AvediaServer

exterity®

AvediaServer Version 5.0
Director Software

Administrator Guide

Notices

Exterity Limited, Ridge Way, Hillend Industrial Park, Dalgety Bay, Fife, KY11 9JD, Scotland, UK

http://www.exterity.com

Document Reference

1300-0070-0001

Edition 5.0 Issue 1(Aug13)

Applications Described by This Guide

AvediaServer™ Channel Monitor Application

AvediaServer™ Director Application

AvediaServer™ Logger Application

AvediaServer™ System Application

AvediaServer™ TFTP Server Application

AvediaServer™ Users Application

Trademarks

AvediaStream, AvediaServer and AvediaPlayer are trademarks or registered trademarks of Exterity Limited.

Microsoft®, Windows®, and Windows Media Player® are U.S. registered trademarks of Microsoft Corporation.

HDMI, the HDMI Logo and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.

Kensington® is a U.S. registered trademarks of ACCO World Corporation.

All other trademarks are the property of their respective owners. All rights reserved.

Disclaimer

The information contained in this document is subject to change without notice.

EXTERITY LIMITED MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Exterity Limited shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Exterity products and replacement parts can be obtained from Exterity. To request more information or parts, email

support@exterity.com

Safety Notices

Before installing and operating these products, please read the safety information contained in this guide.

Table of Contents

Glossary

3

The following terms and definitions are used in this document:

Table 1

DHCP	Dynamic Host Configuration Protocol, a protocol used to allocate IP addresses to devices on an IP network.
EIT	Found in a Transport Stream, the Event Information Table provides information to enable construction of Program Guides
EPG	Electronic Program Guide
FTP	File Transfer Protocol
IGMP	Internet Group Management Protocol, a protocol used to manage multicast traffic on an IP network.
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol, a protocol for synchronizing the clocks of computer systems.
PMS	Property Management System
RTSP	Real Time Streaming Protocol
SAP	Session Announcement Protocol, a protocol used to advertise the presence of multicast sessions on an IP network.
SNMP	Simple Network Administration Protocol
SSH	Secure Shell
TFTP	Trivial File Transfer Protocol, a simple file transfer protocol used on IP networks.
VoD	Video on Demand
XML	Extensible Markup Language

Section 1 - Getting Started

This section contains information on the following:

- An overview of the AvediaServer Software and Applications
- Basic configuration of the AvediaServer
- An overview of the AvediaServer Administrator's Guides

1 AvediaServer Overview

The applications displayed on the AvediaServer desktop are determined by the licence configuration. Table 2 lists the applications. Table 3 lists the application icons and their functions.

Table 2 AvediaServer Software and Applications

AvediaServer Director Software	AvediaServer Producer Software	AvediaServer Creator Software	Additional Optional Applications
Manage the AvediaServer settings, user access to content and applications, and monitor/manage the operation of your IPTV system and its devices.	In addition to all the functions of the Director Software, the Producer enables configuration of end-user interaction with the IPTV system, providing messaging, program guides, and a web server. Configure content encryption and property management systems (PMS) by adding the SecureMedia Link and PMS Link applications.	In addition to all the functions of the Director and the Producer Software, the Creator allows creation and management of recordings and their distribution/availability. Configure content encryption and property management systems (PMS) by adding the SecureMedia Link and PMS Link applications.	These applications must be ordered separately. Their operation is described in the AvediaServer Producer Software - Administrator's Guide and AvediaServer Creator Software - Administrator's Guide
Channel Monitor	**AvediaPlayer Desktop**	**Asset Editor**	**SecureMedia Link**
Director	**AvediaPlayer Desktop Management**	**Asset Manager**	**PMS Link**
Logger	**Channel Announcer**	**Play**	
System	**EPG Server**	**Recorder**	
TFTP Server	**Macro Builder**	**Transfer**	
Users	**Macro Triggers**	**Video On Demand**	
	Messaging		
	Portal Config		
	Web Server		
	(Plus Director Software Applications)	(Plus Director and Producer Software Applications)	

Table 3 Application Icons and Function

AvediaServer Applications

Asset Editor	Asset Manager	AvediaPlayer Desktop	AvediaPlayer Desktop Management
Preview and clip any listed unencrypted asset or recording	Import/Download and configure all stored content	Play back channels and content on a PC or Mac	Monitor and manage AvediaPlayer Desktop usage and activity

AvediaServer Applications

Channel Announcer

Create SAP announcements for channels created by 3rd party streaming devices

Channel Monitor

Monitor the status of all or some of the IPTV channels on the network

Director

Monitor and manage Head end devices, AvediaServers and receivers

EPG Server

Collect and manage the channel data used to display Program Guides on client devices

Logger

Specify and record system information for performance and event monitoring

Macro Builder

Create actions to be performed on devices by specified triggers

Macro Triggers

Configure triggers and specify the macro to be applied in response to the trigger event

Messaging

Set up configurable messages to be displayed on specified devices

Play

Stream content on custom channels

PMS Link

Configure the Server for operation with a Property Management System (PMS)

Portal Config

Configure the Server to provide services through Exterity receivers

Recorder

Create and manage recordings from network channels

SecureMedia Link

Configure the server for use with SecureMedia content encryption

System

Monitor and manage the basic functions of the AvediaServer

TFTP Server

Store and serve files such as firmware for other IPTV devices

Transfer

Configure and manage the location of assets and recorded content, specifying local and remote AvediaServers and FTP destinations.

Users

Create and manage user profiles and capabilities

Video on Demand

Manage content for on demand availability

Web Server

Host a third party website on the AvediaServer

2 Getting Started

This section provides a brief overview of the steps required to bring the AvediaServer up to operational status. Follow the steps below before proceeding with the AvediaServer configuration using the System and Users applications.

- Installing the AvediaServer Chassis
- Installing the AvediaServer on a Virtual Machine Platform
- Configuring the IP Address and DHCP Settings
- Installing AvediaServer and AvediaPlayer Desktop licences

Installing the AvediaServer Chassis

From version 5.0 the AvediaServer is available as a device that combines the server software with a hardware platform (and optional hard disk RAID for some platforms), and also as software only, suitable for installation on a virtual machine platform. Refer to "Installing the AvediaServer on a Virtual Machine Platform" for the minimum system requirements and the installation process.

For all AvediaServer chassis installations refer to the *AvediaServer c1500 Chassis Installation Guide* and carry out all the required installation steps up to and including "Chapter 4 - Switching the AvediaServer On".

Note: Ensure that you adhere to the personal safety guidelines and warnings displayed in the *AvediaServer c1500 Chassis Installation Guide*.

Note: From version 5.0 the physical licence dongle from Exterity has been replaced with a soft licence. The licence file is supplied on a USB memory device with the AvediaServer. It is pre-installed on the AvediaServer hardware platform but must be installed following the AvediaServer software installation on the virtual platform.

Installing the AvediaServer on a Virtual Machine Platform

Installation on a virtual machine gives customers the freedom to use their own hardware and virtual machine with Exterity software. The AvediaServer Virtual Platform option is delivered as an ISO file on a USB memory device and is licensed for a fixed MAC address supplied by Exterity. The licence file is supplied with the AvediaServer virtual platform.

Minimum Virtual Platform Requirements

The minimum Exterity recommendation for a virtual machine equivalent is:

- Intel Quad core X3430 2.40 Ghz Processor
- 2 GB RAM
- 500 GB disk space

In addition:

- Only a virtual machine install is supported, Exterity does not support simple installation on non-Exterity hardware.
- AvediaServer performance under a virtual machine cannot be guaranteed as it depends on factors such as the physical machine, virtual machine configuration parameters, and the number of other virtual machines running on the same hardware.

- Where VoD, Play or Record functions are required Exterity strongly recommends that the AvediaServer virtual machine is the only VM running on the physical machine.

Installation Process

Exterity recommends the use of propriety software such as VMware for the installation of the AvediaServer on a virtual machine. The physical machine should meet the requirements described in "Minimum Virtual Platform Requirements", above.

The AvediaServer software is supplied as an ISO image file on a USB stick. You must ensure that the virtual machine application is configured to allow selection and use of this file type during the installation.

