ADDERLink™ INFINITY Manager (3rd gen)

User Guide

Covers AIM software from **v6.00**



Experts in Connectivity Solutions

ADDER

KVM Extension Solutions

Contents

Introduction

Local feed through 4
AIM basics 5
Supplied items 7
Optional extras 8

Installation

Connections 9
AIM firmware and hardware limitations 11
ALIF model specific requirements 11
Tips for a successful implementation 11
Mounting the AIM server 12

Configuration

Supported browsers 13
Login for admin users 13
Important first configuration steps 14
Adding ADDERLink INFINITY units 15
If an ALIF unit is not located 15
ALIF manual factory reset 16
Front panel indications 17

The AIM Dashboard 18
The AIM menu 19
Active Connections 20
Table View 21
Network View 22
Logs 23
Connection logs 23
Event logs 24
Receivers 25
All Receivers 25
Viewing and editing a receiver entry 26
Receiver groups 29
Viewing and editing a receiver group entry 30
Update firmware 33
Transmitters 34
All Transmitters 34
Viewing and editing a transmitter entry 35
Adding a VDI / Configure Virtual Machine 38
Transmitter groups 39
Viewing and editing a transmitter group entry 40
Update firmware 42
C-USB LAN 43
Viewing and editing a C-USB LAN entry 44
User management 45
Users 45
Viewing and editing a user entry 46
User Groups 47
Viewing and editing a user group entry 48
Directory servers 49

Channels....51
All Channels....51
Viewing and editing a channel entry....52
Channel Groups....53
Viewing and editing a channel group entry....54
Presets....55
Viewing and editing a preset entry....56
System Care > Servers....57
Manage Servers....57
System Care > Global Configuration....58
AIM configuration settings....58
Transmitter....60
Receiver....62
System Care > Network Settings & Tools....65
Settings....65
Tools....68
System Care > Remote Support....70
System Care > Backup....71
Backup....71
Archive....71
XML....71
System Care > Update....72
System Care > Statistics....73

Operation

Logging in....74
The Local OSD screen....75
Listing C-USB LAN transmitters....76
Accessing virtual machines....76
Using the Remote OSD feature....77
OSD view switching with DVI-equipped ALIF receivers....78

Further information

Getting assistance....79
Appendix A - Tips for success when networking ALIF units....80
Appendix B - Troubleshooting....82
Appendix C - Redundant servers: Setting up and swapping out....83
Appendix D - Making an AIM Manager Backup....85
Appendix E - Restoring an AIM Manager Backup....86
Appendix F - Two Factor Authentication (2FA)....88
Setting up 2FA on the AIM User Interface....88
Logging into the AIM web interface....89
Appendix G - AIM export user configuration....91
Appendix H - Configuring SSL on an AIM server....93
Appendix I - Auto Login Feature....94
Appendix J - License upgrading....95
Appendix K - Glossary....96
Appendix L - Copper/fiber modules and cables....99
Appendix M - AIM API....100
Appendix N - DHCP server requirements for ALIF support....124
Appendix O - AIM database schema....126
Appendix P - Technical specifications....128
Appendix Q - Open source licenses....129

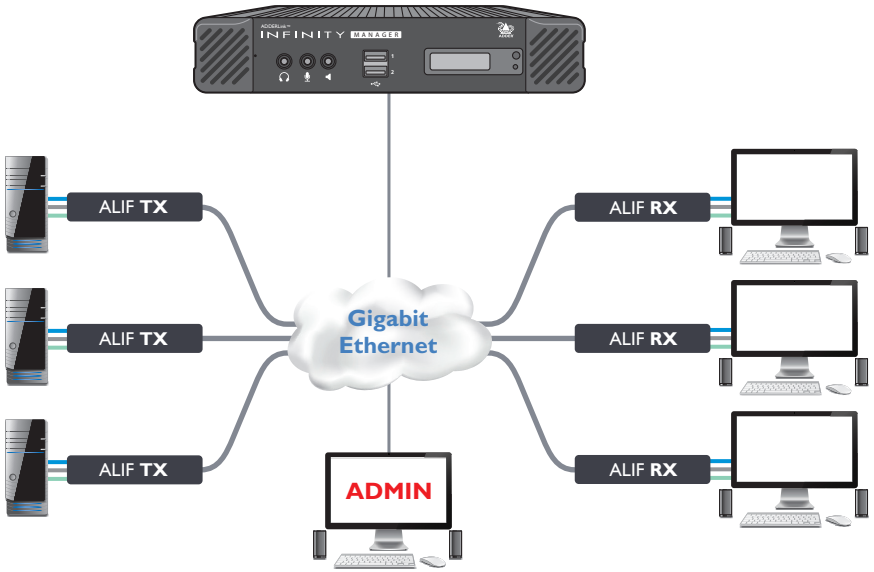
Index

Introduction

ADDERLink™ INFINITY transmitter and receiver units allow multiple remote users to access host computers in a very flexible manner. Such flexibility requires management and coordination – that is where AIM (ADDERLink INFINITY Manager) becomes vital.

AIM is designed to promote the most efficient use of ADDERLink INFINITY (ALIF) units by allowing central control over any number of transmitters and receivers. Using the intuitive AIM web-based interface, one or more administrators can manage potentially thousands of users who are interacting with an almost unlimited number of devices.

AIM operates as a self-contained compact server (including its own DHCP server) unit that can be situated anywhere within your network of ALIF devices:



The AIM server connects to your network and provides administrative control over the various ADDERLink INFINITY transmitters, receivers and their users.

Note: Although the ADDERLink INFINITY units require Gigabit Ethernet connections, in its administrative role, the connection to the AIM server is not speed critical.

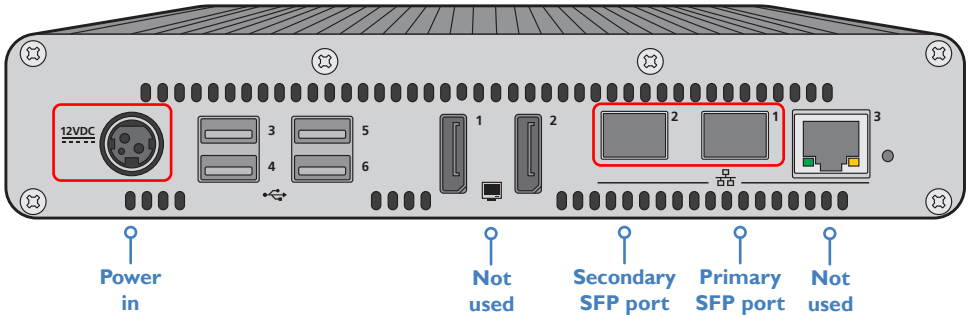
The AIM server is supplied pre-loaded and is straightforward to deploy, requiring only a network connection and a power input to begin operation.

All configuration of your ADDERLink INFINITY transmitters (channels), receivers and users is performed using the intuitive AIM browser interface via a network connected computer.

AIM server front panel



AIM server rear panel - In normal use only the SFP network and power connectors are used (ringed in red)

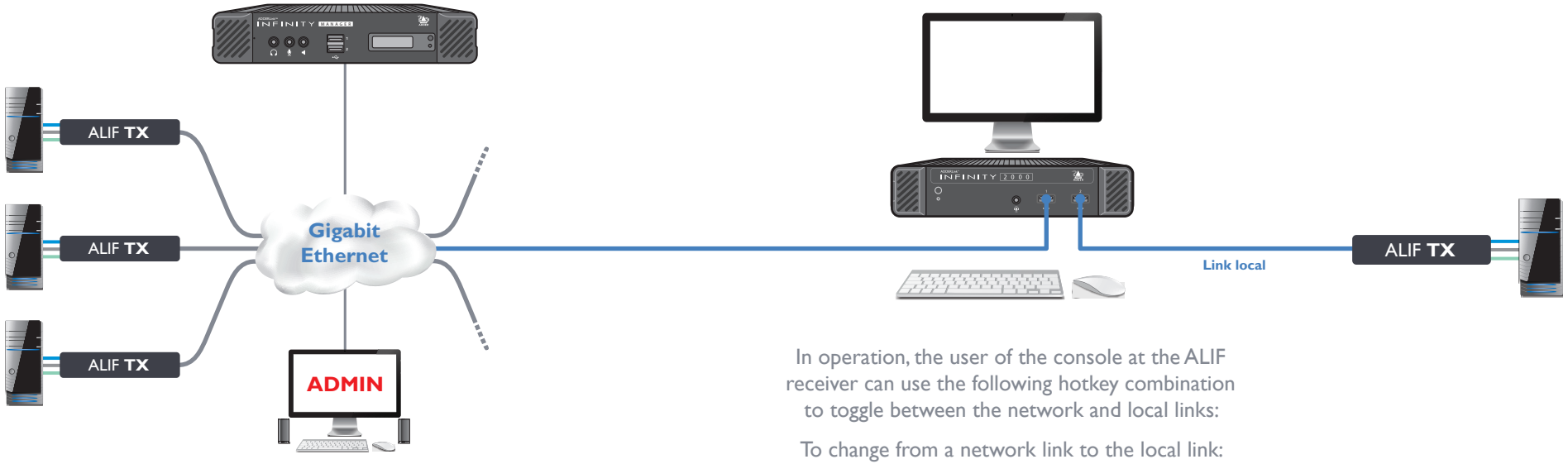


Please see the section Basic steps for a new configuration for assistance with creating AIM installations.

LOCAL FEED THROUGH

ALIF receivers which are equipped with dual IP network ports can be configured to support a local link to a host PC in addition to the main link to the network (when under AIM control). The locally linked PC remains completely isolated from the main network.

To configure this arrangement, ensure that the IP port that is used for the local link is not allocated an IP address.



Note: The local feed through feature is not supported by ALIF3000R units.

In operation, the user of the console at the ALIF receiver can use the following hotkey combination to toggle between the network and local links:

To change from a network link to the local link:
enter CTRL+ALT+L

To change from the local link to a network link:
enter CTRL+ALT +C
to display the OSD and choose
the required connection.

Note: The L and C default hotkeys can be changed within the AIM control panel.

AIM BASICS

Channels

Think of a channel as a 'virtual transmitter'. It is virtual because the video, audio and USB streams of a channel do not necessarily have to originate from the same physical transmitter unit, although in most cases they will. For instance, you could arrange for video and USB streams to be received from one host computer, while the audio stream came from an alternative source. Alternatively, two channels could be configured for the same host computer, each with different access rights to suit particular situations.

Groups

In order to accommodate potentially large numbers of users and devices, AIM uses a system of groups: User Groups, Receiver Groups and Channel Groups. Groups allow the administrator to apply collective settings to all members and also to take full advantage of *Inheritance*. Inheritance allows members of a group to benefit from settings and permissions made within other groups to which their group is linked. This saves administration time because members do not need to be individually altered. For instance, if Sam is in User Group 1, all Channels accessible to User Group 1 will be available to Sam.

User types

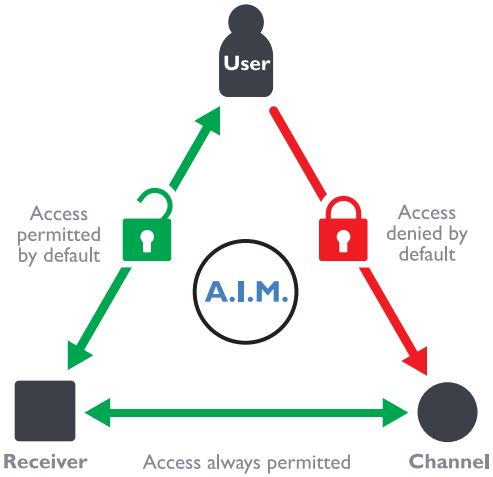
This guide refers to the two main categories of users involved with the AIM system:

- An **Admin (administrator) user** accesses the AIM system via a network-linked computer running an Internet browser. Once the necessary username and password have been entered, Admin users can make changes to the operation of the AIM system.
- A **Regular user** has a keyboard, video monitor and mouse (plus speakers where appropriate) attached to an ADDERLink INFINITY receiver unit and can access one or more computers that are linked to ADDERLink INFINITY transmitters. The ADDERLink INFINITY receiver provides an On-Screen Display (OSD) that lists all accessible computers and allows easy access to them.

Security

Security considerations form a major part of AIM operation, ensuring that users have rapid access only to the systems for which they have permission. At its core, AIM manages an important three-way relationship between the users, the ADDERLink INFINITY receiver(s) and the channels from the host computers.

The diagram shows a representation of the three-way relationship which exists between users, receivers and channels.



To successfully gain access to a channel:

- **The user requires permission to use the receiver,**
- **The receiver requires permission to connect with the channel,**

  AND
- **The user must have permission to access the channel.**

In most cases, the need for three access permissions per connection is unnecessary and raises administration overheads. Hence, by default, AIM grants open access for the user to the receiver and the receiver to the channel while restricting the final, most crucial piece of the puzzle. For those who require it, the lock upon the user to receiver stage can be applied individually or globally.

See Permissions on the next page for more details.

continued

Directory Services

To streamline administration even further, AIM supports Active Directory. By synchronizing with an LDAP/Active Directory server, details of users (including their usernames and group memberships) can be securely synchronised from existing databases in order to both minimize the initial configuration as well as streamline ongoing updates. The following directory services are supported: AD, RH IDM, openLDAP, Azure AD and Google Workplace.

AIM interface

AIM appears in two main ways depending on whether you are an administrator or a regular user.

- For administrators, full access to the ADDERLink INFINITY Manager Suite is granted. The Dashboard provides a central location from which the administrator can view overall operation, make various changes, database backups and also upgrade the firmware of any linked ADDERLink INFINITY unit.
- For regular users, an efficient page layout provides a list of all channels for which you have permission to visit. Against each selectable channel name and description, a series of icons provide clear feedback about current availability.

Permissions

Permissions exist between Users, Receivers, and Channels.

By default, all users are granted permission to access ALL receivers.

By default, all receivers have permission to connect to ALL channels.

As shown in the introductory diagram, the missing part is the permission for a user to access each channel.

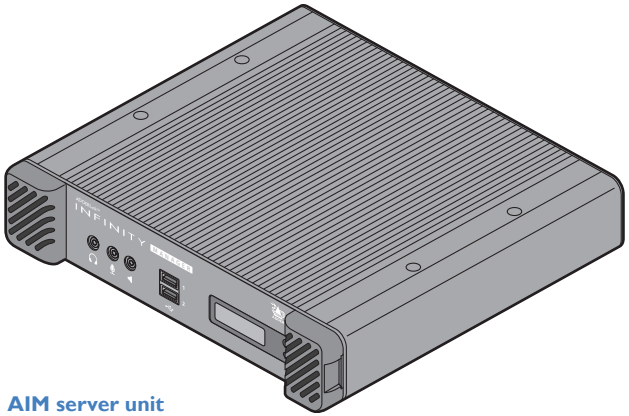
Permissions between a user and a receiver can be applied in any of the following ways:

- User → Receiver
- User → User Group → Receiver
- User → User Group → Receiver Group → Receiver
- User → Receiver Group → Receiver

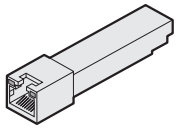
Thus, a very indirect way of granting permissions could be:

- User1 is in UserGroup1,
- UserGroup1 has access to ReceiverGroup1,
- ReceiverGroup1 contains Channel1,
- Therefore, User1 has access to Channel1 indirectly.

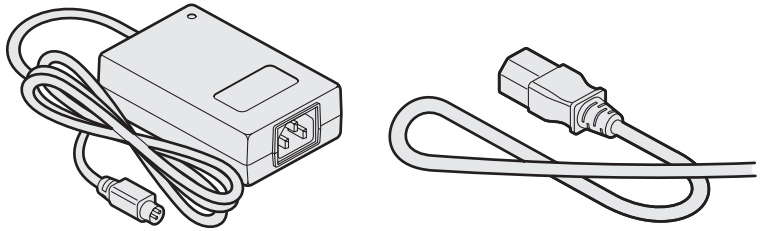
SUPPLIED ITEMS



AIM server unit



1GbE copper SFP module

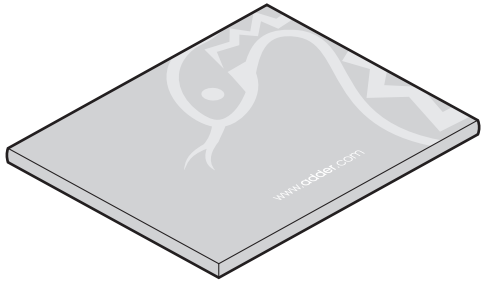


12V, 5A Power supply plus country-specific mains cable

Replacement power adapter with locking connector
Part number: PSU-IEC-12VDC-5A

Country-specific power cords

CAB-IEC-AUS	*(Australia)*
CAB-IEC-EURO	*(Central Europe)*
CAB-IEC-UK	*(United Kingdom)*
CAB-IEC-USA	*(United States)*
CAB-IEC-JAPAN	*(Japan)*

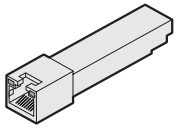


Information wallet
containing:

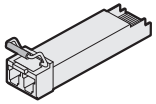
Four self-adhesive rubber feet

Safety document

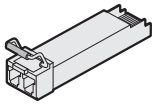
OPTIONAL EXTRAS



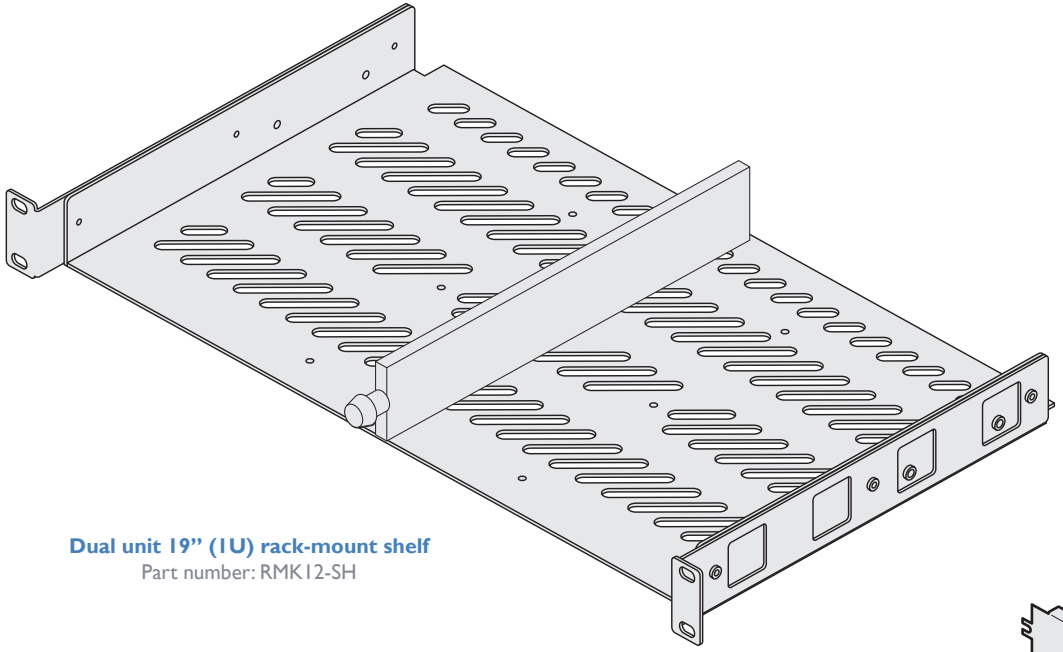
1GbE copper SFP module
Part number: SFP-CATX-RJ45



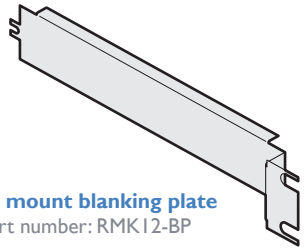
1GbE single mode fiber SFP module
Part number: SFP-SM-LC



1GbE multi mode fiber SFP module
Part number: SFP-MM-LC



Dual unit 19" (1U) rack-mount shelf
Part number: RMK12-SH



Rack mount blanking plate
Part number: RMK12-BP

Installation

CONNECTIONS

The AIM server unit is supplied fully pre-loaded and permits no local user interaction. All configuration takes place remotely via the network connections and as a result only two connections are required: Network and power.

Note: If an existing AIM server must be replaced, follow the important advice given within Appendix C (Swapping out an AIM server).

Note: There is no need to connect a keyboard or mouse to the AIM server as configuration takes place across the network connection.

Network connections

Two SFP ports are located on the rear panel to allow CATx (or fiber) links to separate networks, according to the type of modules that are inserted. The AIM server uses the two ports as follows:

- Port **1** for connection to the internal ALIF network only.
- Port **2** for duplicate connection to the internal ALIF network or connection to external networks to allow admin users to log in when away from the internal network.

Note: Port 1 does not support DHCP and needs to be manually configured, whereas port 2 does support DHCP. The precise operation of the two ports are determined within the AIM server Management Suite.

SFP module types

SFP-CATX-RJ45 for use with CAT5e (and above) cable.
SFP-SM-LC modules require OS1 or OS2 single mode fiber.
SFP-MM-LC modules require OM1, OM2, OM3 or OM4 multi-mode fiber.

See Appendix L for details.

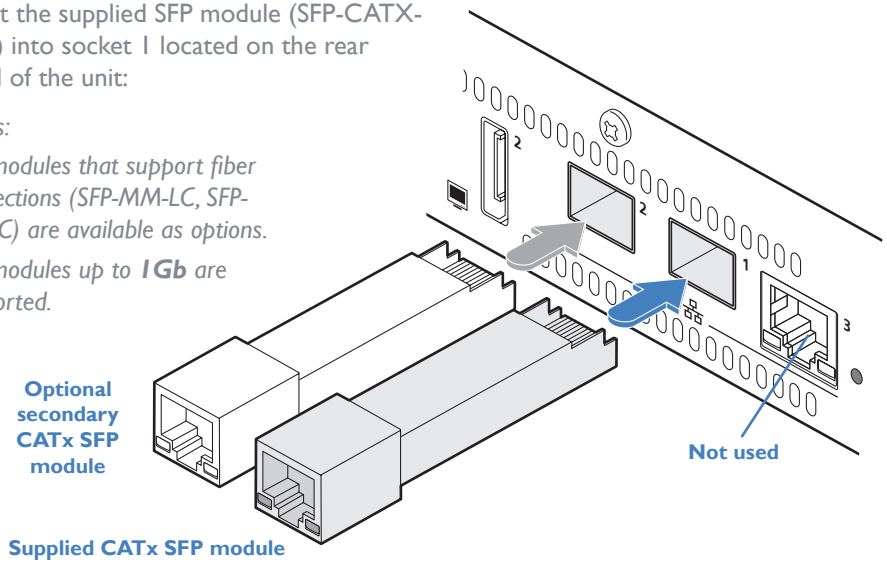
To connect the network port(s)

1 Insert the supplied SFP module (SFP-CATX-RJ45) into socket 1 located on the rear panel of the unit:

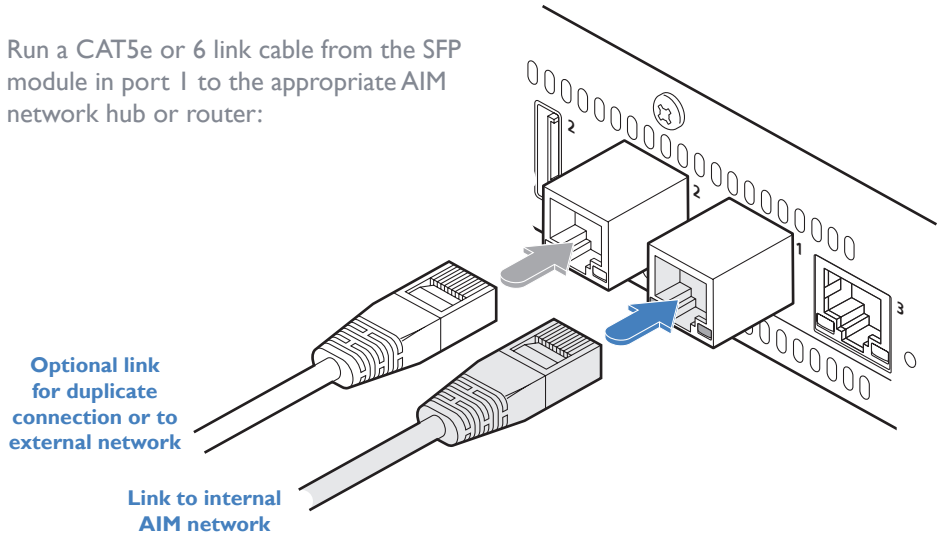
Notes:

SFP modules that support fiber connections (SFP-MM-LC, SFP-SM-LC) are available as options.

*SFP modules up to **1Gb** are supported.*



2 Run a CAT5e or 6 link cable from the SFP module in port 1 to the appropriate AIM network hub or router:



3 If a second SFP module was inserted into port 2, run an appropriate link from that to the required hub, router or gateway.

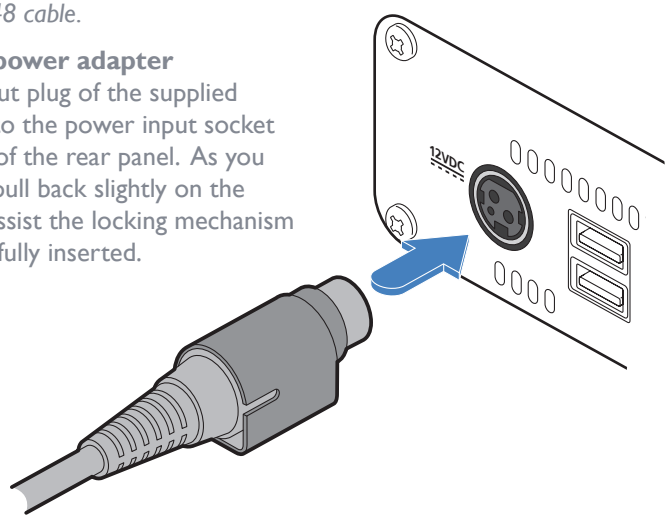
Power supply connection

IMPORTANT: Please read and adhere to the electrical safety information given within the Safety information provided with the AIM server. In particular, do not use an unearthed power socket or extension cable.

Note: The AIM server can also be powered from the optional RED-PSU managed power supply system using a VSC48 cable.

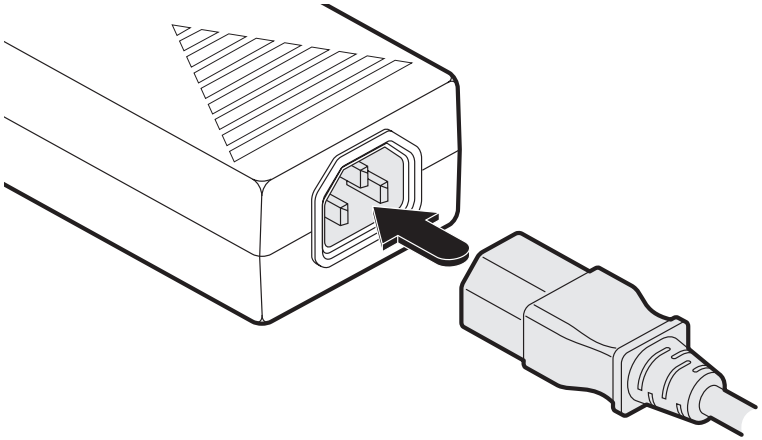
To connect the power adapter

1 Attach the output plug of the supplied power adapter to the power input socket on the left side of the rear panel. As you insert the plug, pull back slightly on the outer body to assist the locking mechanism until the plug is fully inserted.



From the power adapter

2 Insert the IEC connector of the supplied country-specific power cord to the socket of the power adapter.



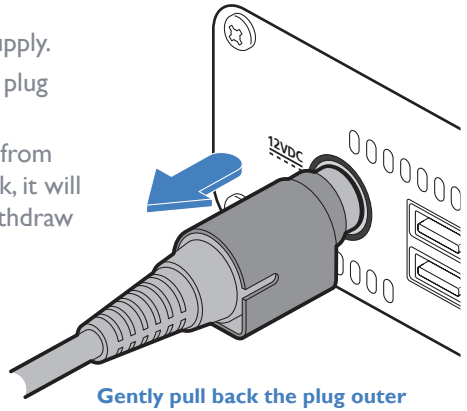
3 Connect the power cord to a nearby mains supply socket.

To disconnect the power adapter

1 Isolate the power adapter from the mains supply.

2 Grasp the outer body of the power adapter plug where it connects with the node.

3 Gently pull the body of the outer plug away from the node. As the body of the plug slides back, it will release from the socket and you can fully withdraw the whole plug.



Gently pull back the plug outer body to release the lock

IMPORTANT: Please read and adhere to the electrical safety information given within the Safety information booklet provided with this product. In particular, do not use an unearthed power socket or extension cable.

Note: The unit and the power adapter generate heat when in operation and will become warm to the touch. Do not enclose them or place them in locations where air cannot circulate to cool the equipment. Do not operate the equipment in ambient temperatures exceeding 40 degrees Centigrade. Do not place the products in contact with equipment whose surface temperature exceeds 40 degrees Centigrade.

AIM FIRMWARE AND HARDWARE LIMITATIONS

IMPORTANT: AIM firmware v6.00 and above requires AIM server generation 3 hardware (ASP-001) or above.

ALIF MODEL SPECIFIC REQUIREMENTS

- **ALIF100T** transmitters require firmware version v4.11 (or greater)
- **ALIF101T** transmitters require firmware version v4.10 (or greater)
- **ALIF102T** transmitters require firmware version v9.02 (or greater)
- **ALIF10xx** endpoints require firmware version v5.2 (or greater)
- **ALIF11xx** endpoints require firmware version v8.0 (or greater)
- **ALIF20xx** endpoints require firmware version v5.2 (or greater)
- **ALIF21xx** endpoints require firmware version v5.02 (or greater)
- **ALIF3000** receivers require firmware version v1.1.2 (or greater)
- **ALIF4000** endpoints require firmware version v5.07 (or greater)

Upgrading and downgrading firmwares

- It is possible to downgrade back to v4.0 if necessary.
- When running v4.13 on AIM generation 3 hardware, the following behavior will be seen on the front panel OLED screen and indicator:
  - OLED The screen will remain blank and not display any details.
  - Indicator The indicator will show only green when powered on, no other colors.

TIPS FOR A SUCCESSFUL IMPLEMENTATION

Installations based upon the ALIF modules vary widely in their scope and complexity. Each implementation is distinct, however, there are numerous tips and best practice recommendations available on the Adder website. Many tips are concerned with the correct selection and configuration of network switches plus the choice of network topology.

Please go to:
https://support.adder.com/tiki/tiki-index.php?page=ALIF%3A%20Getting%20Started

General requirements

- Portfast needs to be enabled on the network switch to ensure that the ALIF to AIM communication happens in a timely manner. Note that Cisco uses the term 'edge port' rather than 'portfast'. The option is enabled on each port to which an AIM unit is connected. Where portfast is not enabled, if a second AIM is added for redundancy, this could result in a mis-configured Backup server.
- If an existing AIM server must be replaced, follow the important advice given within Appendix C (Swapping out an AIM server).
- When configuring the installation for multicasting (and to improve overall performance), the network switch(es) being used must support a minimum of IGMP v2 snooping. For faster performance use switches that support IGMP v3.
- In order to display video resolutions that use a horizontal video resolution of 2048 pixels, the network switch must have support for Jumbo packets.
- Please also see Appendix A - Tips for success when networking ALIF units.

Compatibility matrix

For a full summary of ALIF models and their compatibility with AIM firmware versions, please go to:

https://support.adder.com/tiki/tiki-index.php?page=ALIF%3A%20Compatibility%20Matrix

If the compatibility matrix is not found at the above address, please contact technical support for assistance.

MOUNTING THE AIM SERVER

The AIM unit is designed to be easy to mount within a standard 19" rack using the optional rack-mount shelf (RMK12-SH). The unit is also suitable for free standing use on the desktop. The server chassis requires just a 1U space within the rack.

To mount the AIM server within a rack mount

1 Install the empty rack-mount shelf into your 19" rack frame and fully secure it.

2 Place the AIM unit into one side of the rack-mount shelf so that its rear panel butts up against the small peg located on the side wall.

3 Place the optional blanking plate (RMK12-BP) onto the other side.

4 Locate the supplied thumbscrew and spacer.

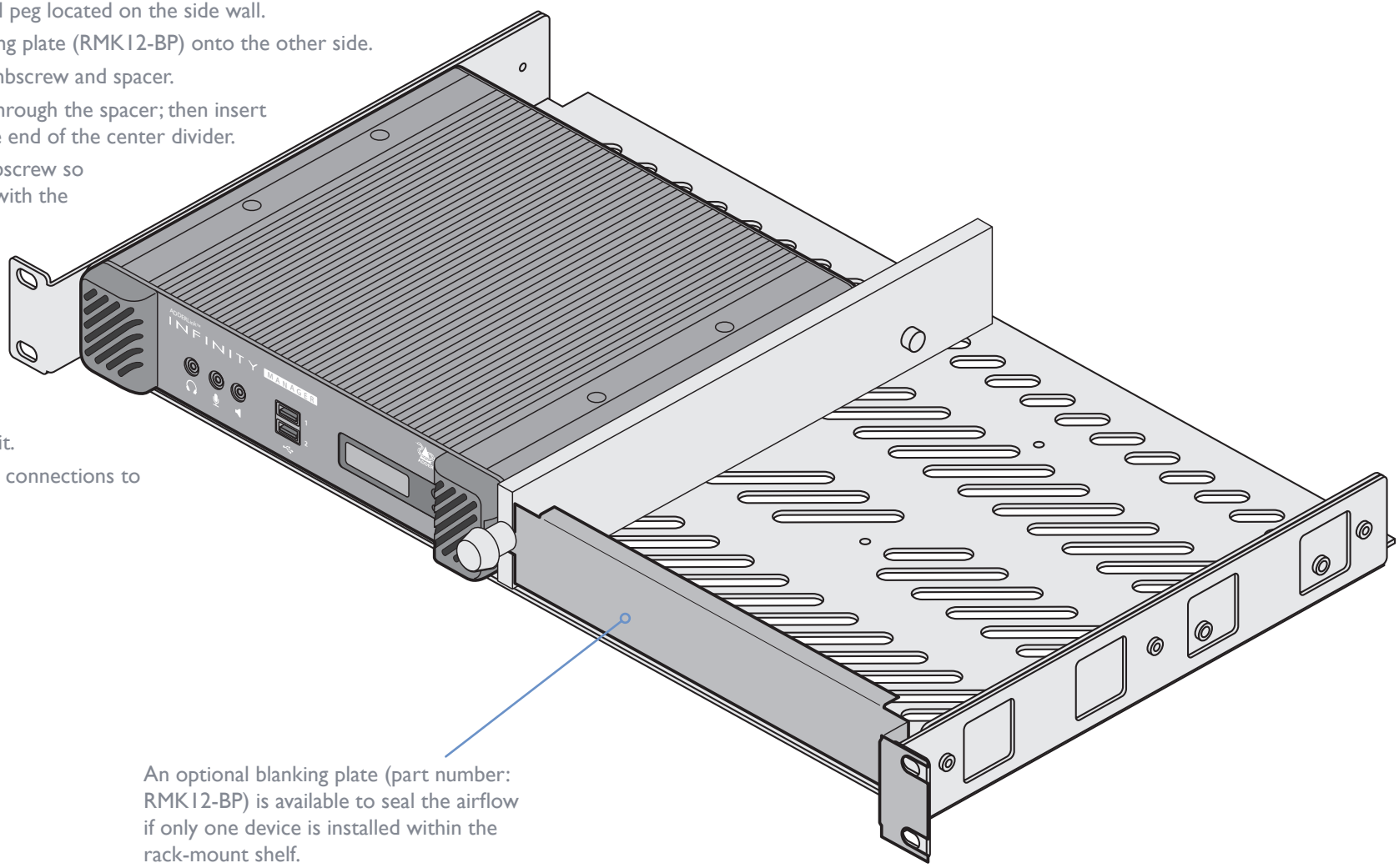
5 Insert the thumbscrew through the spacer; then insert into the small hole at the end of the center divider.

6 Gently tighten the thumbscrew so that the spacer engages with the inner edge of the AIM unit and the blanking plate and holds them in place.

7 Place the power adapter in the rear section of the rack-mount shelf and connect it to the AIM unit.

8 Make all other necessary connections to the AIM unit.

IMPORTANT: When mounting the ALIF units (and their power adapters), ensure that the vents are not obscured and that there is sufficient airflow. The operating temperature range is 0 to 40°C (32 to 104°F) and must not be exceeded. Each power adapter is rated at a maximum of 68.24BTU/hr.



An optional blanking plate (part number: RMK12-BP) is available to seal the airflow if only one device is installed within the rack-mount shelf.

Configuration

This section covers configuration of the ADDERLink INFINITY Manager Suite for administrators. For details about the regular user interface, please see the Operation section.

SUPPORTED BROWSERS

The AIM admin interface requires an A-grade browser with Javascript enabled.

For best results always use the latest version of any browser used.

- Google Chrome
- Firefox
- Edge*
- Safari for MacOS*

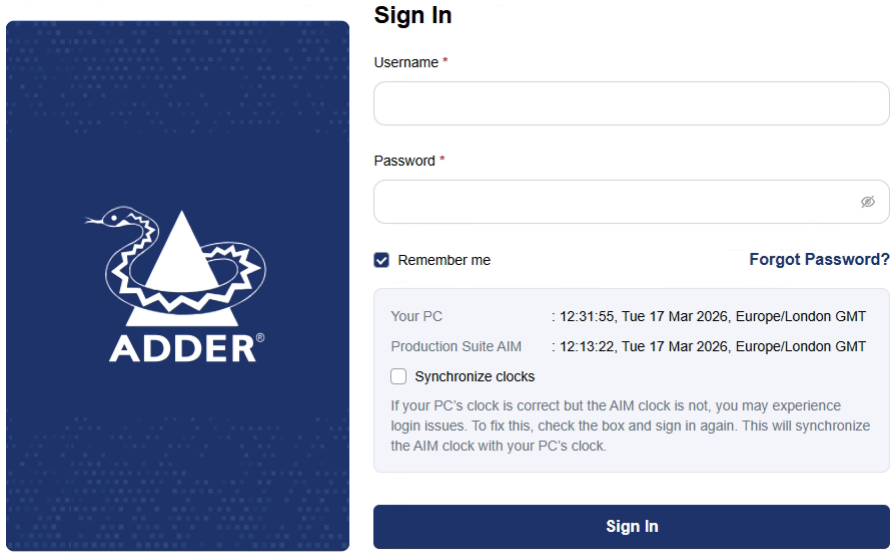
* The most intensive testing has been carried out using Chrome and Firefox. MS Edge and Safari are known to work but testing with these browsers has been limited.

LOGIN FOR ADMIN USERS

1 Ensure that the AIM server is powered on (allow 3 minutes before accessing).

2 Using a computer located anywhere within the local network open a web browser (see Supported browsers list opposite) and enter the default IP address for the AIM server: **169.254.1.3**

The Login page will be displayed:



3 Enter your Username and Password and click the Login button.

The default username is **admin** and the default password is **password**.

You are strongly recommended to change the default admin password as one of your first actions: Go to *Dashboard>Users*. Click on the furthest right icon in the admin row (configure users) and change the password for the admin user.

If you check the **Remember Me** box, a cookie will be stored on the computer, allowing you to access the admin section without having to log in each time. The cookie will survive for up to the *AIM Admin Timeout* period. If you do not check the Remember Me box, you will remain logged in only for the duration of your browser session.

4 Continue to the section Important first configuration steps on the next page.

Forgotten password

If necessary, click the ***Forgotten password*** link to display an assistance page where a secret code will be given. Provide the secret code to Adder support or your distributor to obtain an unlock code which can then be entered to reset your password and gain access.

IMPORTANT FIRST CONFIGURATION STEPS

There are several important configuration steps that must be carried out when starting a new AIM server for the first time.

To determine the AIM server's role and main IP address

1 Switch on and log in to the AIM server; you will be presented with the Servers page.

2 Within the Server page, choose the Role of this new AIM server:

- *Solo* - This will be the only AIM server on the network (with no redundancy and failover), or
- *Primary* - This server will be used as part of a redundant cluster of AIM servers, where it will be the main server used to manage the ALIF units.

3 Click the Save button. You will next be presented with the System Care > Network Settings & Tools > Settings page - see page 65.

4 See the warning below - do not carry out this step while the system is in operation. Within the *Ethernet Port 1* section at the top of the page, change the default *AIM IP Address* (and *Netmask)* options to settings that suit your network configuration and which will be used henceforth for this server.

IMPORTANT: The Ethernet Port 1 AIM IP Address and Netmask settings must NOT be changed during operation of the system. Changing these will invalidate the system's security and require intervention from the Adder technical support staff to restore to a working state.

5 You can now either:

- Continue with other settings on the same page (See *To choose how IP addresses are applied to ALIF units* right), or
- Click the Save button. After a short delay the web browser will automatically redirect itself to the new IP address so that you can continue administering the AIM server.

Note: Ensure that your computer can view the new IP address, otherwise the AIM server will appear to be offline. Depending on your network configuration and that of the computer, you may need to change the computer's configuration to be able to see AIM server's new network address.

IMPORTANT: To use subnet operation, you must have a DHCP server within your network in order to assign IP addresses to the AIM and ALIF endpoints. If subnet operation is used without a DHCP server, the ALIF endpoints will not communicate with AIM As a result, the AIM will need a factory reset in order to be able to revert it back to single subnet mode.

To choose how IP addresses are applied to ALIF devices

1 Log in again to the AIM server and choose the System Care > Network Settings & Tools > Settings page - see page 65.

2 The *Subnet Operation* option may, or may not, be presented at the top of the page.

Note: If Subnet Operation is not present, the AIM server will operate as per the Off setting described below.

