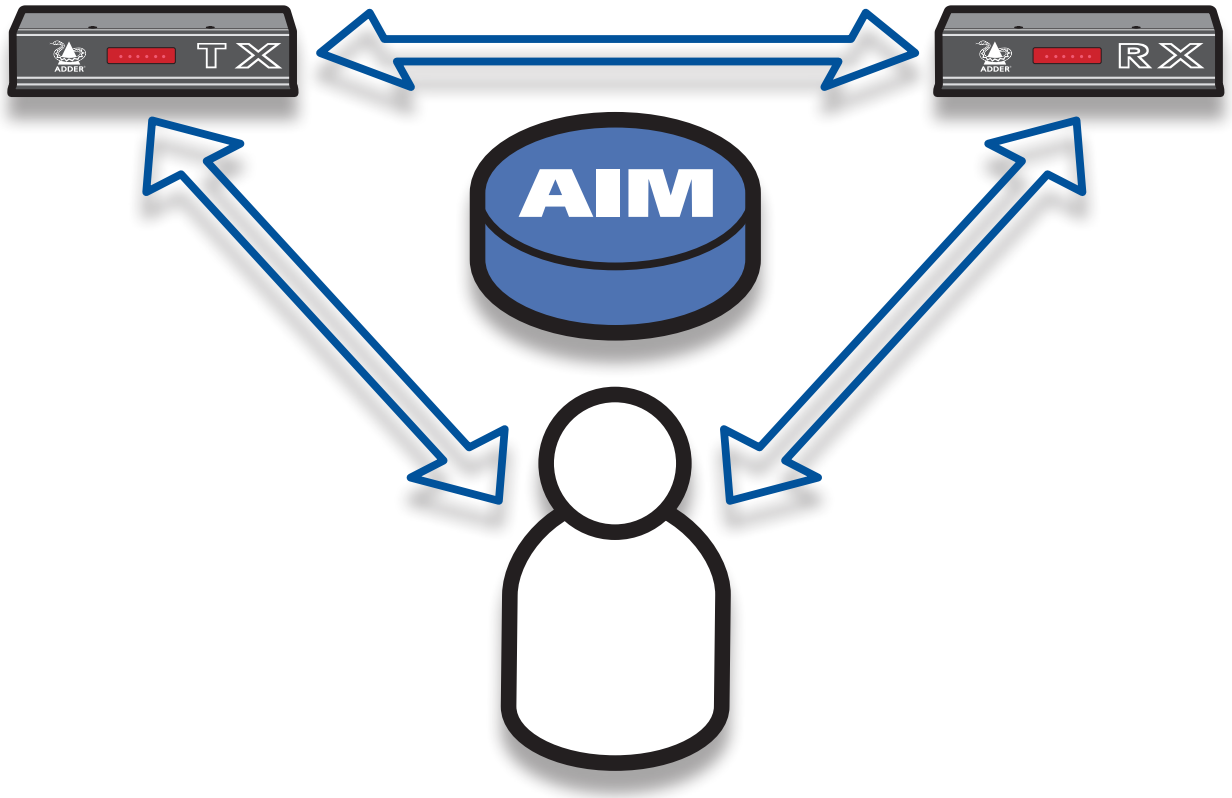
AdderLink Infinity Manager

User Guide



CONTENTS

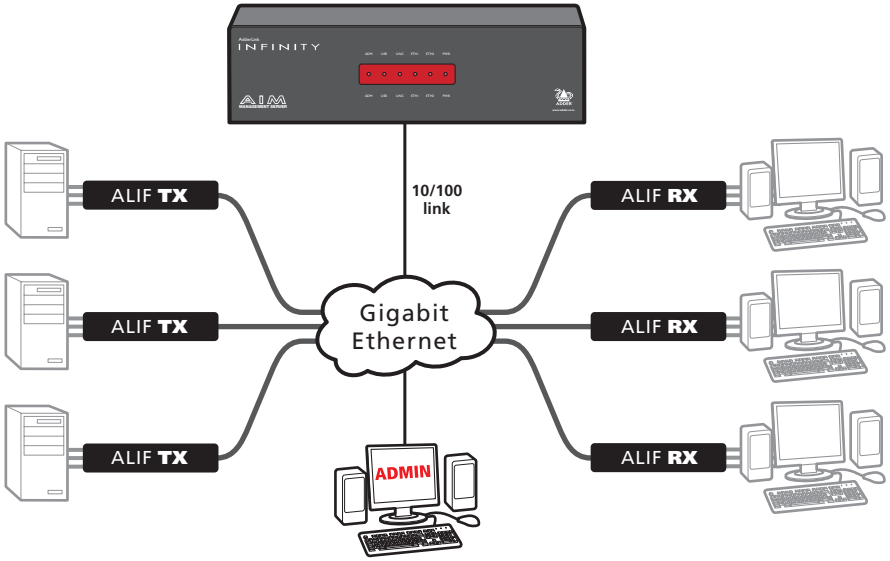
Contents

Introduction

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

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

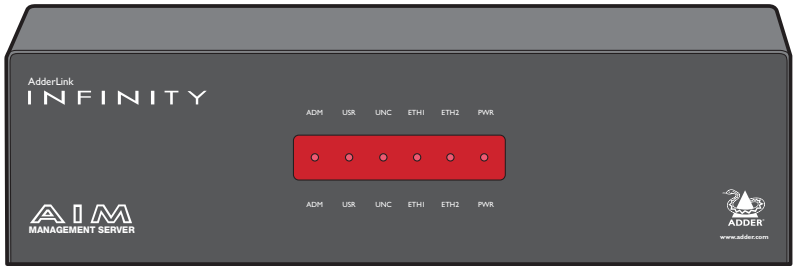
AdderLink Infinity Management operates from a self-contained compact server unit that can be situated anywhere within your network:



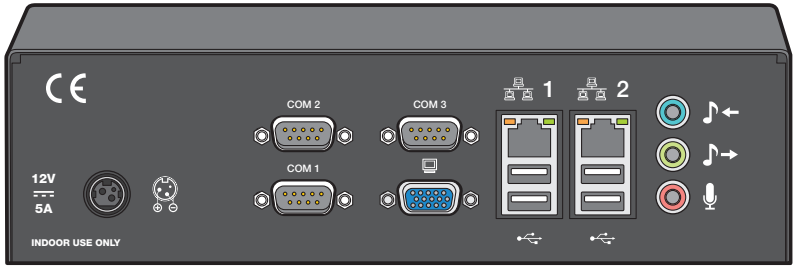
The AIM server connects to your network and provides administrative control over the various AdderLink Infinity transmitters, receivers and their users.
Note: Although the AdderLink Infinity units require Gigabit Ethernet connections, in its administrative role, the AIM server requires only a 10/100Mbps connection to the network.

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

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



The AIM server front panel with status indicators



The AIM 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 AIM installations.

AIM basics

Channels

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

Groups

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

User types

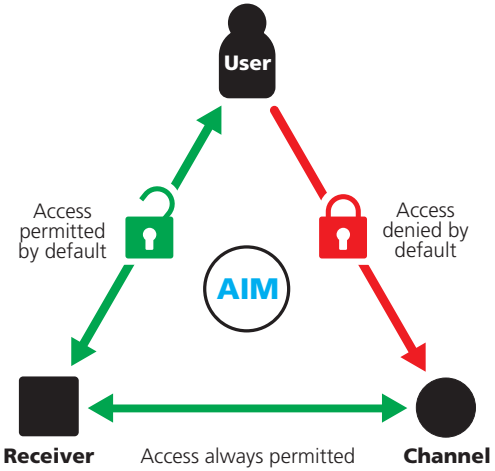
This guide refers to the two main categories of users involved with the AIM system:

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

Security

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

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



To successfully gain access to a channel:

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

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

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

See Permissions on the next page for more details.

continued

Active Directory

To streamline administration even further, AIM supports Active Directory. By synchronising 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 minimise the initial configuration as well as streamline ongoing updates.

AIM interface

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

- For administrators, full access to the AdderLink Infinity Manager Suite is granted. This comprehensive application shows six main tabbed areas: Dashboard, Channels, Receivers, Transmitters, Users and Presets 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.

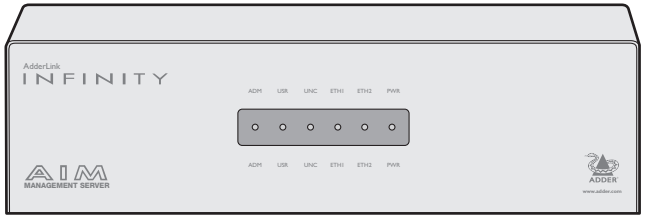
Permissions between a user and a receiver can be applied in any of the following ways:

- User –> Receiver
- User –> User Group –> Receiver
- User –> User Group –> Receiver Group –> Receiver
- User –> Receiver Group –> Receiver

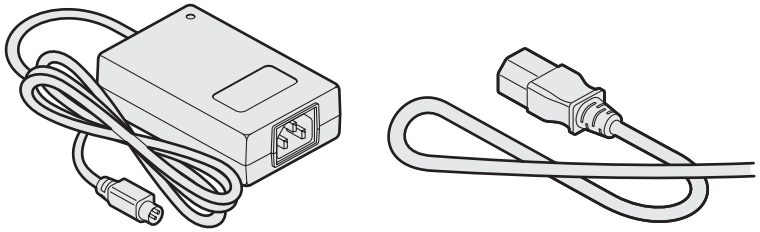
Thus, a very indirect way of granting permissions could be:

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

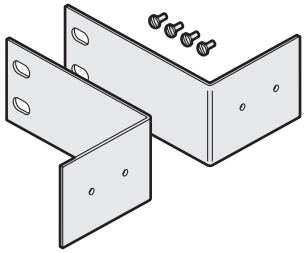
Supplied items



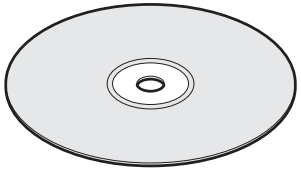
AIM server unit



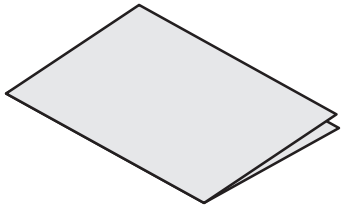
12V, 5A Power supply plus
country-specific mains cable



Rack mount brackets



CD-ROM
(contains this user guide)



Safety leaflet

Installation

Connections

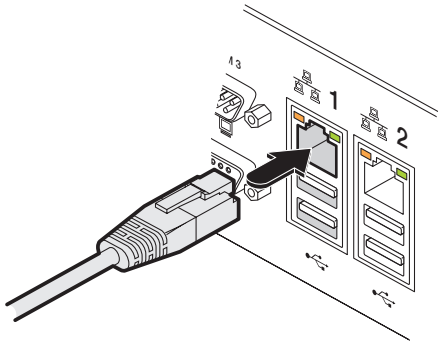
The AIM server unit is supplied fully pre-loaded and permits no local user interaction. All configuration takes place remotely via the network connections and as a result only two connections are required: Network and power.