Caution: The AvediaServer software only functions with the MAC address specified by the licence. When installing the AvediaServer software on a virtual machine you MUST configure its MAC address to match that of the supplied AvediaServer licence.

Note: The following procedure is generic and provides only a guide to the steps required for installation. Refer to the documentation for the virtual machine software in use.

To install the AvediaServer on a virtual machine:

1 Ensure the virtual machine is correctly configured to meet the requirements specified in "Minimum Virtual Platform Requirements" on page 7 and is connected to the IP network.

2 Configure the virtual machine MAC address to match that of the AvediaServer licence supplied by Exterity.

3 Insert the supplied AvediaServer Virtual Platform memory device into a USB port accessible from the browser/PC you are using.

4 Start the virtual machine and locate the AvediaServer software.

5 Proceed with the installation into the virtual machine environment.

6 On completion:

   a. Configure a static IP address for the AvediaServer VM.

   b. Log into the AvediaServer Web Interface and using the System application, install the AvediaServer and licence. Refer to "Managing AvediaServer and AvediaPlayer Desktop Licences" on page 75.

Configuring the IP Address and DHCP Settings

By default, the AvediaServer requires a DHCP Server to be available on the network to assign it an IP address. Allocating a static IP address for the AvediaServer allows continued operation without a DHCP Server.

Exterity strongly recommends using a static IP address for an AvediaServer because other Exterity devices will rely on this address remaining the same.

To assign a static IP address to the AvediaServer, temporarily set up a DHCP server on an isolated network. Once an IP address is assigned to the AvediaServer, you can configure a static IP address using the System application.

Refer to the associated virtual machine documentation to configure an AvediaServer VM installation with a static IP address.

For more information, refer to "Configuring Network Settings" on page 66.

To determine the DHCP assigned address:

There are four methods to find out the IP address assigned via DHCP:

- Check the leased IP address database of the DHCP server. Match the MAC address of the AvediaServer to an allocated IP address.

- If you already have another AvediaServer (release 3.2.0 or later) in the system, click Director > AvediaStream and select AvediaServer from the Device drop-down list. All AvediaServer MAC and IP addresses are listed.

- Connecting directly to an AvediaServer RS-232 port using a null modem cable and another computer

    - Baud rate: 115200

    - Data: 8 bit

    - Stop Bit: 1

    - Parity: None

- If you cannot use any of the methods listed above, connect a keyboard, mouse and monitor directly to the AvediaServer chassis ports.

    a. At the Operating System screen, log in using the username=serveradmin and password=labrador.

    b. Locate and click the Firefox icon or click Applications > Internet > Firefox to launch the browser.

    c. Enter   http://localhost in the browser address field to display the AvediaServer web interface.

    d. Log in locally using the username=admin and password=labrador.

    e. Start the System application and click the Network tab. The AvediaServer IP address information is listed.

Installing AvediaServer and AvediaPlayer Desktop licences

AvediaServer Chassis/Software combinations are delivered with the purchased licences pre-installed and require no further configuration. AvediaServer VM installations require the licences to be installed following the software installation. If you are upgrading AvediaServer application and/or bandwidth licences, adding more AvediaPlayer Desktop licences, or completing an AvediaServer VM installation, refer to the procedures described in "Managing AvediaServer and AvediaPlayer Desktop Licences" on page 75.

3 AvediaServer Applications and Documentation

The Exterity AvediaServer is a modular system both in terms of the physical hardware and the applications. To help you make best use of the AvediaServer and its applications, the following documentation is available.

Hardware

The AvediaServer Installation Guide contains all safety and regulatory information and shows you how to install the AvediaServer in a rack, power it on, and connect it to the IP network. Hard drive replacement for the c1555 chassis is also described. If you have installed AvediaServer in a virtual machine environment, refer to the documentation supplied for the installation device.

Software Modules

Director Software

The *AvediaServer Director Software - Administrator's Guide* shows you how to manage and maintain the core functions of the AvediaServer including its licensing, IP network settings, system name and location, time server, user accounts, and monitor and manage the operation of the IPTV system and its devices.

Refer to the *AvediaServer Director Software - Administrator's Guide* for more information about using the **Channel Monitor**, **Director**, **Logger**, **System**, **TFTP Server**, and **Users** applications.

Producer Software

The *AvediaServer Producer Software - Administrator's Guide* shows you how to manage the client interfaces and deliver content, providing messaging, program guides, content encryption, middleware such as property management systems (PMS), and a web server.

Refer to the *AvediaServer Producer Software - Administrator's Guide* for more information about using the **AvediaPlayer Desktop**, **AvediaPlayer Desktop Management**, **Channel Announcer**, **EPG Server**, **Macro Builder**, **Macro Triggers**, **Messaging**, **Portal Config**, and **Web Server** applications.

Creator Software

The *AvediaServer Creator Software - Administrator's Guide* shows you how to create, edit and manage recordings and configure their distribution and availability.

Refer to the *AvediaServer Creator Software - Administrator's Guide* for more information about using the **Asset Editor**, **Asset Manager**, **Play**, **Recorder**, **Transfer**, and **Video on Demand** applications.

Non-Module Software

The SecureMedia Link and PMS Link are applications which can be ordered in addition to the Producer or Creator Software modules. They are not available with the Director module.

Specialised Applications

Refer to the *AvediaServer Producer Software - Administrator's Guide* or the *AvediaServer Creator Software - Administrator's Guide* for more information about the **SecureMedia Link**, and **PMS Link** applications.

Scope

This edition of the manual refers to version 5.0 of the AvediaServer and describes the operation and use of the applications listed in "AvediaServer Software and Applications" on page 5.

Conventions

The following conventions are used in the AvediaServer Administrator's Guides:

Note: A Note calls attention or adds information that is important for the proper operation of the product.

Caution: A CAUTION notice calls attention to an operating procedure or practice that, if not correctly performed, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

`Courier Font` - is used to identify scripts, code examples, or keyboard commands.

Emphasis is used when referring to another document, for example *AvediaServer Chassis Installation Guide*.

Audience

This manual is intended for use by systems integrators or systems administrators who are installing and setting up Exterity products.

It is assumed that readers are familiar with installing and configuring network-based products. Ideally, readers will also have an understanding of the key features of an IPTV system.

Copyright

The Exterity AvediaServer is a powerful product that allows you to import (copy) content (audio & video) and subsequently distribute that content to large numbers of users over an IP network. Content may have a copyright and you should always secure the permission of the copyright holder in order to copy and transmit the content on the IP network.

Unauthorised use and/or duplication of copyrighted material may be a violation of copyright law in one or many countries/regions. In using the AvediaServer you accept full responsibility for the copyright status of the content you import and transmit on the IP network.

Safety

This guide refers to the AvediaServer applications only. For all Safety and Regulatory information associated with the AvediaServer chassis please refer to the *AvediaServer Chassis Installation Guide* located in the Servers page at: www.exterity.com/support/productdocs.html.
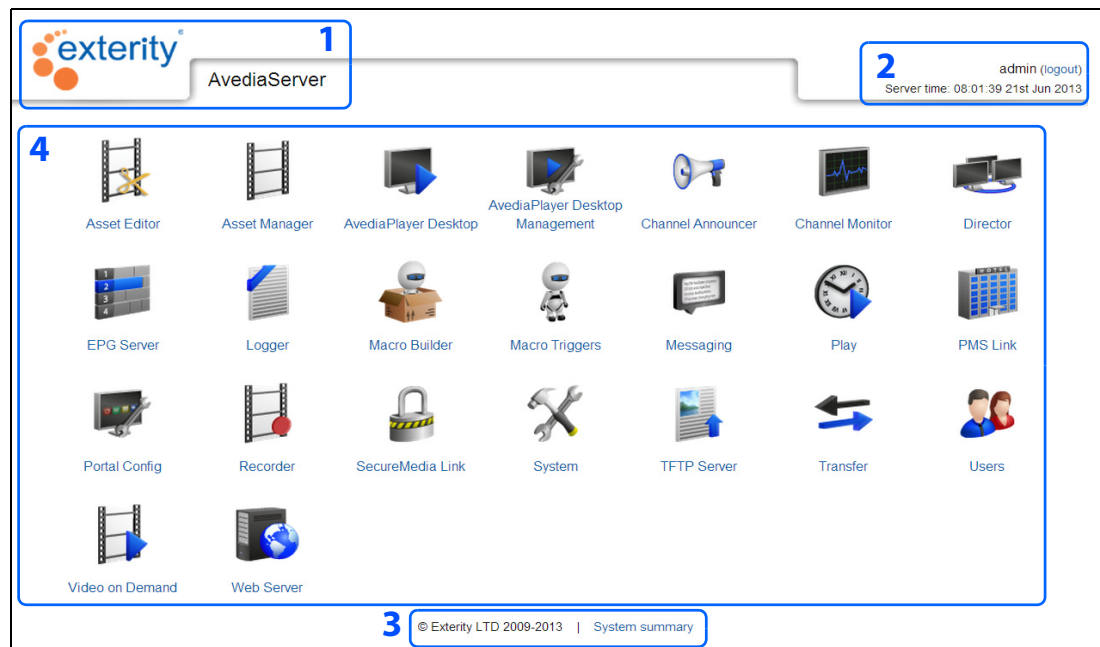
4 Management Interfaces