When the *Subnet Operation* option is present, you have the following choices:

- *Off* - AIM can administer a single subnet and will use its own DHCP (Dynamic Host Configuration Protocol) server to automatically assign IP addresses to new ALIF devices, drawing upon a pool of spare addresses defined by you.
- *On* - AIM can administer devices across multiple subnets, but will rely upon an external DHCP server to assign valid IP addresses to new ALIF devices.

3 If you chose the *Off* setting, you now need to define the boundaries of the IP address pool that will be used by the internal DHCP server. Enter valid start and end addresses to the *IP Pool Lower Limit* and *IP Pool Upper Limit* options.

Note: If you chose the On setting, you will need to perform a similar operation within the external DHCP server. For details about DHCP server requirements, see Appendix N.

For further details about other options within this page, see System Care > Network Settings & Tools > Settings page - see page 65.

4 When all options have been set, click the *Save* button.

5 If you need to change the operation of AIM from single subnet to multi-subnet (or back again) this option only appears after a successful factory reset of AIM

IMPORTANT

Note: If an existing AIM server must be replaced, follow the important advice given within Appendix C (Swapping out an AIM server).

ADDING ADDERLINK INFINITY UNITS

When new ALIF transmitters and receivers are added to a network, they are designed to automatically announce themselves* to the AIM server. Once the AIM server receives its announcement(s), the ALIF units will be added to the administrator's view of the Dashboard. From here you can then begin to configure each new ALIF unit.

** ALIF units can be configured either from their own browser-based configuration utility or via the AIM server. Once an ALIF unit has been configured in one way, it cannot be reconfigured using the other method without undergoing a factory reset. This policy is in place to help prevent accidental overwriting of configurations. It also means that once an ALIF unit has been locally configured, it will not announce itself to the AIM server upon being added to a network.*

When new ALIF devices announce themselves, depending upon how it was initially configured (see Important first configuration steps), the AIM server will either assign IP addresses to new ALIF units automatically, or will rely upon an external DHCP server to do the same. Either way, providing each ALIF device is not already configured and announces itself to the AIM server (see right for potential issues that can prevent this), they will be automatically provided with a suitable IP address so that they may operate within the network. Once ALIF units have been added, you can use the AIM server Dashboard to select and further configure any or all of them.

Further information

Please also see:

- Appendix A - Tips for success when networking ALIF and AIM units
- Appendix B - Troubleshooting
- Appendix C - Redundant servers: Setting up and swapping out
- Appendix D - Making an AIM Manager Backup
- Appendix E - Restoring an AIM Manager Backup
- Appendix F - Two Factor Authentication (2FA)
- Appendix G - AIM export user configuration
- Appendix H - Configuring SSL on an AIM Server
- Appendix I - Auto Login Feature
- Appendix J - Upgrade license
- Appendix K - Glossary
- Appendix L - Copper/fiber modules and cables
- Appendix M - AIM API
- Appendix N - DHCP server requirements for ALIF support
- Appendix O - AIM database schema
- Appendix P - Technical specifications
- Appendix Q - Open source licenses

How to perform a manual factory reset (see next page)

If an ALIF unit is not located

There are several reasons why an ALIF unit might not be located by AIM:

- The ALIF unit has been locally configured or is otherwise not using its factory default setting. Try performing a factory reset on an ALIF that is not being located.
- The ALIF unit is not located in the same Ethernet segment as the AIM server. Double check connections and move units where necessary, so that all reside within the same Ethernet segment.
- There is a potential cabling problem between the ALIF and AIM units. Check and where necessary, replace faulty cables.

ALIF manual factory reset

Where a previously configured ALIF unit is being added to a network for control by an AIM server, you need to ensure that the unit is reset to its default configuration. The procedures given here cover how to perform a reset on the various types of ALIF units.

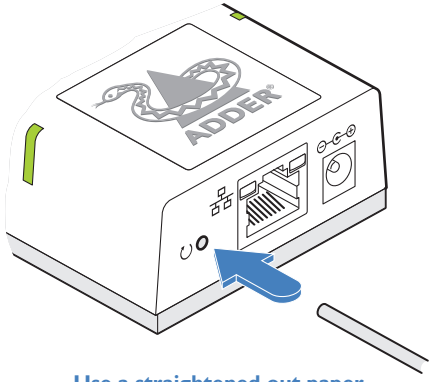
ALIF 100/101/102T models

1 Power on the ALIF100/101/102T unit.

2 Use a narrow implement (e.g. a straightened-out paper clip) to press-and-hold the recessed reset button on the front panel for roughly ten seconds until the indicators turn **blue** *(Note: alternating red/green indications will occur during the fifteen second period while the button is still pressed).*

3 Release the reset switch.

The indicators will remain **blue** for a short while (less than ten seconds) while ALIF100/101/102T unit configures itself and should then change to **green** if all connections are correct; or **orange** if one or more of the video, USB and/or network links are missing.



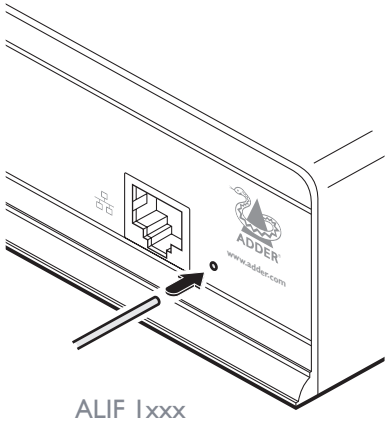
Use a straightened out paper clip to press the reset button for roughly 10 seconds

ALIF 10xx and 20xx models

1 Remove power from the ALIF unit.

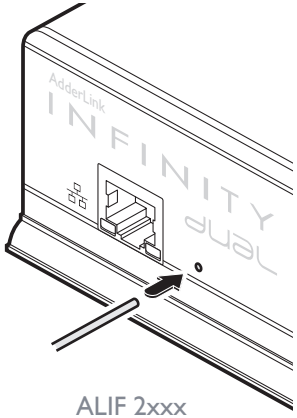
2 Use a narrow implement (e.g. a straightened-out paper clip) to press-and-hold the recessed reset button on the front panel. With the reset button still pressed, re-apply power to the unit and then release the reset button.

After roughly eight seconds, when the factory reset has completed, five of the front panel indicators will flash for a period of three seconds to indicate a successful reset operation.



ALIF 1xxx

Use a straightened out paper clip to press the reset button while powering on the unit



ALIF 2xxx

ALIF 3xxx models

1 Power on the unit.

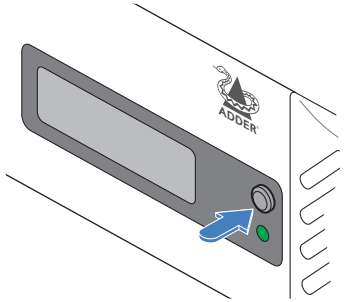
2 Press-and-hold the button located next to the front panel screen for 10 seconds until the indicator flashes blue and the screen shows the message: *Factory resetting device.**

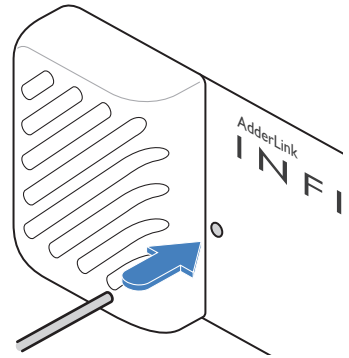
Note: Do not power off the unit at this point.

3 The reset will take place and once complete, the screen will show the message: *Factory Reset Complete. Now Reboot.*

4 Cycle the power using either the recessed power button (see right) or the power adapter input.

** Note: Firmware revisions up to v1.1.1 will behave slightly differently. The message shown on the screen will be 'In factory reset mode' and you will need to cycle the power at that stage to complete the procedure.*



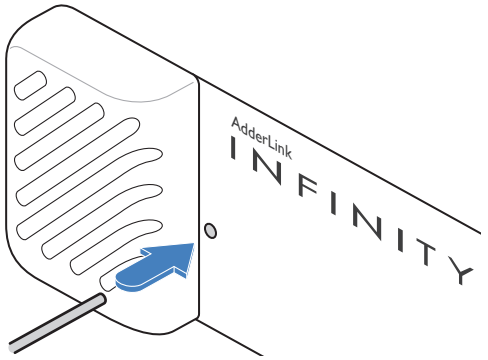


ALIF 11xx, 21xx and 4xxx models

1 Power on the ALIF4000 unit.

2 Use a long narrow implement (e.g. a straightened-out paper clip) to press-and-hold the recessed reset button on the front panel for roughly ten seconds, until the status indicator turns **blue** *(Note: alternating red/green indications will occur during the ten second period while the button is still pressed).*

3 Release the reset switch. The indicator will change to **red** for a short while (less than ten seconds) and then back to **blue** while the unit performs the reset and should then change to an alternative color, usually **orange** initially, signifying that the operation is complete.



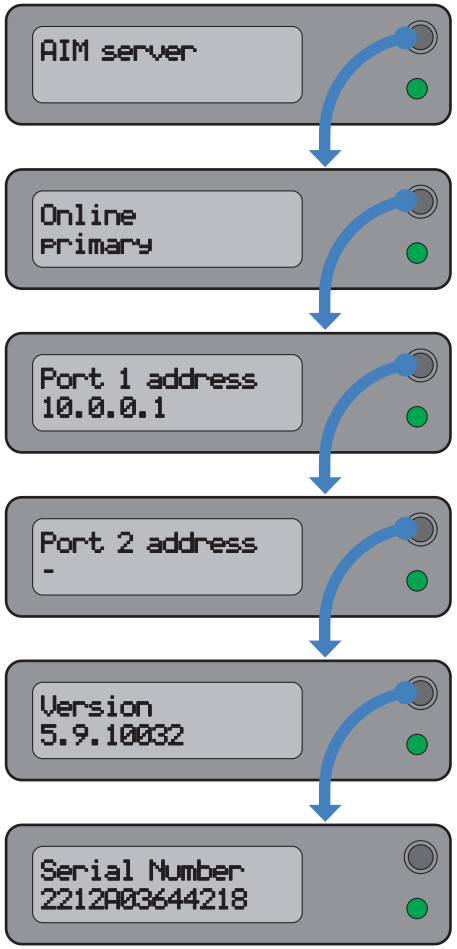
Note: If you are performing a factory reset and intend to disconnect the power immediately after the reset, you must wait at least 30 seconds after you have released the reset button for it to complete the process.

FRONT PANEL INDICATIONS

The front panel of the AIM server unit features an OLED information screen plus a single indicator capable of producing numerous color and flash patterns to provide a useful guide to operation.

OLED screen

Press and release the button to wake the OLED screen and begin showing information. Press the button repeatedly to change between subjects:



Server name

Server status

Network port 1

Network port 2

AIM software version

AIM server serial number

Indicator color and flash patterns

The single front panel indicator uses varying color and flashing patterns to signal key status:

Off	No power.
Green	Powered on and network connection established.
Yellow	No network connection.

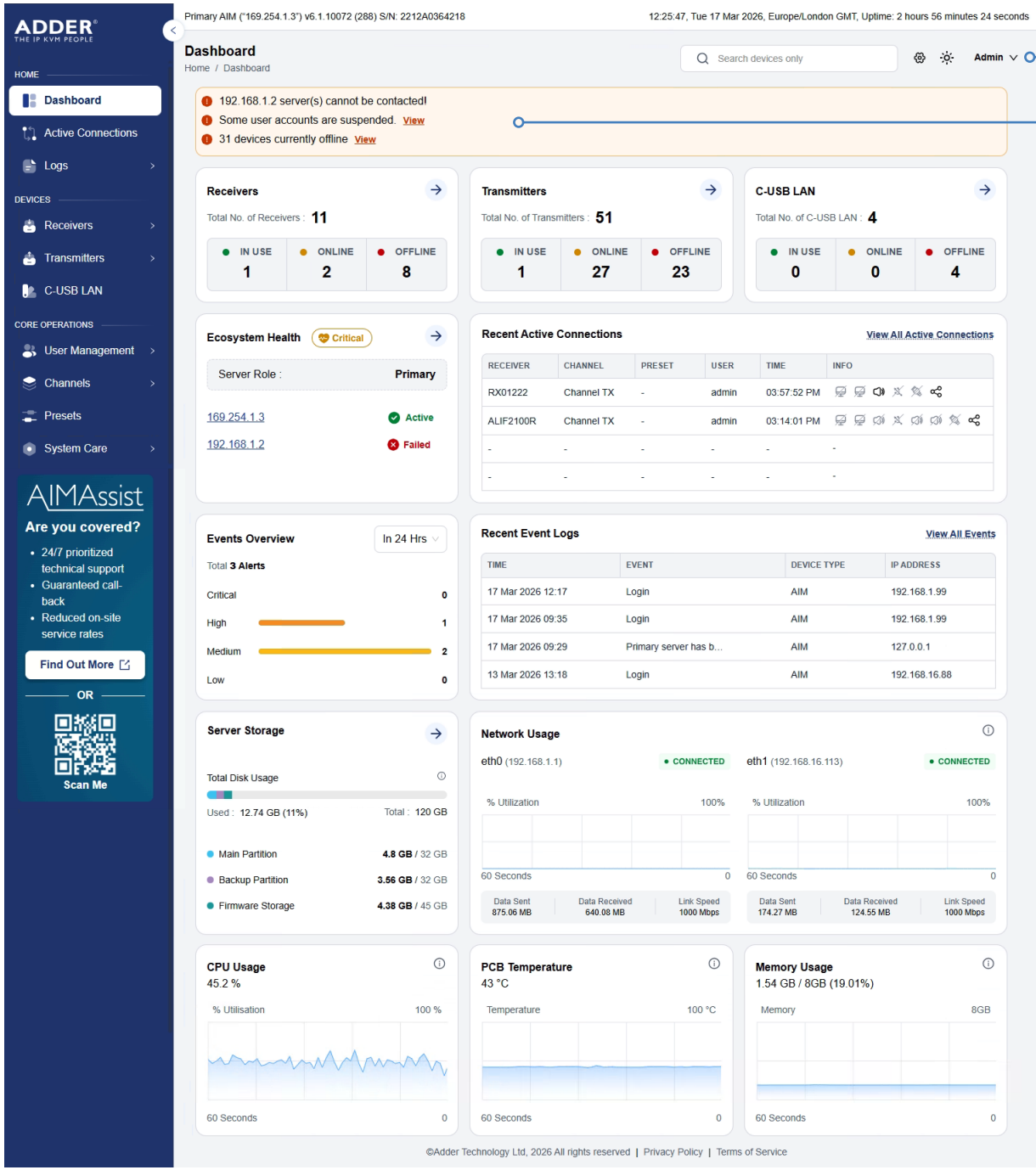
IMPORTANT

Models running AIM software version 4.13 and below will exhibit the following front panel OLED screen and indicator behavior:

- OLED — The screen will remain blank and not display any details.
- Indicator — The indicator will show only green when powered on, no other colors.

THE AIM DASHBOARD

The dashboard provides a comprehensive live overview of the AIM installation with clickable links to many aspects of operation.



Dashboard menu with expandable options

see page 19

Click here to logout - page 19

Latest notifications

Remote devices area

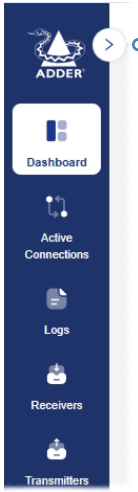
Recent Active Connections

see page 20

Events and logs area

AIM server hardware operation details

Click the arrow icon in the top left corner of the screen to minimise the Dashboard menu:



Click here to return to the full size menu

THE AIM MENU

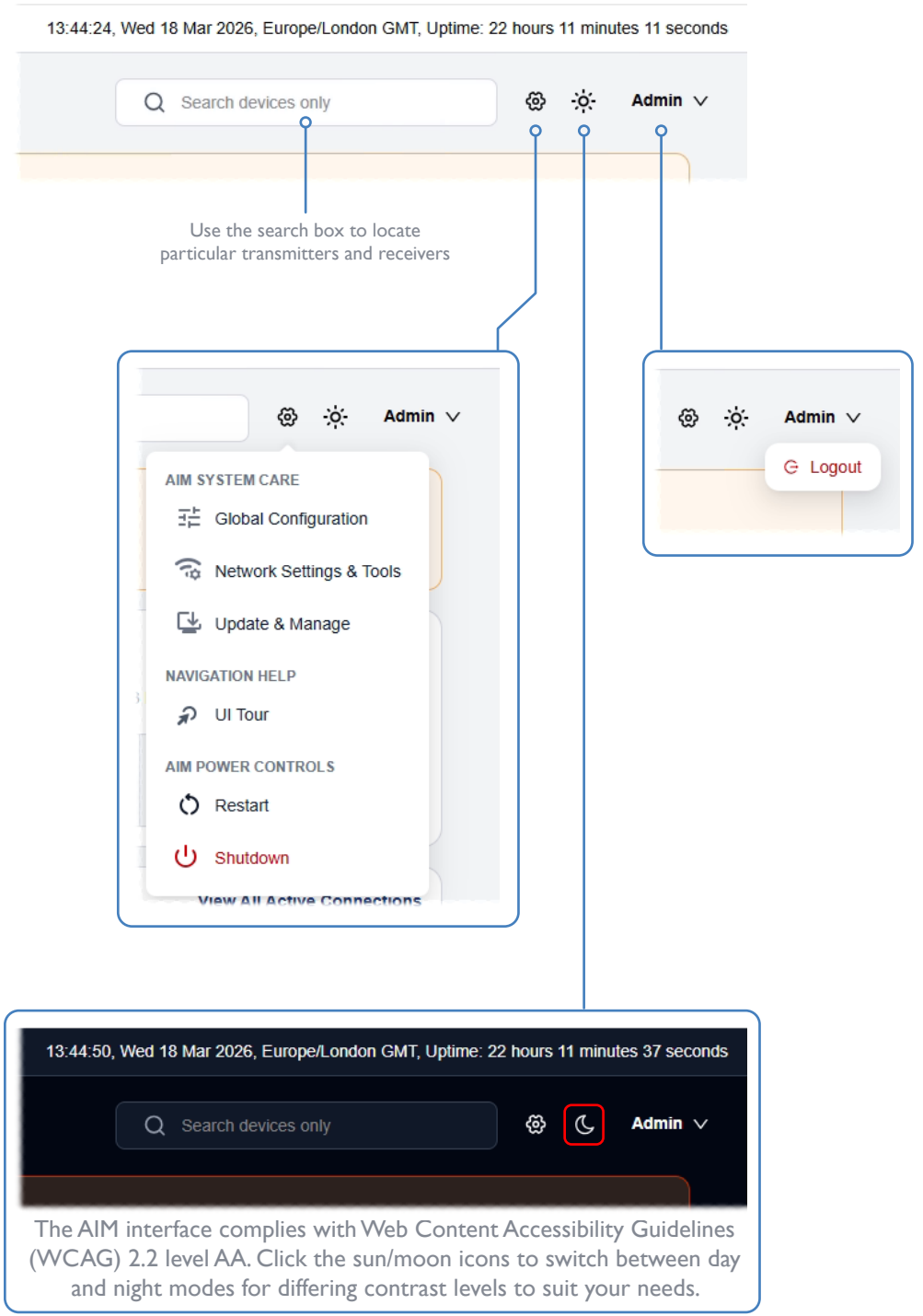
Please click a menu option to access explanations.

ADDER
THE IP KVM PEOPLE

HOME
- Dashboard — page 18
- Active Connections — page 20
- Logs
  - Connection Logs — page 23
  - Event Logs — page 24

DEVICES
- Receivers
  - All Receivers — page 25
  - Receiver Groups — page 29
  - Update Firmware — page 33
- Transmitters
  - All Transmitters — page 34
  - Transmitter Groups — page 39
  - Update Firmware — page 42
- C-USB LAN — page 43

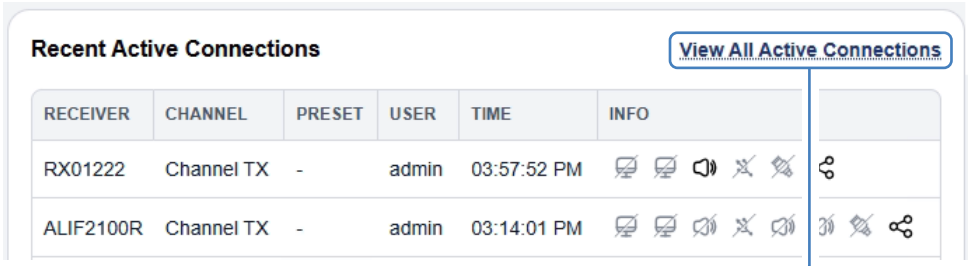
CORE OPERATIONS
- User Management
  - Users — page 45
  - User Groups — page 45
  - Directory Servers — page 49
- Channels
  - All Channels — page 51
  - Channel Groups — page 53
- Presets — page 55
- System Care
  - Servers — page 57
  - Global Configuration — page 58
  - Network Settings & Tools — page 65
  - Remote Support — page 70
  - Backup — page 71
  - Update — page 72
  - Statistics — page 73

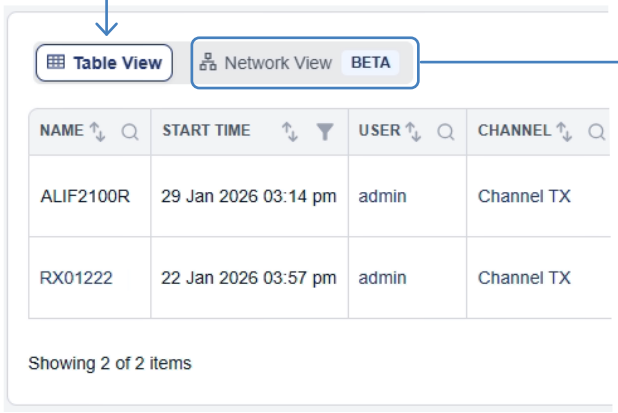


The AIM interface complies with Web Content Accessibility Guidelines (WCAG) 2.2 level AA. Click the sun/moon icons to switch between day and night modes for differing contrast levels to suit your needs.

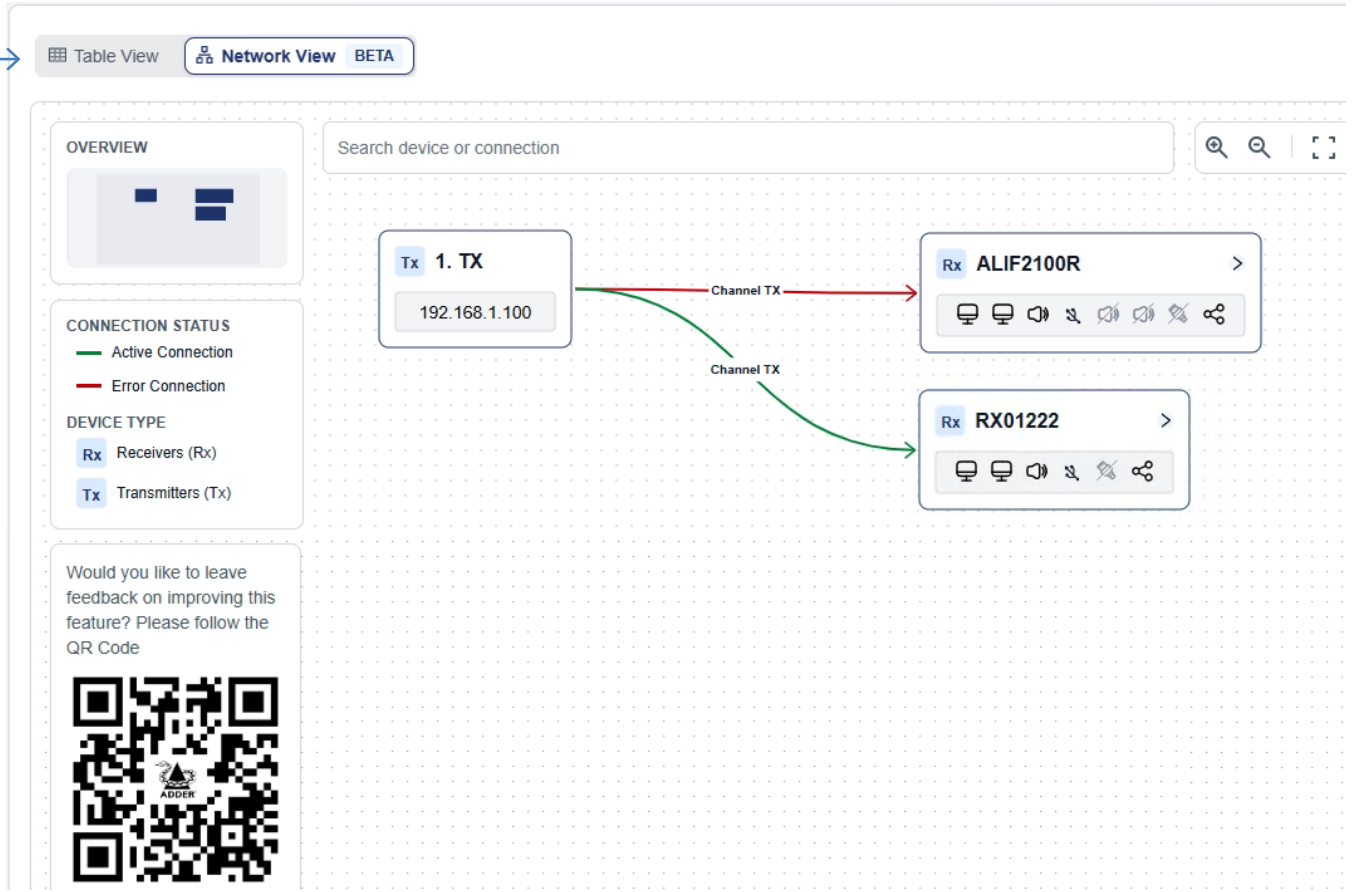
ACTIVE CONNECTIONS

This section provides a live overview of active devices that are under AIM control. You have a choice of viewing the device details in tabular form or a highly intuitive graphical representation.





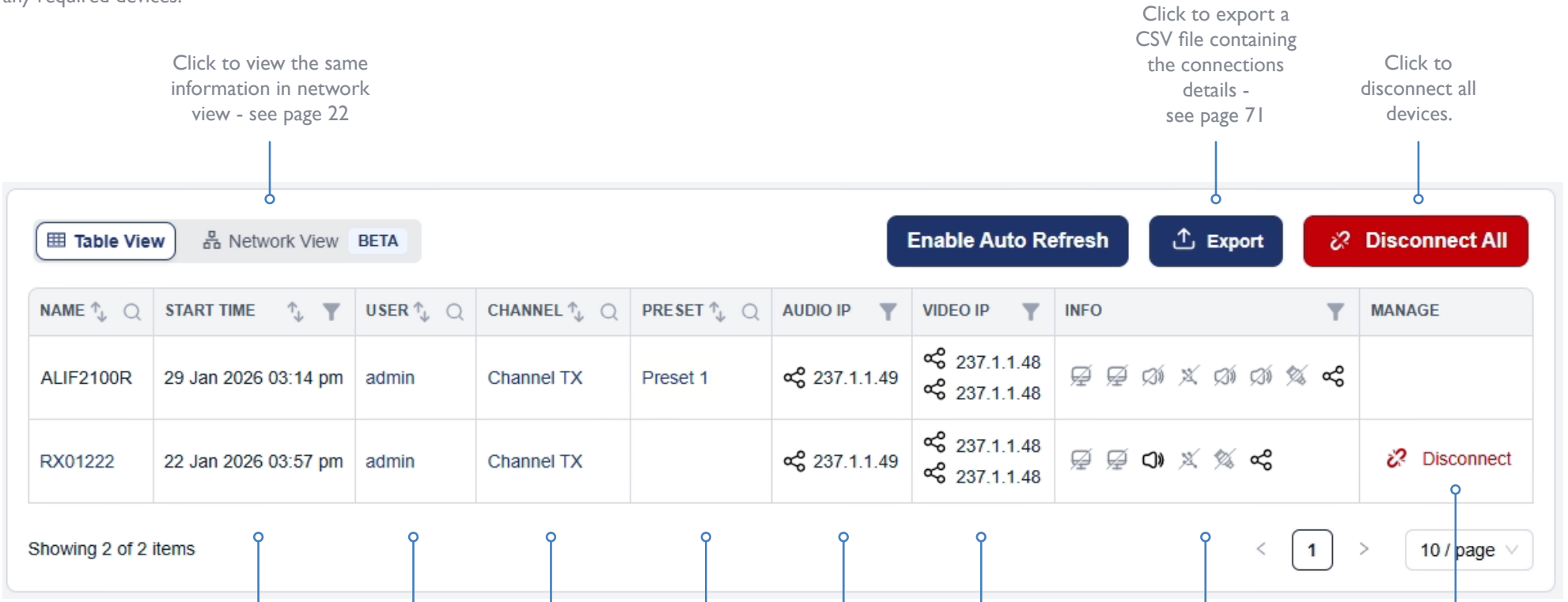
See page 21 for details about the Table View.



See page 22 for details about the Network View.

Active Connections > Table View

The table view lists full details of each controlled device. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required devices.

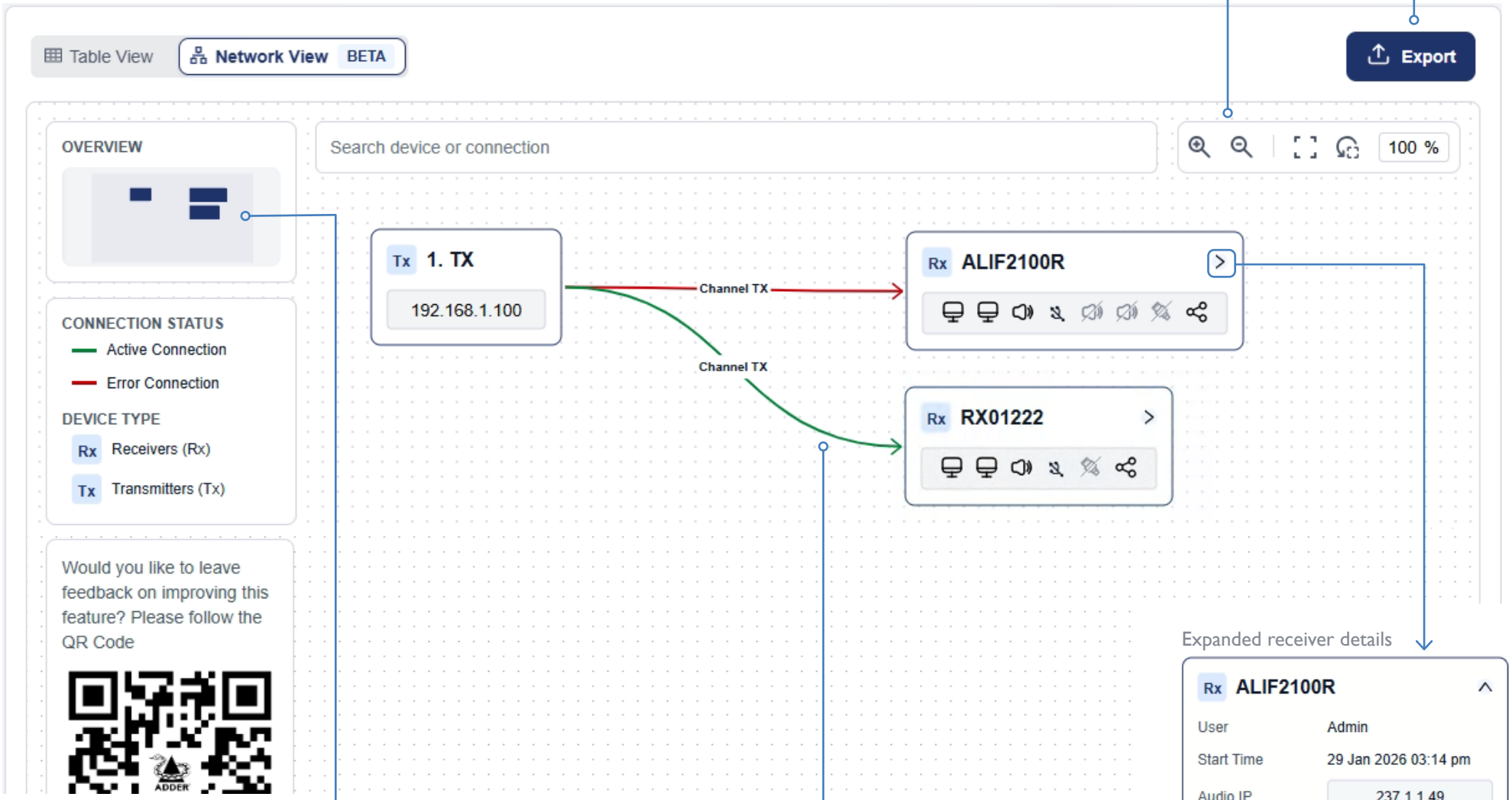


Active Connections > Network View

This view shows a dynamic graphical representation of the AIM network so that you can easily see how the various devices link with each other. You can zoom the view in and out to encompass your particular area of interest; you can also expand the details shown for any receiver unit.

These tools allow you to manipulate the view to suit your needs.

Click to export a CSV file containing the connections details - see page 71



The Overview indicates how your current view relates to the installation as a whole.

Links between transmitters and receivers are either shown in green (active) or red (error).

Expanded receiver details



LOGS

Connection logs

Shows all connections that have occurred within the AIM network. The most recent connections are shown at the top, and the log is paginated (the number of rows per page can be set from the option in the bottom right corner of the page). The log can be filtered to show all connections, or only currently active connections. The search (), filter () and order () options in the various column headers allow you to locate and focus upon any required entries.

The "Audio IP" and "Video IP" columns show whether the audio and video are being sent directly from the transmitter to the receiver or sent as a multicast to a multicast group. Direct links are denoted by the receiver's IP address only; whereas multicasts are indicated by the multicast icon () and the common multicast IP address (the address will be in the range specified within the "Multicast IP Settings" options within the Transmitters configuration page - see "All Transmitters" on page 34).

Actions that you can take within this page:

- Hover the mouse over the receiver, user or channel names to show more information about each item.
- Archive the Connection Log data to a .CSV file. Click the Export button to jump to the System Care > Backup page and then click the Archive button.

Click to auto refresh the page every 30 seconds.

Click to export a CSV file containing the connections details - see page 71

All Connection Logs

Enable Auto Refresh | Export

NAME	START TIME	END TIME	USER	CHANNEL	PRESET	AUDIO IP	VIDEO IP
RX01222	24 Mar 2026 01:32 pm		admin	Channel TX	Preset 1	237.1.1.49	237.1.1.48 237.1.1.48
RX01222	24 Mar 2026 01:32 pm	24 Mar 2026 01:32 pm	admin	Channel TX	Preset 1	237.1.1.49	237.1.1.48 237.1.1.48
RX 3000R	24 Mar 2026 01:22 pm		admin	AIM UI		192.168.1.104	192.168.1.104 -
ALIF3000Rbbfd	24 Mar 2026 01:25 pm	24 Mar 2026 01:26 pm	admin	AIM UI		237.1.1.40	237.1.1.39 -

Entries marked with this icon () are involved in multicast connections.

Event logs

This page lists events that have occurred within the AIM system, with a graphical overview at the top of the page and a full listing below. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required entries.

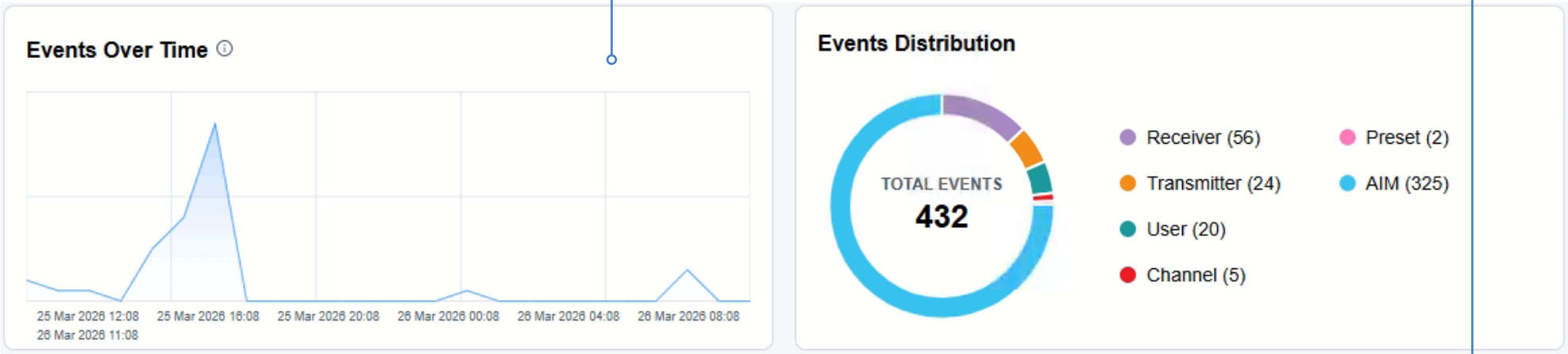
In particular, the From and Priority column headers allow you to filter (▼) the list.

Actions that you can take within this page:

- Archive the Connection Log data to a .CSV file. Click the Export button to jump to the System Care > Backup page and then click the Archive button.

The graphical data representations provide an at-a-glance overview of reported events.

Click to export a CSV file containing the connections details - see page 71



All Events

Export

TIME	EVENT	DETAILS	FROM	DEVICE	PRIORITY	IP ADDRESS
26 Mar 2026 09:56	Login	User 'admin' logged in successfully	AIM	-	MEDIUM	192.168.16.129
25 Mar 2026 18:46	Device status	online	Transmitter	221111	LOW	127.0.0.1
25 Mar 2026 18:46	Device status	online	Receiver	RX 3000R	LOW	127.0.0.1

RECEIVERS

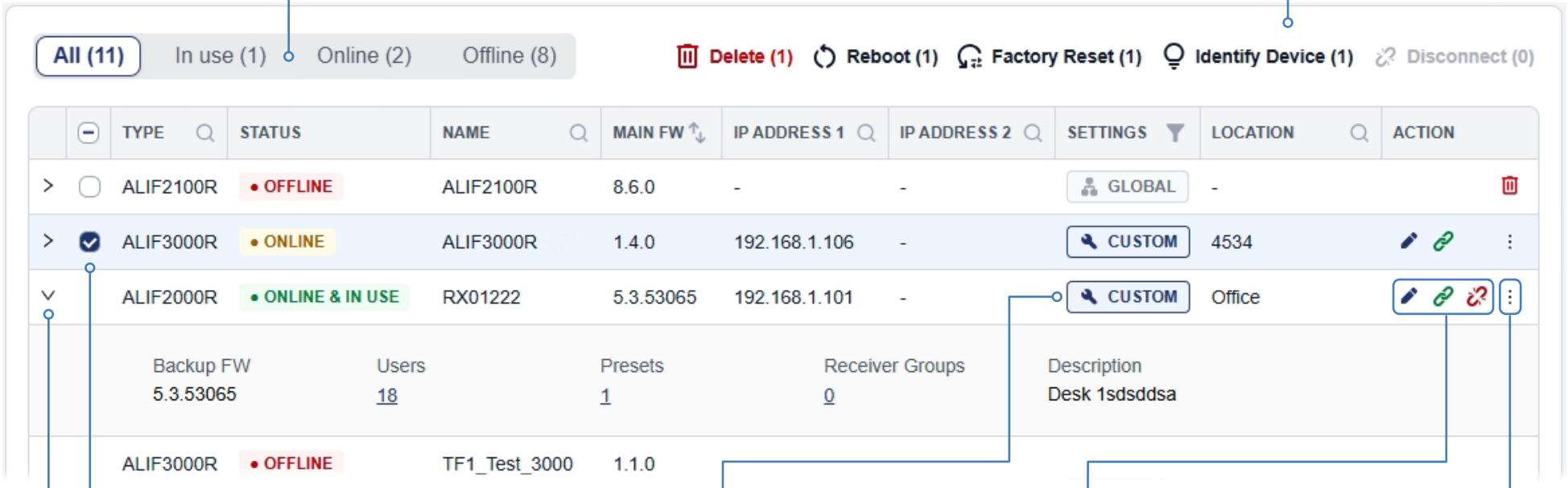
This section allows you to view and edit the individual receivers and also receiver groups registered within the AIM network. From here you can also manage the firmware versions of the installed receiver units.

All Receivers

The table view lists all of the receiver units within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required devices.

Use these options to narrow the list of receivers by their current operational status.

Collective actions (b)
As receivers are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged receivers are listed here. The numbers in brackets indicate how many of the currently tagged receivers would be affected by each operation if it were to be carried out.



Collective actions (a)
To carry out changes/operations on multiple receivers at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

Click the arrow to view a drop down summary of the backup firmware, users, presets, receiver groups and description that are associated with the chosen receiver.

Receivers marked as GLOBAL are using all of the global settings. Those marked as CUSTOM deviate from one or more global settings.

- Edit the receiver details - see page 26.
- Connect to a channel - a list of all channels that have permission to access this receiver will be displayed.
- Disconnect from a channel.

- Reboot
- Factory Reset
- Replace Device
- Identify Device
- Delete

Viewing and editing a receiver entry

When you choose a receiver entry, by clicking its icon in the All Receivers list, you will be able to view and edit the following details:

Device Information

Device Name, Location and Description

These are all useful ways for you to identify the receiver and its origins. A consistent naming and description policy is particularly useful in large installations.

Status

Can be: OFFLINE, ONLINE or ONLINE & IN USE.

Device ID / Type

Identity of the receiver.

Main/Backup Firmware

The current firmware versions contained within the unit.

Serial Number

Unique serial number of the receiver.

Date Added

Time and date of the first addition to the AIM network.

