



Endpoint Management Administration Guide

Software Version 3.7

Document Version 1.0

Technical Support
(866) 927-5465 or support@mutualink.net



Copyright ©2017 Mutualink, Inc. All rights reserved. Published in USA.

Published Date August, 2017

US Patents #7,643,445 | #8,364,153 | #8,320,874 | #8,811,940 | #8,929,851 and other US and International Patents Pending. The furnishing of this document does not give you any license to such patents.

This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Mutualink, Inc. While every precaution has been taken in the preparation of this book, Mutualink, Inc. assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

Mutualink is a trademark of Mutualink, Inc. All other trademarks used herein are the property of their respective owners.

Mutualink, Inc.
1269 South Broad Street
Wallingford, CT 06492
(866) 957-5465

Contents

Preface

Chapter 1: Administration using the EMS

Administration using the EMS	14
Common EMS Elements	15
Login	15
Home Screen	15
Modify Settings Controls	15
Admin Functions	16

Chapter 2: Host Management

System Status	18
Installation Information	18
Network	19
DNS	19
Primary Interface	20
Secondary Network Interface	21
Static Routes	22
NTP Servers	23
Installation Logs	26
Management	27
User Statistics	27
EMS Users	27
Software Update	29
Reboot System	30

Chapter 3: Managing the Endpoint

Interoperability Work Station	32
Interop	32
Multicast Network	34
Presence Multicast	34
KDS Agent	35
NMS Agent	35
Controlled Resources	36
Video Display	37
File Sharing	37
Incident Filtering	39
Integration	41
Device Interface	41
Handset	42
Relay RTP	43
Preferences	45
Audio	45
Auto Mute	47
Auto Accept	47
IWS Preferences	48
Geographic Location	50
Status	52
Endpoint Status	52
Registered Endpoints	53
KDS Agent Status	54
NMS Agent Status	55
Alarms	56
Incidents	56
Application Logs	56
Management	58
Add Endpoint Users	58
Configuration	59

Chapter 4: Radio Network Interface Controller

R-NIC Home Page	64
Interop	64
Endpoint Identity	64
Multicast Network	64
Presence Multicast	65
KDS Agent	65
NMS Agent	65
Ciphers	66
Controlling Endpoints	66
Integration	67
Device Interface	67
External Channels	68
RX Interface	68
Digital RIB (DigitRIB) Settings	69
Download DigitRIB Settings	71
Digital RIB Profiles	71
PTT Device	72
Relay RTP	73
Preferences	74
Audio	74
Audio Codec	74
Geographic Location	75
Status	76
Endpoint Status	76
Registered Endpoints	76
KDS Agent Status	76
Alarms	77
Incidents	77
Logs	78
Management	79
API Users	79
Configuration	79
Restart Endpoint	79
Restart	80

Chapter 5: Telephone Network Interface Controller

T-NIC Home Page	82
Interop	83
Endpoint Identity	83
Multicast Network	83
Presence Multicast	84
KDS Agent	84
NMS Agent	84
Controlling Endpoints	85
Integration	86
Rx Interface	86
VoIP Incoming Calls	87
VoIP Outgoing Calls	87
VoIP Registration	88
VoIP Media	89
Relay RTP	90
Preferences	91
Audio Codec	91
Geographic Location	91
Status	92
Endpoint Status	92
Registered Endpoints	92
KDS Agent Status	92
NMS Agent Status	92
Alarms	92
Incidents	93
Logs	94
Management	95
API Users	95
Configuration	95
Restart	96

Chapter 6: Video Network Interface Controller

V-NIC Home Page	98
Change to Output or Input Video	99
Interop	100
Endpoint Identity	100
Multicast Network	100
Presence Multicast	101
KDS Agent	101
NMS Agent	101
Controlling Endpoints	102
Integration	103
Rx Interface	103
VoIP Incoming Calls	104
VoIP Outgoing Calls	104
VoIP Registration	105
VoIP Media	106
Relay RTP	107
Preferences	108
Audio Codec	108
Geographic Location	108
Status	109
Endpoint Status	109
Registered Endpoints	109
KDS Agent Status	109
NMS Agent Status	109
Alarms	109
Incidents	110
Logs	111
Management	112
API Users	112
Configuration	112
Restart	113

Preface

As part of an effort to improve its product lines, Mutualink periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Mutualink representative if a product does not function properly or does not function as described in this document.

This document was accurate at publication time. New versions of this document might be released on Mutualink, Inc. Check to ensure that you are using the latest version of this document.

For more information on Mutualink products visit us at <https://mutualink.net/our-solution/products/>

Purpose

The purpose of this document is to serve as a reference for the installation and administration / configuration of Mutualink endpoints (IWSs and NICs).

Intended Audience

Anyone responsible for the installation and/or administration of Mutualink endpoints. This would include Mutualink field engineers and technical support engineers, as well as authorized VAR/OEM field and technical support personnel.

Requirements

This document assumes that readers are proficient in IP networking and using the Linux command line.

Revision History

The following table provides a description of document changes.

Revision	Description and/or change
1.0	Initial Release.

Your Comments

Your suggestions are very important to us. They will help make our documentation more useful to you.

Please e-mail comments about this document to Mutualink, Inc at:

techpubs_comments@mutualink.net

Please include the following information when commenting:

- Document title
- Document Version Number (on title page)
- Software Version Number (on title page)
- Page number (if appropriate)

Accessing Online

For information on EMS functions refer to the online help system. The help pages provide a description and explanation of the configuration settings on current EMS page selected.

To access:

1. In top right hand corner, click Username.
2. Click Help.

To navigate to help on a particular EMS configuration setting, click Home or Endpoints.

Terminology

The following table provides a list of possibly terminology used.

Term	Description
Agency	An organization of interest that owns a Mutualink endpoint.
Command Line Interface (CLI)	An interactive shell environment provided to configure, monitor and debug an (EP).
Carried Operated Relay (COR)	A signal from a receiver that gives a positive indication that a carrier or signal is being received and that the receiver is unsquelched. It has the same function as Carrier Operated Squelch (COS).
E&M Signaling	Ear and mouth push to talk (PTT).
End Instrument (EI)	A device or instrument connected to a terminal of a communications circuit.
Endpoint (EP)	A communication node within the Mutualink network. There are two classes of endpoints: NICs and IWSs.
EP Instance	A logical endpoint instance, embodied by Core Software (CoreSW), and sometimes referred to as IMSAPP; the primary software component of an endpoint.
Element Management Service (EMS)	A web-based GUI provided to configure, monitor, and interact with an EP.
Foreign Exchange Office (FXO)	A device with an FXO port has the capability of behaving as a common analog telephone.
Foreign Exchange Subscriber (FXS)	Port that actually delivers the analog line to the subscriber.
Over the Air (OTA)	A standard for the transmission and reception of application-related information in a wireless communications system.
Public Switched Telephone Network (PSTN)	Aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication.
Push to Talk (PTT)	A means of instantaneous communication commonly employed in wireless cellular phone services that uses a button to switch a device from voice transmission mode to voice reception mode.
PuTTY	A free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection. It can also connect to a serial port.

Term	Description
Radio End Instrument (REI)	Radio connected to the wires at the end of a telecommunications link.
Radio Gateway (RG)	Allows one radio to talk to another radio that is many miles away through the power of Radio Over IP (ROIP).
Receive (RX) – SIP (Session Initiation Protocol)	A communications protocol for signaling, for the purpose of controlling multimedia communication sessions.
Secure Shell (SSH)	A cryptographic network protocol for operating network services securely over an unsecured network.
Tone Operated Relay (TOR)	A relay operated by the CTCSS decoder.
Transmit (TX)	The process of sending and propagating an analogue or digital information signal over a physical point-to-point or point-to-multipoint transmission medium, either wired, optical fiber or wireless.
Receive (RX)	The process of receiving a signal.
Session Initiation Protocol (SIP)	Communications protocol for signaling, for the purpose of controlling multimedia communication sessions.
Voice Activity Detection (VAD)	Technique used in speech processing in which the presence or absence of human speech is detected.[1] The main uses of VAD are in speech coding and speech recognition. It can facilitate speech processing, and can also be used to deactivate some processes during non-speech section of an audio session: it can avoid unnecessary coding/transmission of silence packets in Voice over Internet Protocol applications, saving on computation and on network bandwidth.
Voice Operated Exchange (VOX)	Switch that operates when sound over a certain threshold is detected.

CHAPTER

1

Administration using the EMS

The Element Management System (EMS) is the primary administration/configuration interface for all Mutualink Endpoints (EP). The EMS runs within a small web server on each of the EPs and may be accessed using any modern web browser on any operating system; it may be accessed from the local LAN or anywhere on the interconnect network (as long as router firewall rules allow port 443 access).

This chapter describes each page, the information they display, and the actions you can take from the page(s).

- [Administration using the EMS on page 14](#)
- [Common EMS Elements on page 15](#)

Note: *The screens may vary depending on the version of the software.*

Administration using the EMS

The following outlines what is needed to use the EMS to administer/configure all Mutualink EPs.

Starting the EMS

The easiest way to use the EMS is to simply enter the IP address of the target EP in the browser's address bar. If port 80 (http) is open to the EP, it will automatically redirect you to the secure web port 443 (https). If port 80 is not open, then you will have to manually specify the https protocol (e.g. https://10.1.2.3/ems).

If this is the first time you've connected to this EP's EMS, you will probably receive a security warning that the site's certificate is invalid. This is due to the fact that the Mutualink Root CA certificate is not yet trusted by your browser, and the name in the certificate does not match the "hostname" of the web site (i.e. the IP address). After double-checking that you are in fact going to the correct EP, add an exception for the site if required to proceed.

You will then be asked to login – use the appropriate administrator username and password and click **Login** to get to the home page. Refer to [Login on page 15](#).

Common EMS Elements

The following describes the elements of the EMS:

- [Login on page 15](#)
- [Home Screen on page 15](#)
- [Modify Settings Controls on page 15](#)
- [Admin Functions on page 16](#)

Login

Once you have entered the IP address of the target EP in the browser's address you are ready to login. In order to gain access to the EMS you must enter the **Username** and **Password**.

Note: *The information on the screen varies depending on your login credentials.*

Home Screen

The Home screen contains the following information:

1. **Manage Host** button that when selected displays the System Status page. The button changes to **Manage Endpoint**.

Note: *To return to the main page click **Manage Endpoint** again. The button changes back to **Manage Host** and you are return to the Main page.*

2. **User login name:** User you are currently logged in as. For example if you are logged in as **admin**, **admin** displays.
3. Type of EP this is (IWS, R-NIC, etc.), the Agency and Endpoint name, and the Endpoint Primary IP Address.
4. Current Mutualink software version, the endpoint up time since last the last restart of the application, and the date/time stamp when the endpoint was last modified.

Figure 1.

Modify Settings Controls

For each page that can modify settings, the following buttons display:

- **Edit** – will link to the associated area where editable parameters may be changed and saved.
- **Save** – will apply & save any new settings to the EP.
- **Cancel** – will reset any changed fields to their original values (since the last save).

On NICs, the clicking the “**Save**” button may automatically restart the Mutualink software for the new settings to take effect

Note: *This will be destructive to any communications the EP is currently involved in.*

On IWSs, after clicking “**Save**” a message may appear saying that the IWS must be restarted for the new settings to take effect. This just means that the IWS Application must be manually closed and restarted; this is not done automatically as in NICs since there may be a user sitting at the IWS.

Admin Functions

The admin drop-down provides the following:

- **Group:** The user's role determines what level of access a user has to view or edit a particular section.
 - Customer (least access)
 - Field, Support
- **Help:** Information for the Manage Host and Mange Endpoint areas are accessible by selecting **Help**.
- **Change Password:** From here the *admin* password can be changed. The original password must be known to successfully change the *admin* password.
- **Sign Out:** Selecting this will log the user out of the EMS session.

CHAPTER

2

Host Management

This chapter describes each page, the information they display, and the actions you can take from the page(s).

- [System Status on page 18](#)
- [Network on page 19](#)
- [Network on page 19](#)
- [Installation Logs on page 26](#)
- [Management on page 27](#)

System Status

When you select **Manage Host** the **System Status** page displays. The page provides four tabs to manage the endpoint.

The drop-down list from the **Status** tab provides options to view **System Status** and **Installation Information**.

The **System Status** page displays general system information. You cannot edit any information presented on this page.

Note: To return to the main Home page, click **Manage Endpoint**.

Installation Information

The **Installation Information** page displays operating system, software version, and clone image information. You cannot edit any information presented on this page.

Network

The **Network** drop-down list provides:

- [DNS on page 19](#)
- [Primary Interface on page 20](#)
- [Secondary Network Interface on page 21](#)
- [Static Routes on page 22](#)
- [NTP Servers on page 23](#)

DNS

The **DNS Servers** page provides the host name and the primary and secondary DNS server information.



Mutualink™ EMS

Serial Number : 00:30:18:A2:BF:B1
192.168.12.221

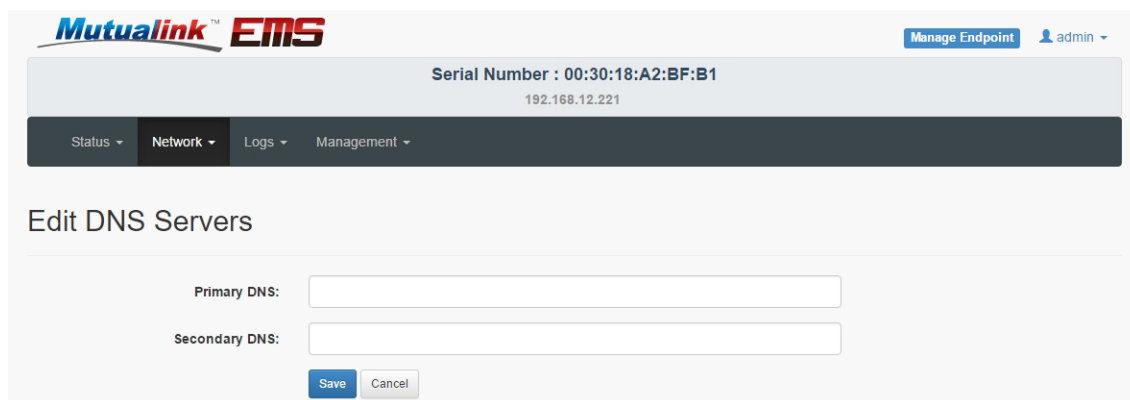
Manage Endpoint admin

Status Network Logs Management

DNS Servers Edit

Hostname: ATOM-VNIC
Primary DNS: Not set
Secondary DNS: Not set

Figure 2. DNS Servers



Mutualink™ EMS

Serial Number : 00:30:18:A2:BF:B1
192.168.12.221

Manage Endpoint admin

Status Network Logs Management

Edit DNS Servers

Primary DNS:
Secondary DNS:

Save Cancel

Figure 3. Edit DNS Servers

- **Primary & secondary DNS servers:** Leave blank for none; may not be needed on private interconnect networks. Note that if DHCP is enabled, these fields are disabled as DHCP will auto-populate these values. If changing from DHCP to a Static IP, make sure you change/delete these values as needed.

Primary Interface

This network interface must be connected to the interconnect network.

- **Name:** Informative only. Primary Network Interface (eth0)
- **DHCP Enabled:** Enables IP auto-config from a DHCP server.

Note: *DHCP should only be used for testing/demo purposes – it should not be enabled on production EPs.*

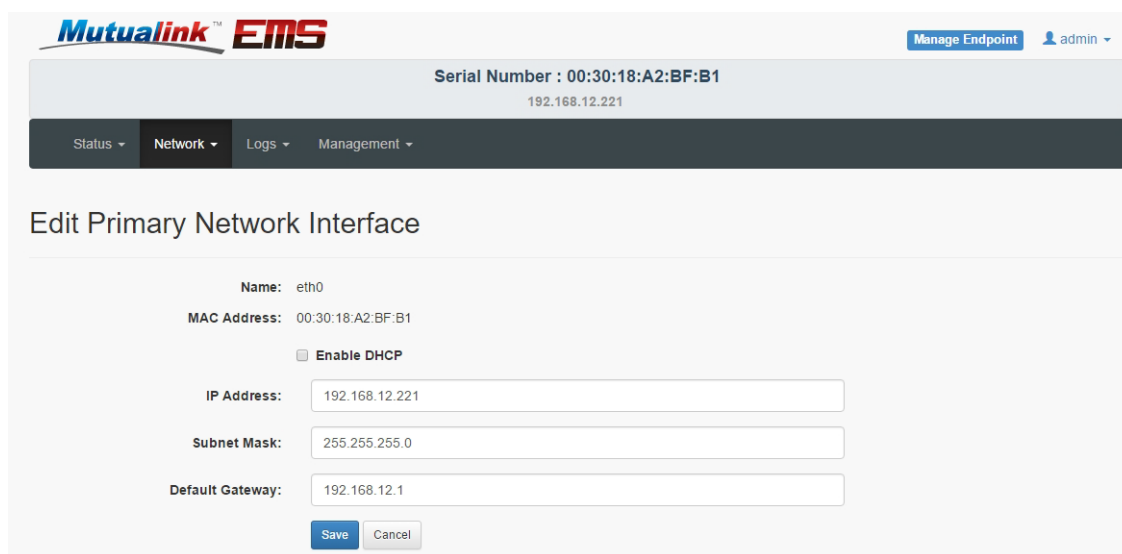
- **MAC Address:**
- **IP Address & Subnet Mask:** As given by the network administrator.
- **Default Gateway:** Gateway used if no static routes match. Disabled if DHCP is enabled.



The screenshot shows the Mutualink EMS web interface. At the top, there's a header with the Mutualink EMS logo and a 'Manage Endpoint' button next to a user icon labeled 'admin'. Below the header, a grey bar displays the 'Serial Number : 00:30:18:D6:F3:1E' and the IP address '192.168.13.39'. A navigation bar with tabs for 'Status', 'Network', 'Logs', and 'Management' is visible. The 'Network' tab is selected, and the page title is 'Primary Network Interface' with an 'Edit' button. The configuration details are listed below:

Name:	eth0
DHCP Enabled:	No
MAC Address:	00:30:18:D6:F3:1E
IP Address:	192.168.13.39
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.13.1

Figure 4. Primary Network Interface



The screenshot shows the 'Edit Primary Network Interface' page in the Mutualink EMS web interface. The header and navigation bar are identical to the previous figure. The page title is 'Edit Primary Network Interface'. The configuration details are shown in a form with input fields and a checkbox:

Name:	eth0
MAC Address:	00:30:18:A2:BF:B1
<input type="checkbox"/> Enable DHCP	
IP Address:	<input type="text" value="192.168.12.221"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.12.1"/>

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

Figure 5. Edit Primary Interface

- **Enable DHCP:** Enables IP auto-config from a DHCP server.

Note: DHCP should only be used for testing/demo purposes – it should not be enabled on production EPs.

- **IP Address & Subnet Mask:** As given by the network administrator.
- **Default Gateway:** Gateway used if no static routes match. Disabled if DHCP is enabled.

Secondary Network Interface

This interface is optional and is typically only used to connect an EP to a customer LAN for sharing of specific information/media. If the optional Ethernet Port 1 is populated in this EP, then the choice of “eth1” will be available. The “VLAN on eth0” choice is always available – this choice enables a Virtual LAN (basically like a second overlay Ethernet interface) on the primary eth0 port; this should be used if desired by the customer network administrator. The VLAN ID will also be assigned by the network administrator.



Figure 6. Secondary Network Interface



Figure 7. Edit Secondary Network Interface

If the optional Ethernet Port 1 is populated in this EP, then the choice of “eth1” will be available. The “VLAN on eth0” choice is always available – this choice enables a Virtual LAN (basically like

a second overlay Ethernet interface) on the primary eth0 port; this should be used if desired by the customer network administrator. The VLAN ID will also be assigned by the network administrator.

This interface is optional and is typically only used to connect an EP to a customer LAN for sharing of specific information/media. If the optional Ethernet Port 1 is populated in this EP, then the choice of “eth1” will be available.

The “VLAN on eth0” choice is always available – this choice enables a Virtual LAN (basically like a second overlay Ethernet interface) on the primary eth0 port; this should be used if desired by the customer network administrator. The VLAN ID will also be assigned by the network administrator.

