



Introduction

A.I.M. basics	3
Supplied items	5

Installation

Connections	6
Front panel indicators	7
Installation requirements	7

Configuration

Supported browsers	8
Login for admin users	8
Adding AdderLink Infinity units	9
If an ALIF unit is not located	9
AdderLink Infinity manual factory reset	9
Basic steps for a new configuration	10
Notes on Zero-config networking	10
The Dashboard tab	11
Upgrading firmware globally on ALIF units	17
The Channels tab	19
The Receivers tab	22
The Transmitters tab	25
The Servers tab	28
The Users tab	29
The Presets tab	33
The Statistics tab	35

Operation

Logging in	36
The Local OSD screen	37
Using the Remote OSD feature	38

Further information

Getting assistance	39
Appendix A - Tips for success when networking ALIF units	40
Appendix B - Troubleshooting	42
Appendix C - Redundant servers: Setting up and swapping out	44
Setting up A.I.M. server redundancy	44
Swapping out an A.I.M. server	45
Appendix D - Glossary	46
Appendix E - A.I.M. API	49
Warranty	57
Safety information	57
Radio Frequency Energy	58

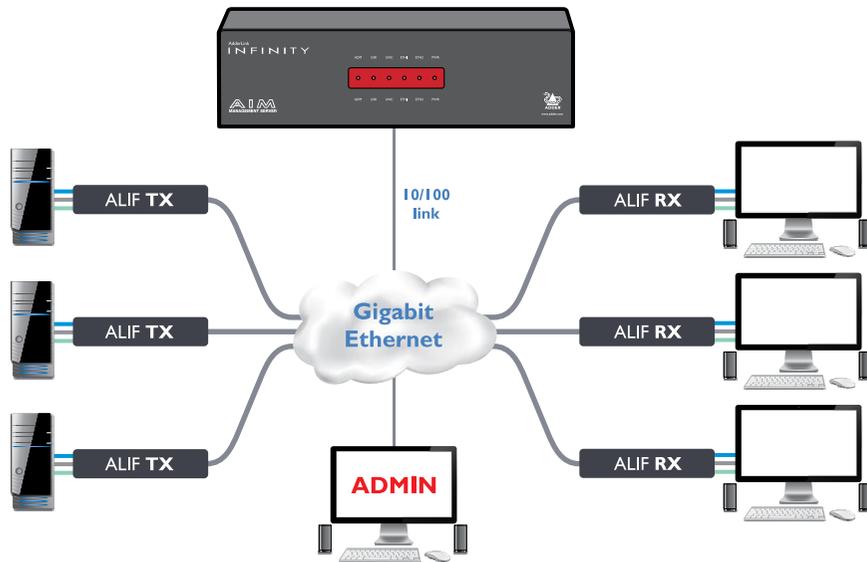
Index

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 A.I.M. (AdderLink Infinity Manager) becomes vital.

A.I.M. 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 A.I.M. web-based interface, one or more administrators can manage potentially thousands of users who are interacting with an almost unlimited number of devices.

A.I.M. operates as a self-contained compact server unit that can be situated anywhere within your network:

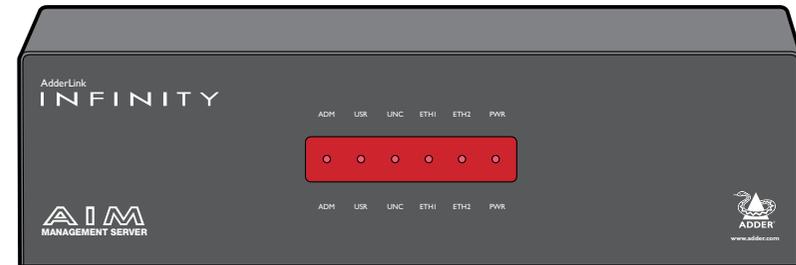


The A.I.M. server connects to your network and provides administrative control over the various AdderLink Infinity transmitters, receivers and their users.

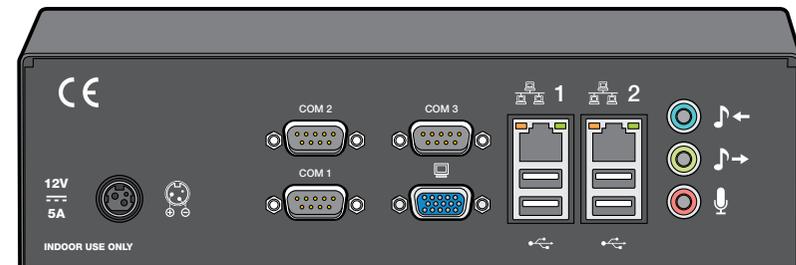
Note: Although the AdderLink Infinity units require Gigabit Ethernet connections, in its administrative role, the A.I.M. server requires only a 10/100Mbps connection to the network.

The A.I.M. 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 are performed using the intuitive A.I.M. browser interface via a network connected computer.



The A.I.M. server front panel with status indicators



The A.I.M. server rear panel. In normal use only the network and power connectors are used.

Please see the section [Basic steps for a new configuration](#) for assistance with creating A.I.M. installations.

A.I.M. 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, A.I.M. 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

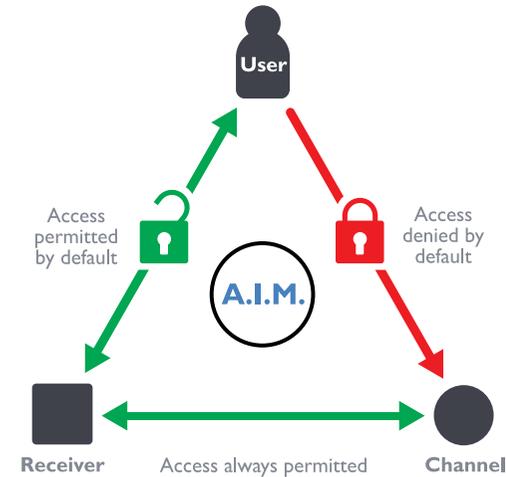
This guide refers to the two main categories of users involved with the A.I.M. system:

- An **Admin (administrator) user** accesses the A.I.M. 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 A.I.M. 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 A.I.M. operation, ensuring that users have rapid access only to the systems for which they have permission. At its core, A.I.M. 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, A.I.M. 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

Active Directory

To streamline administration even further, A.I.M. 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.

A.I.M. interface

A.I.M. 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. This comprehensive application shows eight main tabbed areas: [Dashboard](#), [Channels](#), [Receivers](#), [Transmitters](#), [Servers](#), [Users](#), [Presets](#) and [Statistics](#), each of which contains numerous related pages of settings and options. 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.

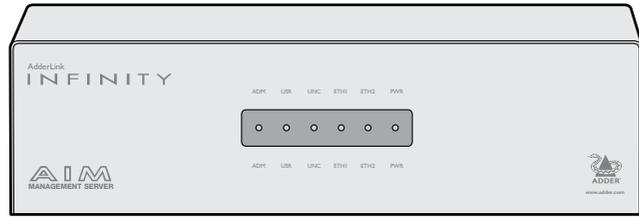
Permissions between a user and a receiver can be applied in any of the following ways:

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

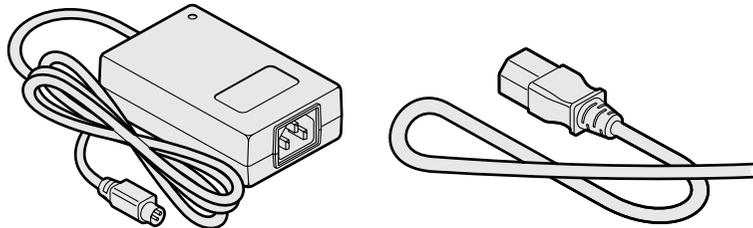
Thus, a very indirect way of granting permissions could be:

- UserI is in UserGroupI,
- UserGroupI has access to ReceiverGroupI,
- ReceiverGroupI contains ChannelI,
- Therefore, UserI has access to ChannelI indirectly.

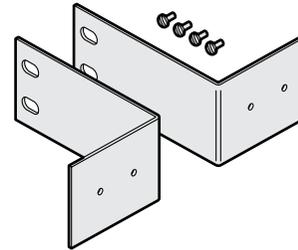
SUPPLIED ITEMS



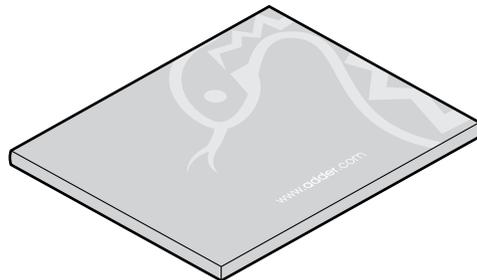
A.I.M. server unit



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



Rack mount brackets



Information wallet
containing:
Four self-adhesive rubber feet
Quick start guide
Safety document

CONNECTIONS

The A.I.M. 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.

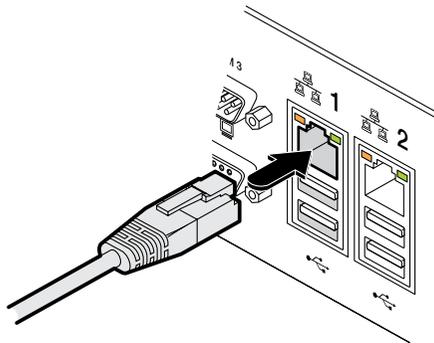
Note: If an existing A.I.M. server must be replaced, follow the important advice given within [Appendix C \(Swapping out an A.I.M. server\)](#).

Network connections

The A.I.M. server has two network connections on the rear panel, labeled **1** and **2**. These allow the unit to be connected to internal and external network connections as required. The external network connection allows admin users located away from the internal network to be able to login.

To connect the internal IP network port

- 1 Run a category 5, 5e or 6 link cable from the appropriate hub or router to the A.I.M. server unit.
- 2 Connect the plug of the link cable into the IP port labeled **1** on the rear panel of the A.I.M. server unit.



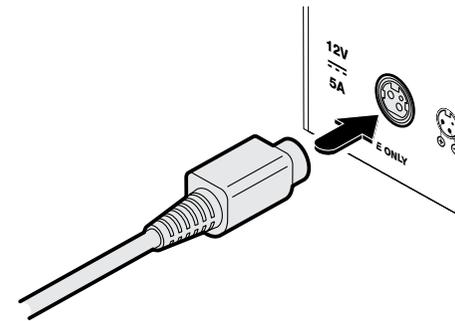
Category 5, 5e or 6 cable from LAN / network switch

Power supply connection

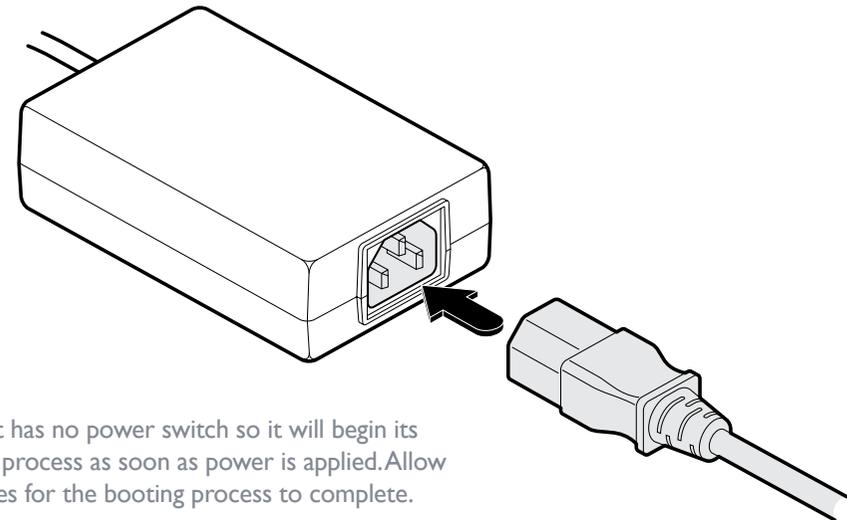
Important: Please read and adhere to the electrical safety information given within the [Safety information](#) section of this guide. In particular, do not use an unearthed power socket or extension cable.