IP Settings

DHCP / Static (1, 2 and 3)

For each network port on the receiver, determines whether the IP address, netmask, gateway and DNS server details should be derived from the AIM DHCP server or input manually.

Note: Static IP addresses are only supported on the ALIF1002, ALIF20xx, ALIF2112T on ports 1 and 2.

DHCP Reservation off

If unticked, the AIM DHCP server will apply the same addressing details to maintain consistency.

MAC Address (1, 2 and 3)

Lists the fixed network identifiers for the various possible receiver ports.

System Settings

Login Required

When selected, anyone can use a receiver terminal and connect to a channel. The channels/permissions displayed to this anonymous user are those that are set for the "anonymous user" that is defined within the User Management section.

Reboot Schedule / Reboot Time - Allows the receiver to be rebooted at a particular time, either once on a particular day or on a recurring basis (hourly, daily or weekly).

Auto Login User

Allows you to authorize a user (or group) account to use the optional Auto Login feature. This option will be grayed out if the Auto Login feature has not been installed. See "Appendix I - Auto Login Feature" on page 94.

Allow Local Feedthrough - When selected, allows the receiver to connect directly to a local source. Feedthrough is supported on the following models: ALIF100x, ALIF20xx, ALIF21xx and ALIF40xx (*ALIF40xx units require firmware version 4.0 or greater to operate a local feed through link).*

On-Screen Display (OSD) Settings

OSD Display Options

Determines the text that will be displayed on the OSD for each receiver: Description, Location or both - or use global settings.

OSD Banner Position

Allows you to determine the position of the OSD banner on each user's screen - or use the global settings.

OSD Launch Icon Size

Determines the default size of the icons used in the OSD. Options include: Small, Medium, Large and Extra Large.

Receiver OSD Alerts

Determine the required setting for pop up OSD alerts: Inherit, No or Yes.

Show Current Channel

When selected, shows the currently connected channel as an overlay.

Touch Show OSD Enable

Determines whether the OSD can be shown on a touchscreen device when supported by certain ALIF devices - at present supported by ALIF2000- and 4000- series receivers.

OSD Touchscreen Monitor Mapping

Allows you to map the USB from a touchscreen monitor to the physical USB port on the receiver to control the OSD.

Viewing and editing a receiver entry *(continued)*

Localization & Input

Keyboard Country
Select the country code of the keyboard connected to the receiver.

Audio Input Type
Select the required audio input type: Mic or Mic Boost.

USB settings
Provides access to various USB peripheral configuration details.

HID Only
This option allows you restrict USB devices to allow only HID (mice, keyboards, tablets, touchscreens, etc.) devices to be connected to the receiver(s).

Disable Mass Storage
This option allows you to prevent the use of USB mass storage devices at the receiver(s). The *HID Only* and *Disable Mass Storage* options both affect how USB devices are supported at the receiver(s). Their use in combination can produce the following results:

HID Only	Disable Mass Storage	Outcome
No	No	No USB restrictions
Yes	No	Allow only HID devices (Mass storage devices are also blocked)
No	Yes	Exclude mass storage devices but allow other USB peripherals (e.g. mice, keyboards, tablets and touchscreens)
Yes	Yes	Allow only HID devices (Mass storage devices are blocked)

Disable Isochronous Endpoint OSD Alerts
When an isochronous USB device is connected to the receiver there will no longer be a warning message. ALIF units do not support isochronous devices.

Enable Isochronous Endpoint Attach
Some USB devices combine many USB devices behind a USB hub. (e.g. a keyboard with audio support). By enabling this option, devices will be allowed to connect to ALIF receivers, however, the isochronous part (e.g. the audio component) of the devices will not work.

Advanced Port Features
This section allows you to determine USB port behavior for use with certain USB devices.

The default is no reserved ports, Merging enabled and no feature code (or Quirk) set. We recommend that these are left at the default settings and are only changed under advice from an Adder FAE.

For each of the four USB ports on the receiver, certain rules can be applied depending upon the USB device connected.

If you have reserved USB ports on the transmitter, you can select which USB port to use for a particular device.

You can turn off USB merging for a particular port. This will slow down switching as the USB device will be enumerated every time that you switch.

You can also enter an advanced feature if it is necessary for your USB device. The drop down lists the feature codes for some known USB devices. Otherwise please contact your local FAE for advice.

Monitor 1/2 Settings

Video Compatibility Check
This reads the EDID from the attached monitor(s) and determines whether they are capable of displaying the selected video mode before connecting a channel. This prevents the receiver showing a black screen and the user being locked out, for instance because a dual link resolution has been selected to display on a single link monitor.

Force 60Hz
If enabled, the receiver frame rate is held at 60Hz regardless of the video input frame rate. The Video Switching options (below) cannot be altered when this option is enabled.

Video Switching
Provides two options for video switching:

- *Fast Switching* (default state) - Retains the same frame rate (at either 50Hz or 60Hz) depending upon which video resolution was displayed first.
- *Match Frame Rate* - Follows the source frame rate and will change the frame rate every time this changes even if the video resolution doesn't change. If you have one receiver switching between 1920x1080@60Hz and 1920x1080@50Hz then this setting will change the frame rate from 60Hz to 50 Hz every time that you switch.

Viewing and editing a receiver entry *(continued)*

At the foot of the receiver entry page are the memberships and permissions where access to any given receiver can be controlled. Such permissions can also be edited by the admin user(s) within receiver group, user group and user pages elsewhere within AIM.

Receiver Groups Membership

This section lists all receiver groups and allows you to grant or deny access to this receiver for each group as a whole.

User Permissions

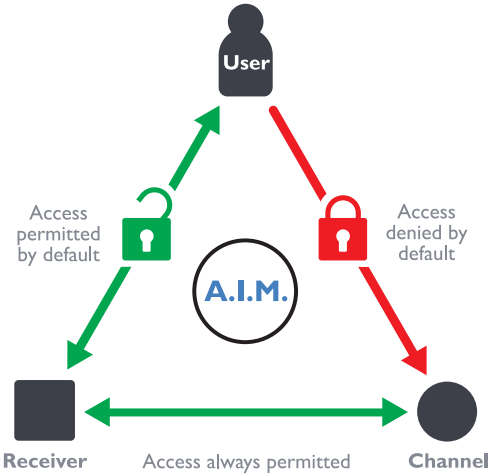
This section lists all users and allows you to grant or deny access to this receiver for each individual user.

User Groups Permissions

This section lists all user groups and allows you to grant or deny access to this receiver for those groups.

AIM security overview

Security considerations form a major part of AIM operation, ensuring that users have rapid access only to the systems for which they have permission. At its core, AIM manages an important three-way relationship between the users, the receiver(s) and the channels from the host computers:



Permissions

Permissions exist between Users, Receivers, and Channels.

By default, all users are granted permission to access ALL receivers.

By default, all receivers have permission to connect to ALL channels.

As shown in the diagram, the missing part is the permission for a user to access each channel.

Permissions between a user and a receiver can be applied in any of the following ways:

- User → Receiver
- User → User Group → Receiver
- User → User Group → Receiver Group → Receiver
- User → Receiver Group → Receiver

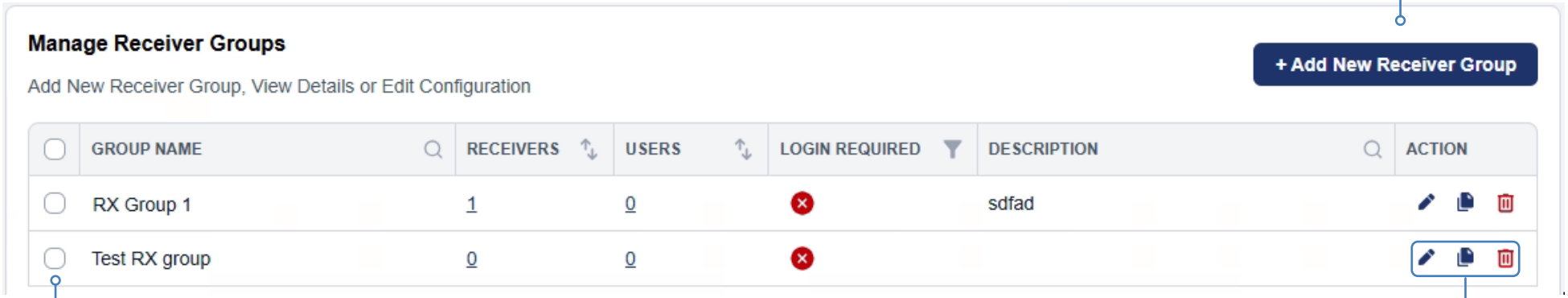
Thus, a very indirect way of granting permissions could be:

- User1 is in UserGroup1,
- UserGroup1 has access to ReceiverGroup1,
- ReceiverGroup1 contains Channel1,
- Therefore, User1 has access to Channel1 indirectly.

Receiver groups

The table view lists all of the receiver groups registered within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required devices.

Click to create a new receiver group - see page 30.



Collective actions
To carry out actions on multiple receiver groups at once, use these tick boxes to tag the ones that you wish to affect. The single collective action is to delete accounts.

- Edit the receiver group details - see page 30.
- Clone the receiver group - this will copy all of the details from the selected group into an edit page where you can adjust any necessary details to create a new group - see page 30.
- Delete the receiver group.

Viewing and editing a receiver group entry

When you choose a receiver group entry, by clicking the or icons (or by clicking the Add New Receiver Group button) in the All Receivers list, you will be able to view and edit the following details:

Group Information

Receiver Group ID, Name and Description

The group name must be populated with a name up to 45 characters. A consistent naming and description policy is particularly useful in large installations.

System Settings

Login Required

- **No**: When selected, anyone can use a receiver terminal and connect to a channel.
- **Use Global Settings**: When selected, the requirement for user log in will be determined by the "Login Required" setting within the User Management pages.
- **Yes**: When selected, a user will need to log in with the username and password defined in the "Users" section. They will only be allowed to log in if they have been granted permission to access devices in the receiver group.

Auto Login User

Allows you to authorize a user (or group) account to use the optional Auto Login feature. This option will be grayed out if the Auto Login feature has not been installed). See "Appendix I - Auto Login Feature" on page 94.

OSD Auto Logout Time

Determines the number of minutes of USB inactivity before the device issues a logout request to AIM. A value of 0 will disable this feature.

OSD Display Options

OSD Display Options

Choose whether to display Description, Location or both on the OSD.

OSD Banner Position

Allows you to determine the position of the OSD banner on each user's screen.

OSD Launch Icon Size

Determines the default size of the icons used in the OSD. Options include: Small, Medium, Large and Extra Large.

Touch Show OSD Enable

Determines whether the OSD can be shown on a touchscreen device when supported by certain ALIF devices - at present supported by ALIF2000- and 4000- series receivers.

OSD Channel & Alerts

Show Current Channel

When selected, shows the currently connected channel as an overlay.

Receiver OSD Alerts

Determine the required setting for pop up OSD alerts: Inherit, No or Yes.

Compatibility Check

Video Compatibility Check

When enabled, this option reads the EDID from the attached monitor and determines whether it is capable of displaying the selected video mode before connecting a channel. This prevents the receiver showing a black screen and the user being locked out because a dual link resolution has been selected to display on a single link monitor.

Audio Compatibility Check

Applicable only to receivers (such as the ALIF4021R) which are capable of processing multichannel digital audio via their DisplayPort™ connections. When enabled, this option reads the EDID from the attached monitor/audio system and determines whether the receiver's current audio setting (e.g. 2 Channel, 6 Channel, 8 Channel) is capable of correctly playing the selected audio (e.g. Stereo, 5.1 or 7.1) mode before connecting a channel.

Viewing and editing a receiver group entry *(continued)*

Localization & Input

USB settings

Provides access to various USB peripheral configuration details:

HID Only

This option allows you restrict USB devices to allow only HID (mice, keyboards, tablets, touchscreens, etc.) devices to be connected to the receiver(s).

Disable Mass Storage

This option allows you to prevent the use of USB mass storage devices at the receiver(s). *Note: ALIF3000 receivers do not support the use of mass storage devices, so this setting has no effect on them.*

The *HID Only* and *Disable Mass Storage* options both affect how USB devices are supported at the receiver(s). Their use in combination can produce the following results:

HID Only	Disable Mass Storage	Outcome
No	No	No USB restrictions
Yes	No	Allow only HID devices (Mass storage devices are also blocked)
No	Yes	Exclude mass storage devices but allow other USB peripherals (e.g. mice, keyboards, tablets and touchscreens)
Yes	Yes	Allow only HID devices (Mass storage devices are blocked)

Disable Isochronous Endpoint OSD Alerts

When an isochronous USB device is connected to the receiver there will no longer be a warning message. ALIF units do not support isochronous devices.

Enable Isochronous Endpoint Attach

Some USB devices combine many USB devices behind a USB hub. (e.g. a keyboard with audio support). By enabling this option, devices will be allowed to connect to ALIF receivers, however, the isochronous part (e.g. the audio component) of the devices will not work.

Advanced Port Features

This section allows you to determine USB port behavior for use with certain USB devices.

The default is no reserved ports, Merging enabled and no feature code (or Quirk) set. We recommend that these are left at the default settings and are only changed under advice from an Adder FAE.

For each of the four USB ports on the receiver, certain rules can be applied depending upon the USB device connected.

If you have reserved USB ports on the transmitter, you can select which USB port to use for a particular device.

You can turn off USB merging for a particular port. This will slow down switching as the USB device will be enumerated every time that you switch.

You can also enter an advanced feature if it is necessary for your USB device. The drop down lists the feature codes for some known USB devices. Otherwise please contact your local FAE for advice.

Connection Notification Settings

This section allows you to override various aspects of notification messages are displayed. Within the section, the notification settings are grouped as follows:

- Border Settings - these options are related to the coloured border that can be shown around the perimeter of the screen to emphasise messages when they are displayed.
- Message Settings - these options are concerned with the appearance and positioning of the message popup windows.
- Notification Types - these four options determine whether or not messages (and accompanying coloured borders) should be displayed to warn of losses of the main signal types: Video, audio, USB and Serial.
- Notification Labels - these options determine the labels displayed on messages concerning the loss of video, audio, USB and serial signals.
- Notification Messages - the entries in this section allow you to determine whether or not the default text strings (that cover various operational conditions) are inherited from the centralised settings.

Viewing and editing a receiver group entry *(continued)*

OSD Touchscreen Monitor Mapping

Allows you to map the USB connection from each touchscreen monitor to the physical USB ports on the receiver - at present supported by ALIF2100R & ALIF4000R receivers.

Monitor Settings

Video Freeze Image on Loss

When enabled, this feature will hold the last frame on screen (with a warning indication) if the communications to the TX or video to the TX are lost - at present supported by ALIF21xx- and 4xxx- series receivers with v7 firmware or later.

Force 60Hz

If enabled, the receiver frame rate is held at 60Hz regardless of the video input frame rate. The Video Switching options (below) cannot be altered when this option is enabled.

Video Switching

Provides two options for video switching:

- *Fast Switching* (default state) - Retains the same frame rate (at either 50Hz or 60Hz) depending upon which video resolution was displayed first.
- *Match Frame Rate* - Follows the source frame rate and will change the frame rate every time this changes even if the video resolution doesn't change. If you have one receiver switching between 1920x1080@60Hz and 1920x1080@50Hz then this setting will change the frame rate from 60Hz to 50 Hz every time that you switch.

Receiver Groups Membership

This section lists all receivers and allows you to grant or deny access for this group as a whole to certain receivers.

User Permissions

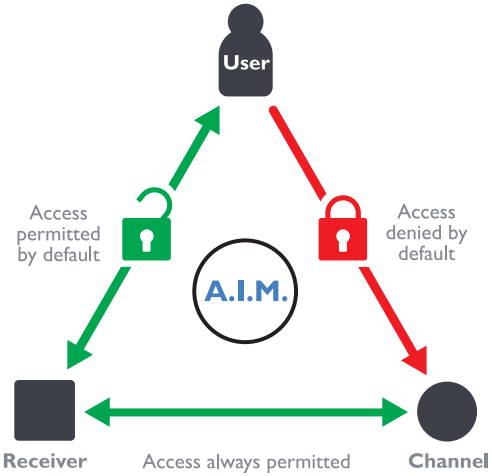
This section lists all users and allows you to grant or deny access to this receiver group for each individual user.

User Groups Permissions

This section lists all user groups and allows you to grant or deny access to this receiver group for those user groups.

AIM security overview

Security considerations form a major part of AIM operation, ensuring that users have rapid access only to the systems for which they have permission. At its core, AIM manages an important three-way relationship between the users, the receiver(s) and the channels from the host computers:



Permissions

Permissions exist between Users, Receivers, and Channels.

By default, all users are granted permission to access ALL receivers.

By default, all receivers have permission to connect to ALL channels.

As shown in the diagram, the missing part is the permission for a user to access each channel.

Permissions between a user and a receiver can be applied in any of the following ways:

- User → Receiver
- User → User Group → Receiver
- User → User Group → Receiver Group → Receiver
- User → Receiver Group → Receiver

Thus, a very indirect way of granting permissions could be:

- User1 is in UserGroup1,
- UserGroup1 has access to ReceiverGroup1,
- ReceiverGroup1 contains Channel1,
- Therefore, User1 has access to Channel1 indirectly.

Update firmware

This section allows you to centrally manage the firmware versions used by the receivers within the AIM network.

Upload New Receivers Firmware

Click the Upload New Firmware button to introduce a new ALIF receiver firmware file into the AIM server (to a maximum size of 2GB). The resulting page provides an area where you can drag and drop the firmware file (or click it to show a file dialog). Once the file is in place the next page will list the compatible receivers and allow you to identify, update and/or reboot the required units.

Install Existing Receivers Firmware

This option is similar to above, but uses firmware files that are already installed within the AIM server. Click the Install onto devices button to choose the firmware file and list the compatible receivers, which you can choose to identify, update and/or reboot, as required.

Delete Existing Receivers Firmware

Allows you to remove existing firmware files that are held on the AIM server.

TRANSMITTERS

This section allows you to view and edit the individual transmitters and also transmitter groups registered within the AIM network. From here you can also manage the firmware versions of the installed transmitter units.

All Transmitters

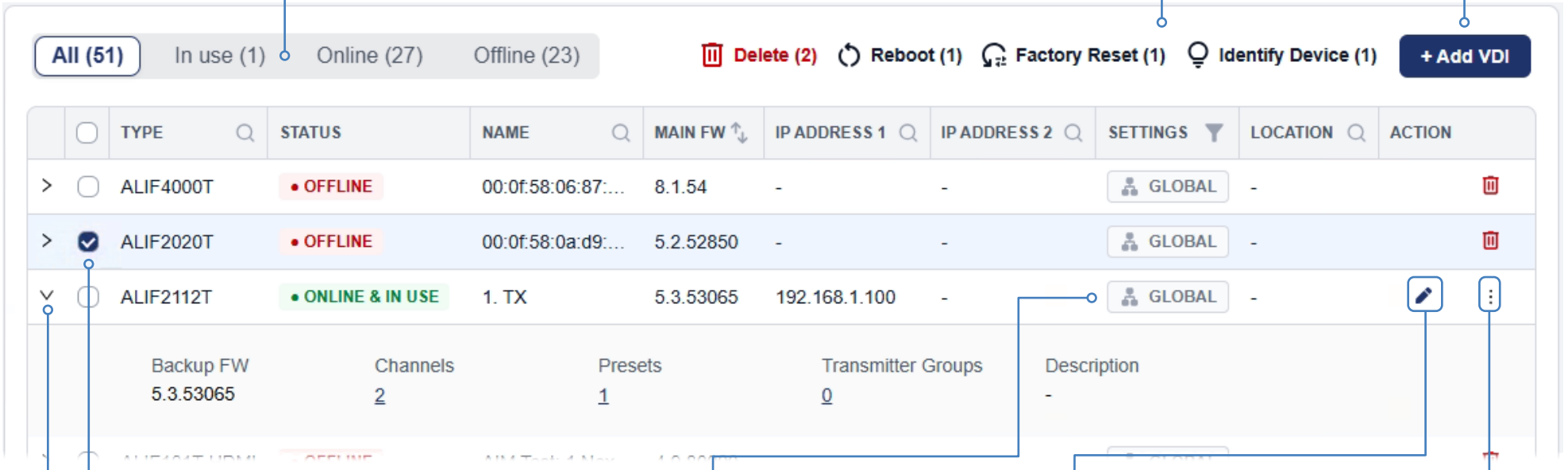
The table view lists all of the transmitter units within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required devices.

Use these options to narrow the list of transmitters by their current operational status.

Collective actions (b)

As transmitters are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged transmitters are listed here. The numbers in brackets indicate how many of the currently tagged transmitters would be affected by each operation if it were to be carried out.

Click to add a virtual machine (a device capable of connecting to the network and sharing their resources directly, without the need for a distinct transmitter. The common term for this is VDI (Virtual Desktop Infrastructure).
See page 38



Collective actions (a)

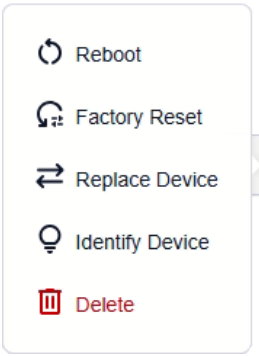
To carry out changes/operations on multiple transmitters at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

Click the arrow to view a drop down summary of the backup firmware, channels, presets, transmitter groups and description that are associated with the chosen transmitter.

Transmitters marked as GLOBAL are using all of the global settings. Those marked as CUSTOM deviate from one or more global settings.

Edit the transmitter details - see page 35.



Viewing and editing a transmitter entry

When you choose a transmitter entry, by clicking its icon in the All Transmitters list, you will be able to view and edit the following details:

Device Information

Device Name, Location and Description

These are all useful ways for you to identify the transmitter and its origins. A consistent naming and description policy is particularly useful in large installations.

Status

Can be: OFFLINE, ONLINE or ONLINE & IN USE.

Device ID / Type

Identity of the transmitter.

Main/Backup Firmware

The current firmware versions contained within the unit.

Serial Number

Unique serial number of the transmitter.

Date Added

Time and date of the first addition to the AIM network.

Multicast IP Settings

Video 1/2 Multicast IPs

Lists the IP addresses that will be used for distributing video signals when multicasting.

Audio Multicast IPs - Lists the IP addresses that will be used for distributing analog audio signals when multicasting.

Digital Audio Multicast IPs - Lists the IP addresses that will be used for distributing digital audio signals when multicasting.

System Settings

Reboot Schedule - Allows the transmitter to be rebooted at a particular time, either once on a particular day or on a recurring basis (hourly, daily or weekly).

IP Settings

DHCP / Static (1 / 2)

For each network port on the transmitter, determines whether the IP address, netmask, gateway and DNS server details should be derived from the AIM DHCP server or input manually.

DHCP Reservation off

If unticked, the AIM DHCP server will apply the same addressing details to maintain consistency.

MAC Address (1 / 2)

Lists the fixed network identifiers for the various possible transmitter ports.

Device Behavior & Limits

Enable Dummy Boot Keyboard

It is often necessary to have a keyboard reported at start up. This setting means that a "Virtual Keyboard" is always reported to the USB host. It may be necessary to disable this for use with some KVM switches.

Enable Audio

Determines the status of the audio feed from the transmitter.

USB Hub Size

Select either a 13 or 7 port USB hub. This determines the number of USB devices that can be connected to a single transmitter.

USB Speed

If required, select USB 1 Full Speed or USB 2 Hi-Speed USB, otherwise leave as Global.

Peak Bandwidth Limiter

The transmitter will use as much of the available network bandwidth as necessary to achieve optimal data quality, although typically the transmitter will use considerably less than the maximum available. In order to prevent the transmitter from 'hogging' too much of the network capacity, you can reduce this setting to place a tighter limit on the maximum bandwidth permissible to the transmitter. Range: 1 to 100%.

Viewing and editing a transmitter entry *(continued)*

Audio / Video Port 1/2 Settings

These two sections allow you to directly adjust various key video controls within the transmitter in order to obtain the most efficient operation taking into account connection speeds and the nature of the video images sent by that transmitter.

Magic Eye

Determines whether the Magic Eye feature should be enabled on certain ALIF transmitters. Magic Eye works to overcome the issues with increased bandwidth usage caused by 'dithering' techniques used on some computers, such as Apple® Macs. See the ALIF dual user guide for more details.

EDID

Determines how the video configuration details should be determined; options include:

- Use a fixed (static) EDID setting from the list (e.g. GENERIC 16:9, 1920x1080 HD1080, 1600x1200 UXGA, etc.). Using a fixed EDID setting can significantly speed up video switching times as EDIDs do not need to be checked, however, all of the installed monitors need to support the chosen resolution. *Note: Care must be taken when selecting a Dual Link Video resolution (e.g. 2560x1600) as certain ALIF units do not support Dual Link Video resolutions. In the case of a Dual Link EDID being set in the Global settings, no EDID will be set on Video port 2 of dual port ALIF transmitters.*
- USE CONNECTED MONITOR'S EDID - Check and use the EDID from the connected display screen at the point of switching. The process of checking EDIDs can cause minor delays while details are collected; enabling *EDID Optimisation* (discussed below) can help to regain some of the switching speed. This setting is shared between the video and digital audio port services on the same EDID port.
- USE SAVED MONITOR'S EDID - The EDID from the first RX to connect since the TX was last rebooted will be stored in flash memory and used for that video port. A reboot of the TX immediately restores and uses that EDID on the port without any RX needing to connect (as per using a fixed EDID mentioned above). This setting is shared between the video and digital audio port services on the same EDID port, but is separate from other EDID ports (ie the two video ports on a dual TX are handled separately). *Note: If this option is not supported by an endpoint or firmware does not support the feature it will default to using the monitor's EDID instead of a saved one.*

Dynamic Range EDID

For ALIF devices which support HDR (such as the ALIF4021T), this option can be used to grant permission to go beyond the standard SDR8 setting and use SDR10 or HDR10 when the connected host and video displays support 30bpp (10bpc) color depths.

EDID Optimization

When this option is ticked, the transmitters will compare the native resolution settings of monitors when switching. If a monitor has the same native resolution as the previous one, the new EDID is not sent to the graphics card. This speeds up switching as the graphics card does not need to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver has a monitor with a different native resolution, then the EDID will be updated to allow for a change in video mode.

Audio EDID

For transmitters which support digital audio via the DisplayPort™ connection(s), this setting determines how the audio should be configured: (USE CONNECTED MONITOR'S EDID, USE SAVED MONITOR'S EDID- see above for details) or a static setting: NONE, 2 CHANNEL *(Stereo)*, 6 CHANNEL *(surround 5.1)* or 8 CHANNEL *(surround 7.1)*. Using a fixed EDID setting can significantly speed up switching times as EDIDs do not need to be checked, however, all of the installed audio devices need to support the chosen format. Where EDIDs are checked, enabling Audio EDID Optimisation (below) can help to regain some of the switching speed.

Audio EDID Optimization

When enabled, transmitters will compare the digital audio settings when switching. If a receiver's digital audio settings are the same as the previous one, the new EDID is not sent to the host system. This speeds up switching as the host system does not need to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver uses a different audio setting, then the EDID will be updated to allow for a change in audio mode.

Hot Plug Detect Control

Determines whether to enable hot plug detection for monitors. By default this is enabled.

Hot Plug Detect Signal Period

By default this is set at 100ms, which is sufficient for most graphics cards. Occasionally it may be necessary to adjust this. An Adder engineer will advise if necessary.

Background Refresh

The transmitter sends portions of the video image only when they change. In order to give the best user experience, the transmitter also sends the whole video image, at a lower frame rate, in the background. The Background Refresh parameter controls the rate at which this background image is sent. The default value is 'every 32 frames', meaning that a full frame is sent in the background every 32 frames. Reducing this to 'every 64 frames' or more will reduce the amount of bandwidth that the transmitter consumes. On a high-traffic network this parameter should be reduced in this way to improve overall system performance. Options: Every 32 frames, Every 64 frames, Every 128 frames, Every 256 frames or Disabled.

Viewing and editing a transmitter entry *(continued)*

Compression

The newer AFZ+ codec complements the existing AFZ codec by providing greater compression for increased speed where pixel perfect results are not the primary focus. The transmitter video configuration page allows you to choose the required compression mode. Choices are:

- 'Pixel perfect' - only uses pixel perfect AFZ,
- 'Adaptive' - guarantees frame rate, builds to pixel perfect,
- 'Smoothest video' - forces the maximum compression, or
- 'Advanced' - allows you to choose the minimum and maximum compression modes:
  - 1 = 'AFZ only (pixel perfect),
  - 2 = 'AFZ+ Minimum compression',
  - 3 = 'AFZ+ Middle compression', or
  - 4 = 'AFZ+ Maximum compression'.

Frame Skipping

Frame Skipping involves 'missing out' video frames between those captured by the transmitter. For video sources that update only infrequently or for those that update very frequently but where high fidelity is not required, frame skipping is a good strategy for reducing the overall bandwidth consumed by the system. Range: 0 to 99%.

Serial Settings

Serial Parity, Serial Data Bits, Serial Stop Bits, Serial Speed

This group of settings allows you to define the key parameters for the AUX port of the transmitter so that it matches the operation of the device attached to it.

Transmitter Group Membership

This section lists all transmitter groups and allows you to grant or deny access to this transmitter for each group as a whole.

Adding a VDI / Configure Virtual Machine

Virtual Machines are capable of connecting to the network and sharing their resources directly, without the need for a distinct transmitter device; the common term for this is VDI (Virtual Desktop Infrastructure). These virtual machines can be accessed across the network directly by specially equipped receivers, such as the ALIF3000.

In the All Transmitters page, click the *+ Add VDI* button in the top right corner.

Description and Location

All VDI types also include Description and Location fields, which are useful identifiers for the transmitter unit and its exact location. These become even more valuable as the number of transmitters within the system increases.

VDI Type

The choice made here will determine the other options that are displayed:

RDP

RDP Name
Enter a valid name for the virtual machine.

IP Address/DNS Name
Enter either a distinct IP address or DNS name for the virtual machine.

Port
The usual port address for RDP connections is 3389.

Domain Name
Enter the domain name if the virtual machine host is part of a Windows domain, eg 'Engineering Dept', 'Marketing', etc. This will mean that users do not need to enter the domain name when they log in. Otherwise, leave this field blank.

Maximum Resolution
This option provides the option to cap the resolution used for connections to improve performance when high resolution monitor settings are used.

VNC

VNC Name
Enter a valid name for the virtual machine.

IP Address/DNS Name
Enter either a distinct IP address or DNS name for the virtual machine.

Port
The usual port address for VNC connections is 5900.

HTML

HTML Name
Enter a valid name for the virtual machine.

HTML URL
Enter the URL for the virtual machine.

Port
The usual port address for HTML connections is 80. For secure connections use 443.

Certificate
Secure websites require a security certificate. Only files with *.pem* or *.crt* extensions are valid.

TERMINAL *(SSH, Secure Shell)*

Terminal Name
Enter a valid name for the virtual machine.

IP Address/DNS Name
Enter either a distinct IP address or DNS name for the virtual machine.

Port
The usual port address for SSH connections is 22.

Horizon

Horizon Name
Enter a valid name for the virtual machine.

Set connection server IP Address or DNS Name
Enter either a distinct IP address or DNS name for the virtual machine.

Set connection server Port
The usual port address for VMWare Horizon connections is 443.

Domain Name
Enter the Windows domain to which the connection server belongs.

Service Name
Enter a service name, if appropriate.

Service Protocol
Choose either BLAST or PCoIP.

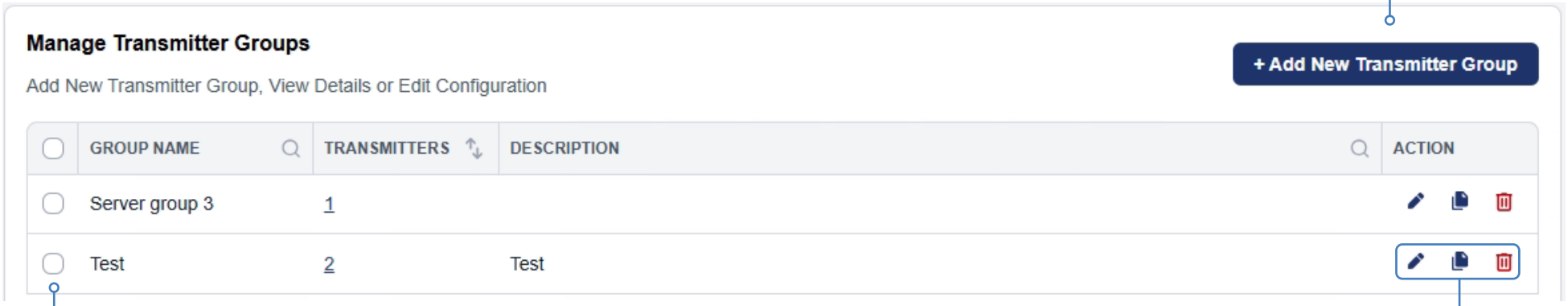
Maximum Resolution
This option provides the option to cap the resolution used for connections to improve performance when high resolution monitor settings are used.

Certificate
Upload all necessary server certificate files in order to allow a secure connection. Only files with .pem or .crt extensions are valid.

Transmitter groups

The table view lists all of the transmitter groups registered within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required devices.

Click to create a new transmitter group - see page 40.



Collective actions
To carry out actions on multiple transmitter groups at once, use these tick boxes to tag the ones that you wish to affect. The single collective action is to delete accounts.

- Edit the transmitter group details - see page 40.
- Clone the transmitter group - this will copy all of the details from the selected group into an edit page where you can adjust any necessary details to create a new group - see page 40.
- Delete the transmitter group.

Viewing and editing a transmitter group entry

When you choose a transmitter group entry, by clicking the ✎ or ⧉ icons (or by clicking the Add New Transmitter Group button) in the All Transmitters list, you will be able to view and edit the following details:

Group Information

Transmitter Group ID, Name and Description

The group name must be populated with a name up to 45 characters. A consistent naming and description policy is particularly useful in large installations.

EDID Settings

EDID

Determines how the video configuration details should be determined; options include:

- Use a fixed (static) EDID setting from the list (e.g. GENERIC 16:9, 1920x1080 HD1080, 1600x1200 UXGA, etc.). Using a fixed EDID setting can significantly speed up video switching times as EDIDs do not need to be checked, however, all of the installed monitors need to support the chosen resolution. *Note: Care must be taken when selecting a Dual Link Video resolution (e.g. 2560x1600) as certain ALIF units do not support Dual Link Video resolutions. In the case of a Dual Link EDID being set in the Global settings, no EDID will be set on Video port 2 of dual port ALIF transmitters.*
- USE CONNECTED MONITOR'S EDID - Check and use the EDID from the connected display screen at the point of switching. The process of checking EDIDs can cause minor delays while details are collected; enabling *EDID Optimisation* (discussed below) can help to regain some of the switching speed. This setting is shared between the video and digital audio port services on the same EDID port.
- USE SAVED MONITOR'S EDID - The EDID from the first RX to connect since the TX was last rebooted will be stored in flash memory and used for that video port. A reboot of the TX immediately restores and uses that EDID on the port without any RX needing to connect (as per using a fixed EDID mentioned above). This setting is shared between the video and digital audio port services on the same EDID port, but is separate from other EDID ports (ie the two video ports on a dual TX are handled separately). *Note: If this option is not supported by an endpoint or firmware does not support the feature it will default to using the monitor's EDID instead of a saved one.*

Dynamic Range EDID

For ALIF devices which support HDR (such as the ALIF4021T), this option can be used to grant permission to go beyond the standard SDR8 setting and use SDR10 or HDR10 when the connected host and video displays support 30bpp (10bpc) color depths.

EDID Optimization

When this option is ticked, the transmitters will compare the native resolution settings of monitors when switching. If a monitor has the same native resolution as the previous one, the new EDID is not sent to the graphics card. This speeds up switching as the graphics card does not need to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver has a monitor with a different native resolution, then the EDID will be updated to allow for a change in video mode.

Display Quality & Compression

Maximum Bits Per Pixel

This option controls the dynamic range mode. When set to 24bpp(8bpc), only SDR8 mode will be supported. When set to 30bpp(10bpc), the transmitter will allow SDR10 or HDR10 mode providing the host computer and attached video displays support those modes. See the user guide for ALIF devices that support 30bpp for a more detailed explanation.

Compression Level

The newer AFZ+ codec complements the existing AFZ codec by providing greater compression for increased speed where pixel perfect results are not the primary focus. The transmitter video configuration page allows you to choose the required compression mode. Choices are:

- 'Pixel perfect' - only uses pixel perfect AFZ,
- 'Adaptive' - guarantees frame rate, builds to pixel perfect,
- 'Smoothest video' - forces the maximum compression, or
- 'Advanced' - allows you to choose the minimum and maximum compression modes:
  - 1 = 'AFZ only (pixel perfect),
  - 2 = 'AFZ+ Minimum compression',
  - 3 = 'AFZ+ Middle compression', or
  - 4 = 'AFZ+ Maximum compression'.

Magic Eye Settings

Magic Eye

Determines whether the Magic Eye feature should be enabled on certain ALIF transmitters (e.g. 100T, 101T, 102T, 10xxT, 11xxT, 20xxT, 21xxT, 40xxT models). Magic Eye works to overcome the issues with increased bandwidth usage caused by 'dithering' techniques used on some computers, such as Apple Macs. See the ALIF dual user guide for more details.

Magic Eye SDR10 Level

Applies only to ALIF4000T units and is only active if the Magic Eye option is set to On. The default level of 1 is suitable for most sources. For Apple Macs with M-CPUs, level 4 may give the best results when using SDR10. In other cases, if SDR10 has no dithering but other color bit depths do, use level 0.

Viewing and editing a transmitter group entry *(continued)*

Audio EDID Settings

Audio EDID

For transmitters which support digital audio via the DisplayPort™ connection(s), this setting determines how the audio should be configured: (USE CONNECTED MONITOR'S EDID, USE SAVED MONITOR'S EDID- see above for details) or a static setting: NONE, 2 CHANNEL *(Stereo)*, 6 CHANNEL *(surround 5.1)* or 8 CHANNEL *(surround 7.1)*. Using a fixed EDID setting can significantly speed up switching times as EDIDs do not need to be checked, however, all of the installed audio devices need to support the chosen format. Where EDIDs are checked, enabling Audio EDID Optimisation (below) can help to regain some of the switching speed.

Audio EDID Optimization

When enabled, transmitters will compare the digital audio settings when switching. If a receiver's digital audio settings are the same as the previous one, the new EDID is not sent to the host system. This speeds up switching as the host system does not need to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver uses a different audio setting, then the EDID will be updated to allow for a change in audio mode.

Audio Settings

Enable Audio

Determines the status of the audio feed from the transmitters.

Enable Digital Audio

Determines the status of the digital audio feed (from HDMI) from the transmitters.

Device Behavior & Limits

Enable Dummy Boot Keyboard

It is often necessary to have a keyboard reported at start up. This setting means that a "Virtual Keyboard" is always reported to the USB host. It may be necessary to disable this for use with some KVM switches.

USB Speed

If required, select USB 1 Full Speed or USB 2 Hi-Speed USB, otherwise leave as Global.

USB Hub Size

Select either a 13 or 7 port USB hub. This determines the number of USB devices that can be connected to a single transmitter.

Hot Plug & Background Settings

Hot Plug Detect Control

Determines whether to enable hot plug detection for monitors. By default this is enabled.

Hot Plug Detect Signal Period

By default this is set at 100ms, which is sufficient for most graphics cards. Occasionally it may be necessary to adjust this. An Adder engineer will advise if necessary.

Background Refresh

The transmitter sends portions of the video image only when they change. In order to give the best user experience, the transmitter also sends the whole video image, at a lower frame rate, in the background. The Background Refresh parameter controls the rate at which this background image is sent. The default value is 'every 32 frames', meaning that a full frame is sent in the background every 32 frames. Reducing this to 'every 64 frames' or more will reduce the amount of bandwidth that the transmitter consumes. On a high-traffic network this parameter should be reduced in this way to improve overall system performance. Options: Every 32 frames, Every 64 frames, Every 128 frames, Every 256 frames or Disabled.

Serial Port Settings

Serial Parity, Serial Data Bits, Serial Stop Bits, Serial Speed

This group of settings allows you to define the key parameters for the AUX port of the transmitter so that it matches the operation of the device attached to it.

Transmitter Groups Membership

This section allows you to easily include or exclude individual transmitters for this group. All relevant group permissions will be applied to all transmitters that are included within the group.

Update firmware

This section allows you to centrally manage the firmware versions used by the transmitters within the AIM network.

Upload New Transmitters Firmware

Click the Upload New Firmware button to introduce a new ALIF transmitter firmware file into the AIM server (to a maximum size of 2GB). The resulting page provides an area where you can drag and drop the firmware file (or click it to show a file dialog). Once the file is in place the next page will list the compatible transmitters and allow you to identify, update and/or reboot the required units.

Install Existing Transmitters Firmware

This option is similar to above, but uses firmware files that are already installed within the AIM server. Click the Install onto devices button to choose the firmware file and list the compatible transmitters, which you can choose to identify, update and/or reboot, as required.

Delete Existing Transmitters Firmware

Allows you to remove existing firmware files that are held on the AIM server.

C-USB LAN

This section allows you to view and edit the individual C-USB LAN devices registered within the AIM network.

The table view lists all of the transmitter units within the AIM network. The search (🔍) and order (↑↓) options in the various column headers allow you to locate and focus upon any required devices.

Use these options to narrow the list of C-USB LAN devices by their current operational status.

Collective actions (b)

As C-USB LAN devices are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged devices are listed here. The numbers in brackets indicate how many of the currently tagged devices would be affected by each operation if it were to be carried out.