Static Routes

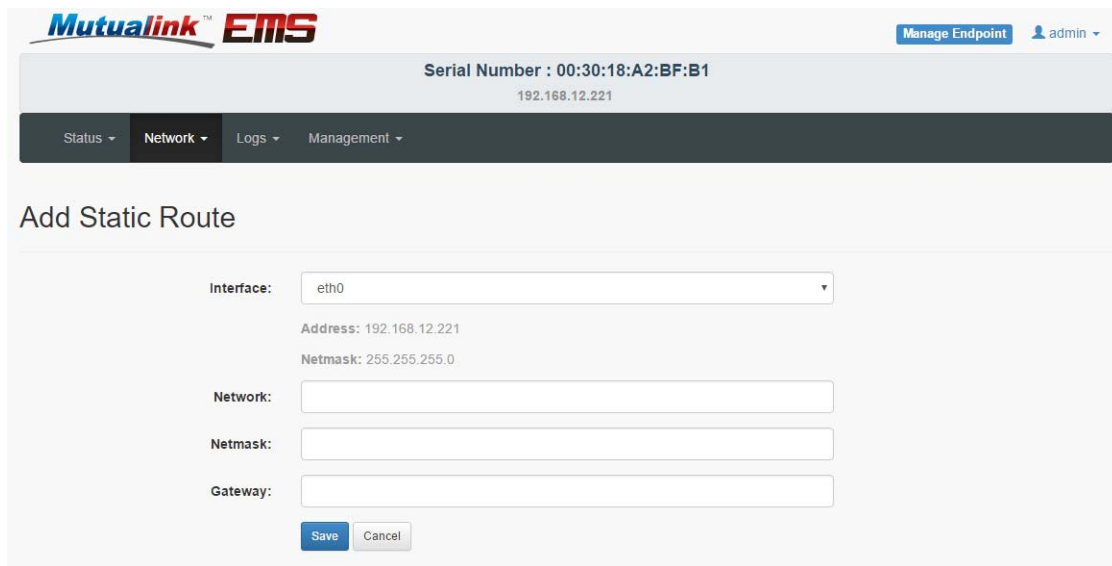
The **Static Routes** option is accessible from the **Network** drop-down list.

This is only applicable if a secondary interface has been enabled, and you know what you're doing.

The table shows the list of static routes currently configured, if any.

These changes take effect immediately on the host routing table.



Figure 8. Static Routes

The screenshot shows the Mutualink EMS web interface. At the top, there is a header with the Mutualink EMS logo on the left, a 'Manage Endpoint' button, and a user profile 'admin' on the right. Below the header, a status bar displays 'Serial Number : 00:30:18:A2:BF:B1' and the IP address '192.168.12.221'. A navigation bar contains links for 'Status', 'Network', 'Logs', and 'Management'. The main content area is titled 'Add Static Route'. It features a form with the following fields: 'Interface' (a dropdown menu showing 'eth0'), 'Address' (displayed as '192.168.12.221'), 'Netmask' (displayed as '255.255.255.0'), 'Network' (an empty text input), 'Netmask' (an empty text input), and 'Gateway' (an empty text input). At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 9. Add Static Route

To add a new route:

1. Click **Add**.
2. Select an Interface.
3. Enter the Network, Netmask, and Gateway values.
4. Click **Save**.

To delete a route:

1. Click **Delete** on the corresponding row on the table.

NTP Servers

If the NTP service is enabled, the page will show the list of NTP servers currently configured. The order of the server entries is not important as with the DNS service.

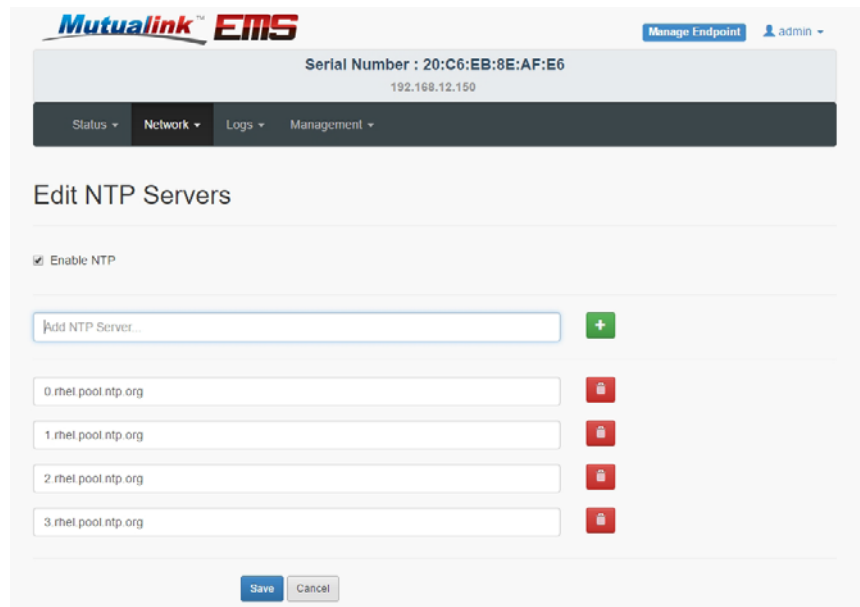
Note: The service will be restarted when the NTP service is enabled as a big change in the system clock will disrupt its audio processing.



Figure 10. NTP Servers

To enable the NTP service on this host, click Edit. Then, on the edit form, check Enable NTP and add/remove to the current list of NTP servers. When you finish setting the server list, click Save to submit your changes.

Similarly to disable the NTP service, click Edit and remove the check from Enable NTP. Then, click Save to submit your changes.



The screenshot shows the 'Edit NTP Servers' page in the Mutualink EMS web interface. At the top, the header includes the Mutualink EMS logo, a 'Manage Endpoint' button, and a user profile 'admin'. Below the header, a grey bar displays the 'Serial Number : 20:C6:EB:8E:AF:E6' and the IP address '192.168.12.150'. A navigation bar with tabs for 'Status', 'Network', 'Logs', and 'Management' is present. The main content area is titled 'Edit NTP Servers'. It features a checkbox labeled 'Enable NTP' which is currently checked. Below this is a text input field labeled 'Add NTP Server...' with a green '+' button to its right. Underneath, there are four existing NTP server entries, each in a text box and followed by a red trash icon: '0.rhel.pool.ntp.org', '1.rhel.pool.ntp.org', '2.rhel.pool.ntp.org', and '3.rhel.pool.ntp.org'. At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 11. Edit NTP Servers

Installation Logs

Installation logs are accessible from the Logs tab.

You can access the logs created by the Endpoint software installer. By default it shows the logs for the last installation, but you can see the last N installations by entering the desired number on the form provided. As search box is also provided to highlight those lines that match the entered keywords.

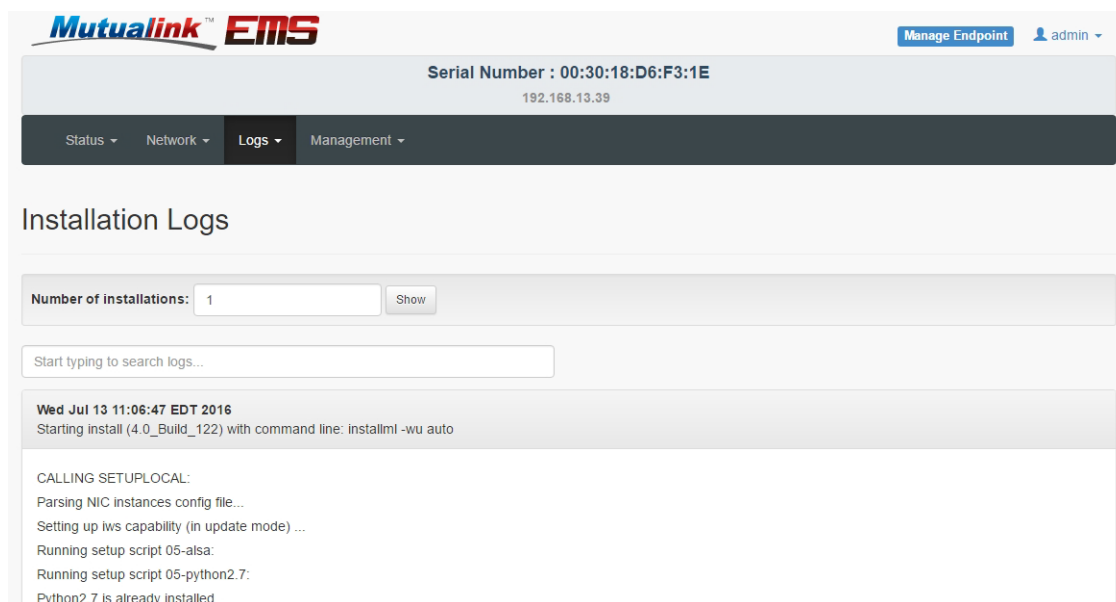


Figure 12. Installation Logs

Management

The **Management** tab allows you to view or perform:

- [User Statistics on page 27](#)
- [EMS Users on page 27](#)
- [Software Update on page 29](#)
- [Reboot System on page 30](#)

User Statistics

You can view the last successful and unsuccessful logins with date, time and IP address.

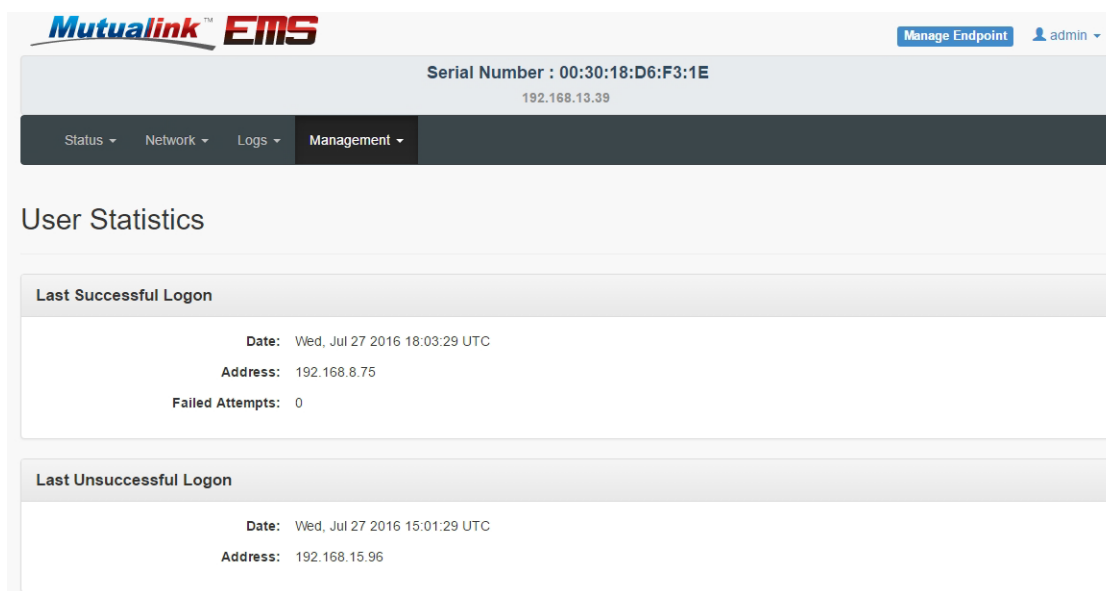


Figure 13. User Statistics

EMS Users

On this page you can add new EMS users in addition to the default admin account. New users are associated with one of the following roles: Customer (least access), Field, Support and

SuperSupport (most access). The user's role determines what level of access a user has to view or edit a particular section.

From this page you can also edit a particular user's record or delete it altogether if your access permissions allow it.

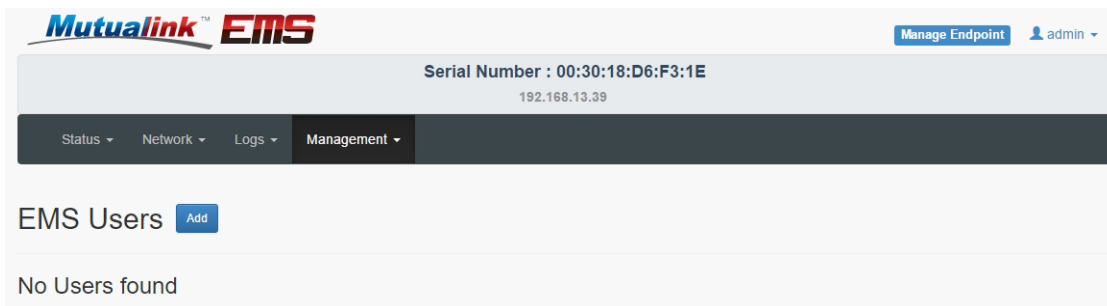


Figure 14. EMS Users

You can add new EMS users in addition to the default admin account.

The screenshot shows the 'Add User' form within the Mutualink EMS interface. The header and navigation bar are identical to Figure 14. The main content area is titled 'Add User'. It contains four input fields: 'Username:', 'Password:', 'Confirm Password:', and 'Role:'. The 'Role:' dropdown menu is open, showing three options: 'Customer' (highlighted in blue), 'Field', and 'Support'.

Figure 15. Add User

New users are associated with one of the following roles:

- Customer (least access)
- Field
- Support

The user's role determines what level of access a user has to view or edit a particular section.

From this page you can also edit a particular user's record or delete it altogether if your access permissions allow it.

Software Update

You can:

- Upload or delete software update packages from the local endpoint repository
- Install software update packages from local disk ("Local Repository"), a USB memory device ("External Media") or an NFS-shared directory ("Remote Repository").

To list the software packages available, select the desired repository and click *View*. The EMS will search in the corresponding location (up to a depth of 5 directories) for any compressed tar files that follow Mutualink's name convention (start with 'EPSW_' or 'mlink_' and have a '.tgz' extension). If the EMS cannot access the directory for any reason, it will show an error at the top of the page whereas if it doesn't find any packages it will show an empty listing.

If you want to search in a directory other than the options provided, you can manually enter the custom directory path on the combobox. In order for the EMS to search this directory, it must be readable by the *field* group.

- To install a software package click **Install** on the corresponding row.
- To delete a software package click **Delete** on the corresponding row.
- To upload a software package to the local endpoint repository, click on **Upload Package** and select the target file.

If the EMS doesn't show any errors related to its size, click on **Start Upload**. Notice that if the upload link to the Endpoint is slow this may take some time.

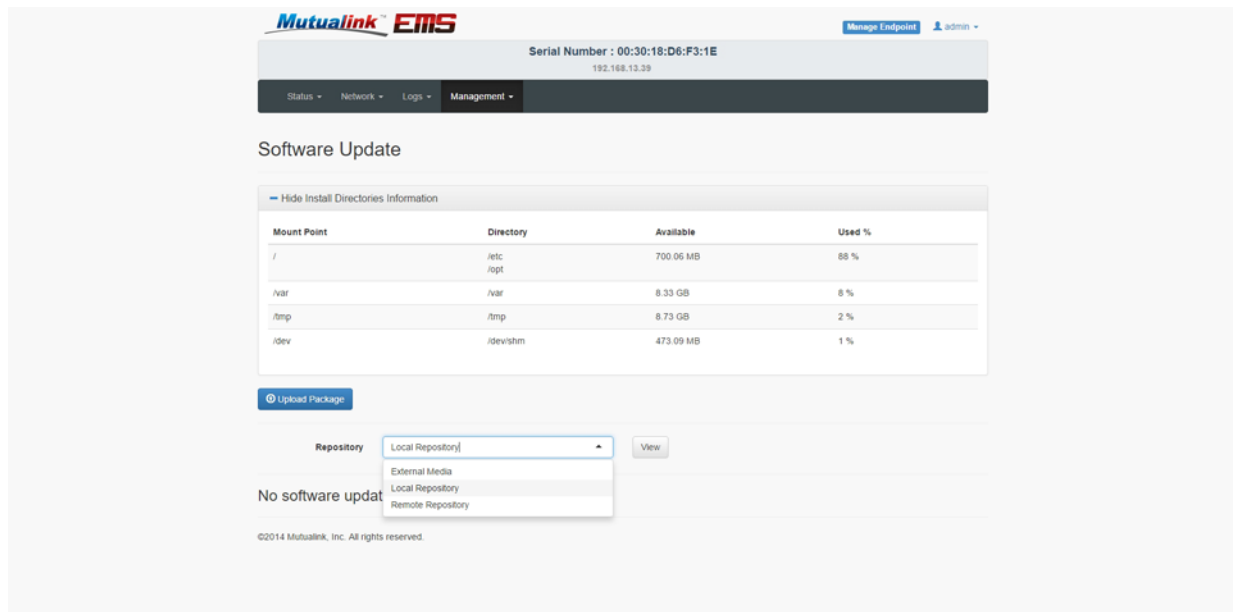


Figure 16. Software Update

Reboot System

A reboot is necessary when you need to restart an appliance IWS. The page will keep polling the system until the Endpoint comes back on and responds with a successful response.

CHAPTER

3

Managing the Endpoint

This chapter describes each page, the information they display, and the actions you can take from the page(s).

- [Interoperability Work Station on page 32](#)
- [Integration on page 41](#)
- [Preferences on page 45](#)
- [Status on page 52](#)
- [Application Logs on page 56](#)
- [Management on page 58](#)

Interoperability Work Station

The following screen shows the **Interoperability Work Station (IWS)** Home Page.

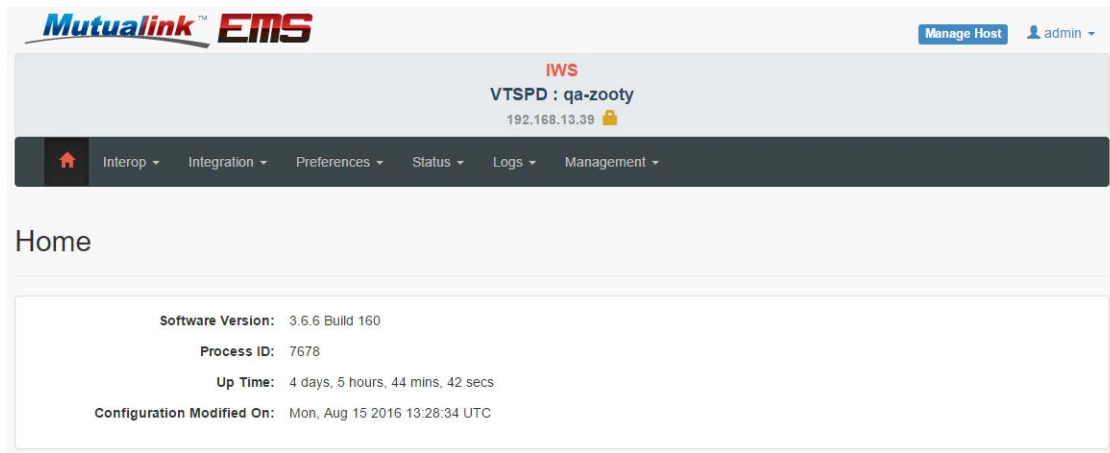


Figure 17. IWS Home Page

The following sections describe the actions you can take from the tabs. Each page displays informative information. You can modify settings by selecting **Edit** from each page.

Interop

From the **Home** page select **Interop**. A drop-down list provides the following:

- [Endpoint Identity on page 33](#)
- [Multicast Network on page 34](#)
- [Presence Multicast on page 34](#)
- [KDS Agent on page 35](#)
- [NMS Agent on page 35](#)
- [Controlled Resources on page 36](#)
- [Video Display on page 37](#)
- [File Sharing on page 37](#)

- Incident Filtering on page 39

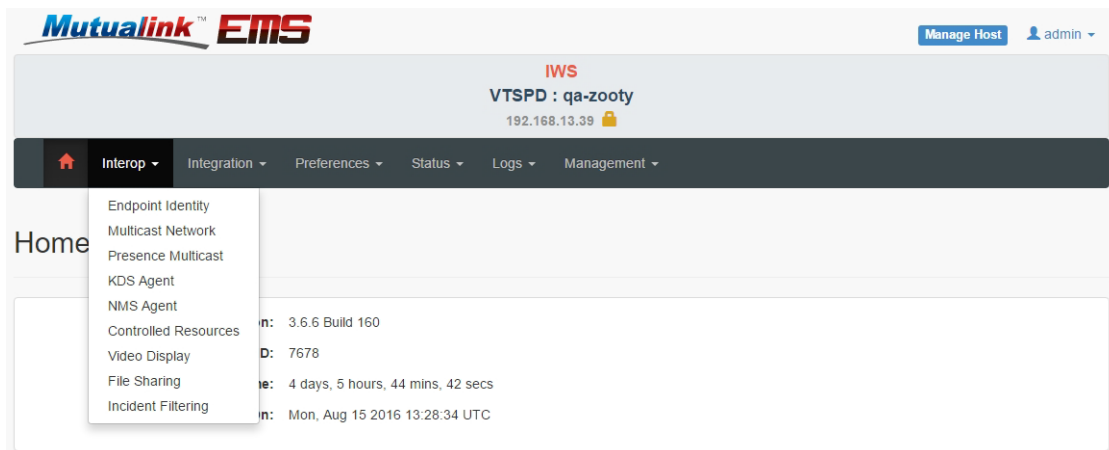


Figure 18. Interop Page

Endpoint Identity

The Endpoint Identity page displays:

- **GUID:** A 128 bit integer that identifies Mutualink entities across its systems. GUIDs are visually represented as a string of 32 hexadecimal digits, e.g. 210-000-1e65cbb75f-2eb7-0026b9810051, where hyphens are used to separate its main fields for clarity.
- **Agency Name:** The name of this agency/organization. The Agency Name must be unique within the encompassing Mutualink system. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **EP Name:** The name of this EP within this agency/organization. The EP Name must be unique just within the agency as the agency name is prefixed when displaying to the users. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **IWS Group (IWSs only):** This IWS should be considered "equivalent" to all other IWSs in the same group, meaning that if another organization wishes to contact this organization, it doesn't matter which IWS in the group answers the call. When an IWS Group is invited to an incident, the first IWS that accepts becomes a member of the incident; the other IWSs stop being alerted.
- **Current Icon:** The currently-selected "Service Type" icon for this EP. This icon visually represents the type of organization this EP belongs to and what standard services might be offered by this EP.