Network connections

The AIM server has two network connections on the rear panel, labelled **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 AIM server unit.
2. Connect the plug of the link cable into the IP port labelled **1** on the rear panel of the AIM server unit.



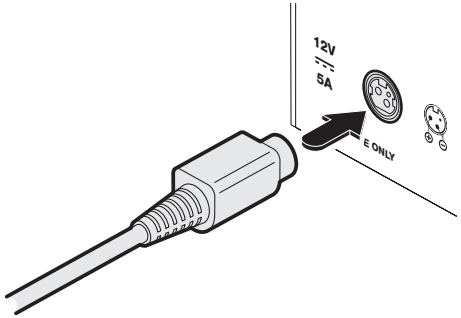
Category 5, 5e or 6 cable from LAN / network switch

Power supply connection

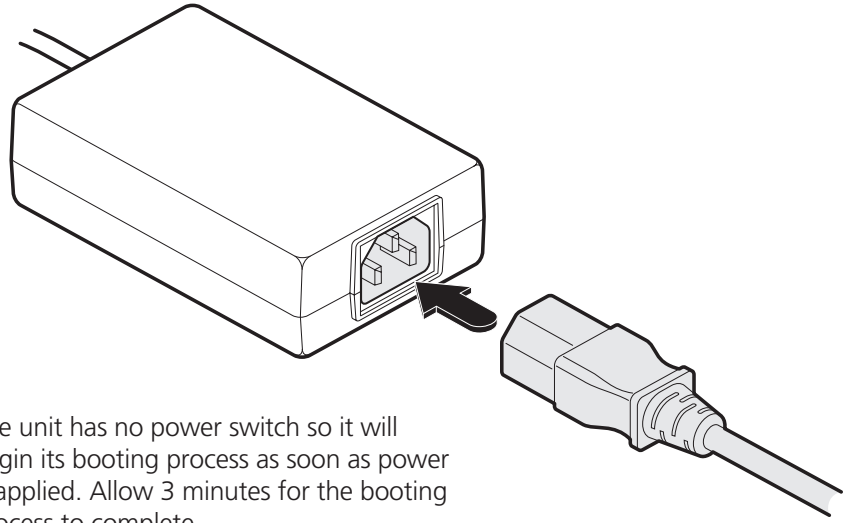
Important: Please read and adhere to the electrical safety information given within the Safety information section of this guide. In particular, do not use an unearthed power socket or extension cable.

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.



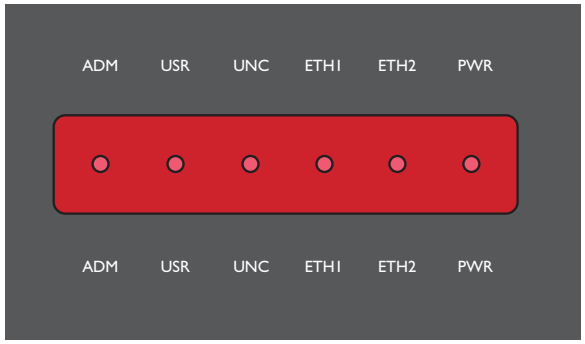
2. Connect the main body of the power supply to a nearby earthed mains outlet.



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

- AIM requires that all AdderLink Infinity units that it controls have firmware version 1.9 or greater.
- 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.

Swapping out an AIM server

If a configured AIM server needs to be replaced within an installation, there are steps that you can take to smooth the transition.

If ALIF devices have already been configured to run with the original AIM server then their default IP addresses will have been changed as part of the installation process. This means that in their current state they will be undetectable to the new AIM server.

There are two ways to introduce the new AIM server into the network, either:

Start from scratch

Place the new AIM server into the network and then perform a factory reset on every ALIF device. This will force the ALIF units back to their default states whereupon they will announce themselves to the new AIM server.

This method requires a certain amount of effort because each ALIF unit must be visited and reset, plus the AIM database will need to be fully reconfigured.

or

Transfer configuration to the new AIM server

1. Before connecting the new AIM server to the main network, connect the new AIM server to a network switch that is isolated from the main network.
2. Use a computer connected to the same switch to login to the new AIM server management suite.
3. Ensure that the new AIM 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 AIM server to match that of the original unit.
5. Restore a backup file of the original AIM server database to the new device.
6. Remove the original AIM server from the network. Connect the new AIM server in its place and power up.

   The replacement unit should now work directly with the installed 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 AIM 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

Google Chrome is the preferred browser because it is faster than Firefox or Internet Explorer.

IMPORTANT

The first time you log in as an admin user to a new AIM unit, you will be presented with the Settings page where you will need to change AIM'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 AIM admin interface until you have changed AIM'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 AIM.

Note: Ensure that your access computer can view the new IP address, otherwise AIM 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 AIM's new network address.

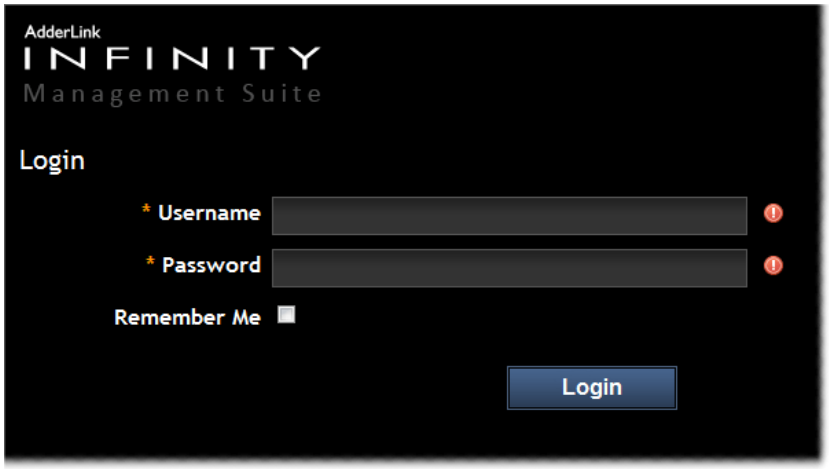
You will then be asked to login again and will have full access to all of AIM's pages.