To connect the power supply

- 1 Attach the output connector of the power supply (country specific power supplies are available) to the power input socket on the left side of the rear panel.



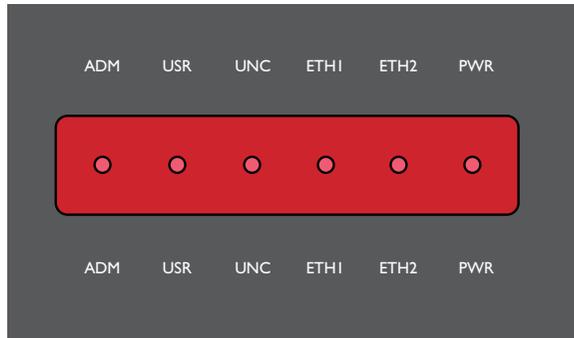
- 2 Connect the main body of the power supply to a nearby earthed mains outlet.



The unit has no power switch so it will begin its booting process as soon as power is applied. Allow 3 minutes for the booting process to complete.

FRONT PANEL INDICATORS

To assist with operational checks and troubleshooting, the front panel provides the following indicators:



- **ADM** On when an administrator is logged in. Flashes when an administrator is accessing the system.
- **USR** On if there are any connections between channels/receivers. Flashes when a user is accessing the system.
- **UNC** Unconfigured RX or TX units are online
- **ETH1** On when connected, flashes with network activity
- **ETH2** On when connected, flashes with network activity
- **PWR** On when power is applied

INSTALLATION REQUIREMENTS

- A.I.M. v2.0 or above requires all ALIF units to be at firmware version 2.0 or greater.
- A.I.M. v3.0 requires all ALIF units to be at firmware version 3.0 or greater.
- When upgrading an ALIF/A.I.M. network from firmware versions 2.0 to 3.0, proceed in the following order: First upgrade the A.I.M. to its version 3.0 firmware; it will subsequently report that it can no longer support the ALIF devices. Next upgrade the ALIF devices to their v3.0 firmware.
- On the network switch(es) that have A.I.M. server(s) attached, ensure that the [portfast](#) option is enabled on each port to which an A.I.M. unit is connected. Where portfast is not enabled, if a second A.I.M. is added for redundancy, this could result in a mis-configured back up server.
- If an existing A.I.M. server must be replaced, follow the important advice given within [Appendix C \(Swapping out an A.I.M. server\)](#).
- 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](#).

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 A.I.M. admin interface requires an A-grade browser with Javascript enabled.

The list of appropriate browsers is as follows:

- Google Chrome v7 or greater
- Firefox v3.5 or greater
- Internet Explorer v8 or greater (IE6 is not supported)
- Safari v5 or greater

IMPORTANT

The first time you log in as an admin user to a new A.I.M. server, you will be presented with the Settings page where you will need to change A.I.M.'s default IP address to one that suits your existing network configuration.

You will NOT be able to perform any other actions or navigate to any other pages within the A.I.M. admin interface until you have changed A.I.M.'s IP address.

To change the IP address, type in a new IP address in the relevant field (you should also change the gateway/netmask details for your network).

When you click Save, after a delay the web browser will automatically redirect itself to the new IP address so that you can continue administering A.I.M.

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

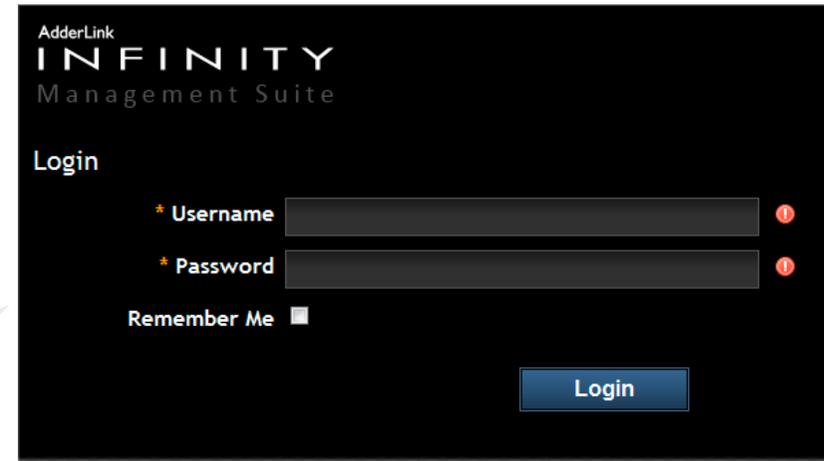
You will then be asked to login again and will have full access to all of A.I.M.'s pages.

Note: If an existing A.I.M. server must be replaced, follow the important advice given within [Appendix C \(Swapping out an A.I.M. server\)](#).

LOGIN FOR ADMIN USERS

- 1 Ensure that the A.I.M. 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 A.I.M. 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.

ADDING ADDERLINK INFINITY UNITS

When new ALIF transmitters and receivers are added to a network, they are designed to automatically announce themselves* to the A.I.M. server. Once the A.I.M. server receives their 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 A.I.M. 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 A.I.M. server upon being added to a network. Please see right for details about resetting an ALIF unit.

If an ALIF unit is not located

There are several reasons why an ALIF unit might not be located by A.I.M.:

- 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 A.I.M. 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 A.I.M. units. Check and where necessary, replace faulty cables.

Further information

Please also see:

- [Basic steps for a new configuration](#)
- [Appendix A - Tips for success when networking ALIF units](#)
- [Appendix B - Troubleshooting](#)
- [Appendix C - Redundant servers: Setting up and swapping out](#)
- [Appendix D - Glossary](#)
- [Appendix E - A.I.M. API](#)

AdderLink Infinity manual factory reset

Where a previously configured ALIF unit is being added to a network for control by an A.I.M. server, you can use this method to reset the unit to its default configuration.

To perform a manual factory reset

- 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.



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

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.

BASIC STEPS FOR A NEW CONFIGURATION

When adding and configuring new devices using an A.I.M. server, these are the basic steps that you need to take:

- 1 Add the new ALIF devices to the network and ensure that they are using a default factory configuration. If necessary, [Reset each one](#).
- 2 Ensure that the A.I.M. server is attached to the same subnet ([installing A.I.M.](#)) as the ALIF units and is powered on.
- 3 On a host computer also connected to the same subnet, use a suitable web browser to [login](#) to the A.I.M. server as the *admin* user. The default IP address for A.I.M servers is 169.254.1.3
- 4 View the [Dashboard](#) page. The ALIF units should announce themselves to the A.I.M. server and as they do so, they will be automatically added at the top of the Dashboard page.
If your ALIF units are not added to the Dashboard page, please see [If an ALIF unit is not located](#).
- 5 Either:
 - Click 'Configure' for a particular ALIF entry to deal with an individual unit in isolation, or
 - Click 'Configure all new devices' to list all units within the *Configure New Devices* page.
- 6 Within the chosen configuration page, perform the following:
 - Substitute the default IP address applied to each ALIF unit for a suitable one (e.g. 192.168.x.y) within the subnet.
 - Optionally use the *Description* and *Location* fields to add unique identifying information for each ALIF unit - this is particularly important for medium to large installations.
Note: Where necessary, click the  icon for a particular ALIF unit to flash the unit's front panel indicators to confirm its location.
 - Click the **Save** button. The new ALIF units will be restarted and will be changed to use their new IP addresses.
- 7 The new ALIF units will be added to the relevant *Transmitter* and *Receiver* pages within the A.I.M. admin view. You can now refine their configurations and organise their relationships with each other and with registered users.

Notes on Zero-config networking

- If you are using a static zero-config address, then the recommended address to be set to at initial log in is 169.254.1.1 This will avoid any potential IP address clashes.
- The AIM/ALIF network uses the following zero-config addresses by default:
 - Primary AIM server: 169.254.1.2 This is a fixed address that is always present.
 - AIM ETH1 configuration: 169.254.1.3 This is the address to use for initial login and will be changed to a permanent network address.
 - Backup AIM server: If the AIM server finds itself on the same network as an active AIM server it will take the role of a backup AIM server. In this role it will assign itself the zero-config address of 69.254.1.4
Future versions of AIM will allow for more than one backup server and will implement clustering. In such installations, the AIM servers will auto assign themselves on the even zero-config addresses:
69.254.1.2 *Master* 169.254.1.4 *First backup* 169.254.1.6 *Second backup*. etc.
 - ALIF TXs - These use the zero-config addresses of 169.254.1.31..33..35.
 - ALIF RXs - These use the zero-config addresses of 169.254.1.32..34..36.
- If there are more than 3 pairs on the network, the zero-config addresses are then randomly assigned but 169.254.1.1 would not get used.

THE DASHBOARD TAB

The Dashboard is your main point of contact for checking and changing the general status of all A.I.M. operations.

Click the DASHBOARD tab to view its initial home page.



The various other Dashboard pages (e.g. Settings, Backups, Updates, etc.) are selectable within the blue section located just below the tabs.

Dashboard > Home

- **Shutdown button** - Allows the admin user to shut down the A.I.M. server. The OSD will no longer work on Receivers. The A.I.M. server will need to be manually started again when next required.
- **Restart** - The admin user can reboot the A.I.M. server. The [OSD](#) and admin section will be unavailable while the server is rebooting. This currently takes about 75 seconds.

Within the Home page*, the different sections provide a variety of information:

- **Warning messages** - Live alerts are displayed concerning any devices that are offline, rebooting, recently added or unconfigured.
- **Latest Active Connections** - shows the five most recent active sessions, detailing for each: When the session started; which user/receiver/channel is involved; the connection type (icons show audio, video, serial, USB, exclusive) and IP addresses in use. The red unplug icon on the far right allows the admin user to disconnect a connection.
- **Event Log** - shows all actions performed by the admin or end-users within the A.I.M. system. See also the [Event Log page](#).
- **Latest Channels** - shows the last five channels created within the A.I.M. system. A channel is created by default when a new transmitter is added and configured. The edit icon next to a channel allows the admin user to configure the channel.