You can edit information on this page by clicking the **Edit** button.

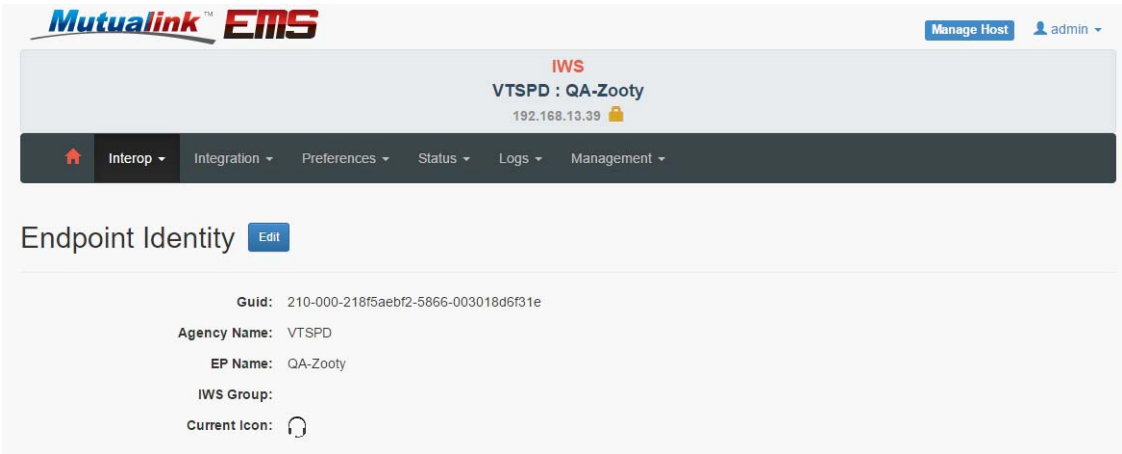


Figure 19. Endpoint Identity

Multicast Network

The **Multicast Network** page displays the following:

- **Multicast Address:** This determines what other EPs both see this EP and are seen by this EP; must be set to the same value on all EPs that wish to communicate; this is typically assigned by the Mutualink system administrator.
- **Jitter Buffer Size:** The initial size of the RTP receive audio jitter buffer. If a network is very bursty, a higher value would be better here, but the end-to-end voice delay increases correspondingly. In reality, our EPs have a fairly good automatic jitter buffer that automatically sizes itself as required, so this parameter should probably be left at the default value.

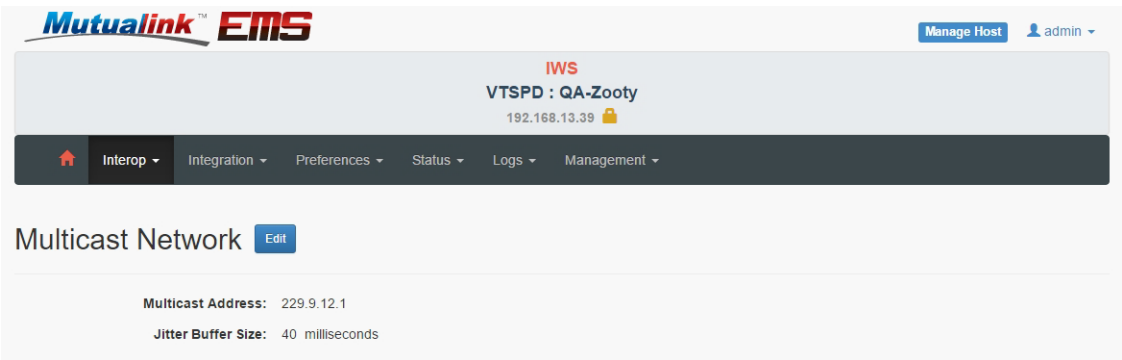


Figure 20. Multicast Network

Figure 21.

Presence Multicast

The **Presence Multicast** determines what other EPs both see this EP and are seen by this EP on the Global network. This value must be set to the same value on all EPs that wish to communicate on the Global network. This is typically assigned by the Mutualink system administrator.

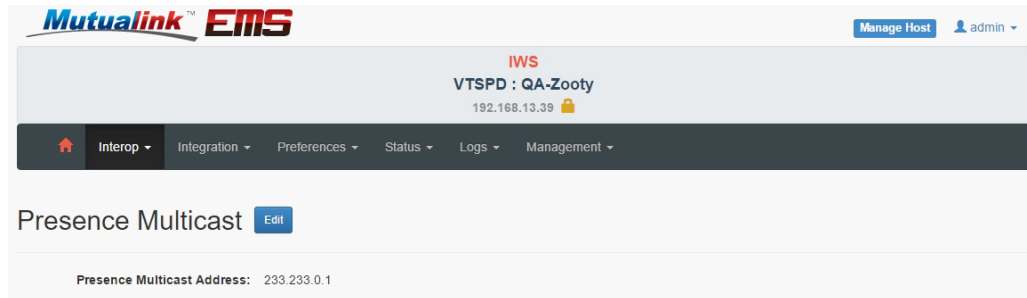


Figure 22. Presence Multicast

KDS Agent

The KDS Agent page displays:

- **Addresses and Port:** IP address and TCP port to the KDS web service (see Network Monitoring Service for details).
- **Update List Period:** Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.
- **Validation Retry Period:** Interval at which the EP will contact the remote service to request authentication on a given Agency.

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

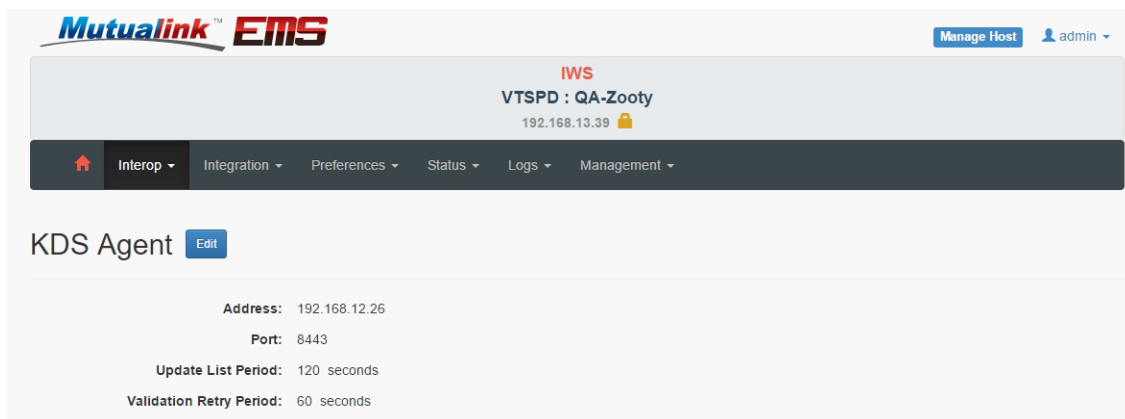


Figure 23. KDS Agent

Figure 24.

NMS Agent

The NMS Agent window displays the following:

- **Addresses:** List of IP addresses where the web remote service can be located. More than one address can be entered separated by colons (:) and the EP will try them out in the order listed.
- **Port:** TCP Port where the remote web service can be located.
- **Heartbeat Period:** Interval at which the EP will send heartbeat messages to the NMS.
- **Alarm Read Period:** Interval at which the EP will report new alarms to the NMS. The EP queues new alarms locally and sends them together at this interval.

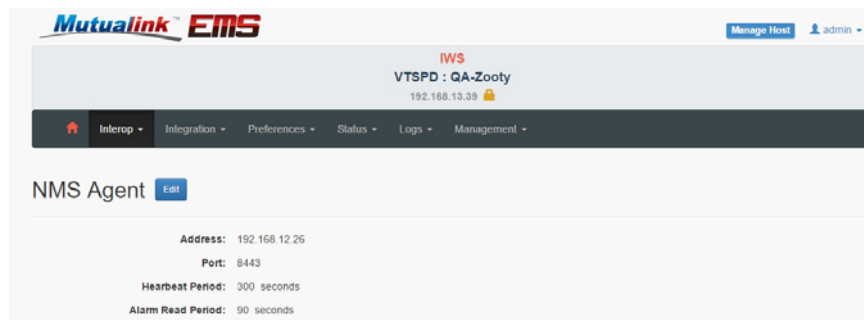


Figure 25. NMS Agent

Controlled Resources

The Controlled Resources pages provides a list of IWSs that are authorized to control this NIC. If an IWS that is not in this list attempts to invite this NIC to an incident or otherwise exercise control over it, the request will be rejected.

Note: To allow the IWS to actually control a NIC, the IWS must be entered in the NIC's list of Authorized IWSs as well, so accomplishing such control is a two-part administrative step

NICs in this list will appear on the IWS's screen as Resources that they can control and invite to incidents, etc.

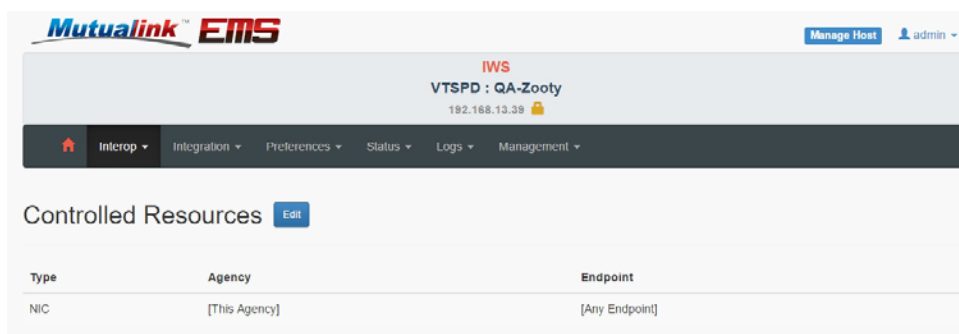


Figure 26. Controlled Resources

Video Display

- **Incident Video Display:** If this setting is disabled, then the IWS will be prevented from viewing video feeds from any V-NICs in an incident. This is enabled by default; an administrator may wish to disable this to control bandwidth usage by a particular IWS, for example.
- **Auto Start Incoming Video:** If this setting is enabled, the IWS will automatically start viewing the video feed from a V-NIC as soon as it joins the incident. If this is not enabled, the user must manually hit the play button to view the feed.
- **Max Incoming Video Bitrate:** If the user attempts to view a video feed that is above this bitrate, they will be disallowed and will receive an error message.

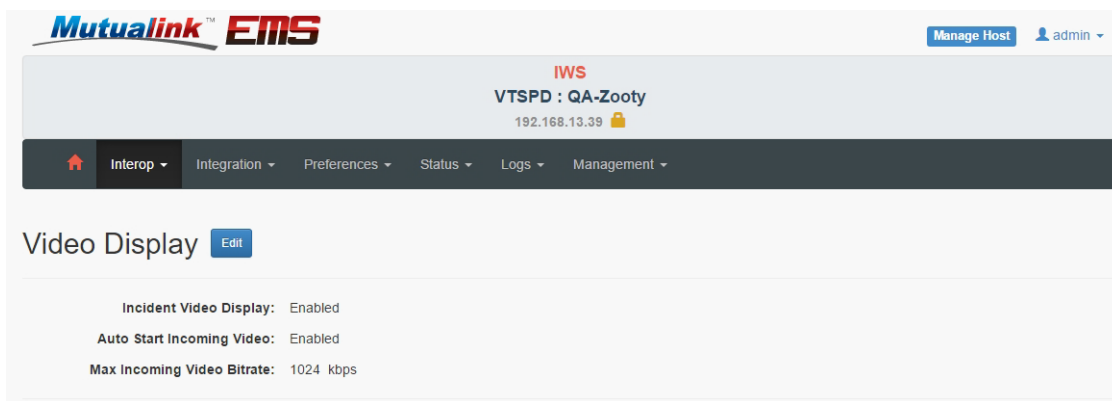


Figure 27. Video Display

File Sharing

If file sharing is enabled, it controls the visibility of the File Sharing feature to the IWS user and the area is visible. If this is disabled, the File Sharing area of incidents does not disable on the IWS.

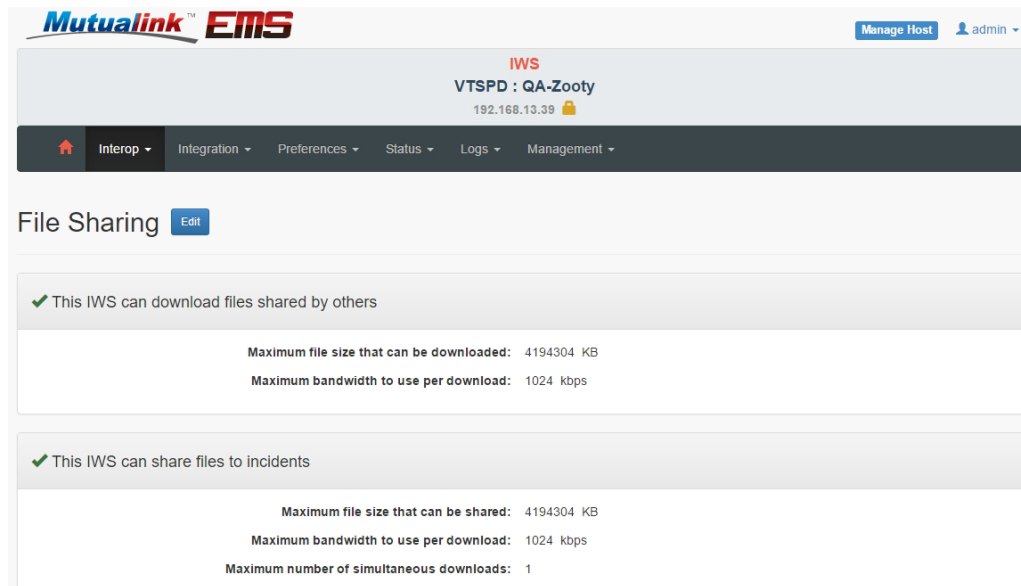


Figure 28. File Sharing

Allow this IWS to download files shared by others

This enables the IWS to download/retrieve files shared by others in an incident. If this is disabled, the user will see the files shared by others, but will not be presented with the options to download the files.

- **Maximum file size that can be downloaded:** Any attempts to download files larger than this will be denied by the IWS.
- **Maximum bandwidth to use per download:** For each file that is being downloaded, only use this much bandwidth (at most) for the download. This allows administrators to control the bandwidth used by this feature. Note that if the user is downloading multiple files at the same time, the total bandwidth used will be cumulative.

Allow this IWS to share files to incidents

This enables the IWS to share/upload files to other IWSs in an incident. If this is disabled, the Share button in the File Sharing area of an incident will be grayed out.

- **Maximum file size that can be shared:** Any attempts to share files larger than this will be denied by the IWS.

- **Maximum bandwidth to use per download:** For each copy of a locally-shared file being downloaded by another IWS, only use this much bandwidth (at most) for the download.
- **Maximum number of simultaneous downloads:** This will limit the total number of simultaneous downloads by other IWSs of files shared by this IWS. The maximum amount of bandwidth that may be used for file sharing in the upstream direction is determined by this value times the above bandwidth-per-download setting.

Note: *If the file sharing feature is enabled but neither uploads or downloads are enabled, the IWS user will see the File Sharing area on every incident, but will not be able to do anything with it. This is the default setting with the rationale that users should know that the feature exists, but enabling this feature requires explicit authorization by the local supervisor.*

Incident Filtering

Show Incidents Involving determines the types of Incidents that will be shown in the User Interface. These values are:

- This IWS
- This IWS or any resource it controls
- This IWS Agency

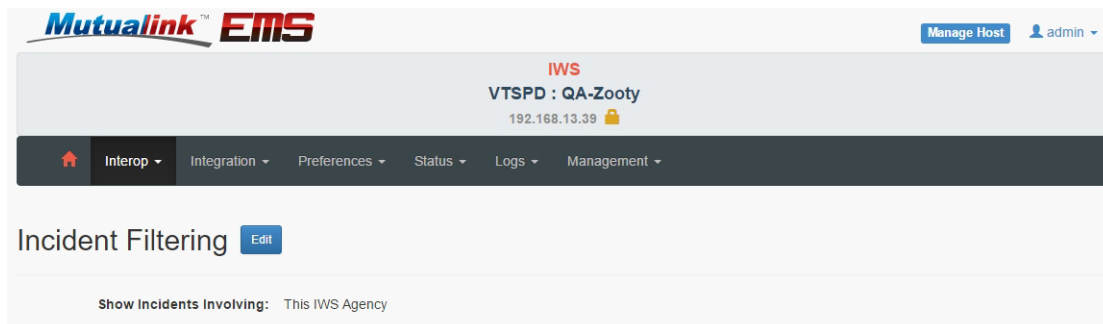


Figure 29. Incident Filtering

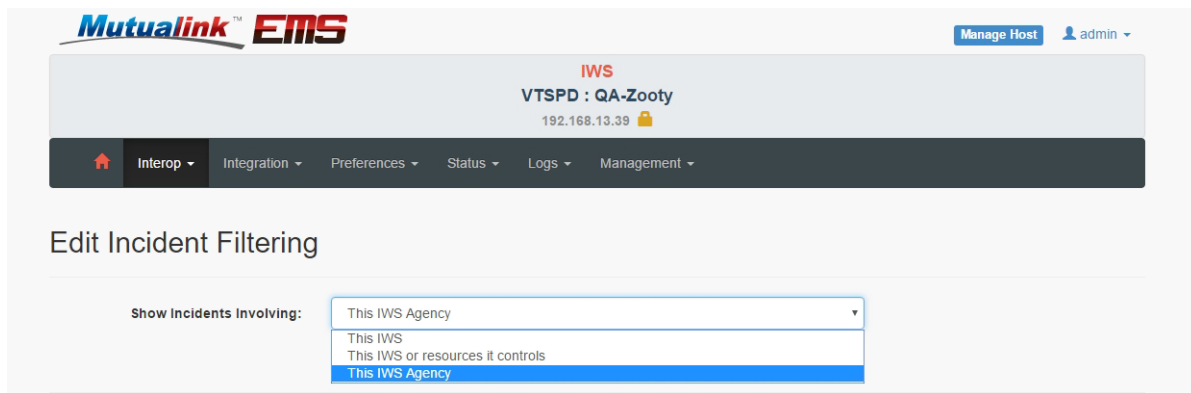


Figure 30. Edit Incident Filtering

Integration

The **Integration** tab allows you to view or perform:

- Device Interface
- Handset
- Relay RTP

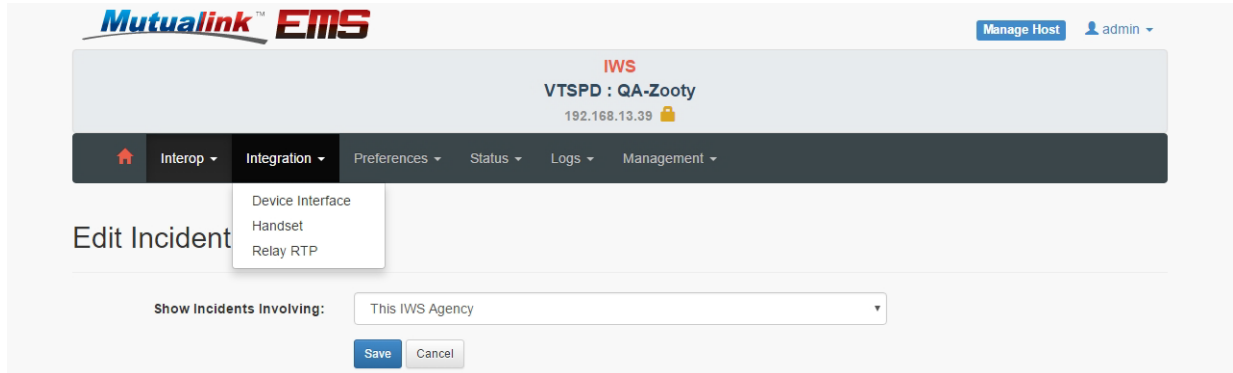


Figure 31. Integration

Device Interface

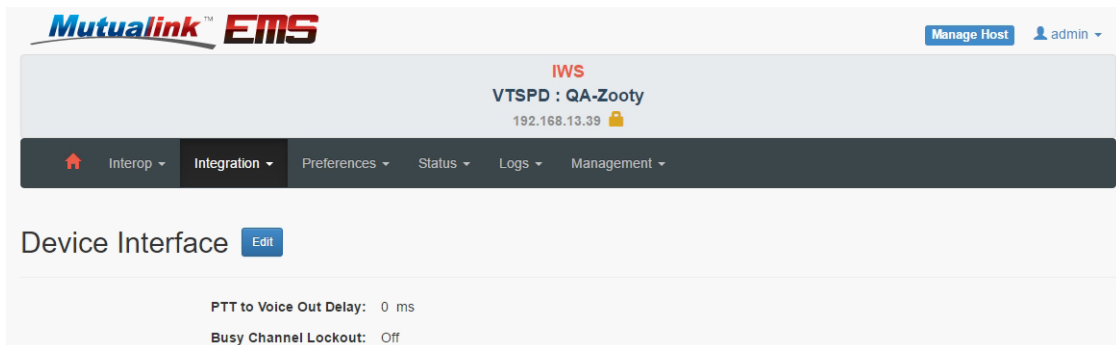
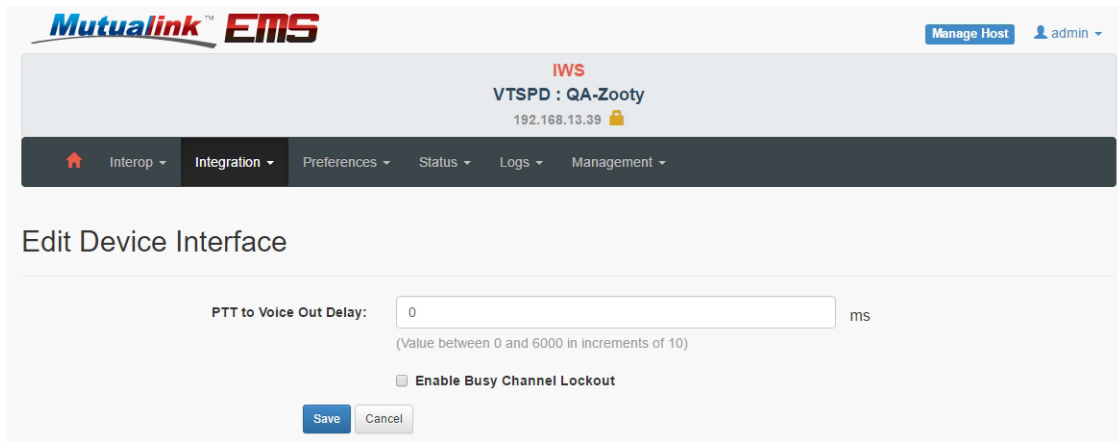


Figure 32. Device Interface

Edit Device Interface

- **PTT to Voice Out Delay:** If the external device requires time to prepare to receive audio after the PTT-Out signal is activated (e.g. a trunked radio system requires time to acquire a transmit channel before we can send it audio), configure that time here. Note that this may also be enabled for non-PTT devices if desired (e.g. to set a constant receive audio delay) for special situations.

- **Enable Busy Channel Lockout:** Enabling this setting will prevent audio being transmitted to the device/accessory while audio is being received from it. Sort of the reverse of VOX Half-duplex, but applicable for both PTT and VOX modes. When this setting is enabled for half-duplex radios, this will prevent incident transmissions from keying up the radio while it is already receiving an over-the-air transmission.



Mutualink™ EMS

Manage Host admin

IWS
VTSPD : QA-Zooty
192.168.13.39

Interop Integration Preferences Status Logs Management

Edit Device Interface

PTT to Voice Out Delay: ms
(Value between 0 and 6000 in increments of 10)

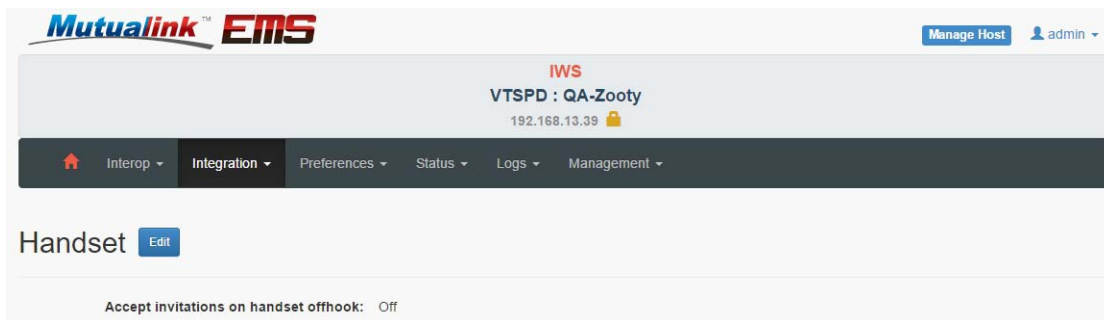
☐ Enable Busy Channel Lockout

Save Cancel

Figure 33. Edit Device Interface

Handset

This feature only applies to IWSs with the Handset option installed.



Mutualink™ EMS

Manage Host admin

IWS
VTSPD : QA-Zooty
192.168.13.39

Interop Integration Preferences Status Logs Management

Handset [Edit](#)

Accept invitations on handset offhook: Off

Figure 34. Handset

If the **Accept invitations on handset offhook** setting is enabled, then any incident invitations that are currently alerting the user will be automatically accepted when the handset is taken offhook. This is analogous to answering a ringing phone.

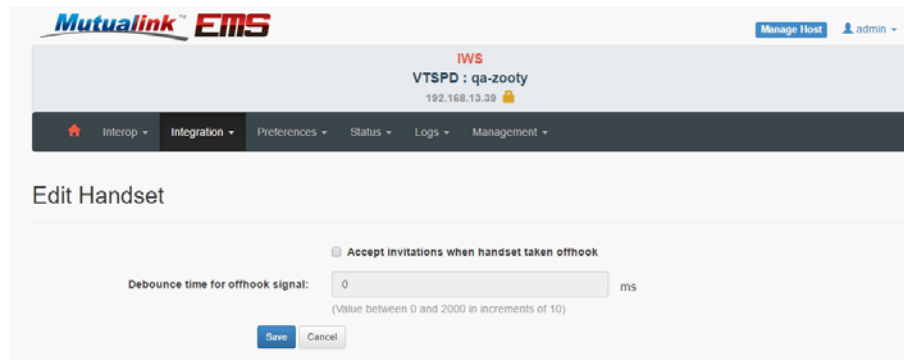


Figure 35. Edit Handset

Relay RTP

At this time, this parameter is meaningful only for T-NICs and IP V-NICs on multi-homed systems. It selects the interface that the Endpoint will use to open an RTP stream to a static destination IP address. You can select between the **Primary** or **Secondary** interfaces, or you can enter an interface name or IP address manually on the combo-box.

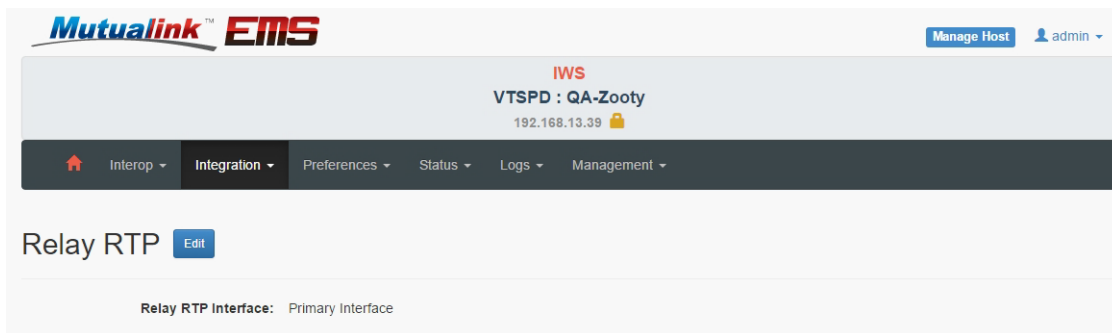


Figure 36. Relay RTP

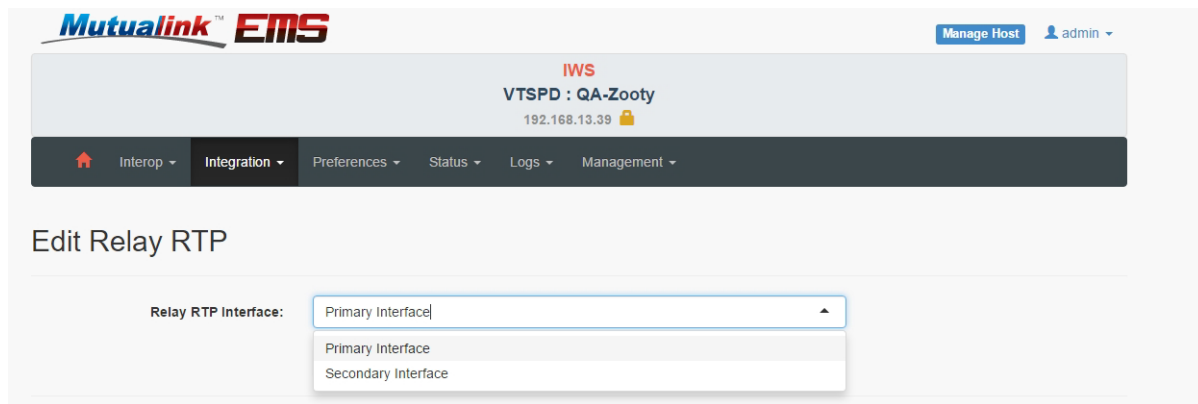


Figure 37. Edit Relay RTP

Preferences

The Preferences tab allows the following:

- [Audio](#) on page 45
- [Auto Mute](#) on page 47
- [Auto Accept](#) on page 47
- [IWS Preferences](#) on page 48
- [Geographic Location](#) on page 50

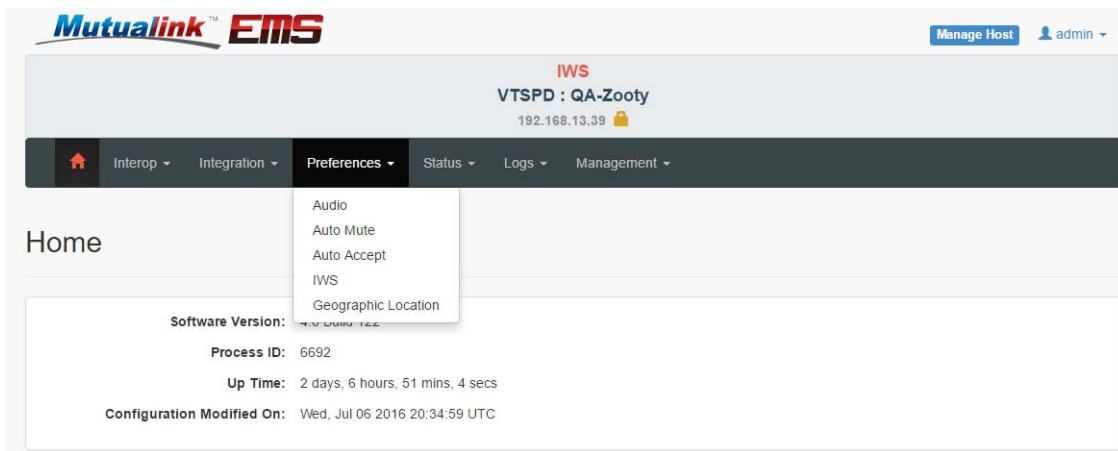


Figure 38. Preferences

Audio

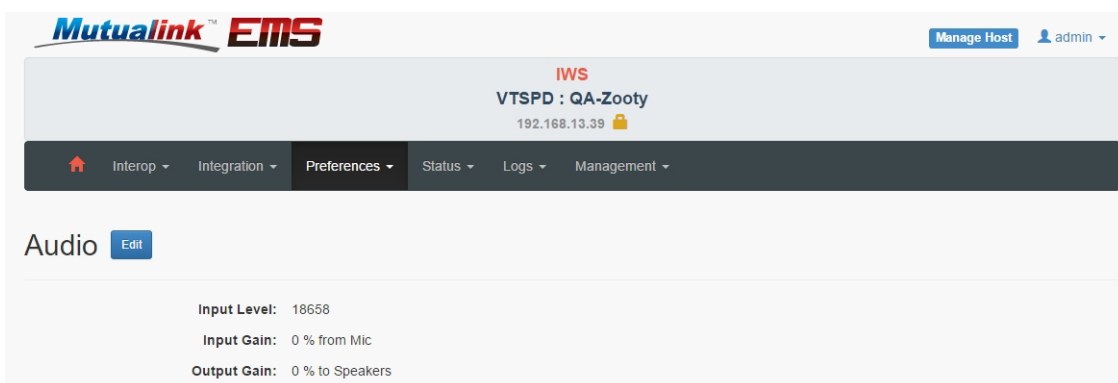


Figure 39. Audio

The screenshot shows the 'Edit Audio' configuration page in the Mutualink EMS IWS interface. The page has a header with the Mutualink EMS logo, a 'Manage Host' button, and a user profile 'admin'. Below the header is a navigation bar with tabs: Interop, Integration, Preferences (selected), Status, Logs, and Management. The main content area is titled 'Edit Audio' and contains the following elements:

- Input Level:** A text field showing '18772' with a 'Refresh' button next to it.
- Input Gain:** A text field showing '0' with a label '% from Mic' and a note '(Value between 0 and 100)'.
- Output Gain:** A text field showing '0' with a label '% to Speakers' and a note '(Value between 0 and 100)'.
- Output Test Tone:** A section containing a 'Time' text field with '120' and a 'secs' label, a 'PTT' checkbox, a 'Start Tone' button, and 'Apply' and 'Done' buttons at the bottom.

Figure 40. Edit Audio

Edit Audio

The following parameters only apply to IWSs and NICs using the built-in sound device (as opposed to external audio devices or accessories).

- **Input Level:** By clicking the Refresh button, the current Input level as read from the audio input line will be displayed. This allows the administrator to see what relative effect the Input Gain and Boost settings have on the input signal. Note that this level is in logarithmic units and is not correlated to dB, etc.
- **Input Gain:** Gain to apply to the input audio signal from external devices (via Mic In or Line In).
- **Output Gain:** Gain to apply to the output audio signal sent to external devices (via Line Out)
- **Output Test Tone:** This feature allows the administrator to send a test tone on the audio output line to the external device for measurement, calibration, etc. The length of the tone can be set and the PTT line can optionally be activated during the tone. To stop the tone before the time elapses, click the **Stop Tone** button.

Note: Make sure the EP is idle before using this test as it will interfere with the EP's functionality.

Auto Mute

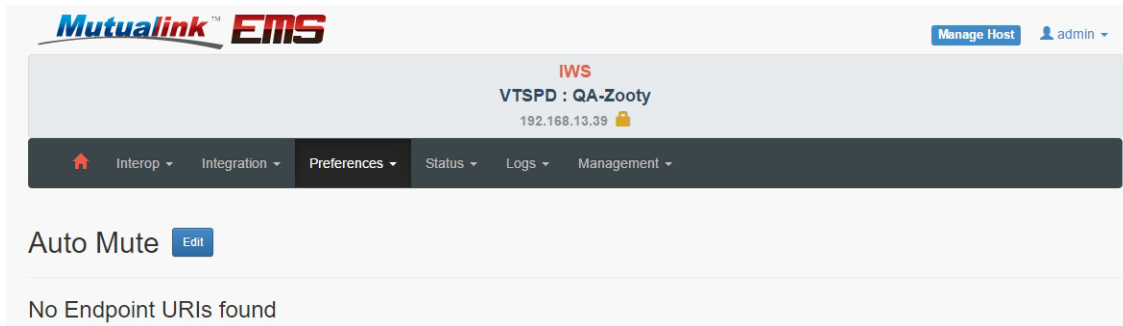


Figure 41. Audio Mute

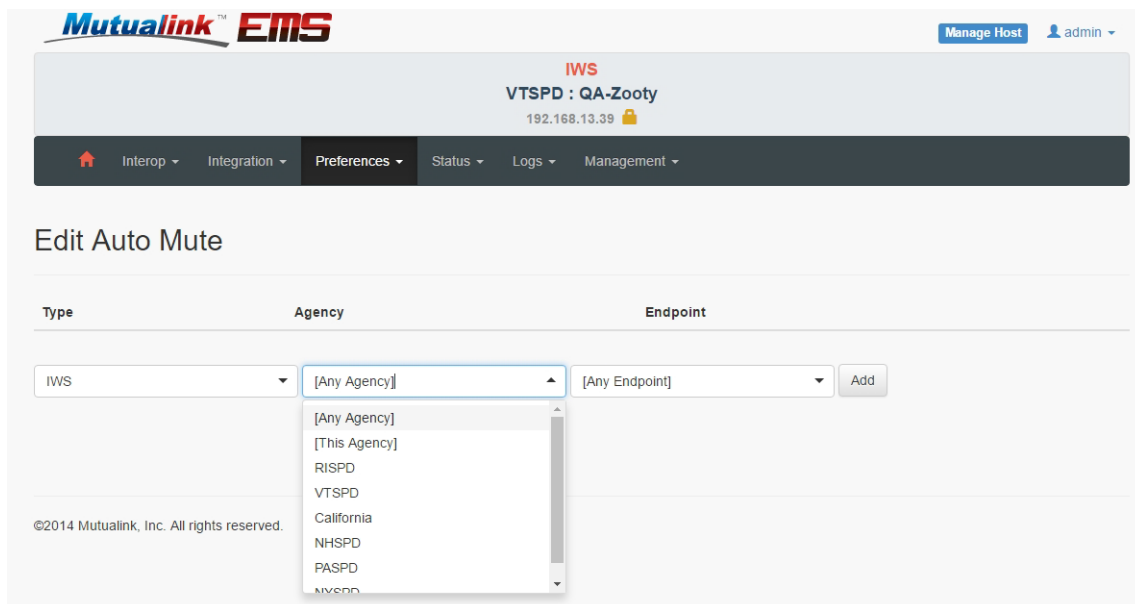


Figure 42. Edit Auto Mute

If an endpoint in this list joins any patch that this IWS is in, then the IWS will automatically Mute that patch; when the endpoint leaves the patch, the IWS will automatically un-Mute the patch. This feature is typically used for audio devices that are in the immediate vicinity of the IWS and where it would be undesirable to hear audio both from the IWS and from the device.

Auto Accept

If an endpoint in this list invites this IWS to an incident, the invitation will automatically be accepted. Administrators may wish to add trusted agencies to this list; some agencies even enable this for all agencies, thereby creating a kind of an immediate intercom system.

