main board being rebooted.
CableCARD stopped Decrypting	Refers to a CableCARD that has stopped decrypting.
Program Lost Bitrate	Refers to lack of presence of MPEG video packets for the program in question. This error is reporting on a single program in a QAM and is not indicating the failure of the QAM as a whole.
SNMP Online Transition	Monitors that the device is actually online via SNMP (if not specified in the profile you will not know if the server is online/offline)

4.5 Working with Interventions

Interventions are the reported actions that were taken by a field technician or actions that may have occurred automatically that resulted in clearing an Alert. Each Alert will need to have an Intervention recorded when it is acknowledged. Later when a report is generated, the Intervention and the person responsible (the user logged into the Monitoring Server) will be registered in the log. Refer to Table 4.5a for a list of interventions and types available. The list is fixed and cannot be changed or modified by the MSO. The list is provided here for your convenience.

Table 4.5a: Interventions List for Reference

	Interventions	Intervention Type
1	CableCARD 0 stopped Decrypting	Automatic Recovery
2	CableCARD 1 stopped Decrypting	Automatic Recovery
3	CableCARD 2 stopped Decrypting	Automatic Recovery
4	CableCARD 3 stopped Decrypting	Automatic Recovery
5	CableCARD 4 stopped Decrypting	Automatic Recovery
6	CableCARD 5 stopped Decrypting	Automatic Recovery
7	CableCARD 6 stopped Decrypting	Automatic Recovery
8	CableCARD 7 stopped Decrypting	Automatic Recovery
9	CableCARD 8 stopped Decrypting	Automatic Recovery
10	CableCARD 9 stopped Decrypting	Automatic Recovery
11	CableCARD regained Entitlement	Automatic Recovery
12	OOB Lock Regained	Automatic Recovery
13	Output QAM regained Bitrate	Automatic Recovery
14	Program Regained Bitrate	Automatic Recovery
15	SDV Tuner Lost Resolve	Automatic Recovery
16	Server Power Cycled (Automatic)	Automatic Recovery
17	Tuner Board Automatically Regained PCR Lock	Automatic Recovery
18	Clicked Apply	Intervention
19	CABLECard Keeps Initializing	Intervention

	Interventions	Intervention Type
20	CableCARD re-provisioned Lost Entitlement	Intervention
21	CABLECard was rebooted, Program lost entitlement	Intervention
22	Clicked Reset Video	Intervention
23	DQAM lost bit rate Unit was Powered cycled	Intervention
24	DQAM lost bitrate DQAM channel was toggled	Intervention
25	DQAM lost bitrate DQAM was Powercycled	Intervention
26	Unit Firmware Updated	Intervention
27	Unit was Reboot	Intervention
28	Scheduled Reboot Occurred	Intervention
29	Temperature High	Intervention
30	Tuner Board Reset Program(s) Lost Bitrate	Intervention
31	Tuner Board was Reset	Program(s) lost entitlement
32	QAM(s) outage across multiple units	No User Report Required
33	Channel(s) outage across multiple units	No User Report Required
34	Local Channel(s) outage	No User Report Required
35	Local QAM(s) outage	No User Report Required
36	Contacted ATX Digital Video Support	No User Report Required
37	Customer Rebooted Modem	No User Report Required
38	IP Address Change	No User Report Required
39	Local Power outage	No User Report Required
40	Login Verified	No User Report Required
41	Monitoring Failure	No User Report Required
42	No Issue Found, All programs are working	No User Report Required
43	Plant Maintenance	No User Report Required
44	RF level(s) were too high	No User Report Required
45	RF level(s) were too low	No User Report Required
46	SNR level(s) were too low	No User Report Required
47	Server Power Cycled (Customer)	No User Report Required
48	Syslog Flood Suppressed	No User Report Required
49	Tuner was Board was replaced (Customer)	No User Report Required
50	Unit has been removed or replaced (Customer)	No User Report Required
51	CableCard was replaced (Customer)	No User Report Required
52	DQAM was replaced (Customer)	No User Report Required
53	Local OOB outage	No User Report Required
54	OOB outage across multiple units	No User Report Required
55	CableCARD 0 Stopped Decrypting	Intervention
56	CableCARD 1 Stopped Decrypting	Intervention
57	CableCARD 2 Stopped Decrypting	Intervention
58	CableCARD 3 Stopped Decrypting	Intervention
59	CableCARD 4 Stopped Decrypting	Intervention
60	CableCARD 5 Stopped Decrypting	Intervention
61	CableCARD 6 Stopped Decrypting	Intervention
62	CableCARD 7 Stopped Decrypting	Intervention
63	CableCARD 8 Stopped Decrypting	Intervention
64	CableCARD 9 Stopped Decrypting	Intervention

This page intentionally left blank.

SYSTEM TAB

5. System Tab

The System page contains the Platform Global settings and includes the categories of Network Configuration, LDAP Configuration, Firmware Upgrades, Power Management, System Time, SNMP and more.

5.1 Chapter Contents

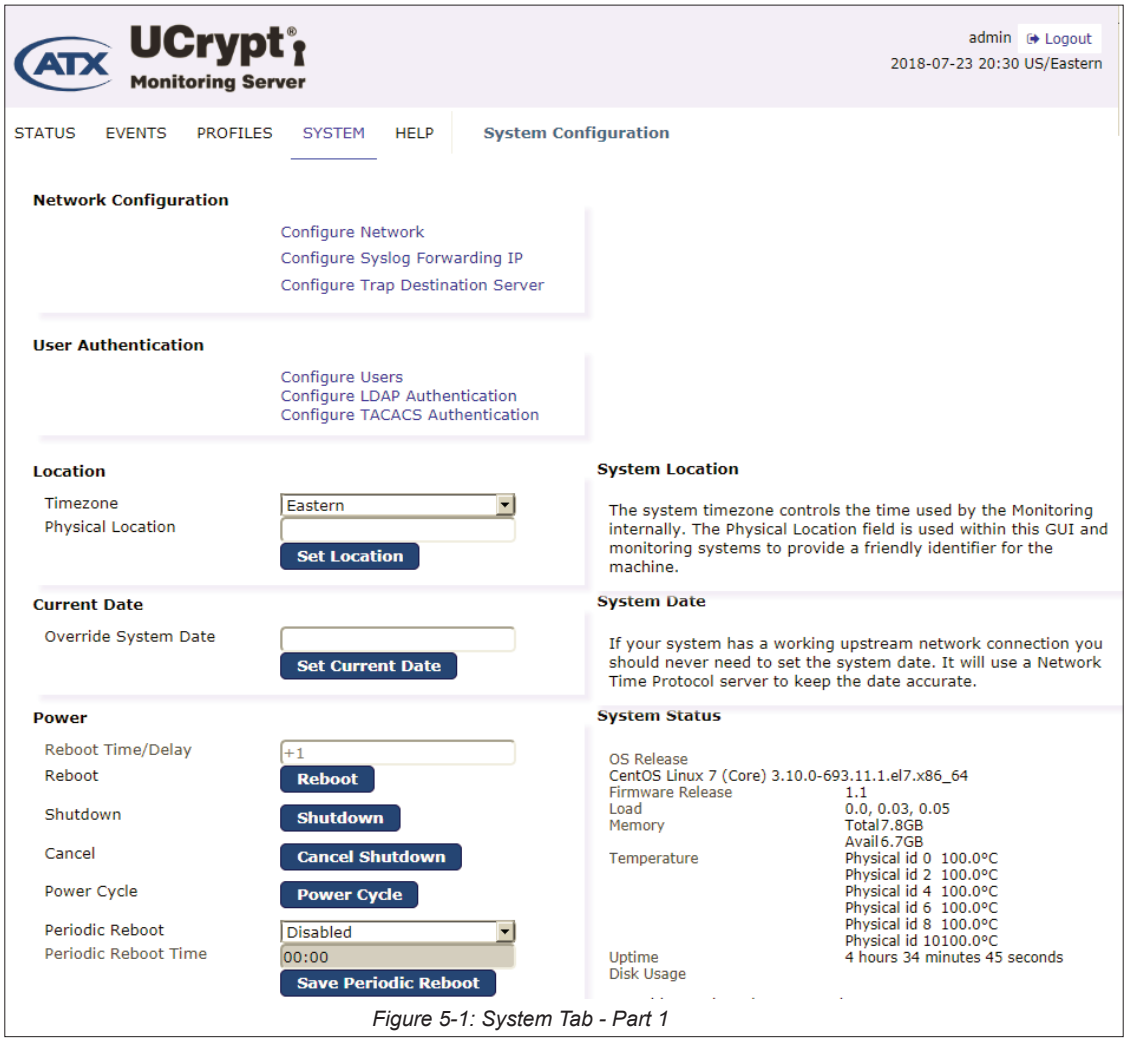

Figure 5-1: System Tab - Part 1

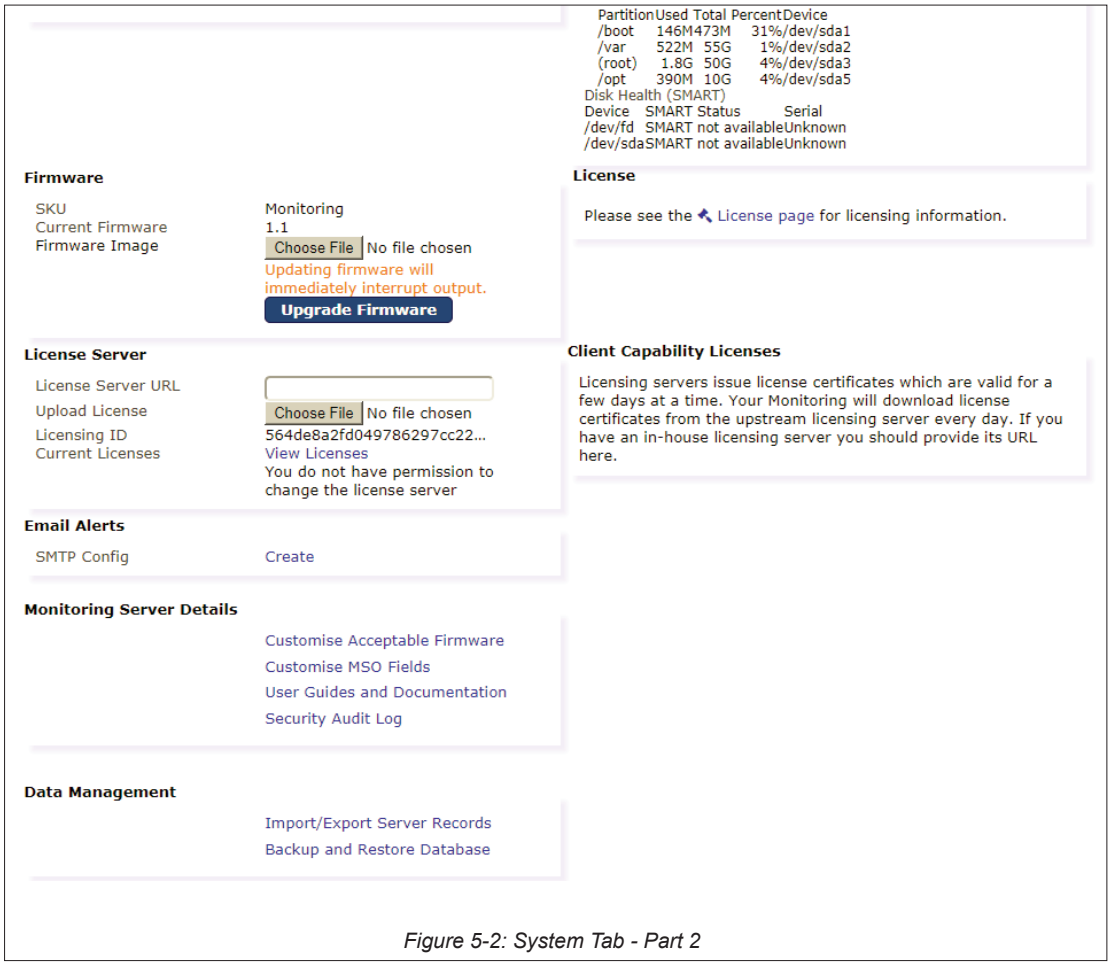

Figure 5-2: System Tab - Part 2

5.2 Network Configuration

From this page you may edit the physical Ethernet port IP addresses and create VLANs.

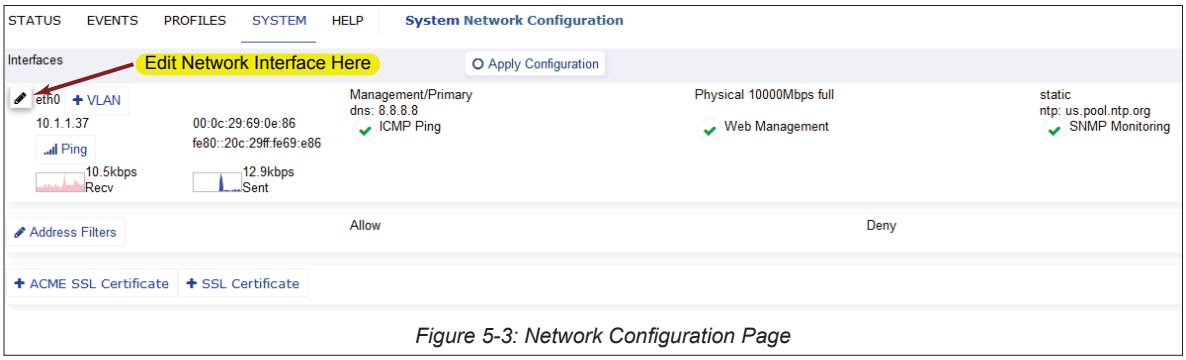

Figure 5-3: Network Configuration Page

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

5.2.1 Interface Role

All Ethernet network interfaces may have their role defined, see Figure 5-4, as one of the following interface types with the conditions and limitations listed:

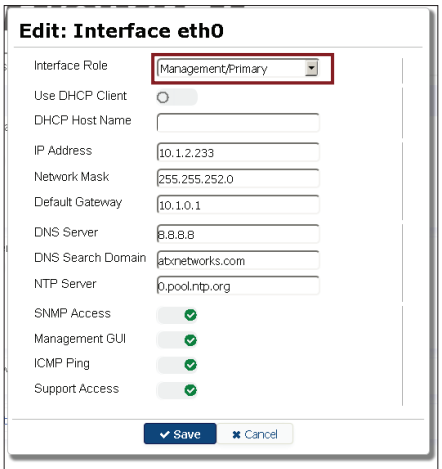

Figure 5-4: Defining Interface Role

Management Role

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

External IP In

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

External IP Out

- The interface which will be used for IP output if a specific interface is not set when defining the output.
- An interface defined as 'External IP Out' may have the Management GUI, SNMP Access & Support Access services enabled if desired via the respective toggle switches.