Login for admin users

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

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

The Login page will be displayed:



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

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

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

If you check the **Remember Me** box, a cookie will be stored on the computer, allowing you to access the admin section without having to log in each time. The cookie expires 2 days after your last use of the system. 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 AIM server. Once the AIM 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 AIM server. Once an ALIF unit has been configured in one way, it cannot be reconfigured using the other method without undergoing a factory reset. This policy is in place to help prevent accidental overwriting of configurations. It also means that once an ALIF unit has been locally configured, it will not announce itself to the AIM server upon being added to a network. 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 AIM:

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

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 - Glossary
- Appendix D - AIM API

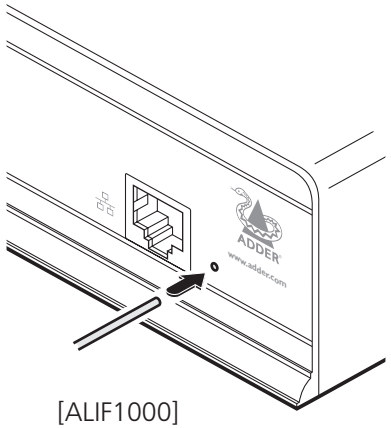
AdderLink Infinity manual factory reset

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

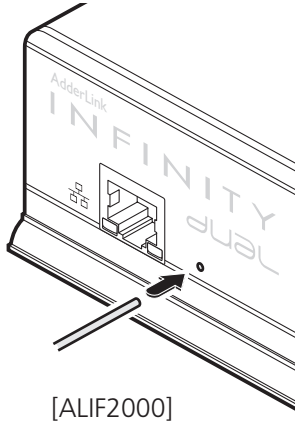
To perform a manual factory reset

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.



[ALIF1000]



[ALIF2000]

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 AIM 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 AIM server is attached to the same subnet (installing AIM) 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 AIM server as the *admin* user.

4 View the Dashboard page. The ALIF units should announce themselves to the AIM 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.

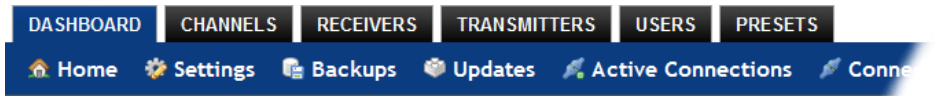
  Note: Where necessary, click the  *icon for a particular ALIF unit to flash the unit's front panel indicators to confirm its location.*
- Click the **Save** button. The new ALIF units will be restarted and will be changed to use their new IP addresses.

7 The new ALIF units will be added to the relevant *Transmitter* and *Receiver* pages within the AIM admin view. You can now refine their configurations and organise their relationships with each other and with registered users.

The Dashboard tab

The Dashboard is your main point of contact for checking and changing the general status of all AIM 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 page

- **Shutdown button** - Allows the admin user to shut down the AIM server. The OSD will no longer work on Receivers. The AIM server will need to be manually started again when next required.
- **Restart** - The admin user can reboot the AIM 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.
- **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 AIM system. See also the Event Log page.
- **Latest Channels** - shows the last five channels created within the AIM 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 AIM admin or at an AdderLink Infinity Receiver).
- **Latest User Registrations** - shows the last five users added to the AIM 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 AIM admin control panel.
- **Latest Receivers** - shows the last five receivers to be added and configured within the AIM network. Click to configure a receiver; click to connect to a channel; or click to disconnect an existing connection.
- **Latest Transmitters** - shows the last five transmitters to be added and configured within the AIM 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 page

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

Most global configuration options for the AIM system are available in the settings page. For configuration options that affect individual receivers, users and channels, see the sections dealing with those tabs.

Check For Updates - If this setting is off, AIM will never attempt to connect to the update server to check for updates. If it is on, the first time the AIM admin section is visited each day, an online check takes place. This check is only ever performed once per day. If new AIM software has been released, the Version number at the top right of the page will now contain a link, allowing automatic upgrade of AIM. See Dashboard > Updates page for further details.

Note: For the AIM unit to successfully locate and use updates it requires access to the Internet, usually via the second Ethernet connection to the rear of the unit. The IP address for the second Ethernet connection can be configured within the Settings page.

Login Required
Determines whether a login is required to use AdderLink Infinity receivers. This is a global setting that applies to all receivers but which can be overridden for specific receivers or receiver groups. Options are:

- No: Anyone can use a receiver without login credentials, using the channels granted to the "Anonymous User" (set further down the page).
- Yes: Users need to login to use a receiver.

Note: Within AIM, Login requirements filter down from the top (i.e. from this setting), but can be overridden at lower levels, such as at the Receiver or Receiver Group levels. See The Receivers Tab section for more details.

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.*

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/Shared only: Prevents users from gaining exclusive access to a channel.
- 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.

Initial Streaming Mode
All new connections are created in unicast mode in order to minimise 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.

DDC
Allows you to force a particular DDC to be sent to receivers, or you can set it to use the DDC of the monitor currently connected to the receiver.

