AdderLink Infinity Manager
## User Guide

AIM

TX

RX
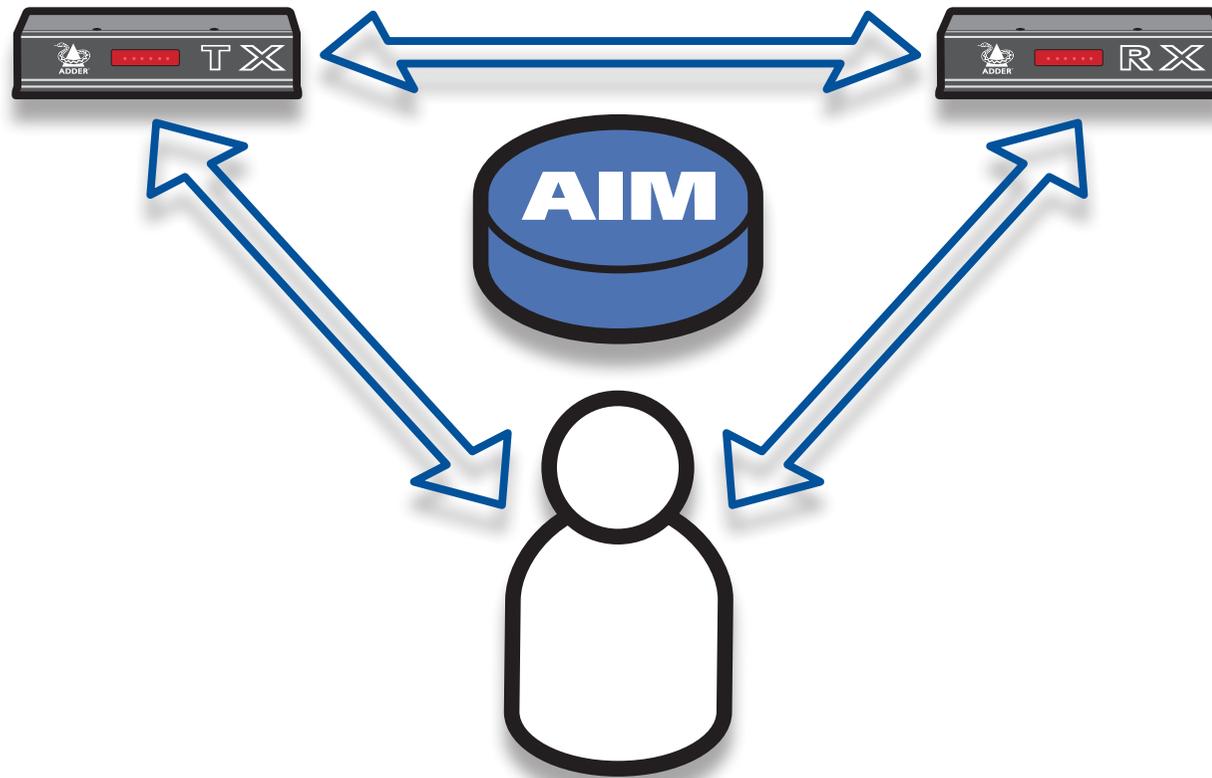
CONTENTS

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 units by allowing central control over any number of transmitters (more commonly referred to as 'Channels' within AIM) 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.