5.2.2 Edit a Network Interface

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

Procedure

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

1. Click the **System** Tab, Figure 5-5 if it is not already selected.
2. Click **Configure Network** under Network Configuration section.

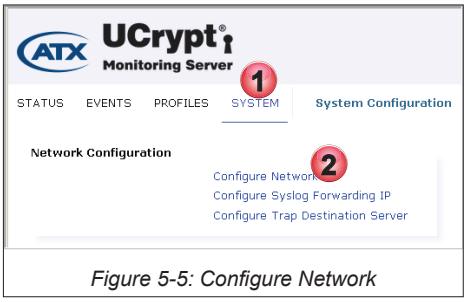

Figure 5-5: Configure Network

3. To edit the eth0 management network settings click the **Edit Icon** on eth0 interface, Figure 5-6.

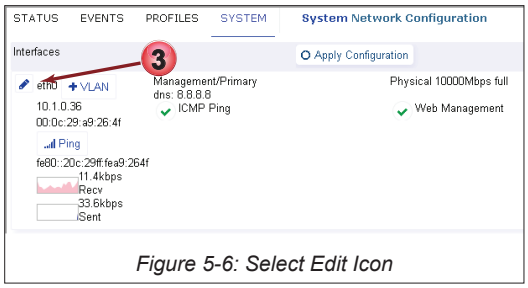

Figure 5-6: Select Edit Icon

4. Edit default values or fill in the Interface Settings form, Figure 5-7 per Table 5.2a and/or your requirements.
5. Click **Save** when finished with edits.

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

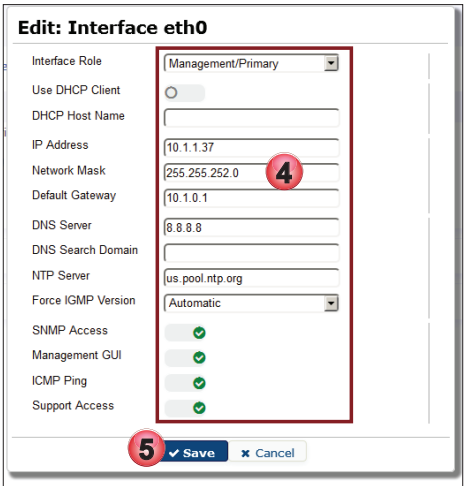

Figure 5-7: Edit eth0 Interface Settings

Table 5.2a: Form Values for eth0 (See Figure 5-7)

Field	Configurable	Value
Interface Role	Dropdown Menu	Management/Primary. Do not change this value for eth0.
Use DHCP Client	Tick Box/Switch	Un-Ticked (Grayed out) for static IP address, tick (checked) for DHCP.
DHCP Host Name	String	Host name used in DHCP requests.
IP Address	IP Address	IP Address v4 or v6
Network Mask	IP Subnet Mask	Network Mask, (ffff:ffff:ffff:: or 255.255.255.0 format).
Default Gateway	IP Address	Routing Gateway for the Interface.
DNS Server	IP Address	DNS Server, only used if specified here.
DNS Search Domain	URL	As required by your network.
NTP Server	IP Address/URL	Network Time Protocol server to which to synchronize this Device.
Force IGMP Version	Dropdown Menu	Chose the IGMP Version from the menu: Automatic(Default), IGMPv2, IGMPv3.
SNMP Access	Tick Box/Switch	Tick to allow SNMP messages on this interface. If enabled, the SNMP port will be enabled on this interface.
Management GUI	Tick Box/Switch	Ticked to expose UI ports on this interface. Must be active on at least one interface.
ICMP Ping	Tick Box/Switch	Tick to enable ping response on this interface.

Field	Configurable	Value
Support Access	Tick Box/Switch	If enabled, the support (ssh) port will be enabled on this interface; note it is strongly encouraged to leave this enabled on at least one interface.

6. When saved, eth0 values are changed but not yet activated on the Server, Figure 5-8.
7. Click **Apply Configuration** to activate the changes.

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

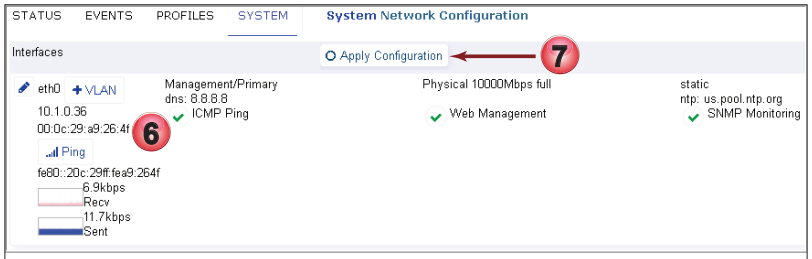

Figure 5-8: Changed Values Applied to eth0

5.2.3 Monitor Network Performance

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

Procedure

This procedure describes monitoring of the network performance histogram.

1. Click the **System** Tab, Figure 5-9.
2. Click **Configure** under **Network Configuration** section.

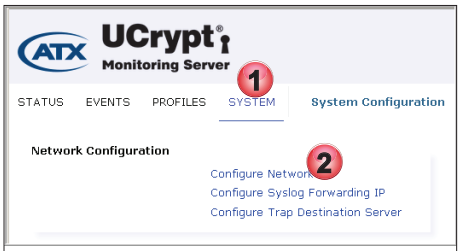

Figure 5-9: Configure Network

3. Histogram of network data sent and received over each individual interface is updated every 10 seconds and shows continuous history for as long as the window is open, Figure 5-10. The current data rate is also shown in Mbps or kbps. The data rate histogram is for comparative purposes only and is not calibrated.

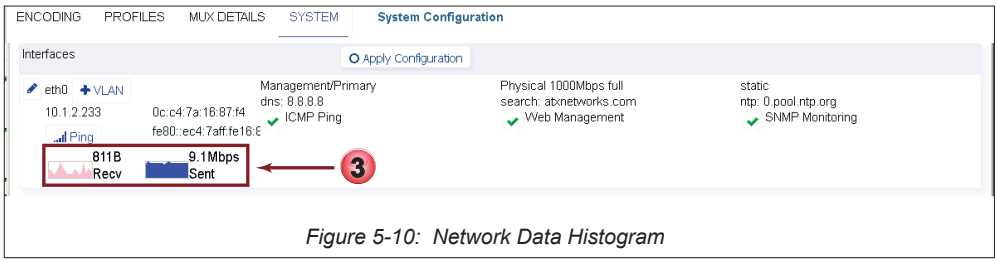

Figure 5-10: Network Data Histogram

5.2.4 Ping Target

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

1. Click the **System** Tab, Figure 5-11.
2. Click **Configure** under **Network Configuration** section.

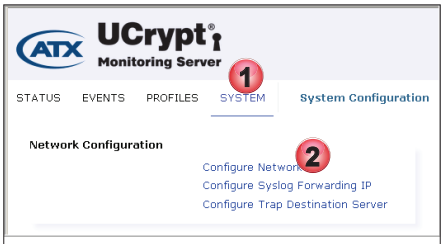

Figure 5-11: Configure Network

3. Click the **Ping** Ping button on any interface to initiate the Ping function, Figure 5-12.

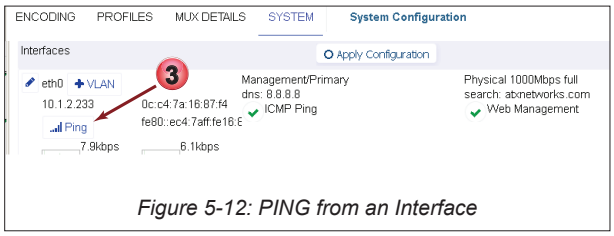

Figure 5-12: PING from an Interface

4. Enter the Target remote IPv4 address of the device to be pinged, Figure 5-13.
5. Click the **Ping** button.

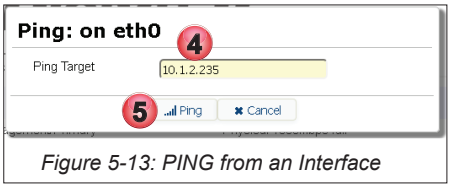

Figure 5-13: PING from an Interface

6. The ping results are shown, Figure 5-14. To continue with another ping to this address, click **Ping** again.
7. Alternately try another target by entering its IP address then click **Ping**.

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

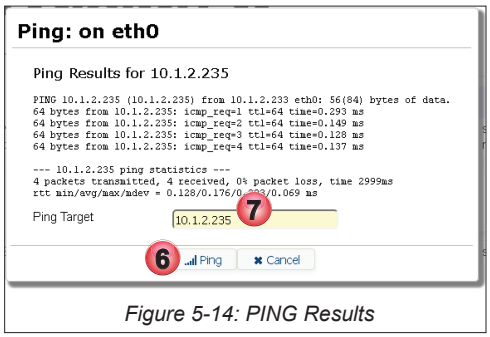

Figure 5-14: PING Results

5.2.5 Configure IP Address Filter

Security concerns may dictate that only certain IP addresses may connect to this Monitoring Server. You may set up IP addresses that are specifically allowed or specifically excluded from logging in the server. This filter has no effect on the IP Addresses of UCrypt servers that are being monitored.

Procedure

This procedure explains how to configure IP Address filters.

1. Click the **System** Tab, Figure 5-15.
2. Click **Configure** under **Network Configuration** section.

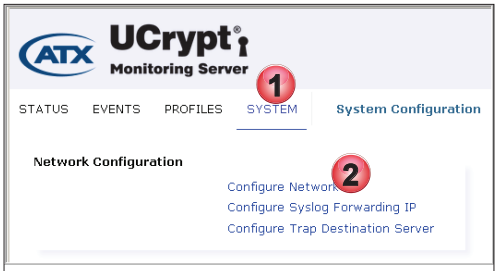

Figure 5-15: Configure Network

3. Click the **Edit Address Filters** Address Filters button, Figure 5-16.

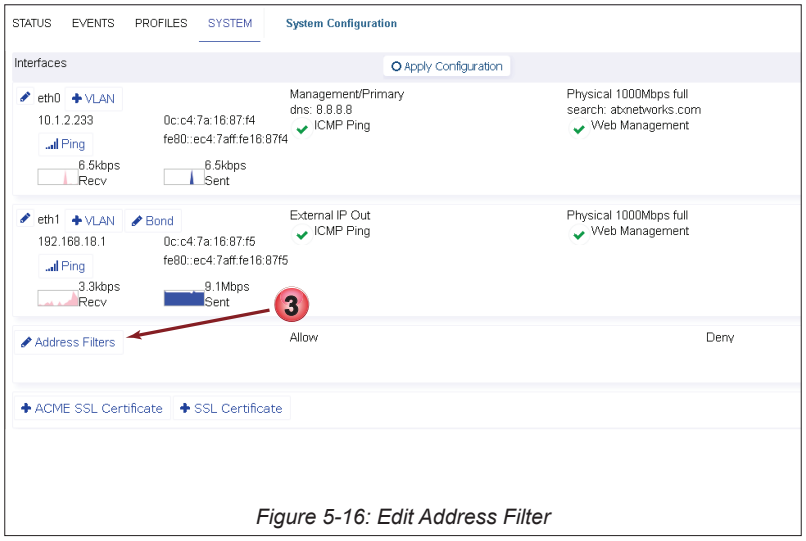

Figure 5-16: Edit Address Filter

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

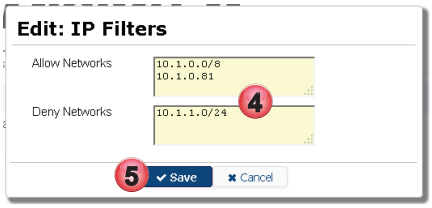

Figure 5-17: Enter Deny or Allow Addresses

6. The entered addresses are displayed adjacent the Edit Address Filters button, Figure 5-18

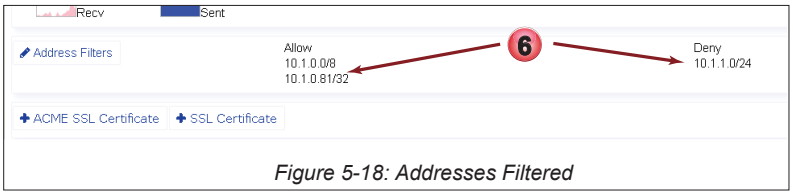

Figure 5-18: Addresses Filtered

5.2.6 Create ACME SSL Certificate

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

Detailed information about obtaining a certificate is available at https://letsencrypt.org/.

1. Click the **System** Tab, Figure 5-19.
2. Click **Configure** under **Network Configuration** section.

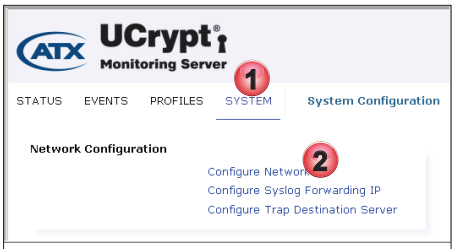

Figure 5-19: Configure Network

3. Click the **+ ACME SSL Certificate** + ACME SSL Certificate button, Figure 5-20.

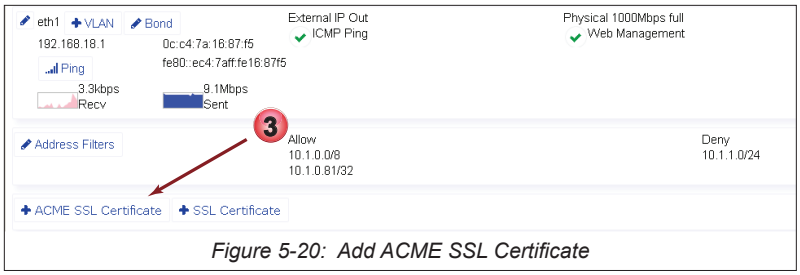

Figure 5-20: Add ACME SSL Certificate

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

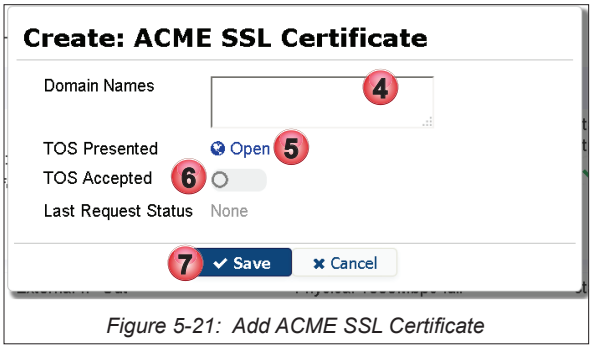

Figure 5-21: Add ACME SSL Certificate

5.2.7 Install SSL Certificate

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

Procedure

This procedure explains how to install an SSL Certificate.