- **Latest User Logins** - shows the last five users who logged in (either to the A.I.M. admin or at an AdderLink Infinity Receiver).
- **Latest User Registrations** - shows the last five users added to the A.I.M. system, with a link to edit the user's details/permissions.
- **Latest Channel Changes** - shows the last five users who changed a channel, either while using the on-screen display (OSD) at an AdderLink Infinity Receiver, or via the A.I.M. admin control panel.
- **Latest Receivers Added** - shows the last five receivers to be added and configured within the A.I.M. network. Click  to configure a receiver; click  to connect to a channel; or click  to disconnect an existing connection.
- **Latest Transmitters Added** - shows the last five transmitters to be added and configured within the A.I.M. network. Click  to configure a transmitter.

*The Home page is auto-refreshed every ten seconds to ensure that the latest information is always available.

Dashboard > Settings

Click the **Settings** option below the Dashboard tab.

The Settings section contains global configuration options for the A.I.M. system and is divided into eight pages, each accessible by clicking the relevant button located below the blue options bar:



General • Transmitters • Receivers • Servers • Network • Time • Mail • Active Directory

For configuration options that affect individual receivers, users channels, etc., see the sections dealing with those tabs.

Dashboard > Settings > General



Receiver OSD Timeout

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

A.I.M. Admin Timeout

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

Anonymous User

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

Hide Dormant Devices

If enabled, devices that have been offline for more than 24 hours will be hidden.

Grant All Users Exclusive Access

Determines whether a user can connect to a channel exclusively and thus prevent any other users from also connecting to that channel. If not set, users can only connect in view-only mode or shared mode. Settings that are applied specifically to a user will override settings applied to user groups they're in, which in turn override this global setting.

Note: If a user has exclusive mode granted or NOT granted at user level, then it doesn't matter what settings there are above (usergroups or global).

- If a user is set to inherit "allow exclusive mode" from their user groups, if any one of their user groups has "allow exclusive mode" granted, then the user will have it granted, even if the rest of the user's usergroups have exclusive mode not granted.
- If a user is set to inherit "allow exclusive mode" from their user groups, and one of the user groups is set to inherit from the global setting - if that global setting is "allow exclusive mode," then effectively the user group is "allow exclusive mode," so the user will be allowed exclusive mode.

Grant All Users Remote OSD Access

If enabled, allows receivers to be switched remotely from another receiver's OSD menu.

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:

- **View only:** Allows users only to view/hear the video and audio output, the USB channel is denied.
- **View/Shared only*:** Prevents users from gaining exclusive access to a channel.
- **Shared only*:** Ensures that all connections are shared.
- **Exclusive only:** Ensures that all connections to a channel are made singularly.
- **View/Shared & Exclusive*:** Permits either type of connection to be made.

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.*

Initial Streaming Mode

All new connections are created in unicast mode in order to minimize multicast traffic on network switches that may have limited [IGMP snooping](#) capabilities. If a second receiver connects to the same channel, the unicast connection is briefly disconnected and replaced with the new multicast connection. The first-connected receiver would experience a brief screen black-out.

Selecting multicast in this option causes new connections to start directly in multicast mode so that subsequent receivers can connect to the same channel or video stream without causing any interruption to the initial video connection.

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. Note the admin configuration web pages remain in English.

Device statistics

Allows the managed devices to generate statistics. This option needs to be enabled before A.I.M. will display any statistics on its statistics page.

Debug Level

This allows information to be collected for diagnostic purposes. Do not use the full level unless advised by an Adder FAE.

API Login required

If enabled, the anonymous use of the A.I.M. API will be disallowed.

Anonymous user

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

Licence

Displays information about the number of devices that can be connected to the A.I.M. server.

Dashboard > Settings > Transmitters



This page applies a standard global configuration to all transmitters.

Magic Eye

Determines whether the Magic Eye feature should be enabled on ALIF dual (2002T) 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.

DDC

Determines whether video configuration details should be harvested from connected display screens or a static fixed EDID report should be used. Care must be taken when selecting a Dual Link Video resolution as only ALIF dual units support a 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 the ALIF dual transmitters.

Hot Plug Detect Control

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

Hot Plug Detect Signal Period

By default this is set at 25ms, 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.

Colour Depth

The color depth to use: 8, 16 or 24 bit.

The next fields are the USB settings. *Note: USB port reservation and advanced USB features will be added to future releases of the A.I.M. management system.*

USB Speed

Select Low/full speed or High speed USB operation.

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: It is not possible to reserve USB ports on the transmitter when used with A.I.M..

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.

Serial Parity, Data Bits, Stop Bits, Speed

These settings determine the default serial port configuration.

Dashboard > Settings > Receivers



This page applies a standard global configuration to all receivers.

Hotkey settings

The first few rows determine the Hotkeys that can be used to invoke certain functions. It is possible to select mouse keys to perform these functions, though it is not possible to use both mouse switching and a hot key combination. It is also not possible to mix left and right function keys. Left Ctrl and Left ALT are the default settings.

Login required

Determines whether it is necessary to log into the receiver.

Enable Receiver OSD Alerts

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

The next fields are the USB settings. *Note: USB port reservation and advanced USB features will be added to future releases of the A.I.M. management system.*

HID only

If enabled, allows only HID (mice and keyboards) devices to be connected to the receivers.

Disable Isochronous Endpoint 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.

Video Compatibility Check

This reads the EDID from the attached monitor and determines whether the monitor 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.

Receiver Keyboard Country Code

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

Audio Input Type

Select the required audio input type.

Dashboard > Settings > Servers

Receivers Servers Network

This page is used to configure redundant operation for the A.I.M. servers.

It is now possible to place two A.I.M. boxes on the same subnet. One A.I.M. box is the Primary (or Master) the other is the secondary (or Slave). If the Primary server fails for any particular reason then the Secondary will take over until the Primary is repaired. This functionality is only possible if both A.I.M. servers have an unlimited devices license and are at v3.xx.

Primary Timeout

The time (in seconds) for the Primary server to be unavailable before the secondary 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.

Require Authentication

If set to No, this allows an unauthenticated A.I.M. HTTPS server to connect to the server in order to act as a Backup. This means that A.I.M. can join the network by merely being plugged in. If set to Yes, a password is required to validate the HTTPS client for A.I.M. to A.I.M. queries.

Cluster Password

This is the password that is used for A.I.M.-to A.I.M. https queries, if the *Require Authentication* option is enabled.

Dashboard > Settings > Network

Servers Network Time

This page applies global network parameters to the A.I.M. network.

Syslog Enabled

Determines whether Syslog should be used to record log data to an external Syslog server.

Syslog IP Address

The address of the external syslog server.

Multicast IP Address

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.

IP Address Pool

To make it easier to add new devices to the network you can now specify an IP address pool that can be used. By stating the lower and upper IP addresses, all those in between will be auto assigned to the ALIF devices when they are acquired by A.I.M.

Ethernet Port 1

The IP address settings for the primary A.I.M. Ethernet port, which can only be configured on a static IP address.

Ethernet Port 2

The IP settings for Ethernet port 2 can be disabled, configured on a static IP address or DHCP used to set the IP address, as required.

Dashboard > Settings > Time



This page deals with all time related settings for the installation.

NTP Enabled

Determines whether an external Network Time Protocol server should be used to provide timing for the installation.

Date, Time, Time Zones

Use these entries to pinpoint the current time, date and location of the installation.

Dashboard > Settings > Mail



This page sets up the email functionality of the A.I.M. server if required. An external Email server is required to sit on the network if this functionality is to be used.

Mail Enabled?

Determines whether the mail features of A.I.M. should be invoked.

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.

Email Address for Alerts

Enter the email address that will be used to send alert messages.

Dashboard > Settings > Active Directory



This page sets up the active directory server, if there is one on your network, and to use active directory to maintain the user database.

AD Enabled?

Determines whether Active Directory features will be used.

Account Suffix

Enter the account suffix for your domain.

Base DN

Specify the base Distinguished Name for the top level of the directory service database that you wish to access.

Domain Controller

Enter the IP address or name of the server that holds the required directory service.

Username, Password

Enter the username and password for the domain account.

Sync Schedule

Choose the most appropriate synchronization schedule, from hourly intervals to daily or weekly.

Dashboard > Backup

You can schedule backup copies of the A.I.M. 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 A.I.M. database. Adder cannot be held responsible for any loss of data, however caused.

Backup Options

Download to your computer: If this option is checked, when you click the “Backup Now” button, the 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: 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 [Dashboard>Settings](#) page.

Note: Emailed backups are encrypted, and these backup files are automatically decrypted by the A.I.M. 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 2am (or quarter past).
- Weekly backups are executed every Sunday at 3am (or quarter past).

Restore from Server

All backups (whether initiated manually or by schedule) are saved on the server together with a time-stamp 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 A.I.M. system before restoring a previous backup. Restoring the contents of a backup file will overwrite ALL data in the A.I.M. system, with the data within the backup file. This includes configured devices, channels, users, connection logs and action logs.

Restore from File

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 A.I.M. system therefore it is advisable to make a backup of the current state of the A.I.M. system before restoring a previous backup.

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.

Download 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 A.I.M. system.

Dashboard > Updates

Upgrade AIM Software

If you have downloaded an update file for A.I.M. software, you can upload it here to the A.I.M. server and A.I.M. will automatically be upgraded to the new version. Upgrade files are encrypted and digitally-signed for A.I.M.-server integrity.

Note: It is not possible to downgrade an A.I.M. server to a previous firmware version.

Reset AIM Configuration

This option can be used to reset A.I.M. to its initial configuration, but will retain any A.I.M. software updates that have been applied. All devices, channels, presets, users, groups, backups, logs and uploaded firmware files will be removed. You are strongly advised to download a recent backup before continuing.

Upload New TX/RX Firmware

Allows you to upload a firmware file to the A.I.M. server, which can then be used to upgrade ALIF TX and RX units using the section below.

Install Firmware onto Devices

Allows you to determine the firmware file to use and which ALIF devices should be upgraded.

Upgrading firmware globally on ALIF units

This method allows the A.I.M. admin user to upgrade firmware on receivers and transmitters, wherever they are located.

- 1 Use the “Upload New TX/RX Firmware” section to place new transmitter and/or receiver firmware file(s) onto the A.I.M. server. Once uploaded, the stored firmware files are listed within the relevant “Available firmware” drop-down boxes within the sections below.
- 2 Within the “Install Firmware onto Devices” section, choose the Device Version (ALIF standard or dual model), Device Type (RX or TX) and Firmware Type (Main or Backup copies).
- 3 Click the Available firmware drop-down box and select the required new firmware version.
- 4 Click the “Install” button to apply the chosen firmware to the devices.
- 4 On the right side of the list, select the devices to which the firmware upgrade will be applied by checking boxes next to each device. The “Select All” option makes it easy to apply firmware to all devices.
- 5 Click the “Upgrade Selected..” button to create a queue of devices to be upgraded. If there are many devices to upgrade, this may take some time.

The status of devices during the upgrade process should be shown in near-real time on the receivers/transmitters pages and on the device’s own page. The page will show whether the device is still in the queue to be upgraded or if it is in the process of rebooting with the new firmware. Note that the process of applying firmware to a device and enacting a reboot takes several minutes to complete.