Hot Plug Detect
Controls whether Hot Plug Detect is allowed to be brought up/down by ALIF RX unit.

USB Speed
Determines the USB version/speed capability of the ALIF system that is reported to the host computer (USB 2 Hi-Speed or USB 1 Full Speed).

USB Hub Size
Determines the USB hub size of the ALIF system that is reported to the host computer (13 or 7 ports).

Hotkey
Allows you to define the default keypress combination that will be used to access the AIM on-screen display (OSD) menu by each user. If the hotkey combination is altered, the change will be applied instantly to all receivers.

Anonymous User
Allows you to nominate a profile for an anonymous user that will be applied to any receivers that do not require login. The channels available to that receiver will be those available to the user that is selected here. You can create a suitable standard user profile in the same way as any other user (see The Users tab) and then choose it within this setting.

Rows per Page
Determines how many rows to show per page in any paginated table within the admin section, e.g. Users, Channels, Receivers, Event/Connection Logs.

AIM IP Address
Defines the IP address to which the AIM server has been set. Connect a display monitor to the VGA port of the AIM unit to discover its current IP address.

The default AIM server IP address is **169.254.1.3**

Note: If the AIM server's IP address is changed, any connected transmitters or receivers will be rebooted.

Gateway IP Address
Defines the network gateway IP address for the AIM server.

Netmask
Defines the netmask for the AIM server.

DNS Server IP Address
Defines the IP address for a suitable DNS server to use within the AIM network.

Syslog IP Address
Defines the IP address for a suitable syslog server to use within the AIM network.

Multicast IP Base
Defines the base IP address for use in multicast configurations (where multiple receivers use the output from a single channel). Multicast IP addresses are assigned in pairs (one for audio, one for video), starting from this lowest IP address. If you expect to have several multicast/shared connections within your AIM network, ensure that sufficient IP addresses are available, starting from this IP address.

Time

NTP Enabled?
If set to No, you will need to enter the date and time manually.

If set to Yes, you need to enter an *NTP Server Address*, declare your *Timezone Area* and your *Timezone Location*.

Note: For the AIM unit to use NTP it requires access to the Internet, usually via the second Ethernet connection to the rear of the unit. The IP address for the second Ethernet connection can be configured within the Settings page.

API
Determines whether login is required (and which user profile to use, if login is made a requirement) when AIM is driven using API scripts from an external system.

Mail Server
A range of settings to define your email server, so that AIM system backups can be automatically emailed to you.

Active Directory
If you wish to import user details from an existing LDAP connection, such as Active Directory, this section allows you to enter all of the necessary details. See Users > Active Directory for details about using Active Directory links.

Dashboard > Backups page

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

IMPORTANT: You are strongly recommended to arrange regular scheduled backups of your AIM database. Adder cannot be held responsible for any loss of data, however caused.

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 AIM server when they are used.

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

- Hourly backups are executed on the hour (or quarter past).
- Daily backups are executed at 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 AIM system before restoring a previous backup. Restoring the contents of a backup file will overwrite ALL data in the AIM system, with the data within the backup file. This includes configured devices, channels, users, connection logs and action logs.

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

Archive Log to CSV Report

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 Reports

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

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

Dashboard > Updates page

Upgrade AIM Software

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

Upload New TX/RX Firmware

This section allows the AIM admin user to upgrade firmware on receivers and transmitters, wherever they are located.

1. Use the "Upload New Firmware" section to place new transmitter and/or receiver firmware file(s) onto the AIM server. Once uploaded, the stored firmware files are listed within the relevant "Available firmware" drop-down boxes within the sections below.
2. Within the relevant "Install Firmware onto..." section, click the drop-down box and select the required new firmware version.
3. Click the "Install" button to display a list of 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 page

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

Dashboard > Connection Log page

Shows all connections that have occurred within the AIM network. The most recent connections are shown at the top, and the log is paginated (the number of rows per page can be set from the 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 page

This page lists events that have occurred within the AIM system. A row of buttons just below the blue options bar allows you to filter log page entries to show only particular categories, as follows:

All | Admin | Users | Login | Channel Changes | Device Status

Where:

- **All**: Lists all events
- **Admin**: Lists automatic events and/or those performed by the admin user (including: backup, scheduled backup, backup restored, updating AIM settings, adding/removing/updating channels/users/devices, Active Directory Sync, Firmware upgrades, AIM 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 AIM 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.

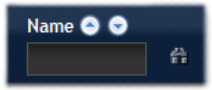
The Channels tab

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 page

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

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.

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 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.

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.

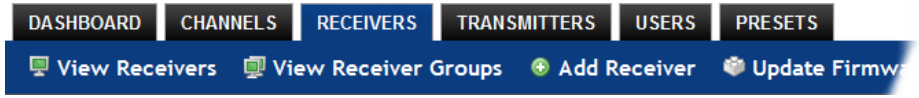
To remove one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the right list and then click to move them back to the left list.

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

The Receivers tab

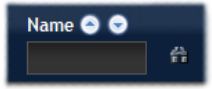
The Receivers tab shows a paginated table of all receiver devices within the AIM network.

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 page

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):

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)

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).

Delete device: Confirmation will be requested. You will need to factory-reset any devices that you wish to re-configure to work with AIM.

Configure device: Displays the "Configure Receiver" page.

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 page

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.

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 page

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.

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.

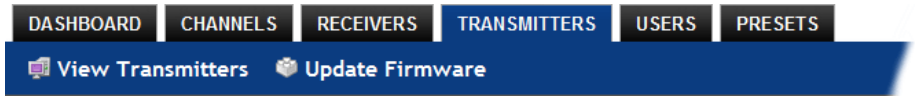
Receivers > Update Firmware

Click this option to go straight to the Dashboard > Updates page. See Dashboard > Updates page for more details.