1. Click the **System** Tab, Figure 5-22.
2. Click **Configure** under **Network Configuration** section.

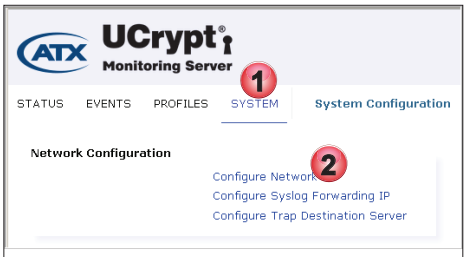

Figure 5-22: Configure Network

3. Click the **+ SSL Certificate** button, Figure 5-23.

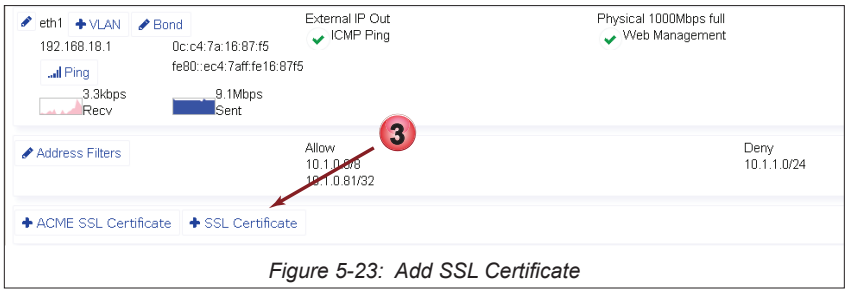

Figure 5-23: Add SSL Certificate

4. To upload an SSL Private Key, click the Private Key **Browse** button, Figure 5-24.
5. To upload an SSL Public Certificate, click the Public Certificate **Browse** button.
6. Click **Save**.

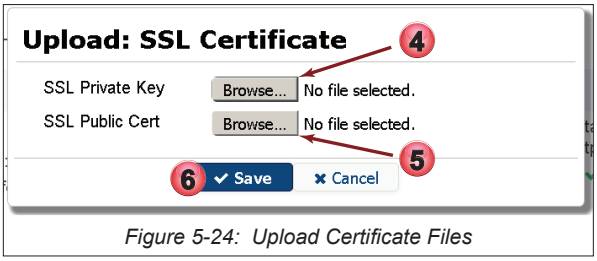

Figure 5-24: Upload Certificate Files

5.2.8 Create or Edit VLAN

Your application may require a management VLAN to allow remote Monitoring Server management. We will show here how to create a management VLAN on the interface eth0 on the Server. We do not explain all the steps required to set up a VLAN system on your equipment.

Procedure

This procedure explains how to configure a VLAN on the Monitoring Server. We do not include configuration of the far end switches or your equipment.

1. Click the **System** Tab if it is not already selected, Figure 5-25.
2. Click **Configure Network** under Network Configuration section.

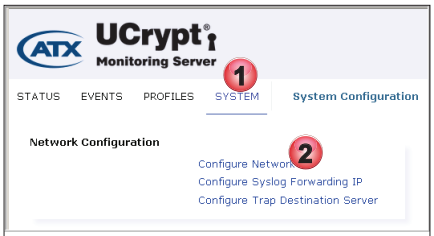

Figure 5-25: Configure Network

3. Click **+VLAN** on the eth0 interface to add a VLAN for remote Server management, Figure 5-26.

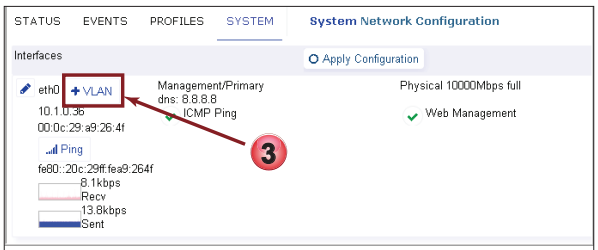

Figure 5-26: Add VLAN

4. Edit or fill in the VLAN settings form, Figure 5-27, according to Table 5.2a and your system requirements.
5. Click **Save** when finished.

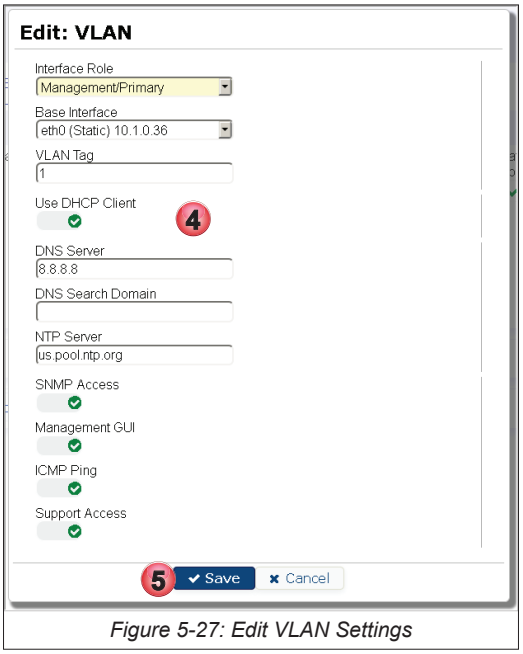

Figure 5-27: Edit VLAN Settings

Table 5.2a: VLAN Settings (See Figure 5-27)

Field	Configurable	Value
Interface Role	Dropdown Menu	Management/Primary. Other options are available which should not be selected if you are setting up a VLAN for remote management.
Base Address	Dropdown Menu	Base address on which VLAN will operate.
VLAN Tag	Integer	802.1Q VLAN Tag identifier to apply to the connection.
Use DHCP Client	Tick Box/Switch	Un-Ticked (Grayed out) for static IP address, ticked (checked) for DHCP.
DNS Server	IP Address	An external DNS server which can resolve URLs.
DNS Search Domain	URL/IP Address	The DNS search domain as required by your network.
NTP Server	URL/IP Address	An accessible external NTP server to synchronize clock time on the Monitoring Server.
SNMP Access	Tick Box/Switch	Tick to allow SNMP messages on this interface. If enabled, the SNMP port will be enabled on this interface.
Management GUI	Tick Box/Switch	Ticked to expose UI ports on this interface. Must be active on at least one interface.
ICMP Ping	Tick Box/Switch	Tick to enable ping response on this interface.
Support Access	Tick Box/Switch	If enabled, the support (ssh) port will be enabled on this interface; note it is strongly encouraged to leave this enabled on at least one interface.

6. A VLAN is added to Interfaces with a name such as eth0.1 but is not yet activated, Figure 5-28.
7. Click **Apply Configuration** button to activate changes.
8. If it is required to edit any existing interface, click the **Edit Icon** for the interface.
9. Created VLANs may be deleted by clicking the red **X** icon.

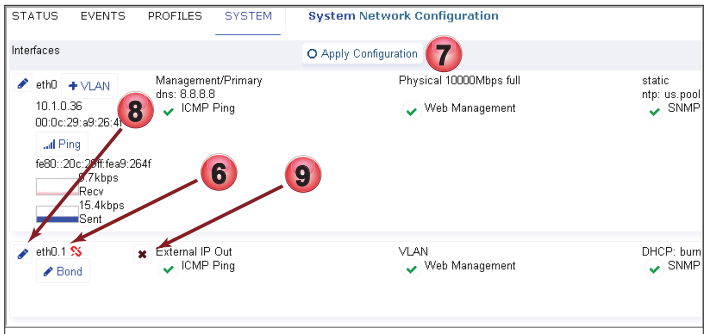

Figure 5-28: VLAN is Added to Interfaces

5.3 Syslog Forwarding

This feature is required if a firewall exists between monitored UCrypt Servers and the Monitoring Server. In this case you may specify that syslogs received from monitored UCrypt Servers are forwarded to the firewall or router IP address. The firewall or router will then need to have UDP port 10514 forwarded to the Monitoring Server. The IP address specified here will be used to inform all monitored UCrypt Servers to send their syslog reports to this address instead of directly to the Monitoring Server.

Procedure

This procedure explains how to set up a syslog forwarding IP address.

1. Click the **System** tab if it is not already selected, Figure 5-29.
2. Click **Configure Syslog Forwarding IP** under Network Configuration.

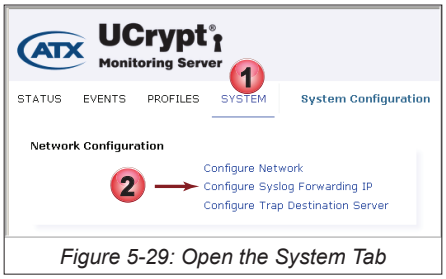

Figure 5-29: Open the System Tab

3. The **Syslog - Forwarding Network Configuration** page opens and announces the current forwarding address, see Figure 5-30. In this example no forwarding is configured as the Monitoring Server address is shown.
4. Enter the IP address of the firewall or router. If the forwarding address is already set, then to end this forwarding feature, select the detected internal IP address of the Monitoring Server.
5. Click **Save** to apply this new setting. Remember to configure the router or firewall to forward UDP port 10514 to the Monitoring Server.

Click the **System** tab to return to the System page or click any other tab to continue configuration.

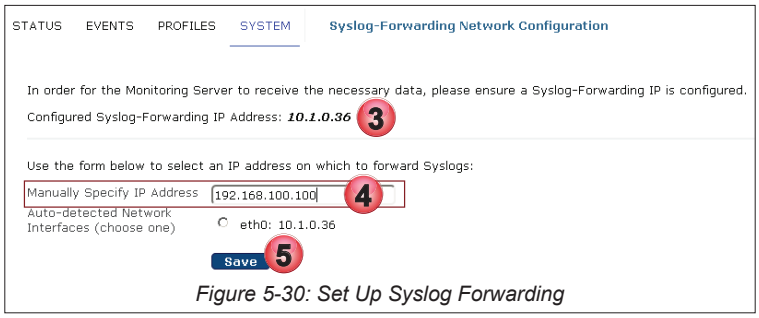

Figure 5-30: Set Up Syslog Forwarding

5.4 Configure SNMP

You may configure the Monitor Server to send SNMP traps Northbound to a management server. A MIB is available to download from the configuration page.

Procedure

This procedure explains how to configure SNMP trap destination settings.

1. Click the **System** tab if it is not already selected, Figure 5-31.
2. Click **Configure Trap Destination Server** under Network Configuration section.

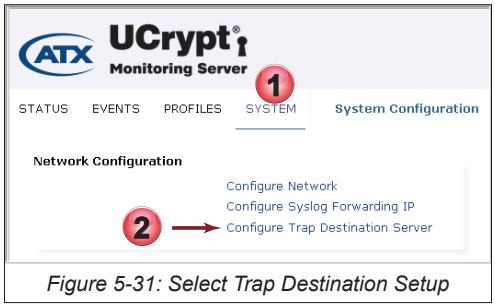

Figure 5-31: Select Trap Destination Setup

3. The **SNMP Trap Configuration (Northbound)** page opens, see Figure 5-32.
4. Click the **Download Monitoring Server MIB** link to save a copy of the MIB then compile the MIB into your system management server. We do not provide specific information about compiling MIBs into your system in this document.
5. Enter appropriate values for your system in the form using Table 5.4a for guidance.
6. Click **Save** to apply the changes made on this form.

Click the **System** tab to return to the System page or any other tab to continue configuration.

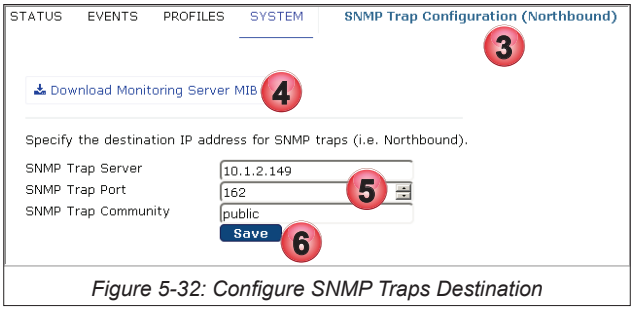

Figure 5-32: Configure SNMP Traps Destination

Table 5.4a: SNMP Trap Configuration (See Figure 5-32)

Field	Value	Description
SNMP Trap Server	IP Address	The management server IP address to which to send SNMP traps.
SNMP Trap Port	Integer	Defines the SNMP Port number. Default is 162.
SNMP Trap Community	Button	SNMP Community for the trap server.
Save	Button	Saves and applies any changes made on this form.

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

5.5 User Configuration

All technicians who will be on duty to receive Alert messages by email and respond to problems should be included individually in the user database. Use the LDAP configuration to add users. Use this section to view users that have been added through LDAP. Users are not actually configured here, they are configured within LDAP.

Procedure

This procedure outlines steps to view configured users previously done through LDAP.

1. Click the **System** tab if it is not already selected, Figure 5-33.
2. Click **Configure Users** under the User Authentication section.

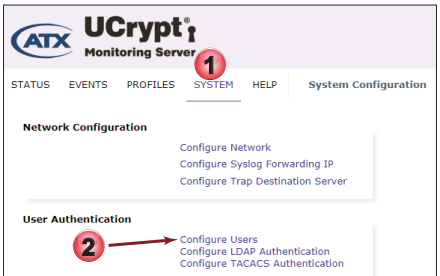

Figure 5-33: Open User Configuration

3. The User Accounts page opens, see Figure 5-34.
4. View existing users that have been previously configured within LDAP.

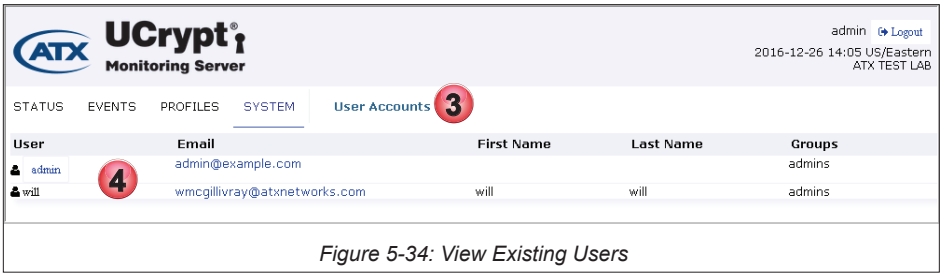

Figure 5-34: View Existing Users

5.6 LDAP Authentication Configuration

All users for the Monitoring Server must be added through LDAP (Lightweight Directory Access Protocol). To access the LDAP configuration follow this procedure.

Procedure

This procedure outlines steps to configure the LDAP to register users of the Monitoring Server.

1. Click the **System** tab if it is not already selected, Figure 5-35.
2. Under the User Authentication section, click **Configure LDAP Authentication**.