Dashboard > Active Connections

Shows only connections that are currently active within the A.I.M. network. Please refer to the Connection Log page section below.

Dashboard > Connection Log

Shows all connections that have occurred within the A.I.M. 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 [Dashboard > Settings](#) page). The log can be filtered to show all connections, or only currently active connections. Current connections have no “end time” and a disconnect icon ().

The “Audio Broadcast IP” and “Video Broadcast IP” columns show whether the audio and video are being sent directly from the transmitter to the receiver or broadcast to a multicast group. Direct links are denoted by the receiver’s IP address only; whereas multicast broadcasts are indicated by the multicast icon () and the common multicast IP address (the address will be in the range specified within the “Multicast IP Address” option of the Dashboard > Settings page).

Actions that you can take within this page include:

- Hover the mouse over the receiver, user or channel names to show more information about each item.
- Hover the mouse over the five “Info” icons to see descriptions (audio on/off; video on/off; USB on/off; shared/exclusive mode; serial on/off).
- Click  to end a connection between a receiver and a channel.

Dashboard > Event Log

This page lists events that have occurred within the A.I.M. system. A drop downlist box is available at the top of the page that allows you to filter log page entries to show only particular categories, as follows:

- **All:** Lists all events
- **Admin:** Lists automatic events and/or those performed by the admin user (including: backup, scheduled backup, backup restored, updating A.I.M. settings, adding/removing/updating channels/users/devices, Active Directory Sync, Firmware upgrades, A.I.M. upgrades, etc).
- **Users:** Lists events performed by regular users (including: login, logout, channel connections, disconnects, etc).
- **Login:** Lists login and logout events, whether performed via the admin console or receiver devices.
- **Channel Changes:** Lists only channel changes (connections & disconnects).
- **Device Status:** Lists new devices that are added to the A.I.M. network, get restarted/rebooted or go online/offline

You can archive Event Log data to a CSV file via the “Archive log data” link, which jumps to the relevant section within the [Dashboard > Backups](#) page.

THE CHANNELS TAB

The Channels tab 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.

Click the CHANNELS tab to view the initial View Channels page.



The various other Channels pages (e.g. Add Channel, View Channel Groups, etc.) are selectable within the blue section located just below the tabs.

Search filters

The key fields (Name, Description and Location) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click to start the search. Optionally use the buttons to invert the order of the listing.



The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "mac" in the name, and "mixed" in the description). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter, (you can also empty the search box and click again).

Channels > View Channels

This page lists all channels that currently exist within the A.I.M. system. A channel is automatically created for every transmitter when it is added and configured within the A.I.M. 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.

Within the list of channels, the Allowed Connections column indicates how each channel may be accessed by users. By default, these settings are inherited from the global setting (configurable within the [Dashboard > Settings](#) page), however, each channel can be altered as required. The icons denote the following connection rules:

- Connection details inherited from the global setting
- Shared access
- Exclusive access
- View only

The Channel Groups column shows to how many channel groups each channel belongs. The Users column indicates how many users have permission to view each channel.

Actions that you can take within this page include:

- **Create a new channel:** Click the "Add Channel" option.
- **Create a new channel group:** Click the "Add Channel Group" option.
- **Configure an existing channel:** Click for the required channel.
- **Delete a channel:** Click for the required channel.
- **View a channel group:** Click the "View Channel Groups" button.

Channels > Add or Configure a Channel

From the View Channels page, you can add a new channel or configure an existing channel:

- To create a new channel: Click the “Add Channel” option.
- To configure an existing channel: Click  for a channel.

The Add and Configure pages are similar in content.

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, Audio, USB and Serial

These drop down boxes list all of the available streams from installed transmitters. When creating a channel, you can choose to take all four 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.

Allowed Connections

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

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 setting** - uses the setting of the “Allowed Connection Modes” option within the [Dashboard > Settings](#) page.
- **View only** - allows users only to view/hear the video and audio output, the USB channel is denied.
- **View/Shared only*** - denies exclusive mode to all users.
- **Exclusive only** - forces all user connections to be exclusive only.
- **View/Shared & Exclusive*** - allows all types of connection modes.

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

Group Membership

Groups provide a quick and easy way to manage settings for channels. By making a channel part of a particular group, the channel automatically inherits the key settings of that group.

The group membership section displays existing channel groups in the left list (to which the current channel does not belong) and the channel groups in the right list to which it does belong.

To add the channel to groups: Highlight one or more (use the CTRL key if selecting more than one) group names in the left list and then click  to add the name(s) to the right list.

Note: You can also include or exclude individual channels by double clicking on them.

To add the channel to all groups: Click  to move all group names from the left to the right list.

To remove the channel from groups: Highlight one or more (use the CTRL key if selecting more than one) group names in the right list and then click  to move the name(s) back to the left list.

To remove the channel from all groups: Click  to move all group names from the right to the left list.

Permissions

This section allows you to determine which users and user groups should be given access to this channel. Individual users and user groups are handled within separate subsections, but both use the same method for inclusion and exclusion.

To include one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the left list and then click  to add them to the right list.

To include all users (or groups): Click  to move all user/group names from the left to the right list.

To remove one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the right list and then click  to move them back to the left list.

To remove all users (or groups): Click  to move all user/group names from the right to the left list.

Channels > Add or Configure Channel Group

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.

From the View Channels page, you can add a new channel group or configure an existing channel group:

- To create a new channel: Click the “Add Channel Group” option.
- To configure an existing channel: Click “the View Channel Groups” option and then click  for a group.

The Add and Configure Channel Group pages are similar in content.

Channel Group and Description

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.

Channel Group Membership

Allows you to determine which channels should be members of the group. By making a channel part of the group, each channel automatically inherits the key settings of the group.

To add a channel to the group: Highlight one or more (use the CTRL key if selecting more than one) channel names in the left list and then click  to add the name(s) to the right list.

Note: You can also include or exclude individual channels by double clicking on them.

To add all channels to the group: Click  to move all channel names from the left to the right list.

To remove a channel from the group: Highlight one or more (use the CTRL key if selecting more than one) channel names in the right list and then click  to move the name(s) back to the left list.

To remove all channels from the group: Click  to move all channel names from the right to the left list.

Permissions

This section allows you to determine which users and user groups should be given access to channels within this group. Individual users and user groups are handled within separate sub-sections, but both use the same method for inclusion and exclusion.

To include one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the left list and then click  to add them to the right list.

To include all users (or groups): Click  to move all user/group names from the left to the right list.

To remove one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the right list and then click  to move them back to the left list.

To remove all users (or groups): Click  to move all user/group names from the right to the left list.

THE RECEIVERS TAB

The Receivers tab shows a paginated table of all receiver devices within the A.I.M. network.

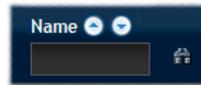
Click the RECEIVERS tab to view the initial View Receivers page.



The other Receivers pages (e.g. View Receiver Groups, Add Receiver Group, etc.) are selectable within the blue section located just below the tabs.

Search filters

The key fields (Name, Description and Location) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click to start the search. Optionally use the buttons to invert the order of the listing.



The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "mac" in the name, and "mixed" in the description). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter, (you can also empty the search box and click again).

Receivers > View Receivers

The table shows the following information for each receiver:

- Name
- IP address
- Description & Location
- Online status
- Firmware revision of receiver unit
- Manage (admin options - see below)

The Manage icons are as follows:

(Note: You can hover your mouse pointer over any icons to reveal additional information):

- Configure device:** Displays the "[Configure Receiver](#)" page.
- Reboot device:** Allows you to reboot or reset a unit to its factory settings. A popup will ask which task you wish to carry out. A reboot is useful if a device enters an unknown state. A reset will return the unit to its factory default state and reset its IP address (the unit will retain any firmware updates that have been applied).
- Identify unit:** Causes the LED lights to flash on the front of the selected unit. An alert will be shown if the unit cannot be contacted (e.g. if it is offline).
- Delete device:** Confirmation will be requested. You will need to factory-reset any devices that you wish to re-configure to work with A.I.M..
- Connect to a channel:** A list of available channels is shown, along with connection modes (view/shared/exclusive). The admin user can thus remotely change channel on any receiver.
- Disconnect:** If a receiver is currently connected to a channel, clicking the disconnect icon will end the connection, regardless of who is connected. Hovering over the icon will show which user is connected, which channel they are connected to, and when the connection was created.

Receivers > Configure Receiver

From the View Receivers page, you can configure details for a receiver:

- Click  for a receiver.

Note: If the IP address of the receiver is changed, the device will need to reboot itself.

Login Required

- **No:** 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 [Dashboard > Settings](#) page.
- **Inherit from Receiver Groups:** When selected, the requirement for user login will be determined by the “Login Required” settings within the Receiver Groups to which this unit belongs:
 - If ANY of the receiver groups (to which this receiver belongs) are set as “Login Required = Yes”, this receiver will require login.
 - If ANY of the receiver groups (to which this receiver belongs) are set as “Login Required = Inherit...” and the global setting is “login required = yes”, then this receiver will require login.
 - If ALL receiver groups (to which this receiver belongs) are set as “Login Required = No”, then this receiver will NOT require login.
- **Yes:** When selected, a user will need to login with the username and password defined in the “Users” section. They will only be allowed to login if they have been granted permission to access that particular receiver.

Receiver OSD Alerts

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

The next fields are the USB settings

Note: USB port reservation and advanced USB features will be added to future releases of the A.I.M. management system.

HID Only

If enabled, allows only HID (mice and keyboards) devices to be connected to the receivers.

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.

Audio Input Type

Select the required audio input type.

Video Compatibility Check

This reads the EDID from the attached monitor and determines whether the monitor 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.

Receiver Keyboard Country Code

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

Group Membership

To facilitate collective permission-granting for numerous receivers, a receiver can belong to one or more receiver groups. Any permissions applied to the receiver group are inherited by all receivers that are included within the receiver group. For example, multiple receivers can be made available to a user by placing them all in a receiver group and then granting the user permission to use that receiver group.

Permissions

This is hidden by default as, by default, all users have access to all receivers. You can deny access to particular receivers for a user in this section. However, be aware that users who are included within user groups may have access to the same receivers via their groups.

Receivers > Add Receiver Group or Configure Group

From the View Receiver Groups page, you can create a new group or configure an existing group:

- To create a new group: Click the “Add Receiver Group” option.
- To configure an existing group: Click  for a group.

The Add and Configure pages are similar in content.

Login Required

- **No:** 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” defined within the [Dashboard > Settings](#) page.
- **Inherit from global setting:** When selected, the requirement for user login will be determined by the “Login Required” setting within the [Dashboard > Settings](#) page.
- **Yes:** When selected, a user will need to login with the username and password defined in the “Users” section. They will only be allowed to login if they have been granted permission to access devices in the receiver group.

Enable Receiver OSD Alerts

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

The next fields are the USB settings

Note: USB port reservation and advanced USB features will be added to future releases of the A.I.M. management system.

HID Only

If enabled, allows only HID (mice and keyboards) devices to be connected to the receivers.

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.

Enable Video Compatibility Check

This reads the EDID from the attached monitor and determines whether the monitor 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.