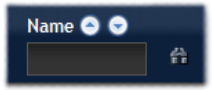
The Transmitters tab

The Transmitters tab shows a paginated table of all transmitter devices within the AIM 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 page

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):

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)

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).

Delete device: Confirmation will be requested. You will need to factory-reset any devices that you wish to re-configure to work with AIM.

Configure device: Displays the "Configure Transmitter" page.

Transmitters > Configure Transmitter page

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.

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
Allows you to use a global DDC setting, the monitor's DDC or a particular DDC chosen from the list.

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 colour 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 colour reproduction. Options: 24 bit, 16 bit or 8 bit.

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

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.

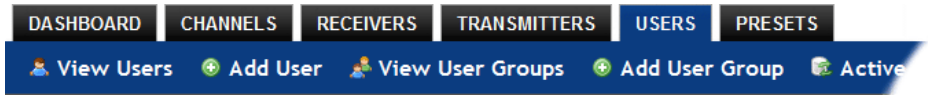
Transmitters > Update Firmware

Click this option to go straight to the Dashboard > Updates page. See Dashboard > Updates page for more details.

The Users tab

The Users tab shows a paginated table of all users within the AIM network. Within the list, the admin user is always present and cannot be deleted - in order to avoid being locked out of the AIM 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 (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 "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)
- Admin - indicates whether the user has admin privileges

The Edit option icons are as follows:

Configure user: Displays the "Configure User" page.

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 AIM installation.

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

First Name, Last Name and 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.

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

Admin?
When set to Yes, the user is granted privileges to login to the AIM 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.*

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 AIM 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.*

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, AIM can be synchronised 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 AIM user database, they will be imported.
   - If an AD user is already in the AIM user database, they are kept.
   - If an AD user is NOT marked for import/sync from the AD import page, and they already exist in the AIM user database, they will be removed from the AIM user database during the sync operation.

     IMPORTANT: It is thus vital to ensure that all users you want in the AIM system are always selected for import/sync, otherwise they will be removed.
2. You can choose to synchronise 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 synchronisation. 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 synchronise the selected items into the AIM user database.

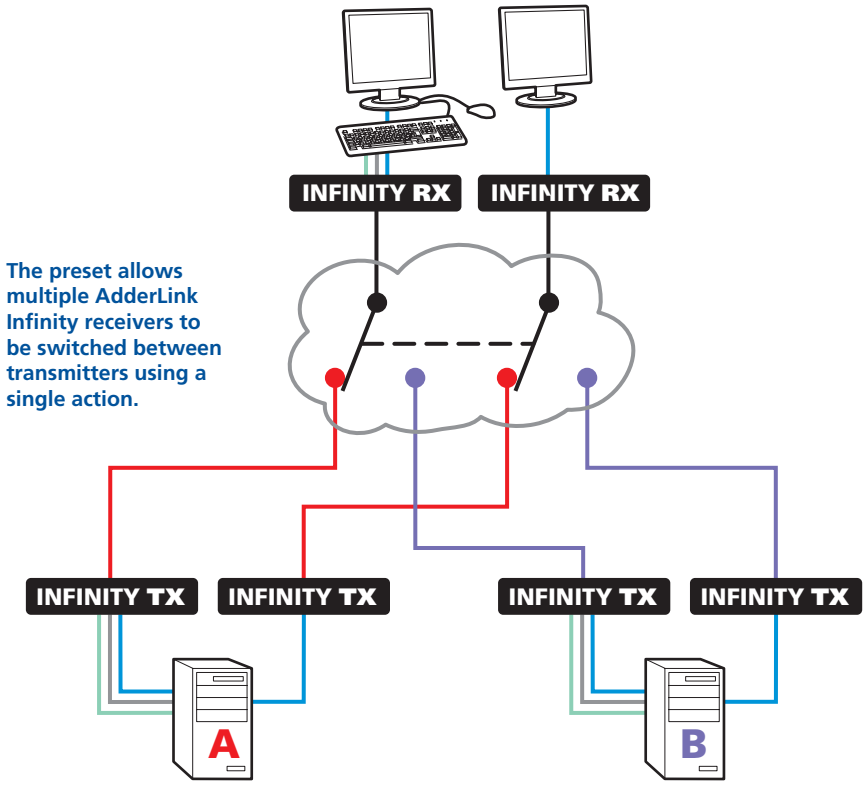
Note: AIM will only import folders/groups/users up to the limit set by the AD server. There is a known issue: AIM can only import x users/groups from AD where x is the limit set on the AD server. Any users/groups beyond this limit will not be imported.

Active Directory Tips

- A backup schedule is recommended so that any changes on the AD server are carried across to the AIM server regularly. You can choose from hourly/daily or weekly syncs. The settings/filters saved on this screen will be applied to each subsequent sync, ensuring that your list of users is kept accurate.
- To temporarily remove a particular user from AIM access, without having to make complicated LDAP filters, simply edit the AIM user to be suspended (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 AIM if they contain users that are set to be imported too (i.e. a group will not be imported, even if it contains users, unless its users match the sync filters).
- Associations between users and user groups can only be made on the AD server - it is not possible to edit user/user-group membership for AD users/groups on the AIM server.
- Users and groups are technically "synchronized" rather than "imported" - each time a sync takes place, details are updated and if a user no longer matches the sync filters, they will be removed from the AIM user list.

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.