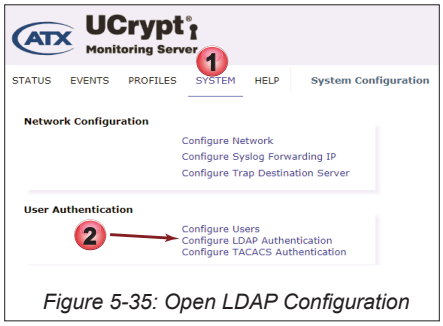

Figure 5-35: Open LDAP Configuration

3. The User Accounts page for configuring LDAP opens, see Figure 5-36.
4. Enter the LDAP configuration by completing the form.
5. Click **Save LDAP Settings**.
6. Click **Check Connection**.
7. The Monitoring Server connects to the LDAP server and confirms established connection by displaying the **Connection Established** ✔ Connection Established indicator.
8. Select the **Local Groups** that an LDAP group maps to by checking the corresponding checkbox. Note that LDAP users who belong to groups that are NOT mapped to local groups will be unable to login to the Monitoring Server. This setting is saved automatically when ticked/unticked.
9. You can view the currently configured Users by clicking Configure Users. There are no configuration controls on that page.
10. When finished, click **Back to System Page**.

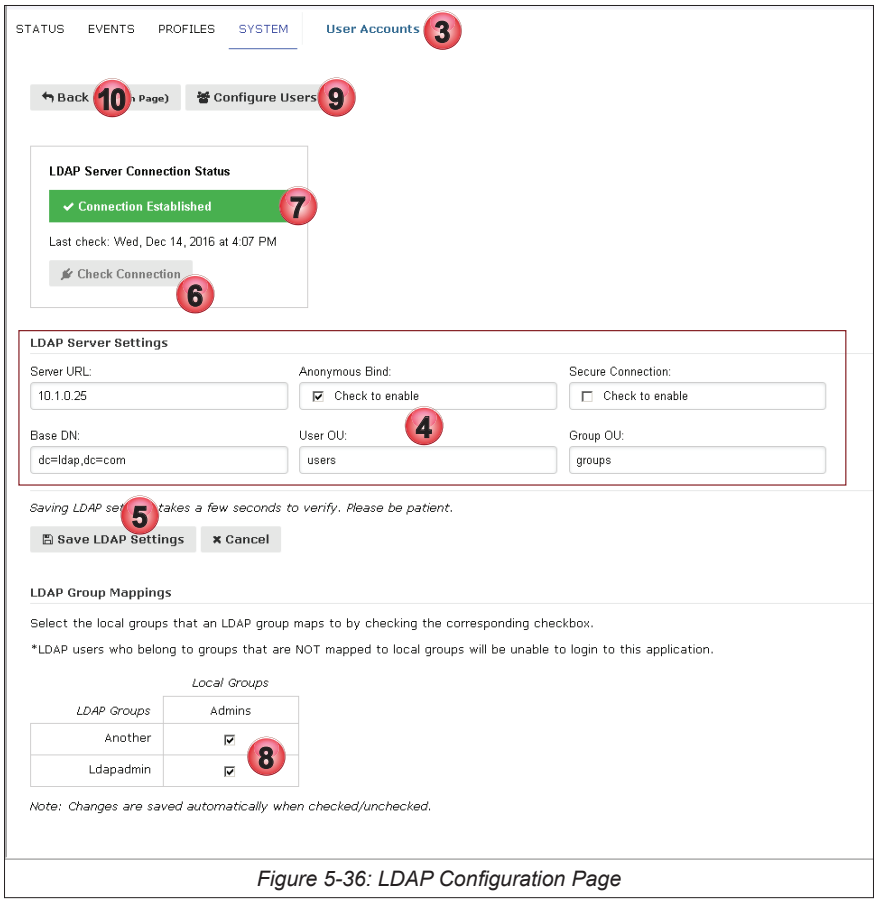

Figure 5-36: LDAP Configuration Page

5.7 Configure TACACS+ Authentication

Terminal Access Controller Access-Control System (TACACS, usually pronounced like tack-axe) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server(Wikipedia). Use of TACACS+ for user access allows more fine grained control of user permissions.

Procedure

This procedure outlines steps to activate and edit TACACS+ Settings.

1. Click the **System** tab if it is not already selected, Figure 5-37.
2. Click **Configure TACACS Authentication** under the User Authentication section.

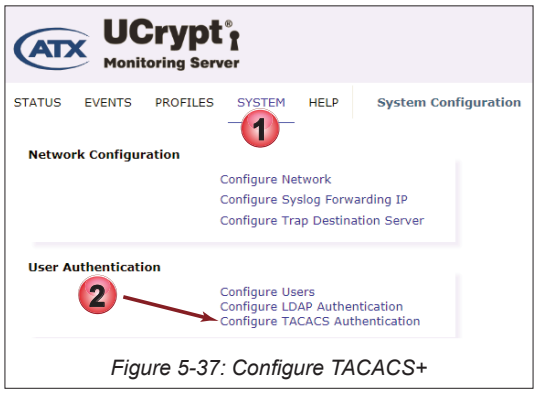

Figure 5-37: Configure TACACS+

3. The **Configure TACACS+ Server** page opens, see Figure 5-38. To activate TACACS+ click the tick box.
4. Enter the TACACS+ Server IPv4 address, Port and the Secret(the shared secret(password) used to authenticate using the TACACS+ Server). If the secret contains spaces, enclose the whole secret within quotes. You may click the **EYE** icon or **Show Secret** to view the secret password, otherwise it is hidden.

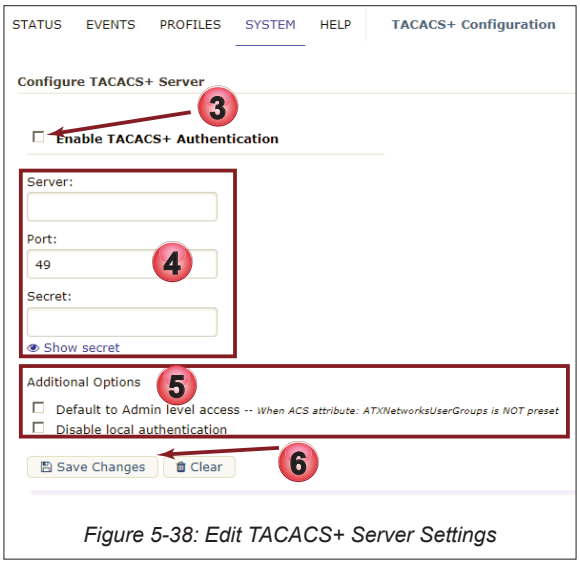

Figure 5-38: Edit TACACS+ Server Settings

5. Additional options are available:
   a) Default to Admin Level Access:

      Tick to cause a default to admin level access when ACS (Access Control System) attribute 'ATXNetworkUserGroups' is not present.

      NOTE: ATXNetworksUserGroup (an ACS attribute) is referencing a custom attribute within an ACS shell profile. If a user logs in and they are not part of the specified custom attribute, in this case 'ATXNetworkUserGroup' which values include admins,masters,tacacsadmin then the server defaults to admin level access.

b) Disable Local Access

Tick to disable local user/password authentication. THis stops any user from logging in to the Server outside of TACACS+ authentication.

6. Click **Save Changes** when finished making changes to apply those changes to the server. You may also click the Clear button to clear all settings back to factory default then click **Save Changes**.

5.8 Location

This section, Figure 5-39, allows setting the time zone for the machine as well as a friendly name for positive identification while logged in.

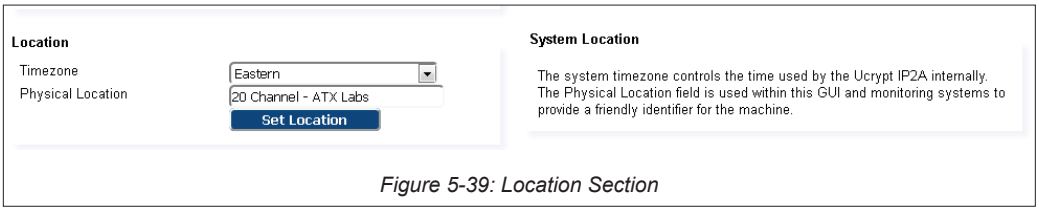

Figure 5-39: Location Section

5.8.1 Timezone

Setting the Timezone will result in accurate time being displayed in logs and in the UI. Time will be taken from an NTP (Network Time Protocol) server. The NTP server is internally predefined but may also be changed by entering a new URL on any of the network interfaces that have access to an NTP server. Access that by editing each/any interface that has access to an NTP server, see “5.2.2 Edit a Network Interface” on page 5-3.

5.8.2 Physical Location

The system timezone controls the time used by the Monitoring Server internally. The Physical Location field is used within this GUI and monitoring systems to provide a friendly identifier for the machine for its location which is displayed in the header when logged in. This name will help to positively identify the unit being worked on.

Procedure

This procedure explains how to configure the Location information for display within the UCrypt Server GUI.

1. Click the **System** tab if it isn’t already selected, Figure 5-40.
2. In the **Location** section, enter a **Friendly Name** in the **Physical Location** window to identify the unit to the user when logged in. There is no limit to the number of characters as the line extends across the header to accommodate the text string.
3. Click **Set Location**.
4. The name will be displayed in the header when logged into the Monitoring Server.

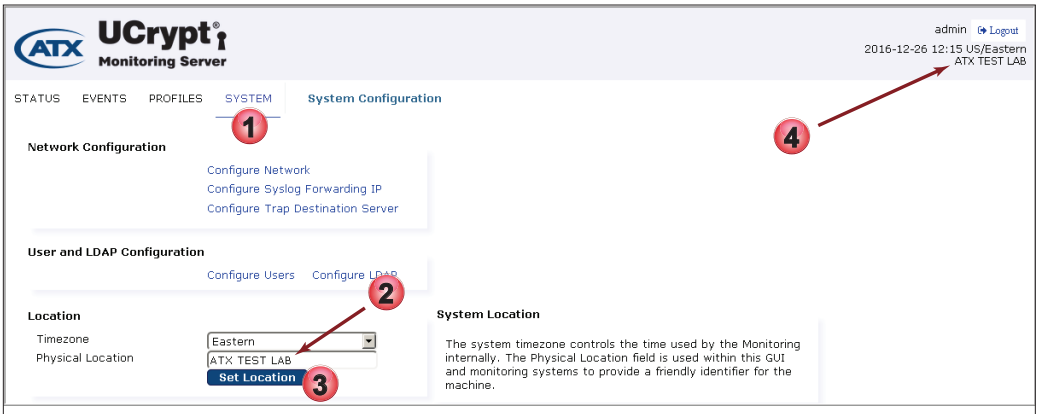

Figure 5-40: Set Friendly Location Name

5.9 Current Date

The date within the Monitoring Server GUI is kept current by use of NTP (Network Time Protocol) but you may choose to override that here if there is no time server accessible.

Procedure

This procedure explains how to override the time and date for the UCrypt Monitoring Server.

1. Click the **System** tab if it isn't already selected, Figure 5-41
2. If it is necessary to change the time on the Monitoring Server use the format **YYYY-mm-dd HH:MM:SS** As an example for **May 26 2016 11:40 AM** enter **2016-05-26 11:40:00**
3. Click **Set Current Time.**
4. If an incorrect time and date is entered, there may be a discrepancy reported in the entered time against the time and date on your management PC which will manifest itself as the Time and Date being shown in red, Figure 5-53. In this case adjust the entered date to the correct date and time.

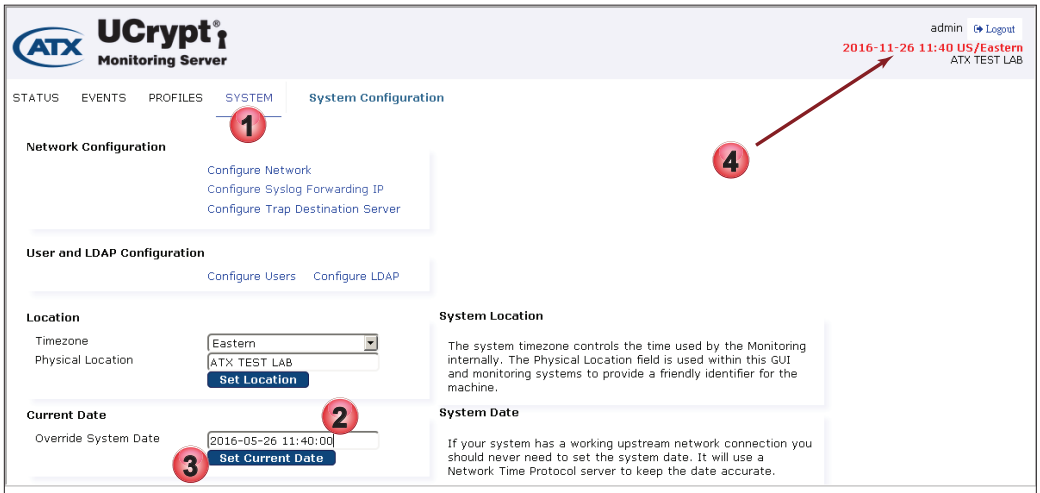

Figure 5-41: Set Date & Time

5.10 Power Management

Power management features such as such as Reboot, Shutdown, Power Cycle and Periodic Reboot are accessed here, Figure 5-42. Table 5.10a summarizes the controls and settings configuration.

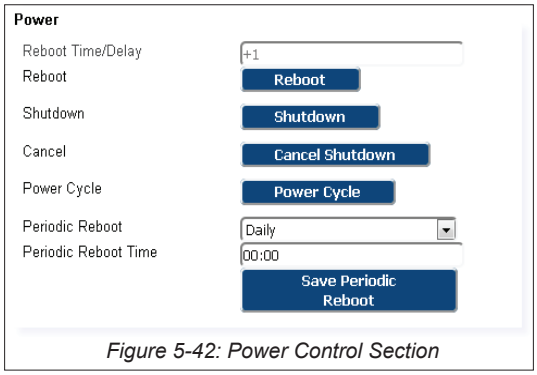

Figure 5-42: Power Control Section

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

Table 5.10a: Power Section Configuration (See Figure 5-42)

Field	Value	Description
Reboot Time/Delay	Integer	If specified the reboot will occur at this time specified in local server time as HH:MM (24Hr) or +MM (minutes in the future). Default is **1 minute** in the future.
Reboot	Button	Reboots the Monitoring Server with a warm boot.
Shutdown	Button	Schedule a shutdown to occur in **1 minute.** Power off the system until it is manually power cycled. This takes a unit out of service until field personnel arrive for a power recycle.
Cancel Shutdown	Button	Cancel pending shutdown or reboot if a shutdown was scheduled and it is decided to not allow follow through. This button immediately cancels the pending action.
Power Cycle	Button	This feature is not implemented on this Server. The Monitoring Server is a Virtual Machine.
Periodic Reboot	Dropdown	Enables periodic reboot of machine at frequency chosen: Disabled, Daily or Weekly(which will occur on Sunday).
Periodic Reboot Time	Integer	The system may be configured to perform a reboot at the time specified in the dialog box. Time must be entered in 24 hour format using HH.MM notation.
Save Periodic Reboot	Button	It is necessary to save the changes to the **Power** settings that were made. Failing to save the settings will result in the changes being discarded when navigating away from the System page.

5.11 System Status

Many Linux and hardware status parameters are presented in the System Status section, see Figure 5-43. Your system values will be different than those displayed here.