The AvediaServer has two management interfaces as follows:

- Web Management Interface
- Admin Interface

Web Management Interface

You can manage every aspect of AvediaServer functionality using the Web Management Interface and the available applications. The Web Management Interface is optimised for Microsoft Internet Explorer and Mozilla Firefox browsers.

Figure 1 *AvediaServer – Web Management Interface*

Table 4

Element	Description	
1	Logo and active application	Displays the active application. Figure 1 shows the AvediaServer home screen with all available applications. To return to the home screen from an application, click the Exterity logo.
		Click the selected application name (or the down arrow) to hide the application page. This allows you to see and/or select another application from the home screen.

Table 4

2	User, Logout, and time	The logged-in user name, logout function and server time are displayed. This is either 'admin' or an assigned user name. If Active Directory access has been configured the user's common name is displayed. Click logout to close the session and return to the login screen.
3	System summary	The System summary function displays basic information about the AvediaServer such as the IP address, serial number and configured name and location. Click the Exterity logo to return to the home screen.
4	Applications	All the applications enabled by the licence configuration or login profiles are displayed on the home screen.

Open the Web Management Interface as follows:

1   Determine the IP address of the AvediaServer using the methods described in Configure the IP address and DHCP Settings.

2   Open a browser window and enter the IP address of the AvediaServer directly into the address field.

The AvediaServer login page is displayed:

Figure 2   *AvediaServer login page*

3   The default login details are:

    Username: admin

    Password: labrador

4   The Web Management Interface opens in your browser, as shown in Figure 2.

5   Refer to Table 4 for interface summary information.

Note: By logging into the AvediaServer you are accepting the terms of the Exterity Licence Agreement.

The administrator can change the admin password in the Users application. For more information, refer to "Changing the Admin Account" on page 94.
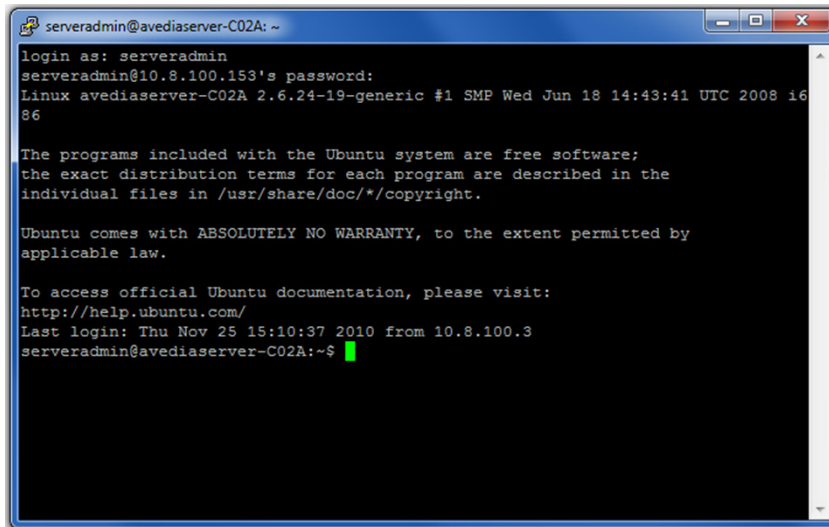
Admin Interface

In certain circumstances it may not be possible to manage the AvediaServer via the Web Management Interface. If you know the IP address of the AvediaServer, you can use a terminal application (such as PuTTY) to provide an SSH connection to the Linux kernel.

Alternatively, connect a mouse, keyboard, and VGA monitor to the AvediaServer chassis interfaces.

Log into the Admin Interface using the following login details:

Username: serveradmin

Password: labrador

Figure 3 *Admin interface*

Note: The same login credentials can be used for local access when using directly connected monitor, keyboard and mouse.

Section 2 - Director Applications

This section contains the following:

- Using the Director Application
- Using the Channel Monitor Application
- Using the Logger Application
- Using the System Application
- Using the Users Application

5 Using the Director Application

The AvediaServer Director application is provided with all AvediaServer configurations and allows administrators, or users with administrator level access (specified by their profile), to control and manage the IPTV system from anywhere on the network.

Figure 4 *Director – All Devices Page*

With the AvediaServer Director application you can:

View

Using the available view options the Director application offers four views (All Devices, New Devices, AvediaStream, and Receivers) of key information:

• A matrix of all the Exterity devices on the network, showing details such as:

  • Device type

  • Location

  • IP address

• New device view listing all Exterity devices that have been recently discovered over a configurable time interval.

• Scheduled task view showing all scheduled commands.

Monitor

• User selections (content/volume) on any receiver in the IPTV network (Receivers page only).

Control

- AvediaStream TVgateways for live broadcast TV and radio.

- AvediaStream Encoders for video from DVD/Blu-ray players and video cameras.

- AvediaStream Transcoder for streamed AV transcoding.

- AvediaServer to set name, location and ping.

- AvediaPlayer Receivers for single or multiple unit control such as display of messages, channel and volume change settings.

- Mass configuration of multiple IPTV devices e.g. upgrades and mass channel change.

- Task scheduling; any command that can be sent to a device can be scheduled to run at a later date.

Note: You must be a member of the admin profile, or have the Director application access enabled in your profile to access the Director functions. Refer to the Users application section of the Managing the AvediaServer - Administrator's Guide for more information.

Access Director functions from the AvediaServer Web Management Interface homepage by

clicking the Director [image] icon and selecting the menu page as required.

Figure 4 shows the Director application open at the All Devices page.

Getting Started

This section shows you how to carry out the basic configuration of the Director application. Unless specifically required, use the default settings to manage the devices and channels within the IPTV network.

Note: The Device Listener and Channel Listener services must be running on the System application Services page for devices and channels to be added automatically. Ensure the Start on Boot Disable button is displayed, indicating the services are configured to start on boot.

Figure 5 *Device and Channel Listener Services*

Director Configuration

The Director application Configuration page allows you to specify the Channel Monitoring and Device Monitoring ageing settings, and the SNMP (Simple Network Management Protocol) settings.

Figure 6 *Director Application – Configuration Page*

Device Monitoring

The AvediaServer Director application discovers Exterity devices by listening for device discovery messages. These discovery messages, known as keep-alive traps, are SNMP traps broadcast to UDP port 162. AvediaPlayer r92xx receivers with v2.0 firmware or later, TVgateway 4.2.11 or later, SD encoder 2.3.3 or later, and HD encoder 1.3.4 or later can unicast or multicast.

These messages are local to a subnet/VLAN. If any of the Exterity devices are on a different subnet/VLAN from the AvediaServer, you must configure the router to forward these broadcasts to the AvediaServer, or manually add the devices.

If you add the devices manually without forwarding the SNMP Multicast trap, after the defined timeout, the units are highlighted (RED) in the AvediaServer Director.

The keep-alive traps sent by Exterity devices occur at 30 second intervals and are used by the Director application device ageing process. On discovering a new device, a new line containing the device details is added to the list. You can list devices by type using the filters available on the device view pages, All Devices, AvediaStream and Receivers. You can also determine the most recently added devices using the New Devices page (default one minute). All pages are available in the Director application.