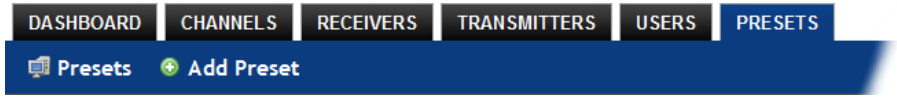


The preset allows multiple AdderLink Infinity receivers to be switched between transmitters using a single action.

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 AIM 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
- 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.

Operation

For non-admin users, AdderLink Infinity Manager offers a clear way to choose and access multiple channels.

Logging in

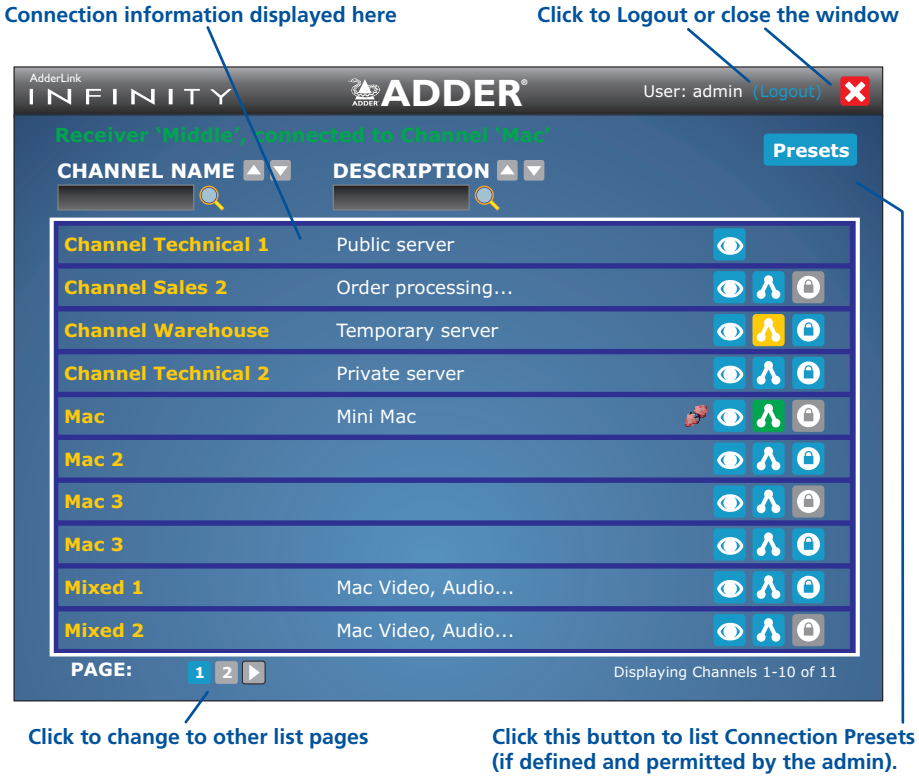
1 On the keyboard connected to your AdderLink Infinity receiver, press the hotkey combination **Ctrl-Alt-C** to display the On-Screen Display or OSD (your administrator may have changed the hotkey combination).

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.

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.

The list of channels for which you have permission will be shown:



Meanings of icons

- Connect in view-only mode.
- Connect in shared mode.
- Connect in exclusive mode.
- Choice not currently available (because someone else is currently connected, therefore exclusive connection is not possible).
- You are currently connected to this channel.
- Another user has connected this receiver to this channel.
- 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.

Further information

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

- Getting assistance - see right
- Appendix A - Tips for success when networking ALIF and AIM units
- Appendix B - Troubleshooting
- Appendix C - Glossary
- Appendix D - AIM 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 minimise 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 maximise network efficiency and help minimise 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
- Cisco 3750
- Cisco 4500
- Cisco 6500
- Extreme Networks X480
- HP Procurve 2810
- HP Procurve 2910
- H3C 5120
- HuaWei Quidway s5328c-EI (Layer 3 switch)

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

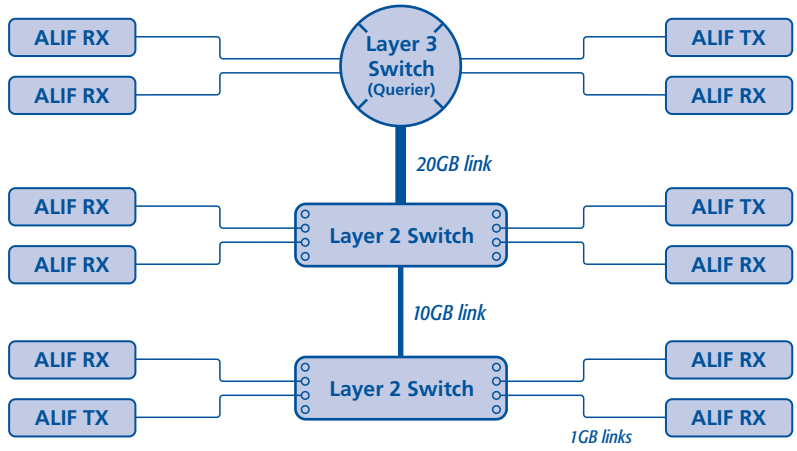
Creating an efficient network layout

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 AIM server is used to administer multiple ALIF transceivers, ensure the AIM server and all ALIF units reside in the same subnet.
- Do not use VGA to DVI converters, instead replace VGA video cards in older systems with suitable DVI replacements. Converters cause ALIF TX units to massively increase data output.
- Stackable switches will allow you to create more ports at each cascade level.
- Wherever possible, create a private network.