Group Membership

This section allows you to easily include or exclude individual receivers for this group. All relevant group permissions will be applied to all receivers that are included within the group. Receivers that are not currently included in this group within the left list and those receivers that are included within the right list.

To add a receiver to this group: Highlight one or more (use the CTRL key if selecting more than one) receiver names in the left list and then click  to add the name(s) to the right list.

To add all receivers to the group: Click  to move all receiver names from the left to the right list.

To remove a receiver from the group: Highlight one or more (use the CTRL key if selecting more than one) receiver names in the right list and then click  to move the name(s) back to the left list.

To remove all receivers from the group: Click  to move all receiver names from the right to the left list.

Permissions

This is hidden by default because all users have access to all receivers. You can deny access to the receiver group, however, be aware that users who are included within user groups may have been given access to the receiver group via their user groups.

Receivers > Update Firmware

Click this option to go straight to the Dashboard > Updates page.

See [Dashboard > Updates](#) for more details.

THE TRANSMITTERS TAB

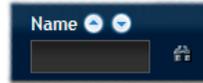
The Transmitters tab shows a paginated table of all transmitter devices within the A.I.M. network.

Click the TRANSMITTERS tab to view the transmitters page.



Search filters

The key fields (Name, Description and Location) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click  to start the search. Optionally use the   buttons to invert the order of the listing.



The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "mac" in the name, and "mixed" in the description). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter, (you can also empty the search box and click  again).

Transmitters > View Transmitters

The table shows the following information for each receiver:

- Name
- IP address
- Channels (attributed to each transmitter)
- Manage (admin options - see below)
- Online status
- Firmware revision of transmitter
- Description & Location

The Manage icons are as follows:

(Note: You can hover your mouse pointer over any icons to reveal additional information):

-  **Configure device:** Displays the "[Configure Transmitter](#)" page.
-  **Reboot device:** Allows you to reboot or reset a unit to its factory settings. A popup will ask which task you wish to carry out. A reboot is useful if a device enters an unknown state. A reset will return the unit to its factory default state and reset its IP address (the unit will retain any firmware updates that have been applied).
-  **Identify unit:** Causes the LED lights to flash on the front of the selected unit. An alert will be shown if the unit cannot be contacted (e.g. if it is offline).
-  **Delete device:** Confirmation will be requested. You will need to factory-reset any devices that you wish to re-configure to work with A.I.M.

Transmitters > Configure Transmitter

When you click  for a particular transmitter, this page lists information about the unit and allows numerous settings to be configured.

IP Address

Allows you to alter the IP address of the transmitter unit. Any change in address will be enacted when you click the “Save” button at the foot of the page. Any IP connections currently made to the transmitter will be ended.

Device Name, Description and Location

These 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.

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

Select Low/full speed or High speed USB operation.

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.

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 95%.

Video Settings

This section allows 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.

DDC

Determines whether video configuration details should be harvested from connected display screens or a static fixed EDID report should be used. Care must be taken when selecting a Dual Link Video resolution as only ALIF dual units support a 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 the ALIF dual transmitters.

Hot Plug Detect Control

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

Hot Plug Detect Signal Period

By default this is set at 25ms, 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.

Colour Depth

This parameter determines the number of bits required to define the color of every pixel. The maximum (and default) value is ‘24 bit’. By reducing the value you can significantly reduce bandwidth consumption, at the cost of video color reproduction. Options: 24 bit, 16 bit or 8 bit.

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.

Transmitters > Update Firmware

Click this option to go straight to the Dashboard > Updates page. See [Dashboard > Updates](#) for more details.

Transmitters > Configure New Transmitter

This page is displayed whenever a new transmitter is added to the network.

The IP Address 1 field, showing 0.0.0.0, is for an unconfigured device on its zero config address. Before A.I.M. can add the device into its database, a new IP address must be added to IP Address 1. This is the system IP address and applies equally for ALIF (1000 series) and ALIF dual (2000 series).

ALIF dual units have a Teaming port which provides a second 1 Gigabyte link port which can be used for bandwidth doubling and/or redundancy. The IP address 2 field is for the Teaming port. In order to use the Teaming port, IP address 2 field must be given a valid IP address. For ALIF (1000) units, this field will remain blank.

THE SERVERS TAB

The Servers tab shows a table of all servers within the A.I.M. network.

Click the SERVERS tab to view the page.



For installations that require greater redundancy, it is possible to have two AIM servers running on the same subnet. If the primary server fails then a secondary server with the same database can take over until the primary unit recovers.

Each server entry will have one of four possible states within the *Rôle* column:

- **Unconfigured** The server is a factory fresh device or has performed a full factory reset. This does not yet have a proper role.
- **Solo** This is a server acting as a standalone A.I.M. All A.I.M. servers with firmware below 3.0 will be in this state. If there is only going to be one A.I.M. on the subnet, this is the Role that will be used.
- **Primary** The server is configured as a fully functional A.I.M. from which a back-up server can be slaved.
- **BackUp** This server is configured to serve as a back up to the Primary.

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

- **Active** This server is functioning as an A.I.M. server and is administering ALIF devices. Primary or Solo servers with this status are fully functional A.I.M. 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.
- **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.

Servers > Configure Server

When you click  for a particular server, this page lists information about the unit and allows several basic settings to be configured.

Rôle

Allows you to change the server's function between primary and solo (see descriptions left).

Device Name, Description and Location

These are useful identifiers for the server unit and its exact location. These become even more valuable as the number of servers within the system increases.

For details about setting up server redundancy, please see [Appendix C - Redundant servers: Setting up and swapping out.](#)

THE USERS TAB

The Users tab shows a paginated table of all users within the A.I.M. network. Within the list, the admin user is always present and cannot be deleted - in order to avoid being locked out of the A.I.M. system. The username and name details of the admin account, however, can be edited as required.

Click the USERS tab to view the initial View Users page.



The other user pages (e.g. Add User, View User Groups, etc.) are selectable within the blue section located just below the tabs.

Search filters

The key fields (Username, First Name and Last Name) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click to start the search. Optionally use the buttons to invert the order of the listing.



The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "B" in the Username, and "Smith" in the Last Name). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter, (you can also empty the search box and click again).

Users > View Users page

The table shows the following information for each user:

- AD - indicates whether the user was imported from Active Directory
- Username
 - First Name
 - Last Name
- User Groups - the number of user groups to which the user belongs
- Channels - the number of channels to which the user has access
- Receivers - the number of receivers to which the user has access
- Allow Exclusive? - indicates whether the user is permitted to access channels in exclusive mode (✓ - Yes, ✗ - No, - Inherited setting from user groups)
- Suspended - indicates the user account status (✓ - User is suspended, ✗ - User account is active, i.e. not suspended)
- AIM Admin - indicates whether the user has admin privileges

The Edit option icons are as follows:

- Configure user:** Displays the "Configure User" page.
- Clone user:** Create a complete copy of the currently selected user entry.
- Delete user:** Confirmation will be requested.

Users > Add User or Configure User page

From the View Users page, you can add a new user or configure an existing user:

- To add a user: Click the “Add User” option.
- To configure an existing user: Click  for a user.

The Add and Configure pages are similar in content.

Username

The username is mandatory and must be unique within the A.I.M. 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 A.I.M. the next time a sync takes place with Active Directory.

First Name, Last Name and Email

The First Name, Last Names 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.

Require Password?

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

Password

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

AIM Admin?

When set to Yes, the user is granted privileges to login to the A.I.M. admin system and make changes.

Account Suspended?

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

Allow Exclusive Mode?

Defines whether the user is able to connect to channels exclusively (preventing other users from sharing the connection). 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 exclusively, then the user will have permission to connect exclusively. *Note: It is an additional requirement that the channel being accessed by the user, must also permit exclusive access.*

Enable Remote OSD?

Supported in firmware v3.0 or greater. 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.

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. User groups to which the user is not currently a member are shown in the left list and those to which the user is a member are shown within the right list. See [Including and excluding a user..](#) on the next page for details about including and excluding group membership.

Permissions

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

See [Including and excluding a user...](#) on the next page for details about including and excluding channels and/or channel groups.

Receiver and Receiver Group Permissions

Receiver and Receiver Group Permissions are hidden by default because 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 by revealing this section.

Users > Add User Group or Configure Group page

From the View User Groups page, you can create a new group or configure an existing group:

- To create a new group: Click the “Add User Group” option.
- To configure an existing group: Click  for a group.

The Add and Configure pages are similar in content.

User Group Name

The User Group name must be unique within the A.I.M. installation.

Allow Exclusive Mode?

Defines whether the users within the group will be able to connect to channels exclusively (preventing other users from sharing the connection). When this is set to “Inherit from global setting”, the setting for the “Grant all users exclusive access” option (within [Dashboard > Settings](#)) will be applied. *Note: The final arbiter of whether any user can gain exclusive access is always whether the channel being accessed is also set to allow exclusive 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.

Group Membership

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. See [Including and excluding a user...](#) on the right for details about including and excluding group membership.

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.*

See [Including and excluding a user...](#) right for details about including and excluding channels and/or channel groups.

Receiver and Receiver Group Permissions

Receiver and Receiver Group Permissions are hidden by default because 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 by revealing this section.

Including and excluding a user within group or channels

The Group Membership and Permissions section use the same method to determine inclusion and exclusion:

To add the user to a group or grant access to a channel: Highlight one or more (use the CTRL key if selecting more than one) of the entries in the left list and then click  to add them to the right list (you can also double-click on an entry to quickly add it).

To add the user to all groups or grant access to all channels: Click  to move all entries from the left to the right list.

To remove the user from a group or channel: Highlight one or more (use the CTRL key if selecting more than one) entries in the right list and then click  to move them back to the left list (you can also double-click on an entry to quickly remove it).

To remove the user from all groups or channels: Click  to move all entries from the right to the left list.

Users > Active Directory

To simplify integration alongside existing systems within organisations, A.I.M. 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 the [Dashboard > Settings](#) page. Once configured, the Users > Active Directory page (called “Import Users from Active Directory”) will allow you to scan the AD server for a list of folders and users/groups within those folders.

Choosing users and groups

Once scanned, the “Import Users from Active Directory” page shows all folders that are available on the AD server.

- 1 Use the “Include Users” and “Include Groups” checkbox columns on the right hand side of the folder lists to select which items to import (with optional additional LDAP filters where necessary).
 - If an AD user was not in the A.I.M. user database, they will be imported.
 - If an AD user is already in the A.I.M. 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 A.I.M. user database, they will be removed from the A.I.M. user database during the sync operation.
IMPORTANT: It is thus vital to ensure that all users you want in the A.I.M. system are always selected for import/sync, otherwise they will be removed.
- 2 Choose the required “Re-Synchronize” interval. Choices are Never, Hourly, Daily or Weekly.
- 3 You can choose to synchronize immediately or to preview the results of your settings:
 - Click the “Preview” button to view the list of users that will be added/updated/removed on this synchronization. Once previewed, you can either go ahead with the sync or return to the filter page and edit your settings.
 - Click the “Save & Sync” button to synchronize the selected items into the A.I.M. user database.