Collective actions (a)

To carry out changes/operations on multiple devices at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

- Edit the C-USB LAN details - see page 44.
- Indicates that the device is currently linked.
- Click to break the existing link.
- Delete the C-USB LAN device.

Viewing and editing a C-USB LAN entry

When you click the icon for an entry in the C-USB LAN list, you will be able to view and edit the details listed below. When Editing a C-USB LAN Receiver, you can associate it with an ALIF Receiver. You will then get a list of C-USB LAN Transmitters on the OSD from which it can connect to.

C-USB LAN Information

Channel Group Name and Description

These are all useful ways for you to identify the channel group. A consistent naming and description policy is particularly useful in large installations.

User Permission

This section defines to which users can access this device.

User Group Permission

This section defines the user groups that can use the device. Any permissions applied to the user group are inherited by all users in the user group.

USER MANAGEMENT

This section allows you to view and edit the users and also user groups registered within the AIM network. From here you can also manage the directory servers.

Users

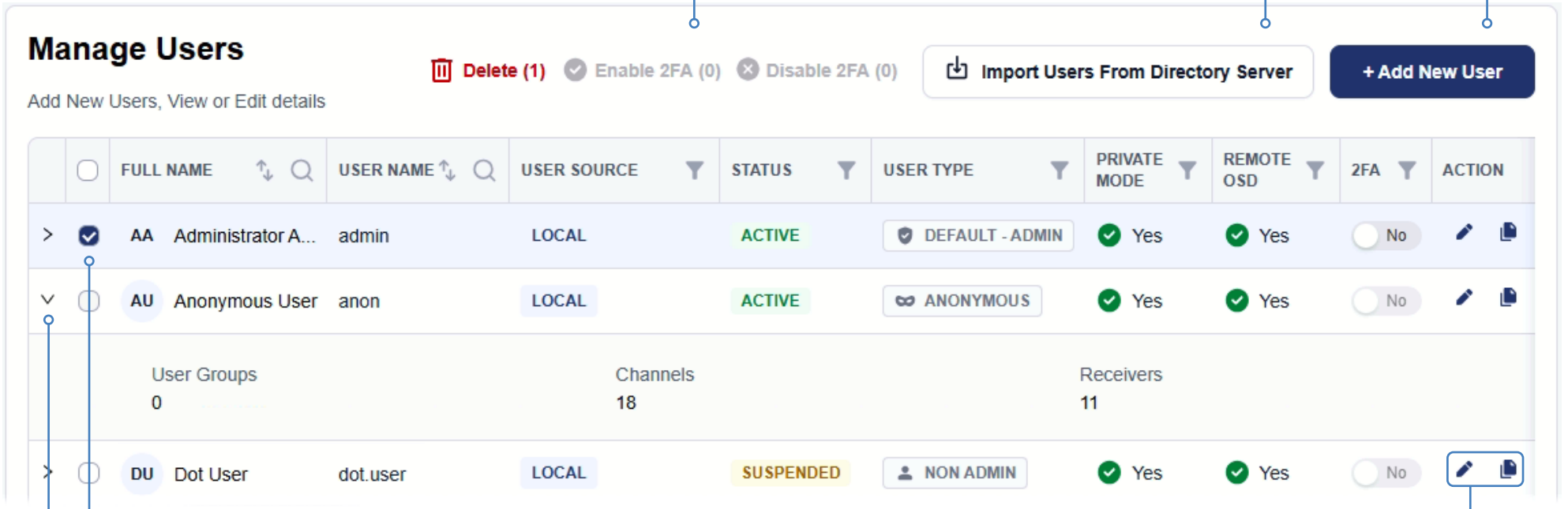
The table view lists all of the users registered within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required users.

Collective actions (b)

As users are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged entries are listed here. The numbers in brackets indicate how many of the currently tagged entries would be affected by each operation if it were to be carried out.

Click to import user details from directory servers - see page 46.

Click to add a new user - see page 46.



Collective actions (a)

To carry out changes/operations on multiple users at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

Click the arrow to view a drop down summary of the user groups, channels and receivers that are associated with the chosen user.

- Edit the user entry - see page 46.
- Clone the user entry - this will copy all of the details from the selected user into an edit page where you can adjust any necessary details to create a new user - see page 46.

Viewing and editing a user entry

When you choose a user entry, by clicking the ✎ or 🗎 icons (or by clicking the Add New User button) in the Users list, you will be able to view and edit the following details:

User Details

Username

The username is mandatory and must be unique within the AIM installation.

Note: If a user is synced with Active Directory, it is not possible to change the Username, First/Last Name, Password, or User Group membership. These items must be edited on the Active Directory server and the changes will filter through to AIM the next time a sync takes place with Active Directory.

First Name, Last Name and E-Mail

The First Name, Last Name and Email address entries are optional but are advisable within an installation of any size or one that will be administered by more than one person.

Security & Access

Require Password

Determines whether the chosen user must enter a password to gain access to channels and/or AIM admin system.

Password

The password is required for logging into a channel and/or for logging into the AIM admin system, if the user is to be granted admin privileges.

2FA Required?

Allows you to stipulate that the new user must use two-factor authentication when logging in to AIM. Both Google and Microsoft Authenticators are supported. For further details, please see Appendix F - Two Factor Authentication (2FA).

Note: If two-factor authentication is to be used, the AIM system must be linked to a local NTP server to maintain accurate time. Failure to do so could cause unreliable 2FA operation and the possibility of being locked out. See System Care > Network Settings & Tools > Settings.

Roles & Permissions

AIM Administrator?

When set to Yes, the user is granted privileges to log into the AIM admin system and make changes.

Suspend Account?

Allows the admin user to temporarily prevent the user from logging in without the need to delete the whole account.

Allow Private Mode?

Defines whether the user is able to connect to channels privately (locking out other users during a session). When this is set to "Inherit from User Groups/Global Setting", if ANY user-group that a user is a member of is granted permission to connect privately, then the user will have permission to connect privately. *Note: It is an additional requirement that the channel being accessed by the user must also permit private access.*

Enable Remote OSD?

This option determines whether the chosen user should be permitted to use the remote OSD functionality which permits access to remote receivers in order to change channels or presets even though a user has not logged into those receivers. Please see Using the Remote OSD feature for details.

User Group Membership

This section defines the user groups to which the user will be a member. Any permissions applied to the user group are inherited by all users in the user group.

Channel Permissions

This section defines to which channels the user should have access. *Note: Only the channels for which a user is given permission to access will appear within their channel list.*

Channel Group Permissions

This section defines to which channel groups the user should have access. *Note: Only the channel groups for which a user is given permission to access will appear within the list.*

Receiver and Receiver Group Permissions

All users are initially granted permission to use all receivers. If desired, permission to use a receiver and/or receiver group may be withdrawn from a user within these sections.

USB Extenders Permissions

This section allows you to grant access for the user to C-USB LAN devices.

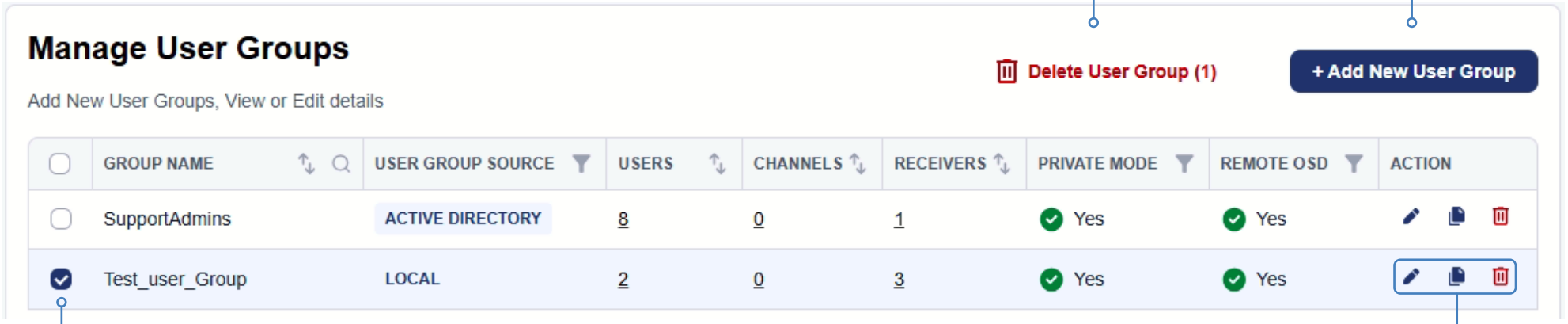
User Groups

The table view lists all of the user groups registered within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required users.

Collective actions (b)

As users are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged entries are listed here. The numbers in brackets indicate how many of the currently tagged entries would be affected by the action if it were to be carried out.

Click to add a new user group - see page 48.



Collective actions (a)

To carry out changes/operations on multiple user groups at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

- Edit the user group details - see page 48.
- Clone the user group - this will copy all of the details from the selected user group into an edit page where you can adjust any necessary details to create a new group - see page 48.
- Delete the user group.

Viewing and editing a user group entry

When you choose a user group entry, by clicking the or icons (or by clicking the Add New User Group button) in the Users list, you will be able to view and edit the following details:

User Group Details

User Group Name

The User Group name must be unique within the AIM installation.

Allow Private Mode?

Defines whether the users within the group will be able to connect to channels privately (locking out other users during the session). When this is set to "Use Global Setting", the setting for the "Grant all users private access" option will be applied. *Note: The final arbiter of whether any user can gain private access is always whether the channel being accessed is also set to allow private connections.*

Enable Remote OSD?

Determines whether members of the chosen user group should be permitted to gain OSD access to remote receivers in order to change channels.

User Permissions

This section allows you to select which users should be members of the group. Any permissions applied to the user group are inherited by all users in the user group. Users who are not currently members are shown in the left list and those who are members are shown within the right list.

Channel Permissions

This section defines to which channels and/or channel groups the user within this group should have access. *Note: Only the channels/channel groups for which a user is given permission to access will appear within their channel list.*

Channel Group Permissions

This section defines to which channels and/or channel groups the user within this group should have access. *Note: Only the channels/channel groups for which a user is given permission to access will appear within their channel list.*

Receiver Permissions

All users/user groups are initially granted permission to use all receivers. If desired, permission to use a receiver and/or receiver group may be withdrawn from members of this user group using this section.

Directory servers

To simplify integration alongside existing systems within organizations, AIM can be synchronized with an LDAP/Active Directory server. This allows a list of users (and user groups), together with usernames and group memberships to be quickly imported and kept up to date.

Initial configuration

The basic Active Directory (AD) server details are defined in this page. Once configured, click the Import Users from Directory Server button to scan the AD server for a list of folders and users/groups within those folders.

- If an AD user was not in the AIM user database, they will be imported.
- If an AD user is already in the AIM user database, they are kept.
- If an AD user is NOT marked for import/sync from the AD import page, and they already exist in the AIM user database, they will be removed from the AIM user database during the sync operation.
- IMPORTANT: It is thus vital to ensure that all users you want in the AIM system are always selected for import/sync, otherwise they will be removed.

LDAP & Sync Configuration

Enable/Disable LDAP

Click to start/stop the synchronization process.

Edit Sync Settings

Allows you to set a specific synchronization time to avoid conflicts. The schedule can be set hourly, daily or weekly.

Server List

Click the icon to edit the server details:

Server Details

Server Type

Choose the required directory server type from the drop down list.

Server Name and Description

Use these fields to provide clear identification of the LDAP server.

Domain Information

Account Suffix

The account suffix for your domain, e.g. *@mydomain.local*

Base DN

Specify the base Distinguished Name for the top level of the directory service database that you wish to access, e.g. *DC=mydomain,DC=local*

Filter

Optionally enter filter terms to search particular folders in the directory server.

Connection Settings

Domain Controller

Specify a server name or IP address of the LDAP server, e.g. *dc01.mydomain.local*

Note: When using the secure version of LDAP, which is more common, you need to prefix the IP address or name with ldaps://

Username and Password

Enter a valid domain account name.

Other

GSSAPI Kerberos Support

Enable this option to use secure authentication.

Kerberos Operating Manual

Click to display a summary of valid LDAP and Kerberos field values. See page 50.

Active Directory Tips

- A backup schedule is recommended so that any changes on the AD server are carried across to the AIM server regularly. You can choose from hourly/daily or weekly syncs. The settings/filters saved on this screen will be applied to each subsequent sync, ensuring that your list of users is kept accurate.
- To temporarily remove a particular user from AIM access, without having to make complicated LDAP filters, simply edit the AIM user to be suspended in the *User Management > Users page* - see page 45. Even though they will continue to be imported/synced from AD, they will be prevented from logging on.
- All LDAP filters should be self-contained, e.g: (!(cn=a*))
- Be sure to save any changes made to the sync settings before clicking the "sync-now" option. Otherwise, the next scheduled sync operation will overwrite any user changes you made in your "sync-now".
- User groups are only imported from AD to AIM if they contain users that are set to be imported too (i.e. a group will not be imported, even if it contains users, unless its users match the sync filters).

  Note: If a group contains more than 1499 users, then the group is returned as empty.
- Associations between users and user groups can only be made on the AD server - it is not possible to edit user/user-group membership for AD users/groups on the AIM server.
- Users and groups are technically "synchronized" rather than "imported" - each time a sync takes place, details are updated and if a user no longer matches the sync filters, they will be removed from the AIM user list.

LDAP Server fields

Field	Value
Server Type	Type of Directory Server (Active Directory or Redhat IDM or OpenLDAP or Azure AD or Google Workspace)
Server Name	Name of the server given by user
Description	Description of the server given by user
Account Suffix	The account suffix of your domain account (e.g: @mycompany.com)
Base DN	The base distinguished name of your domain account (e.g: DC=mycompany, DC=com)
Filter	Filter to search particular folders in directory server (e.g. ((ou=Employee)(ou=Contractor)))
Domain Controller	Server name or IP address of the LDAP server (e.g: dc01.mycompany.com)
Username	Username set in the domain account
Password	Password set in the domain account
Certificate	This will allow a secure connection. Only files with cer and crt extensions are valid (applicable only for Google Workspace and Azure AD)
Key in Use	This is required alongside a certificate for establishing a secure connection. Only files with key extensions are valid (applicable only for Google Workspace)

- If GSSAPI Kerberos Support is enabled, the user will need to fill in the additional Kerberos server information to facilitate secure authentication.

Kerberos Server fields

Field	Value
Server IP/ Hostname	The IP/hostname of the service machine, Eg: 192.168.15.104/kdc.mycompany.com where 192.168.15.104 and kdc.mycompany.com are IP and hostname of host system respectively. It refers to the network location of the KDC.
Server Realm	The Kerberos realm associated with the Directory server domain. It is the realm to which KDC belongs (e.g: mycompany.com)
Server Principal Name (SPN)	The SPN represents the service that the user is trying to access. For LDAP service request, the SPN would be "ldap/hostname of the service machine". Created for each service or application that wants to authenticate using Kerberos. These principals are registered in the KDC and are used to validate service requests (e.g:ldap/kdc.mycompany.com)

CHANNELS

This page provides access to all settings and options related directly to the video, audio and USB streams, collectively known as channels, emanating from any number of transmitters.

All Channels

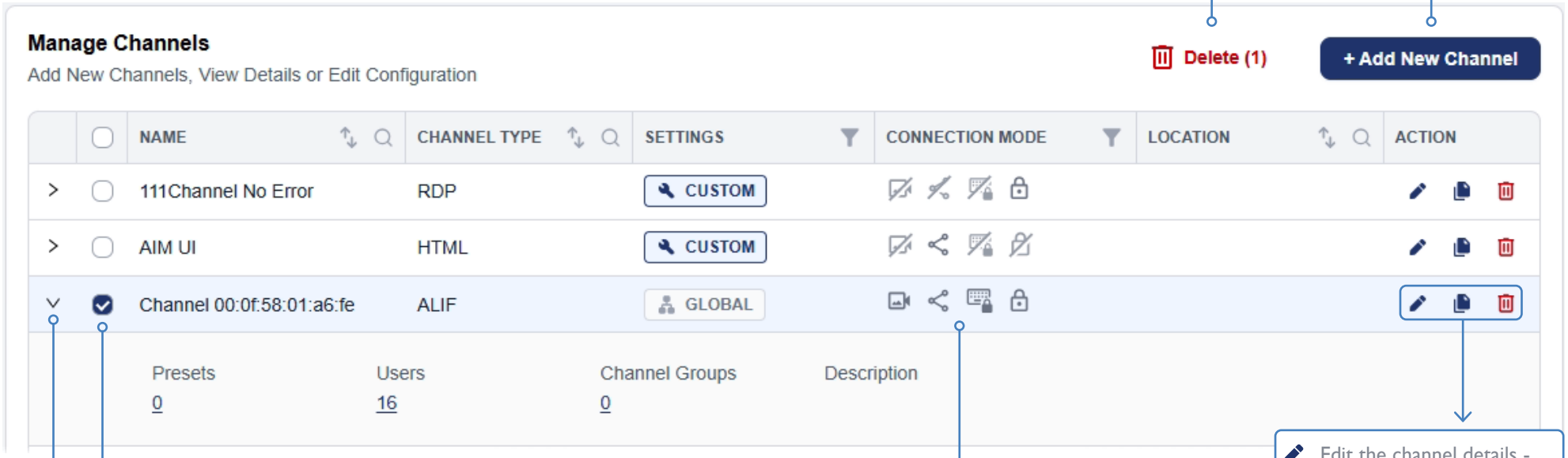
This page lists all channels that currently exist within the AIM system. A channel is automatically created for every transmitter when it is added and configured within the AIM network. The new default channel for each added transmitter will inherit the name of the transmitter. Such default names can be altered at any time and additionally, you can also create new channels manually, if necessary.

The table view lists all of the channels registered within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required channels.

Collective actions (b)

As channels are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged entries are listed here. The numbers in brackets indicate how many of the currently tagged entries would be affected by each operation if it were to be carried out.

Click to add a new channel - see page 52.



Collective actions (a)

To carry out changes/operations on multiple channels at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

Click the arrow to view a drop down summary of the presets, users, channel groups and description that are associated with the chosen channel.

Connection modes

- Video only
- Shared
- Exclusive
- Private

- Edit the channel details - see page 52.
- Clone the channel - this will copy all of the details from the selected channel into an edit page where you can adjust any necessary details to create a channel - see page 52.
- Delete the channel.

Viewing and editing a channel entry

When you choose a channel entry, by clicking the or icons (or by clicking the Add New Channel button) in the Channels list, you will be able to view and edit the following details:

Channel Information

Channel Name, Description and Location

These are all useful ways for you to identify the channel and its origins. A consistent naming and description policy is particularly useful in large installations.

Video Output, Audio Output and Hardware Connections

These drop down boxes list all of the available streams from installed transmitters. When creating a channel, you can choose to take all streams from the same transmitter or from different ones, as required.

Notes:

- Where necessary, channels can be created without video, audio, USB and/or serial.
- Only one receiver can use a transmitter's serial port at any time.
- Digital audio is the audio signal that is derived from video signals, such as DisplayPort™ connections and is only available on certain dual port ALIF models.
- *When specifying dual-head video channels, we recommend that you avoid choosing video sources from two different transmitters. Highly active video from two sources can result in video degradation and loss.*

OSD Settings

Override OSD Banner Position

Allows you to override the global setting for the positioning of the OSD banner for this channel.

Mark this channel as sensitive in the OSD

This will mark the channel as sensitive within the OSD channels list.

Connection Mode

This section allows you to define the types of connections that you wish to permit users to make. You can define particular individual or combined connection types to suit requirements.

Note: Channel Modes are not configurable on VDIs due to the nature of their connections.

Note: This setting for each channel acts as the final arbiter of whether exclusive access can actually be achieved. If you deny exclusive access rights within this setting, then exclusive access for any user cannot take place for this channel, regardless of settings made elsewhere.

- **Inherit from global** - uses the setting of the "Allowed Connection Modes" option within the Dashboard > Settings page.
- **Set for this channel** - permits you to choose modes manually:
  - **Video-Only**: Allows users only to view the video output; the USB channel is denied.
  - **Shared**: Allows users to control a system in conjunction with other users.
  - **Exclusive**: Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.
  - **Private**: Allows a user to gain private access to a system, while locking out all others.

Channel Group Permissions

This section defines to which channels and/or channel groups the user within this group should have access. *Note: Only the channels/channel groups for which a user is given permission to access will appear within their channel list.*

User Permissions

This section defines to which users can access this channel.

User Group Permissions

This section defines the user groups that can use the channel. Any permissions applied to the user group are inherited by all users in the user group.

Channel Groups

Channel groups allow easy permission-granting for several channels at once. Permissions can be set to determine which users can access channels within a channel group. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required users.

Collective actions (b)

As channels are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged entries are listed here. The numbers in brackets indicate how many of the currently tagged entries would be affected by the action if it were to be carried out.

Click to add a new channel group - see page 54.



Collective actions (a)

To carry out changes/operations on multiple channel groups at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

- Edit the user group details - see page 54.
- Clone the channel group - this will copy all of the details from the selected channel group into an edit page where you can adjust any necessary details to create a new group - see page 54.
- Delete the channel group.

Viewing and editing a channel group entry

When you choose a channel group entry, by clicking the or icons (or by clicking the Add New Channel Group button) in the Channel groups list, you will be able to view and edit the following details:

Channel Information

Channel Group Name and Description

These are all useful ways for you to identify the channel group. A consistent naming and description policy is particularly useful in large installations.

Channel Group Membership

This section defines to which channels and/or channel groups the user within this group should have access. *Note: Only the channels/channel groups for which a user is given permission to access will appear within their channel list.*

User Permission

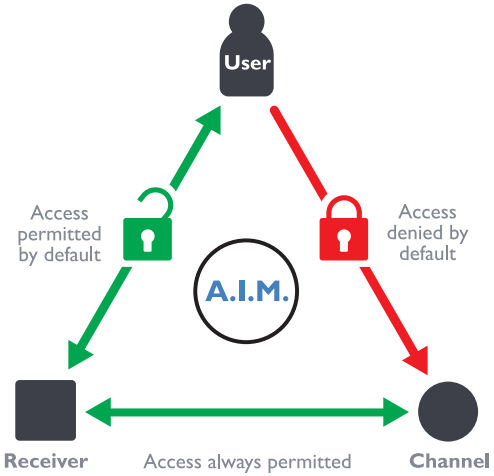
This section defines to which users can access this channel group.

User Group Permission

This section defines the user groups that can use the channel group. Any permissions applied to the user group are inherited by all users in the user group.

AIM security overview

Security considerations form a major part of AIM operation, ensuring that users have rapid access only to the systems for which they have permission. At its core, AIM manages an important three-way relationship between the users, the receiver(s) and the channels from the host computers:



Permissions

Permissions exist between Users, Receivers, and Channels.

By default, all users are granted permission to access ALL receivers.

By default, all receivers have permission to connect to ALL channels.

As shown in the diagram, the missing part is the permission for a user to access each channel.

Permissions between a user and a receiver can be applied in any of the following ways:

- User → Receiver
- User → User Group → Receiver
- User → User Group → Receiver Group → Receiver
- User → Receiver Group → Receiver

Thus, a very indirect way of granting permissions could be:

- User1 is in UserGroup1,
- UserGroup1 has access to ReceiverGroup1,
- ReceiverGroup1 contains Channel1,
- Therefore, User1 has access to Channel1 indirectly.

PRESETS

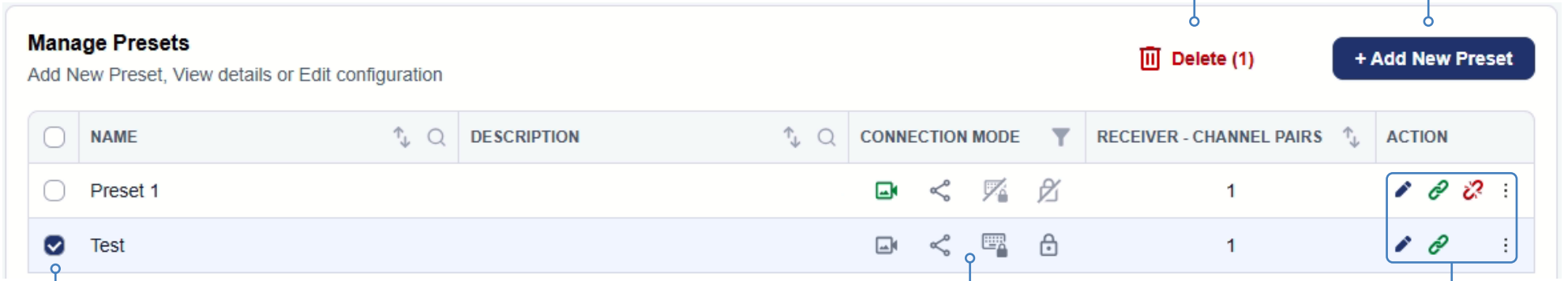
Presets enable multiple actions to be pre-defined so that they can be initiated with a single action. This feature is particularly useful when switching multiple ADDERLink INFINITY units, where multiple video heads need to be switched in unison between different server systems. According to how a preset is configured, it is possible to have one or more receivers connected to separate channels (i.e. unicast) or multiple receivers connected to a single channel (i.e. multicast).

The table view lists all of the presets registered within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required channels.

Collective actions (b)

As presets are tagged using the tick boxes (on the left side of each line), the possible actions that could be carried out on the tagged entries are listed here. The numbers in brackets indicate how many of the currently tagged entries would be affected by each operation if it were to be carried out.

Click to add a new channel - see page 56.



Collective actions (a)

To carry out changes/operations on multiple presets at once, use these tick boxes to tag the ones that you wish to affect. See also top right.

If required, use the tick box in the column header to, in turn, select all and deselect all.

Connection modes

- Video only
- Shared
- Exclusive
- Private

Non-authorized modes are crossed out.

Modes appear in green when connected.

- Edit the preset details - see page 56.
- Duplicate the preset - this will copy all of the details from the selected preset into an edit page where you can adjust any necessary details to create a new entry - see page 56.
- Click to break an existing connection.
- Delete the preset.

Viewing and editing a preset entry

When you choose a preset entry, by clicking the or icons (or by clicking the Add New Preset button) in the presets list, you will be able to view and edit the following details:

Preset Information

Preset Name and Description

These are all useful ways for you to identify the preset. A consistent naming and description policy is particularly useful in large installations.

Receiver - Channel Pair

This section is where receivers are paired with channels - up to four pairings can be made within a single preset. The drop down boxes list all of the available receivers and channels.

Click the Add New Pair button to begin a new pairing.

Connection Mode

This section allows you to define the types of connections that you wish to permit users of this preset to make. You can define particular individual or combined connection types to suit requirements.

Note: Channel Modes are not configurable on VDIs due to the nature of their connections.

Note: This setting for each channel acts as the final arbiter of whether exclusive access can actually be achieved. If you deny exclusive access rights within this setting, then exclusive access for any user cannot take place for this channel, regardless of settings made elsewhere.

- **Inherit From Global** - uses the setting of the "Allowed Connection Modes" option within the System Care > Global Configuration page - see page 58.
- **Set For this Channel** - permits you to choose modes manually:
  - **Video-Only**: Allows users only to view the video output; the USB channel is denied.
  - **Shared**: Allows users to control a system in conjunction with other users.
  - **Exclusive**: Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.
  - **Private**: Allows a user to gain private access to a system, while locking out all others.

Remember to click the **Save** button in the bottom right corner.

Manage Servers

For installations that require greater redundancy, it is possible to have two or more AIM servers running on the same subnet. If used on multiple subnets it is possible to have two or more servers on each subnet. If the primary server fails then alternative servers with the same database can take over until the primary unit recovers.

Note: If a backup or satellite AIM is promoted to primary and it is using https, you will need to download the new certificate otherwise https will not work.

Each server entry will have one of five possible states within the ***Role*** column:

- **Unconfigured** The server is a factory fresh device or has performed a full factory reset. This does not yet have a proper rôle.
- **Solo** This is a server acting as a standalone AIM server. If there is only going to be one AIM server on the subnet, this is the Role that should be used.
- **Primary** The server is configured as a fully functional AIM from which a back-up server can be slaved.
- **Backup** If more than one server is on the same subnet this is a primary backup configuration. If there are three servers on the same subnet you will have one primary and two backups.
- **Satellite** This is the rôle of a server on a different subnet to the primary. If you have multiple servers on the different subnet these would all be called satellite servers. If you had a configuration with two servers on Vlan 1, two servers on Vlan 2 and 1 server on Vlan 3, AIM would report 1 primary on Vlan 1, 1 Backup on Vlan 1, 2 satellites on Vlan 2 and 1 satellite on Vlan3.

Each server entry will also show one of six entries within the *Status* column:

- **Active** This server is functioning as an AIM server and is administering ALIF devices. Primary or Solo servers with this status are fully functional AIM servers that will accept network configuration changes. A Backup server with this status is functioning as an Active Primary. It will execute channel changes, but will not accept network configuration changes.
- **Standby** This server is currently maintaining its database as a copy of the primary in readiness to take over if necessary.
- **Offline** This server should be maintaining a copy of the primary's database, but is not doing so. The offline status of a satellite server means that it is ready to take over ALIFs on its own subnet if necessary, but that it cannot communicate with the primary server.
- **Initialising** This is the initial status upon start up. This should not persist beyond the initial start up procedure.
- **Quiescent** This is an inactive server on the network. It will not function without remedial action from its system administration. A typical reason for this is the presence of another server on the network blocking its configured role. i.e. two servers are configured as a primary on the same subnet.
- **Failed** This server has suffered a serious internal failure.

Server Global Configurations

Timeout Settings

Primary Timeout

The time (in seconds) for the Primary server to be unavailable before the Backup takes over.

Quiescent Timeout

The time after which an inactive (*Quiescent*) server is assumed to have disappeared.

Backup Check Interval

The interval between the Primary server querying its backups to determine if they are all on-line.

Backup Timeout

The period of time that a backup server can be off line or uncontactable before it is treated as a failed server.

Timeout Settings

Authentication Required?

If set to 'Yes', then a new, unconfigured AIM server will be unable to join the cluster automatically; its behavior will be to report itself as unconfigured and quiescent, and request a password. Entering the cluster password will then allow it to join the cluster as a Backup.

Cluster Password

This is the password that is used for AIM-to AIM https queries if the *Require Authentication* option is enabled.

SYSTEM CARE > GLOBAL CONFIGURATION

This page provides access to base configuration settings for:

- The AIM system itself,
- Transmitters, and
- Receivers.

AIM configuration settings

Security Settings

2FA OTP Window

Determines how long a one-time password will remain valid. For example, a value of 2 will make an OTP valid for 1 minute before and after the current time. Valid values are from 1-9, however, lower values are recommended. For further details, please see Appendix F - Two Factor Authentication (2FA).

Disable AIM UI over KVM Network

When set to Yes, access to the AIM WebUI will be disabled (effective at the next login) when the Eth2 port is enabled. If this option is enabled and a network is not available on the Eth2 port then AIM can still be accessed via the Eth1 port.

Anonymous User

Determines which user is shown in the log when a receiver is set to 'No login required'.

Disable Password Reset

This prevents the password reset button from appearing on the login page.

Timeout Settings

Receiver OSD Timeout

Determines the time period of inactivity within the OSD after which a standard user will be automatically logged out.

AIM Administrator Timeout

Determines the time period of inactivity within the AIM config pages after which an admin user will be automatically logged out.

Device Visibility

Hide Dormant Devices

When enabled, this option hides devices that have been offline for more than 24 hours (excludes RDP servers).

Show Outdated Devices

When enabled, this option shows devices that are outdated for the current AIM version (excludes RDP servers).

Allowed Connection Modes

Determines the global setting that will be applied to all new channels concerning connection modes. The setting made here is only applied as a default and can be overridden at the channel level, where necessary. Options are:

- **Video-Only**: Allows users only to view the video output, the USB channel is denied.
- **Shared**:* Allows users to control a system in conjunction with other users.
- **Exclusive**: Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.
- **Private**: Allows a user to gain private access to a system, while locking out all others.

Note: By default, all new channels are set to inherit this global value. So it's easy to change all channel connection modes simply by changing the global setting. If a channel has its own setting, the global setting has no effect on that channel.

** If USB is disabled, Shared mode will not be available as an option.*

Display Settings

Rows per Page

The number of rows to display in all paginated tables in the admin section.

Locale

Determines the language shown on the OSD menus of the receivers; the admin configuration web pages will remain in English.

Language Packs

Allows you to manage the installation of optional language packs for use within AIM.

All User Feature Permission

This section manages the global access rights for users as related to specific functions, such as allowing private access, force disconnect, etc.

Diagnostics

Debug Level

This allows information to be collected for diagnostic purposes. Options range from Normal to High, Full or Extra.

In order to prevent excess debug logging from potentially overloading the ALIF network, when the level is raised to any setting above *Normal*, a Timeout setting will be shown. This allows you to set a time period after which the raised debug level will be automatically returned to the Normal setting. Timeout options range from 5 minutes to 2 days.

The Debug Level setting should not be changed from *Normal* unless advised by Adder Support.

AIM configuration settings *(continued)*

API

Login Required
If enabled, the anonymous use of the AIM API will be disallowed.

Anonymous user
Determines the user permissions to be used when the API is accessed without logging in.

Licensing

Devices Configured
Indicates the number of devices currently operational under the license.

Upgrade License - (see Appendix J for details)
Displays information about the number of devices that can be connected to the AIM server.

Licensed Features - Displays the level of operation permitted under the current license. Click view/change to see more detail and gain a unique identifier that can be declared to Adder when upgrading a license.

Transmitter

EDID Settings

EDID Optimization

When this option is ticked, the transmitters will compare the native resolution settings of monitors when switching. If a monitor has the same native resolution as the previous one, the new EDID is not sent to the graphics card. This speeds up switching as the graphics card does not need to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver has a monitor with a different native resolution, then the EDID will be updated to allow for a change in video mode.

EDID

Determines how the video configuration details should be determined; options include:

- Use a fixed (static) EDID setting from the list (e.g. GENERIC 16:9, 1920x1080 HD1080, 1600x1200 UXGA, etc.). Using a fixed EDID setting can significantly speed up video switching times as EDIDs do not need to be checked, however, all of the installed monitors need to support the chosen resolution. *Note: Care must be taken when selecting a Dual Link Video resolution (e.g. 2560x1600) as certain ALIF units do not support Dual Link Video resolutions. In the case of a Dual Link EDID being set in the Global settings, no EDID will be set on Video port 2 of dual port ALIF transmitters.*
- USE CONNECTED MONITOR'S EDID - Check and use the EDID from the connected display screen at the point of switching. The process of checking EDIDs can cause minor delays while details are collected; enabling *EDID Optimisation* (discussed below) can help to regain some of the switching speed. This setting is shared between the video and digital audio port services on the same EDID port.
- USE SAVED MONITOR'S EDID - The EDID from the first RX to connect since the TX was last rebooted will be stored in flash memory and used for that video port. A reboot of the TX immediately restores and uses that EDID on the port without any RX needing to connect (as per using a fixed EDID mentioned above). This setting is shared between the video and digital audio port services on the same EDID port, but is separate from other EDID ports (ie the two video ports on a dual TX are handled separately). *Note: If this option is not supported by an endpoint or firmware does not support the feature it will default to using the monitor's EDID instead of a saved one.*

Maximum VDI Resolution

This option provides the option to cap the resolution used for VDI connections to improve performance when high resolution monitor settings are used.

Dynamic Range EDID

For ALIF devices which support HDR (such as the ALIF4021T), this option can be used to grant permission to go beyond the standard SDR8 setting and use SDR10 or HDR10 when the connected host and video displays support 30bpp (10bpc) color depths.

Display Quality & Compression

Maximum Bits Per Pixel

This option controls the dynamic range mode. When set to 24bpp(8bpc), only SDR8 mode will be supported. When set to 30bpp(10bpc), the transmitter will allow SDR10 or HDR10 mode providing the host computer and attached video displays support those modes. See the user guide for ALIF devices that support 30bpp for a more detailed explanation.

Compression Level

The newer AFZ+ codec complements the existing AFZ codec by providing greater compression for increased speed where pixel perfect results are not the primary focus. The transmitter video configuration page allows you to choose the required compression mode. Choices are:

- 'Pixel Perfect' - only uses pixel perfect AFZ,
- 'Adaptive' - guarantees frame rate, builds to pixel perfect,
- 'Smoothest Video' - forces the maximum compression, or
- 'Advanced' - allows you to choose the minimum and maximum compression modes:
  - 1 = 'AFZ only (pixel perfect),
  - 2 = 'AFZ+ Minimum compression',
  - 3 = 'AFZ+ Middle compression', or
  - 4 = 'AFZ+ Maximum compression'.

Magic Eye Settings

Magic Eye

Determines whether the Magic Eye feature should be enabled on ALIF transmitters. Magic Eye works to overcome the issues with increased bandwidth usage caused by 'dithering' techniques used on some computers, such as Apple® Macs. See the ALIF dual user guide for more details.

Magic Eye SDR10 Level

Applies only to ALIF4000T units and is only active if the Magic Eye option is set to On. The default level of 1 is suitable for most sources. For Apple Macs with M-CPUs, level 4 may give the best results when using SDR10. In other cases, if SDR10 has no dithering but other color bit depths do, use level 0.

Transmitter *(continued)*

Audio EDID Settings

Audio EDID Optimization

When this option is ticked, the transmitters will compare the digital audio settings when switching. If a receiver's digital audio settings are the same as the previous one, the new EDID is not sent to the host system. This speeds up switching as the host system does not need to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver uses a different audio setting, then the EDID will be updated to allow for a change in audio mode.

Audio EDID

For transmitters which support digital audio via the DisplayPort™ connection(s), this setting determines how the audio should be configured: (USE CONNECTED MONITOR'S EDID, USE SAVED MONITOR'S EDID- see left for details) or a static setting: NONE, 2 CHANNEL *(Stereo)*, 6 CHANNEL *(surround 5.1)* or 8 CHANNEL *(surround 7.1)*. Using a fixed EDID setting can significantly speed up switching times as EDIDs do not need to be checked, however, all of the installed audio devices need to support the chosen format. Where EDIDs are checked, enabling Audio EDID Optimization (below) can help to regain some of the switching speed.

Audio EDID Settings

Enable Audio

This option controls the standard analog audio feed, available via the 3.5mm audio jacks.

Enable Digital Audio

This option controls the (multi-channel) digital audio feed available via the HDMI connection as supported by numerous ALIF devices.

USB Behaviour & Limits

Enable Dummy Boot Keyboard

It is often necessary to have a keyboard reported at start up. This setting means that a "Virtual Keyboard" is always reported to the USB host. It may be necessary to disable this for use with some KVM switches.

Reserved USB ports

This setting lets you set aside a specific number of USB ports (up to 8) on the transmitter that can be made available for certain USB devices which require a quirk setting under advanced USB features, connected to a receiver.

Note: This setting can only be applied globally; it is not found with individual transmitter configurations because all receivers need to know how many USB ports are available for the advanced USB features.

USB Speed

Determines standard USB operation: USB1 Full speed or USB 2 Hi-speed.

USB Hub Size

Select either a 13 or 7 port USB hub. This determines the number of USB devices that can be connected to a single Transmitter.

Note: In order to access the BIOS on some host machines it is necessary to change this setting to 7 ports.

Hot Plug & Background Settings

Hot Plug Detect Control

Determines whether to enable hot plug detection for monitors. By default this is enabled.

Hot Plug Detect Signal Period

By default this is set at 100ms, which is sufficient for most graphics cards. Occasionally it may be necessary to adjust this. An Adder FAE will advise if necessary.

Background Refresh

The number of frames between sending an entire frame of video data. Setting this to a longer period or disabling this will reduce the bandwidth required.

Serial Port Settings

These allow you to match the serial configuration being used by the attached PC host.

Receiver

User & Hotkey Settings

Show Multi-User Information
When set to Yes, the names of other users who are currently viewing the same channel will be displayed within the OSD.

Enable OSD Hotkeys
Determines whether the hotkeys that invoke the OSD are enabled or disabled. *Note: For this option only, either or both of the Windows keys can be chosen for use as part of the hotkey sequence.*

Enable Connection Hotkeys
Determines whether the hotkeys that switch channels are enabled or disabled. This affects all of the hotkey settings below.

Disconnect Hotkeys
Determines the hotkey combination used to end the current connection.

Shortcut and Extended Hotkeys
Shortcut hotkeys allow quick connection to channels 0 to 9. Extended hotkeys also allow quick connection to those same channels, but then offer a further set of connections from channels 10 to 99. It is important to set a different combination of **Extended Hotkeys** to those configured for the **Shortcut Hotkeys** setting.

Note: For all types of hotkeys, Left Ctrl and Left Alt are the default settings. It is not possible to use a mixture of left and right Ctrl/Alt/Shift keys for any given function.

Other Hotkey Settings
The next six settings determine the Hotkeys that can be used to invoke certain functions, such as last-used channel selection, connection mode and feedthrough selection.

For all of these hotkey settings it is possible to choose mouse buttons to perform the functions, however, it is not possible to use a mixture of mouse buttons and keyboard keys in combination; it must all one or the other type.

OSD Display Options

OSD Display Options
Determines which information should be shown within the OSD for the receiver. Options are Show Description, Show Location or Show Both Description & Location.

OSD Banner Position
Determines the screen location of the OSD banner (when enabled in the above setting), which will state the currently viewed channel name.

OSD Launch Icon Size
Determines the default size of the icons used in the OSD. Options include: Small, Medium, Large and Extra Large.

OSD Channel & Alerts

Receiver OSD Alerts
Determines whether pop up OSD alerts should be displayed for users.

Touch show OSD enable
Determines whether the OSD can be shown on a touchscreen device when supported by certain ALIF devices - at present supported by ALIF1102R, ALIF2100R and ALIF4000R receivers.

Show Current Channel
When enabled, displays the channel name on the OSD banner (in the position determined in the setting below).