The recommended layout

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



- 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.
- Optimise the settings on the ALIF transmitters:
  - If colour quality is important, then leave Colourdepth 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 Colourdepth.
  - 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: AIM cannot locate working ALIF units.

There are a few possible causes:

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

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

Remedies:

- Ensure that the ALIF units and the AIM server are located within the same subnet. AIM cannot cross subnet boundaries.
- Manually reset the ALIF units to their zero config IP addresses. Please refer to the ALIF user guide for details.
- Enable *portfast* on all switch ports that have ALIF units attached to them or try temporarily disabling STP on the switches while AIM is attempting to locate ALIF units.

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 colour depth of images by diffusing or altering the colour 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

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 customise 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 colour 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 colour 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:

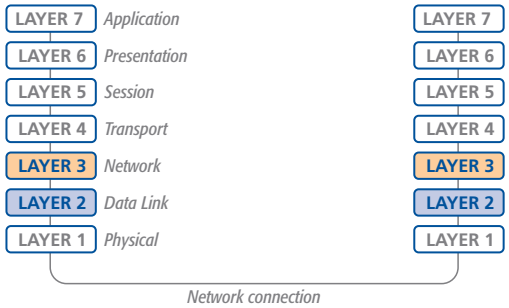
- **Store and forward** is the original method and requires the switch to save each entire data packet to buffer memory, run an error check and then forward if no error is found (or otherwise discard it).
- **Cut-through** was developed to address the latency issues suffered by some store and forward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

AIM API

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

Note: This section refers to AIM version 1.3 released 17th February 2011.

Methods

login	(http://<aim.ip.address>/api/#login)
logout	(http://<aim.ip.address>/api/#logout)
get_presets	(http://<aim.ip.address>/api/#get_presets)
connect_preset	(http://<aim.ip.address>/api/#connect_preset)
disconnect_preset	(http://<aim.ip.address>/api/#disconnect_preset)

login

The API will require a valid AIM user's login credentials to be presented in the first request. The API will return an authentication code, which must be passed in all future requests. This authentication code can be re-used until a logout request is made, at which point the authentication code will no longer be valid.

The concept of an 'anonymous user' can apply to the API. If no login username and password are provided, the API will return an authentication token for the anonymous user (either the same one as for the OSD, or else an 'anonymous API user' account can be created).

Input parameters:

- username
- password
- v (the AIM API version this request is designed for)

Output values:

- timestamp - the current server time
- version - the current API version number
- token - an authentication code for future API requests

Examples

Input:

/api/?v=1&method=login&username=xxxxx&password=xxxxx

Output:

```
<api_response>
    <version>1</version>
    <timestamp>2011-02-04 15:26:20</timestamp>
    <success>1</success>
    <token>5cf494a71c29e9465a57a81e0a2d602c</token>
</api_response>
```

or

```
<api_response>
    <version>1</version>
    <timestamp>2011-02-04 15:26:20</timestamp>
    <success>0</success>
    <errors>
      <error>
        <code>2</code>
        <msg>Invalid username or password</msg>
      </error>
    </errors>
</api_response>
```

This method was last updated in API version 1

logout

The authentication token provided by the Login function can be used until the logout function is called.

Input parameters:
- token
- v (the AIM API version this request is designed for)

Output values:
- timestamp
- success - 0 = fail, 1 = success

Examples

Input:
/api/?method=logout&token=xxxxx&v=0.1

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>2011-02-04 15:24:15</timestamp>
    <success>0</success>
    <errors>
       <error>
          <code>3</code>
          <msg>Error logging out (you may already have logged out)</msg>
       </error>
    </errors>
</api_response>
```

This method was last updated in API version 1

get_presets

This simple function returns a list of presets available to the authenticated user.

Input parameters:
- token
- v (the AIM API version this request is designed for)
- results_per_page (number of results per page, default = 1000)
- page (page number to start showing results for, default = 1)

Output values:
- version
- timestamp
- success
-.page (page number)
- results_per_page (number of results per page, default = unlimited)
- count_presets - the number of presets available to the authenticated user
- total_presets - the total number of presets 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)

continued

Examples

Input:
/api/?v=1&method=get_presets&token=xxxxx

Output:
<api_response>
<version>1</version>
<timestamp>2011-02-04 15:30:07</timestamp>
<success>1</success>
<page>1</page>
<results_per_page>10</results_per_page>
<count_presets>2</count_presets>
<total_presets>2</total_presets>
<connection_preset item="1">
<cp_id>3</cp_id>
<cp_name>CP1</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>
This method was last updated in API version 1

connect_preset

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

Input parameters:
- token
- v (the AIM API version this request is designed for)
- id - the ID of the preset (acquired from get_presets)
- 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
- timestamp
- 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>2011-02-04 15:24:15</timestamp>
<success>1</success>
</api_response>
or
<api_response>
<version>1</version>
<timestamp>2011-02-04 15:24:15</timestamp>
<success>0</success>
<errors>
<error>
<code>217</code>
<msg>A receiver/channel is already in use by someone else</msg>
</error>
</errors>
</api_response>
This method was last updated in API version 1

disconnect_preset

This function disconnects all channel-receiver pairs in a preset, or disconnects ALL connections in the whole AIM network.

Input parameters:

- token
- v (the AIM API version this request is designed for)
- id (optional. If not supplied, all connections will be ended)
- force - whether to ignore errors with some of the preset's pairs or not

Output values:

- version
- timestamp
- 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>2011-02-04 15:24:15</timestamp>
    <success>1</success>
</api_response>
```

This method was last updated in API version 1

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

Documentation by: CORPORATE TEXT & DESIGN www.ctxd.com

Part No. MAN-AIM • Release 1.3c

Index