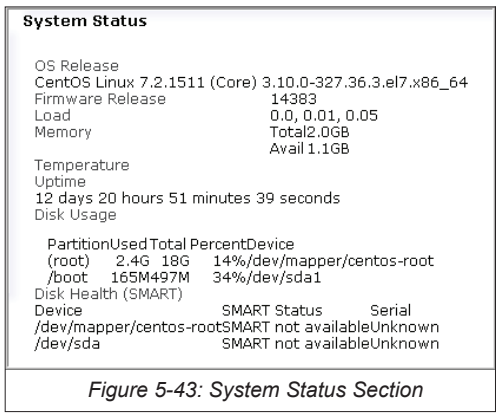

Figure 5-43: System Status Section

5.12 Firmware

The firmware version installed is reported here, Figure 5-44. Firmware upgrades, when available, are obtained from ATX Networks Technical Support group. Obtain the file and save it to your Management Computer before beginning the upgrade.

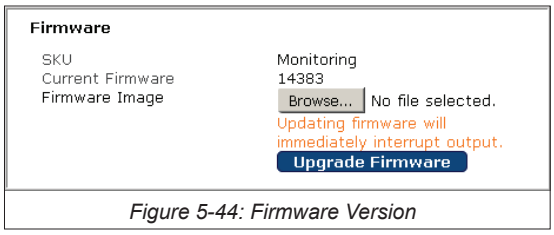

Figure 5-44: Firmware Version

5.13 Licence Server

Licensing servers issue license certificates which are valid for a few days at a time. Your Monitoring Server will download license certificates from the upstream licensing server every day. If you have an in-house licensing server you should provide its URL here.

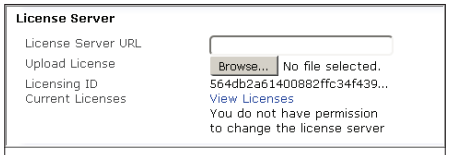

Figure 5-45: Licence Server

Contact ATX Networks Technical Support Group if you have concerns about the licence server settings.

5.14 Email Alerts

This form allows you to configure the SMTP account which will be used to send email from the system. You will likely want to create a special account solely for the use of this server. The configuration link changes to reflect the actual email that is configured as shown in Figure 5-46 and Figure 5-47.

Figure 5-46: Link to Configure Email Alerts

Figure 5-47: Email Alerts Link After Creation

Procedure

This procedure explains how to configure SMTP settings to enable email Alert messages.

1. Click the **System** tab if it isn't already selected.
2. In the **Email Alerts** section, click the **Create** link, Figure 5-48.

Figure 5-48: Link to Configure SMTP

3. Enter the SMTP parameters in the form. **Email Recipients** is used only for test purposes, enter the email address for the test message then delete this email address after testing is done. See Table 5.14a for guidance.
4. To test that the settings are correct, send a test message to the email address, click **Test**. When finished testing, delete the email recipient.
5. Click the **Save** button.

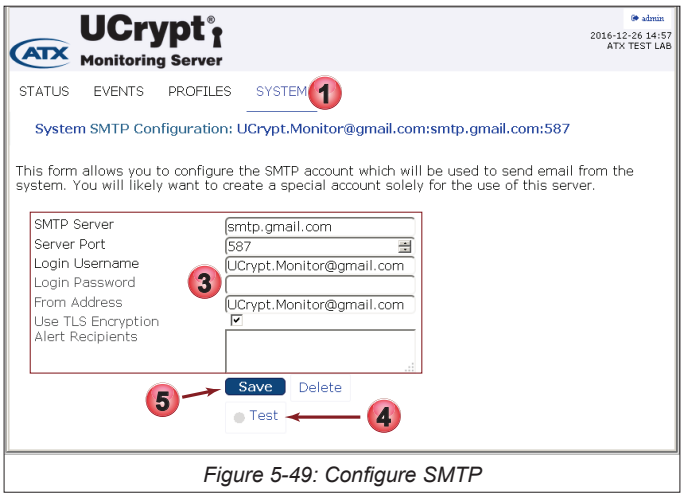

Figure 5-49: Configure SMTP

Table 5.14a: Email Configuration Form Settings (See Figure 5-49)

Field	Configurable	Value Entered
SMTP Server	String	Fully qualified domain name of the server to connect to i.e. mail.example.com
Server Port	integer	Port on which to connect; default is 25 for un-encrypted, 465 for encrypted connections. Use port 587 for Goggle email.
Login Username	String/Email address	The authentication address used to connect to the email server. i.e. example@example.com
Login Password	String	The authentication password used to connect to the email server.
From Address	String/Email address	The email address from which massages will be sent (your server may require this to match the account name.
Use TLS Encryption	Tick Box	Tick to use TLS encryption on this connection. Use this if supported by your email server.
Alert Recipients	String/Email address	Used only for test purposes, enter the email address for the test message then delete this email address after testing is done.
Save	Button	Click to save and apply changes.
Delete	Button/Link	Click to delete the account entered.
Test	Button	Click to send a test message to the recipient listed in the dialog “Alert Recipients’ using the configuration entered.

5.15 Monitoring Server Details

This section, see Figure 5-50, provides links to two Monitoring Server configuration pages as well as a link to the operating manual (the one you are currently reading).

5.15.1 Customize Acceptable Software

The firmware for your base of installed remote Devices may be updated from time to time. This tool aids in keeping remote Device firmware updated by notifying technicians of machines that have not been updated. To ensure that you are notified of outdated firmware, enter the acceptable firmware version for each product in your fleet in the provided form.

Procedure

This procedure explains how to set up the Acceptable Firmware versions page.

1. Click the **System** tab if isn’t already selected.
2. In the **Monitoring Server Details** section, click the **Customize Acceptable Firmware** link , Figure 5-50.

Figure 5-50: Customize Acceptable Firmware

3. On the **Customize Acceptable Firmware** page that opens, enter the applicable firmware versions adjacent the models of monitored Devices in service in your systems, Figure 5-51. You can get these version numbers from ATX Networks Technical Support or directly from firmware files provided by ATX Networks. If using the firmware file, use the entire number less any extensions that are part of the file name.
4. Click **Save** to apply the changes.
5. Click **Back to System Page** to proceed back to the System page.

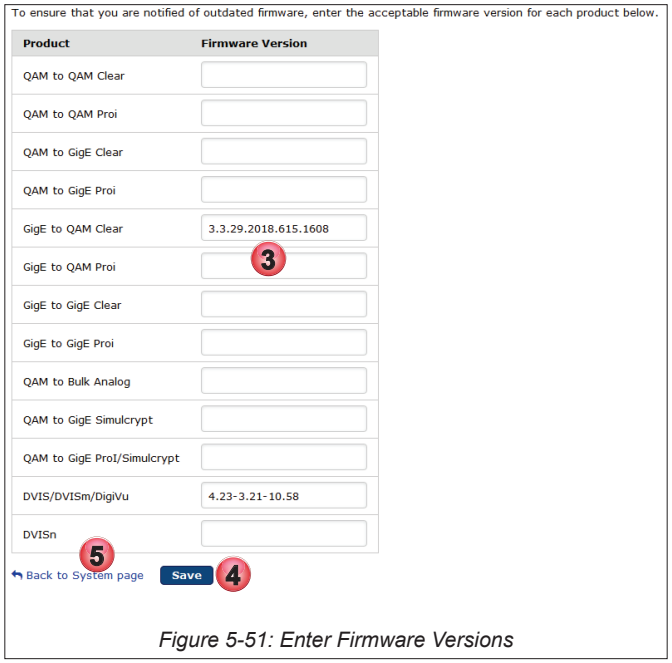

Figure 5-51: Enter Firmware Versions

6. In the event of a mismatch between installed and acceptable versions, a warning will be displayed adjacent the Device with the mismatch, Figure 5-52. The entered number is compared to the firmware version number installed in each machine and must match exactly, so even a typo may cause a mismatch error.

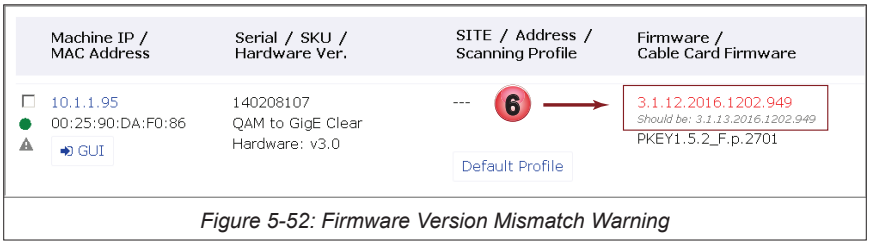

Figure 5-52: Firmware Version Mismatch Warning

5.15.2 Customize MSO Fields

MSO fields are the Monitored Device Identification column headings, highlighted in Figure 5-53, found in the Servers (Monitored Devices) list on the Status Page. The highlighted fields may be changed to suit specific needs and terminology. Procedure to change these fields is found at “2.6.1 Customize MSO Fields” on page 2-12.

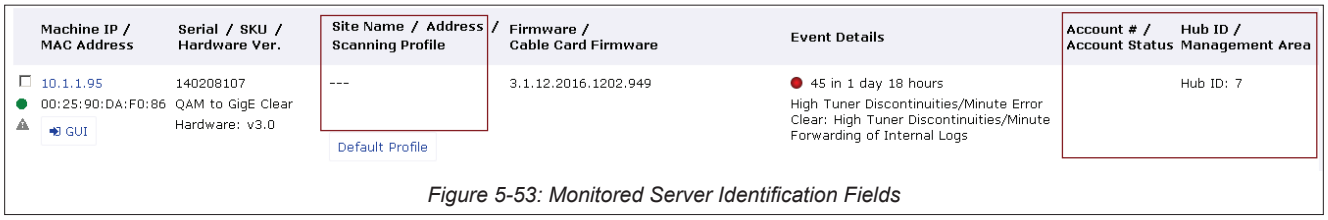

Figure 5-53: Monitored Server Identification Fields

5.16 User Guides and Documentation

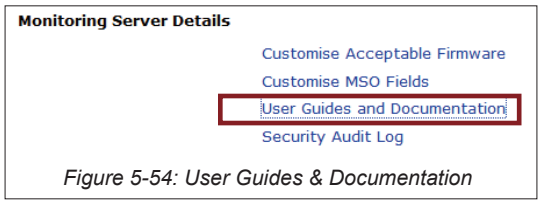

Figure 5-54: User Guides & Documentation

This link connects to a page that provides further links to all published documentation for products supported on this platform, Figure 5-55. Click any of these links to go directly to online ATX documentation.

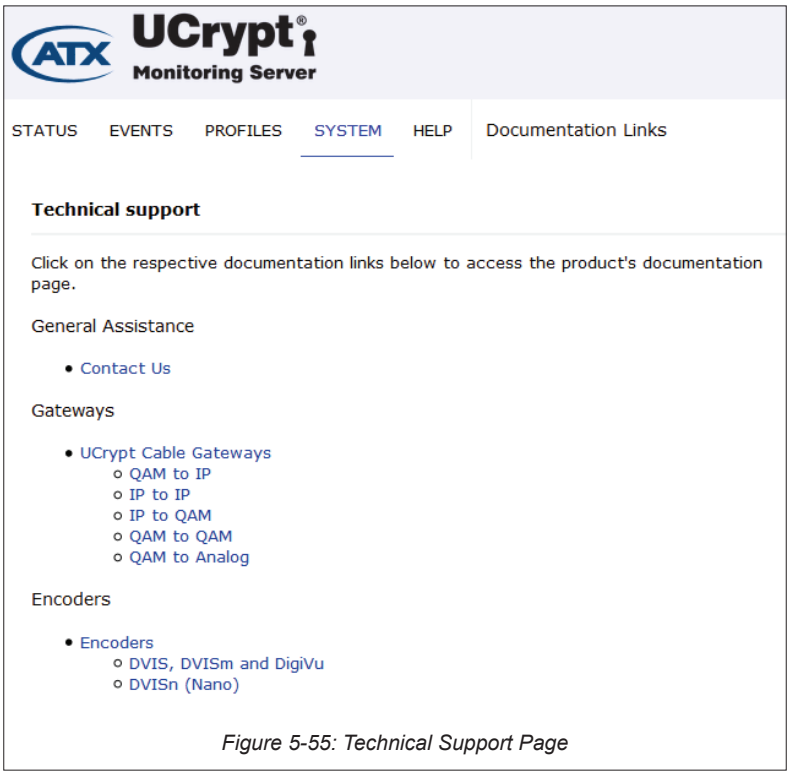

Figure 5-55: Technical Support Page

5.17 Data Management

This section provides for bulk addition of UCrypt Servers as well as backup and restoration of the Monitoring Server database.

Figure 5-56: Data Management Section

5.17.1 Import/Export Server Records

To enable bulk addition of remote Devices to the Monitoring Server you may upload a CSV (Comma Separated Values) file which lists the servers to be added. This method may be used initially to add servers or later to add additional servers. The file must be in a very specific template format so there is a facility to allow downloading the template.

Procedure

1. Click the **System** tab if it isn't already selected.
2. In the Data Management section, click the link **Import/Export Server Records**, Figure 5-57.

Figure 5-57: Data Management Section

3. Click the **Download CSV Template** link to get a copy of the required template, Figure 5-58. Save the file to your PC.

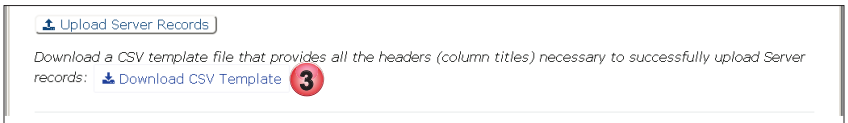

Figure 5-58: Click Download Template Link

4. Open the template file as a spreadsheet and under 'ip' enter the **IP addresses** of the emote Devices, Figure 5-59.
5. Under 'product' enter **ucrypt** for each UCrypt Server or **dvis** for DVIS and DigiVu equipment then **Save** the spreadsheet file. These are the only entries required.

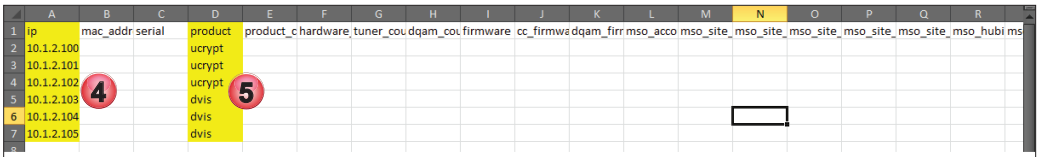

Figure 5-59: Completed Template Entries

6. In the Upload Server Records section, click **Browse**, Figure 5-60.

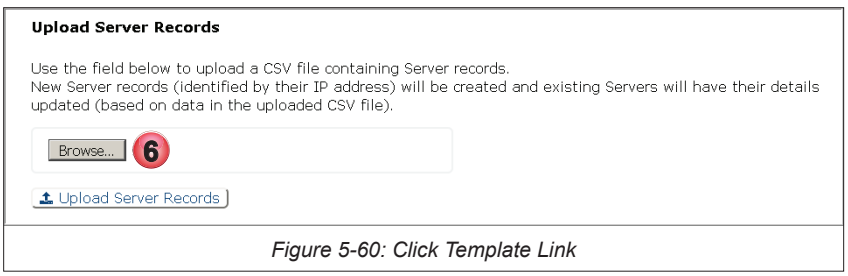

Figure 5-60: Click Template Link

7. Select the spreadsheet file saved earlier in your file explorer window, Figure 5-61.
8. Click **Open** (your browser may display this differently).