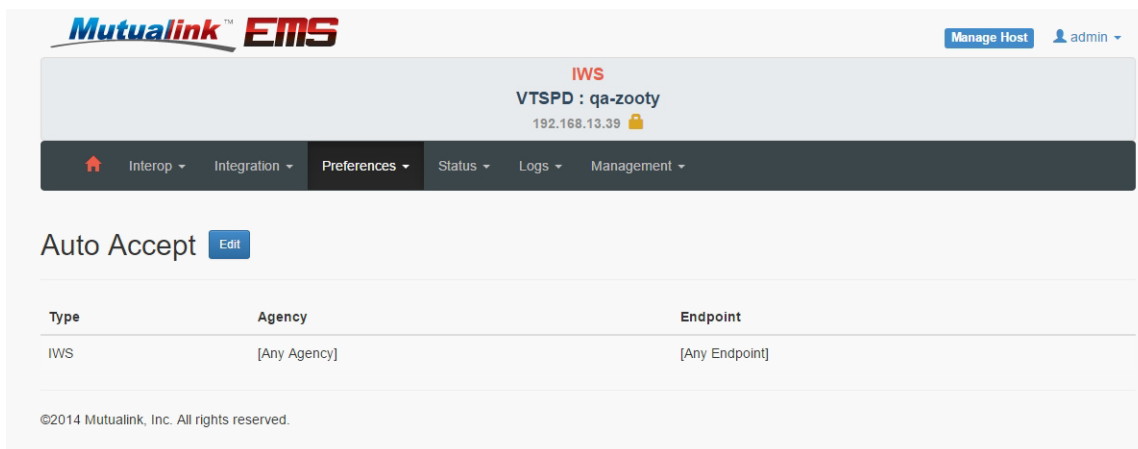


Figure 43. Auto Accept

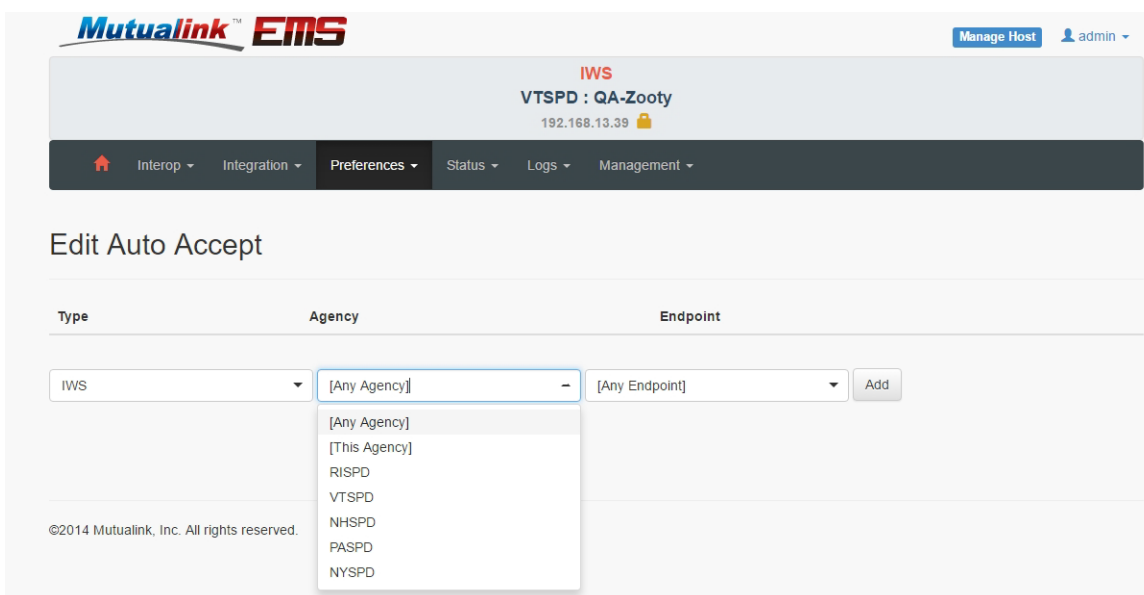


Figure 44. Edit Auto Accept

IWS Preferences

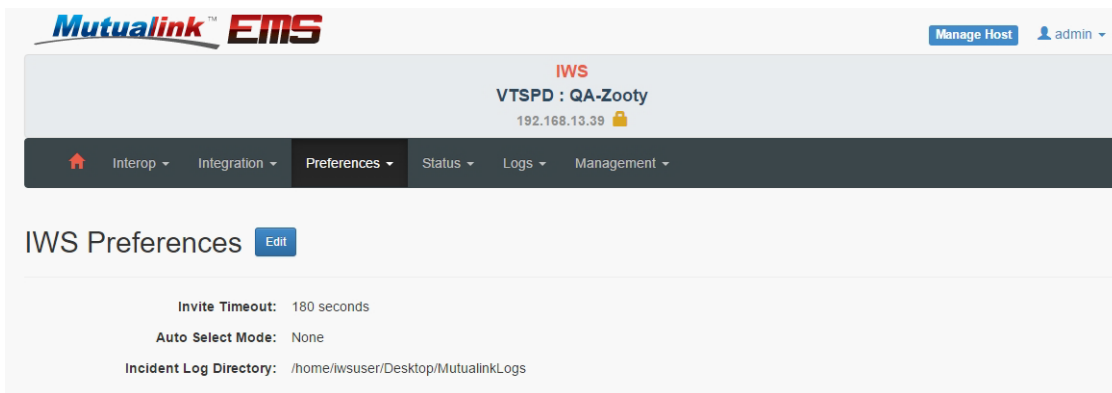


Figure 45. IWS Preferences

Edit IWS Preferences

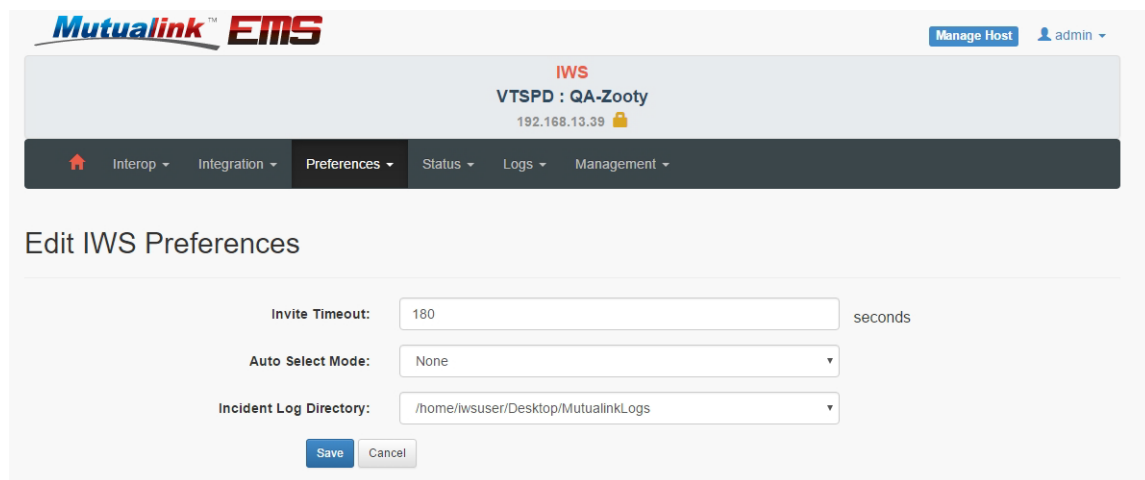


Figure 46. Edit IWS Preferences

Invite Timeout

If the IWS user does not accept or reject an incoming incident invitation within this time period, it will be rejected as **No Answer**.

AutoSelect Mode

This setting controls what should happen if an External PTT switch (e.g. headset, footswitch, or mic) is activated when no patch is selected in the IWS GUI:

- **None:** Nothing happens; no audio is transmitted.

- **Last Received:** The patch we last received audio on is automatically selected and keyed up.
- **Last Transmitted:** The patch we last transmitted on is automatically selected and keyed up.
- **Last Accepted:** A patch from the incident we last accepted is automatically selected and keyed up. If the invitation came from an IWS, the Intercom patch is selected; if the invitation came from a NIC, the Tx patch is selected.

Incident Log Directory

This controls whether logs of activity within all incidents are kept. If this is blank, no logs are kept. By default, logs are created in the MutualinkLogs directory on the IWS user's desktop

Geographic Location

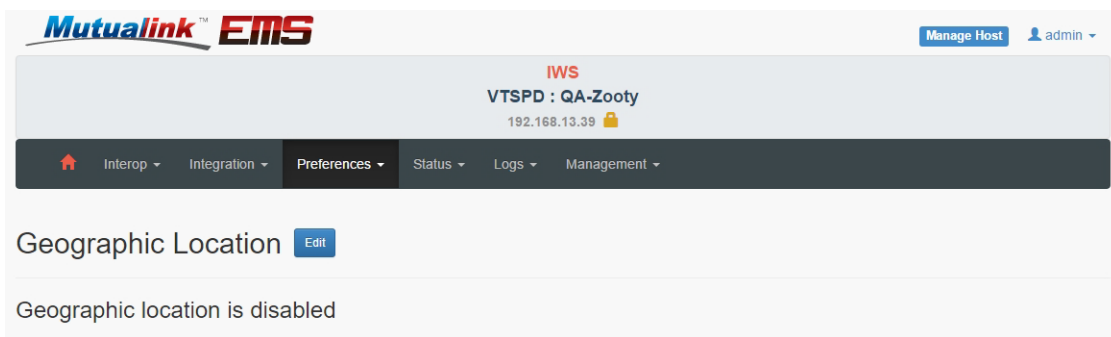


Figure 47. Geographic Location

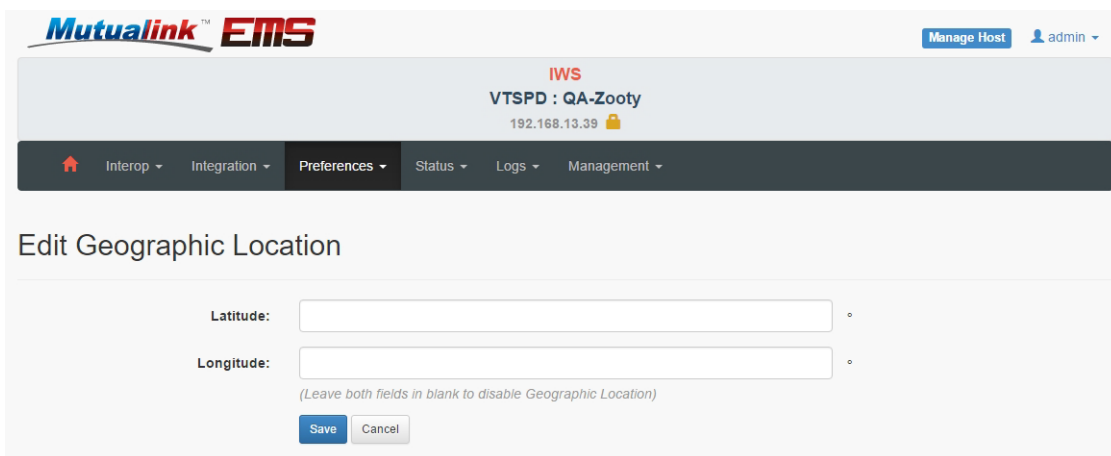


Figure 48. Geographic Location

Set the default latitude and longitude to be announced for this endpoint geographical location.

To disable publishing, send both geographical coordinates blank.

Status

The Status tab allows the following:

- [Endpoint Status on page 52](#)
- [Registered Endpoints on page 53](#)
- [KDS Agent Status on page 54](#)
- [NMS Agent Status on page 55](#)
- [Alarms on page 56](#)
- [Incidents on page 56](#)

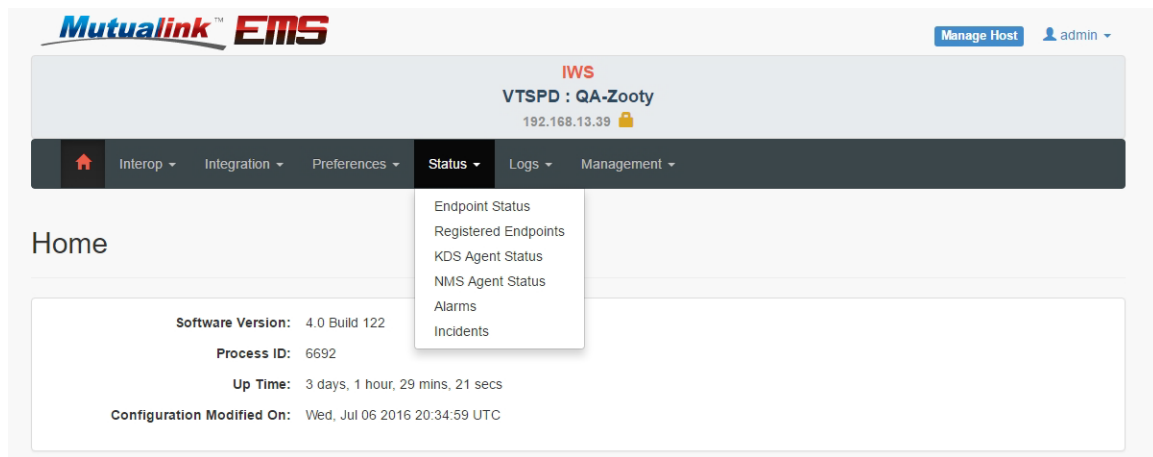


Figure 49. Status

Endpoint Status

The Endpoint Status page under the Status menu shows more detailed high-level status items for this Endpoint.

The screenshot shows the Mutualink EMS IWS interface. At the top, the Mutualink EMS logo is on the left, and 'Manage Host' and 'admin' are on the right. Below the logo, the text 'IWS VTSPD : QA-Zooty' is displayed, followed by the IP address '192.168.13.39' and a lock icon. A navigation bar contains links for Home, Interop, Integration, Preferences, Status (selected), Logs, and Management. The main section is titled 'Endpoint Status' and contains the following information:

- URI: IWS/VTSPD/QA-Zooty
- Type: IWS
- IP Address: 192.168.13.39
- Secured: true
- Multicast Address: 229.9.12.1:5001

Below this is an 'Additional Information' section with the following details:

- SSRC: 0x499c143c (1234965564)
- File sharing enabled? Feature= Yes, Server=Yes, Client=Yes
- Server Directory: /var/ftp/pub
- Server Control Port: 50021
- Vox Enabled? No
- BusyTxLockout? No
- PTTIO: Device=CIB, Status=[DSR=1 CTS=0 CD=1 RI=0 : DTR=0 RTS=0], PttOut=0
- GP02=MicActive
- Current Patch: None
- RTP Rx Enabled? Yes
- RTP Tx Enabled? No
- RTP Tx Active? No
- Selected Patch: (invalid)

Figure 50. Endpoint Status

Registered Endpoints

Displays all the endpoints this EP has auto-discovered on the interconnect network, along with their IP addresses, attributes, etc.

URI	GUID	SIP Address	Secured	Attributes
CHAN/Mutualink/Phone	210-000-21e24d5f74-2452-40a8f01e4d4c	192.168.104.151:5060	🔒	ssrc=1462841228 icon=13 Phone SipTcp 1inv
CHAN/PASPD/MFG-TEST-EVOC-VNIC1	210-000-205c8877a0-54fa-002246104490	192.168.12.131:5060	🔒	ssrc=1462800109 icon=29 Video SipTcp 1inv
CHAN/PASPD/MFG-TEST-IVNIC1	210-000-1fa534b911-8fb9-003018aaf6d	192.168.12.228:5060	🔒	ssrc=1467511706 icon=29 Video SipTcp 1inv
CHAN/PASPD/MFG-TEST-OVNIC1	210-000-1ff405ce90-e16c-003018ae2aa9	192.168.12.74:5060	🔒	ssrc=1467607803 icon=51 SipTcp 1inv
CHAN/PASPD/MFG-TEST-RNIC1	210-000-1ea9c2d074-99ca-003018a766e2	192.168.12.229:5060	🔒	ssrc=1467473228 SipTcp 1inv
CHAN/PASPD/MFG-TEST-TNIC1	210-000-20102604fd-c78b-003018a4beaf	192.168.12.225:5060	🔒	ssrc=1467845245 icon=13 Phone SipTcp 1inv
CHAN/PASPD/MFG-TEST-TNIC2	210-000-20cb398e51-6d84-003018ac074f	192.168.12.75:5060	🔒	ssrc=1467410979 icon=13 Phone SipTcp 1inv
CHAN/RISPD-Boston-Hospitals/Video	210-000-212635e052-b5d6-40f2e933c629	192.168.112.57:5062	🔒	icon=29 Video SipTcp 1inv TalkGroup

Figure 51. Registered Endpoints

KDS Agent Status

Secure Status: Secure

Connection Address: 192.168.12.26:8443

Connection Status: OK

Last Good Transaction: Thu, 28 Jul 2016 14:22:51 UTC +0000

Public Key List ID: 033e0cae-9440-41ae-a73e-d4593080e8dd;2016-07-28 13:28:49+0000

Figure 52. KDS Agent Status

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

- **Addresses and Port:** IP address and TCP port to the KDS web service.
- **Period to update my authorized peer list:** Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.
- **Period to retry authentication request:** Interval at which the EP will contact the remote service to request authentication on a given Agency.

NMS Agent Status

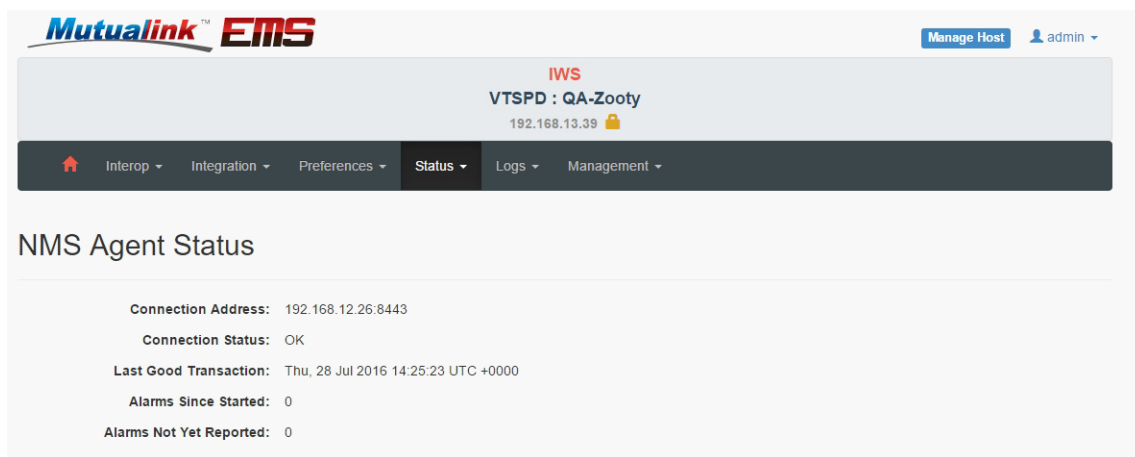


Figure 53. NMS Agent Status

- **Connection Address:** List of IP addresses where the web remote service can be located. More than one address can be entered separated by colons (:) and the EP will try them out in the order listed.
- Connection Status:
- Last Good Transaction:
- Alarms Since Started:
- Alarms Not Yet Reported:
- **Port:** TCP Port where the remote web service can be located.
- **Period to send heartbeat:** Interval at which the EP will send heartbeat messages to the NMS.
- **Period to report alarms:** Interval at which the EP will report new alarms to the NMS. The EP queues new alarms locally and sends them together at this interval

Alarms

Displays any current alarms active on this EP.

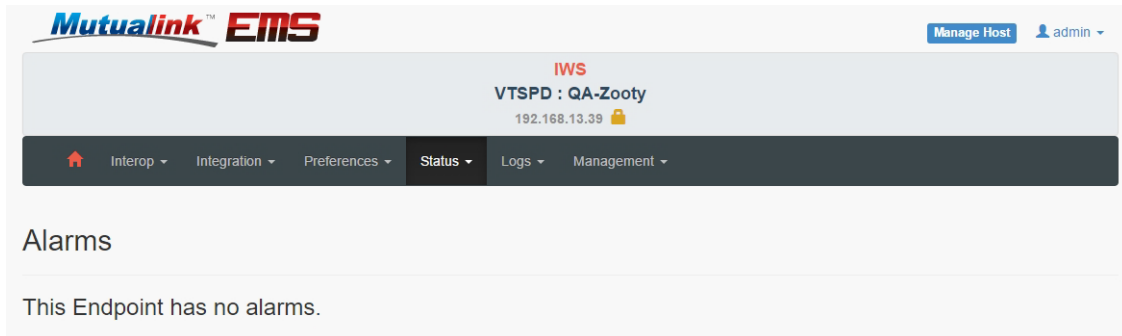


Figure 54. Alarms

Incidents

Displays the incidents and patches that we are a member of, along with associated network information, active SIP sessions, etc.