Adder Infinity Management operates from a self-contained compact server unit that can be situated anywhere within your network:
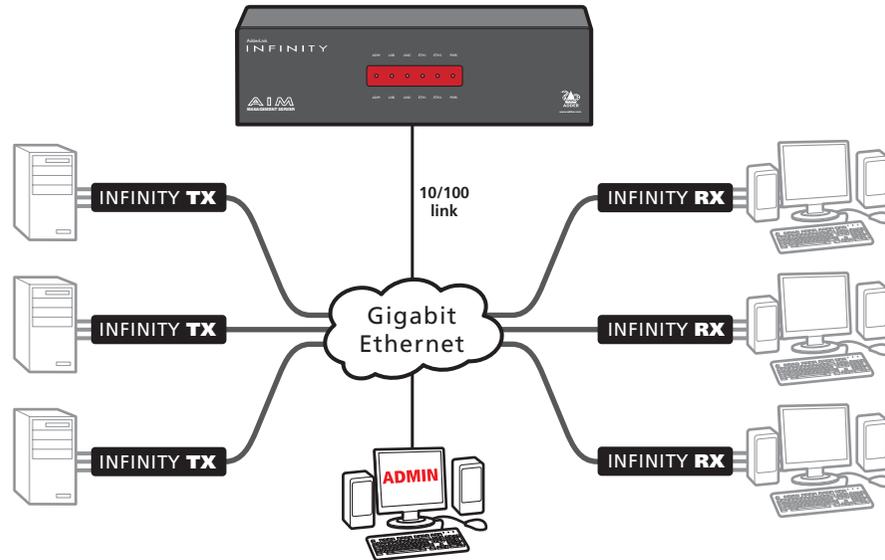
The AIM server connects to your network and provides administrative control over the various Infinity transmitters, receivers and their users.
Note: Although the Infinity units require Gigabit Ethernet connections, in its administrative role, the AIM server requires only a 10/100Mbps connection to the 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 Infinity transmitters (channels), receivers and users are performed using the intuitive AIM browser interface via a network connected computer.
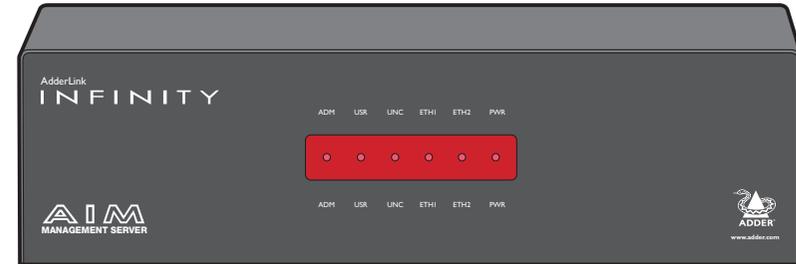
The AIM server front panel with status indicators
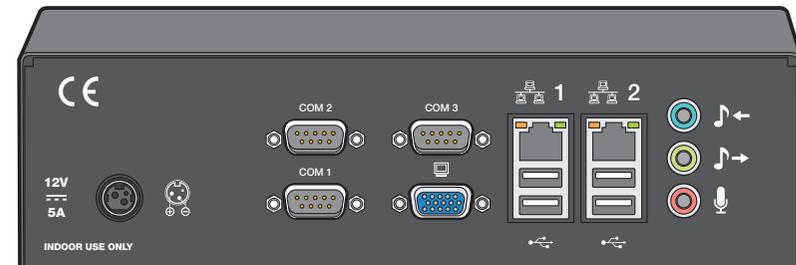
The AIM server rear panel. In normal use only the network and power connectors are used.

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 Infinity receiver unit and can access one or more computers that are linked to Infinity transmitters. The 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 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.
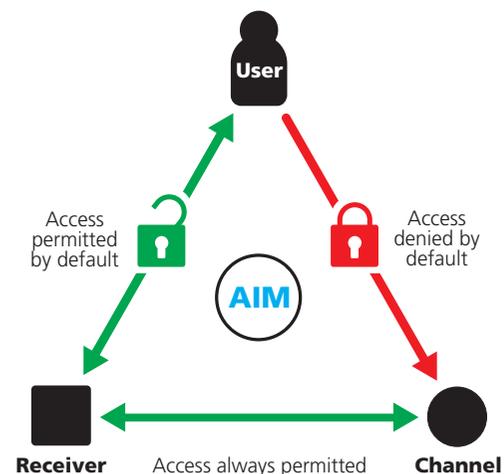
To successfully gain access to a channel:

- 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.