Login Messages & Timing

OSD Login Message
Text entered in this box will be displayed as a message to all users who access the OSD login page.

OSD Auto Logout Time
Determines the period of USB port inactivity before the device will issue a logout request to AIM. Default value of 0 means never log out.

OSD Touchscreen Monitor Mapping

Allows you to map the USB connection from each touchscreen monitor to the physical USB ports on the receiver - at present supported by ALIF2100R & ALIF4000R receivers.

Monitor Settings

Video Freeze Image on Loss
When enabled, this feature will hold the last frame on screen (with a warning indication) if the communications to the TX or video to the TX are lost - at present supported by ALIF21xx- and 4xxx- series receivers with v7 firmware or later.

Force 60Hz
If enabled, the receiver frame rate is held at 60Hz regardless of the video input frame rate. The Video Switching options (below) cannot be altered when this option is enabled.

Video Switching
Provides two options for video switching:

- *Fast Switching* (default state) - Retains the same frame rate (at either 50Hz or 60Hz) depending upon which video resolution was displayed first.
- *Match Frame Rate* - Follows the source frame rate and will change the frame rate every time this changes even if the video resolution doesn't change. If you have one receiver switching between 1920x1080@**60**Hz and 1920x1080@**50**Hz then this setting will change the frame rate from 60Hz to 50Hz every time that you switch.

Receiver *(continued)*

Compatibility Check

Video Compatibility Check

When enabled, this option reads the EDID from the attached monitor and determines whether it is capable of displaying the selected video mode before connecting a channel. This prevents the receiver showing a black screen and the user being locked out because a dual link resolution has been selected to display on a single link monitor.

Audio Compatibility Check

Applicable only to receivers (such as the ALIF4000 series) which are capable of processing multichannel digital audio via their DisplayPort™ connections. When enabled, this option reads the EDID from the attached monitor/audio system and determines whether the receiver's current audio setting (e.g. 2 Channel, 6 Channel, 8 Channel) is capable of correctly playing the selected audio (e.g. Stereo, 5.1 or 7.1) mode before connecting a channel.

Authentication Settings

Login Required

Determines whether it is necessary to log into the receiver.

Auto Login User

Allows you to authorize a user (or group) account to use the optional Auto Login feature. This option will be grayed out if the Auto Login feature has not been installed. See "Appendix I - Auto Login Feature" on page 94 for more details.

Enable OSD In Auto Login

When enabled, a user will be permitted to open the OSD following an auto login.

Localization & Input

Keyboard Country

Select the country code of the keyboard connected to the receiver.

Audio Input

Select the required audio input type: Mic or Mic Boost.

USB Settings

HID Only

This option allows you restrict USB devices to allow only HID (mice, keyboards, tablets, touchscreens, etc.) devices to be connected to the receiver(s).

Disable Mass Storage

This option allows you to prevent the use of USB mass storage devices at the receiver(s).

The *HID Only* and *Disable Mass Storage* options both affect how USB devices are supported at the receiver(s). Their use in combination can produce the following results:

HID Only	Disable Mass Storage	Outcome
No	No	No USB restrictions
Yes	No	Allow only HID devices (Mass storage devices are also blocked)
No	Yes	Exclude mass storage devices but allow other USB peripherals (e.g. mice, keyboards, tablets and touchscreens)
Yes	Yes	Allow only HID devices (Mass storage devices are blocked)

Disable Isochronous Endpoint OSD Alerts

When an isochronous USB device is connected to the receiver there will no longer be a warning message. ALIF units do not support isochronous devices.

Enable Isochronous Endpoint Attach

Some USB devices combine many USB devices behind a USB hub. e.g. a keyboard with audio support. By enabling this option, devices will be allowed to connect to ALIF receivers, however, the isochronous part (e.g. the audio component) of the devices will not work.

Advanced Port Features

This section allows you to determine USB port behavior for use with certain USB devices.

The default is no reserved ports, Merging enabled and no feature code (or Quirk) set. It is recommended that these are left at the default settings and are only changed under advice from an Adder FAE.

For each of the four USB ports on the receiver, certain rules can be applied depending upon the USB device connected.

If you have reserved USB ports on the transmitter, you can select which USB port to use for a particular device.

You can turn off USB merging for a particular port. This will slow down switching as the USB device will be enumerated every time that you switch.

You can also enter an advanced feature if it is necessary for your USB device. The drop down lists the feature codes for some known USB devices. Otherwise please contact your local FAE for advice.

Receiver *(continued)*

Connection Notification Settings

This section allows you to determine the default settings for notifications for all receivers and receiver groups. The defaults configured here can be separately overridden for any receiver or receiver group.

The notification settings are grouped as follows:

- Border Settings - these options are related to the coloured border that can be shown around the perimeter of the screen to emphasise messages when they are displayed.
- Message Settings - these options are concerned with the appearance and positioning of the message popup windows.
- Notification Types - these four options determine whether or not messages (and accompanying coloured borders) should be displayed to warn of losses of the main signal types: Video, audio, USB and Serial.
- Notification Labels - these four text fields determine the labels displayed on messages concerning the loss of video, audio, USB and serial signals.
- Notification Messages - the entries in this section allow you to edit the text strings that form the basis of all notification messages.

Settings

AIM Connectivity

Subnet Operation
Indicates the current DHCP server arrangement: either an external DHCP server is enabled (Subnet Operation ON) or an internal DHCP server in use (Subnet Operation OFF).

Host Name
Enter a hostname for the installation. This field must be populated.

DNS Domain Name
Enter a suitable domain name for the installation. This field must be populated.

Gateway IP Address
Defines the IP address of an optional gateway device.

Note: Only a single gateway can be specified within an AIM server. If both Ethernet ports are to be used in multi-subnet mode, it is important to specify a single gateway IP address that suits both Ethernet ports. Communications between AIM and the ALIF endpoints on the different subnets will be affected if using multi-subnet mode without a jointly valid gateway.

Require SSL for Web
If set to yes, a valid certificate will need to be downloaded and all connections will then take place using HTTPS:// connections rather than the default HTTP:// connection types - "Appendix H - Configuring SSL on an AIM server" on page 93.

Classless Static Routing
This option allows you to define one or more static routing paths to other subnets. A sub-page will be opened when you click this option. Within the sub-page, click the Add New option to include a new entry. For each entry you need to define the Destination and Router IP addresses plus a suitable classless subnet Mask.

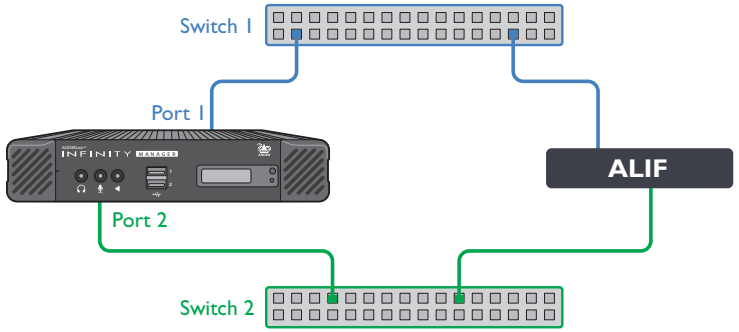
Ethernet Port 1
The primary AIM server Ethernet port can only be configured using a static IP address. Use the three options provided to configure the IP address, netmask and DNS server address.

Ethernet Port 2
The Backup AIM server Ethernet port can be configured to either: gain its details via a *DHCP* server; use a *Static* IP address, netmask and DNS server address, or alternatively be set to *Bonded* operation, whereupon three further *Bonding Mode* options are displayed:

- **Active-Backup** - This can be used when both of the AIM server's network connections are linked to the same network switch. This option provides a failover to cater for the possibility of hardware failure or connectivity failure between the AIM server and the switch.

  In this mode, one of the AIM server's network ports will be active while the other remains dormant. If the active port experiences a failure, such as a loss of connection, its configuration is automatically transferred to the Backup port. Once the original primary port resumes connectivity, this will become the backup and be placed into a dormant mode.

- **Broadcast** - This option would be used when the twin ports of the AIM server and all attached ALIF devices are split between duplicate networks:



  The 'Separate Device Networks' option mentioned earlier would be enabled on the AIM server and the respective network connections on the endpoints are connected accordingly (e.g. copper to copper on only switch 1 and SFP to SFP only on switch 2).

  In Broadcast mode, both of the AIM server network connections mirror each other, i.e. duplicate network traffic is sent out on both connections. It is assumed that the connected devices will only listen to the network traffic intended for themselves and *drop/ignore* all other traffic intended for other devices. This mode is robust but inefficient because half of the packets are discarded.

- **802.3ad** - This mode uses a similar topology to *Active-Backup*, (i.e. both network ports connected to the same switch) but has two important differences: Both of the AIM server network ports are used simultaneously, and the network switch must support LACP *(Link Aggregation Control Protocol)*.

  The AIM server will 'merge' *(aggregate)* the two connections and treat them as one. The only exception to this would be on 'multi-subnet racks' where it would be possible to have each network connection on different switches.

  This mode provides the benefit of increased bandwidth availability between the AIM server and the network, but also provides a layer of redundancy. If one of the network connections is lost, the remaining connection would take over until the link is restored.

  The network traffic is not split on a packet by packet basis between the connections; it operates on a connection basis. When a connection is established between the AIM server and one of the ALIF endpoints, this would travel via one port. When a second connection to another endpoint is established, this could use the same port or it may use the other. There is no order to which network port is used for any connection.

Note: When changing between bonded and any other mode, a warning message will be displayed and, when the Save button is clicked, will cause the AIM server to be rebooted.

Disable Event Log for bonding Broadcast - This option is displayed when broadcast bonding mode is enabled. If set to Yes, unnecessary error messages that report very brief breaks in connection will be suppressed.

Settings *(continued)*

Device Connectivity - IP Pool

IP Pool Lower/Upper Limits (not shown in multi-subnet mode)
When the AIM server is used in single subnet mode, these two fields are used to define the range (pool) of IP addresses that the AIM server can automatically assign to new ALIF endpoint devices. The AIM server contains its own DHCP server with which it applies the available IP addresses to ALIF endpoint devices.

When used in multi-subnet mode, the internal DHCP server with the AIM is disabled and instead the AIM server will rely upon an external DHCP server to provide valid IP address details.

Multicasting

Multicast IP Base
The start address for the multicast IP addresses to be used. Multicast IP addresses are in the range 237.1.1.1 to 239.255.255.255. This setting lets you adjust this range of IP Multicast addresses. It is important to allow sufficient addresses for your system. For instance, if the multicast IP address base was set to 239.255.255.252 there would only be 4 multicast addresses available.

Always Allow Multicast
This is a legacy setting that is ignored by current ALIF devices and should be set to *No*. This will instruct ALIF10xx, ALIF20xx and ALIF2112Ts, ALIF10xTs to unnecessarily use multicast for one-to-one connections as well as for one-to-many connections.

Use Global Multicast Addresses
Ordinarily, multicast addresses are set individually for each transmitter. However for installations with many transmitters (particularly dual video port models, which require six multicast addresses each), selecting this option allows you to configure just six multicast IP addresses to use globally across the whole installation. *Note: This option requires full support for IGMP v3, which allows source-specific joins.*

IGMP version
By default, force IGMPv2 is enabled. However, if your network supports IGMPv3 you can take advantage of the IGMPv3 features by applying the *Force v3* option.

Interfaces

Separate Device Networks
When this option is set to 'Yes', the ALIF devices within the network will be instructed to promote a further level of network resilience by treating their copper and fiber/teaming connections as independent links via separate switches (in conjunction with dual independent cabling schemes). See the diagram on the previous page. If one connection route is compromised, the other will continue unaffected. During normal operation, when both connection routes are operating, transfer speeds are boosted by the copper and fiber links working in parallel.

The two Ethernet ports of the AIM server can be connected to the two separate network switches to ensure that AIM control remains in place if one network switch should become unavailable.

Route of Last Resort
This option is appropriate when the AIM server is used in multi-subnet mode. In such cases, it is possible that the AIM server is not directly connected to the same subnetwork as some or all of the ALIF endpoints. Therefore, it will be necessary for the ALIF unit(s) to communicate back to the AIM server via a gateway device (see *Gateway IP Address* above). This option is used to indicate which interface has the gateway configured.

Device Network Port
This lets the admin specify which port on AIM to use for ALIF control. This is either the default Port 1 or either port if the AIM has ETH1 and ETH2 connected to the ALIF network.

Monitoring - Packet Loss Alerts

Packet loss monitoring is available if Statistics are enabled on one or more of the receivers being monitored (see System Care > Statistics). You will need to set up an Simple Network Management Protocol (SNMP) trap and/or declare a suitable email account (see System Care > Network Settings & Tools > Tools) to receive notification when packet loss drops below the chosen threshold/time frame:

Packet-Loss Alert Threshold
Determines when to issue a trap/alert based upon a threshold percentage of video packets that have been dropped at the receiver.

Packet-Loss Alert Window
Determines the sampling period (in seconds) in determining the packet-loss threshold (see above).

Settings *(continued)*

NTP

This page deals with all time related settings for the installation and allows up to three external NTP servers to be defined.

IMPORTANT: If two-factor authentication is to be used, the AIM system must be linked to a local NTP server to maintain accurate time. Failure to do so could cause unreliable 2FA operation and the possibility of being locked out.

NTP Enabled
Determines whether one or more external Network Time Protocol servers should be used to provide timing for the installation.

Server 1/2/3 Address
Enter the IP address of the NTP server(s).

Note: IP addresses must be used, domain names cannot be used.

NTP Key Number(s)/NTP Key(s)
If you wish to use Symmetric key authentication for the server, enter an appropriate NTP key number and key. If you need to add more NTP servers, click the Set option next to the NTP Server 2 or 3 entries.

Universal Timezone?
When set to Yes, AIM will use Coordinated Universal Time (UTC).

Time Zone Area and Time Zone Location
Use these entries to pinpoint the current location of the installation.

Tools

Syslog

Edit Settings:

Syslog IP Address and Port
The IP address and Port of the external syslog server. *Note: Ensure that this is not set to the AIM's IP address as AIM cannot log its own syslog messages.*

Syslog Filter
Determines the type of events that should be reported to the Syslog server.

Secure Syslog Enabled
When set to Yes the syslog entries will be encrypted using the x509/name authentication method. Use the *Certificate* option to upload valid server certificate files with .pem and .crt extensions.

SNMP

Edit Settings:

NMS Address
Enter a valid IP address for the Network Management System (SNMP server).

Username
Enter a valid Username for the Network Management System.

Allowed Connection Method
This option allows the AIM to connect to an external SNMP (Simple Network Management Protocol) server. If SNMP is enabled, there are three connection modes:

- Authentication + Privacy
- Authentication Only
- No Authentication or Privacy

There are two authentication types (SHA) or (MD5) and two Privacy types (AES) or (DES).

Note: SHA1 is supported at 192bits and AES at 128bits.

The MIB file can be downloaded from http://<IP>/AIM-MIB.txt

The response is split into three sections:

The first reports status of each individual endpoint:

deviceIndex,
deviceType, (ALIF type i.e ALIF2002R)
deviceFirmware, (firmware revision)
deviceName,
deviceIdentifier,
deviceIP1,
deviceMAC1,
deviceIP2,
deviceMAC2,
deviceSerialNum,
deviceStatus,
deviceLock,
deviceEth1Status,
deviceEth2Status,

The second part is returned from AIM:

numRx, (Number of RX units on system)
numTx, (number of Tx units on system)
numActiveConnexions,
serverCPULoad,
serverMemoryUsage,
serverSoftwareVersion,
serverDiskSpace,

The third part is the reporting of lost packets:

rxHead, (Which video head you are monitoring)
packetsSent,
packetsDropped

Tools *(continued)*

More Tools

This section provides useful network diagnostic tools.

IP Routes - Displays the main and default IP route list tables plus the address(es) of the current DNS server(s).

Network Trace - Use only under strict instruction from Support.

Ping - The Ping tool allows you to ping an IP address or domain name. Once chosen, enter the Hostname or IP address that you wish to ping and click the Start button. The result of the ping process will be displayed after a short delay.

Email Alerts

An external Email server is required to sit on the network if this functionality is to be used.

Enable E-Mail Alerts:

SMTP Domain name/IP
Enter the name or IP address of the external SMTP server that will be used to process all outgoing mail.

SMTP Port
Enter the appropriate port on the SMTP server.

Username, Password
Enter the appropriate username and password for access to the SMTP server.

From Address
Enter the email address that will be listed as the sender of alert messages.

Secure SMTP Enabled
When set to Yes, AIM will use Transport Layer Security (TLS) and Secure Sockets Layer (SSL) to encrypt all emails sent via SMTP.

Email Address for Alerts
Enter the email address to which alert messages should be sent.

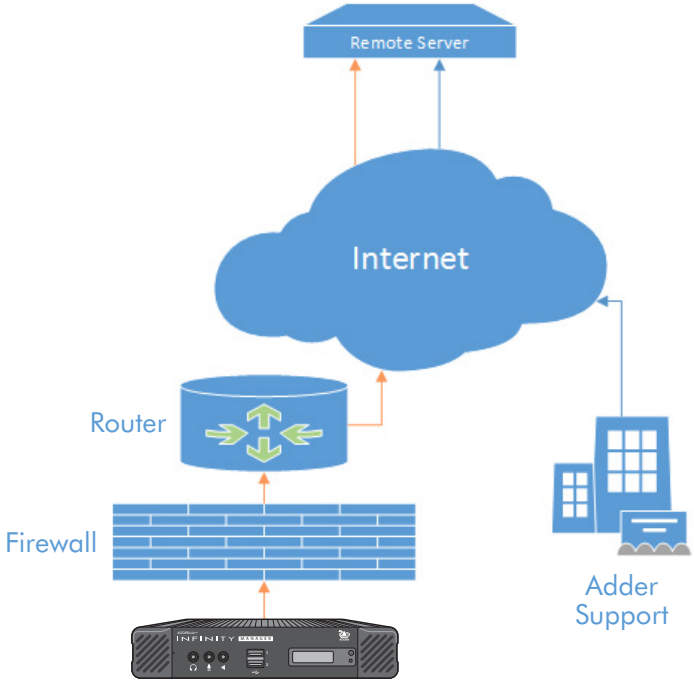
Suppress Similar Alerts
Allows you to optionally define a time period within which similar alerts to one already received will be suppressed.

Filter Alerts
These options allow you to choose which alert types should be reported.

Remote Support

The AIM manager has a remote support feature that allows technical support to connect should the need arise. It works by establishing a secure SSL connection with a managed secure server hosted on the internet. Using a reverse tunnel, technical support can connect to the manager via the secure server. Each support representative has unique SSL keys for full traceability when making a remote connection. To protect the manager against unauthorized access, Remote Support is disabled by default. Access is only granted by Enabling Support and giving the support representative a unique one-time password which is automatically generated each time it is enabled.

Below is a diagram that shows how the feature works:



Note: There have been different versions of this Remote Support feature where the behavior varies slightly. We recommend that you have the latest firmware installed.

Enable Remote Support

Click this button

- AIM must be connected to a network which has internet access.
- You will need to configure an IP address, gateway and DNS for the port being used.
- You will need to ensure that outbound port 22 is not blocked by the firewall or router to the internet. You can choose other ports such as 80, 443, 53, 2222, 10222.
- The AIM will show a port number and one-time password (OTP) which are required to remotely access the manager.
- If the port number changes after 1 minute, this means that either 1) The port is used by another Remote session or 2) The manager has been unable to access the remote server. If port number continues to change, please check your network and firewall settings.
- Please contact support@adder.com, stating the port number and one-time password that you have been given. If you have changed the admin password from the default, then please could you create a temporary administrator account so that we can access the web interface if required.

Web Interface Access

During the Remote Support session, we may need access to the AIM's web interface. So that you do not need to reveal or change your Admin password, create a temporary user and set it as an AIM Administrator. Please let us know the user and password that you have created.

Troubleshooting

In the event that you do not see a port number, check the following:

- You have outbound port enabled on your firewall, typically 22, 443, 53, 2222 or 10222.
- There is only one gateway on the AIM Manager; ensure that the gateway is correct. If you set the Ethernet port 2 to DHCP, the gateway from the DHCP server is not used.
- Try manually assigning an IP address, subnet mask, gateway and DNS Setting to the port being used.

Test Connection

Use this button to check that a remote support server can be reached from your network. After a short delay a list of accessible ports will be displayed.

Backup

You can schedule backup copies of the AIM database (containing all devices, users, channels and logs) to be made on a recurring basis and you can also perform backups on demand, as required.

IMPORTANT: You are strongly recommended to arrange regular scheduled backups of your AIM database. Adder cannot be held responsible for any loss of data, however caused. For further details, please see "Appendix D - Making an AIM Manager Backup" on page 85.

Backup Now

A backup file will be saved to the server and then will be presented as a download in your browser, so that you may save a local copy of the backup file.

Email Backup To: If this option is checked, a copy of the backup file will be sent to the email address specified in the "Email Backup To" field. The backup file will be emailed either when you click "Backup Now" and/or according to the option selected in the Schedule section.

Note: Use of the Email backup option requires a valid email address to be stored within the System Care > Network Settings & Tools > Tools page - see page 68.

Note: Emailed backups are encrypted, and these backup files are automatically decrypted by the AIM server when they are used.

Schedule: Determines how often a backup should be created. There are set periods for the various options:

- Hourly backups are executed on the hour (or quarter past).
- Daily backups are executed at 2 a.m. (or quarter past).
- Weekly backups are executed every Sunday at 3 a.m. (or quarter past).

Backups on the Server

All backups (whether initiated manually or by schedule) are saved on the server together with a timestamp of when the backup was run. If required, you can select a previous backup and restore its contents. Alternatively, you can download the backup file to another location.

IMPORTANT: It is advisable to make a backup of the current state of the AIM system before restoring a previous backup. Restoring the contents of a backup file will overwrite ALL data in the AIM system with the data within the backup file. This includes configured devices, channels, users, connection logs and action logs.

Upload Backups

Use this option to upload a backup file that you have previously downloaded or received by email. This will overwrite the contents of the current AIM system; therefore it is advisable to make a backup of the current state of the AIM system before restoring a previous backup.

Archive

Archive Log to CSV File

You can archive connection or log data to a CSV file and, at the same time, remove old log data from the database.

Click "Archive" to save a CSV file to the server.

Manage CSV Archive

You can download any CSV archive that was created in the archive step (described above) by selecting from the archives saved on the server.

The CSV archive can be opened in Microsoft Excel (or similar) to perform detailed analysis of actions and connections within the AIM system.

Download Debug File

The purpose of the "Download Debug File" is to prove support with a copy of the internal log files for diagnostics. The file is encrypted and can only be open by Adder.

Auto Delete Logs

This section allows you to select a suitable time period for auto deleting the debug logs. The choices are Daily, Weekly and Monthly. Optionally, logs can be auto archived to CSV files prior to deletion.

XML

Allows you to store user configuration snapshots at various periods in time and later compare the contents of any of those stored snapshots with the current AIM database user configuration.

Download Latest XML

A compressed XML file containing the configuration details will be created and stored.

Compare XML

Makes a comparison between a stored snapshot and the current configuration.

For details about using these features, please see "Appendix G - AIM export user configuration" on page 91.

SYSTEM CARE > UPDATE

Update AIM Software

This option allows you to upgrade (or downgrade, if required) the AIM server firmware while preserving all configuration data. Firmware files are encrypted and digitally-signed for AIM-server integrity.

Regenerate AIM Certificate

If a browser displays the message: *Not Secure with SSL enabled*, use this option to regenerate all the certificates required for authentication.

Reset AIM Configuration

This option can be used to reset AIM to its initial configuration or a previous upgrade. When the AIM server is reset, all devices, channels, presets, users, groups and logs will be removed. *Note: You are recommended to take a backup onto an external device before starting the upgrade process.*

If one or more previous upgrades have been installed on this system, you will be given the option to choose either the original factory image or the last upgrade image. They will be listed by version number - click the appropriate radio button to select.

Two other options are available within this section:

- *Also reset the server IP address* - When ticked, the IP address will be reset to the default: **169.254.1.3** and you will be reminded to manually navigate to that address.
- *Also delete security certificates and keys* - When ticked, all certificates and keys held within the server will be removed.

When the required options have been chosen, click the **Reset AIM Configuration** button to commence.

Restart Web Server

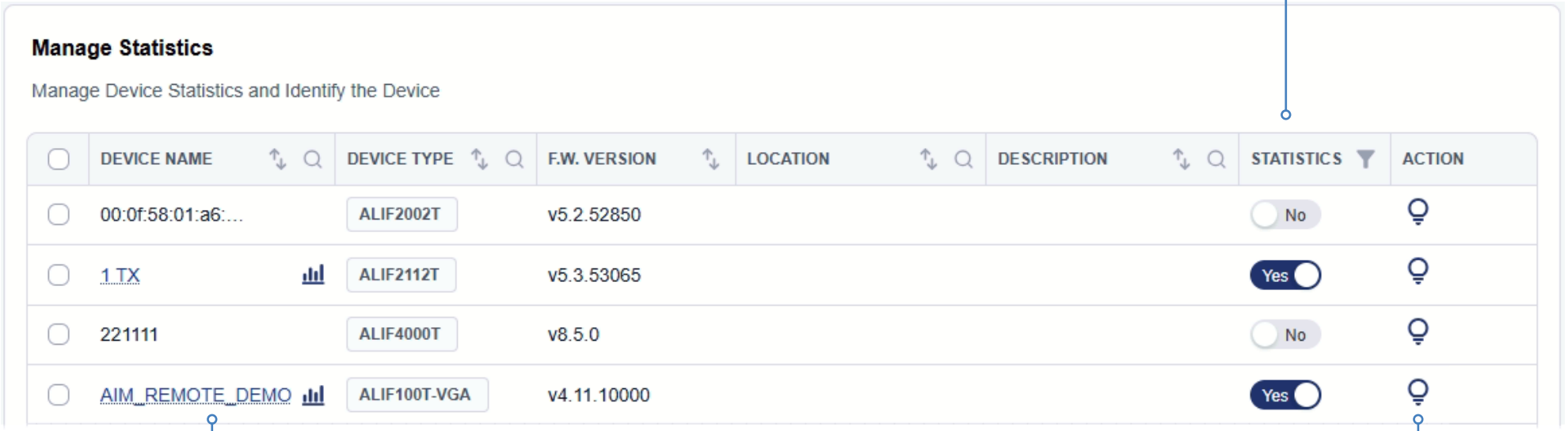
Occasionally, when changing certain key settings, such as the Locale, it may be necessary to restart the main web server underlying AIM. If functionality is lost after changing the Locale setting use this Restart button to restore correct operation.

SYSTEM CARE > STATISTICS

The Statistics page provides an opportunity to view a range of real-time data measurements related to any links within the AIM network. This is particularly useful for optimization and troubleshooting purposes.

The table view lists all of the devices registered within the AIM network. The search (🔍), filter (▼) and order (↑↓) options in the various column headers allow you to locate and focus upon any required entries.

Use this column to determine whether statistics are required for each device.



When the graph logo (📊) appears against an entry, then statistics are available. Click the link in the Device Name column to view the statistics feed in a new browser window.

Click the bulb icon to flash the LED lights on the front panel of the device. A message will be displayed if the device cannot be located (ie, if it is offline).

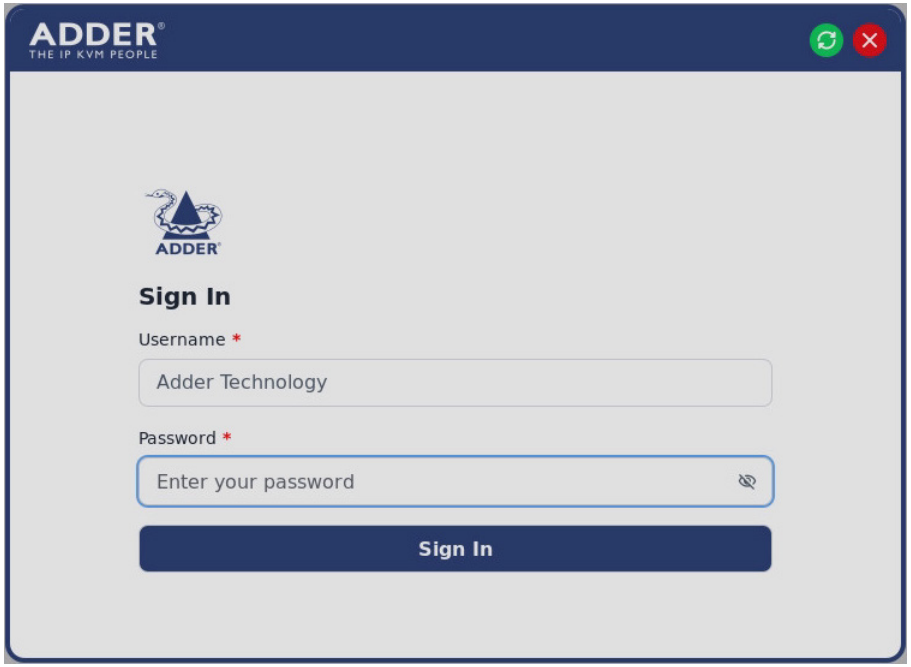
Operation

For non-admin users, the On-Screen Display provides a clear way to choose and access multiple channels.

LOGGING IN

1 On the keyboard connected to your ADDERLink INFINITY receiver, press the hotkey combination **Ctrl-Alt-C** to display the On-Screen Display or OSD (this hotkey combination can be altered on the System Care > Global Configuration > Receiver page - see page 62).

You will either see the list of channels for which you have permission or be presented with the following login:



2 Enter your Username and Password and click the Sign In button to display the Local OSD screen.

Once logged in, you will remain logged in until either you click the Logout link in the top right of the OSD; or there is no activity for two days or until the ADDERLink INFINITY unit is rebooted.

Hotkey shortcuts

The following can be used with the Local OSD (& Remote OSD). These defaults can be altered within the System Care > Global Configuration > Receiver page - see page 62.

Left Ctrl + Left Alt + **C**:	Launch the OSD
Left Ctrl + Left Alt + **X**:	Disconnect the current receiver
Left Ctrl + Left Alt + **3**:	Connect to the channel/preset saved in shortcut slot 3
Left Ctrl + Left Alt + **A**:	Re-connect to the last channel
Left Ctrl + Left Alt + **L**:	Switch between a locally linked TX and your regular channel
Left Ctrl + Left Alt + **V**:	Change the current connection to the video-only mode
Left Ctrl + Left Alt + **S**:	Change the current connection to the shared mode
Left Ctrl + Left Alt + **E**:	Change the current connection to the exclusive mode
Left Ctrl + Left Alt + **P**:	Change the current connection to the private mode

Creating/using favorites and shortcuts

When the OSD contains many possible channels and presets, it can be useful to mark the most commonly visited ones as favorites. For those channels that you'd like to access by keyboard shortcut, there are also ten assignable hotkeys.

To create a new favorite

- Click the ☆ icon next to the required channel or preset.

To display favorites

- Click the star in the header on the left side to change between show only favorites and show all channels and presets.

To create a new hotkey shortcut

1 On the left side of the channels or presets you will see a column labeled 'HOTKEY'. In that column, click the **+** icon for the channel or preset entry to which you wish to apply a hotkey shortcut. The OSD will list the first hotkey slots numbered 0 to 7. Any available slots will be listed as ASSIGN HOTKEY. Click anywhere on an available slot to begin applying a hotkey*.

2 In the resulting page, the hotkey designations will be shown together with the available connection mode(s) - (*Video-Only*, *Shared*, *Exclusive* or *Private*). Click the tickbox of the required connection mode.

3 Click the Save button.

You will now be able to access the chosen channel by using the hotkeys (Left Ctrl + Left Alt, as standard) plus the number of the chosen slot.

* *Notes:*

- *To remove a previous channel from a slot, click the ✕ icon on the right side of the slot.*
- *Optionally click a number listed along the foot of the page to access further hotkey slots.*

THE LOCAL OSD SCREEN

Once logged in, the list of channels for which you have permission are shown in the Local OSD (blue) screen.

- To choose a channel/preset, click on one of the connection icons ( ) shown to the right of the required channel/preset name (see the *Connection buttons* box below right).
- Where many channels/presets are listed, use the Channel Name and Description search boxes and list arrows to filter the choices.
- To use the Remote OSD feature, click the Remote OSD icon in the top border.

Favorites & hotkey icons

☆ Click to add this channel/ preset as a favorite

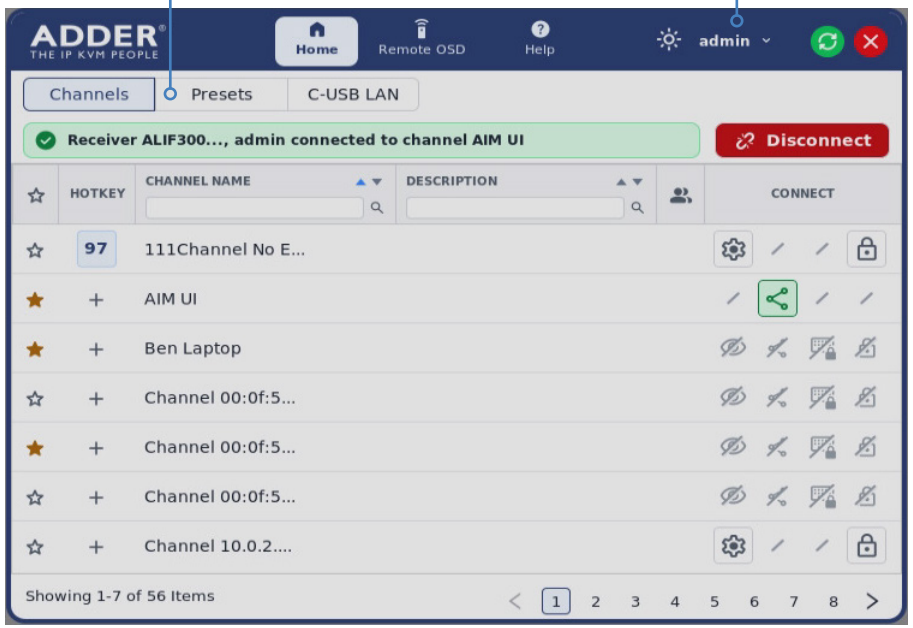
★ Marked as a favorite

97 Numbered shortcut - use CTRL-ALT-97 to call up this channel/preset

Change between viewing Channels, Presets & C-USB LAN devices here. DVI-equipped ALIF receivers operate differently - see page 78

Click to use the Remote OSD - see page 77

Click to Logout



Top corner icons

Refresh the current page

Close the OSD

Mouse-over feature

Hover your mouse over any channel/preset name to see the text in full.

Connection buttons

There are five connection options:

Video-Only: Allows users only to view the video output, the USB channel is denied.

Shared: Allows users to control a system in conjunction with other users.

Exclusive: Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.

Private: Allows a user to gain private access to a system, while locking out all others.

VM credentials: Displays a login screen to allow users to enter their username and password for access to the corresponding virtual machine. See next page.

Connection buttons shown in **dark gray** are ready to select. Icons in **green** are in operation and those shown crossed out in **light gray** are not available.

Click the red **Disconnect** button in the top right corner to end a connection.

Listing C-USB LAN transmitters

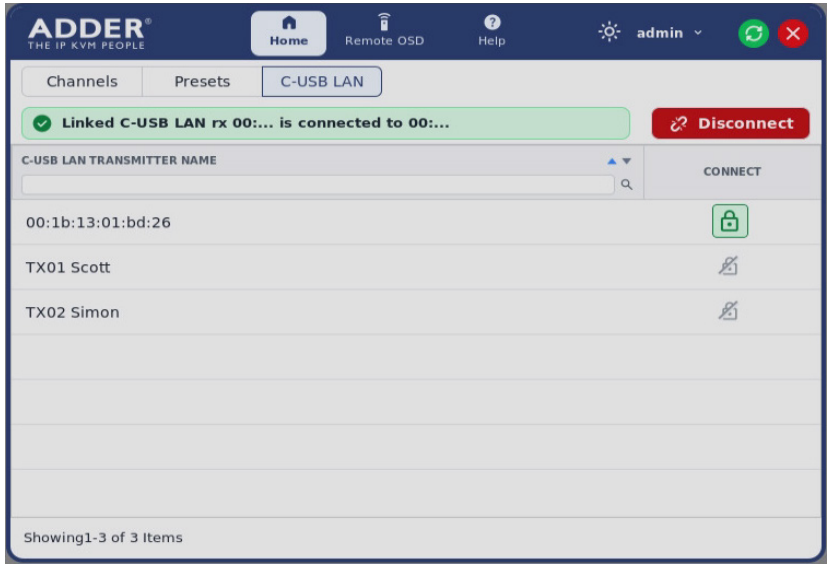
In addition to listing channels and presets, the OSD screen can also list the C-USB LAN transmitters that are associated with the current receiver.

To list all associated C-USB LAN transmitters

1 Login to the OSD from the appropriate ALIF receiver and display the OSD: CTRL + ALT + C

2 In the top left corner of the OSD screen, click the C-USB LAN button.

The list of devices will be displayed:



C-USB LAN transmitters can only be accessed in Private mode, so the icon is shown in green when it has been connected: .

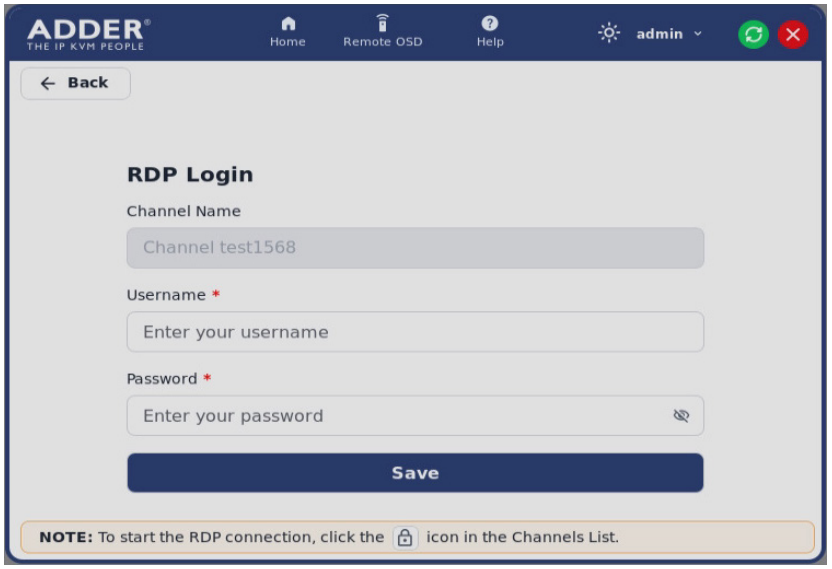
Accessing virtual machines

Before you can access a virtual machine you need to first enter your login credentials.

To enter your credentials

1 Login to the OSD from the appropriate ALIF receiver and display the OSD: CTRL + ALT + C

2 In the list of channels, to the right of the required virtual machine entry, click the icon to display the login page:



3 Enter your Username and Password *(depending on the type of virtual machine being accessed, other credentials may be requested)* and click the SAVE button.

You will be returned to the main OSD page. The icon will now be green to show that your details are stored.

To access a virtual machine

1 Login to the OSD from the appropriate ALIF receiver and display the OSD: CTRL + ALT + C

2 In the list of channels, to the right of the required virtual machine entry, click the icon to display the video feed from the chosen system. Virtual machine links can only accessed as private connections.

To clear your credentials

1 Login to the OSD from the appropriate ALIF receiver and display the OSD: CTRL + ALT + C

2 In the list of channels, to the right of the required virtual machine entry, click the icon to display the login credentials page.

3 Click the Clear Credentials button in the top right corner. You will be returned to the main OSD page. The icon will now be dark gray to show that no details are stored.

Using the Remote OSD feature

The Remote OSD feature allows authorized users to access and take control of ALIF receivers other than the one to which they are connected. Once linked in, users can then determine which channels the remote receivers should link with.

Remote OSD requires that a user must have been given specific authorization to access one or more remote receivers.

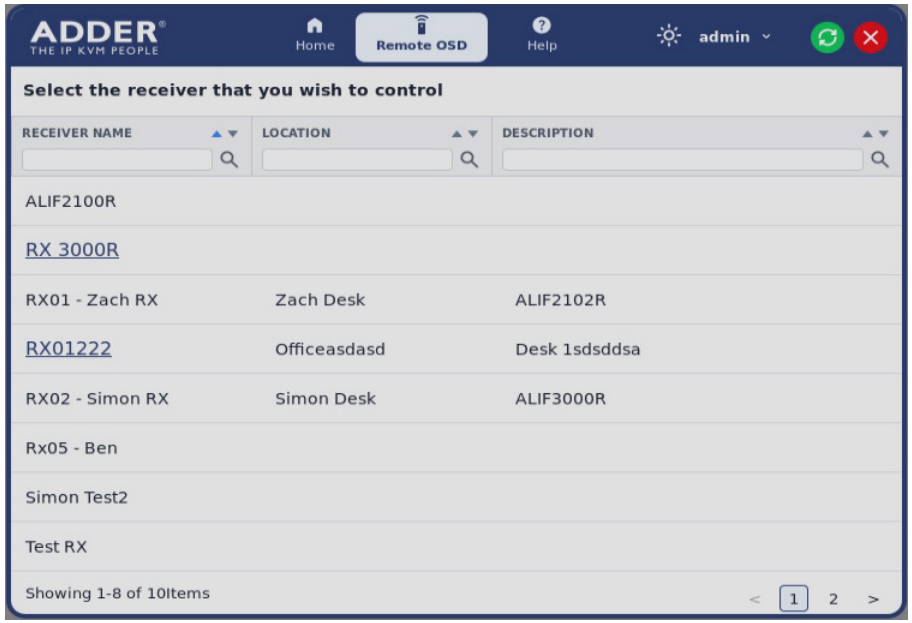
To access the Remote OSD

1 On the keyboard connected to your ALIF receiver, press the hotkey combination **Ctrl-Alt-C** to display the Local OSD login screen.