Device Ageing

Device ageing is enabled by default, and the colour coding of a device entry in the view pages indicates normal operation (no colour), a period of inactivity (yellow), or a more serious problem such as an un-contactable device (red). Device ageing is enabled/disabled using the checkbox on the Configuration page. The following settings are available (default values are in brackets):

- Device Ageing (enabled): Check/un-check the box as appropriate. When checked, device ageing is enabled.

- Device Query Interval (30): Specifies the length of delay between the receipt of a device discovery message and the query from the server in response: (30-600 seconds). A larger value reduces network traffic between the AvediaServer and the device.

Note: Devices are permanently highlighted red if the Device Listener is turned off (for more than 180 seconds). Ensure it is enabled on the System application Services page.

Also, if the Director application cannot receive device discovery messages from them, if for example, the devices are on a different subnet/VLAN, you may want to disable the device ageing feature.

If you add the devices manually without forwarding the SNMP Multicast trap, after the defined timeout, the units are highlighted (RED) in the AvediaServer Director.

To configure device monitoring:

1   Start the Director application.

2   Click the Configuration tab:

3   Click the Device Ageing check box.

4   Enter the value in seconds for the Device Query Interval you want to use to monitor device activity.

5   Click Apply.

SNMP

In most cases SNMPv2 is used to communicate with Exterity devices in the IPTV network. The community string is a password which the Director must present to a device in order to change any settings. All Exterity devices on the network must use the same community string. If you want to use a non-default community string, you must first configure this on the individual devices via the web interface or by importing a configuration.

Note: All end devices must use the same community string. If they do not, devices may not be visible, or contactable by the Director. Refer to "Configuring the SNMP Community Strings" on page 66 for more information.

To configure SNMPv2:

1   Start the Director application.

2   Click the Configuration tab:

3   Enter the required Read/write community string: The default is public.

4   Enter the required Read only community string: The default is public.

5   Enter a value for the SNMP retries per device: This configures the number of times the Director application retries an SNMP request before deciding it cannot communicate with the device. The default is 1, the range 1 to 10.

6   Enter a value for SNMP initial timeout period: This configures the time Director waits for a response from a device before retrying, or after reaching the specified number of retries, deciding it cannot communicate with the device. The default is 2 seconds, the range 1 to 30.

7   Click Apply.

Enabling the Windows Telnet Client

You can click the icon in the AvediaServer Director application device view pages to make a telnet connection to a device and use the admin interface. This process makes use of the Windows Telnet client, which is not enabled by default.

To enable the Windows telnet client (Windows 7 example):

1   Click the Windows Start button and select Control Panel.

2   Select Programs and Features from the list.

3   Click on the Turn Windows features on or off hyperlink.

4   Click the Telnet Client checkbox.
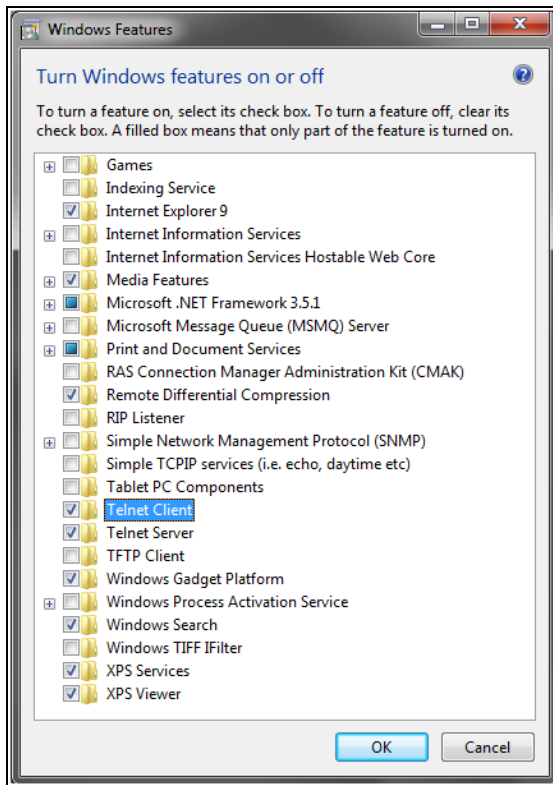

Figure 7 *Enabling Windows Telnet Client*

5   Click OK to apply the settings and close the window.

Viewing Devices

AvediaServer Director collects data from the devices in the IPTV system and presents the information in orderable and searchable lists. This data is displayed on several pages of the Director application as listed in Table 2. The Device Listener must be enabled for accurate and up-to-date device information. Device Listener is located on the System application Services page.

Table 5 Device View Pages

Page	Description
All Devices	Lists details of all discovered devices in the IPTV network including AvediaStream Encoders, Transcoder, TVgateways, Receivers, Chassis Monitors, and AvediaServers.
New Devices	Lists details of newly discovered IPTV Network devices. (Default one minute.)
AvediaStream	Lists details of all devices capable of streaming content on the network: AvediaServers, Encoders, Transcoder, and TVgateways.
Receivers	Lists details of all IPTV receivers including receiver specific parameters such as the currently selected channel.

Using the active functions on these pages you can order the information by any of the listed parameters. In addition you can apply functions such as reboot to a single device, a group of selected devices, or to all.

Device View Pages

The device view pages offer similar listing and action functions. The Receivers page also gives you the option of displaying additional device specific information.

Figure 8 *Director – All Devices Page*

Page Layout and Functions

This section describes the highlighted areas of the Device View Page shown in Figure 3 and the functions available.

1   Page Title

2   Actions and Filters

3   Column Headings

4   Select, Filter, and Column Search Functions

5   Device Details

6   Page Control

Page Title

The pages available from the Director application are displayed in tabs. Device views include All Devices, New Devices, AvediaStream, and Receivers.
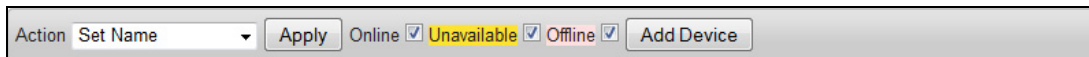

Figure 9 *Page Titles*

Actions and Filters

The Filter functions allow you to include or omit Unavailable and Offline devices in the table. The Action drop-down list allows you to perform functions, such as reboot, on single or groups of devices.

All Pages

Figure 10 *All pages action bar*

- Action drop-down list and Apply button – allow you to perform operations on devices selected in the list. Select actions from the drop-down list, then click Apply. Refer to "Managing Devices" on page 25 for more information.

- Online – This filter function populates the list with on-line devices when enabled by a tick in the check box.

- Unavailable – This filter function includes Unavailable devices in the list when enabled by a tick in the check box. The unavailable status is determined by the time expired since the previous device discovery message as specified by the Device Ageing settings.

- Offline – This filter function includes Offline devices in the list when enabled by a tick in the check box. The Offline status is determined by the time expired since the previous device discovery message as specified by the Device Ageing settings.

    Note: Ensure the Device Listener Service is enabled on the System application Services page to ensure up-to-date device information.

- Add Device – This function allows you to manually add a device. For more information refer to "Manual Device Addition" on page 35.

New Devices Page Only
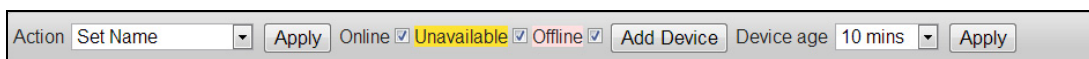
Figure 11 *New Devices Page Action Bar*

- Device age drop-down list and Apply button – Allows you to list devices by the length of time since discovery by the Director application. To view most recently discovered devices, select a short time value.

Receivers Page Only
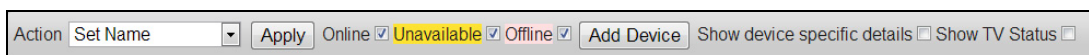
Figure 12 *Receivers Page Action Bar*

- Show device specific details – When enabled, shows additional Receiver information in the table. For more information refer to "Additional Receivers Page Information" on page 23.

- Show TV Status – When enabled, shows the status of the connected TV. (Only available with certain TV models using the serial interface, not available through CEC.)

Column Headings

Column Headings allow you to order the list by the heading title. For example, to order the list by device name click Name. To invert the order press Name again.

The default list order is sorted by Device.