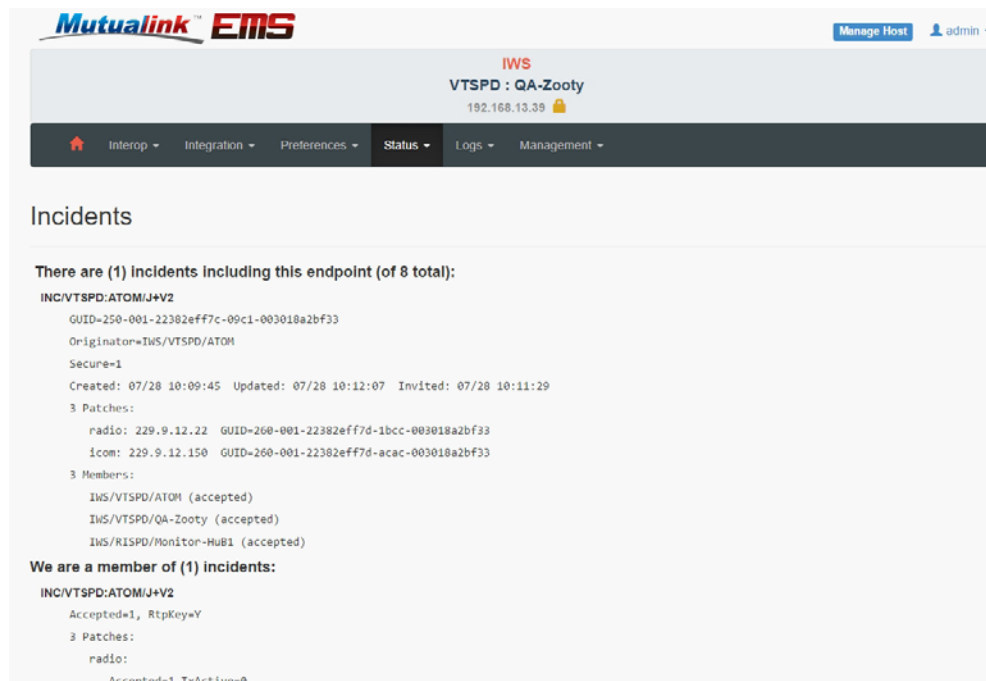


Figure 55. Incidents

Application Logs

To view logs, selection **Application**. The Endpoint logs page allows you can view the Mutualink application logs. The page will show the most recent lines on the selected file. You can view

more lines by changing the default value in the form text box. You can also do a case insensitive search on a list of space separated keywords.

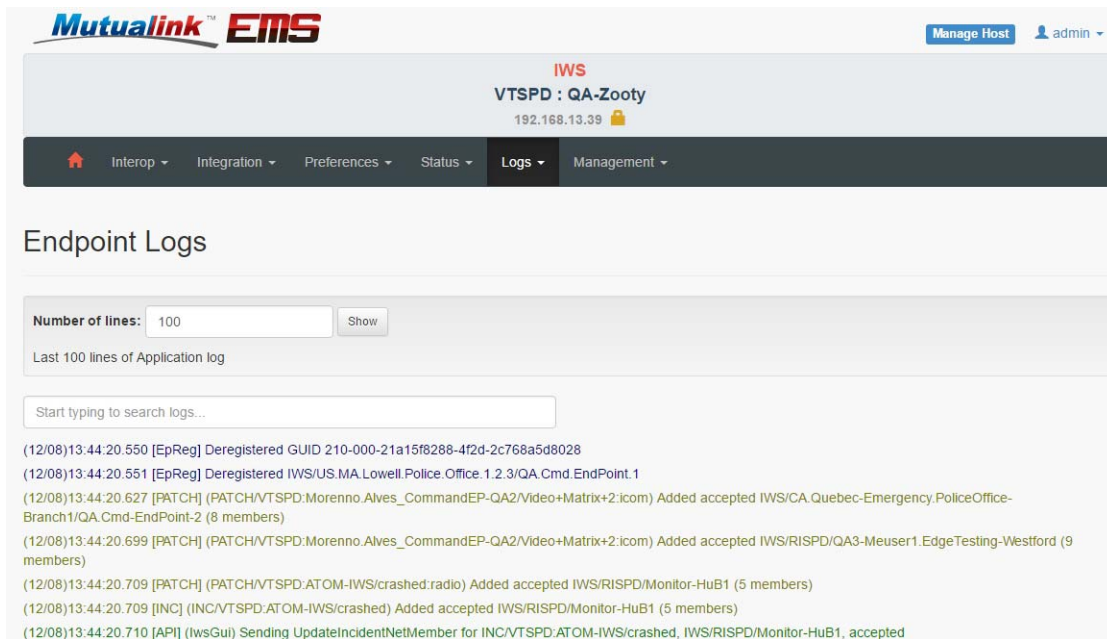


Figure 56. Endpoint Application Logs

Management

The Management tab allows you to view endpoints users and the configuration.

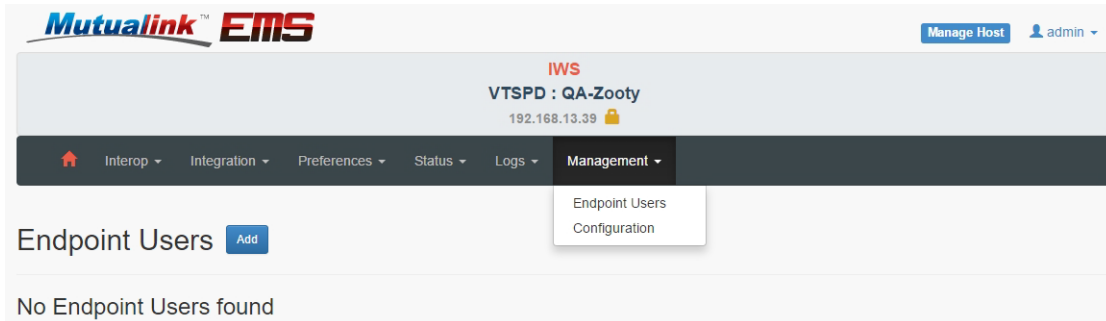


Figure 57. Endpoint Users

Add Endpoint Users

The screenshot shows the 'Add Endpoint User' form. It includes fields for 'Username', 'Password', and 'Confirm Password'. Below these are 'Capabilities' with checkboxes for 'Interactive', 'Audio', 'Transmit Video', 'Receive Video', 'Show Files', 'Receive Files', and 'Transmit Files'. There is also a 'Subnet' field with a note: '(Leave empty to allow connections from all IP addresses)'. At the bottom are 'Save' and 'Cancel' buttons.

Figure 58. Add Endpoint User

Click on the 'External API Users' link to manage the list of users that can connect to the EP on its external application interface. On the 'External API Users' page, you will see a list of the current users and their properties. From this page you can add a new user or edit/delete an existing one.

If you choose to add or edit a user, the external API user form will be displayed. In this form you can specify the name (only for new users), password, allowed capabilities, and subnets from which external clients can connect (using the <address>/<maskbits> format).

The allowed capabilities for an external client are:

- **Interactive:** The client should be presented with dialog boxes that the endpoint generates to request information or report errors and warnings.
- **Audio:** A remote client can request an audio connection (replacing the speakers & microphone connected to the IWS)
- **Transmit Video:** A remote client can send video to the incident (via a helper input V-NIC under control of the IWS).
- **Receive Video:** A remote client can receive video from an incident.
- **Show Files:** File sharing functionality should be exposed to the client.
- **Receive Files:** The client can download files shared by other incident participants.
- **Transmit Files:** The client can share files to an incident.

If no allowed subnet is specified, it will accept connections from all IP addresses.

Configuration

On this page you can view the Endpoint configuration file. You can also perform a backup and restore.

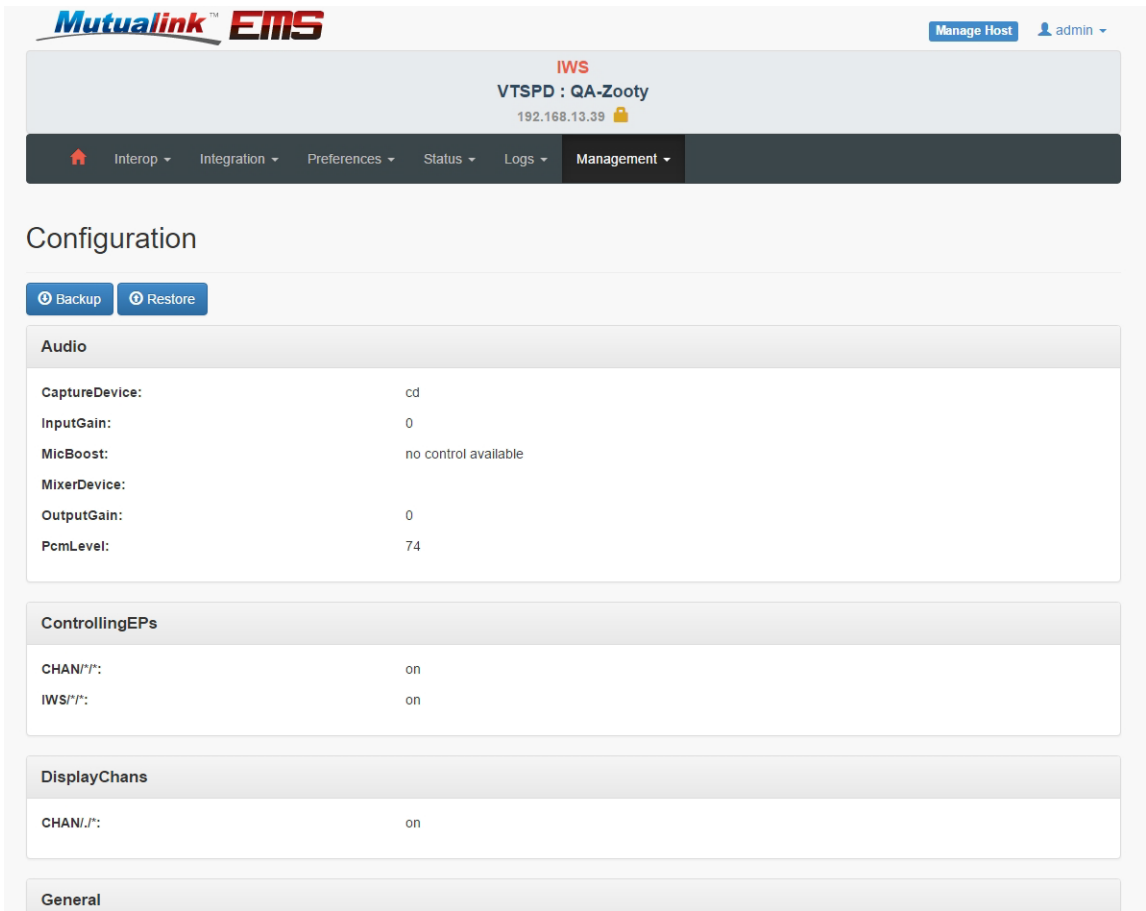


Figure 59. Configuration

Backup

Click on **Backup** to download a copy of the Endpoint configuration file.

Note: Downloads vary depending on your operating system. The figure shown here is from a Windows 10 system.

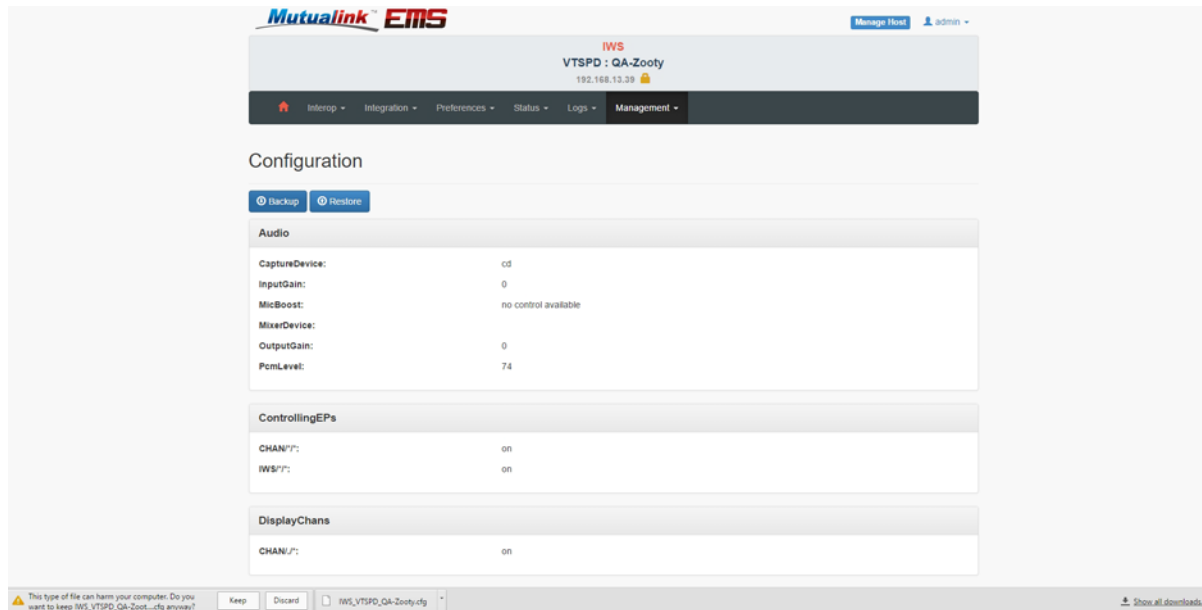


Figure 60. Backup

Restore

To restore a previously backed-up file, click on **Restore** and select the file from your local storage. Then click **Start Upload** to transfer and apply that configuration.

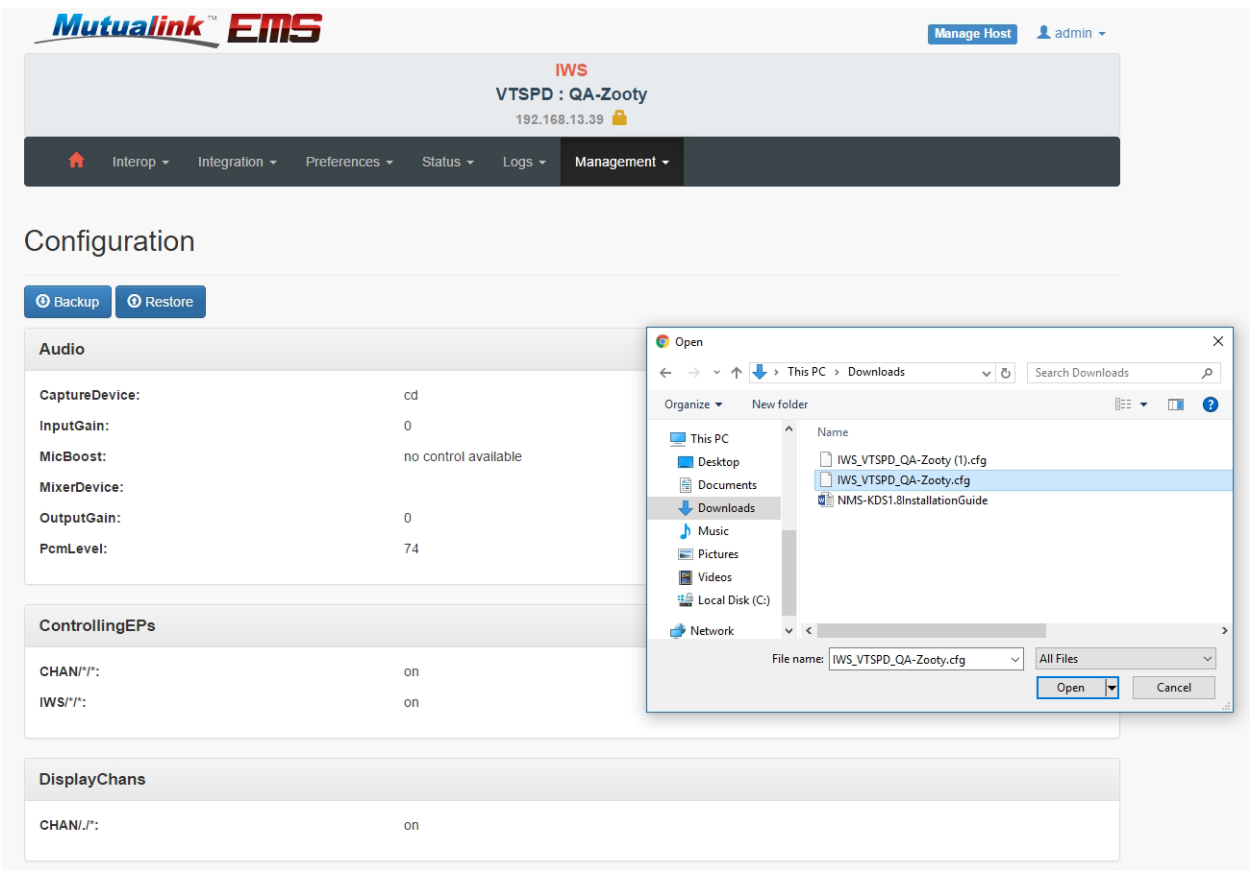


Figure 61. Restore

CHAPTER

4

Radio Network Interface Controller

The Radio Network Interface Controller (R-NIC) integrates radios at all frequency ranges (UHF, VHF, 800MHz) and broadcast protocols whether conventional or trunked, analog or digital.

The R-NIC interfaces with push to talk wireless networks.

This chapter describes each page, the information they display, and the actions you can take from the page(s).

- [R-NIC Home Page on page 64](#)
- [Integration on page 67](#)
- [Preferences on page 74](#)
- [Status on page 76](#)
- [Logs on page 78](#)
- [Management on page 79](#)

R-NIC Home Page

The following sections describe the actions you can take from the tabs. Each page displays informative information.

Note: Each page provides an **Edit** option to modify settings.

Interop

There are six options from the Interop tab.

- Endpoint Identity
- Multicast Network
- Presence Multicast
- KDS Agent
- NMS Agent
- Ciphers
- Controlling Endpoints

Endpoint Identity

The **Endpoint Identity** page displays:

- **GUID:** A 128 bit integer that identifies Mutualink entities across its systems. GUIDs are visually represented as a string of 32 hexadecimal digits, e.g. 210-000-1e65cbb75f-2eb7-0026b9810051, where hyphens are used to separate its main fields for clarity.
- **Agency Name:** The name of this agency/organization. The Agency Name must be unique within the encompassing Mutualink system. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **EP Name:** The name of this EP within this agency/organization. The EP Name must be unique just within the agency as the agency name is prefixed when displaying to the users. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **Current Icon:** The currently-selected "Service Type" icon for this EP. This icon visually represents the type of organization this EP belongs to and what standard services might be offered by this EP.

Multicast Network

The **Multicast Network** page displays the following:

- **Multicast Address:** This determines what other EPs both see this EP and are seen by this EP; must be set to the same value on all EPs that wish to communicate; this is typically assigned by the Mutualink system administrator.
- **Jitter Buffer Size:** The initial size of the RTP receive audio jitter buffer. If a network is very bursty, a higher value would be better here, but the end-to-end voice delay increases correspondingly. In reality, our EPs have a fairly good automatic jitter buffer that automatically sizes itself as required, so this parameter should probably be left at the default value.

Presence Multicast

The **Presence Multicast** determines what other EPs both see this EP and are seen by this EP on the Global network.

This value must be set to the same value on all EPs that wish to communicate on the Global network.

KDS Agent

The **KDS Agent** page displays:

- **Addresses and Port:** IP address and TCP port to the KDS web service (see Network Monitoring Service for details).
- **Update List Period:** Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.
- **Validation Retry Period:** Interval at which the EP will contact the remote service to request authentication on a given Agency.

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

NMS Agent

The **NMS Agent** window displays the following:

- **Addresses:** List of IP addresses where the web remote service can be located. More than one address can be entered separated by colons (:) and the EP will try them out in the order listed.
- **Port:** TCP Port where the remote web service can be located.
- **Heartbeat Period:** Interval at which the EP will send heartbeat messages to the NMS.
- **Alarm Read Period:** Interval at which the EP will report new alarms to the NMS. The EP queues new alarms locally and sends them together at this interval.

Ciphers

The **Ciphers** window displays the incident cipher. You can edit the cipher.

Controlling Endpoints

This is the list of IWSs that are authorized to control this NIC. If an IWS that is not in this list attempts to invite this NIC to an incident or otherwise exercise control over it, the request will be rejected.

Integration

The **Intergration** tab allows you to view or perform:

- Device Interface
- External Channels
- RX Interface
- DigiRIB Settings
- DigiRIB Profiles
- PTT Device
- Relay RTP

Device Interface

The Device Interface has different fields depending on the Rx Interface Mode setting selected.

PTT to Voice Out Delay: If the external device requires time to prepare to receive audio after the PTT-Out signal is activated (e.g. a trunked radio system requires time to acquire a transmit channel before we can send it audio), configure that time here. Note that this may also be enabled for non-PTT devices if desired (e.g. to set a constant receive audio delay) for special situations.