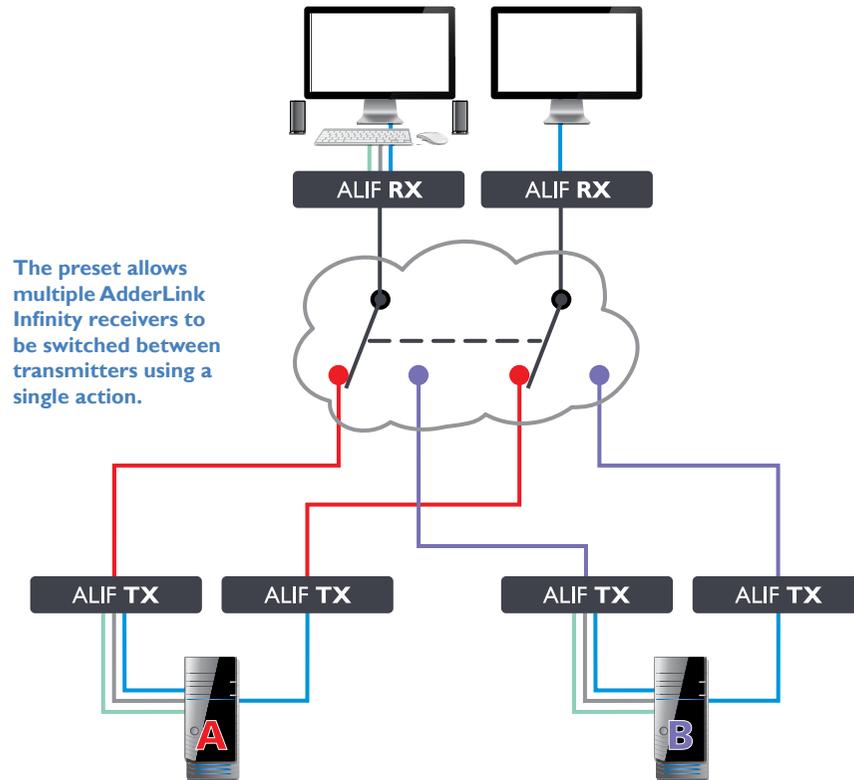
Note: A.I.M. will only import folders/groups/users up to the limit set by the AD server. There is a known issue: A.I.M. can only import x users/groups from AD where x is the limit set on the AD server. Any users/groups beyond this limit will not be imported.

Active Directory Tips

- A backup schedule is recommended so that any changes on the AD server are carried across to the A.I.M. 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 A.I.M. access, without having to make complicated LDAP filters, simply edit the A.I.M. user to be suspended (see [Users > Add User or Configure User page](#)). 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 A.I.M. 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).
- 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 A.I.M. 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 A.I.M. user list.

THE PRESETS TAB

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, such as in the example below where multiple video heads need to be switched in unison between different server systems.



The preset allows multiple AdderLink Infinity receivers to be switched between transmitters using a single action.

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 Presets page is where the admin user can create and configure new and existing presets.

Click the PRESETS tab to view the Presets page.



The nature of each preset, i.e. which receiver connects to which channel(s), is defined by the admin. The permitted connection modes are worked out according to:

- The topology of the preset, AND
- The current connections within the A.I.M. network.

For instance, if two receivers in a preset are configured to connect to the same channel (multicast), it will not be possible to connect to the preset in exclusive mode.

The presets table shows the preset name, description, allowed connection modes, and number of receiver-channel pairs in the preset.

If any preset-pairs are misconfigured (e.g. a channel no longer exists), a warning triangle will appear. The preset will NOT be usable if any receiver-channel pairs are misconfigured.

The admin user can connect any presets using the standard view/shared/exclusive buttons.

Note: There are no permissions to set for a preset. Instead, a preset will only be available to users who have permission to use ALL receivers and channels within the preset. In other words, permissions on the preset are implied by the permissions on the preset's contents.

continued

Presets > Add or Configure Presets page

From the Presets page, you can add a new preset or configure an existing preset:

- To create a new preset: Click the “Add Preset” option.
- To configure an existing preset: Click  for a preset.

The Add and Configure pages are similar in content.

Preset Name and Description

The Preset Name is mandatory, whereas the Description is optional but recommended when numerous presets will be used. A consistent naming and description policy is particularly useful in large installations.

Receiver - Channel Pairs

Pair 1

From the two drop down lists, choose a receiver and a corresponding channel for it to connect with. This base pair can be altered but cannot be deleted from the preset.

Add another pair

Click this link to define another receiver/channel pairing.

Note: While channels can be assigned to multiple receivers, each receiver may only appear once within a single preset.

Allowed Connections

Choose one of the following connection rules to be applied to the preset:

- Inherit from global setting   
- View only 
- View/Shared only  
- Shared only 
- Exclusive only 
- View/Shared & Exclusive   

Note: If multicasting is present (e.g. two or more receivers connected to the same channel or two channels containing the same audio/video end point), it will not be possible to choose the ‘Exclusive only’ connection mode.

THE STATISTICS TAB

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

Click the STATISTICS tab to view the page.



To view statistics

- 1 Choose the unit(s). From the displayed list of all ALIF transmitters and receivers on the network, place a tick against one or two units that you wish to view and click Submit.
- 2 Choose the data series for the chosen ALIF units. From the displayed list of data series, place a tick against the items from the three groups (bandwidth, packet count and frame count) that you wish to view and click Submit.

A dynamic graph will be displayed showing the chosen data series for the selected ALIF units.

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 Dashboard > Settings > Receivers page).

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 Login 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 standard shortcuts are available for use with the Local OSD (and [Remote OSD](#)). These default hotkey combinations can be altered within the Dashboard > Settings > Receivers page.

- 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 + **V**: Change the current connection to the view-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

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

- 1 Click the  icon next to the required channel or preset.
- 2 Click the **SAVE**  button at the top of the page.

To display favorites

The star shown at the top of the channel list has three appearances to represent the three display modes. Click the star to change the mode:

-  Currently showing all channels/presets.
-  Currently showing only favorites.
-  Currently showing only numbered shortcuts.

To create a new hotkey shortcut

- 1 Click the  icon next to the required channel or preset. The screen will list the ten hotkey slots, with any available slots listed as EMPTY. Click the number prefix (from 1 to 0) of an available slot.

Note: To remove a previous channel from a slot, click the  icon on the right side of the slot.

- 2 You will now be asked to choose which mode should be used to access the channel when using this shortcut. Select *View Only*, *Shared* or *Exclusive*, as appropriate.
- 3 Click the **SAVE**  button at the top of the page. As mentioned above, you will now be able to access the chosen channel by using the hotkeys (Left Ctrl + Left Alt, as standard) plus the number that you assigned to it.

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 blue 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 icon in the top right corner.

Favorites icons

- Currently showing all channels/presets
- Currently showing only favorites
- Currently showing only numbered shortcuts
- Click to add this channel as a favorite
- This channel is a numbered shortcut

Sorting icons

- Currently showing channels and presets. Click to change
- Currently showing only channels. Click to change
- Currently showing only presets. Click to change
- Filter this column using the specified term
- Remove the search filter
- Click to sort the list in ascending order via this column
- The list is sorted in ascending order via this column



Click to Logout

Top corner icons

- Enter '[Remote OSD](#)' mode
- Exit 'Remote OSD' mode
- Display the help pages
- Exit from the help pages
- Refresh the current page
- Close the OSD

Click to change to other list pages

Connection buttons

- | View only mode | Shared mode | Exclusive mode | < There are three connection modes |
|----------------|---|----------------|---|
| | | | Click to connect to the channel/preset |
| | | | You are currently connected to the channel/preset |
| | | | Another user is connected to the channel/preset |
| | | | You are unable to connect to the channel/preset |
| Blank | Connection mode not permitted by admin (e.g. a channel doesn't allow exclusive connections or a user doesn't have exclusive rights) | | |
| | End this connection | | |

Using the Remote OSD feature

The Remote OSD feature allows authorized users to access and take control of AdderLink Infinity 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 the following:

- The A.I.M. server(s) and all ALIF units must have firmware version 3.0 or greater.
- 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 AdderLink Infinity receiver, press the hotkey combination **Ctrl-Alt-C** to display the [Local OSD](#) login screen.

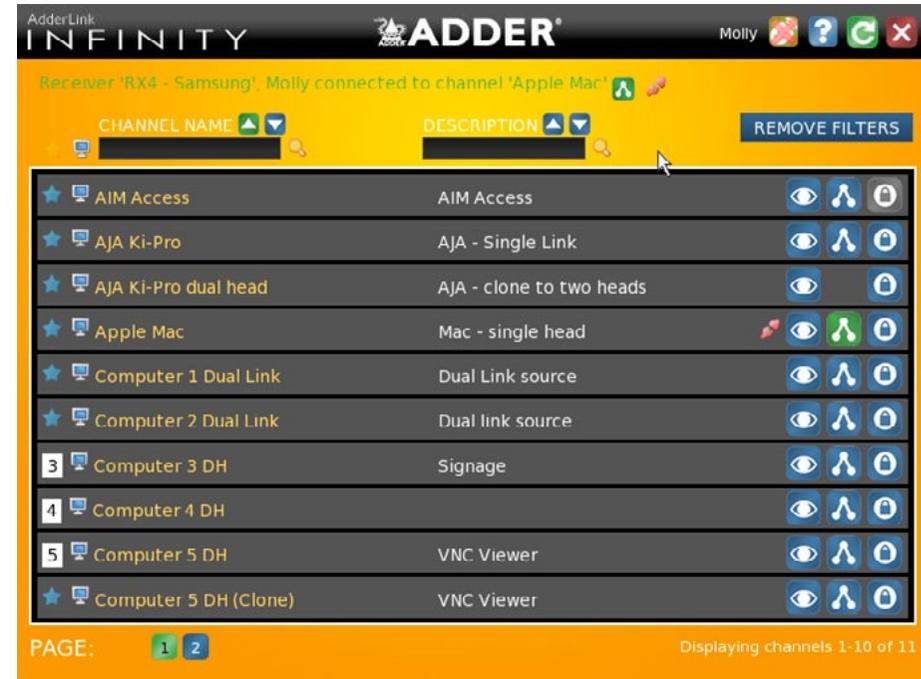
2 If required, enter your Username and Password and click the Login button.

3 In the top right corner, click the 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 background 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 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 icon in the top right corner.

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

- Getting assistance - see right
- [Appendix A](#) - Tips for success when networking ALIF and A.I.M. units
- [Appendix B](#) - Troubleshooting
- [Appendix C](#) - Redundant servers: Setting up and swapping out
- [Appendix D](#) - Glossary
- [Appendix E](#) - A.I.M.API
- [Safety information](#)
- [Warranty](#)
- [Radio frequency energy statements](#)

GETTING ASSISTANCE

If you are still experiencing problems after checking the information contained within this guide, then we provide a number of other solutions:

- **Online solutions and updates** – www.adder.com/support
Check the Support section of the adder.com website for the latest solutions and firmware updates.
- **Adder Forum** – forum.adder.com
Use our forum to access FAQs and discussions.
- **Technical support** – www.adder.com/contact-support-form
For technical support, use the contact form in the Support section of the adder.com website - your regional office will then get in contact with you.