Figure 13 *Column Headings*

- Device – Displays the type of IPTV device: AvediaServer, Encoder, Transcoder, TVgateway, Chassis Monitor, or Receiver.

- Version – Displays the version of firmware running on the device.

- Name – Displays the name assigned to the device. You can change this using the Set Name Action as described in "Naming a Device" on page 34.

- Location – Displays the assigned location name of the device. You can change this using the Set Location Action as described in "Assigning a Device Location" on page 34.

- MAC – Displays the MAC address of the device.

- Address – Displays the IP address of the device.

- TFTP Server – Displays the configured address of the TFTP Server. The TFTP Server is used for functions such as uploading new firmware to a device. You can change this using the Set TFTP Server Action as described in "Setting a Device TFTP Server Address" on page 29.

- Syslog Server – Displays the configured address of the Syslog Server. The Syslog Server is used by devices for storing system log files. You can change this using the Set Syslog Server Action as described in "Setting the Device Syslog Server Address" on page 32.

Additional Receivers Page Information

The Receivers page displays additional information about each receiver such as the selected channel.

Current Mode	Channel	Volume	Groups	EPG Server	Browser Homepage	TV Status
▼	<search>	<search>	<search>	<search>	<search>	▼
AV	BBC NEWS	20	all	10.8.100.153	www.exterity.com	Unknown
AV	AvediaStream (AR+ESK) 000073-A	0	all		10.8.100.84/portal	Unknown
AV	BBC TWO Scot	20	all	0.0.0.0		Unknown

Figure 14 *Additional receiver information*

To view this information click the Receivers tab and click the Show device specific details checkbox in the Actions and Filters panel. You can change one or more receivers using the Actions listed. In addition to the details shown on All Devices, New Devices and AvediaStream pages, the Receivers page also lists the following:

- Current Mode – Displays the current receiver mode, for example, AV, Browser, EPG, and Splash screen. You can use the Mode drop-down list to display only receivers in a specific mode.

- Channel – Displays the channel name, or multicast address if the channel name is not known, of the currently selected channel for the receiver. You can also search for any receivers playing a specific channel by entering the channel name or multicast information into the Channel <search> field. You can change the selected channel one or more receivers using the Set Channel Action, as described in "Setting a Channel" on page 38.

- Volume – Displays the current receiver volume setting. You can search for any receivers set to a specific level by entering the value into the Volume <search> field. You can change the volume setting on one or more receivers using the Volume Action as described in "Setting the Volume" on page 41.

- Groups – Displays the name of the groups from which the receiver can access AV content. You can search for any receivers set to a specific group by entering the group name into the Groups <search> field. You can change the group setting one or more receivers using the Groups Action as described in "Setting Groups" on page 40.

- Browser Homepage – Displays the URL for the Homepage configured for the receiver. You can search for any receivers set to a specific homepage by entering the url into the Browser Homepage <search> field. You can change the homepage setting on one or more receivers using the Set Homepage Action as described in "Setting the Homepage" on page 39.

- TV Status – Use this to filter the list to find receivers where the connected TV is powered on. This function is only applicable if the receiver is connected via the serial interface to a TV supporting an external control connection (when the Show TV Status checkbox is ticked. Also not available when connected using CEC to a supported TV).

Select, Filter, and Column Search Functions

Select, Filter, and <search> functions allow you to globally select or deselect devices, filter for specific device types or version numbers, and to search for a specific value in a table column.

Device	Version	Name	Location	MAC	Address	TFTP Server	Syslog Server
Select: ▾ All ▾	▾	<search>	<search>	<search>	<search>	<search>	<search>

Figure 15

- Select and Filter – Allows you to select, or deselect, all devices in the list. You can filter for a device type and/or a specific firmware version using the drop-down selections. For example, to list and select all version 2.1.0 AvediaStream Encoders, select All from the Select drop-down list, Encoder from the Device drop-down list, and 2.1.0 from the Version list.

- Column Search – Allows you find a device using only one specified parameter. For example, to determine which device is using a specific IP address, enter the address into the Address <search> field. Click Return/Enter to initiate the search and display the device (if found). You can refine a search by adding search criteria into more than one column. To reset the search, delete the criteria from the search fields and click on the page.

Device Details

Each row lists the Device Details in accordance with the column headings.

☐	Encoder	9.9.9	e2110-022447	🔧 HW Lab	00:18:1C:02:24:47	10.8.100.108	194.168.0.28	
☐	Receiver	2.0.1	00005e	🔧 Default	00:18:1C:00:00:5E	10.8.100.157	10.8.64.24	0.0.0.0(disabled)

Figure 16 *Device Details*

- ☐ – use the check box to select/deselect a device.

- Colour coding - The status is indicated by the colour coding, red and yellow indicating Unavailable and Offline. If Unavailable and Offline checkboxes are de-selected, only on-line devices are displayed. If selected (a tick in the check box), the device listing is highlighted in the same colour as the Actions and filters panel.

- Select Checkbox – Indicates if the device has been selected in order to execute a selected Action.

- Name Hyperlink – Allows you to access the Web management interface for the device. To access a device, click the name link and enter the user name and password as prompted.

- Telnet Hyperlink – is shown in the 🔧 hyperlinked icon. Click the icon to open the device admin interface using telnet. (Only available when it is supported by the device type.)

Note: A telnet client must be associated with your browser to access the device with the telnet hyperlink. Refer to "Enabling the Windows Telnet Client" on page 19 for more information.

Page Control

The paging step buttons allow you to page through longer lists of devices. You can also choose to display more or fewer devices on a single page by selecting a value from the drop-down list. The default number of devices per page is 10. The total number of devices is also shown in brackets, for example: (1-10 of 35 Device(s)).

⏮ ◀ Page 4 of 8 (31-40 of 77 devices) ▾ ▶ ⏭

Figure 17 *Page Control*

Navigate through the pages by clicking the step forward/back single arrows, or the jump to end/beginning double-arrows.

Managing Devices

This section describes how to manage devices in the IPTV network. You can carry out maintenance and configuration procedures on the devices listed in any of the four device viewing pages.

The procedures are available from the Action drop-down list on the All Devices, New Devices, AvediaStream and Receiver pages. Not all actions can be applied to all devices, as shown in Table 6.

Table 6 Actions and Devices

Action	AvediaServer	Encoder & Transcoder	Receiver	TVgateway	Chassis Monitor
Set Name	✓	✓	✓	✓	✓
Set Location	✓	✓	✓	✓	✓
Reboot		✓	✓	✓	✓
Ping	✓	✓	✓	✓	✓
Upgrade Firmware		✓	✓	✓	✓
Factory Reset		✓	✓	✓	✓
Export Config		✓	✓	✓	✓
Import Config		✓	✓	✓	✓
Set TFTP Server		✓	✓	✓	✓
Set Syslog Server		✓	✓	✓	✓
IR Assistant		✓			
Set Display Mode			✓		
Set Channel			✓		
Set Homepage			✓		
Set Groups			✓		
Set Splash Screen			✓		
Set Volume			✓		
Refresh	✓	✓	✓	✓	✓
Delete	✓	✓	✓	✓	✓

Many of these actions can be performed individually from the web management interface of the respective device. However, the Director application allows you to select and group together same-type devices and simultaneously apply a procedure, greatly reducing the time required to perform tasks such as firmware upgrades. If more detailed device configuration is required, access the Web Interface by clicking on the respective device Name hyperlink.

Actions can be divided into three groups:

• Maintenance Tasks

• Configuration Tasks

• Receiver Operational Tasks

Maintenance Tasks

This section details maintenance tasks which can be carried out on Exterity devices using the Action function. These are:

• Rebooting a device

• Pinging a device

• Resetting a device to factory settings

• Deleting a device

The following tasks require the use of a TFTP Server. Refer to Chapter 9, "Using the TFTP Server Application" to configure the AvediaServer TFTP Server application before carrying out the following tasks:

- Setting the Device TFTP Server Address

- Upgrading Device Firmware

- Exporting a Device Configuration

- Importing a Device Configuration

After setting the Device Syslog Server Address a device can send its log files to a specified Syslog server.

Rebooting a Device

You can reboot a device if you simply want to return a device to the configured state, or suspect it is not operating correctly. Rebooting is often used as the second step in correcting a suspected fault situation (following Ping) and also has the benefit that physical access to the device is not required. You can reboot Encoders, Transcoders, Chassis Monitors, TVgateways and Receivers.