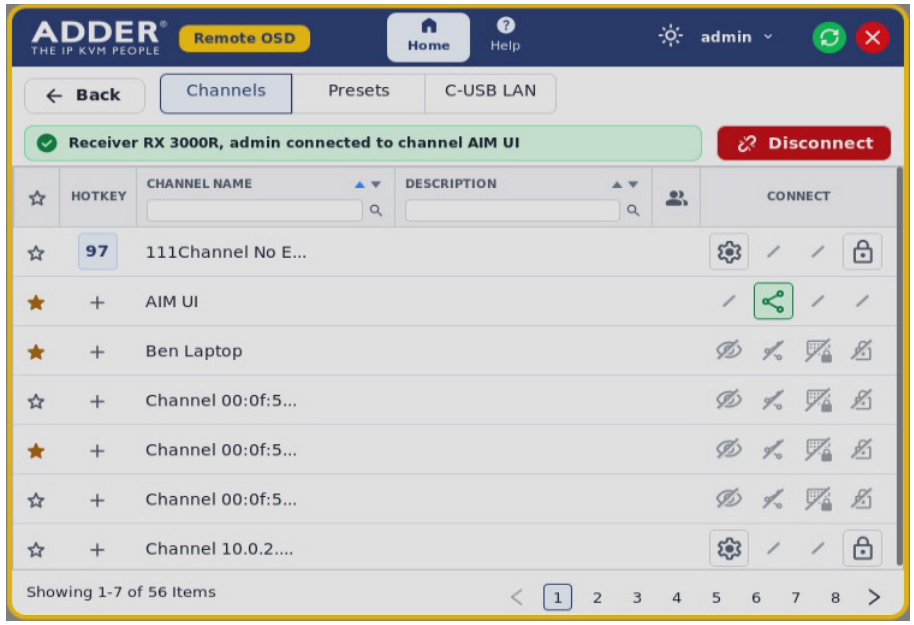
2 If required, enter your Username and Password and click the Login button.

3 In the top border, click the Remote OSD icon.

4 The screen will list all of the receivers to which you have access rights. Click on the required receiver from the list:



5 The Remote OSD for the chosen ALIF receiver will be displayed. Remote OSDs always have a yellow border to differentiate them from the standard local OSD:



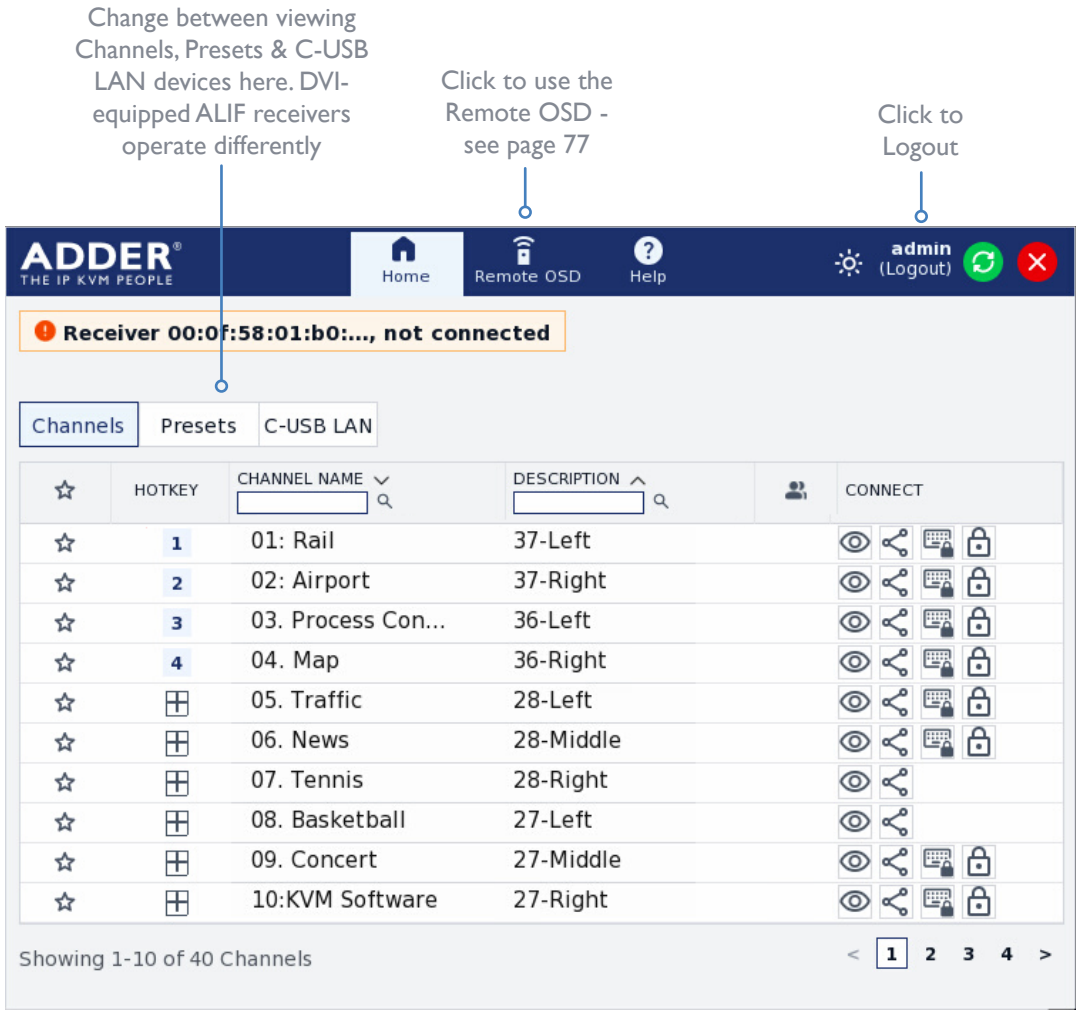
6 The behavior of the controls is generally the same as for the Local OSD screen with the following exceptions:

- To avoid confusion, you cannot login or logout while in Remote OSD mode. Click the Home icon to first return to the Local OSD.
- Hotkeys will only affect the current receiver to which you are connected, not the remotely-controlled receiver.

7 To exit from the Remote OSD, click the Home icon in the middle of the top border.

OSD view switching with DVI-equipped ALIF receivers

When viewing the OSD on the above listed DVI-equipped ALIF receivers (ALIF1002R, ALIF2000R and ALIF2020R), the page has a slightly different appearance to HDMI®/DisplayPort™-equipped devices although operation is very similar:



Favorites & hotkey icons

☆ Click to add this channel/preset as a favorite

★ Marked as a favorite

97 Numbered shortcut - use CTRL-ALT-97 to call up this channel/preset

Top corner icons

Refresh the current page

Close the OSD

Mouse-over feature

Hover your mouse over any channel/preset name to see the text in full.

Connection buttons

There are five connection options:

Video-Only: Allows users only to view the video output, the USB channel is denied.

Shared: Allows users to control a system in conjunction with other users.

Exclusive: Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.

Private: Allows a user to gain private access to a system, while locking out all others.

VM credentials: Displays a login screen to allow users to enter their username and password for access to the corresponding virtual machine.

Connection buttons shown in **dark gray** are ready to select. Icons in **green** are in operation and those shown crossed out in **light gray** are not available.

Click the red **Disconnect** button in the top right corner to end a connection.

Further information

This chapter contains a variety of information, including the following:

- Getting assistance - see right
- Appendix A - Tips for success when networking ALIF and AIM units
- Appendix B - Troubleshooting
- Appendix C - Redundant servers: Setting up and swapping out
- Appendix D - Making an AIM Manager Backup
- Appendix E - Restoring an AIM Manager Backup
- Appendix F - Two Factor Authentication (2FA)
- Appendix G - AIM export user configuration
- Appendix H - Configuring SSL on an AIM Server
- Appendix I - Auto Login Feature
- Appendix J - Upgrade license
- Appendix K - Glossary
- Appendix L - Copper/fiber modules and cables
- Appendix M - AIM API
- Appendix N - DHCP server requirements for ALIF support
- Appendix O - AIM database schema
- Appendix P - Technical specifications
- Appendix Q - Open source licenses

GETTING ASSISTANCE

If you are still experiencing problems after checking the information contained within this guide, then please refer to the Support section of our website:

www.adder.com

APPENDIX A - Tips for success when networking ALIF units

ALIF units use multiple strategies to minimize the amount of data that they send across networks. However, data overheads can be quite high, particularly when very high resolution video is being transferred, so it is important to take steps to maximize network efficiency and help minimize data output. The tips given in this section have been proven to produce very beneficial results.

Summary of steps

- Choose the right kind of switch.
- Create an efficient network layout.
- Configure the switches and devices correctly.

Choosing the right switch

Layer 2 switches are what bind all of the hosts together in the subnet. However, they are all not created equally, so choose carefully. In particular look for the following:

- Gigabit (1000Mbps) or faster Ethernet ports,
- Support for IGMP v2 (or v3) snooping,
- Support for Jumbo frames up to 9216-byte size,
- High bandwidth connections between switches, preferably Fibre Channel.
- Look for switches that perform their most onerous tasks (e.g. IGMP snooping) using multiple dedicated processors (ASICS).
- Ensure the maximum number of concurrent 'snoopable groups' the switch can handle meets or exceeds the number of ALIF transmitters that will be used to create multicast groups.
- Check the throughput of the switch: Full duplex, 1Gbps up- and down- stream speeds per port.
- Use the same switch make and model throughout a single subnet.
- You also need a Layer 3 switch. Ensure that it can operate efficiently as an IGMP Querier.

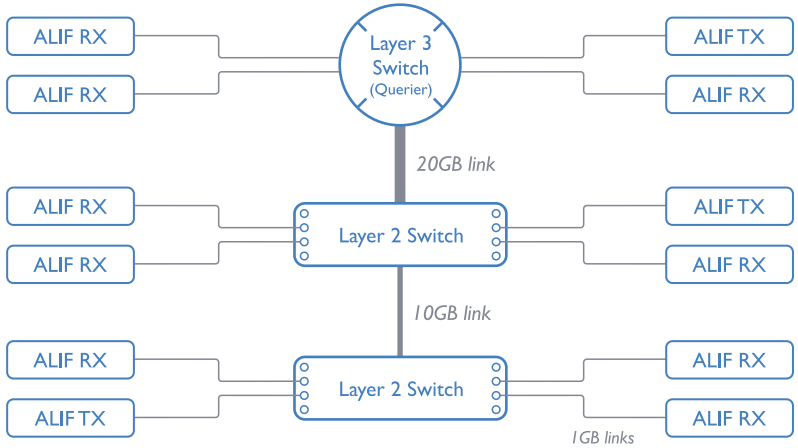
Creating an efficient network layout

Network layout is vital. The use of IGMP snooping also introduces certain constraints, so take heed:

- Keep it flat. Use a basic line-cascade structure rather than a pyramid or tree arrangement (see note below).
- Keep the distances between the switches as short as possible.
- Ensure sufficient bandwidth between switches to eliminate bottlenecks.
- Where the AIM server is used to administer multiple ALIF transceivers, ensure the AIM server and all ALIF units reside in the same subnet.
- Do not use VGA to DVI converters, instead replace VGA video cards in older systems with suitable DVI replacements. Converters cause ALIF TX units to massively increase data output.
- Stackable switches will allow you to create more ports at each cascade level.
- Wherever possible, create a private network.

The recommended layout

The layout shown below has been found to provide the most efficient network layout for rapid throughput when using IGMP snooping:



Note: From firmware version 3.0, tree and hierarchical structures of network switches are also supported. The Transmitter now joins its own multicast group so there is always a route from the querier to the transmitter which was previously missing in firmware versions 2.9 and below.

- Use no more than two cascade levels.
- Ensure high bandwidth between the two L2 switches and very high bandwidth between the top L2 and the L3, typically 10GB and 20GB, respectively for 48 port L2 switches.

continued

Configuring the switches and devices

The layout is vital but so too is the configuration:

- Enable IGMP Snooping on all L2 switches.
- Ensure that IGMP Fast-Leave is enabled on all switches with ALIF units connected directly to them.
- Enable the L3 switch as an IGMP Querier.
- Enable Spanning Tree Protocol (STP) on all switches and importantly also enable portfast (edge-port) only on all switch ports that have ALIF units connected.
- If any hosts will use any video resolutions using 2048 horizontal pixels (e.g. 2048 x 1152), ensure that Jumbo Frames are enabled on all switches.
- Choose an appropriate forwarding mode on all switches. Use Cut-through if available, otherwise Store and forward.
- Optimize the settings on the ALIF transmitters:
  - If moving video images are being shown frequently, then leave Frame Skipping at a low percentage and instead reduce the Peak bandwidth limiter and Colour Depth.
  - Where screens are quite static, try increasing the Background Refresh interval and/or increasing the Frame skipping percentage setting.

  Make changes to the ALIF transmitters one at a time, in small steps, and view typical video images so that you can attribute positive or negative results to the appropriate control.

APPENDIX B - Troubleshooting

Problem: AIM cannot locate working ALIF units.

There are a few possible causes:

- The ALIF units must be reset back to their zero config IP addresses for AIM discovery. If you have a working network of ALIFs without AIM and then add AIM to the network AIM will not discover the ALIFs until they are reset to the zero config IP addresses.
- This could be caused by Layer 2 Cisco switches that have Spanning Tree Protocol (STP) enabled but do not also have *portfast* enabled on the ports to which ALIF units are connected. Without portfast enabled, ALIF units will all be assigned the same zero config IP address at reboot and AIM will only acquire them one at a time on a random basis.

  You can easily tell whether portfast is enabled on a switch that is running STP: When you plug the link cable from a working ALIF unit into the switch port, check how long it takes for the port indicator to change from orange to green. If it takes roughly one second, portfast is on; if it takes roughly thirty seconds then portfast is disabled.

Remedies:

- Ensure that the ALIF units and the AIM server are located within the same subnet. AIM cannot cross subnet boundaries.
- Manually reset the ALIF units to their zero config IP addresses. Please refer to the ALIF user guide for details.
- Enable *portfast* on all switch ports that have ALIF units attached to them or try temporarily disabling STP on the switches while AIM is attempting to locate ALIF units.
- Change to ensure AIM and ALIFs can communicate with each other. If on different subnets, confirm that the gateway is correctly configured and there is routing between the subnets.
- Manually factory reset the ALIF endpoints so they can be seen by an AIM.

Problem: The mouse pointer of the ALIF receiver is slow or sluggish when moved across the screen.

This issue is often related to either using dithering on the video output of one or more transmitting computers or using VGA-to-DVI video converters.

Dithering is used to improve the perceived quality and color depth of images by diffusing or altering the color of pixels between video frames. This practice is commonly used on Apple® Mac computers using ATI or Nvidia graphics cards. VGA-to-DVI converters unwittingly produce a similar issue by creating high levels of pixel background noise.

ALIF units attempt to considerably reduce network traffic by transmitting only the pixels that change between successive video frames. When dithering is enabled and/or VGA-to-DVI converters are used, this can have the effect of changing almost every pixel between each frame, thus forcing the ALIF transmitter to send the whole of every frame, resulting in greatly increased network traffic and what's perceived as sluggish performance.

Remedies:

- **Linux® PCs** - Check the video settings on the PC. If the Dither video box option is enabled, disable it.
- **Apple® Mac with ATI® graphics** - Use the ALIF 2000 series unit with Magic Eye dither removal feature.
- **Windows® PCs** - If you suspect these issues with PCs, contact technical support for assistance.

Problem: The front panel OLED screen is blank.

AIM server 3 hardware running software version 4.13 will result in no details being shown on the OLED screen. Upgrade the software to gain the expected screen behavior.

APPENDIX C - Redundant servers: Setting up and swapping out

This appendix contains two main sections related to the creation and repair of AIM server installations that employ redundancy.

- Setting up AIM server redundancy - below
- Swapping out an AIM server - on next page

Setting up AIM server redundancy

This section details the steps required to successfully configure two AIM units as primary and backup servers.

1 Set the Role entry to **Primary** on the primary server.

2 Configure its Ethernet port 1 Address.

3 Ensure that password requirements is set to **NO**.

4 Add the new Backup AIM server to the network. The Backup server must have the same license as the primary and must also be running the same version of firmware as the Primary. It is not possible to have two servers with different licenses in a cluster. This unit must have its factory default settings in place. The new server will appear within the main Servers tab and be identified as being Unconfigured.

5 Wait five minutes for automatic server replication to take place and the backup database to be transferred from the primary unit. After this period, the new Backup server will be added to the list on the main Servers tab. Its Role will be shown as backup and its Status as standby.

6 The initial configuration of the Backup is done from the Primary. Click the ✎ icon to view the configuration.

Operation of Redundancy

If the Primary server fails for any reason (for example, loss of power or a network issue) then the Backup server will failover. This will happen automatically without any user intervention, however it is not instantaneous. The failover time required is the value entered in the primary timeout plus 30 seconds for the process to happen. The ADDERLink INFINITY extenders will start communication with the second IP address that is stored in their configuration and the redundant server will take control of the ADDERLink Infinities. When the redundant server is acting as the primary it is not possible to add any new devices or change the configuration. If this is required then the backup server can be promoted to be the primary.

When the primary server comes back online then it will resume its role as the primary. If however the backup server has been promoted to primary, when the primary server comes back its role will need to be factory reset back to the backup. After doing this the ADDERLink INFINITY endpoints will need to be rebooted. It is not possible to have two primary servers on the same network.

Both the primary and the backup server periodically synchronize their databases to ensure that they are identical. If for any reason the backup server is powered down then any changes to the system configuration will not be maintained by the backup server.

Swapping out an AIM server

When ALIF devices connect with an AIM Manager for the first time, they exchange SSL certificates that create a mutual trust. In this state ALIF devices will not be able to connect to a new or untrusted AIM Manager. Therefore, if an existing AIM server needs to be replaced within an installation, follow one of the basic procedures given here to smooth the transition.

For solo AIM servers (if the solo is still operating)

1 Before connecting the new AIM server to the main network, connect the new AIM server to a network switch that is isolated from the main network.
2 Use a computer connected to the same switch to login to the new AIM server management suite.
3 Set the Role entry from Solo to Primary.
4 Add in the new unconfigured server as a Backup.
5 Remove the original solo server from the network.
6 Promote the Backup to Primary. Then change its Role to Solo.
7 All the devices will appear as offline. Using a paperclip, perform a factory reset on all the ALIF endpoints so as they acquire the new certificate and keys. All ALIF units require a minimum of firmware version 3.3.

AIM installations with redundancy

The correct procedure depends on which AIM server has failed:

Primary server failure

1 Promote the Backup server to be the primary server.
2 Replace the faulty primary AIM server with a replacement unit that has the same license version and has its default factory settings in place.
3 The replacement server, which must have the same firmware version, will begin communicating with the primary server and download the database so that it can operate as the Backup server. This process may take ten minutes.

Backup server failure

1 Delete the failed server from the database.
2 Replace the failed backup server with a new unit that has the same license version and has its default factory settings in place.
3 The replacement server will begin communicating with the primary server and download the database so that it can operate as the backup server. This process may take ten minutes.

Starting from scratch

If none of the above procedures are used, then the following will be necessary. Each ALIF unit must be visited and reset, plus the AIM database will need to be fully reconfigured.

1 Place a new AIM server into the network and then perform a factory reset on every ALIF device. This will force the ALIF units back to their default states whereupon they will announce themselves to the new AIM server.
2 Use a computer connected to the same network to login to the new AIM server management suite and begin to recreate the database of devices and users.

APPENDIX D - Making an AIM Manager Backup

Overview

An AIM Manager Backup allows you to take a snapshot of the configuration, which can be restored at a later date if required. The database schema has been designed so that it can be restored to different firmware versions.

An AIM Manager Backup can be taken in different ways:

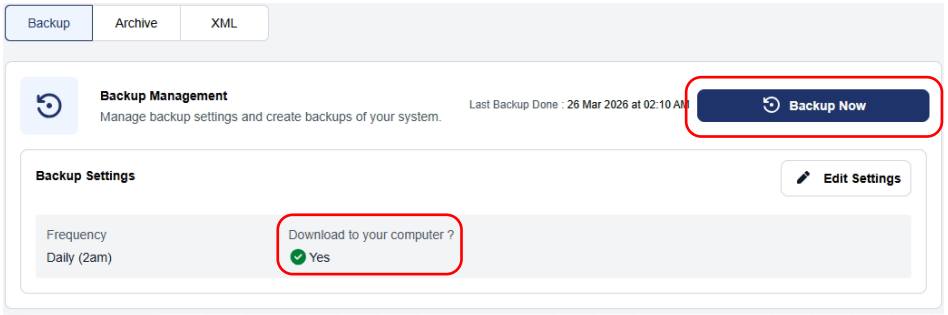
- Manual download to your computer using the Web interface.
- Automatic schedule, which is either:
  - Stored locally on the AIM, or
  - Sent via email (if configured).

Note: Backups do not contain the network settings and their contents can not be modified.

Manual Backup download to your computer

1 Open the AIM interface and navigate to **System Care > Backup**.

2 In the Backup Management section, make sure that **Download to your computer** is ticked. If not, click the **Edit Settings** button, tick the Download to your computer option and click the **Save Settings** button below to commit the change.



To download a local copy of the Backup file:

- Click the **Backup Now** button. After a second or two, you should receive the file via your web browser. The file name includes the AIM version, date and time of when it was taken. It also creates a local backup that is stored on the AIM itself.

Automatic Backups by schedule

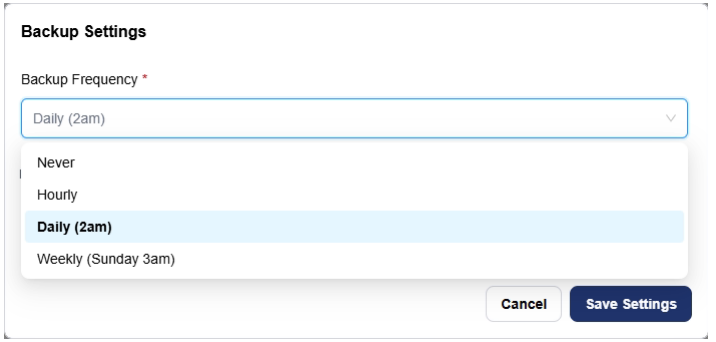
You can use the schedule feature to automatically store a backup locally on the AIM and, if configured, also send a copy to a specified email address.

For details about how to configure backup emails, please visit www.adder.com, choose the Support –> Knowledge Base option and search for 'ALIF: AIM Mail Setup Example'.

To schedule automatic backups

1 Open the AIM interface and navigate to System Care > Backup.

2 In the Backup Settings section, click the **Edit Settings** button and choose the required **Backup Frequency**: Hourly, Daily or Weekly:

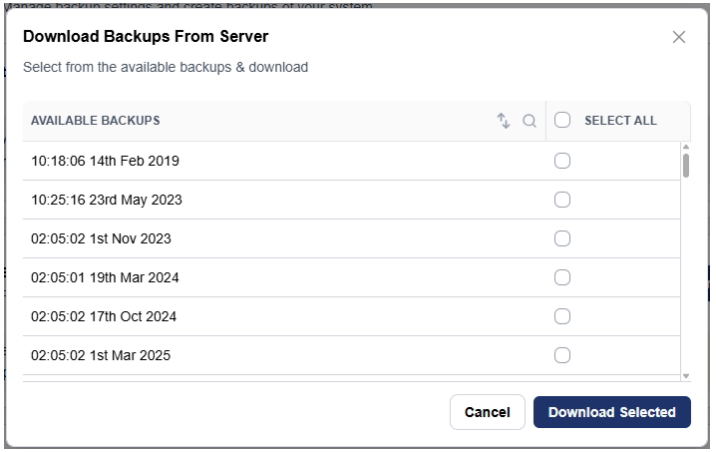


3 Click the **Save Settings** button.

Viewing stored backups

The number of backups stored is managed using an algorithm that ensures that the most recent and oldest backups are kept, but automatically deletes ones in between to save on disk space.

1 In the **Backups on the Server** section, click on the **Download** button to view the list of available backups:



2 To download any of the locally stored AIM Backups to your computer, tick the required entries from the list and click the **Download Selected** button.

APPENDIX E - Restoring an AIM Manager Backup

Warning

Restoring a Backup file will remove all the current data and replace it with the backup data. The network settings will remain unchanged.

Important

- When restoring to an AIM Manager that has a Backup or Satellite AIM attached, you must factory reset the Backup and/or Satellite AIMs after the restore completes for the database to be re-synchronized.
- A backup file does not contain any of the SSL/TLS security keys that are used by the AIM and endpoints to secure the communication between them. If you are restoring the Backup to a new AIM or to one where endpoints have been deleted, you will need to factory reset the endpoints after you have restored the backup to the AIM for them to be shown online. This is to allow the AIM and endpoints to establish new SSL/TLS keys.
- It is safe to restore a Backup taken from an AIM with an earlier version of firmware to a newer version on the second generation AIM Manager. However, if you are using the 1st generation AIM Manager and have a Backup taken from an AIM with 2.5 firmware or below, do not attempt to restore it to an AIM running 3.3 or above. If you need to do this, please seek assistance from Adder Support.

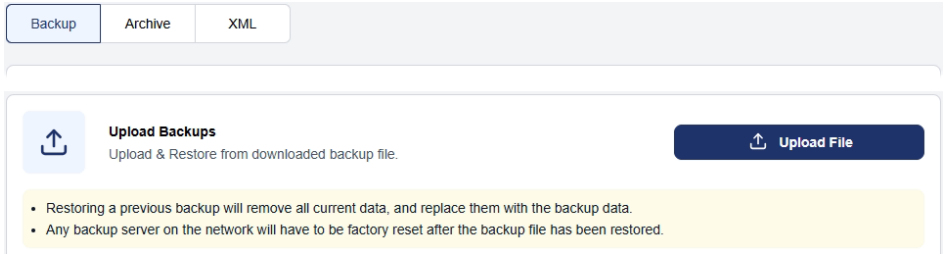
Two ways to restore a Backup

You can restore a Backup file to a Primary or Solo AIM Manager in either of two ways:

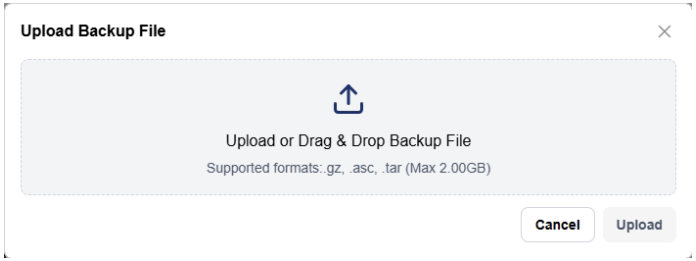
- Using a Backup file that was downloaded from an AIM Manager.
- Choosing a Backup that has been automatically stored on an AIM Manager.

Restoring a Backup file

1 Open the AIM interface and navigate to **System Care > Backup**:



2 In the **Upload Backups** section, click on **Upload File**. The Upload Backup File popup will be displayed:



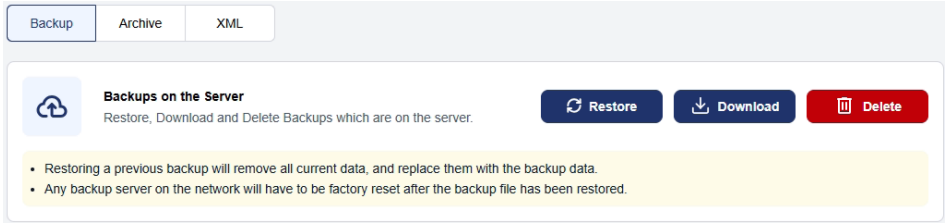
3 Either drag and drop the required backup file into the upload area, or click on the large Upload button and choose the Backup file from the resulting file dialog. AIM will check the backup file.

4 If the chosen file is valid, click the Upload to apply the backup file.

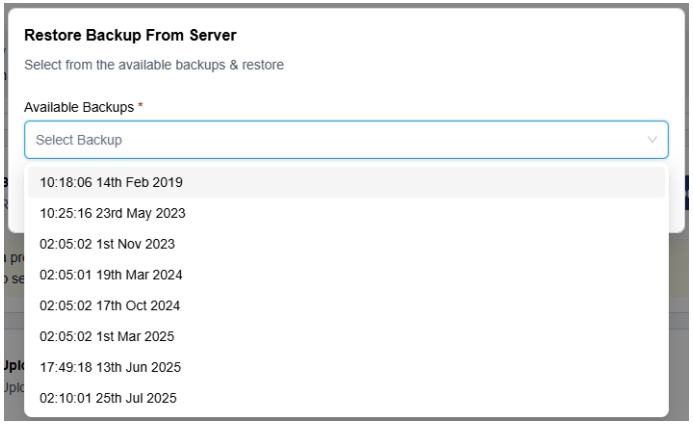
- It may take a few minutes for the Backup file to be restored. Once complete you will be returned to the Backup page.
- If you have any Backup or Satellite AIM Managers, these will need to be factory reset now.
- If you are restoring the Backup to a new AIM or one where end points in the backup have been previously deleted from AIM, then you will need to factory reset the endpoints for them to appear online and interact with AIM.

Restoring a stored Backup file

1 Open the AIM interface and navigate to **System Care > Backup**:

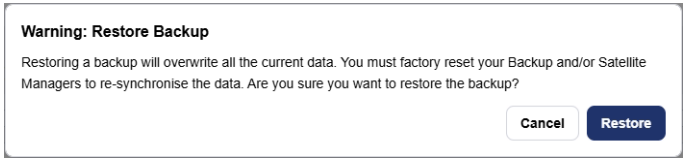


2 In the **Backups on the Server** section, click the **Restore** button. The Upload Backup File popup will be displayed:



3 Click the Available Backups drop down and select the required file from the list.

4 Click the **Restore button**. A warning will be given:



5 If you are sure of the file choice, click the **Restore** button to continue.

- If you have any Backup or Satellite AIM Managers, these will need to be factory reset now.
- If you are restoring the Backup to a new AIM or one where endpoints in the backup have been previously deleted from the AIM, then you will need to factory reset the endpoints for them to appear online and interact with the AIM.

APPENDIX F - TWO FACTOR AUTHENTICATION (2FA)

Overview

Introduced in AIM v5.10, two-factor authentication (2FA) requires two forms of identification for users to log in to the OSD and administrators into the AIM's web interface. To log in, the user will be challenged with entering their password and a time-based 'One Time Password' (OTP), generated with an authenticator application, like the Microsoft or Google Authenticators. A new OTP is generated every 30 seconds. This feature is optional and can be enabled on an individual basis.

IMPORTANT

You must use an NTP (Network Time Protocol) Server to use this feature. Since the One Time Password is time-based, the AIM's system clock must be kept in sync. Without this, the clock could drift over time, preventing the OTP from working and stop users logging into the system.

Enabling 2FA

Log into the AIM's web interface.

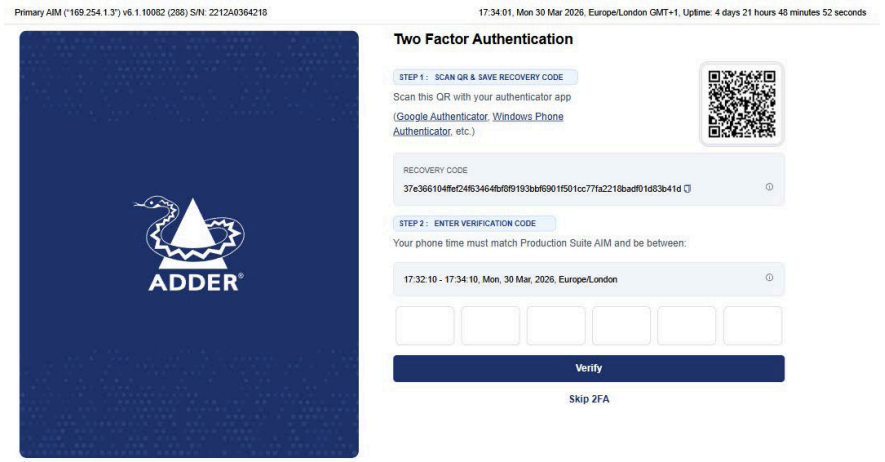
From the Side Menu, choose User Management and then Users.

There are several ways of enabling 2FA for users, except the anon and api_anon user accounts:

- **Option 1**: In the 2FA column for each user, you can use the toggle button to enable and disable.
- **Option 2**: Select the users you wish to modify using the check boxes. At the top right of the list, you can choose to Enable 2FA or Disable 2FA. The number in brackets indicates how many of your selected users are eligible for that specification (e.g., if a user already has 2FA enabled, they will only be counted under the 'Disable' action).
- **Option 3**: When you edit a user, in the Security & Access section, you can toggle the 2FA Required. Password Required must also be enabled.

Setting up 2FA on the AIM User Interface

Administrators who have not yet configured 2FA will be prompted to do so immediately after logging into the AIM:



On the page will find the following elements:-

- A **QR code** that you need to set up the Authenticator application.
- The **Recovery code**. This is a one-time unique password that you should copy and store somewhere securely. This code can be used to login should you have problems using the OTP.
- The **date and the time period** where the OTP password generated from the Authenticator will be valid, Whilst the authenticator application changes the code every 30 seconds. the AIM will allow login provided that the OTP code is valid between these times. By default this is a 2-minute period, however, this can be changed under System Care -> Global Configuration -> Security Settings and changing the **2FA OTP Window** time. This can be set between 1 and 9 minutes.
- Six single number OTP input boxes to enter the six-digit code that is generated from the Authenticator application.

Setting up the Authenticator

Many applications support time-based One Time Passwords, these include Google Authenticator, Microsoft Authenticator, and Authy to name but a few. They are typically installed on your mobile phone and use the same standard algorithm to generate the codes. The following instructions demonstrate how to configure this in Microsoft Authenticator on Android:

1 Install and open the Microsoft Authenticator.

2 Click on the + symbol at the top to add an Account.

3 From the list of options choose **Other account**.

4 Using the Camera, scan the QR Code.

5 You should now see an entry in the Authenticator list called **AIM Authentication_** followed by the user name.

Completing the Setup

1 Using the Authenticator, now open the **AIM Authentication** and enter the **OTP** that it gives you into the AIM.

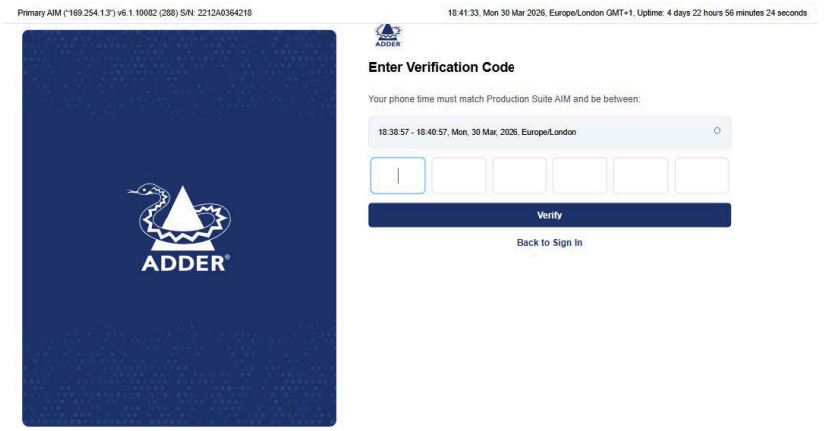
2 Press **Verify**.

3 Provided that the OTP code is accepted, you will now need to use the OTP every time you login.

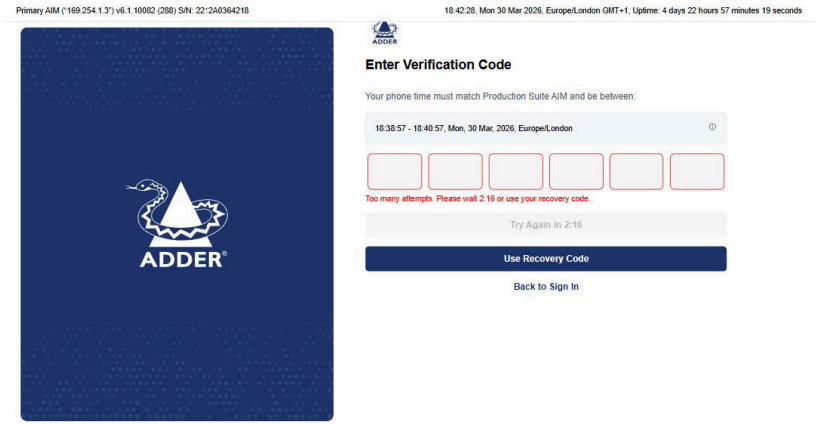
Note: If you decide to skip the 2FA and set it up later, the QR Code used to setup the Authenticator will change, requiring you reset up the Authenticator application again.

Logging into the AIM web interface

The next time you login into the AIM you will just see the following screen without the QR Code etc:

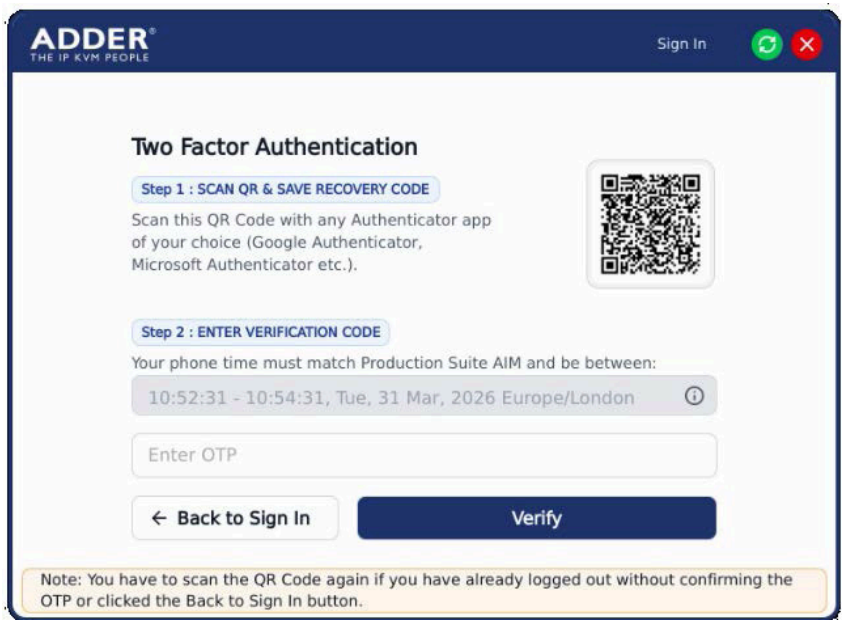


If you enter an incorrect OTP, you get an opportunity to enter it again. After five incorrect attempts, you will be blocked for five minutes. If you no longer are able to provide a OTP, you can use the one-time recovery password to login. Entering the Recovery code and clicking Disable 2FA will turn the feature off.



Setting up 2FA for a User on the OSD

After 2FA has been enabled, the first time a user raises and logs into the OSD they will need to setup their time-based One Time Password(OTP):



Setting up the Authenticator

1 Install and open the Microsoft Authenticator.

2 Click on the + symbol at the top to add an Account.

3 From the list of options choose **Other account**.

4 Using the Camera, scan the QR Code.

5 You should now see an entry in the Authenticator list called **AIM Authentication_** followed by the user name.

Completing the Setup

1 Using the Authenticator, now open the AIM Authentication and enter the OTP that it gives you into the OSD.

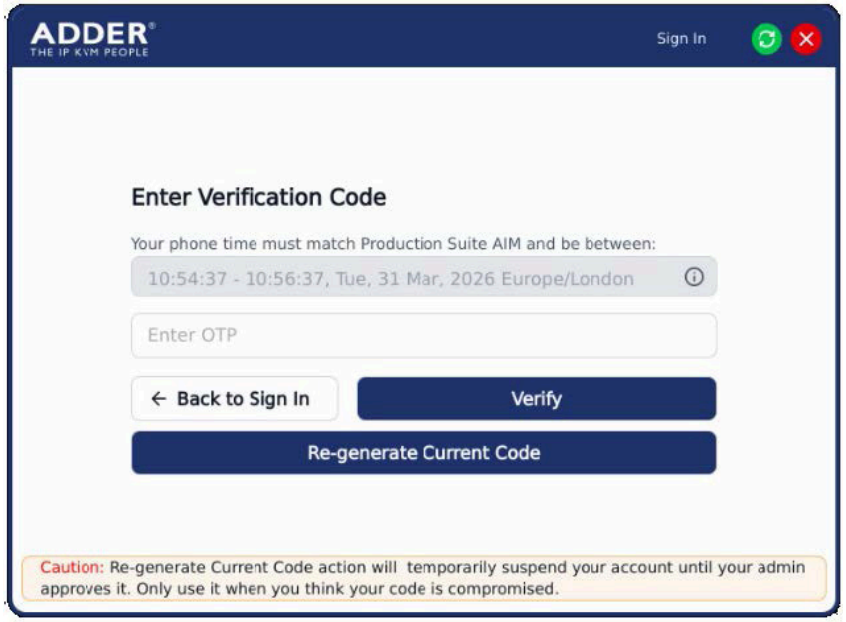
2 Press Verify.

3 Provided that the OTP code is accepted, you will now need to use the OTP every time you login.

Logging into the OSD

Important: If you enter the OTP incorrectly five times in a row the account is automatically suspended.

The next time you login into the OSD you will just see the following without the QR Code. Re-generating the code will automatically suspend the account, requiring intervention by an administrator to unsuspend it. However, this will enable the user to create a new code in the Authenticator application to login.