- **Enable Busy Channel Lockout:** Enabling this setting will prevent audio being transmitted to the device/accessory while audio is being received from it. Sort of the reverse of VOX Half-duplex, but applicable for both PTT and VOX modes. When this setting is enabled for half-duplex radios, this will prevent incident transmissions from keying up the radio while it is already receiving an over-the-air transmission.
- **TxGrant truncates PTT to Voice Out Delay:** If the TxGrant signal goes active during the PTT to Voice Out Delay period, this means that the channel was successfully acquired and the delay can be terminated, thereby allowing audio to flow freely to the radio.
 - **Debounce time for the TxGrant signal:** On some radios, the TxGrant signal will get spurious active indications – this value may be increased until those undesired activations are ignored.
 - **TxGrant signal minimum duration:** Minimum time that the TxGrant signal must be asserted before the application acknowledges and processes the event. For some integrations, this time must be larger than the optimum debounce time, so the operator can use this parameter to increase the time necessary to validate the asserted signal without affecting back-to-back transmissions from the incident. Enter 0 or leave empty if this is not needed.

- **Radio Monitor:** When enabled this allows the operator to hear all transmissions on any logical channel sharing the same frequency. The operator should use this function to determine if the frequency is clear before using the frequency for his purposes. In the Mutualink case, an IWS can activate the monitor function on the radio via the R-NIC. Any audio received from the device under integration while in monitor mode is transmitted to the incident as any other audio is.

External Channels

The External Channels is an optional feature to enable the multi-channel capability of R-NICs and analog input V-NICs. R-NICs may currently have two external channels defined. The channel in use is controlled by the assigned output control line of the USB RIB or pin number 6 of the serial RIB, which may either go directly to the radio/device, or may control an internal EIA Tone option board. Analog input V-NICs have four video input ports/channels, of which only one may be in use at any time.

In R-NICs, you can also specify the time in milliseconds that it should pulse PTT when the external channel is changed (default is 0).

If a NIC only has channel 1 available/connected, then there is no need to populate these fields – the NIC will always use channel 1 by default.

When a multi-channel NIC is invited to an incident by an IWS, the IWS user will be prompted for which of the available (non-blank) channels should be used by the NIC in this incident. This prompt will contain the channel names populated in these fields, so these names should make sense to any controlling IWS user.

RX Interface

The different fields depending on the Rx Interface Mode setting selected.

- **Interface Mode:** This setting controls how audio is received from a connected device or accessory. Mode selection does not take effect immediately if the NIC is already in an incident. It will take effect when the NIC joins the next incident.
 - **PTT/COR (or just PTT):** The receive audio is controlled by the presence of a PTT/COR signal. When this signal is active, audio is assumed to be present; when it's inactive, audio is ignored. This setting is appropriate for R-NICs that have a PTT-In or COR/TOR signal defined as well as IWSs that use the IWS GUI or external device to indicate a PTT. This is the only valid value for IWSs.
 - **VOX Full-Duplex:** When there is no available control signal to indicate when audio is present, the VOX (Voice Operated Xmission) feature is used. This feature basically assumes that valid audio is present when the audio level rises above a

specific threshold. Full-duplex means that audio may be simultaneously received from and transmitted to the connected device.

- **VOX Half-duplex:** Similar to VOX Full-duplex, this setting will prevent audio from being received from the device while we are transmitting audio to it. This should be used for devices that reflect back the transmitted audio signal in some way (even if it's a PTT-beep, etc.). If you have trouble with a NIC kicking back an audio signal every time it receives an incident transmission, this may be the setting for you.
- **VOX Delay:** This is the minimum amount of time (in milliseconds) that the audio signal must be above the VOX Level to be considered a valid audio signal. Increase this if the audio line is subject to short bursts of noise, but a value too high risks truncating the start of the audio signal.
- **VOX Level:** Sets the VOX audio threshold; an audio signal above this level is considered valid receive audio, any signal below is ignored. Note that this value is in the same logarithmic units as the Input Level display so the values can be correlated.
- **Hang Time:** [PTT Mode only] This sets the amount of time after we drop PTT-Out (at the end of a transmission) when a “phantom” COR/TOR/PTT-In signal could be activated. Typically only applicable for a simplex repeated radio channel, this occurs when the radio switches to receive mode after it transmits and receives a remnant of its own transmission (due to configuration of Hang Time on the repeater). During this period, we will ignore the state of the COR/TOR/PTT-In signal.
- **Hang Time VOX:** If this is enabled, the NIC will automatically switch to VOX mode only during the above Hang Time period. This allows the NIC to receive a valid response to its transmission (for example)
- **AutoDetect Output:** This feature assists in the configuration of the above settings. For each AutoDetect run, PTT will be keyed and released, then we will monitor the incoming control lines and audio levels to try and discover the optimal values. This should be run several times to get a good sampling, and it must be done while no radio traffic is active – if any radio traffic is present, the AutoDetect results should be invalidated. Once good values are determined, they may be tweaked as necessary before clicking the Save button.

Digital RIB (DigitRIB) Settings

The Digital RIB page allows you to edit, download, or save the current settings.

General

- **Control Signal Voltage Source:** Source of the reference voltage for input and output signals. The source can be the internal +5v supply, an internal +12v supply (if

the R-NIC is so equipped), or an external power supply that is connected to the device integration connector.

Control Inputs

For each function listed select a value for the following parameters:

- **Pin Numbers:** Pin on the device integration connector at which the specified function will accept input.
- **Active Level:** Controls whether a high voltage (the reference voltage level) is a logic "true" (active high) or "false" (active low) signal.
- **Debounce Time:** Specifies the number of milliseconds that an input must maintain a consistent value before the Mutualink software recognizes the signal as valid.

Mutualink software currently supports the following input control functions:

- **PTT In:** Indicates the device under integration is receiving an audio signal to be transmitted to the Mutualink network.
- **TX Grant:** Indicates the device under integration is granting the Mutualink software permission to transmit audio to the device.

Control Outputs

For each function listed select a *Pin Number* and an *Active Level* value.

Mutualink software currently supports the following output control functions:

- **PTT Out:** Triggers the device under integration to allow the Mutualink software to transmit audio to the device.
- **Power Enable:** Allows the Mutualink software to power-up the device under integration upon startup.
- **Channel Select:** Allows the Mutualink software to select a channel to be used for transmission per the configuration of the device under integration.
- **Monitor:** Provide access to the device under integration monitor capability. This capability allows the operator to hear all transmissions on any logical channel sharing the same frequency.

Audio

For Tx & Rx audio, select a value for the following parameters:

- **Interface Mode:** Provides control over the type of audio interface of the device under integration.
 - *Single-mode* consists of a single line referenced to ground.
 - *Differential* consists of a pair of balanced lines - one positive signal, one negative signal.
 - *Use Tx (2-wire)* mode available for the receive mode directs the Mutualink system to switch a single set of lines between receive and transmit modes.
- **Termination:** Controls what impedance, if any, should be applied to the audio line.
- **Max Voltage:** Specifies the intended voltage range the audio interface to the device under integration.

Download DigitRIB Settings

The download varies depending on your operating system.

Download

To download a copy of the currently settings as a profile, click on *Download*. The downloaded text file can then be shared and uploaded into other R-NICs.

Save

Any given configuration can be saved in a user profile so that it can be restored later if needed. To save it, click on *Save* and enter a name for the new profile. The input field will display a list of available profiles so that you can either overwrite an existing profile or edit an existing name to follow some convention. If the profile is saved successfully, you will see it listed as a user profile the next time you click on [Digital RIB Profiles](#).

You cannot overwrite factory profiles. If you select a factory profile from the list, it will save a copy as a user profile using the same name.

Digital RIB Profiles

Radio Cable Cross Reference

This provides the list of cables and connectors are suitable for a profile. This list maybe updated at any time by Mutualink.

Upload Profile

To load a profile:

1. Click on *Upload Profile*.
2. Select a file to upload.

If you want to rename the file, enter the desired name on the *Profile Name* field.

3. Click *Start Upload* to transfer and install the profile on the R-NIC.

The uploaded profile will be shown as a user profile on the *DigiRIB Profiles* page.

Set Current Settings from a Profile (Apply)

Configurations for well known device integrations can be applied from saved profiles rather than setting every parameter from scratch. These profiles can be pre-loaded at manufacturing (Factory Profiles) or saved by the user (User Profiles).

To load a profile:

1. Click on the corresponding tab and look for the desired profile from the list shown.
2. Click **Apply** and the configuration specified in the selected profile is applied dynamically to the Endpoint (no restart is needed).

If the profile is loaded successfully, its name will be shown at the top of the [Digital RIB \(DigiRIB\) Settings](#).

Downloading Profiles

To download a Digital RIB Profiles click on the down arrow next to Apply.

Deleting Profiles

If a saved user profile is not needed any more it can be deleted. Look for the desired profile and then click *Delete* on the corresponding entry. Notice that users cannot delete factory profiles and therefore the *Delete* button will not be shown for those entries.

PTT Device

The PTT device window allows configuration of protocol-based advanced radio integrations. The installer must verify that the radios are configured correctly with regard to serial port parameters (baud, data bits, stop bits, parity, flow control). An incorrect configuration will result in a nonfunctional integration. Cable diagrams and radio programming notes are available for the currently integrated radios.

Each type of PTT Device requires specific information based on configuration of the attached device or where cables are physically plugged in:

- **PTT Wire Interface:** DigiRIB using GPIO controls.

- **QChat:** The serial port device will be something like /dev/digiSerial1 to address the DigiRIB embedded serial port. The *Bridge Phone Number* is the phone number of the phone embedded in the QChat bridge.
- **MotoTRBO:** Specify the address of the connected radio.
- **Tone Remote:** Playing tones over the DigiRIB
- **P25:** Covers the Kenwood P25, Tait and Sepura radios where control path is over the embedded serial port in the DigiRIB. For Kenwood or Tait protocols: Serial Port Device will be /dev/digiSerial1 (for a single radio instance), Baud rate should be 9600, 8 data bits, stop bits are 1 for Tait, 2 for Kenwood, no parity and no hardware flow control. For Sepura protocol: Serial Port Device will be /dev/sepuraSerial1, Baud rate should be 38400, 8 data bits, stop bit is 1, no parity and no hardware flow control.

Relay RTP

At this time, this parameter is meaningful only for T-NICs and IP V-NICs on multi-homed systems. It selects the interface that the Endpoint will use to open an RTP stream to a static destination IP address.

You can select between the **Primary** or **Secondary** interfaces, or you can enter an interface name or IP address manually on the combo-box.

Preferences

The **Preferences** tab allows you to view or perform:

- Audio
- Audio Codec
- Geographic Location

Audio

The following parameters only apply to IWSs and NICs using the built-in sound device (as opposed to external audio devices or accessories).

- **Input Level**

By clicking the Refresh button, the current Input level as read from the audio input line will be displayed. This allows the administrator to see what relative effect the Input Gain and Boost settings have on the input signal. Note that this level is in logarithmic units and is not correlated to dB, etc.

- **Input Gain**

Gain to apply to the input audio signal from external devices (via Mic In or Line In).

- **Output Gain**

Gain to apply to the output audio signal sent to external devices (via Line Out)

- **Output Test Tone**

This feature allows the administrator to send a test tone on the audio output line to the external device for measurement, calibration, etc. The length of the tone can be set and the PTT line can optionally be activated during the tone. To stop the tone before the time elapses, click the Stop Tone button.

Note: Make sure the EP is idle before using this test as it will interfere with the EP's functionality.

Audio Codec

Select from the list the audio codec that this endpoint will use when participating in an incident.

Available selections are:

- G711U
- G729B
- G711U (preferred), G729B (alternate)

- G729B (preferred), G711U (alternate)

Geographic Location

Set the default latitude and longitude to be announced for this endpoint geographical location.

To disable publishing, leave both geographical coordinates blank.

Status

The Status tab allows the following:

- Endpoint Status
- Registered Endpoints
- KDS Agent Status
- NMS Agent Status
- Alarms
- Incidents

Endpoint Status

The **Endpoint Status** page shows more detailed high-level status items for this Endpoint.

Registered Endpoints

Displays all the endpoints this endpoint has auto-discovered on the interconnect network, along with their IP addresses, attributes, etc.

KDS Agent Status

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

- **Addresses and Port:** IP address and TCP port to the KDS web service.
- **Period to update my authorized peer list:** Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.
- **Period to retry authentication request:** Interval at which the EP will contact the remote service to request authentication on a given Agency.
- **Connection Address:** List of IP addresses where the web remote service can be located. More than one address can be entered separated by colons (:) and the EP will try them out in the order listed.
- **Connection Status:** Details status of connection.
- **Last Good Transaction:** Time of transaction.
- **Alarms Since Started:** Number of queued alarms.
- **Alarms Not Yet Reported:** Number of new alarms queued but not reported.
- **Port:** TCP Port where the remote web service can be located.

- **Period to send heartbeat:** Interval at which the EP will send heartbeat messages to the NMS.
- **Period to report alarms:** Interval at which the EP will report new alarms to the NMS. The EP queues new alarms locally and sends them together at this interval

Alarms

Displays any current alarms active on this EP.

Incidents

Displays the incidents and patches that we are a member of, along with associated network information, active SIP sessions, etc.

Logs

To view logs, selection **Application**. The Endpoint logs page allows you can view the Mutualink application logs. The page will show the most recent lines on the selected file.

You can view more lines by changing the default value in the form text box. You can also do a case insensitive search on a list of space separated keywords.

Management

The Management tab allows you to view endpoints users and the configuration.

API Users

Click on the 'External API Users' link to manage the list of users that can connect to the EP on its external application interface. On the 'External API Users' page, you will see a list of the current users and their properties. From this page you can add a new user or edit/delete an existing one.

If you choose to add or edit a user, the external API user form will be displayed. In this form you can specify the name (only for new users), password, allowed capabilities, and subnets from which external clients can connect (using the <address>/<maskbits> format).

The allowed capabilities for an external client are:

- **Interactive:** The client should be presented with dialog boxes that the endpoint generates to request information or report errors and warnings.
- **Audio:** A remote client can request an audio connection (replacing the speakers & microphone connected to the IWS)
- **Transmit:** VideoA remote client can send video to the incident (via a helper input V-NIC under control of the IWS).
- **Receive Video:** A remote client can receive video from an incident.
- **Show Files:** File sharing functionality should be exposed to the client.
- **Receive Files:** The client can download files shared by other incident participants.
- **Transmit Files:** The client can share files to an incident.

If no allowed subnet is specified, it will accept connections from all IP addresses.

Configuration

On this page you can view the Endpoint configuration file. You can also perform the following.

- Backup
 - Download a copy of the Endpoint configuration file.
- Restore
 - Restores a previously backed-up file. You select the file from your local storage and start the upload to transfer and apply that configuration.

Restart Endpoint

To restart a NIC click on the corresponding button at the Restart menu page. Currently, IWS appliances cannot be restarted from the web page. You have to reboot the whole system.

Restart

To restart a NIC click on the corresponding button at the Restart menu page. Currently, IWS appliances cannot be restarted from the web page. You have to reboot the whole system.

CHAPTER

5

Telephone Network Interface Controller

Mutualink's Telephony Network Interface Controller (T-NIC) Series of Secure Controllers allows any telephone, anywhere on earth, to participate with two-way radio systems in incidents on both an inbound and outbound basis.

Mutualink's T-NIC serves as a gateway to the telephony network via several interfaces. The native VoIP interface takes advantage of either SIP or RTP standards to interface with external VoIP PBXs or PSTN gateways; POTS interfaces are achieved through station interfaces. The T-NIC allows users to either call out to specific phone numbers or alternatively callers can dial into the T-NIC to participate in an incident.

T-NIC Home Page

The following sections describe the actions you can take from the tabs. Each page displays informative information.

Note: Each page provides an **Edit** option to modify settings.

To select a T-NIC:

1. Click **Show All Instances**.
2. From the **Endpoints Enabled on Host List** select a T-NIC.

The T-NIC Home page displays.

Interop

There are six options from the **Interop** tab.

- [Endpoint Identity](#)
- [Multicast Network](#)
- [Presence Multicast](#)
- [KDS Agent](#)
- [NMS Agent](#)
- [Controlling Endpoints](#)

Endpoint Identity

The **Endpoint Identity** page displays:

- **GUID**

A 128 bit integer that identifies Mutualink entities across its systems. GUIDs are visually represented as a string of 32 hexadecimal digits, e.g. 210-000-1e65cbb75f-2eb7-0026b9810051, where hyphens are used to separate its main fields for clarity.
- **Agency Name**

The name of this agency/organization. The Agency Name must be unique within the encompassing Mutualink system. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **EP Name**

The name of this EP within this agency/organization. The EP Name must be unique just within the agency as the agency name is prefixed when displaying to the users. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **Current Icon**

The currently-selected "Service Type" icon for this EP. This icon visually represents the type of organization this EP belongs to and what standard services might be offered by this EP.

Multicast Network

The **Multicast Network** page displays the following:

- **Multicast Address**

This determines what other EPs both see this EP and are seen by this EP; must be set to the same value on all EPs that wish to communicate; this is typically assigned by the Mutualink system administrator.

- **Jitter Buffer Size**

The initial size of the RTP receive audio jitter buffer. If a network is very bursty, a higher value would be better here, but the end-to-end voice delay increases correspondingly. In reality, our EPs have a fairly good automatic jitter buffer that automatically sizes itself as required, so this parameter should probably be left at the default value.

Presence Multicast

The **Presence Multicast** determines what other EPs both see this EP and are seen by this EP on the Global network.

This value must be set to the same value on all EPs that wish to communicate on the Global network.

KDS Agent

The **KDS Agent** page displays:

- **Addresses and Port**

IP address and TCP port to the KDS web service (see Network Monitoring Service for details).

- **Update List Period**

Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.

- **Validation Retry Period**

Interval at which the EP will contact the remote service to request authentication on a given Agency.

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

NMS Agent

The **NMS Agent** window displays the following:

- **Addresses**

List of IP addresses where the web remote service can be located. More than one address can be entered separated by colons (:) and the EP will try them out in the order listed.

- **Port**

TCP Port where the remote web service can be located.

- **Heartbeat Period: Interval at which the EP will send heartbeat messages to the NMS.**

- **Alarm Read Period**

Interval at which the EP will report new alarms to the NMS. The EP queues new alarms locally and sends them together at this interval.

Controlling Endpoints

This is the list of IWSs that are authorized to control this NIC. If an IWS that is not in this list attempts to invite this NIC to an incident or otherwise exercise control over it, the request will be rejected.

Integration

The **Intergration** tab allows you to view or perform:

- [Rx Interface](#)
- [VoIP Incoming Calls](#)
- [VoIP Outgoing Calls](#)
- [VoIP Registration](#)
- [VoIP Media](#)
- [Relay RTP](#)

Rx Interface

The **RX Interface** has different fields depending on the Rx Interface Mode setting selected.

- **Interface Mode**

This setting controls how audio is received from a connected device or accessory. Mode selection does not take effect immediately if the NIC is already in an incident. It will take effect when the NIC joins the next incident.

- **VOX Full-Duplex:** When there is no available control signal to indicate when audio is present, the VOX (Voice Operated Xmission) feature is used. This feature basically assumes that valid audio is present when the audio level rises above a specific threshold. Full-duplex means that audio may be simultaneously received from and transmitted to the connected device.
- **VOX Half-duplex:** Similar to VOX Full-duplex, this setting will prevent audio from being received from the device while we are transmitting audio to it. This should be used for devices that reflect back the transmitted audio signal in some way (even if it's a PTT-beep, etc.). If you have trouble with a NIC kicking back an audio signal every time it receives an incident transmission, this may be the setting for you.

- **VOX Delay**

This is the minimum amount of time (in milliseconds) that the audio signal must be above the VOX Level to be considered a valid audio signal. Increase this if the audio line is subject to short bursts of noise, but a value too high risks truncating the start of the audio signal.

- **VOX Level**

Sets the VOX audio threshold; an audio signal above this level is considered valid receive audio, any signal below is ignored. Note that this value is in the same logarithmic units as the Input Level display so the values can be correlated.

VoIP Incoming Calls

This feature allows incoming SIP calls to initiate incidents to selected endpoints. When a SIP incoming call is received, the target SIP username is checked against this list; if a match is found, an incident is initiated to the specified endpoint. If no match is found but a catch-all entry is present, the incident will be initiated to the catch-all target endpoint. If neither of these situations apply, then the call will be rejected.

VoIP Outgoing Calls

By default, the T-NIC uses the SIP protocol for outgoing calls so it can call any VoIP device.

0.0.0.1 SIP Address Destination

When SIP is enabled (by selecting *SIP address*), the following settings are available:

- **Enable SIP over TCP**

Whether SIP uses TCP or UDP as a transport to external VoIP devices. TCP is preferred due to the guaranteed delivery attributes, but some older SIP devices do not yet support TCP.