To reboot devices:

1   Open the Director application and select a suitable device view page to locate the device(s) you want to reboot. If necessary, use the Device filter, column heading list ordering, or search functions to help you find the device(s).

2   Select the device(s) for rebooting. If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

3   Click the Action drop-down list and choose Reboot.

4   Click Apply.
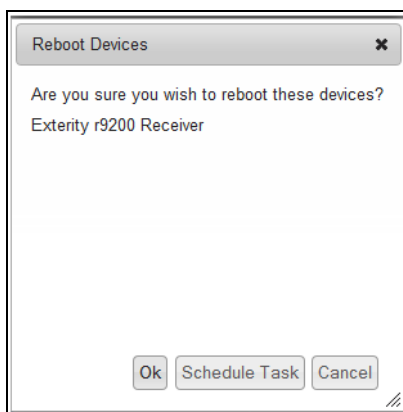
Figure 18 *Rebooting a receiver*

5   Click Ok to continue. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

6   Confirm the Name entry for the device steps through the following sequence:

   a. Reboot scheduled

   b. Reboot in progress

   c. ✅ and device name

The ✅ mark indicates the operation has been successful and is complete. If unsuccessful, a ❌ is displayed.
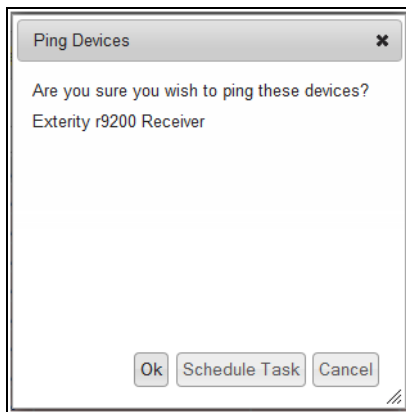
Pinging a Device

A ping test performs a basic but effective check to determine if devices are reachable across the network and can return the packets as received. You can ping all devices.

To ping devices:

1. Open the respective Device View page for the device, or devices you want to ping.

2. Use the Device filter, column heading list ordering or search functions to help you find the device(s).

3. Select the device(s) you want to ping. If, after filtering, the list contains only the required devices, you can choose All from the Select drop-down list.

4. Click the Action drop-down list and choose Ping.

5. Click Apply.

Figure 19 *Pinging a Device*

6. Click Ok to continue. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

7. Confirm the Address entry for the device steps through the following sequence:

   a. Ping scheduled

   b. ✔ and device address

The ✔ mark indicates the operation has been successful and is complete. If unsuccessful, a ✖ is displayed.
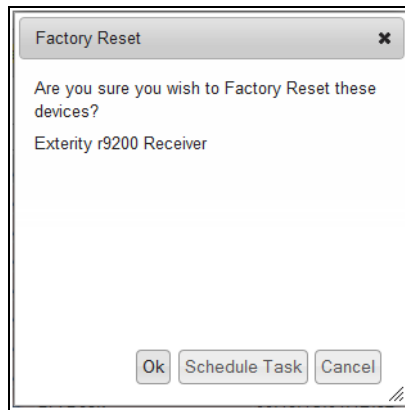
Resetting a Device to Factory Settings

A device can be returned to a known condition using the Factory Reset action. Using this action clears all configured fields and returns all settings to their default value. You can reset encoders, transcoders, TVgateways, chassis monitors, and receivers.

Note: The device is also returned to DHCP operation. With no available DHCP Server on the network the device my be lost.

To reset devices to factory settings:

1. Open the respective Device View page for the device, or devices you want to reset.

2. Use the Device filter, column heading list ordering or search functions to help you find the device(s).

3. Select the device(s) you want to reset. If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4. Click the Action drop-down list and choose Factory Reset.

5. Click Apply.

Figure 20 *Resetting to factory Values*

6 Click Ok to continue. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

7 The following message is displayed:
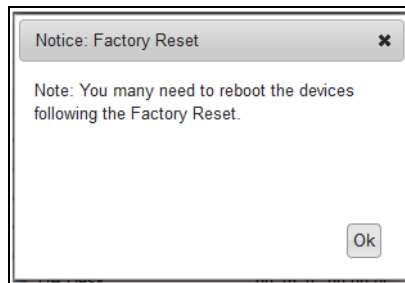
Figure 21 *Reboot Notice*

Note: "Rebooting a Device" on page 26 describes the rebooting procedure.

8 Confirm the Address entry for the device steps through the following sequence:

a. Factory Reset scheduled

b. ✔ and device address

The ✔ mark indicates the operation has been successful and is complete. If unsuccessful, a ✖ is displayed.

Deleting a Device

Devices discovered by the Director application remain listed unless manually deleted. For example, a device may have been a temporary addition to the system and has now been removed. Its details remain in the table but are redundant. You can delete all device types, including AvediaPlayer Desktop clients.

To delete a device from the list:

1 Open the respective Device View page for the device, or devices you want to remove.

2 Use the Device filter, column heading list ordering or search functions to help you find the device(s).

3 Click the Select check box for the device(s) to be deleted. If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4 Click the Action drop-down list and choose Delete.

Click Apply to delete.

5 Confirm the device(s) has been removed.

Setting a Device TFTP Server Address

Exterity devices use TFTP to download firmware images and other files (for example, IR config files and splash screens). In order to carry out any of these tasks, the device must be configured with the IP address of the TFTP Server. You can configure the TFTP server address for Encoders, Transcoders, TVgateways, Chassis Monitors, and Receivers. Enter the IP address of a known TFTP server, or accept the default IP address of the local AvediaServer TFTP Server application if you also want to use it as the TFTP server.

To set the device's TFTP server address:

1   Open the respective Device View page for the device, or devices, you want to set.

2   Use the Device filter, column heading list ordering or search functions to help you find the device(s).

3   Select the device(s) for setting the server address. If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose Set TFTP Server.

5   Click Apply.
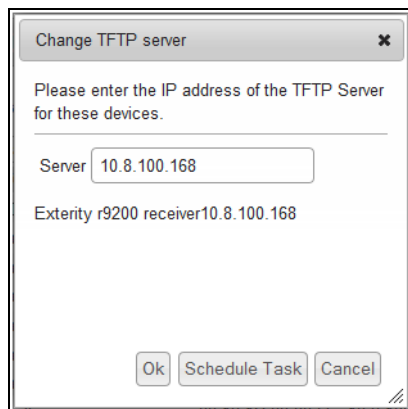
Figure 22 *Changing TFTP Server*

6   Enter the IP address and click Ok. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

7   Confirm the TFTP Server entry for the device steps through the following sequence:

   a.   TFTP Server change scheduled

   b.   TFTP Server change in progress

   c.   TFTP Server address and ✅

The ✅ mark indicates the operation has been successful and is complete. If unsuccessful, a ❌ is displayed.

Upgrading Device Firmware

Before upgrading, ensure that the TFTP server address is set correctly on the device(s) you want to upgrade and that the appropriate firmware files are present in the root directory of the TFTP server. Once the upgrade is initiated, the device(s) downloads firmware from the TFTP server.You can upgrade Encoders, Transcoders, TVgateways, Chassis Monitors, and Receivers.
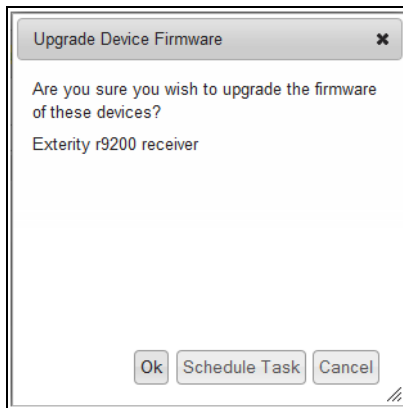
Ensure the required firmware file has been made available in the root directory on the TFTP Server application, and that the TFTP server address has been configured on each device you want to upgrade. Refer to "Uploading Files to the TFTP Server" on page 89, "Copying Files to and from TFTP root" on page 92, and "Setting a Device TFTP Server Address" on page 29 for more information.