APPENDIX G - AIM EXPORT USER CONFIGURATION

Overview

The Export User Configuration feature allows you to extract all the Settings, Channels, Receivers and Transmitters configuration from the database in XML format from the AIM Manager. The purpose of which is to be able to track/audit changes made between two given periods. This feature was added in AIM firmware v5.2.

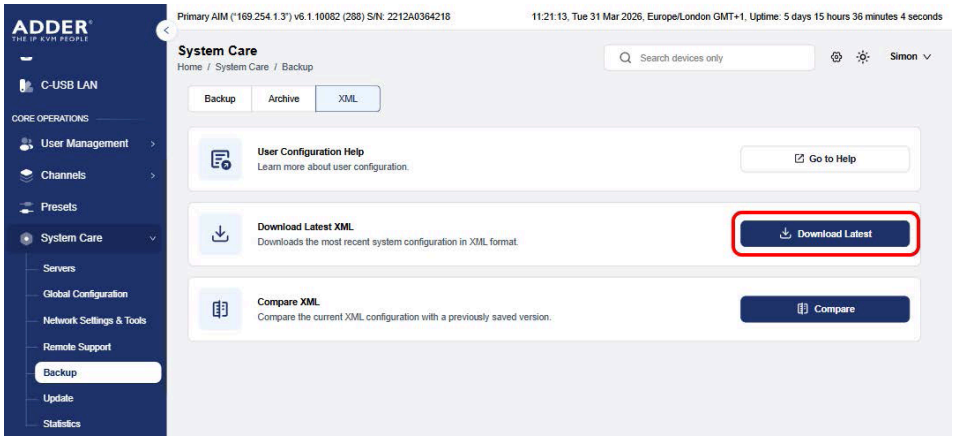
Exporting the Configuration

1 Log into the AIM's web interface.

2 From the side menu, choose **System Care** and then **Backup**.

3 Click on the **XML** tab at the top.

4 Click on **Download Latest**:

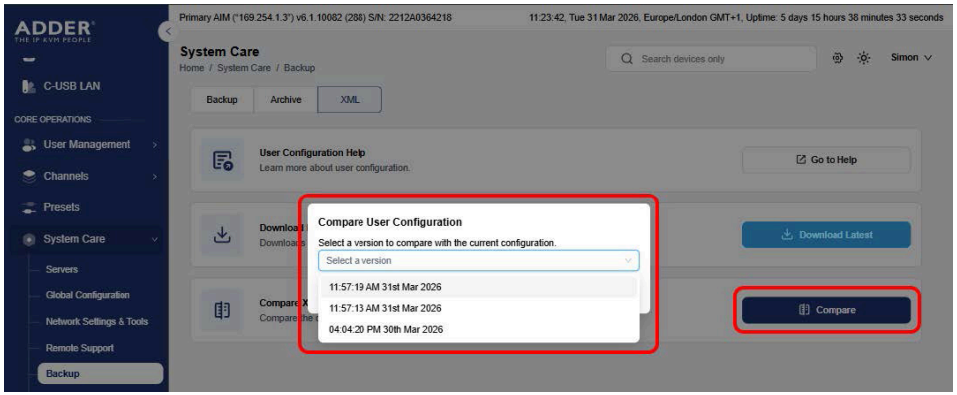


- This generates a gzip file containing a configuration XML file with the AIM Settings that is downloaded to your browser. You will need an application that can decompress gzip files to read it locally.
- A time stamped copy of the file is also stored locally, for later comparison.

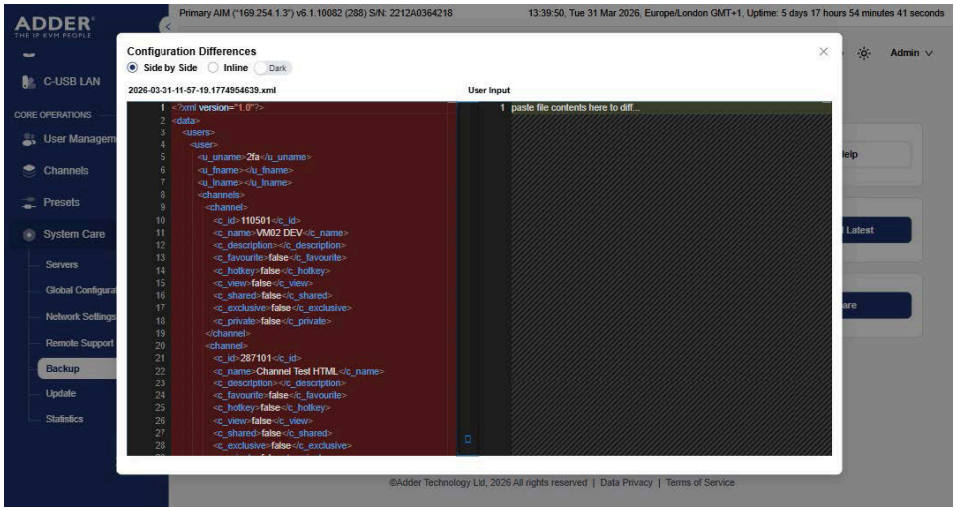
Comparing Configurations

In order to see the configuration changes, you need to:-

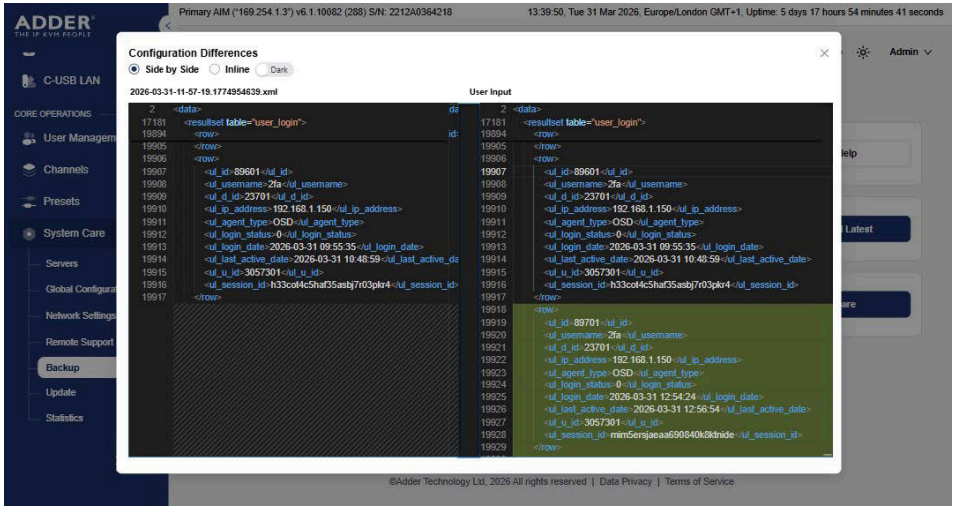
- Have a copy of a previously exported **User Configuration**. The XML file needs to be extracted from the file and loaded into a text editor.
- Download the **latest User Configuration** from the AIM (see Exporting the Configuration section above). This is to generate a snapshot of the current state.
- Click on the **Compare** button.
- From the list of time stamped configurations, choose the latest one:



- Click on the **Compare** button in the dialog window.
- Copy the XML text from the text editor which contains the output from the previously exported configuration, and paste it into the **User Input** window on the right:



- When scrolling through the configuration XML file, any differences will be highlighted:



APPENDIX H - Configuring SSL on an AIM server

Where an AIM server is required to use secure access, eg via external networks, then a valid SSL certificate needs to be associated with the server.

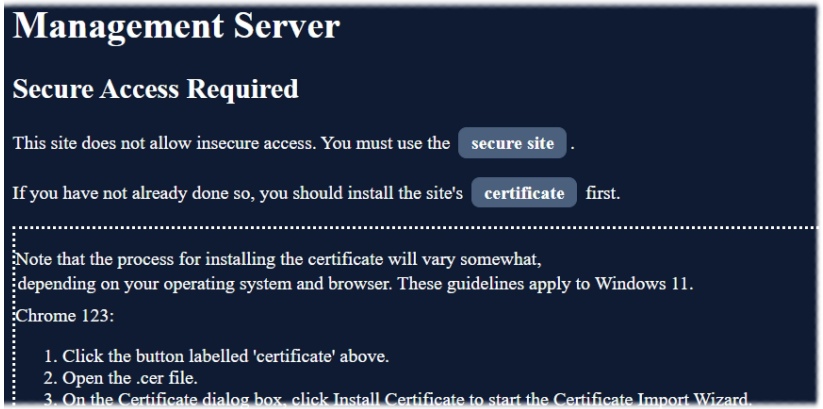
Note: Certificates will not work with link-local IP addresses (e.g. 169.254.1.2) when accessing the AIM server.

To associate an SSL certificate with an AIM server

1 Access the System Care > Update page and in the Regenerate AIM Certificate section, click the Regenerate Certificates button.

2 Access the System Care > Network Settings & Tools > Settings page. As the certificate for the server has now changed, you will see a warning message that the connection is not private - continue to the destination regardless.

3 Choose Yes for the Require SSL for Web option and click the Save button. The Management Server page will be displayed to generate and install an SSL certificate:



4 Click the button labelled certificate and then open the resulting .cer file.

5 On the Certificate dialog box, click Install Certificate to start the Certificate Import Wizard.

6 On the Welcome page, click Next.

7 On the Certificate Store page, select Place all certificates in the following store and click Browse.

8 Select Trusted Root Certification Authorities.

9 On the Certificate Store page, click Next.

10 On the Summary Page, review the details and click Finish.

APPENDIX I - Auto Login Feature

Auto Login is an optional service, available from AIM software release v5.2 onwards, that can be added at any time to an AIM installation. Its purpose is to allow receivers/users (defined individually, by receiver group or globally) to use hotkeys to switch channels without the need to login to the OSD. This feature is useful for applications where a range of transmitter outputs are available for selection and display, but where user interaction is otherwise not required or appropriate.

Note: When configuring the Auto Login feature, bear in mind that any channels to which a receiver/user has been granted access and which have been assigned hotkeys, can be accessed by anyone who has physical access to the receiver and knowledge of the necessary hotkeys.

To add the Auto Login feature

- Purchase and install the necessary Auto Login license.
  See "Appendix J - License upgrading" on page 95.

To authorize users for Auto Login

Once the Auto Login feature has been licensed, receivers/users can be authorized to use it, either:

- individually, or *see page 26*
- by receiver group *see page 30*

To set Auto Login hotkeys for a user

1 Login to the user's local OSD (see "Logging in" on page 74).

2 On the left side of the channels or presets you will see a column labeled 'HOTKEY'. In that column, click the **+** icon for the channel or preset entry to which you wish to apply a hotkey shortcut. The OSD will list the first hotkey slots numbered 0 to 7. Any available slots will be listed as ASSIGN HOTKEY. Click anywhere on an available slot to begin applying a hotkey*.

3 In the resulting page, the hotkey designations will be shown together with the available connection mode(s) - (*Video-Only*, *Shared*, *Exclusive* or *Private*). Click the tickbox of the required connection mode.

4 Click the Save button. The user will now be able to access the chosen channel without logging in by using the hotkeys (Left Ctrl + Left Alt, as standard) plus the number assigned to it.

* *Notes:*

- *To remove a previous channel from a slot, click the*  *icon on the right side of the slot.*
- *Optionally click a number listed along the foot of the page to access further hotkey slots.*

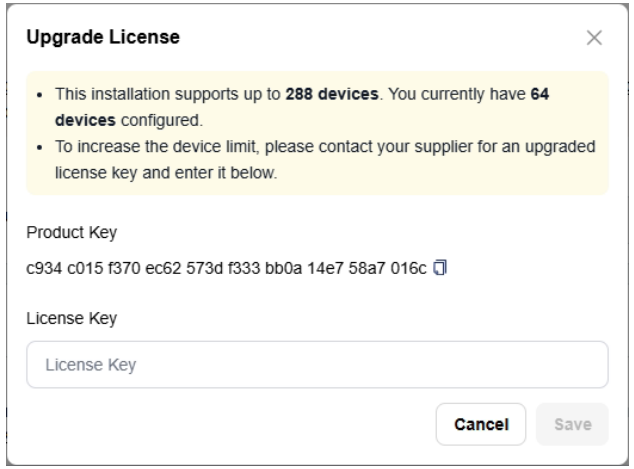
APPENDIX J - License upgrading

Various features of AIM servers are extensible and are licensed accordingly, such as the number of devices that can be managed or additional features, such as multi subnet operation and auto-login. As your installation grows you can purchase an updated AIM license at any time using the procedure outlined below. A range of licenses are available for primary only and primary/failover bundles:

- AIMLIC-48 License for 48 endpoints
- AIMLIC-48-BCK Licenses for Primary and Failover units 48 endpoints
- AIMLIC-96 License for 96 endpoints
- AIMLIC-96-BCK Licenses for Primary and Failover units 96 endpoints
- AIMLIC-192 License for 192 endpoints
- AIMLIC-192-BCK Licenses for Primary and Failover units 192 endpoints
- AIMLIC-288 License for 288 endpoints
- AIMLIC-288-BCK Licenses for Primary and Failover units 288 endpoints
- AIMLIC-UNL License for unlimited endpoints
- AIMLIC-UNL-BCK Licenses for Primary and Failover units unlimited endpoints

To upgrade your AIM license

1 Visit the System Care > Global Configuration page (see page 58) of the AIM unit to be upgraded. At the foot of the page, in the Licensing section, click the **Upgrade License** button. A popup will show a identifier code that is unique to your AIM server:



2 Contact your supplier and quote all of the following:

- The unique Product Key code,
- The serial number of the AIM server (marked on a label on the base of the unit),
- The current number of supported devices, and
- The number of devices to which you wish to upgrade.

The supplier will provide a license key code, which is unique to your AIM server.

Note: It is important that you only enter the license key into the specific AIM server.

3 Enter the supplied unique code into the License Key field and click Save.

If the upgrade is successful, the new status of the chosen feature will be shown on the System Care > Global Configuration page.

APPENDIX K - Glossary

Internet Group Management Protocol

Where an ALIF transmitter is required to stream video to two or more receivers, multicasting is the method used.

Multicasting involves the delivery of identical data to multiple receivers simultaneously without the need to maintain individual links. When multicast data packets enter a subnet the natural reaction of the switches that bind all the hosts together within the subnet, is to spread the multicast data to all of their ports. This is referred to as Multicast flooding and means that the hosts (or at least their network interfaces) are required to process plenty of data that they didn't request. IGMP offers a partial solution.

The Internet Group Management Protocol (IGMP) is designed to prevent multicast flooding by allowing Layer 3 switches to check whether host computers within their care are interested in receiving particular multicast transmissions. They can then direct multicast data only to those points that require it and can shut off a multicast stream if the subnet has no recipients.

There are currently three IGMP versions: 1, 2 and 3, with each version building upon the capabilities of the previous one:

- IGMPv1 allows host computers to opt into a multicast transmission using a Join Group message. It is then incumbent on the router to discover when they no longer wish to receive; this is achieved by polling them (see IGMP Querier below) until they no longer respond.
- IGMPv2 includes the means for hosts to opt out as well as in, using a Leave Group message.
- IGMPv3 encompasses the abilities of versions 1 and 2 but also adds the ability for hosts to specify particular sources of multicast data.

ADDERLink INFINITY units make use of IGMPv2 when performing multicasts to ensure that no unnecessary congestion is caused.

IGMP Snooping

The IGMP messages are effective but only operate at layer 2 - intended for routers to determine whether multicast data should enter a subnet. A relatively recent development has taken place within the switches that glue together all of the hosts within each subnet: IGMP Snooping. IGMP snooping means these layer 2 devices now have the ability to take a peek at the IGMP messages. As a result, the switches can then determine exactly which of their own hosts have requested to receive a multicast – and only pass on multicast data to those hosts.

IGMP Querier

When IGMP is used, each subnet requires one Layer 3 switch to act as a Querier. In this lead role, the switch periodically sends out IGMP Query messages and in response all hosts report which multicast streams they wish to receive. The Querier device and all snooping Layer 2 switches then update their lists accordingly (the lists are also updated when Join Group and Leave Group (IGMPv2) messages are received).

IGMP Fast-Leave (aka Immediate Leave)

When a device/host no longer wishes to receive a multicast transmission, it can issue an IGMP Leave Group message as mentioned above. This causes the switch to issue an IGMP Group-Specific Query message on the port (that the Leave Group was received on) to check no other receivers exist on that connection that wish to remain a part of the multicast. This process has a cost in terms of switch processor activity and time.

Where ALIF units are connected directly to the switch (with no other devices on the same port) then enabling IGMP Fast-Leave mode means that switches can immediately remove receivers without going through a full checking procedure. Where multiple units are regularly joining and leaving multicasts, this can speed up performance considerably.

Jumbo frames (Jumbo packets)

Since its commercial introduction in 1980, the Ethernet standard has been successfully extended and adapted to keep pace with the ever improving capabilities of computer systems. The achievable data rates, for instance, have risen in ten-fold leaps from the original 10Mbit/s to a current maximum of 100Gbit/s.

While data speeds have increased massively, the standard defining the number of bytes (known as the Payload) placed into each data packet has remained resolutely stuck at its original level of 1500 bytes. This standard was set during the original speed era (10Mbits/s) and offered the best compromise at that speed between the time taken to process each packet and the time required to resend faulty packets due to transmission errors.

But now networks are much faster and files/data streams are much larger; so time for a change? Unfortunately, a wholesale change to the packet size is not straightforward as it is a fundamental standard and changing it would mean a loss of backward compatibility with older systems.

Larger payload options have been around for a while, however, they have often been vendor specific and at present they remain outside the official standard. There is, however, increased consensus on an optional 'Jumbo' payload size of 9000 bytes and this is fully supported by the ADDERLink INFINITY (ALIF) units.

Jumbo frames (or Jumbo packets) offer advantages for ALIF units when transmitting certain high resolution video signals across a network. This is because the increased data in each packet reduces the number of packets that need to be transferred and dealt with - thus reducing latency times.

The main problem is that for jumbo frames to be possible on a network, all of the devices on the network must support them.

Spanning Tree Protocol (STP)

In order to build a robust network, it is necessary to include certain levels of redundancy within the interconnections between switches. This will help to ensure that a failure of one link does not lead to a complete failure of the whole network.

The danger of multiple links is that data packets, especially multicast packets, become involved in continual loops as neighbouring switches use the duplicated links to send and resend them to each other.

To prevent such bridging loops from occurring, the Spanning Tree Protocol (STP), operating at layer 2, is used within each switch. STP encourages all switches to communicate and learn about each other. It prevents bridging loops by blocking newly discovered links until it can discover the nature of the link: is it a new host or a new switch?

The problem with this is that the discovery process can take up to 50 seconds before the block is lifted, causing problematic timeouts.

The answer to this issue is to enable the **portfast/edge port** variable for all host links on a switch. This will cause any new connection to go immediately into forwarding mode. However, take particular care not to enable portfast (edge port) on any switch to switch connections as this will result in bridging loops.

Forwarding modes

In essence, the job of a layer 2 switch is to transfer, as fast as possible, data packets arriving at one port out to another port as determined by the destination address. This is known as data forwarding and most switches offer a choice of methods to achieve this. Choosing the most appropriate forwarding method can often have a sizeable impact on the overall speed of switching:

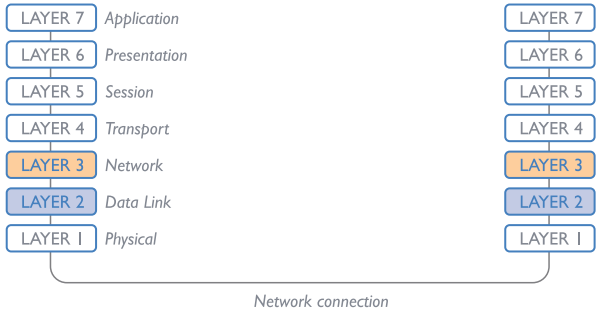
- **Store and forward** is the original method and requires the switch to save each entire data packet to buffer memory, run an error check and then forward if no error is found (or otherwise discard it).
- **Cut-through** was developed to address the latency issues suffered by some store and forward switches. The switch begins interpreting each data packet as it arrives. Once the initial addressing information has been read, the switch immediately begins forwarding the data packet while the remainder is still arriving. Once all of the packet has been received, an error check is performed and, if necessary, the packet is tagged as being in error. This checking 'on-the-fly' means that cut-through switches cannot discard faulty packets themselves. However, on receipt of the marked packet, a host will carry out the discard process.
- **Fragment-free** is a hybrid of the above two methods. It waits until the first 64 bits have been received before beginning to forward each data packet. This way the switch is more likely to locate and discard faulty packets that are fragmented due to collisions with other data packets.
- **Adaptive** switches automatically choose between the above methods. Usually they start out as a cut-through switches and change to store and forward or fragment-free methods if large number of errors or collisions are detected.

So which one to choose? The *Cut-through* method has the least latency so is usually the best to use with ADDERLink INFINITY units. However, if the network components and/or cabling generate a lot of errors, the *Store and forward* method should probably be used. On higher end store and forward switches, latency is rarely an issue.

Layer 2 and Layer 3: The OSI model

When discussing network switches, the terms Layer 2 and Layer 3 are very often used. These refer to parts of the Open System Interconnection (OSI) model, a standardised way to categorize the necessary functions of any standard network.

There are seven layers in the OSI model and these define the steps needed to get the data created by you (imagine that you are Layer 8) reliably down onto the transmission medium (the cable, optical fibre, radio wave, etc.) that carries the data to another user; to complete the picture, consider the transmission medium is Layer 0. In general, think of the functions carried out by the layers at the top as being complex, becoming less complex as you go lower down.



As your data travel down from you towards the transmission medium (the cable), they are successively encapsulated at each layer within a new wrapper (along with a few instructions), ready for transport. Once transmission has been made to the intended destination, the reverse occurs: Each wrapper is stripped away and the instructions examined until finally only the original data are left.

So why are Layer 2 and Layer 3 of particular importance when discussing ADDERLink INFINITY? Because the successful transmission of data relies upon fast and reliable passage through network switches – and most of these operate at either Layer 2 or Layer 3.

continued

The job of any network switch is to receive each incoming network packet, strip away only the first few wrappers to discover the intended destination then rewrap the packet and send it in the correct direction.

In simplified terms, the wrapper that is added at Layer 2 (by the sending system) includes the physical address of the intended recipient system, i.e. the unique MAC address (for example, 09:f8:33:d7:66:12) that is assigned to every networking device at manufacture. Deciphering recipients at this level is more straightforward than at Layer 3, where the address of the recipient is represented by a logical IP address (e.g. 192.168.0.10) and requires greater knowledge of the surrounding network structure. Due to their more complex circuitry, Layer 3 switches are more expensive than Layer 2 switches of a similar build quality and are used more sparingly within installations.

APPENDIX L - Copper/fiber modules and cables

To suit your installation layout, copper and fiber modules are available for the AIM server unit to support various CATx and fiber optic cables. The specifications for all are summarized in this table:

Name	Fiber size	Type	Coding		Distance at 1Gbps	Adder part number for SFP module
			Normal applications	Suggested print nomenclature		
OM1	(62.5/125)	Multimode (TIA-492AAAA)	Orange	62.5/125	220m	SFP-MM-LC
OM2	(50/125)	Multimode (TIA-492AAAB)	Orange	50/125	550m	"
OM3	(50/125)	Multimode (850 nm Laser-optimized) (TIA-492AAAC)	Aqua	850 LO 50 /125	550m	"
OM4	(50/125)	Multimode (850 nm Laser-optimized) (TIA-492AAAC)	Aqua	850 LO 50 /125	550m	"
OS1 and OS2	(9/125)	Single-mode (TIA-492C000 / TIA-492E000)	Yellow	SM/NZDS, SM	10Km	SFP-SM-LC
CATx	n/a	CAT5e and above	n/a	n/a	100m	SFP-CATX-RJ45

Note: *SFP modules up to **1Gb** are supported.*

APPENDIX M - AIM API

The AIM API provides access for external applications to key routines used within the AIM server. This appendix provides a reference to the available methods. For an online version, go to: https://support.adder.com/tiki/tiki-index.php?page=ALIF%3A+API

Note: The API is documented as an HTML file and is found by going to the following address: http://<ip address>/api/

A windows application called the AIM Controller is available for download, whose purpose is to demo and show you the API working in action. An example C# API class has been written and published on Github. It is free to download (https://github.com/AdderAPI/AIM-Manager), but comes with no support or warranty,

Best Practices

Do not log in and generate a new token for every API request. When you first connect to the AIM, log in and store a copy of the token that you are given, and use it for future requests. Each token that you request creates a stored session within the AIM Manager. The duration of the session is defined by the AIM's Admin timeout that is set on the web interface under Dashboard -> Settings -> General. Creating a new token on every request will result in hundreds if not thousands of stored sessions, each taking a small amount of space on the AIM's SSD drive. If a particularly long session duration is set, for example 3 years, then this could easily fill the drive over time since they don't get deleted until they expire.

Do not keep the HTTP port open. When making a request, simply send the API command, wait for the response and then close the connection. A typical web browser will fetch the html page and its associated files such as images, javascripts and ccs files and then close the connection. The AIM runs a standard Apache web service. There is no guarantee that the HTTP connection that you initially establish will always remain open.

The API is restful based; this means that you have to periodically request information from the AIM and compare the previous and latest responses to see what has changed. Be careful not to continuously send API requests as they consume resources on the AIM. Requesting the Devices, Channels, Presets and C-USB information every 5-10 seconds should usually suffice to monitor changes.

Session tokens are linked to the IP address of the host that connected to the AIM. If you change the IP address of the host and use the same token then the API will throw an error telling you that there is a mismatch.

On the AIM Controller API demo the procedure below has been used when sending API requests. This ensures that you are working with a valid token, assuming your login credentials are correct. The initial API request does not send a token, however the procedure takes care of that.

Example Connection Procedure

1 Establish the HTTP connection.

2 Send the API request (with the stored token, if known)

3 Read the response.

- If the response is a Login error then
  - Send a login request with the appropriate username and password.
  - Read the response.
  - If the login request is successful, extract and store the new token.
    - Go back to step 2 and resend the original API request with the stored token.
  - If the login request fails, then handle appropriately.
- If the response is a different error, then handle it appropriately.

4 Close the HTTP connection.

5 Process the response.

Repeat above procedure for the next API command.

Using a Web Browser to test the API

You can use a web browser to issue test API commands to the AIM Manager, however, when you authenticate and receive a token, a web session is also created between the browser and AIM. If you try to use the same web browser to also access the AIM's admin web interface, a different session will be created. This can cause the API token to become invalid on the browser. To resolve this, we recommend that you use two different web browsers, for example, Google Chrome for the API and FireFox for the AIM's admin web interface. This will allow two different sessions to operate simultaneously. This only affects web browsers.

API version: 18

Changelog

v18 (AIM v6.2)
UPDATED APIs:

- disk_usage: This API now includes networkTraceDumpsSize, firmwarePartitionUsedPercent and updated backupUsedPercent.

v17 (AIM v6.1)
UPDATED APIs:

- get_devices: This API now includes additional device details filter.
- get_servers: Replaced disk_space with disk_usage in the response and revised the field description.
- connect_channel: This API now supports temporary username and password for VDI connections.

v16 (AIM v5.14)
UPDATED APIs:

- get_servers: This API now includes additional server details information and server state data.

v15 (AIM v5.12)
UPDATED APIs:

- promote: This api will now work for Satellite AIM too.

v14 (AIM v5.10)
ADDED APIs:

- logout_device: Allows logging out of a specific device.

UPDATED APIs:

- get_servers: Improved server retrieval.
- get_all_c_usb: Modified condition to get an empty address if the device is offline.
- get_devices: Added total_c_usbs.

v13 (AIM v5.9)
UPDATED APIs:

- get_devices: Added channel_id in response.

v12 (AIM v5.8)
ADDED APIs:

- disk_usage: Retrieves disk usage details for both main and backup partitions.

UPDATED APIs:

- get_channels: Updated favourites and hotkey information with user-specific values.

v11 (AIM v5.6)
UPDATED APIs:

- get_channels: This command now respond correctly on a Backup AIM in Acting Primary mode.
- get_presets: This command now respond correctly on a Backup AIM in Acting Primary mode.
- connect_preset: This command now respond correctly on a Backup AIM in Acting Primary mode.
- disconnect_preset: This command now respond correctly on a Backup AIM in Acting Primary mode.
- get_all_c_usb: This command now respond correctly on a Backup AIM in Acting Primary mode.
- update_c_usb: This command now respond correctly on a Backup AIM in Acting Primary mode.
- connect_c_usb: This command now respond correctly on a Backup AIM in Acting Primary mode.
- disconnect_c_usb: This command now respond correctly on a Backup AIM in Acting Primary mode.

v10 (AIM v5.4)
ADDED APIs:

- identify_device: Allows identification of the device

UPDATED APIs:

- get_channels: Added total_channels in response.

v9 (AIM v5.2)
ADDED APIs:

- replace_device: Replaces a configured device with an unconfigured device.
- promote: Promotes a Backup/Satellite AIM server, temporarily acting as the Primary, to become the Primary AIM server.
- get_servers: Returns a list of servers.

v8 (AIM v5.0)
UPDATED APIs:

- get_channels: Modified channel output values.
- get_devices: Added new values to the output.

v7 (AIM v4.8)
ADDED APIs:

- reboot_devices: Sends reboot command to the specified devices

v6 (AIM v4.5)
ADDED APIs:

- get_all_c_usb: Returns a list of the C-USB LAN network extenders.
- delete_c_usb: Deletes a C-USB LAN network extender.
- update_c_usb: Updates the name field for a C-USB LAN network extender
- connect_c_usb: Connects a C-USB LAN network extender receiver.
- disconnect_c_usb: Disconnects a C-USB LAN network extender receiver.

v5 (AIM v4.3)
ADDED APIs:

- update_device: Updates the description and location fields for a device.

UPDATED APIs:

- get_devices
- connect_channel
- connect_preset
- create_channel
- create_preset

v4 (AIM v4.1)
ADDED APIs:

- create_channel: Allows creating a new channel.
- delete_channel: Allows deleting an existing channel.

UPDATED APIs:

- get_channels

v3 (AIM v3.2)
ADDED APIs:

- create_preset: Allows creating a new preset.
- delete_preset: Allows deleting an existing preset.

v2 (AIM v2.3)
ADDED APIs:

- get_devices: Returns a list of devices.
- get_channels: Returns a list of channels.
- connect_channel: Allows connection of a receiver to a channel.
- disconnect_channel: Allows disconnecting a receiver, a number of receivers or all connected receivers.

Updated version compatibility information.

v1 (AIM v1.3)
ADDED APIs:

- login: Authenicates a user and establishes a session.
- logout: Terminates the user session and logs the user out.
- get_presets: Returns a list of presets available to the authenticated user.
- connect_preset: Allows connecting all channel-receiver pairs in a preset.
- disconnect_preset: Allows disconnecting all channel-receiver pairs in a preset, or disconnects ALL connections in the whole AIM network.

API version: 18

Methods

login
logout
logout_device
get_devices
disk_usage
get_channels
get_presets
connect_channel
connect_preset
disconnect_channel
disconnect_preset
create_preset
delete_preset
create_channel
delete_channel
update_device
promote
get_all_c_usb
delete_c_usb
update_c_usb
connect_c_usb
disconnect_c_usb
reboot_devices
replace_device
get_servers
identify_device

login

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards

The API will require a valid AIM user's login credentials to be presented in the first request. The API will return an authentication code, which must be passed in all future requests. This authentication code can be re-used until a logout request is made, at which point the authentication code will no longer be valid.

The concept of an 'anonymous user' can apply to the API. If no login username and password are provided, the API will return an authentication token for the anonymous user (either the same one as for the OSD, or else an 'anonymous API user' account can be created).

Input parameters:

- username
- password
- v (the AIM API version this request is designed for)

Output values:

- timestamp - the current server time
- version - the current API version number
- token - an authentication code for future API requests
- success

Examples

Input:

/api/?v=1&method=login&username=xxxxx&password=xxxxx

Output:

```
<api_response>
  <version>1</version>
  <timestamp>2012-12-14 12:12:12</timestamp>
  <success>1</success>
  <token>5cf494a71c29e9465a57a81e0a2d602c</token>
</api_response>
```

or

```
<api_response>
  <version>1</version>
  <timestamp>2012-12-14 12:12:12</timestamp>
  <success>0</success>
  <errors>
    <error>
      <code>2</code>
      <msg>Invalid username or password</msg>
    </error>
  </errors>
</api_response>
```

logout

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards

The authentication token provided by the 'login' method can be used until the 'logout' method is called.

Input parameters:

- token
- v (the AIM API version this request is designed for)

Output values:

- timestamp - the current server time
- success - 0 = fail, 1 = success

Examples

Input:

/api/?method=logout&token=xxxxx&v=1

Output:

```
<api_response>
  <version>1</version>
  <timestamp>2011-02-04 15:24:15</time>
  <success>1</success>
</api_response>
```

or

```
<api_response>
  <version>1</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>0</success>
  <errors>
    <error>
      <code>3</code>
      <msg>Error logging out (you may already have logged out)</msg>
    </error>
  </errors>
</api_response>
```

logout_device

This method was last updated in API version 14, and is compatible with API requests from version 14 onwards

This simple method logout a user from receiver.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- rx_id - the ID of the receiver

Output values:

- version - the current API version number
- timestamp - the current server time
- success - 0 = fail, 1 = success

Examples

Input:
/api/?v=14&method=logout_device&rx_id=1&token=xxxxx

Output:

```
<api_response>
  <version>14</version>
  <timestamp>2023-08-25 12:39:49</time>
  <success>1</success>
</api_response>
```

or

```
<api_response>
  <version>14</version>
  <timestamp>2023-08-25 12:39:49</timestamp>
  <success>0</success>
  <errors>
    <error>
      <code>3</code>
      <msg>Error logging out (you may already have logged out)</msg>
    </error>
  </errors>
</api_response>
```

get_devices

This method was last updated in API version 17, and is compatible with API requests from version 2 onwards

This method returns a list of devices.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- device_type ('rx' = receivers, 'tx' = transmitters. Default = 'rx')
- filter_d_name (Optional. Device name search string)
- filter_d_description (Optional. Device description search string)
- filter_d_location (Optional. Device location search string)
- filter_d_ip_address (Optional. Device ip address search string)
- filter_d_ip_address2 (Optional. Device ip address search string)
- filter_custom_settings (Optional. Filters devices based on configuration type whether the device is using custom settings or global settings.)
- sort (Optional. Sort results by 'name'/'description'/'location'. Default = 'name')
- sort_dir (Optional. Sort direction for results 'asc'/'desc'. Default = 'asc')
- status (Optional. '','outdated_aim_ip','rebooting','offline','factory_resetting','outdated_firmware','invalid_backup_firmware','rebooting','upgrading_firmware','backup_mode','unconfigured')
- show_all (Optional. If set and not blank, shows all receivers, not just those the logged-in user is permitted to use)
- page (page number to start showing results for, default = 1)
- results_per_page (number of results per page, default = 1000)

Output values:

- version - the current API version number
- timestamp - the current server time
- success
- page (page number)
- results_per_page (number of results per page, default = unlimited)
- total_devices - the total number of devices
- count_devices - the number of devices on this page
- for each device:
  - attribute: item (e.g. 17th device)
  - d_id (device ID)
  - d_serial_number (the device's serial number, if it is reported)
  - d_mac_address (MAC address for interface 1)
  - d_mac_address2 (MAC address for interface 2)
  - d_name (device name)
  - d_online (0 = interface 1 offline, 1 = interface 1 online)
  - d_online2 (0 = interface 2 offline, 1 = interface 2 online)
  - d_type (rx, tx)
  - d_version (0 = RDP SERVER, 1 = ALIF1000R/ALIF1000T, 2 = ALIF2000R/ALIF2000T/ALIF2002T/ALIF2112T/ALIF1002R/ALIF1002T/ALIF2020R/ALIF2020T/ALIF100T/ALIF100T-VGA/ALIF101T-HDMI, 3 = ALIF2100R/ALIF1102R/ALIF2100T/ALIF2124T/ALIF1104T/ALIF102T-DP/ALIF102T-HM, 4 = ALIF4000R/ALIF4000T, 8 = ALIF3000R)

- d_variant ('a' = ALIF2100R/ALIF2100T,'b' = ALIF2002T/ALIF2124T,'c' = HORIZON SERVER, v' = ALIF2112T/VNC SERVER,'s' = ALIF1002R/ALIF1102R/ALIF1002T,'t' = ALIF2020R/ALIF2020T/TERMINAL VDI,'d' = ALIF100T/ALIF102T-DP,'e' = ALIF102T-HM, 'f' = ALIF100T-VGA,'h' = ALIF101T-HDMI/ALIF1104T/HTML SERVER)
- d_ip_address0 (IP address for interface 3, only for ALIF3000R)
- d_ip_address (IP address for interface 1)
- d_ip_address2 (IP address for interface 2)
- d_description (device description)
- d_location (device location)
- d_configured (0 = no, 1 = yes)
- d_valid_firmware (0 = no, 1 = yes)
- d_valid_backup_firmware (0 = no, 1 = yes)
- d_firmware (firmware version, e.g. 2.5.17879)
- d_backup_firmware (backup firmware version)
- d_date_added (Date device added to AIM network e.g. 2012-07-13 22:17:22)
- d_status (0 = device offline, 1 = device online, 2 = rebooting, 3 = factory resetting, 4 = firmware_upgrading, 6 = running backup firmware, 10 = RDP device)
- d_domain_no (VDI domain number counts number of instances mapped on same IP address)

The following property is only returned for transmitters:

- count_transmitter_channels (the number of channels containing this transmitter)
- count_transmitter_presets (the number of presets containing this transmitter)
- video1_multicast_ip (Video 1 Multicast IPs)
- video2_multicast_ip (Video 2 Multicast IPs)
- audio_multicast_ip (USB Audio Multicast IPs)
- digital_audio1_multicast_ip (Digital Audio 1 Multicast IPs)
- digital_audio2_multicast_ip (Digital Audio 2 Multicast IPs)
- analog_audio_multicast_ip (Analog Audio Multicast IPs)

The following properties are only returned for receivers:

- con_c_id (id of the channel last connected)
- con_exclusive (0/1 - if the last connection is/was in private mode)
- con_control (1/2/3 - 1 if the last connection is/was video-only, 2 if in exclusive mode, 3 if in shared mode)
- con_start_time (start time of last connection e.g. 2012-09-07 13:33:17)
- con_end_time (empty if connection still active, else date/time the connection was ended e.g. 2012-09-07 13:33:17)
- u_username (username of the user who initiated the last connection)
- u_id (user ID of the user who initiated the last connection)
- c_name (name of the channel last connected)
- count_receiver_groups (the number of receiver groups this receiver is a part of)
- count_receiver_presets (the number of presets this receiver is a part of)
- count_users (the number of users who have access to this receiver)

Examples

Input:

/api/?v=2&method=get_devices&token=xxxxx

/api/?v=2&method=get_devices&device_type=tx&page=2&results_per_page=3&token=xxxxx

Output:

```
<api_response>
  <version>2</version>
  <timestamp>2012-09-12 14:56:11</timestamp>
  <success>1</success>
  <page>2</page>
  <results_per_page>3</results_per_page>
  <total_devices>12</total_devices>
  <count_devices>3</count_devices>
  <devices>
    <device item="4">
      <d_id>170</d_id>
      <d_serial_number>1409A0000159</d_serial_number>
      <d_mac_address>00:0F:58:01:6E:3D</d_mac_address>
      <d_mac_address2>00:0F:58:5B:6E:3D</d_mac_address2>
      <d_name>RX 123</d_name>
      <d_online>1</d_online>
      <d_online2>0</d_online2>
      <d_type>rx</d_type>
      <d_version>2</d_version>
      <d_variant></d_variant>
      <d_ip_address0/>
```

```
      <d_ip_address>10.10.10.66</d_ip_address>
      <d_ip_address2>10.10.10.67</d_ip_address2>
      <d_description></d_description>
      <d_location>Server Rack 3</d_location>
      <d_configured>1</d_configured>
      <d_valid_firmware>1</d_valid_firmware>
      <d_valid_backup_firmware>1</d_valid_backup_firmware>
      <d_firmware>2.3.16682</d_firmware>
      <d_backup_firmware>2.3.16682</d_backup_firmware>
      <d_date_added>2012-07-14 01:37:07</d_date_added>
      <d_status>1</d_status>
      <d_domain_no>0</d_domain_no>
      <con_c_id>Channel ID</con_c_id>
      <con_exclusive>0</con_exclusive>
      <con_control>1</con_control>
      <con_start_time>2012-09-07 13:33:19</con_start_time>
      <con_end_time/>
      <u_username>admin</u_username>
      <u_id>1</u_id>
      <c_name>Channel 1</c_name>
      <count_receiver_groups>1</count_receiver_groups>
      <count_receiver_presets>2</count_receiver_presets>
      <count_users>1</count_users>
    </device>
  </devices>
</api_response>

<api_response>
  <version>2</version>
  <timestamp>2012-09-12 14:56:11</timestamp>
  <success>1</success>
  <page>1</page>
  <results_per_page>1</results_per_page>
  <total_devices>1</total_devices>
  <count_devices>1</count_devices>
  <devices>
    <device item="1">
      <d_id>64</d_id>
      <d_serial_number/>
      <d_mac_address>00:0F:58:01:56:85</d_mac_address>
      <d_mac_address2>00:0F:58:5B:56:85</d_mac_address2>
      <d_name>TX 456</d_name>
      <d_online>0</d_online>
      <d_online2>0</d_online2>
      <d_type>tx</d_type>
      <d_version>1</d_version>
      <d_variant></d_variant>
      <d_ip_address0/>
      <d_ip_address>1.1.201.31</d_ip_address>
      <d_ip_address2>1.1.201.32</d_ip_address2>
      <d_description></d_description>
      <d_location></d_location>
      <d_configured>1</d_configured>
      <d_valid_firmware>1</d_valid_firmware>
      <d_valid_backup_firmware>1</d_valid_backup_firmware>
      <d_firmware>2.1.15747</d_firmware>
      <d_backup_firmware>2.1.15747</d_backup_firmware>
      <d_date_added>2012-07-13 17:50:04</d_date_added>
      <d_status>0</d_status>
      <d_domain_no>0</d_domain_no>
      <count_transmitter_channels>3</count_transmitter_channels>
      <count_transmitter_presets>1</count_transmitter_presets>
    </device>
  </devices>
</api_response>
```

disk_usage

This method was last updated in API version 12, and is compatible with API requests from version 12 onwards

This method return main and backup disk partition usage.