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 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 ChannelGroup1,
- ChannelGroup1 contains Channel1,
- Therefore, User1 has access to Channel1 indirectly,

Supplied items
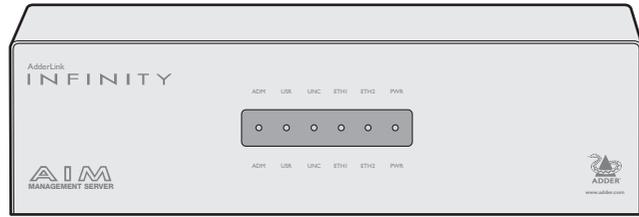
AIM server unit
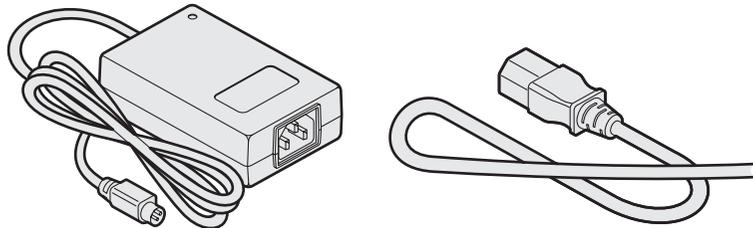
12V, 5A Power supply plus country-specific mains cable
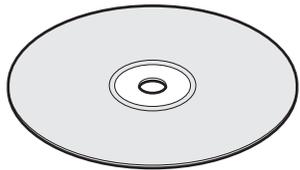
CD-ROM (contains this user guide)
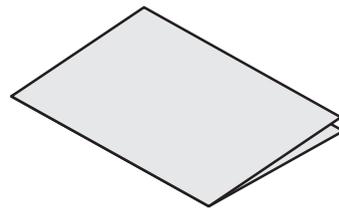
Safety leaflet

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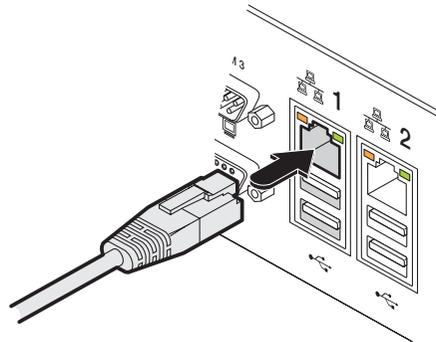
Category 5, 5e or 6 cable from LAN / network switch

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.
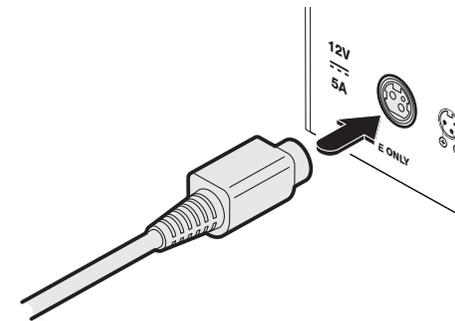
2 Connect the main body of the power supply to a nearby earthed mains outlet.
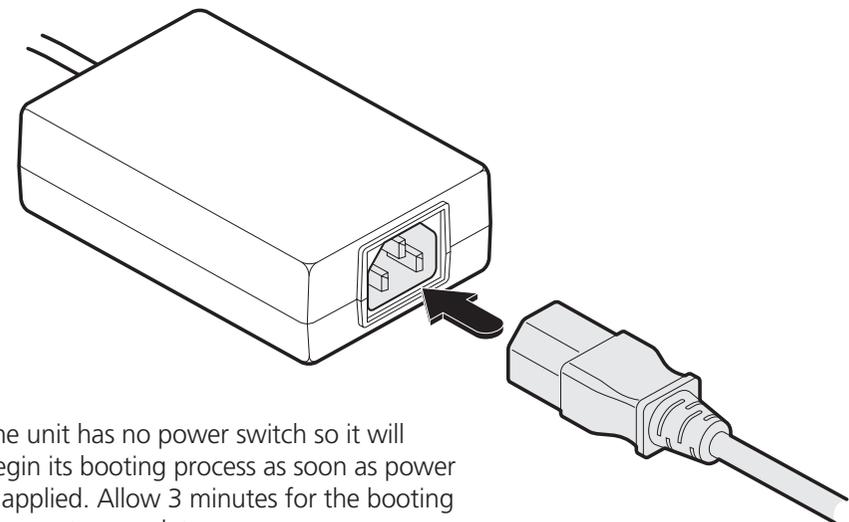
The unit has no power switch so it will begin its booting process as soon as power is applied. Allow 3 minutes for the booting process to complete.