To upgrade device firmware:

1   Open the Device View page for the device you want to upgrade.

2   Use the Device filter, column heading list ordering or search functions to help you find the device(s).

3   Select the device(s) for upgrading. If, after filtering, the list contains only the required devices, choose All from the Select drop-down list.

4   Click the Action drop-down list and choose Upgrade Firmware.

5   Click Apply.

Upgrade Device Firmware   ✖

Are you sure you wish to upgrade the firmware
of these devices?

Exterity r9200 receiver

[Ok] [Schedule Task] [Cancel]

Figure 23   *Upgrading Device Firmware*

6   Click Ok to continue. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

7   Confirm the Name entry for the device steps through the following sequence:

 a.   Firmware Upgrade scheduled

 b.   Device name and ✅

8   The ✅ mark indicates the operation has been successful and is complete. If unsuccessful, a ❌ is displayed.

Note: The upgrade process may require a longer period of time than the configured device ageing settings. This is likely to result in the device being highlighted in red, indicating it is offline, until the process has been completed.

Exporting a Device Configuration

Once you have configured a device, you can save its settings to another location using the AvediaServer TFTP Server application. If required, you can subsequently use the saved settings to restore a device to that configuration. Device name, Location and IP addressing information is not exported, therefore an exported configuration can be imported onto other units. You can export the configuration of Encoders, Transcoders, TVgateways, Chassis Monitors, and Receivers.

Note: Ensure that the TFTP Server address is configured correctly. Refer to "Setting a Device TFTP Server Address" on page 29 for more information.
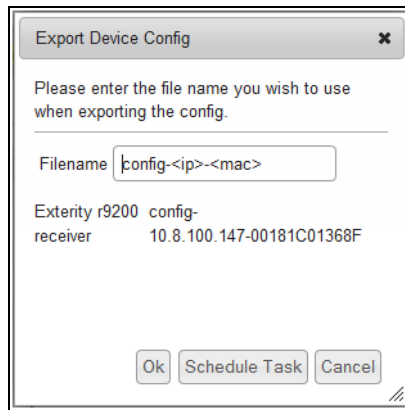
To export a device configuration:

1   Open the respective Device View page for the device with the configuration you want to save.

2   Use the Device filter, column heading list ordering or search functions to help you find the device.

3   Select the required device(s).

Click the Action drop-down list and choose Export Configuration.

4   Click Apply.

Figure 24 *Exporting device configuration*

5   Enter the file name you want to use and click Ok to continue. The default file name is config-<ip>-<mac>. (config-IP address of the device-MAC address of the device.) Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

6   Confirm the Name entry for the device steps through the following sequence:

   a.   Export Config scheduled

   b.   Export in progress

   c.   Name and ✅

7   The ✅ mark indicates the operation has been successful and is complete. If unsuccessful, a ❌ is displayed.
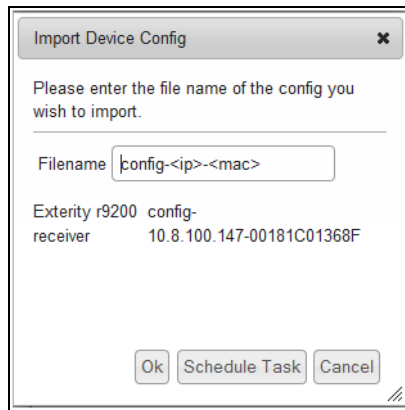
Importing Device Configuration

You can import previously saved device configuration files. As the name and IP address of a device is not saved as part of the configuration file, you can apply a single saved configuration to multiple devices if required.

Ensure the required configuration file has been made available in the root directory of your TFTP server, and that the TFTP server address has been configured on each device you want to upgrade. Refer to "Uploading Files to the TFTP Server" on page 89, "Copying Files to and from TFTP root" on page 92, and "Setting a Device TFTP Server Address" on page 29 for more information.

To import device configuration:

1   Open the respective Device View page for the device(s) you want to assign to a known configuration.

2   Use the Device filter, column heading list ordering or search functions to help you find the device.

3   Select the required device(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose Import Config.

5   Click Apply.

Figure 25 *Importing device configuration*

6 Click Ok to continue, Cancel to abort, or click Schedule Task to specify when this operation should take place. See "Creating Scheduled Tasks" on page 42 for more information about the Schedule Task option.

7 Confirm the Location entry for the device steps through the following sequence:

   a. Import Config scheduled

   b. Import Config in progress

   c. New device location and ✅

The ✅ mark indicates the operation is successful and complete. If unsuccessful, a ❌ is displayed.
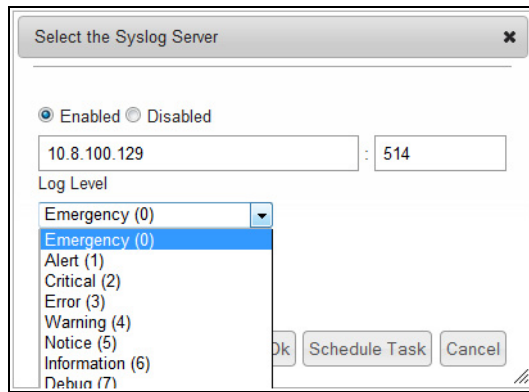
Setting the Device Syslog Server Address

Exterity devices store log files locally by default. However, you can configure the Logger application for storing system log files. In order to save the files, the remote device must be configured with the IP address of the Logger application. In addition to the address of the Logger, you can set the logging level on the remote device. Encoders, Transcoders, TVgateways, Chassis Monitors, and Receivers can be configured for remote logging to the Logger application.

Note: To configure the syslog server address on a remote device click the device Name hyperlink, log in, and set the remote address in the logging page of the web management interface using the IP address of the AvediaServer.

To set the syslog server address:

1 Open the respective Device View page for the device, or devices you want to configure.

2 Use the Device filter, column heading list ordering or search functions to help you find the device(s).

3 Select the required device(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4 Click the Action drop-down list and choose Set Syslog Server. Click Apply and the following window is displayed:

Figure 26 *Setting Syslog Server Address*

5   Enter the IP address of the syslog server where the log files are to be stored. This is most likely the local AvediaServer but can be a remote server if preferred.

6   Enter the port number on the syslog server. The default value is 514.

7   If not already set, click Enabled.

8   Select an option from the Log Level drop-down list. The values range from 0-Emergency to 7-Debug, where 0 creates the least debug information, 7 the most.

9   Click Ok to continue. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

10   Confirm the Name entry for the device steps through the following sequence:

   a.   Syslog Server change scheduled

   b.   Name and ✅

The ✅ mark indicates the operation is successful and complete. If unsuccessful, a ❌ is displayed.

Configuration Tasks

This section details some configuration tasks which can be applied to Exterity devices using the actions available on the device view pages. If more detailed configuration is required for a device, access its web management interface by clicking the respective device Name hyperlink. All tasks can be initiated immediately or scheduled to occur at a specified time. Many configuration actions apply only to Receivers and are highlighted. The Localisation page is also used.

You can apply the following types of configurations using the Action function:

•   Set Name

•   Set Location

•   Manual Device Addition

Receiver only Actions:

•   Set Display Mode

•   Set Channel

•   Set Homepage

•   Set Groups

•   Change the Splash Screen
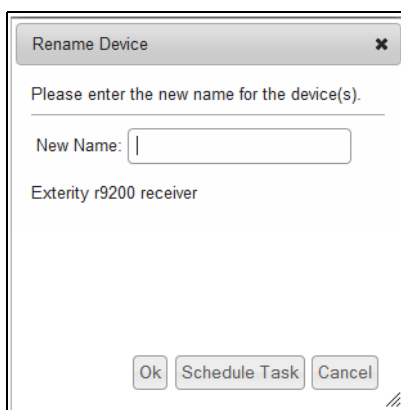
•   Set Volume

Naming a Device

Naming a device, and adding a location, helps you manage devices in the IPTV network. You can name Encoders, Transcoders, TVgateways, Chassis Monitors, AvediaServers, and Receivers. A representative naming system for Receivers is both useful and important for PMS systems where the guest's name is matched to the Receiver name/location.

To name devices:

1   Open the respective Device View page for the device you want to name.

2   Use the Device filter, column heading list ordering or search functions to help you find the device.

3   Select the device from the list.

Click the Action drop-down list and choose Set Name.