Input parameters:
- token
- v (the AIM API version this request is designed for)

Output values:
- version - the current API version number
- timestamp - the current server time
- success
- mainUsedPercent - Percentage of main disk partition full.
- backupUsedPercent - Percentage of backup disk partition in use.
- firmwarePartitionUsedPercent - Percentage of firmware disk partition in use.
- dbSize - Total size of database.
- dbEventLogSize - Database event log size.
- dbConnectionLogSize - Database connection log size.
- backupsSize - Backup files size.
- archivesSize - Archived logs size.
- firmwareSize - Firmware file size.
- debugSize - Debug log size.
- debugSizeAll - All debug log size.
- aimUpgradesSize - AIM upgrade files size.
- networkTraceDumpsSize - Network trace dumps size in KB (0 if no capture file exists).

Examples

Input:
/api/?v=12&method=disk_usage&token=xxxxx

Output:
<api_response>
<version>1</version>
<timestamp>2011-02-04 15:24:15</time>
<success>1</success>
<mainusedpercent>25</mainusedpercent>
<backupUsedPercent>13</backupUsedPercent>
<firmwarePartitionUsedPercent>9</firmwarePartitionUsedPercent>
<dbsize>2608</dbsize>
<dbeventlogsize>96</dbeventlogsize>
<dpconnectionlogsize>32</dpconnectionlogsize>
<backupssize>96</backupssize>
<archivessize>0</archivessize>
<firmwaresize>0</firmwaresize>
<debugSize>0</debugSize>
<debugSizeAll>0</debugSizeAll>
<aimupgradesize>791</aimupgradesize>
<networkTraceDumpsSize>5850</networkTraceDumpsSize>
</api_response>

get_channels

This method was last updated in API version 12, and is compatible with API requests from version 2 onwards

This method returns a list of channels available to the authenticated user, for a specific receiver.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- page (page number to start showing results for, default = 1)
- results_per_page (number of results per page, default = 1000)
- device_id (ID of the receiver that this channel will be connected to. Recommended to ensure full checks for connection mode availability.
- filter_c_name (channel name search string)
- filter_c_description (channel description search string)
- filter_c_location (channel location search string)
- filter_favourites (set this non-empty to only show a user's favourites)

Output values:
- version - the current API version number
- timestamp - the current server time
- success
- page (page number)
- results_per_page (number of results per page, default = unlimited)
- total_channels - total number of channels available (only available on API version 10 or

above)

- count_channels - the number of channels on this page, available to the authenticated user
- for each channel:
  - attribute: item (e.g. 17th channel)
  - c_id (channel id)
  - c_name (channel name)
  - c_description (channel description)
  - c_location (channel location)
  - c_channel_type (channel type)
  - c_tx_id (device ID)
  - channel_online (device status)
  - c_favourite (true if this channel is in the user's favourites, false if not)
  - view_button (disabled/enabled/hidden - whether the user can connect to the preset in video-only mode.

    disabled = no, because something is in use by someone else. hidden = never. enabled = yes

    If the device_id of the proposed receiver to be used in the connection is not provided,

    this will not necessarily be an accurate indication of whether other connections may actually interfere)
  - shared_button (disabled/enabled/hidden - as above, but in shared mode)
  - control_button (disabled/enabled/hidden - as above, but in exclusive mode)
  - exclusive_button (disabled/enabled/hidden - as above, but in private mode)

Additional channel output values in version 4:

- c_video1 (device ID)
- c_video1_head (1|2)
- c_video2 (device ID)
- c_video2_head (1|2)
- c_audio (device ID)
- c_usb (device ID)
- c_serial (device ID)

Additional channel output values in version 8:

- c_usb1 (device ID)
- c_audio1 (device ID)
- c_audio2 (device ID)
- c_sensitive
- c_rdp_id (RDP ID) only for RDP devices.

Additional channel output values in version 12:

- c_hotkey_Shared (hotkey number if hotkey exist for Shared mode, empty if doesn't exists)
- c_hotkey_Video_Only (hotkey number if hotkey exist for Video Only mode, empty if doesn't exists)
- c_hotkey_Private (hotkey number if hotkey exist for Private mode, empty if doesn't exists)
- c_hotkey_Exclusive (hotkey number if hotkey exist for Exclusive mode, empty if doesn't exists)

Examples

Input:

/api/?v=2&method=get_channels&token=xxxxx

Version 2 output:

```
<api_response>
  <version>2</version>
  <timestamp>2012-12-14 12:12:12</timestamp>
  <success>1</success>
  <page>1</page>
  <results_per_page>10</results_per_page>
  <count_channels>2</count_channels>
  <channel item="1">
    <c_id>3</c_id>
    <c_name>Channel 1</c_name>
    <c_description>Description for Channel 1</c_description>
    <c_location>Location of Channel 1</c_location>
    <c_favourite>false</c_favourite>
    <view_button>disabled</view_button>
```

```
    <shared_button>disabled</shared_button>
    <control_button>disabled</control_button>
    <exclusive_button>disabled</exclusive_button>
  </channel>
  <channel item="2">
    <c_id>5</c_id>
    <c_name>Channel 2</c_name>
    <c_description>Description for Channel 2</c_description>
    <c_location>Location of Channel 2</c_location>
    <c_favourite>2</c_favourite>
    <view_button>enabled</view_button>
    <shared_button>enabled</shared_button>
    <control_button>enabled</control_button>
    <exclusive_button>hidden</exclusive_button>
  </channel>
</api_response>
```

Input:
/api/?v=10&method=get_channels&token=xxxxx

Version 10 output:

```
<api_response>
  <version>2</version>
  <timestamp>2012-12-14 12:12:12</timestamp>
  <success>1</success>
  <page>1</page>
  <results_per_page>10</results_per_page>
  <total_channels>2</total_channels>
  <count_channels>2</count_channels>
  <channel item="1">
    <c_id>3</c_id>
    <c_name>Channel 1</c_name>
    <c_description>Description for Channel 1</c_description>
    <c_location>Location of Channel 1</c_location>
    <c_favourite>false</c_favourite>
    <view_button>disabled</view_button>
    <shared_button>disabled</shared_button>
    <control_button>disabled</control_button>
    <exclusive_button>disabled</exclusive_button>
  </channel>
  <channel item="2">
    <c_id>5</c_id>
    <c_name>Channel 2</c_name>
    <c_description>Description for Channel 2</c_description>
    <c_location>Location of Channel 2</c_location>
    <c_favourite>2</c_favourite>
    <view_button>enabled</view_button>
    <shared_button>enabled</shared_button>
    <control_button>enabled</control_button>
    <exclusive_button>hidden</exclusive_button>
  </channel>
</api_response>
```

Input:
/api/?v=12&method=get_channels&token=xxxxx

Version 12 output:

```
<api_response>
  <version>12</version>
  <timestamp>2023-03-23 05:32:54</timestamp>
  <success>1</success>
  <page>1</page>
  <results_per_page>1000</results_per_page>
  <total_channels>2</total_channels>
  <count_channels>2</count_channels>
  <channels>
    <channel item="1">
      <c_id>16237601</c_id>
      <c_name>Channel TX</c_name>
```

```
    <c_description></c_description>
    <c_location></c_location>
    <c_channel_type>ALIF</c_channel_type>
    <c_tx_id>1101</c_tx_id>
    <c_hotkey_Shared>6</c_hotkey_Shared>
    <c_hotkey_Video_Only>5</c_hotkey_Video_Only>
    <c_hotkey_Private>4</c_hotkey_Private>
    <c_hotkey_Exclusive>7</c_hotkey_Exclusive>
    <c_favourite>true</c_favourite>
    <channel_online>1</channel_online>
    <c_video1>1101</c_video1>
    <c_video1_head>1</c_video1_head>
    <c_video2 />
    <c_video2_head />
    <c_audio>1101</c_audio>
    <c_usb>1101</c_usb>
    <c_usb1 />
    <c_serial />
    <c_audio1 />
    <c_audio2 />
    <c_sensitive>0</c_sensitive>
    <view_button>enabled</view_button>
    <shared_button>enabled</shared_button>
    <control_button>enabled</control_button>
    <exclusive_button>disabled</exclusive_button>
</channel>
<channel item="2">
    <c_id>12606601</c_id>
    <c_name>channel 2</c_name>
    <c_description></c_description>
    <c_location></c_location>
    <c_channel_type>ALIF</c_channel_type>
    <c_tx_id>1101</c_tx_id>
    <c_hotkey_Shared></c_hotkey_Shared>
    <c_hotkey_Video_Only></c_hotkey_Video_Only>
    <c_hotkey_Private></c_hotkey_Private>
    <c_hotkey_Exclusive></c_hotkey_Exclusive>
    <c_favourite>false</c_favourite>
    <channel_online>1</channel_online>
    <c_video1>1101</c_video1>
    <c_video1_head>1</c_video1_head>
    <c_video2 />
    <c_video2_head />
    <c_audio />
    <c_usb />
    <c_usb1 />
    <c_serial />
    <c_audio1 />
    <c_audio2 />
    <c_sensitive>0</c_sensitive>
    <view_button>enabled</view_button>
    <shared_button>hidden</shared_button>
    <control_button>hidden</control_button>
    <exclusive_button>disabled</exclusive_button>
  </channel>
 </channels>
</api_response>
```


get_presets

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards

This simple method returns a list of presets available to the authenticated user.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- results_per_page (number of results per page, default = 1000)
- page (page number to start showing results for, default = 1)

Output values:

- version - the current API version number

- timestamp - the current server time
- success
- page (page number)
- results_per_page (number of results per page, default = unlimited)
- total_presets - the total number of presets available to the authenticated user
- count_presets - the number of presets on this page, available to the authenticated user
- for each connection_preset:
  - attribute: item (e.g. 17th preset)
  - cp_id (preset id)
    - cp_name (preset name)
    - cp_description (preset description)
    - cp_pairs (the number of channel-receiver pairs in this preset)
  - problem_cp_pairs (the number of channel-receiver pairs that are mis-configured (e.g. receiver offline, receiver not defined)
  - cp_active (whether all, any, or none of the channel-receiver pairs in this preset are currently connected; values are 'full', 'partial', and 'none')
  - connected_rx_count_with_different_user (the number of receivers in this preset that are already connected by different user)
  - view_button (disabled/enabled/hidden - whether the user can connect to the preset in video-only mode.
    disabled = no, because something is in use by someone else. hidden = never. enabled = yes)
  - shared_button (disabled/enabled/hidden - as above, but in shared mode)
  - control_button (disabled/enabled/hidden - as above, but in exclusive mode)
  - exclusive_button (disabled/enabled/hidden - as above, but in private mode)

Examples

Input:
/api/?v=1&method=get_presets&token=xxxxx

Output:

```
<api_response>
  <version>1</version>
  <timestamp>2012-12-14 12:12:12</timestamp>
  <success>1</success>
  <page>1</page>
  <results_per_page>10</results_per_page>
  <total_presets>2</total_presets>
  <count_presets>2</count_presets>
  <connection_preset item="1">
    <cp_id>3</cp_id>
    <cp_name>Preset 1</cp_name>
    <cp_description>Description for Preset 1</cp_description>
    <cp_pairs>1</cp_pairs>
    <problem_cp_pairs/>
    <cp_active>full</cp_active>
    <connected_rx_count_with_different_user>1</connected_rx_count_with_
different_user>
    <view_button>disabled</view_button>
    <shared_button>disabled</shared_button>
    <control_button>disabled</control_button>
    <exclusive_button>disabled</exclusive_button>
  </connection_preset>
  <connection_preset item="2">
    <cp_id>4</cp_id>
    <cp_name>Preset 2</cp_name>
    <cp_description>Description for Preset 2</cp_description>
    <cp_pairs>2</cp_pairs>
    <problem_cp_pairs/>
    <cp_active>none</cp_active>
    <connected_rx_count_with_different_user/>
    <view_button>enabled</view_button>
    <shared_button>hidden</shared_button>
    <control_button>hidden</control_button>
    <exclusive_button>hidden</exclusive_button>
  </connection_preset>
</api_response>
```

connect_channel

This method was last updated in API version 17, and is compatible with API requests

from version 2 onwards

This simple method connects a receiver to a channel.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- c_id - the ID of the channel (acquired from get_channels)
- rx_id - the ID of the receiver (acquired from get_devices)
- mode (optional, 'v', 's', 'e', 'p' - defaults to 's') - the mode in which to connect the channel
- v_username (optional) the username for VDI login (RDP / VNC / Terminal / Horizon channels only)
- password (optional) the password for VDI login (RDP / VNC / Terminal / Horizon channels only)
- vnc_password (optional) the VNC authentication password (VNC channels only, required in addition to username and password when connecting to a VNC channel)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (optional, if anything went wrong with connecting the channel)

Examples

Input:

/api/?v=5&method=connect_channel&token=xxxxx&c_id=1&rx_id=2&mode=e

Output:

```
<api_response>
  <version>2</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

or

```
<api_response>
  <version>2</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>0</success>
  <errors>
    <error>
      <code>231</code>
      <msg>ERROR - private connection not available</msg>
    </error>
  </errors>
</api_response>
```

connect_preset

This method was last updated in API version 5, and is compatible with API requests from version 1 onwards

This simple method connects all channel-receiver pairs in a preset.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- id - the ID of the preset (acquired from get_presets)
- mode (optional, 'v', 's', 'e', 'p' - defaults to 's') - the mode in which to connect the preset
- force (optional, 0/1 - defaults to 0) - whether to ignore errors with some of the preset's pairs or not

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (optional, if anything went wrong with connecting the presets)

Examples

Input:

/api/?v=5&method=connect_preset&token=xxxxx&id=1&force=1

Output:

```
<api_response>
  <version>1</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

or

```
<api_response>
  <version>1</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>0</success>
  <errors>
    <error>
      <code>210</code>
      <msg>ERROR - A receiver is in use by another user</msg>
    </error>
  </errors>
</api_response>
```

disconnect_channel

This method was last updated in API version 2, and is compatible with API requests from version 2 onwards

This method disconnects a receiver, a number of receivers, or all connected receivers.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- rx_id (ID(s) of the receiver, as an integer, or comma-separated set of integers. Optional. If not supplied, all connections will be ended)
- force - whether to disconnect existing connections by other users, or for offline receivers

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:

/api/?v=2&method=disconnect_channel&token=xxxxx (disconnect all your online, connected channels)

/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1 (disconnect channel 1, if you connected it and it's online)

/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1,2,3 (disconnect channels 1, 2, and 3, if you connected them and they're online)

/api/?v=2&method=disconnect_channel&token=xxxxx&force=1 (force disconnect all connected channels)

/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1,3&force=1 (force disconnect channels 1 and 3)

Output:

```
<api_response>
  <version>2</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

disconnect_preset

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards

This method disconnects all channel-receiver pairs in a preset, or disconnects ALL connections in the whole AIM network.

Input parameters:

- token

- v (the AIM API version this request is designed for)
- id (optional. If not supplied, all connections will be ended)
- force - whether to ignore errors with some of the preset's pairs or not

Output values:
- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=1&method=disconnect_preset&token=xxxxx&id=1&force=1

Output:
<api_response>
<version>1</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
</api_response>

create_preset

This method was last updated in API version 5, and is compatible with API requests from version 3 onwards

This method creates a new preset.

The API user must have admin privileges to call this method successfully.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- name (the display name for the new preset)
- pairs (a comma-separated list of the channel IDreceiver ID pairs for the preset, where each ID in the pair is separated by a hyphen)
- allowed (the permitted connection modes for the preset. Optional; if omitted, the global setting will be inherited.

Permitted values are any combination of the characters:
v - video-only
s - shared
e - exclusive
p - private

Output values:
- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)
- id (the ID of the new preset, if it was created)

Examples

Input:
/api/?v=5&method=create_preset&token=xxxxx&name=my_preset&pairs=1-1,1-2,2-3,2-4&allowed=vs

Output:
<api_response>
<version>3</version>
<timestamp>2012-12-12 12:12:12</timestamp>
<success>1</success>
<id>5</id>
</api_response>

delete_preset

This method was last updated in API version 3, and is compatible with API requests from version 3 onwards

This method deletes a preset.

The API user must have admin privileges to call this method successfully.

Input parameters:
- token
- v (the AIM API version this request is designed for)

- id (the ID of the preset to be deleted)

Output values:
- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=3&method=delete_preset&token=xxxxx&id=5

Output:
<api_response>
  <version>3</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>

create_channel

This method was last updated in API version 5, and is compatible with API requests from version 4 onwards

This method creates a new channel.

The API user must have admin privileges to call this method successfully.

NB that, although the source device ID inputs are each optional, at least one is required.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- name (the display name for the new channel)
- desc (the display description for the new channel. Optional, default is empty.)
- loc (the display location for the new channel. Optional, default is empty.)
- allowed (the permitted connection modes for the channel. Optional; if omitted, the global setting will be inherited.
  Permitted values are any combination of the characters:
  v - video-only
  s - shared
  e - exclusive
  p - private
- video1 (device ID of video source 1. Optional, default is empty.)
- video1head (video head number for source 1. Optional, default is 1.)
- video2 (device ID of video source 2. Optional, default is empty.)
- video2head (video head number for source 2. Optional, default is 1.)
- audio (device ID of the audio source. Optional, default is empty.)
- usb (device ID of the usb source. Optional, default is empty.)
- serial (device ID of the serial source. Optional, default is empty.)
- groupname (the name of a channel group of which the created channel will be a member. Optional, default is empty.)

Output values:
- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)
- id (the ID of the new channel, if it was created)

Examples

Input:
/api/?v=5&method=create_channel&token=xxxxx&name=my_channel&video1=21&audio=81&groupname=my_channel_group

Output:
<api_response>
  <version>3</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
  <id>91</success>
</api_response>

delete_channel

This method was last updated in API version 4, and is compatible with API requests from version 4 onwards

This method deletes a channel.

The API user must have admin privileges to call this method successfully.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- id (the ID of the channel to be deleted)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:

/api/?v=4&method=delete_channel&token=xxxxx&id=5

Output:

```
<api_response>
  <version>4</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

update_device

This method was last updated in API version 5, and is compatible with API requests from version 5 onwards

This method updates the description and location fields for a device.

The API user must have admin privileges to call this method successfully.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- id (the ID of the device to be updated)
- desc (the display description for the device. Optional, if not supplied, the description will not be changed. To delete an existing value, set it to the underscore character.)
- loc (the display location for the new channel. Optional, if not supplied, the location will not be changed. To delete an existing value, set it to the underscore character.)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:

/api/?v=5&method=update_device&token=xxxxx&id=1501&desc=John's Desk&loc=room 5

Output:

```
<api_response>
  <version>5</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

promote

This method was last updated in API version 15, and is compatible with API requests from version 9 onwards

This method promotes Backup/Satellite AIM server temporarily acting as Primary to Primary AIM server.

The API user must have admin privileges to call this method successfully.

Input parameters:

- token
- v (the AIM API version this request is designed for)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=9&method=promote&token=xxxxx

Output:
<api_response>
  <version>9</version>
  <timestamp>2021-06-01 11:04:35</timestamp>
  <success>1</success>
</api_response>

or

<api_response>
  <version>9</version>
  <timestamp>2021-06-06 11:04:35</timestamp>
  <success>0</success>
  <errors>
    <error>
      <code>17</code>
      <msg>ERROR - This request will only be processed by an active Backup/Satellite AIM </msg>
    </error>
  </errors>
</api_response>

get_all_c_usb

This method was last updated in API version 14, and is compatible with API requests from version 6 onwards

This method returns a list of the C-USB LAN network extenders.

Input parameters:
- token
- v (the AIM API version this request is designed for)

Output values:
- version - the current API version number
- timestamp - the current server time
- success
- total_c_usbs - the total number of C-USB LAN network extenders
- count_c_usbs - the total number of C-USB LAN network extenders
- for each C-USB LAN network extender:
  - attribute: item (e.g. 17th C-USB LAN extender)
  - mac (C-USB LAN extender MAC address)
  - type (rx, tx)
  - name (customisable name)
  - online (0, 1)
  - ip (C-USB LAN extender IP address)
  - connectedTo (if connected, the MAC address of the connected C-USB LAN extender)

Examples

Input:
/api/?v=6&method=get_all_c_usb&token=xxxxx

Output:

<api_response>
  <version>6</version>
  <timestamp>2012-12-14 12:12:12</timestamp>
  <success>1</success>
  <count_c_usbs>2</count_c_usbs>
  <c_usb_lan_extenders>
    <c_usb item="1">
      <mac>aa:aa:aa:aa:aa:aa</mac>

```
      <type>rx</type>
      <name>John's Desk</name>
      <online>1</online>
      <ip>10.10.10.25</ip>
      <connectedTo>bb:bb:bb:bb:bb:bb</connectedTo>
    </c_usb>
    <c_usb item="2">
      <mac>bb:bb:bb:bb:bb:bb</mac>
      <type>tx</type>
      <name>John's PC</name>
      <online>1</online>
      <ip>10.10.10.27</ip>
    </c_usb>
  </c_usb_lan_extenders>
</api_response>
```

Input:
/api/?v=14&method=get_all_c_usb&token=xxxxx

Version 14 output:

```
<api_response>
  <version>14</version>
  <timestamp>2023-12-01 05:56:43</timestamp>
  <success>1</success>
  <total_c_usbs>0</total_c_usbs>
  <count_c_usbs>0</count_c_usbs>
</api_response>
```

delete_c_usb

This method was last updated in API version 6, and is compatible with API requests from version 6 onwards

This method deletes a C-USB LAN network extender.

The API user must have admin privileges to call this method successfully.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- mac (the C-USB LAN extender MAC address)

Output values:
- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=6&method=delete_c_usb&token=xxxxx&mac=aa:aa:aa:aa:aa:aa

Output:

```
<api_response>
  <version>6</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

update_c_usb

This method was last updated in API version 6, and is compatible with API requests from version 6 onwards

This method updates the name field for a C-USB LAN network extender.

The API user must have admin privileges to call this method successfully.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- mac (the C-USB LAN extender MAC address)
- name (the new display name for the C-USB LAN extender)

Output values:
- version - the current API version number
- timestamp - the current server time

- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=6&method=update_c_usb&token=xxxxx&mac=aa:aa:aa:aa:aa:aa&name=John's Desk

Output:
<api_response>
  <version>6</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>

connect_c_usb

This method was last updated in API version 6, and is compatible with API requests from version 6 onwards

This method connects a C-USB LAN network extender receiver

to a C-USB LAN network extender transmitter.

Note that if either the receiver or the transmitter is currently connected, it will have to be disconnected first.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- rx (the MAC address of the C-USB LAN extender receiver)
- tx (the MAC address of the C-USB LAN extender transmitter)

Output values:
- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=6&method=connect_c_usb&token=xxxxx&rx=aa:aa:aa:aa:aa:aa&tx=bb:bb:bb:bb:bb:bb

Output:
<api_response>
  <version>6</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>

disconnect_c_usb

This method was last updated in API version 6, and is compatible with API requests from version 6 onwards

This method disconnects a C-USB LAN network extender receiver.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- mac (the MAC address of the C-USB LAN extender receiver)

Output values:
- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=6&method=disconnect_c_usb&token=xxxxx&mac=aa:aa:aa:aa:aa:aa

Output:
<api_response>

```
  <version>6</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

reboot_devices

This method was last updated in API version 7, and is compatible with API requests from version 7 onwards

This method sends a reboot command to the specified devices.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- ids (a comma-separated list of IDs of the devices to be rebooted)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:

/api/?v=7&method=reboot_devices&token=xxxxx&ids=101,1701,501

Output:

```
<api_response>
  <version>7</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

replace_device

This method was last updated in API version 9, and is compatible with API requests from version 9 onwards

This method replaces the device with the unconfigured device

Input parameters:

- token
- v (the AIM API version this request is designed for)
- d_id (device ID)
- r_d_id (device ID with which the user wants to replace their device)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:

/api/?v=9&method=replace_device&d_id=101&r_d_id=102&token=xxxxx

Output:

```
<api_response>
  <version>9</version>
  <timestamp>2021-06-03 15:30:06</timestamp>
  <success>1</success>
</api_response>
```

or

```
<api_response>
  <version>9</version>
  <timestamp>2021-06-03 15:30:06</timestamp>
  <success>0</success>
  <errors>
    <error>
      <code>9</code>
      <msg>You must provide an ID</msg>
```

```
    </error>
  </errors>
</api_response>
```

get_servers

This method was last updated in API version 17, and is compatible with API requests from version 9 onwards

This method returns a list of servers.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- page (page number to start showing results for, default = 1)
- results_per_page (number of results per page, default = 1000)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)
- page (page number)
- results_per_page (number of results per page, default = unlimited)
- total_servers - the total number of servers
- count_servers - the number of servers on this page
- attribute: item (e.g. 1st server)
- id (the id for the server)
- name (the display name for the server)
- role - the role of AIM - primary, backup, solo, unconfigured
- status - the status of AIM - active, standby, failed, quiscent
- ip - the server IP on which AIM is running
- mac - MAC address
- eth1 - 0 = no, 1 = DHCP, 2 = Static, 3 = bonded
- ip2 - if eth1 is not enabled then this field will be empty
- mac2 - if eth1 is not enabled then this field will be empty
- eth0_status - the status of Eth0 interface
- eth1_status - the status of Eth1 interface
- CPU_load - CPU load average value over the past 1 minute
- memory_usage - Memory usage of the system in percentage
- software_version - Software version of the current AIM
- disk_usage - Disk usage percentage of the root filesystem (/)
- description (the display description for the server. Optional, default is empty.)
- location (the display location for the server. Optional, default is empty.)

Examples

Input:

/api/?v=9&method=get_servers&token=xxxxx

/api/?v=9&method=get_servers&page=2&results_per_page=3&token=xxxxx

Output:

```
<api_response>
  <version>9</version>
  <timestamp>2021-06-01 16:10:28</timestamp>
  <success>1</success>
  <page>1</page>
  <results_per_page>1000</results_per_page>
  <total_servers>2</total_servers>
  <count_servers>2</count_servers>
  <servers>
    <server item="1">
      <id>1</id>
      <name>192.168.22.105</name>
      <role>primary</role>
      <status>active</status>
      <ip>192.168.22.105</ip>
      <mac>70:85:c2:1c:21:6e</mac>
      <eth1>0</eth1>
      <ip2></ip2>
      <mac2></mac2>
      <eth0_status>UP</eth0_status>
      <eth1_status>DOWN</eth1_status>
      <CPU_load>0.1</CPU_load>
```

```
    <memory_usage>18%</memory_usage>
    <software_version>5.12.10015</software_version>
    <disk_usage>10%</disk_usage>
    <description></description>
    <location></location>
</server>
<server item="2">
    <id>2</id>
    <name>192.168.22.106</name>
    <role>backup</role>
    <status>standby</status>
    <ip>192.168.14.107</ip>
    <mac>70:85:c2:1c:22:6e</mac>
    <eth1>0</eth1>
    <ip2></ip2>
    <mac2></mac2>
    <eth0_status>UP</eth0_status>
    <eth1_status>DOWN</eth1_status>
    <CPU_load></CPU_load>
    <memory_usage></memory_usage>
    <software_version></software_version>
    <disk_usage></disk_usage>
    <description></description>
    <location></location>
    </server>
  </servers>
</api_response>
```

identify_device

This method was last updated in API version 10, and is compatible with API requests from version 10 onwards

This method sends a identify command to the specified devices.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- id (ID of the device)

Output values:

- version - the current API version number
- timestamp - the current server time
- success (0 = fail, 1 = success)
- errors (if anything failed, details are returned here)

Examples

Input:

/api/?v=10&method=identify_device&token=xxxxx&id=101

Output:

```
<api_response>
  <version>7</version>
  <timestamp>2012-12-12 12:12:12</timestamp>
  <success>1</success>
</api_response>
```

APPENDIX N - DHCP server requirements for ALIF support

Version 1.0

ALIF DHCP client

The ALIF DHCP client will identify itself to a DHCP server using DHCP option 60 (Vendor-Class-Identifier) containing the brand string appropriate to the firmware, e.g. Adder.

The ALIF DHCP client will also provide the DHCP server with its unique hostname and a request for DHCP option 125 (Vendor Identified Vendor Sub Options). See Using DHCP option 125 for details.

DHCP server

A DHCP server will use the Vendor-Class-Identifier to identify an ALIF and supply it with Adder vendor information encapsulated in the Adder Enterprise number (25119) within DHCP option 125 (Vendor Identified Vendor Sub Options).

As of ALIF firmware version 4.2, the required Adder vendor information to be encapsulated is:

Sub-option 1: Array of IP addresses of all AIM servers in the cluster.

Note: ALIF will ignore any DHCP OFFER not containing this information.

Example Gamma (Cisco IOS DHCPd, Adder, AIM servers: 10.0.20.5, 10.0.20.6)

```
ip dhcp pool vlan20
    network 10.0.20.0 255.255.255.0
    default-router 10.0.20.1
    option 60 ascii "adder"
    option 125 hex 0000.621f.0a01.080a.0014.050a.0014.06
```

where:

0x000621f	*Adder Enterprise number (25119)*
0x0a	*Length*
0x01	*Sub-option 1*
0x08	*Length*
0x0a001405	*10.0.20.5 (Primary AIM)*
0x0a001406	*10.0.20.6 (Backup AIM)*

Example Alpha (ISC DHCPd, Adder, AIM servers: 10.0.20.5, 10.0.20.6)

```
# ISC DHCPd configuration for Adder
set vendor-string = option vendor-class-identifier;
option space adder code width 1 length width 1;
option adder.aim-servers code 1 = array of ip-address;
option space vivso code width 4 length width 1;
option vivso.iana code 0 = string;
option vivso.adder code 25119 = encapsulate adder;
option option-125 code 125 = encapsulate vivso;
default-lease-time 3600;
max-lease-time 7200;
log-facility local7;
class "adder"
{
    match if option vendor-class-identifier = "adder";
}
subnet 10.0.20.0 netmask 255.255.255.0
{
    pool
    {
        allow members of "adder";
        vendor-option-space adder;
        option domain-name "customer.com";
        option domain-name-servers 10.0.20.2;
        option routers 10.0.20.1;
        option vivso.iana 01:01:01;
        option adder.aim-servers 10.0.20.5,10.0.20.6;
        range 10.0.20.100 10.0.20.200;
    }
}
```

Using DHCP Option 125

DHCP Option 125 is a vendor-specific feature that provides additional information to the ALIF Receivers and Transmitters when requesting an IP Address. The option gives the endpoints the IP Address of the Primary and any other Backup or Satellite AIM Servers that reside on the network.

The information is provided in a hex code which can be formatted slightly differently depending on the DHCP Server, but will typically look like:

000621f0a01080a0014050a001406

The Hex code is broken down to the following elements:

000621f	Adder Enterprise number (25119)
0a	Length A
01	Sub-option 1
08	Length B
0a001405	10.0.20.5 (Primary AIM)
0a001406	10.0.20.6 (Backup AIM)

The Adder Enterprise element of hex code is fixed and does not change, however the IP Address and lengths A & B hex values will change depending on the INFINITY configuration.

The first IP address in the list must always be the Primary AIM Server, followed by the Backup then Satellite AIMs.

There are a number of online websites that help you convert an IP Address into a hex number. Alternatively, you could use a Calculator with a Hex and Dec function which you may find is built into your computer's operating system.

An IP Address hex code can be calculated by converting each of the four octet decimals individually into hex.

Decimal	Hex
10	0a
0	00
20	14
5	05

10.0.20.5 = 0a001405

Each hex IP Address is 4-bytes in length:

0a	00	14	05	
1	1	1	1	(Total 4 bytes)

The Lengths A and B values will change depending on the number of IP Addresses that are included.

The Length B value is the total byte count of the hex IP Addresses. In the example below, there are 2x IP hex addresses. Each IP hex address is 4-bytes, therefore Length B is 8-bytes in total which equates to 08 in hex.



Length A includes Sub-option 1 (1-byte) and the Length B value (1-byte) plus the total of Length B (8-bytes). This makes the total 10-bytes which equates to 0a in hex.



Example

In the following example an additional IP address will be added to the existing DHCP option 125 hex code shown previously. It will be a Satellite AIM whose IP address is 10.0.30.1 which is on a different subnet.

Step 1: Convert IP Address 10.0.30.1 into hex, which is 0a001e01. Add it to the end of the hex code:

000621f..01..0a0014050a0014060a001e01

Step 2: Calculate Length B. Since we now have 3x IP addresses and each hex address is 4-bytes, the total length is 12-bytes which equates to 0c in hex:

000621f..010c0a0014050a0014060a001e01

Step 3: Calculate Length A. This is the total of Length B plus the byte count for Sub-option 1 and the Length B value. The Sub-option 1 and Length B values are 1-byte each, the Length B total is 12-bytes. This makes the total of Length A to be 14-bytes which equates to 0e in hex:

000621f0e010c0a0014050a0014060a001e01

APPENDIX O - AIM database schema

Settings

Value	Meaning
login_required	Anon cannot login into the receiver
auto_login_user	Allows hotkey access to the user without any login
show_multi_user_info	Disable(0) or Enable(1) the use of multi-user feature on OSD
osd_alerts	Disable(0) or Enable(1) alerts on OSD
show_osd_banner	Disable(0) or Enable(1) OSD Banner
osd_hotkeys_disabled	Disable(0) or Enable(1) the use of OSD Hotkey
osd_login_message	Message to display on the osd login page
keyboard_country	Keyboard country code for receiver
download_backup	Download the Database Backup File to Computer,if value set to 1
backup_schedule	Schedule the database backup at server (Never/0, Hourly/1, Daily/2,Weekly/3)
allow_users_exclusive_mode	Allow all users to access the Private Mode
ad_schedule	Sync Schedule the active directory (Never/0, Hourly/1, Daily/2,Weekly/3)
allow_force_disconnect	Disable(0) or Enable(1) any user logged in to receiver to disconnect the channel connected by another user
allow_disconnect_all_receivers	Disable(0) or Enable(1) Disconnect all receivers icon on dashboard

Allowed modes

Value	Meaning
0	inherit
1	view/shared only
2	exclusive only
3	view/shared & exclusive
4	view only

On-line Status

Value	Meaning
0	offline
1	online
2	rebooting
3	factory_resetting
4	firmware_upgrading
5	online, but unconfigured
6	running backup firmware
7	device ID no longer online

Configure Status

Value	Meaning
0	Unconfigured
1	Configured and Saved

OSD Banner Position

Value	Meaning
4,4	Top Left
4,50	Top Center
4,96	Top Right
96,4	Bottom Left
96,50	Bottom Center
96,96	Bottom Right

continued

Channel

Value	Meaning
c_id	Channel ID.
c_name	Channel Name.
c_description	Description for the channel.
c_favourite	True if this channel is in user's favourites, False if not.
c_hotkey	True if this channel has hotkey, False if not.
c_view	True if this channel is connected in View mode, False if not.
c_shared	True if this channel is connected in Shared mode, False if not.
c_exclusive	True if this channel is connected in Exclusive mode, False if not.
c_private	True if this channel is connected in Private mode, False if not.
c_allowed_modes	An integer value representing allowed modes for the channel. Refer the Allowed modes table for more details.
c_location	Location for the channel.
c_users_count	Number of users with access permissions for the channel.
c_sensitive	Channel not Sensitive(0) or Channel is Sensitive(1).
c_channel_type	Type of connected channel.
c_osd_banner_pos	OSD Banner position value for the channel.
c_domain_no	For Horizon Channels, service name should be unique.

User

Value	Meaning
u_username	Name of the user.
u_firstname	First name of the user.
u_lastname	Last name of the user.
u_email	Email ID of the user.
u_token	Login session token passed instead of login credentials. Used only for API calls.
u_created_date	Date the user entry was created.
u_last_login_date	Date the user last logged in (to AIM admin or the OSD).
u_suspended	Whether the user has access to AIM (1) or not (0).
u_admin	Whether the user has access to AIM admin (1) or not (0).
u_allow_exclusive_mode	Whether the user can connect to channels in Private mode (1) or not allowed (0) or inherit (-1).
u_allow_remote_osd	Enable (1) or disable (0) or inherit (-1) remote OSD for the user.
u_ldap_import	Whether the user was imported from Directory Server (1) or created by AIM admin (0).
u_ldap_last_import_date	The last time this user's information was synced with Directory Server.
u_ldap_dn	Distinguished Name, if the user was imported from Directory Server.
u_ldap_server_id	This user's Directory Server ID.
u_2fa_enabled	Whether two-factor authentication is enabled (1) or disabled (0) for this user.
u_2fa_secret	Two-factor authentication secret key used to generate OTP.
u_2fa_renew_requested	Whether this user has requested (1) or not requested (0)to renew two-factor authentication.

APPENDIX P - Technical specifications

Hardware
Industrial specification server with solid state memory

Software
Closed system with bespoke application preloaded

Physical design
1U short-depth (230mm) server

WxHxD: 16.93" x 1.75" x 9.05"
430mm x 44.5mm x 230mm

Weight: 5.95 lbs
2.7kg

Power
Input rating of server: 12VDC 2.0A

Power Adapter

Input: 100-240VAC 50/60Hz 1.5A

Output: 12VDC 5.0A

Connector: IEC input

IMPORTANT: A defective power adapter MUST only be replaced with this make and model: Adder order code: PSU-IEC-12VDC-5A

Permitted operational ambient conditions
Operating temperature: 0 to 40°C / 32 to 104°F

Relative Humidity: 10-90% non-condensing

Permitted Altitude: <2000m

Approvals: CE, FCC

APPENDIX Q - OPEN SOURCE LICENSES

This product includes binaries that are derived from the open source community by Adder under the GNU General Public License v2. Please follow the link below to view the full list of open source licenses used:

https://support.adder.com/tiki/tiki-index.php?page=AIM:-OpenSource-Licence

The software included in this product contains copyrighted software that is licensed under the GNU General Public License (GPL). You may obtain the complete Corresponding Source Code from Adder for a period of three years after the last shipment of this product, which will be no earlier than 2028, by contacting support@adder.com or writing to:

Attn: ACD/Open Source Request,
Adder Technology Ltd,
Saxon Way, Bar Hill,
Cambridge, CB23 8SL,
United Kingdom

Please write "Source for product XXXXXXXX" in the subject line,
where XXXXXXXX is the model and version number.

This offer is valid to anyone in receipt of this information.



www.adder.com

Documentation by: CORPORATE TEXT & DESIGN www.ctxd.com

© 2026 Adder Technology Limited
All trademarks are acknowledged.
Part No. MAN-000016 • Release 7.2

Index

Symbols

2FA 46,58,67,88

A

Accessing virtual machines 76
Active Connections 20
Adding a VDI 38
AIM menu 19
All Channels 51
All Receivers 25
All Transmitters 34
Auto Login
  explanation 94
  user authorisation 30,63

B

Backup
  AIM manager 85
  system care 71
Base DN 49
Browsers
  supported 13

C

Cable spec
  null modem 81
Channel Groups 53
Channels 51
  what are they? 5
Clear credentials 76
Connection logs 23
Contrast
  screen 19
Credentials
  VM 76
C-USB LAN 43,76

D

Dashboard 18
Directory servers 49
Distinguished Name 49

E

Event logs 24

F

Factory reset 16
Favorites 74
Frame Skipping 40
Front panel indicators 17

G

Global Configuration
  system care 58
Glossary 96
Groups
  what are they? 5
GSSAPI 50

H

Horizon 38
Hotkey settings 63
Hotkey shortcuts 74

I

IGMP 96
Indicators 17
IP port
  connecting 9

K

Kerberos 50

L

LDAP 49
License upgrade 95
Logging in
  administrators 13
  normal users 74
  OSD 74
Logout 19
Logs
  connection 23
  event 24

M

Magic Eye 40

N

Networking ALIF
  tips 80
Network ports
  configuration 66
Network Settings & Tools
  system care 65
Network View
  active connections 22

O

On-Screen Display 5,74,75,77
OSD 5
  logging in 74
  login 74
  main screen 75
  On Screen Display 75
  remote 77
  shortcuts 74

P

Permissions 6,28,32,54
Port
  VDI 38
Portfast 97
Presets 55

R

RDP 38
Receiver groups 29
Receivers 25
Redundant servers
  setting up 83
Regular user 5
Relationship
  three-way 5
Remote OSD 77
Remote support
  test connection 70
Remote Support
  system care 70
Reset
  manual 16
Restart web server 72
Restore
  AIM Manager 86

S

Security 5,28,32,54
Server redundancy 83
Servers
  system care 57
SFP ports 9
Shortcuts 74
Specifications 128
SSL
  configuring certificate 93
Statistics
  system care 73
Swapping an AIM server 83

T

Table View
  active connections 21
Technical specifications
  15,79,124,126,128
Terminal 38
Test Connection
  remote support 70
Transmitter groups 39
Transmitters 34
Troubleshooting 82
Two Factor Authentication
  46,58,67,88

U

Update
  system care 72
Update firmware
  receivers 33
  transmitters 42
Upgrade license 95
User Groups 47
User management 45

V

VDI 38
Virtual Desktop Infrastructure
  34,38
VM credentials 75,76,78
VNC 38