Front panel indicators

To assist with operational checks and troubleshooting, the front panel provides the following indicators:
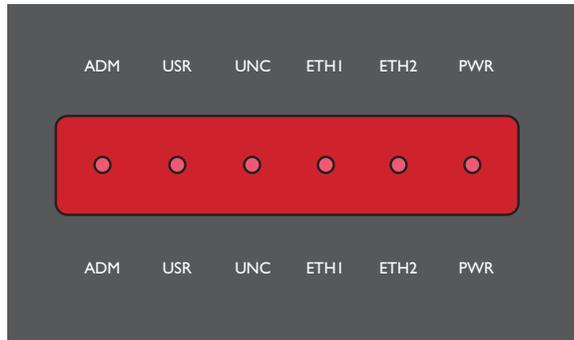
- **ADM**   On when an administrator is logged in. Flashes when an administrator is accessing the system.
- **USR**   On if there are any connections between channels/receivers. Flashes when a user is accessing the system.
- **UNC**   Unconfigured RX or TX units are online
- **ETH1**   On when connected, 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 above 1920 x 1080 the network switch must have support for Jumbo packets.

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
- Opera   to be determined

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, the unit will reboot itself. This may take 2-3 minutes, after which 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 Infinity units

When new transmitters and receivers are added to an AIM network, they will automatically announce themselves and their details will be displayed within the administrator's view of the Dashboard.

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 when the session started, which user/receiver/channel are 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 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 channel, either while using the on-screen display (OSD) at an 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 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 Infinity receivers. This is a global setting which 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 which 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. 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.

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
Not fully supported. Set this to be the AIM IP Address if you do not have a syslog server.

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 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.

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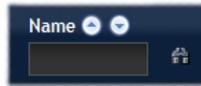
Click the CHANNELS tab to view the initial View Channels page.

| DASHBOARD | CHANNELS | RECEIVERS | TRANSMITTERS | USERS | PRESETS |

🖵 View Channels   ⊕ Add Channel   🖵 View Channel Groups   ⊕ Add Channel Grou

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.

Note: Only one receiver can use a transmitter's serial port at any time. Thus, it's possible to create a channel without Serial.

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.

16

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

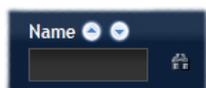The Receivers tab shows a paginated table of all receiver devices within the AIM network.

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

| DASHBOARD | CHANNELS | RECEIVERS | TRANSMITTERS | USERS | PRESETS |

🖥 View Receivers   🖥 View Receiver Groups   ⊕ Add Receiver   📦 Update Firmw

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.

Name ⊙ ⊙

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" which 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
In order 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" which is 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.
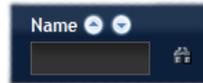
The Transmitters tab

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

Click the TRANSMITTERS tab to view the transmitters page.

DASHBOARD	CHANNELS	RECEIVERS	TRANSMITTERS	USERS	PRESETS

🖥 View Transmitters ⬢ Update Firmware

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 ![icon] 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 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. 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 100%.