- **Static SIP destination**

If this is populated, the T-NIC will call this SIP address every time it is invited into an incident; the IWS user will not even be asked for an address/number to call. This is useful for "hotline" type applications that support SIP.

- **Default SIP domain or outbound proxy**

If the destination address from the IWS user does not include a domain/hostname (e.g. phone numbers), what SIP domain should these calls be forwarded to? By default, this is the local host (IP pseudo-address 127.0.0.1) if an embedded asterisk PBX is installed. If you're using an outbound SIP proxy to route external outbound SIP calls, use this field to specify its address. To specify a custom port append the address with the corresponding port value, i.e. `<address>:<port>`.

- **Display Name**

Display name for external calls and registration, for example "Bob Smith".

- **Username**

SIP username for external calls, registration and authentication.

- **Password**

Password used for authenticating the username at the specified realm. Used only if authentication is requested.

- **Authentication Realm**

The name of the authentication realm for outgoing calls (if different from outbound proxy). Used only if authentication is requested.

- **Enable sending DTMFs via SIP INFO**

If this is enabled (the default), we will enable sending DTMF codes via SIP INFO messages instead of in-band or by using RFC4733 RTP.

- **Prefer SIP INFO over RFC4733**

If both methods are supported by an external device, which method should we use?

0.0.0.2 Static IP Address Destination

If the use of SIP is disabled (by selecting *Static IP Address*), then the T-NIC will connect to a specific IP address every time it is invited into an incident; the IWS user will not even be asked for an address/number to call. This is useful for “hotline” type applications that do not support SIP. In this mode, the following settings are available:

- **Destination IP address**

The static IP address to connect to – this may be either a unicast or multicast address.

- **Destination RTP port**

The UDP port on the destination IP address to send RTP (voice) packets to.

- **Local RTP port**

The local port that the far end device should send RTP packets to. If using a multicast address, this port must be the same as the Destination RTP Port. Leave this blank to use the default.

- **Codec**

What voice codec should the RTP packets use? All devices will typically support PCM uLaw – only choose Linear16 if required by the far end device.

- PCM uLaw:

- **Payload Type:** For Linear16, what dynamic RTP payload type should be used? This must agree with the far end device configuration.

VoIP Registration

SIP registration is used for routing incoming calls. The registration consists of the T-NIC telling a SIP Registrar where it can be reached for incoming calls (that is, when somebody makes a SIP call to that user).

When this option is selected the form will show the following configuration options:

- **Duration of registration**

Number of seconds during which our registration should be valid. After this time passes, the T-NIC will re-register. A value of 300-600 seconds (5-10 minutes) is typical.

- **Retry period on failure**

Number of seconds after which the T-NIC will retry a failed registration attempt.

- **SIP Server Address**

The IP address or hostname of the SIP registrar we will register with. Leave this field empty if it will use the same address as the outbound proxy used for outgoing calls. While many simple SIP deployments use the same address for the outbound proxy and the registrar, larger deployments may use different servers for each of these functions.

- **Display Name**

Display name for registration (if different from display name used outgoing calls).

- **Username**

SIP username used for registration (if different from username used outgoing calls).

- **Password**

Password used for authenticating the username at the specified realm (if different from password used outgoing calls). Used only if authentication is requested.

- **Authentication Realm**

The name of the authentication realm for registrations (if different from the registrar address). Used only if authentication is requested.

VoIP Media

The following settings are available whether SIP is enabled or not:

- **RTCP Interval**

Number of seconds between RTCP transmissions; 10 seconds is a good default. Enable RTCP if the far end device(s) supports it. Leave blank to disable RTCP.

- **DTMF duration**

Duration of the DTMF “on” period in milliseconds. Don't change unless required.

- **DTMF inter-digit pause**

How long to pause between DTMF digits in milliseconds. Don't change unless required.

- **Send DTMFs inband**

Enable to send DTMF tones in the inband audio stream as well as out-of-band using either RFC4733 or SIP INFO. This is not recommended unless required for a special application.

Relay RTP

At this time, this parameter is meaningful only for T-NICs and IP V-NICs on multi-homed systems. It selects the interface that the Endpoint will use to open an RTP stream to a static destination IP address.

You can select between the **Primary** or **Secondary** interfaces, or you can enter an interface name or IP address manually on the combo-box.

Preferences

The **Preferences** tab allows you to view or perform:

- [Audio Codec](#)
- [Geographic Location](#)

Audio Codec

Select from the list the audio codec that this endpoint will use when participating in an incident.

Available selections are:

- G711U
- G729B
- G711U (preferred), G729B (alternate)
- G729B (preferred), G711U (alternate)

Geographic Location

Set the default latitude and longitude to be announced for this endpoint geographical location.

To disable publishing, leave both geographical coordinates blank.

Status

The Status tab allows the following:

- Endpoint Status
- Registered Endpoints
- KDS Agent Status
- NMS Agent Status
- Alarms
- Incidents

Endpoint Status

The **Endpoint Status** page shows more detailed high-level status items for this Endpoint.

Registered Endpoints

Displays all the endpoints this endpoint has auto-discovered on the interconnect network, along with their IP addresses, attributes, etc.

KDS Agent Status

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

- Addresses and Port: IP address and TCP port to the KDS web service.
- Period to update my authorized peer list: Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.
- Period to retry authentication request: Interval at which the EP will contact the remote service to request authentication on a given Agency.

NMS Agent Status

The Network Monitoring Service (NMS agent) page displays:

- Connection Address
- Connection Status
- Last Good Transaction
- Alarms Since Started
- Alarms Not Yet Reported

Alarms

Displays any current alarms active on this EP.

Incidents

Displays the incidents and patches that we are a member of, along with associated network information, active SIP sessions, etc.

Logs

To view logs, selection **Application**. The Endpoint logs page allows you can view the Mutualink application logs. The page will show the most recent lines on the selected file.

You can view more lines by changing the default value in the form text box. You can also do a case insensitive search on a list of space separated keywords.

Management

The Management tab allows you to view endpoints users and the configuration.

API Users

API Users manages the list of users that can connect to the EP on its external application interface. On the 'External API Users' page, you will see a list of the current users and their properties. From this page you can add a new user or edit/delete an existing one.

If you choose to add or edit a user, the external API user form will be displayed. In this form you can specify the name (only for new users), password, allowed capabilities, and subnets from which external clients can connect (using the <address>/<maskbits> format).

The allowed capabilities for an external client are:

- **Interactive**

The client should be presented with dialog boxes that the endpoint generates to request information or report errors and warnings.

- **Audio**

A remote client can request an audio connection (replacing the speakers & microphone connected to the IWS)

- **Transmit**

VideoA remote client can send video to the incident (via a helper input V-NIC under control of the IWS).

- **Receive Video**

A remote client can receive video from an incident.

- **Show Files**

File sharing functionality should be exposed to the client.

- **Receive Files**

The client can download files shared by other incident participants.

- **Transmit Files**

The client can share files to an incident.

If no allowed subnet is specified, it will accept connections from all IP addresses.

Configuration

On this page you can view the Endpoint configuration file. You can also perform the following.

- **Backup**

Download a copy of the Endpoint configuration file.

- **Restore**

Restores a previously backed-up file. You select the file from your local storage and start the upload to transfer and apply that configuration.

Restart

To restart a NIC click on the corresponding button at the Restart menu page. Currently, IWS appliances cannot be restarted from the web page. You have to reboot the whole system.

CHAPTER

6

Video Network Interface Controller

On V-NICs, a button is provided to switch between the input and output types. When clicked, the windows change back and fourth.

Both windows display software version, and the date and time the configuration was modified on.

V-NIC Home Page

The following sections describe the actions you can take from the tabs. Each page displays informative information.

Note: Each page provides an **Edit** option to modify settings.

To select a T-NIC:

1. Click **Show All Instances**.
2. From the **Endpoints Enabled on Host List** select a V-NIC.

The V-NIC Home page displays.

Change to Output or Input Video

The following screens shows example of the Home page when you change from either output or input V-NIC.

Once you click, the button changes to **Change to Input V-NIC** and a message displays that the endpoint has changed.

To change back, click **Change to Input V-NIC**.

Interop

There are six options from the **Interop** tab.

- [Endpoint Identity](#)
- [Multicast Network](#)
- [Presence Multicast](#)
- [KDS Agent](#)
- [NMS Agent](#)
- [Controlling Endpoints](#)

Endpoint Identity

The **Endpoint Identity** page displays:

- **GUID**

A 128 bit integer that identifies Mutualink entities across its systems. GUIDs are visually represented as a string of 32 hexadecimal digits, e.g. 210-000-1e65cbb75f-2eb7-0026b9810051, where hyphens are used to separate its main fields for clarity.
- **Agency Name**

The name of this agency/organization. The Agency Name must be unique within the encompassing Mutualink system. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **EP Name**

The name of this EP within this agency/organization. The EP Name must be unique just within the agency as the agency name is prefixed when displaying to the users. See the Mutualink EP Naming Conventions document for production EP requirements here.
- **Current Icon**

The currently-selected "Service Type" icon for this EP. This icon visually represents the type of organization this EP belongs to and what standard services might be offered by this EP.

Multicast Network

The **Multicast Network** page displays the following:

- **Multicast Address**

This determines what other EPs both see this EP and are seen by this EP; must be set to the same value on all EPs that wish to communicate; this is typically assigned by the Mutualink system administrator.

- **Jitter Buffer Size**

The initial size of the RTP receive audio jitter buffer. If a network is very bursty, a higher value would be better here, but the end-to-end voice delay increases correspondingly. In reality, our EPs have a fairly good automatic jitter buffer that automatically sizes itself as required, so this parameter should probably be left at the default value.

Presence Multicast

The **Presence Multicast** determines what other EPs both see this EP and are seen by this EP on the Global network.

This value must be set to the same value on all EPs that wish to communicate on the Global network.

KDS Agent

The **KDS Agent** page displays:

- **Addresses and Port**

IP address and TCP port to the KDS web service (see Network Monitoring Service for details).

- **Update List Period**

Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.

- **Validation Retry Period**

Interval at which the EP will contact the remote service to request authentication on a given Agency.

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

NMS Agent

The **NMS Agent** window displays the following:

- **Addresses**

List of IP addresses where the web remote service can be located. More than one address can be entered separated by colons (:) and the EP will try them out in the order listed.

- **Port**

TCP Port where the remote web service can be located.

- **Heartbeat Period: Interval at which the EP will send heartbeat messages to the NMS.**

- **Alarm Read Period**

Interval at which the EP will report new alarms to the NMS. The EP queues new alarms locally and sends them together at this interval.

Controlling Endpoints

This is the list of IWSs that are authorized to control this NIC. If an IWS that is not in this list attempts to invite this NIC to an incident or otherwise exercise control over it, the request will be rejected.

Integration

The **Intergration** tab allows you to view or perform:

- [Rx Interface](#)
- [VoIP Incoming Calls](#)
- [VoIP Outgoing Calls](#)
- [VoIP Registration](#)
- [VoIP Media](#)
- [Relay RTP](#)

Rx Interface

The **RX Interface** has different fields depending on the Rx Interface Mode setting selected.

- **Interface Mode**

This setting controls how audio is received from a connected device or accessory. Mode selection does not take effect immediately if the NIC is already in an incident. It will take effect when the NIC joins the next incident.

- **VOX Full-Duplex:** When there is no available control signal to indicate when audio is present, the VOX (Voice Operated Xmission) feature is used. This feature basically assumes that valid audio is present when the audio level rises above a specific threshold. Full-duplex means that audio may be simultaneously received from and transmitted to the connected device.
- **VOX Half-duplex:** Similar to VOX Full-duplex, this setting will prevent audio from being received from the device while we are transmitting audio to it. This should be used for devices that reflect back the transmitted audio signal in some way (even if it's a PTT-beep, etc.). If you have trouble with a NIC kicking back an audio signal every time it receives an incident transmission, this may be the setting for you.

- **VOX Delay**

This is the minimum amount of time (in milliseconds) that the audio signal must be above the VOX Level to be considered a valid audio signal. Increase this if the audio line is subject to short bursts of noise, but a value too high risks truncating the start of the audio signal.

- **VOX Level**

Sets the VOX audio threshold; an audio signal above this level is considered valid receive audio, any signal below is ignored. Note that this value is in the same logarithmic units as the Input Level display so the values can be correlated.

VoIP Incoming Calls

This feature allows incoming SIP calls to initiate incidents to selected endpoints. When a SIP incoming call is received, the target SIP username is checked against this list; if a match is found, an incident is initiated to the specified endpoint. If no match is found but a catch-all entry is present, the incident will be initiated to the catch-all target endpoint. If neither of these situations apply, then the call will be rejected.

VoIP Outgoing Calls

By default, the T-NIC uses the SIP protocol for outgoing calls so it can call any VoIP device.

0.0.0.3 SIP Address Destination

When SIP is enabled (by selecting *SIP address*), the following settings are available:

- **Enable SIP over TCP**

Whether SIP uses TCP or UDP as a transport to external VoIP devices. TCP is preferred due to the guaranteed delivery attributes, but some older SIP devices do not yet support TCP.

- **Static SIP destination**

If this is populated, the T-NIC will call this SIP address every time it is invited into an incident; the IWS user will not even be asked for an address/number to call. This is useful for "hotline" type applications that support SIP.

- **Default SIP domain or outbound proxy**

If the destination address from the IWS user does not include a domain/hostname (e.g. phone numbers), what SIP domain should these calls be forwarded to? By default, this is the local host (IP pseudo-address 127.0.0.1) if an embedded asterisk PBX is installed. If you're using an outbound SIP proxy to route external outbound SIP calls, use this field to specify its address. To specify a custom port append the address with the corresponding port value, i.e. `<address>:<port>`.

- **Display Name**

Display name for external calls and registration, for example "Bob Smith".

- **Username**

SIP username for external calls, registration and authentication.

- **Password**

Password used for authenticating the username at the specified realm. Used only if authentication is requested.

- **Authentication Realm**

The name of the authentication realm for outgoing calls (if different from outbound proxy). Used only if authentication is requested.

- **Enable sending DTMFs via SIP INFO**

If this is enabled (the default), we will enable sending DTMF codes via SIP INFO messages instead of in-band or by using RFC4733 RTP.

- **Prefer SIP INFO over RFC4733**

If both methods are supported by an external device, which method should we use?

0.0.0.4 Static IP Address Destination

If the use of SIP is disabled (by selecting *Static IP Address*), then the T-NIC will connect to a specific IP address every time it is invited into an incident; the IWS user will not even be asked for an address/number to call. This is useful for “hotline” type applications that do not support SIP. In this mode, the following settings are available:

- **Destination IP address**

The static IP address to connect to – this may be either a unicast or multicast address.

- **Destination RTP port**

The UDP port on the destination IP address to send RTP (voice) packets to.

- **Local RTP port**

The local port that the far end device should send RTP packets to. If using a multicast address, this port must be the same as the Destination RTP Port. Leave this blank to use the default.

- **Codec**

What voice codec should the RTP packets use? All devices will typically support PCM uLaw – only choose Linear16 if required by the far end device.

- PCM uLaw:

- **Payload Type:** For Linear16, what dynamic RTP payload type should be used? This must agree with the far end device configuration.

VoIP Registration

SIP registration is used for routing incoming calls. The registration consists of the T-NIC telling a SIP Registrar where it can be reached for incoming calls (that is, when somebody makes a SIP call to that user).

When this option is selected the form will show the following configuration options:

- **Duration of registration**

Number of seconds during which our registration should be valid. After this time passes, the T-NIC will re-register. A value of 300-600 seconds (5-10 minutes) is typical.

- **Retry period on failure**

Number of seconds after which the T-NIC will retry a failed registration attempt.

- **SIP Server Address**

The IP address or hostname of the SIP registrar we will register with. Leave this field empty if it will use the same address as the outbound proxy used for outgoing calls. While many simple SIP deployments use the same address for the outbound proxy and the registrar, larger deployments may use different servers for each of these functions.

- **Display Name**

Display name for registration (if different from display name used outgoing calls).

- **Username**

SIP username used for registration (if different from username used outgoing calls).

- **Password**

Password used for authenticating the username at the specified realm (if different from password used outgoing calls). Used only if authentication is requested.

- **Authentication Realm**

The name of the authentication realm for registrations (if different from the registrar address). Used only if authentication is requested.

VoIP Media

The following settings are available whether SIP is enabled or not:

- **RTCP Interval**

Number of seconds between RTCP transmissions; 10 seconds is a good default. Enable RTCP if the far end device(s) supports it. Leave blank to disable RTCP.

- **DTMF duration**

Duration of the DTMF “on” period in milliseconds. Don't change unless required.

- **DTMF inter-digit pause**

How long to pause between DTMF digits in milliseconds. Don't change unless required.

- **Send DTMFs inband**

Enable to send DTMF tones in the inband audio stream as well as out-of-band using either RFC4733 or SIP INFO. This is not recommended unless required for a special application.

Relay RTP

At this time, this parameter is meaningful only for T-NICs and IP V-NICs on multi-homed systems. It selects the interface that the Endpoint will use to open an RTP stream to a static destination IP address.

You can select between the **Primary** or **Secondary** interfaces, or you can enter an interface name or IP address manually on the combo-box.

Preferences

The **Preferences** tab allows you to view or perform:

- [Audio Codec](#)
- [Geographic Location](#)

Audio Codec

Select from the list the audio codec that this endpoint will use when participating in an incident.

Available selections are:

- G711U
- G729B
- G711U (preferred), G729B (alternate)
- G729B (preferred), G711U (alternate)

Geographic Location

Set the default latitude and longitude to be announced for this endpoint geographical location.

To disable publishing, leave both geographical coordinates blank.

Status

The Status tab allows the following:

- Endpoint Status
- Registered Endpoints
- KDS Agent Status
- NMS Agent Status
- Alarms
- Incidents

Endpoint Status

The **Endpoint Status** page shows more detailed high-level status items for this Endpoint.

Registered Endpoints

Displays all the endpoints this endpoint has auto-discovered on the interconnect network, along with their IP addresses, attributes, etc.

KDS Agent Status

At any point in time the Endpoint is either asking to be authorized or asking for an update to its authorized peer list.

- Addresses and Port: IP address and TCP port to the KDS web service.
- Period to update my authorized peer list: Interval at which the EP will contact the remote service to check if a new EP has been authorized or rejected from its current list.
- Period to retry authentication request: Interval at which the EP will contact the remote service to request authentication on a given Agency.

NMS Agent Status

The Network Monitoring Service (NMS agent) page displays:

- **Connection Address**
- **Connection Status**
- **Last Good Transaction**
- **Alarms Since Started**
- **Alarms Not Yet Reported**

Alarms

Displays any current alarms active on this EP.

Incidents

Displays the incidents and patches that we are a member of, along with associated network information, active SIP sessions, etc.

Logs

To view logs, selection **Application**. The Endpoint logs page allows you can view the Mutualink application logs. The page will show the most recent lines on the selected file.

You can view more lines by changing the default value in the form text box. You can also do a case insensitive search on a list of space separated keywords.

Management

The Management tab allows you to view endpoints users and the configuration.

API Users

API Users manages the list of users that can connect to the EP on its external application interface. On the 'External API Users' page, you will see a list of the current users and their properties. From this page you can add a new user or edit/delete an existing one.

If you choose to add or edit a user, the external API user form will be displayed. In this form you can specify the name (only for new users), password, allowed capabilities, and subnets from which external clients can connect (using the <address>/<maskbits> format).

The allowed capabilities for an external client are:

- **Interactive**

The client should be presented with dialog boxes that the endpoint generates to request information or report errors and warnings.

- **Audio**

A remote client can request an audio connection (replacing the speakers & microphone connected to the IWS)

- **Transmit**

VideoA remote client can send video to the incident (via a helper input V-NIC under control of the IWS).

- **Receive Video**

A remote client can receive video from an incident.

- **Show Files**

File sharing functionality should be exposed to the client.

- **Receive Files**

The client can download files shared by other incident participants.

- **Transmit Files**

The client can share files to an incident.

If no allowed subnet is specified, it will accept connections from all IP addresses.

Configuration

On this page you can view the Endpoint configuration file. You can also perform the following.

- **Backup**

Download a copy of the Endpoint configuration file.

- **Restore**

Restores a previously backed-up file. You select the file from your local storage and start the upload to transfer and apply that configuration.

Restart

To restart a NIC click on the corresponding button at the Restart menu page. Currently, IWS appliances cannot be restarted from the web page. You have to reboot the whole system.