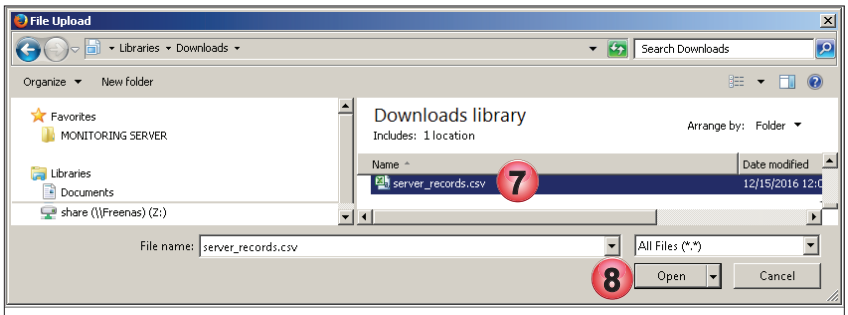

Figure 5-61: Select Server Records File

9. The selected file will be displayed beside the browse button, Figure 5-62.
10. Click the **Upload Server Records** button.

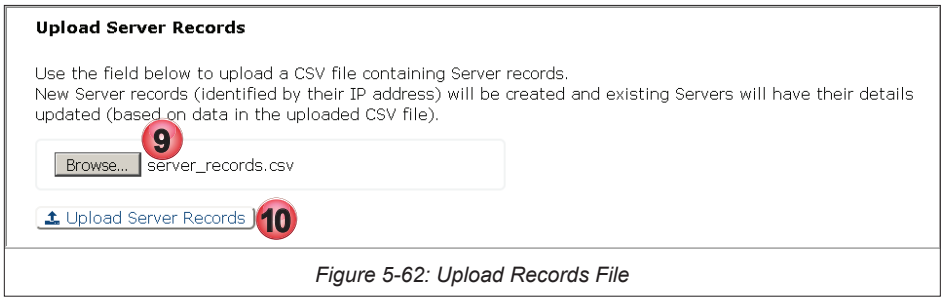

Figure 5-62: Upload Records File

11. A confirmation page displays results, Figure 5-63. Added servers will be listed in green.
12. Servers that cannot be reached or cannot be added will have errors listed in red with the reasons they could not be added and possible solutions.
13. Click **Back to System Page** to return to configuration.

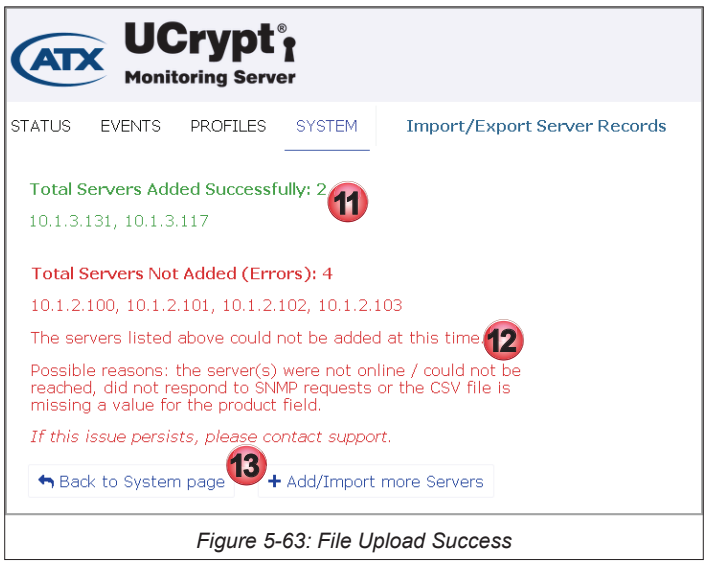

Figure 5-63: File Upload Success

5.17.2 Backup and Restore Database

It is always good to have a backup of the Monitoring Server database available and therefore backups are done automatically without any user intervention.

The backup file will remain on the Monitoring Server and may be manually downloaded to your PC along with an optional MD5 checksum file for verification if desired. We recommend saving the backup file to an external storage device such as your PC since restoring the database will require the file to reside outside the Monitoring Server. A backup made on schedule will be uploaded to an ftp server.

Procedure

This procedure explains how to create a one time backup on the spot.

1. Click the **System** tab if it isn't already selected.
2. In the **Data Management** section, click the **Backup and Restore Database** link, Figure 5-64.

Figure 5-64: Backup and Restore Database

3. On the **Backups** page that opens, click the **Backup Now** button, Figure 5-65.

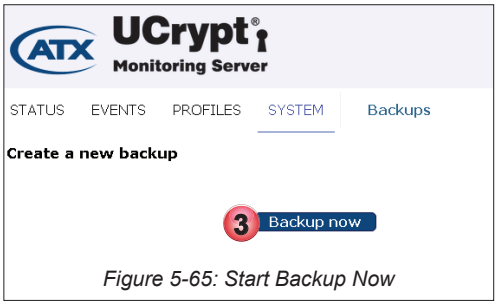

Figure 5-65: Start Backup Now

4. A new backup is created without further announcement and is added to the list of **Existing Backups** further down the page, Figure 5-66. Click the **file link** to download the backup file to your computer.
5. Each date stamped backup file has an accompanying MD5 checksum file to verify integrity. Click the **file link** to download the MD5 file to your computer.

Procedure to Restore a Backup

6. After first saving the backup files to your computer, click the labeled **Browse** buttons to select the saved files on your computer or external drive, Figure 5-66. Selecting the MD5 file is optional but recommended to ensure file integrity.
7. Click the **Restore** button to begin the database restoration.

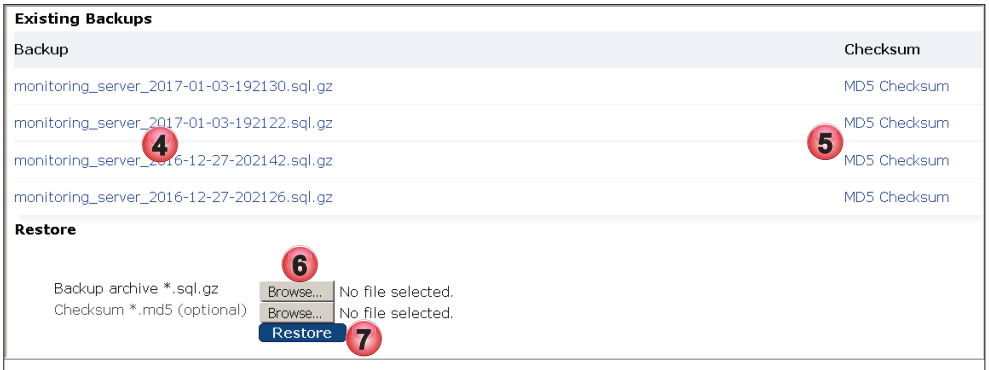

Figure 5-66: Backup Files with MD5

Scheduled FTP Backups

Backup of the Monitoring Server database may be scheduled to be completed and uploaded to an FTP server on a flexible schedule. A standard password protected FTP server must be available to receive these files.

Procedure

This procedure explains how to set up a scheduled backup. The Monitoring Server will need access to an FTP server.

1. Click the **System** tab if it is not already selected.
2. Click the **Backup and Restore Database** link, Figure 5-67.

Figure 5-67: Data Management Section

3. From the Scheduled FTP Backups page, tick the **Enable Scheduled Backups** tick box, Figure 5-68.
4. With the dropdown menus, select the backup **Frequency** and **day of the week** (if weekly was selected).
5. Enter the **Periodic Backup Time** in 24hr notation, HH:MM.
6. Enter the **FTP Host** address and login credentials.
7. Click **Save FTP Configuration** button to apply the configuration. The Monitoring Server will attempt to contact the FTP server and will confirm success or failure of the connection. If the connection fails, the FTP Server information entered will not be saved.

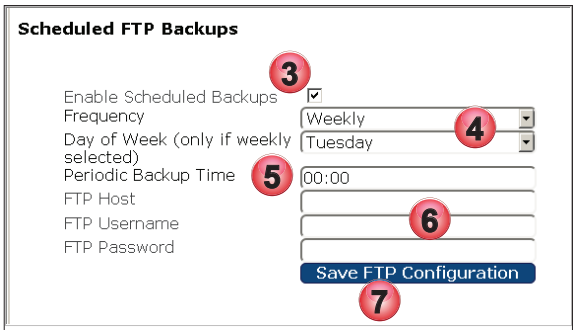

Figure 5-68: FTP Backup Setup

REMOTE DEVICE ALERTS

6. Remote Device Alerts

Alerts generated by UCrypt, DVIS and DigiVu Devices are included here in a condensed form for convenience and reference only. These same Alerts are also found in the operation manual for your product.

6.1 Chapter Contents

6.2 DVIS HD/SD Issue

6.2.1 Refers to

A detected problem with an encoder input card. The input cards can develop problems that may be detected.

6.2.2 Repetition of Alert

Alert is sent only once per event, that is, if an input card problem or failure is detected, only one alert is sent. Is the problem remits, then another alert will be sent if it occurs again.

6.2.3 Urgency

Critical.

6.2.4 Probable Causes

1. An input card has failed.
2. An input card needs to be re-seated in its slot.
3. Device plugged into card (DVD Player, computer, etc) may be not plugged in, or could be turned off.
4. DVIS not receiving video signal.

6.2.5 Next Steps

1. Re-seat card.
2. Replace card.
3. Confirm device connected to input port is operational and cables are secure.

6.3 DVIS Fan Error

6.3.1 Refers to

The failure of external cooling fans of the DVIS Device. The DVIS contains number of fans installed on the front panel to assure that the internal temperature is maintained at a level that will allow a long service life under almost all site conditions that could reasonably be encountered. The DVIS is designed to continue to work efficiently with up to half of the fans in failed mode under normal room temperature ambient conditions.

6.3.2 Repetition of Alert

Alert is sent only once per event, that is, if a fan fails, an alert is sent, but no further notification is generated. Each fan is monitored and reported on independently. When a fan is replaced, the alarm condition for that fan is automatically remitted, then the DVIS will again send a failure alert if/when that specific fan fails again.

6.3.3 Urgency

Low.

6.3.4 Probable Causes

1. A DVIS external cooling fan has failed.

6.3.5 Next Steps

1. Check for how many fans are in failure mode. If this is the first failed fan, no immediate action need be taken. The equipment should operate normally with only 2 of 4 installed fans active under normal room temperature ambient conditions. If ambient temperature around the DVIS is expected to remain under 80°F (27°C), then just replace the fan on the next site visit.
2. If 2 fans have failed and the ambient room temperature will remain below 80°F (27°C), then the fans should be replaced as soon as possible but this should not require an immediate visit.
3. If more than 2 fans have failed and the ambient room temperature could exceed 80°F (27°C), then the fans should be replaced as soon as possible.

6.4 UCrypt Temperature Error

6.4.1 Refers to

The internal operating temperature of the UCrypt CPU Cores. The Mainboard CPU(s) core temperatures are monitored. The alert threshold is at a core temperature of 167°F (75°C) which reflects an ambient air temperature surrounding the UCrypt of about 107°F (42°C). Due to normal variabilities, these specified temperatures might be slightly different.

6.4.2 Repetition of Alert

Alert is sent only once per event, that is, if the temperature rises above the threshold and stays there, no further alerts will be sent. If the temperature drops below the threshold then raises again above the threshold, the alert is resent when the temperature again exceeds the threshold.

6.4.3 Urgency

Critical.

6.4.4 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

This alert is generated when the ambient air temperature is nearing the critical level where the equipment may fail due to inability to keep the CPU cool enough. The UCrypt is designed to operate to published specifications at temperatures between +32°F and +122°F (0°C and 50°C). At elevated temperatures, the UCrypt will continue to operate but the lifetime of the equipment is likely to be reduced. This alert is warning that the UCrypt is operating at temperatures higher than it is specified to operate at. If this alert is received multiple times over several days it may indicate a recurring temperature problem in the room where the equipment is installed. Knowledge of the ambient conditions of the installation will help to judge if physically attending to the UCrypt immediately is justified.

An Internal Issue

This alert could be generated when external UCrypt cooling fans have failed. If this is the case, there will be fan failure alerts as well. The UCrypt can operate with up to 2 failed fans under normal room temperature ambient conditions of about 72°F (22°C) but if ambient temperatures are elevated, all fans will be needed.

6.4.5 Probable Causes

1. External equipment fans have failed (check for fan errors on ‘System’ page under ‘Health’).
2. External ambient air temperature is above 122°F (50°C).

6.4.6 Next Steps

1. Check for Fan Errors on ‘System’ page under ‘Health’ (See also next section: Fan Errors). If fans have failed then this may explain the high temperature error. The UCrypt is capable of normal operation with only 2 of the 4 installed fans active under normal room temperature ambient conditions. If ambient temperature around the UCrypt is under 122°F (50°C), then just replacing the fans should correct the problem.
2. If fans have not failed, then check the ambient room temperature where the equipment is installed. If ambient temperature around the UCrypt is over about 122°F (50°C), then try to solve the problem of high ambient room temperature.
3. Install additional cooling if the room temperature above 122°F (50°C) persists.

6.5 UCrypt Fan Error

6.5.1 Refers to

The failure of external cooling fans of the UCrypt. The UCrypt contains four or more fans installed on the front panel to assure that the internal temperature is maintained at a level that will allow a long service life under almost all site conditions that could reasonably be encountered. The UCrypt is designed to continue to work efficiently with up to 2 failed fans under normal room temperature ambient conditions.

6.5.2 Repetition of Alert

Alert is sent only once per event, that is, if a fan fails, an alert is sent, but no further notification is generated. Each fan is monitored and reported on independently. When a fan is replaced, the alarm condition for that fan is automatically remitted, then the UCrypt will again send a failure alert if/when that specific fan fails again.

6.5.3 Urgency

Low.

6.5.4 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

This alert is not caused by outside influences.

An Internal Issue

This alert is generated when an external UCrypt cooling fan is detected to have failed. Only one notification will be sent per failed fan occurrence.