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](#).

Layer 2 (and 3) switches known to work

- | | | |
|--------------|-------------------------|---|
| • Cisco 2960 | • Extreme Networks X480 | • HuaWei Quidway s5328c-EI (Layer 3 switch) |
| • Cisco 3750 | • HP Procurve 2810 | |
| • Cisco 4500 | • HP Procurve 2910 | |
| • Cisco 6500 | • H3C 5120 | |

For the latest list of switches known to work with ALIF and setup instructions for them, please go to www.adder.com

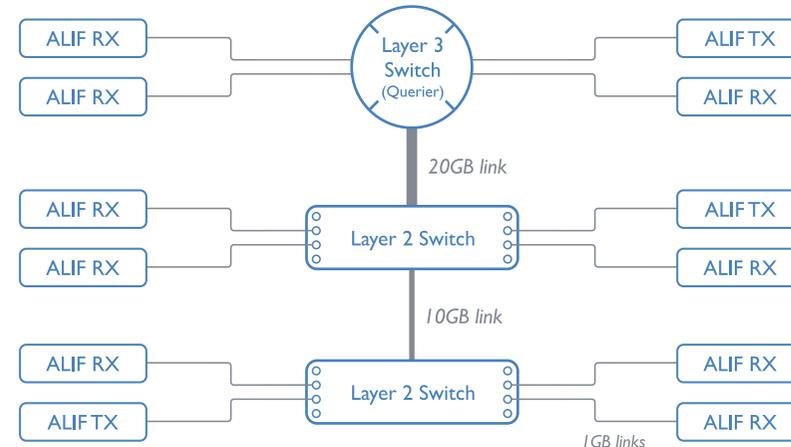
Creating an efficient network layout

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.
- Keep the distances between the switches as short as possible.
- Ensure sufficient bandwidth between switches to eliminate bottlenecks.
- Where the A.I.M. server is used to administer multiple ALIF transceivers, ensure the A.I.M. 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:



- 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](#) (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 color quality is important, then leave Colour Depth at 24 bits and adjust other controls,
 - 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.

- Ensure that all ALIF units are fully updated to the latest firmware version (at least v2.1).

APPENDIX B - Troubleshooting

Problem:The video image of the ALIF receiver shows horizontal lines across the screen.

This issue is known as *Blinding* because the resulting video image looks as though you're viewing it through a venetian blind.

When video is transmitted by ALIF units, the various lines of each screen are divided up and transmitted as separate data packets. If the reception of those packets is disturbed, then blinding is caused. The lines are displayed in place of the missing video data packets.

There are several possible causes for the loss of data packets:

- Incorrect switch configuration. The problem could be caused by multicast flooding, which causes unnecessary network traffic. This is what IGMP snooping is designed to combat, however, there can be numerous causes of the flooding.
- Speed/memory bandwidth issues within one or more switches. The speed and capabilities of different switch models varies greatly. If a switch cannot maintain pace with the quantity of data being sent through it, then it will inevitably start dropping packets.
- One or more ALIF units may be outputting Jumbo frames due to the video resolution (2048 horizontal pixels) being used. If jumbo frames are output by an ALIF unit, but the network switches have not been configured to use jumbo frames, the switches will attempt to break the large packets down into standard packets. This process introduces a certain latency and could be a cause for dropped packets.
- One or more ALIF units may be using an old firmware version. Firmware versions prior to v2.1 exhibited an issue with the timing of IGMP join and leave commands that caused multicast flooding in certain configurations.

Remedies:

- Ensure that [IGMP snooping](#) is enabled on all switches within the subnet.
- Where each ALIF unit is connected as the sole device on a port connection to a switch, enable [IGMP Fast-Leave \(aka Immediate Leave\)](#) to reduce unnecessary processing on each switch.
- Check the video resolution(s) being fed into the ALIF transmitters. If resolutions using 2048 horizontal pixels are unavoidable then ensure that [Jumbo frames](#) are enabled on all switches.
- Check the [forwarding mode](#) on the switches. If *Store and forward* is being used, try selecting *Cut-through* as this mode causes reduced latency on lesser switch designs.
- Ensure that one device within the subnet is correctly configured as an [IGMP Querier](#), usually a multicast router.
- Ensure that the firmware in every ALIF unit is version 2.1 or greater.
- Try adjusting the transmitter settings on each ALIF to make the output data stream as efficient as possible. See [Alter ALIF transmitter video settings if necessary](#) for details.

Problem:The audio output of the ALIF receiver sounds like a scratched record.

This issue is called Audio crackle and is a symptom of the same problem that produces blinding (see left). The issue is related to missing data packets.

Remedies:

As per blinding discussed previously.

continued

Problem:A.I.M. 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 A.I.M. discovery. If you have a working network of ALIF's without A.I.M. and then add A.I.M. to the network A.I.M. 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 A.I.M. 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 A.I.M. server are located within the same subnet. A.I.M. 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 A.I.M. is attempting to locate ALIF units.

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 Nvidia graphics** - Use the Adder utility for Macs (contact technical support).
- **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.

APPENDIX C - Redundant servers: Setting up and swapping out

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

- Setting up A.I.M. server redundancy - below
- Swapping out an A.I.M. server - on [next page](#)

Setting up A.I.M. server redundancy

This section details the steps required to successfully configure two A.I.M. units as primary and secondary servers.

- 1 First determine the password requirements for A.I.M. servers. Access the Dashboard > Settings page and click Servers button. Set the *Require Authentication* option as required. If set to No, then new servers can join the network as soon as they are plugged in. If set to Yes, you will need to enter a *Cluster Password* in the field below and this must be set on every A.I.M. server.
- 2 Within the main Servers tab, choose the A.I.M. unit that you wish to use as the primary server.
- 3 Click  for the chosen A.I.M. server to display the Configure Server page and change the *Rôle* entry to **primary** and click Save.
- 4 Add the new secondary A.I.M. server to the network. This unit must have its factory default settings in place. The new server should 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 secondary server should be added to the list on the main Servers tab. Its *Rôle* will be shown as *backup* and its Status as *standby*.
Note: If the transfer of the backup database is interrupted and only a partial database is transferred, then the problem will be reported within the management server page. If this occurs, it will not be possible to log in to the backup database and the firmware version of the backup will be reported as V. After five minutes, you should be given the options of Reboot and Factory Reset. Choose the factory reset option in order to clear this issue.
- 6 You can now configure the secondary server in either of two ways:
 - Click the  icon to configure the server remotely from the primary server.
 - Click the  icon to open a restricted page in order to configure the server directly from its own IP address. If you use this option, the configuration options are limited to: *view the logs; update/reset AIM and configure this server.*

Swapping out an A.I.M. server

Once ALIF devices have been configured to run with an A.I.M. server, their default IP addresses are automatically changed as part of the installation process. In this state the ALIF devices become undetectable to any new A.I.M. server that does not have access to the database of devices. Therefore, if an existing A.I.M. server needs to be replaced within an installation, follow one of the basic procedures given here to smooth the transition.

The correct procedure to use depends on whether you are using a solo A.I.M. server (firmware versions below 3.0 can only be used as solo servers) or a pair of A.I.M. servers in a primary/backup redundancy arrangement:

For solo A.I.M. servers (and those with firmware below v3.0)

- 1 Before connecting the new A.I.M. server to the main network, [connect](#) the new A.I.M. 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 A.I.M. server management suite.
- 3 Ensure that the new A.I.M. server is running the same firmware version as the one being replaced ([upgrade](#) if necessary). The firmware version is shown in the top right hand corner of every page of the management suite (just below the Adder logo).
- 4 [Set the IP address](#) of the new A.I.M. server to match that of the original unit.
- 5 [Restore a backup file](#) of the original A.I.M. server database to the new device.
- 6 Remove the original A.I.M. server from the network. Connect the new A.I.M. server in its place and power up.

The replacement unit should now work directly with the installed ALIF units.

For dual A.I.M. installations using redundancy

The correct procedure depends on which A.I.M. server has failed:

Primary server failure

- 1 Promote the backup server to be the primary server.
- 2 Replace the faulty primary A.I.M. server with a replacement unit.
If the replacement A.I.M. server has a firmware version below 3.0 then contact it on the 169.254.1.3 address and [upgrade](#) to 3.0. After the upgrade, reboot the unit.
- 3 The replacement server should begin communicating with primary server and download the database so that it can operate as the backup server.

Backup server failure

- 1 Replace the failed backup server with a new unit that has firmware version 3.0 or greater and has its default factory settings in place.
- 2 The replacement server should begin communicating with primary server and download the database so that it can operate as the backup server.

Starting from scratch

If none of the above procedures are used, then the following will be necessary. This will require a certain amount of effort because each ALIF unit must be visited and reset, plus the A.I.M. database will need to be fully reconfigured.

- 1 Place a new A.I.M. 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 A.I.M. server.
- 2 Use a computer connected to the same network to [login](#) to the new A.I.M. server management suite and begin to recreate the database of devices and users.

APPENDIX D - 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** 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 on any switch to switch connections as this will result in bridging loops.

ALIF transmitter video settings

Each ALIF transmitter includes controls to help you customize how video data is transmitted. When configured correctly for the application, these can help to increase data efficiency.

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.

Colour Depth

This parameter determines the number of bits required to define the color of every pixel. The maximum (and default) value is '24 bit'. By reducing the value you can significantly reduce bandwidth consumption, at the cost of video color reproduction.

Peak Bandwidth Limiter

The transmitter will employ a 'best effort' strategy in sending video and other data over the IP network. This means it 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.

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.

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:

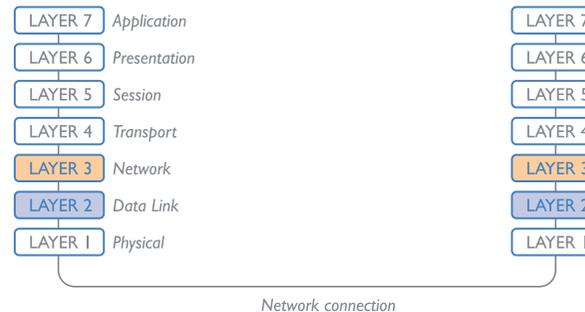
- **Store and forward** is the original method and requires the switch to save each entire data packet to buffer memory, run an error check and then forward if no error is found (or otherwise discard it).
- **Cut-through** was developed to address the latency issues suffered by some store and forward 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.

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 E - A.I.M.API

The A.I.M.API provides access for external applications to key routines used within the A.I.M. server. This appendix provides a reference to the available methods.