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.
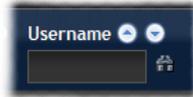
The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "B" in the Username, and "Smith" in the Last Name). Search terms are case-insensitive. You can re-sort and paginate on filtered 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, which is 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 infinity units, such as in the example below where multiple video heads need to be switched in unison between different server systems.
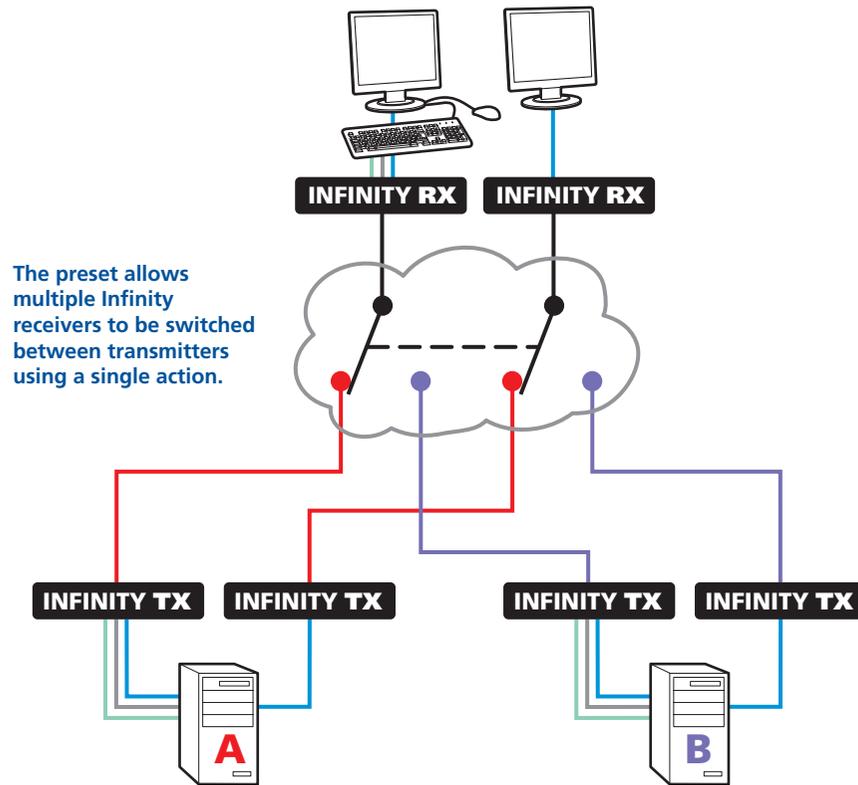

The preset allows multiple Infinity receivers to be switched between transmitters using a single action.

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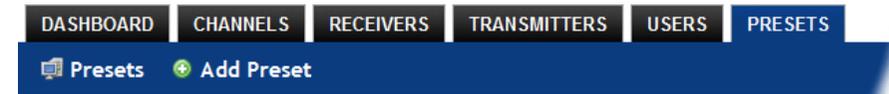
The nature of each preset, i.e. which receiver connects to which channel(s), is defined by the admin. The permitted connection modes are worked out according to:

- 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.

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).

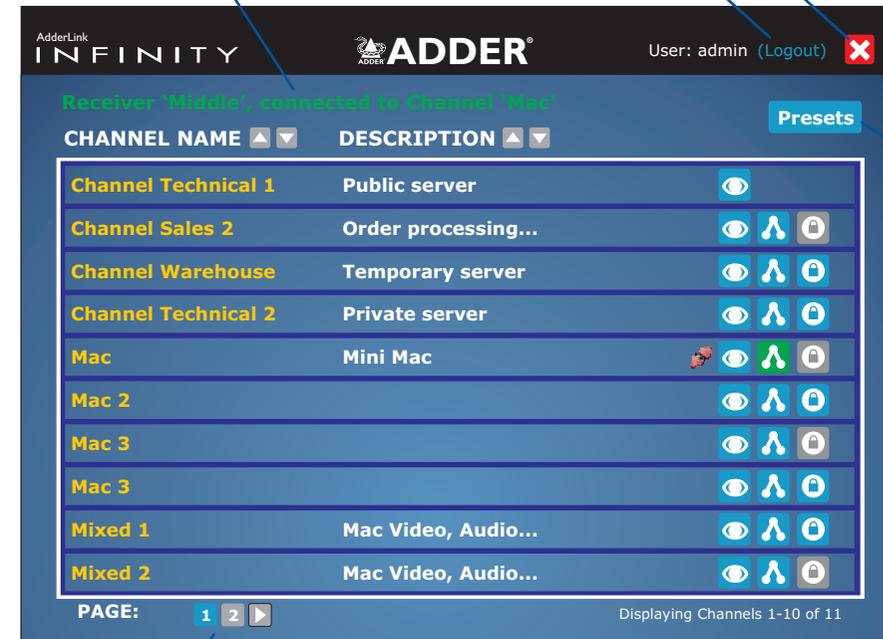You will either see the list of channels for which you have permission or be presented with the following login:

AdderLink
I N F I N I T Y   **ADDER**®   ✖

Login

* Username   [_____]
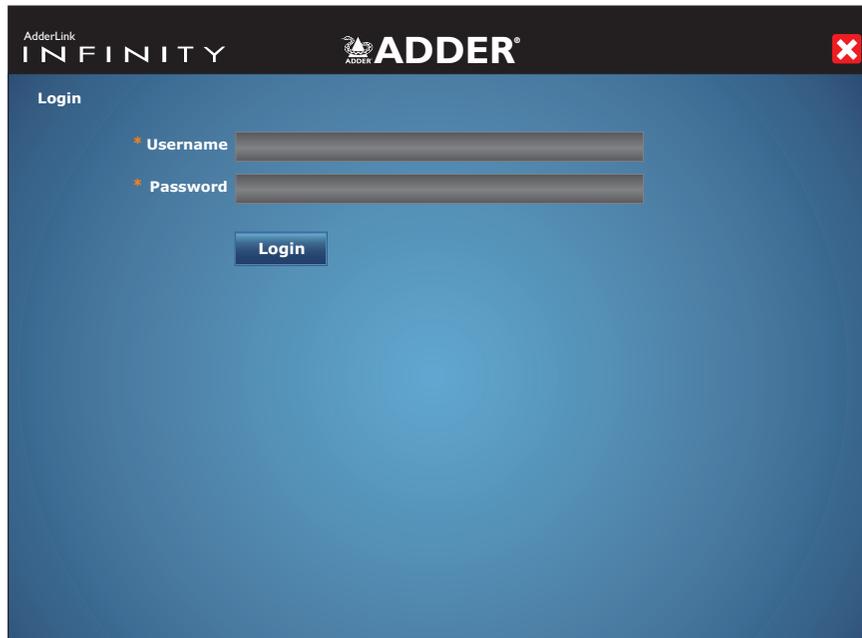
* Password   [_____]

[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 Infinity unit is rebooted.

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

Connection information displayed here   **Click to Logout or close the window**

AdderLink
I N F I N I T Y   **ADDER**®   User: admin (Logout)   ✖

Receiver 'Middle', connected to Channel 'Mac'   [Presets]

CHANNEL NAME ▲▼	DESCRIPTION ▲▼	
Channel Technical 1	Public server	👁
Channel Sales 2	Order processing...	👁 ⋀ 🔒
Channel Warehouse	Temporary server	👁 ⋀ 🔒
Channel Technical 2	Private server	👁 ⋀ 🔒
Mac	Mini Mac	🚀 👁 ⋀ 🔒
Mac 2		👁 ⋀ 🔒
Mac 3		👁 ⋀ 🔒
Mac 3		👁 ⋀ 🔒
Mixed 1	Mac Video, Audio...	👁 ⋀ 🔒
Mixed 2	Mac Video, Audio...	👁 ⋀ 🔒

PAGE: [1][2][▶]   Displaying Channels 1-10 of 11

Click to change to other list pages   **Click this button to list Connection Presets (if defined and permitted by the admin).**

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).

⋀   Currently connected to this channel in this mode.

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.

28

Further information

Getting assistance

- Adder Technology website – *www.adder.com*
  Check the Support section of our website for the latest solutions and driver files.

- Email – *support@adder.com*

- Fax   in the UK: **01954 780081**
              in the US: **+1 888 275 1117**

- Phone   in the UK: **01954 780044**
              in the US: **+1 888 932 3337**

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.

INSTALLATION

CONFIGURATION

OPERATION

FURTHER INFORMATION

INDEX

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.

INSTALLATION

CONFIGURATION

OPERATION

FURTHER
INFORMATION

INDEX

Index