6.5.5 Probable Causes

1. A UCrypt external cooling fan has failed.

6.5.6 Next Steps

1. Check for how many fans are in failure mode. If this is the first failed fan, no immediate action need be taken. The equipment should operate normally with only 2 of 4 installed fans active under normal room temperature ambient conditions. If ambient temperature around the UCrypt is expected to remain under 80°F (27°C), then just replace the fan on the next site visit.
2. If 2 fans have failed and the ambient room temperature will remain below 80°F (27°C), then the fans should be replaced as soon as possible but this should not require an immediate visit.
3. If more than 2 fans have failed and the ambient room temperature could exceed 80°F (27°C), then the fans should be replaced as soon as possible.
4. The urgency may be further judged by the occurrence of a Temperature Error alert. If multiple fans have failed and there is a temperature alert, the replacement of fans should be attended to as soon as possible to avoid the equipment failing catastrophically.

6.6 UCrypt EAS Event

6.6.1 Refers to

Reception of an event related to the Emergency Alert System (EAS). Each EAS event will be reported as an alert without details as to the specific nature of the EAS event. An official test of the EAS system will be reported with the same alert as a real EAS event.

6.6.2 Repetition of Alert

Alert is sent only once per EAS event. No further notification is generated.

6.6.3 Customer Symptoms

Customer experiences loss of regular programming for duration of EAS event. Customer may receive substitute programming consisting of force tune Details Channel or text message for the duration of the event.

6.6.4 Urgency

Informational purposes only.

6.6.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

This alert is generated when the EAS event is received via the OOB carrier or Inband if applicable. Expect this alert to be sent with every test of the EAS system.

An Internal Issue

There are no internal issues that will cause this alert.

6.6.6 Probable Causes

1. An EAS event message has been received.

6.6.7 Next Steps

1. There is no need for any action to be taken for this alert. The alert is informational only.

6.7 UCrypt Channel Map Update Exception

6.7.1 Refers to

The inability of the UCrypt to accommodate a program move as required by a channel map update. The Channel Map is also known as the Virtual Channel Table and is transmitted by the Cable Service Provider on the OOB carrier to inform the system STBs of the current location of each program carried on the cable system. This relates the “Cable Channel” to the EIA QAM channel and MPEG program number (the EIA Major and Minor Channel Numbers) of each service. The Channel Map is sent from time to time to reflect the moving of programs to different QAM channels etc. This alert will be sent if there are no available tuners to acquire a QAM channel if the QAM channel was not previously being received. This will be a very rare event most likely to happen on a UCrypt where all available tuners must be used to process the desired programs and at least one tuner is processing multiple programs.

6.7.2 Repetition of Alert

Alert is sent once when a ‘program follow’ is not able to be accommodated. No further notification is generated until the issue is rectified and another instance of ‘failure to follow’ a program due to insufficient resources occurs again.

6.7.3 Customer Symptoms

Customer experiences loss of the program affected by the alert as there is no available tuner for the program. All remaining programming is unaffected.

6.7.4 Urgency

Critical.

6.7.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

This alert is generated when the Channel Map Update is received and there are not enough tuners to receive the required number of QAM channels. This further indicates that a previously tuned and received program was lost due to insufficient

tuner resources.

An Internal Issue

This alert is not generated by any internal issues or conditions other than the lack of sufficient installed tuners.

6.7.6 Probable Causes

1. During initial configuration, all available tuners were required to tune the desired lineup and now an additional unavailable tuner is required to continue to deliver the same lineup.

6.7.7 Next Steps

1. Analyze the occurrence of this alert with respect to the program specified as being affected and the changes in the most recent Channel Map Update (channel map update info will need to be acquired internally from system channel map administrators).
2. Have the channel that caused the error replaced back into a multiplex contained on one of the QAMs already tuned by the UCrypt in question.
3. Drop the affected channel from the lineup.
4. Upgrade the number of QAM tuners if the UCrypt in question has less than 60 tuners installed.

6.8 UCrypt CableCARD™ Module Entitlement Error

6.8.1 Refers to

A specific program on a specific CableCARD module does not possess an entitlement enabling it to be decrypted. Entitlement is necessary for a CableCARD module to decrypt programming therefore a loss of entitlement will result in a loss of that program on the UCrypt output. Each program must be authorized by the Cable Service Provider's billing system allowing it to be decrypted on a specific CableCARD/host slot pair. The Host is the physical slot that the CableCARD module is inserted into and the "slot" or "Host" itself has a unique identification number. The ID number from the Host and the ID number from the CableCARD are "paired" in the billing system. CableCARD modules may not be moved between UCrypt devices without re-pairing.

6.8.2 Repetition of Alert

This message is sent only once when it is determined that a specific CableCARD module no longer possesses entitlement to decrypt the associated program. If the card re-acquires entitlement, then looses it again, another alert is sent.

6.8.3 Customer Symptoms

Customer experiences loss of all encrypted programming on affected CableCARD module(s) for the duration that the error condition exists. All programming that arrives at the UCrypt in the clear as well as all programming on unaffected CableCARD modules is processed normally.

6.8.4 Urgency

Medium - Critical.

6.8.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

An occurrence of a CableCARD module losing entitlement with no outside influence is rare, though it may be possible. Usually the card re-acquires entitlement by itself and requires no action. A permanent loss of entitlement on a particular program most likely indicates an error in the billing system configuration and/or pairing process for that specific CableCARD module .

An Internal Issue

This alert is not generated by any internal issues or conditions.

6.8.6 Probable Causes

1. The CableCARD module has not been properly validated & authorized in the Cable Service Provider's Billing System.
2. The correct package with the program at issue has not been sent in the form of a 'hit' to the CableCARD module .
3. A previously paired CableCARD module has been removed from the billing system.
4. A previously authorized service has been changed or deleted in the billing system.
5. The CableCARD module's entitlement has expired prior to the card receiving an entitlement renewal message.
6. If entitlement has been restored since the alert, there was a temporary loss of entitlement by the CableCARD which

either rectified itself or required an automatic re-start of the CableCARD by the UCrypt equipment to rectify.

6.8.7 Next Steps

1. Check if the problem has corrected itself by checking ‘status’ of program in question on ‘Channel View’ page.
2. This problem may correct itself the next time entitlement messages are distributed on the network. The CableCARD entitlement per program normally expires after a time and is refreshed automatically. If the CableCARD module ID and Host ID are not setup correctly in the billing system there is a possibility the refresh does not happen as expected or required. There may be other issues that could potentially cause this within the billing system.
3. If this problem has not corrected itself, contact the Cable Service Provider’s administration to ensure that the CableCARD/host slot pair are properly recorded in the billing system. Find the CableCARD module and Host ID numbers by following paths:
   a) Cisco: CableCARD View>CableCARD Setup>Cisco CableCARD/Host ID screen.
   b) Motorola: CableCARD View>CableCARD Setup>CableCARD Pairing.

   Report the CableCARD module and Host ID numbers to your administrator.
4. Pay particular attention to the ‘DATA’ field in Cisco/SA environments as this field changes over time, but must be re-entered with the correct current data if a card is being re-validated or re-hit.
5. Have the administrator resend (Hit) the entitlement message to the CableCARD module.
6. Repeated problems with the same CableCARD may indicate a problem deeper within the DAC/DNCS which cannot be resolved by access at the billing system level. In this case, the assistance of a DAC/DNCS administrator may be necessary to completely remove the CableCARD module and host IDs from the DAC/DNCS inventory and re-enter it from scratch.
7. There is a problem with the physical CableCARD module and replacement may be necessary.

6.9 UCrypt Tuner Lost PCR Lock Error

6.9.1 Refers to

The loss of Program Clock Reference on a specific multiplex or QAM channel. PCR is required to process programs so it is necessary to maintain PCR lock at all times.

6.9.2 Repetition of Alert

This alert is sent once per event, so if PCR lock is lost and is reacquired, the alert will be sent again if/when it loses lock again. If lock is not reacquired, the Alert will not be sent again.

6.9.3 Customer Symptoms

Customer experiences loss of all programs on the affected tuner for the duration that the error condition exists.

6.9.4 Urgency

Medium - High.

6.9.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

It would be expected that during certain operations such as plant maintenance when disrupting a tuned QAM or an RF outage, the PCR lock would be lost. A loss due to a factor similar to this does not require any action as the UCrypt will regain lock when the QAM is properly restored. It could be considered normal to lose PCR lock occasionally if this does not reoccur repeatedly. The occasional loss does not require any attention.

An Internal Issue

Repeated occurrences of loss of PCR lock will require attention to determine the cause, which can be either internal or external to the UCrypt.

6.9.6 Probable Causes

1. The subject QAM was not available on the cable system at the time of the error.
2. Plant distortions make it difficult for the UCrypt tuner to maintain lock on the subject QAM.
3. Plant maintenance has been occurring at the time of the error.
4. An internal service affecting operation within the UCrypt (such as hitting ‘apply’ or reboot) was performed just prior to the alert.

5. Hardware tuner in the UCrypt equipment is failing.

6.9.7 Next Steps

1. Check if the program has corrected itself by checking ‘status’ of the program on ‘Channel View’ page and checking for indication of persisting PCR lock error message on ‘CableCARD View’ page.
2. Check if there was an ‘apply’ or ‘reboot’ performed just prior to the error message in the logs. If so, this is normal operation.
3. Consider if there was plant maintenance happening during the subject time period. Plant outages will cause this problem. Were there other alerts that occurred at the same time or were there many or all tuners affected at the same time indicating plant as the source.
4. Analyze if only one tuner board was affected or if all tuners were affected. If all were affected, the likelihood is that there was an external influence such as an outage or an internal operation such as a UCrypt system ‘apply’ or ‘reboot’ which causes this message to appear while the tuners are unlocked in the midst of the operation (which is normal and as per design).
5. Analyze if the signal levels at the UCrypt are in spec and if all QAM channels are flat in response.
6. If a single tuner is always affected in a similar way, and recurring alerts are reported over several days, this may indicate an external problem, so measure signal levels and MER to determine system performance ahead of the UCrypt on the affected channel.
7. If plant distortions and signal level problems have been eliminated, the UCrypt hardware tuner is likely failing.

6.10 UCrypt Lost OOB Lock Error

6.10.1 Refers to

The UCrypt has lost reception on the specified OOB carrier. There is an OOB carrier tuner on each CableCARD module / host slot port installed in the UCrypt. Your UCrypt may have between 1 and 10 OOB tuners installed depending on the ordered configuration.

6.10.2 Repetition of Alert

This alert is sent only once each time a specific OOB carrier loses lock. No further alert will be sent until the OOB carrier locks again in the tuner and then again loses lock.

6.10.3 Customer Symptoms

No symptom directly as a result of this error. Extended duration of this error could result in customer experiencing loss of all programs on the associated CableCARD module as the module eventually looses its entitlement.

6.10.4 Urgency

Medium.

6.10.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

If all tuners lose lock simultaneously this is almost certainly an indication of OOB impairment on the plant as it’s extremely improbable that all individual OOB tuners would experience hardware failures at the exact same time. This is usually caused by plant maintenance activities.

An Internal Issue

If just a single tuner board is losing OOB lock repeatedly, this is an indication of a potential hardware issue with that board since any impairment to the OOB on the plant side should affect all tuners equally.

6.10.6 Probable Causes

1. The subject OOB carrier was not available on the cable system at the time of the error.
2. Plant distortions make it difficult for the UCrypt tuner to maintain lock on the subject OOB Carrier.
3. Plant maintenance had been occurring at the time of the error.
4. Hardware tuner internal to the UCrypt equipment is failing.

6.10.7 Next Steps

1. Determine if multiple OOB carriers lose lock at the same time. Multiple carriers losing lock at one time may indicate external causes such as maintenance activities.

2. Note if the loss of lock occurs during maintenance windows indicating external causes.
3. Note if other alerts trigger at almost the same time, again indicating external causes.
4. A single loss on a specific tuner very occasionally or rarely may be considered normal.
5. Recurring losses of lock over time on a specific tuner may indicate a hardware problem especially if other tuners in the UCrypt equipment operate normally.

6.11 UCrypt High Tuner Discontinuities/Minute Error

6.11.1 Refers to

MPEG level packet loss at a specific QAM tuner (Tuner #0 to #5) on a specific Host card (Card #0 to #9). This is the packet loss related to a QAM multiplex and not a specific program within the multiplex. There may be bit error correction in the system but this problem is reporting uncorrectable bit errors resulting in packet loss as this is measured post error correction. This should always be zero under the best circumstances but some uncorrectable errors may still occur but are not visible in the picture up to about 500/minute, therefore the UCrypt will only begin to send alerts where the discontinuities exceed 200/minute.

6.11.2 Repetition of Alert

The UCrypt will send an alert each time there are more than 200 discontinuities recorded on a specific QAM in a one minute time frame.

6.11.3 Customer Symptoms

Customer experiences noticeable artifacts and/or other impairments starting at an error level of about 500 discontinuities/min, with impairments escalating with higher levels of discontinuities up to and including loss of all programs on the affected tuner for the most severe conditions for the duration that the error condition exists. The resulting customer experience will be both random and variable depending on the conditions causing the error and it is not possible to quantify them further.

6.11.4 Urgency

Low - High.

6.11.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

If the number of discontinuities is low (a few hundred per minute) and infrequently reported, this is considered normal as just about all cable plants experience some brief moments of signal impairment for a multitude of reasons. If the discontinuities are above 500/minute and occur frequently and across many QAM tuners, urgent attention is indicated as there are likely system problems with the level and/or signal quality hitting the input to the equipment. If the discontinuities are above 500/minute and occur frequently on a single QAM tuner only, this typically indicates either a problem with the level and/or signal quality on the particular QAM frequency at the UCrypt input.

An Internal Issue

If the discontinuities are above 500/minute and occur frequently on a single QAM tuner only, it may indicate a potential hardware issue with that particular tuner.

6.11.6 Probable Causes

1. Input RF levels are either not set to the UCrypt's ideal operating range, certain QAM levels are unbalanced on the plant or the SNR or MER of the QAM signal is below the threshold the equipment can handle without errors.
2. Plant maintenance had been occurring at the time of the error.
3. Hardware tuner internal to the UCrypt is failing.

6.11.7 Next Steps

1. Check if the program has corrected itself by checking 'status' of the program on 'Channel View' page.
2. Analyze the log to determine if there have been multiple tuners sending alerts at about the same time. If multiple tuners are reporting problems especially if they reside on different host boards, this indicates a problem external to the UCrypt.
3. Analyze the log to determine if the errors are occurring at times when plant or headend maintenance may be occurring.
4. Check the 'All Tuner Diagnostics' page on the UCrypt GUI and ensure all tuned frequencies are showing signal levels between 0 and +15 dBmV and SNRs greater than 32 dB.
5. If symptoms point to external causes, then measurement of plant carrier levels and MER may be required.

6. If a single tuner persistently reports errors or tuners on a single CableCARD module or tuners on a single tuner board are persistently in error and the RF signal level and MER on the QAM in question have been confirmed to be within spec at the UCrypt input, this could indicate a failing tuner board internal to the UCrypt equipment.