API version: 2

Changelog

- v2 (A.I.M. v2.3) - added *get_devices*, *get_channels*, *connect_channel*, *disconnect_channel*. Updated version compatibility information.
- v1 (A.I.M. v1.3) - added *login*, *logout*, *get_presets*, *connect_preset*, *disconnect_preset*

Methods

login	(http://<A.I.M..ip.address>/api/#login)
logout	(http://<A.I.M..ip.address>/api/#logout)
get_devices	(http://<A.I.M..ip.address>/api/#get_devices)
get_channels	(http://<A.I.M..ip.address>/api/#get_channels)
get_presets	(http://<A.I.M..ip.address>/api/#get_presets)
connect_channel	(http://<A.I.M..ip.address>/api/#connect_channel)
connect_preset	(http://<A.I.M..ip.address>/api/#connect_preset)
disconnect_channel	(http://<A.I.M..ip.address>/api/#disconnect_channel)
disconnect_preset	(http://<A.I.M..ip.address>/api/#disconnect_preset)

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 A.I.M. 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 A.I.M.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 function can be used until the logout function is called.

Input parameters:

- token
- v (the A.I.M.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>
```

get_devices

This method was last updated in API version 2, and is compatible with API requests from version 2 onwards.

This function returns a list of devices.

Input parameters:

- token
- v (the A.I.M.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)
- sort (Optional. Sort results by 'name'/'description'/'location'. Default = 'name')
- sort_dir (Optional. Sort direction for results 'asc'/'desc'. Default = 'asc')
- status (Optional. ',outdated_A.I.M._ip','rebooting','offline','outdated_firmware','invalid_backup_firmware','rebooting','upgrading_firmware','backup_mode')
- 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

continued

get_devices (continued)

- for each device:

- attribute: item (e.g. 17th device)
- d_id (device id)
- d_mac_address (device MAC address)
- d_name (device name)
- d_description (device description)
- d_location (device location)
- d_online (0 = offline, 1 = online, 2 = rebooting, 3 = factory_resetting, 4 = firmware_upgrading, 6 = running backup firmware)
- d_type (rx, tx)
- d_version (1 = Infinity ALIF 1000, 2 = Infinity Dual ALIF 2000/2002/2112)
- d_variant ('', 'b' = ALIF 2002, 'v' = ALIF 2112)
- d_ip_address
- 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 A.I.M. network e.g. 2012-07-13 22:17:22)

The following property is only returned for transmitters:

- count_transmitter_channels (the number of channels containing this transmitter)

The following properties are only returned for receivers:

- 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)
- con_exclusive (0/1 - if the last connection is/was in exclusive mode)
- con_control (0/1 - if the last connection has/had USB enabled)
- 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_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_mac_address>00:0F:58:01:6E:3D</d_mac_address>
      <d_name>RX 123</d_name>
      <d_online>1</d_online>
      <d_type>rx</d_type>
      <d_version>2</d_version>
      <d_variant></d_variant>
      <d_ip_address>10.10.10.66</d_ip_address>
      <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>
      <con_exclusive>0</con_exclusive>
```

continued

get_devices (continued)

```

    <con_control>I</con_control>
    <con_start_time>2012-09-07 13:33:19</con_start_time>
    <con_end_time/>
    <u_username>admin</u_username>
    <u_id>I</u_id>
    <c_name>Channel I</c_name>
    <count_receiver_groups>I</count_receiver_groups>
    <count_users>I</count_users>
    <custom_settings>0</custom_settings>
  </device>
</devices>
</api_response>

```

```

<api_response>
  <version>2</version>
  <timestamp>2012-09-12 14:56:11</timestamp>
  <success>I</success>
  <page>I</page>
  <results_per_page>I</results_per_page>
  <total_devices>I</total_devices>
  <count_devices>I</count_devices>
  <devices>
    <device item="1">
      <d_id>64</d_id>
      <d_mac_address>00:0F:58:01:56:85</d_mac_address>
      <d_name>TX 456</d_name>
      <d_online>0</d_online>
      <d_type>tx</d_type>
      <d_version>I</d_version>
      <d_variant></d_variant>
      <d_ip_address>1.1.201.31</d_ip_address>
      <d_description></d_description>
      <d_location></d_location>
      <d_configured>I</d_configured>
      <d_valid_firmware>I</d_valid_firmware>

```

```

    <d_valid_backup_firmware>I</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>
    <count_transmitter_channels>3</count_transmitter_channels>
    <custom_settings>0</custom_settings>
  </device>
</devices>
</api_response>

```

get_channels

This method was last updated in API version 2, and is compatible with API requests from version 2 onwards

This simple function returns a list of channels available to the authenticated user, for a specific receiver.

Input parameters:

- token
- v (the A.I.M. 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)
- count_channels - the number of channels on this page, available to the authenticated user

continued

get_channels (continued)

- 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_favourite (true if this channel is in the user's favourites, 0-9 if it's a numbered shortcut)

- view_button (disabled/enabled/hidden - whether the user can connect to the preset in view-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)

- exclusive_button (disabled/enabled/hidden - as above, but in exclusive mode)

Examples

Input:

```
/api/?v=2&method=get_channels&token=xxxxx
```

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>
```

```
<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>disabled</view_button>
```

```
<shared_button>enabled</shared_button>
```

```
<exclusive_button>hidden</exclusive_button>
```

```
</channel>
```

```
</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 function returns a list of presets available to the authenticated user.

Input parameters:

- token
- v (the A.I.M. 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))
 - count_active_cp (the number of channel-receiver pairs in this preset that are already connected)
 - connected_rx_count (the number of receivers in this preset that are already connected)
 - view_button (disabled/enabled/hidden - whether the user can connect to the preset in view-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)
 - exclusive_button (disabled/enabled/hidden - as above, but in exclusive 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/>
    <count_active_cp/>
    <connected_rx_count>1</connected_rx_count>
    <view_button>disabled</view_button>
    <shared_button>disabled</shared_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/>
    <count_active_cp/>
    <connected_rx_count/>
    <view_button>enabled</view_button>
    <shared_button>hidden</shared_button>
    <exclusive_button>hidden</exclusive_button>
  </connection_preset>
</api_response>
```

connect_channel

This method was last updated in API version 2, and is compatible with API requests from version 2 onwards

This simple function connects a receiver to a channel.

Input parameters:

- token
- v (the A.I.M.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_receivers)
- view_only (optional, 0/1 - defaults to 0)
- exclusive (optional, 0/1 - defaults to 0)

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=2&method=connect_channel&token=xxxxx&c_id=1&rx_id=2&exclusive=1
```

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 - exclusive connection not available</msg>
    </error>
  </errors>
</api_response>
```

connect_preset

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards

This simple function connects all channel-receiver pairs in a preset.

Input parameters:

- token
- v (the A.I.M.API version this request is designed for)
- id - the ID of the preset (acquired from get_presets)
- view_only (optional, 0/1 - defaults to 0)
- exclusive (optional, 0/1 - defaults to 0)
- 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 (optional, if anything went wrong with connecting the presets)

Examples

Input:

```
/api/?v=1&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>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 function disconnects a receiver, a number of receivers, or all connected receivers.

Input parameters:

- token
- v (the A.I.M. 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&rx_id=1  
/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1,2,3  
/api/?v=2&method=disconnect_channel&token=xxxxx&force=1
```

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 function disconnects all channel-receiver pairs in a preset, or disconnects ALL connections in the whole A.I.M. network.

Input parameters:

- token
- v (the A.I.M. 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>
```

SAFETY INFORMATION

- For use in dry, oil free indoor environments only.
- Warning - live parts contained within power adapter.
- No user serviceable parts within power adapter - do not dismantle.
- Plug the power adapter into a socket outlet close to the module that it is powering.
- Replace the power adapter with a manufacturer approved type only.
- Do not use the power adapter if the power adapter case becomes damaged, cracked or broken or if you suspect that it is not operating properly.
- Do not attempt to service the unit yourself.
- Not suitable for use in hazardous or explosive environments or next to highly flammable materials.
- Do not use the power adapter if the power adapter case becomes damaged, cracked or broken or if you suspect that it is not operating properly.
- If you use a power extension cable, make sure the total ampere rating of the devices plugged into the extension cable do not exceed the cable's ampere rating. Also, make sure that the total ampere rating of all the devices plugged into the wall outlet does not exceed the wall outlet's ampere rating.
- The power adapter can get warm in operation – do not situate it in an enclosed space without any ventilation.

WARRANTY

Adder Technology Ltd warrants that this product shall be free from defects in workmanship and materials for a period of two years from the date of original purchase. If the product should fail to operate correctly in normal use during the warranty period, Adder will replace or repair it free of charge. No liability can be accepted for damage due to misuse or circumstances outside Adder's control. Also Adder will not be responsible for any loss, damage or injury arising directly or indirectly from the use of this product. Adder's total liability under the terms of this warranty shall in all circumstances be limited to the replacement value of this product.

If any difficulty is experienced in the installation or use of this product that you are unable to resolve, please contact your supplier.



RADIO FREQUENCY ENERGY

All interface cables used with this equipment must be shielded in order to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

European EMC directive 2004/108/EC

This equipment has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in the European standard EN55022. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions may cause harmful interference to radio or television reception. However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference with one or more of the following measures: (a) Reorient or relocate the receiving antenna. (b) Increase the separation between the equipment and the receiver. (c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected. (d) Consult the supplier or an experienced radio/TV technician for help.

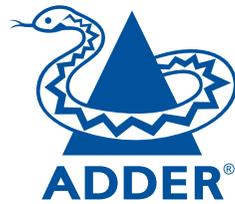
FCC Compliance Statement (United States)

This equipment generates, uses and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in Subpart J of part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area may cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference. Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Canadian Department of Communications RFI statement

This equipment does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le règlement sur le brouillage radioélectriques publié par le ministère des Communications du Canada.



Web: www.adder.com

Contact: www.adder.com/contact-details

Support: forum.adder.com

A

Active Directory 4,32

B

Base DN 15

Browsers
supported 8

C

Cable spec
null modem 41

Channel
add channel group 21
configure channel group 21

Channels
add a channel 20
configure a channel 20
view channels page 19
what are they? 3

Channels tab 19

Connections
transmitter - power in 6

D

Dashboard
active connections page 17
backups page 16
connection log page 17
event log page 18
home page 11
settings page 12
updates page 17
Dashboard tab 11
Distinguished Name 15

F

Factory reset 9
Favorites 36
Frame Skipping 26

G

Groups
what are they? 3

H

Hotkey settings 13
Hotkey shortcuts 36

I

IP port
connecting 6

L

LDAP 15
Logging in
administrators 8
normal users 36

O

On-Screen Display 3,36,37,38
OSD 3
login 36
main screen 37
remote 38
shortcuts 36

P

Peak Bandwidth Limiter 26
Permissions 4
Presets 33
add presets page 34
configure presets page 34
Presets tab 33

R

Receivers
add receiver group page 24
configure group page 24
configure receiver page 23
view receivers page 22
Receivers tab 22
Redundant servers
setting up 44
Regular user 3
Relationship
three-way 3
Remote OSD 38
Reset
manual 9

S

Safety information 57
Search filters 19
Security 3
Server redundancy 44
Servers tab 28
Shortcuts 36
Statistics tab 35
Swapping an AIM server 44

T

Transmitters
configure transmitter page 26
update firmware 26
view transmitters page 25
Transmitters tab 25
Troubleshooting 39

U

Users
active directory 32
add user group page 31
add user page 30
configure group page 31
configure user page 30
view users page 29
Users tab 29

Z

Zero-config addresses 10