6.12 UCrypt Program Lost Bitrate Error

6.12.1 Refers to

Lack of presence of MPEG video packets for the program in question. This error is reporting on a single program in a QAM and is not indicating the failure of the QAM as a whole.

6.12.2 Repetition of Alert

This alert is sent at every occurrence of the detection of a bitrate that is lost. If the stream is reacquired, then the alert is sent again upon the next bit rate loss detection.

6.12.3 Customer Symptoms

Customer experiences loss of program reported by the error for the duration that the error condition exists.

6.12.4 Urgency

Medium - High.

6.12.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

To have an occasional but rare alert of lost bitrate could be considered normal as there are many possible causes, many of them cable system related, or it may happen as a result of a UCrypt operation such as an ‘apply’ or reboot and does not require any attention if the UCrypt is able to recover from the problem by itself. It may be that a program was taken out of service momentarily at the headend. A repeated alert of this nature should be cause to investigate why a single program is consistently losing bitrate.

An Internal Issue

If a program is consistently losing bitrate and/or fails to re-acquire bit rate when it can be verified the same program is in fact operating properly on the plant, this may be an indication of either a UCrypt software or hardware based issue.

6.12.6 Probable Causes

1. If the error is seen immediately following an ‘apply’ or ‘reboot’ this is considered normal and is not an issue.
2. The UCrypt software failed to re-acquire the program video stream after an outage condition.
3. The program was unavailable (or is still not available) on the cable system plant at the time of the error.
4. There is a hardware failure of the tuner or demodulator in question.

6.12.7 Next Steps

1. Investigate if bitrate on the program in question has been re-acquired by the UCrypt typically indicated by the program status returning to ‘green’ on the ‘Channel View’ page. Also check the video bitrate on the program specific details page. If it has not been re-acquired, an ‘Apply’ or a ‘reboot’ may be necessary in order to re-acquire.
2. Investigate why the subject program was not available and/or is still not available on the cable system plant at the time of the error.

6.13 UCrypt Multiplex Dropping Error

6.13.1 Refers to

The aggregate bit rate of the specific QAM is exceeding 38.8 Mb/s or the internal multiplexer is failing to properly process all packets as it should. Each program that is assigned to a multiplex is variable bit rate and the sum total of all the assigned programs is likely exceeding, from time to time, the bit rate limit of the affected QAM. This may happen when several programs are taken from various QAMs and multiplexed together on another QAM and there has not been sufficient headroom left to accommodate the variable bit rate nature of the programs. The UCrypt does not rate shape programs so the operator must ensure that too many programs are not placed in any single output QAM.

6.13.2 Repetition of Alert

This alert is sent each time that it is detected that the bit rate for the specific QAM has exceeded the 38.8 Mb/s limit. If the bit

rate then falls below 38.8 Mb/s the alert will be sent next time that the bit rate again exceeds 38.8 Mb/s.

6.13.3 Customer Symptoms

Customer experiences flickering, artifacts and/or other impairments on all programs on the affected multiplex for the duration that the error condition exists with the degree of impairments escalating with the severity of the condition. The resulting effects will be both random and variable depending on the conditions causing the error and it is not possible to quantify them further.

6.13.4 Urgency

Medium.

6.13.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

If this alert is received repeatedly, it indicates that the variable bit rate nature of the programs assigned to a QAM are peaking above 38.8 Mb/s under some content conditions and a brief outage or picture breakup is occurring on all programs on that QAM at the time of the peak rate. The programs on the affected QAM must be spread out over more QAMs. The total aggregate bit rate on the affected QAM must be reduced.

An Internal Issue

Read the paragraph above as this is the most likely cause. If it is absolutely clear that the multiplex specified in the alert is not being oversubscribed (i.e. it only has a single program assigned to the output MPTS or has 2 HD's that the operator knows for sure are not exceeding 38.8 Mb/s) then the error is likely indicating a temporary failure by the multiplexer to properly process all packets as it should. This is a rare but possible internal UCrypt cause.

6.13.6 Probable Causes

1. There are too many programs assigned to the affected QAM and the aggregate bit rate of the programs exceeds 38.8 Mb/s occasionally or frequently.
2. Internal UCrypt multiplexer error.

6.13.7 Next Steps

1. Analyze the number of programs and the maximum possible aggregate bite rate of those programs that are assigned to the specific troubled QAM and attempt to calculate if only a single program or more are required to be removed from this multiplex then start removing programs until this alert no longer occurs.
2. Analyze the log for the consistency of the alert over time. It is possible that a single error may occur and may not necessarily indicate a serious problem requiring attention.
3. It is possible for this error to be an indication of an internal software failing. First eliminate the possibility of too many programs in the QAM.
4. If an immediate resolution to the issue is necessary, a reboot of the UCrypt should be attempted.

6.14 UCrypt Output QAM Lost Bitrate Error

6.14.1 Refers to

QAM Modulator stops modulating at 38.8 Mb/s. The bit stream from the internal multiplexer to the QAM modulator has failed. This error indicates that the modulator has failed to acquire the bit stream properly.

6.14.2 Repetition of Alert

This alert is sent each time it is detected that a QAM has stopped modulating the 38.8 Mb/s stream. If the stream again starts modulating and fails again, the alert is sent again.

6.14.3 Customer Symptoms

Customer experiences loss of all programs on the affected QAM for the duration that the error condition exists.

6.14.4 Urgency

Low - High.

6.14.5 Cases where Alert is likely a result of:

Outside influence or normal operation

If only a rare occurrence of an output QAM losing bit rate is reported, this could happen due to programs losing bit rate during

plant maintenance or other operations, or may happen as a result of an effected UCrypt system operation such as an 'apply' or reboot and does not require any attention if the UCrypt is able to recover from the problem by itself.

An Internal Issue

If this alert is sent frequently over a period of hours or days it is usually an indication of internal hardware/software issues within the device and requires urgent attention.

6.14.6 Probable Causes

1. Plant conditions or an effected UCrypt operation (apply, reboot) have caused a QAM modulator channel to lose its input stream momentarily.
2. The QAM modulator within the UCrypt is failing.

6.14.7 Next Steps

1. If the QAM loses bit rate occasionally but the UCrypt recovers from the problem without outside help, this may be ignored, especially if the reoccurrence is very rare.
2. This alert, received frequently, may be an indication that there is an internal failure in the UCrypt.

6.15 UCrypt Output QAM Channel Restarting Error

6.15.1 Refers to

PCR accuracy is abnormal at the output of the UCrypt program multiplexer. When PCR accuracy is intolerable, the QAM modulator restarts or re-acquires lock. This alert is sent at a threshold of 3 restarts per minute.

6.15.2 Repetition of Alert

This alert is sent every time that the threshold of the alert is exceeded in a one minute period.

6.15.3 Customer Symptoms

Customer experiences a very brief flicker impairment on all programs on the affected QAM at the time that the error condition occurs. The impairment is so brief that it sometimes may only be noticed if there are many restarts per minute.

6.15.4 Urgency

Low - High.

6.15.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

If only a rare occurrence of an output QAM restarting is reported, this could be considered normal and does not require any attention if the UCrypt is able to recover from the problem by itself.

An Internal Issue

Repeated occurrences of an output QAM restarting, is usually indicative of excessive variation in PCR accuracy in the multiplexed output stream being sent to the QAM modulator channel in question.

6.15.6 Probable Causes

1. Maintenance at the single program level (i.e. not broadband RF system maintenance) at the headend or intentionally effected UCrypt operation such as programming changes.
2. Excessive variation in PCR accuracy in the multiplexed output stream being sent to the QAM modulator channel in question indicating internal issues.
3. The output QAM modulator module internal to the UCrypt is failing.

6.15.7 Next Steps

1. If the QAM restarts occasionally but the UCrypt recovers from the problem without outside help, this may be ignored, especially if the reoccurrence is rare and restarts are low (well under 5 per minute).
2. This alert, received frequently, could more likely be indicating an internal UCrypt software issue especially if many restarts are being reported over a period of time.

6.16 UCrypt SDV Lost Resolve Error

6.16.1 Refers to

Tuning Adapter tried to determine the frequency of the channel but it received an error message.

6.16.2 Repetition of Alert

This alert will be sent every time it occurs.

6.16.3 Customer Symptoms

The channel will be missing from the output.

6.16.4 Urgency

Medium - High.

6.16.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

Tuning Adapter losing lock, provisioning issue, session manager not sending information back to adapter.

An Internal Issue

There are more SDV programs configured than the number of Tuning Adapter tuners.

6.16.6 Probable Causes

1. Provisioning issue.
2. Session manager did not send information to the Tuning Adapter.
3. Require another Tuning Adapter.

6.16.7 Next Steps

1. Verify the Tuning Adapter is properly provisioned.
2. Check the configuration on the UCrypt device; the number of SDV programs should be equal to or less than the number of Tuning Adapter tuners. Add additional Tuning Adapter if required.

6.17 UCrypt Tuning Resolver Lost Lock Error

6.17.1 Refers to

Tuning Adapter lost lock to the Data Carousel.

6.17.2 Repetition of Alert

This alert is sent every time the event occurs.

6.17.3 Customer Symptoms

- No issue immediately.
- Extended outage may cause programs to be dropped.

6.17.4 Urgency

Medium.

6.17.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

Issue in the RF signal.

An Internal Issue

None.

6.17.6 Probable Causes

1. Signal Issue.
2. Plant maintenance had been occurring at the time of the error.
3. Plant distortions make it difficult for the Tuning Adapter to maintain lock on the data carousel.
4. Hardware issue on the Tuning Adapter.

6.17.7 Next Steps

1. Note if the loss of lock occurs during maintenance windows indicating external cause.
2. A single loss on a Tuning Adapter occurring rarely may be considered normal.
3. Recurring losses of lock over time on a specific tuner may indicate a hardware problem.

6.18 UCrypt Power Supply Failure

6.18.1 Refers to

Failure of one of the two redundant power supply modules. This failure could be caused also by the lack of AC input to one power supply if they are fed from redundant power sources.

6.18.2 Repetition of Alert

This alert is sent only once, when detected.

6.18.3 Customer Symptoms

Customer experiences no change to normal operation.

6.18.4 Urgency

Low - High.

6.18.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

This alert may be caused by the lack of AC input to the affected power supply if the AC feeds are setup with redundancy, but cannot be caused by any normal operation of the equipment.

An Internal Issue

This alert may be triggered by the failure of an internal power supply. A site visit is required to resolve the cause.

6.18.6 Probable Causes

1. Internal redundant power supply failure.
2. No AC power in supply circuit.
3. AC power cord for power supply has been removed or unplugged.

6.18.7 Next Steps

1. Check AC power cord to power supplies.
2. Check for presence of AC power at supply receptacle.
3. Exchange failed power supply module.

6.19 UCrypt Plant Maintenance Exception

6.19.1 Refers to

The scheduled check of programs that are either missing or are not decrypting. On the System page under the ‘Power’ section, the device may be configured to do a “Scheduled Outage Check”. If this feature has been configured, then this alert refers to a missing or improperly decrypted program.

6.19.2 Repetition of Alert

This alert is sent every time that a program is detected to be missing or not properly decrypted when tested according to the defined schedule.

6.19.3 Customer Symptoms

Customer will be aware of the missing or improperly decrypted program that is being reported and the intention is to restore this program through the scheduled maintenance reboot process.

6.19.4 Urgency

Low - High.

6.19.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

If only a rare occurrence of a missing channel is reported, this could be considered normal and does not require any attention if the device is able to recover from the problem by itself. This may be an indication of problems at the originators site, the broadcaster of the program.

An Internal Issue

Repeated occurrences of a missing channel, could be the result of internal hardware that is failing or firmware related issue. ATX support group should be notified for further analysis.

6.19.6 Probable Causes

1. Plant Maintenance was occurring at the time of the Alert.
2. Headend Maintenance was being done on that program at the time of Alert.
3. The CableCARD lost decryption authorization for the program and did not recover.
4. Internal hardware or firmware related issue. Contact ATX Support for further analysis.

6.19.7 Next Steps

1. If the program is reported missing occasionally but the UCrypt recovers from the problem without outside help, this may be ignored, especially if the reoccurrence is rare and frequency of reports are very low.
2. This alert, received frequently, could more likely be indicating an internal UCrypt software issue especially if many channels are reported missing over a period of time.

6.20 UCrypt DQAM Configured But Not Detected

6.20.1 Refers to

UCrypt device configuration has program assigned to a DQAM module but the DQAM has not been detected.

6.20.2 Repetition of Alert

Alert ius sent only once per occurrence.

6.20.3 Customer Symptoms

All programs assigned will be missing.

6.20.4 Urgency

High.

6.20.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

If this alert is accompanied by other alerts, analyze all of the alerts to determine a possible outside cause as there may be some common problem which cannot be predicted here. This alert would not normally be expected.

An Internal issue

Possible over heating of the DQAM, or DQAM, not powering up.

Bad internal network connection, bad internal slot, or a f/w issue.

6.20.6 Probable Causes

1. Dead or failing DQAM module.

6.20.7 Next Steps

1. Power Cycle unit.
2. Ensure fans are all functional.
3. Ensure ambient air temperature is within specification.
4. For assistance with troubleshooting suspected hardware or software issues, Contact ATX Networks technical support.

6.21 UCrypt Tuner Board Configured But Not Detected

6.21.1 Refers to

Programs known to be assigned to tuner boards will be missing from the output.

6.21.2 Repetition of Alert

Alert is sent only once per occurrence.

6.21.3 Customer Symptoms

Missing programs.

6.21.4 Urgency

High

6.21.5 Cases Where Alert is Likely a Result of:

Outside influence or normal operation

If this alert is accompanied by other alerts, analyze the sum total of the alerts to determine a possible outside cause as there may be some common problem which cannot be predicted here. This alert would not normally be expected. The UCrypt may be installed in a dirty environment whereby the slots of the motherboard have become dirty and connections to tuner boards are failing.

An Internal Issue

Dirty motherboard PCIe slot, bad PCIe slot, f/w issue, internal overheating.

6.21.6 Probable Causes

1. Dirty unit, defective PCIe slot contacts.
2. Failing tuner board.

6.21.7 Next Steps

1. Power Cycle unit.
2. Ensure fans are all functional.
3. Ensure ambient air temperature is within specification.

This page intentionally left blank

SERVICE & SUPPORT

7. Service & Support

7.1 Contact ATX Networks

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

TECHNICAL SUPPORT

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

SALES ASSISTANCE

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

FOR HELP WITH AN EXISTING ORDER

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

7.2 Warranty Information

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

ISO
9001:15
REGISTERED

© 2019 by ATX Networks Corp. and its affiliates (collectively "ATX Networks Corp."). All rights reserved. This material may not be published, broadcast, rewritten, or redistributed. Information in this document is subject to change without notice.

Rev. 11/19 (ANW1175)

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