4   Click Apply to display the following window:

Figure 27   *Renaming a device*

5   Enter the name you want to use and click Ok. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

6   Confirm the Name entry for the device steps through the following sequence:

   a.   Rename scheduled

   b.   Rename in progress

   c.   New device name and ✅

The ✅ mark indicates the operation has been successful and is complete. If unsuccessful, a ❌ is displayed.
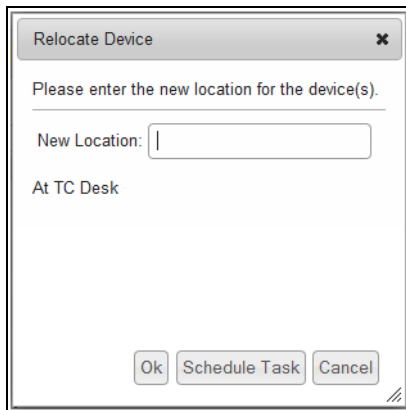
Assigning a Device Location

Assigning a representative location name to a device (and a name) helps you manage devices in the IPTV network. You can assign a location to Encoders, Transcoders, TVgateways, Chassis Monitors, AvediaServers, and Receivers.

To assign a location to devices:

1   Open the respective Device View page for the device, or devices you want to assign to a location.

2   Use the Device filter, column heading list ordering or search functions to help you find the device.

3   Select the required device(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose Set Location.

5   Click Apply to display the following window:

Figure 28 *Specifying a Device Location*

6   Click Ok to continue. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

7   Confirm the Location entry for the device steps through the following sequence:

   a.   Relocate scheduled

   b.   Relocate in progress

   c.   New device location and

The   mark indicates the operation has been successful and is complete. If unsuccessful, a   is displayed.

Manual Device Addition

In some installations network configurations can prevent keep-alive traps reaching the AvediaServer; therefore devices are not discovered automatically. However, devices can be added manually using the Add Device button available on the All Devices, New Devices, AvediaStream and Receivers pages. Once added, the AvediaServer can directly query the device(s) to obtain status information. The MAC and IP addresses are required to manually add a device.

Note: Only Exterity device types are supported.

To add a device manually:

1   Click All Devices, New Devices, AvediaStream or the Receivers tab.

2   Click Add Device:

Figure 29 *Adding a device*

3   Select the Device Type from the drop-down list.

4   Enter the device MAC address.

5   Enter the device IP address.

6   Click Ok.

Confirm the device is now listed on a Device View page.

Using the IR Assistant

The IR Assistant enables you to send IR commands from Exterity Encoders to their connected AV equipment. This can be used, for example, to pause/play a DVD player connected to an encoder.

Note: Before the IR Assistant can be used with a device such as an encoder, the device must be set up to be able to send out IR commands. Please refer to the device user documentation for further details.

To send an IR command:

1   Click the AvediaStream tab.

2   Select the encoder connected to the AV source you want to control.

3   Click the Action drop-down list and select IR Assistant.

4   Click Apply.

5   Select the remote control device file from the Remote drop-down list.

6   Select the command you want to send from the Command drop-down list.
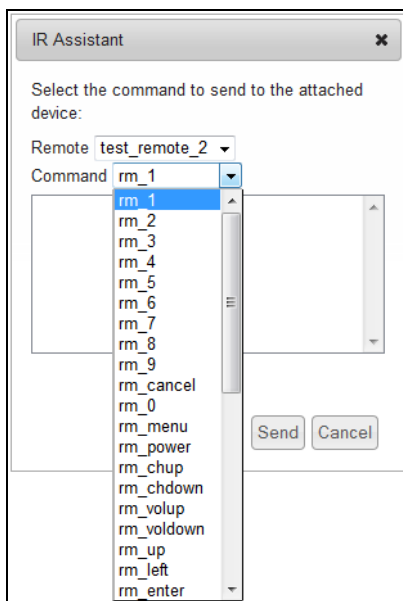
Figure 30 *Remote Assistant Function List*

7   Click Send to send the command.

8   The IR Assistant Widow confirms the command has been sent:
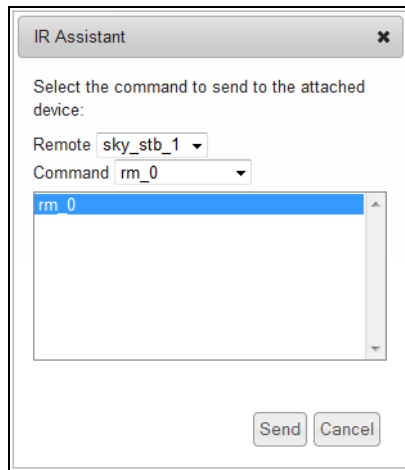
Figure 31 *Sending the Remote Command*

Receiver Operational Tasks

The following actions can only be applied to receivers.

- Set Display Mode
- Set Channel
- Set Homepage
- Set Groups
- Set Splash Screen
- Set Volume

Setting a Display Mode

You can change the display mode of Exterity receivers. Options are Off (Standby), AV, Browser, Splash, and Playlist.

To set the display mode:

1 Open the Receivers page.

2 Use the Name and Location column list ordering or search functions to help find the receiver(s).

3 Select the required receiver(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4 Click the Action drop-down list and choose Set Display Mode.

Click Apply to display the following window:
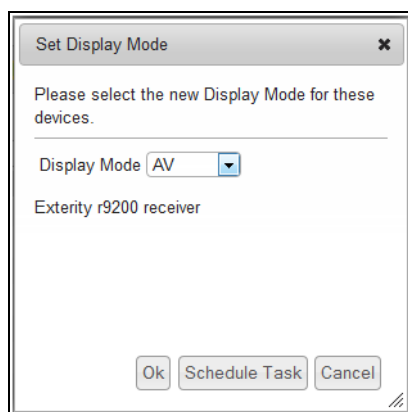
Figure 32 *Setting the receiver display mode*

5   Select the required mode from the Display Mode drop-down list and click Ok. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

6   Confirm the Name entry for the device steps through the following sequence:

   a.   Display Mode change scheduled

   b.   Display Mode change in progress

   c.   Name and ✅

The ✅ mark indicates the operation has been successful and is complete. Click Show device specific details and confirm that the Current Mode value is correct. If unsuccessful, a ❌ is displayed.
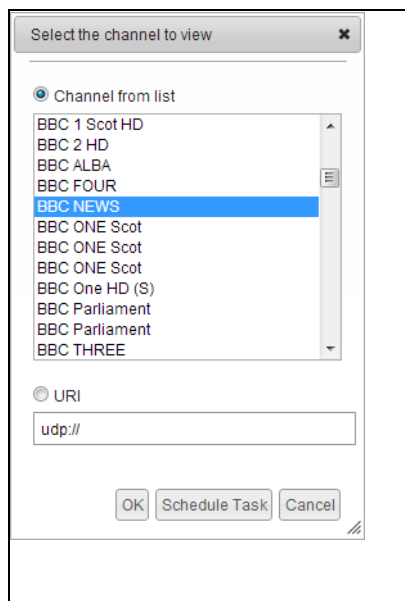
Setting a Channel

You can set the channel on Exterity receivers. The selected channel is displayed on the attached TV. You can use this feature to set multiple TVs to a specific channel simultaneously.

Note: The Channel Listener service must be enabled.

To set the channel:

1   Open the Receivers page.

2   Use the Name and Location column list ordering or search functions to help find the receiver(s).

3   Select the required receiver(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose Set Channel.

5   Click Apply to display the following window:

Figure 33 *Setting a channel*

6   Click either:

   •   The Channel from list button and select a channel from the list, or

   •   The URI button and enter the multicast address and port number of the channel stream.

   If you are specifying the URL of a channel, use the following format:

   ```
   <protocol>://<address>[:<port>][/<filename>]
   ```

Examples:

- Multicast stream (UDP or RTP): udp://239.192.0.72:5000

- VoD playback (RTSP): rtsp://10.8.64.72:8554/football.mpg

7   Click Ok to continue or refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

8   Confirm the Name entry for the device steps through the following sequence:

   a. Channel change scheduled

   b. Channel change in progress

   c. Name and ✔

The ✔ mark indicates the operation is successful and complete. Click show device specific details and confirm that the Channel is correct. If unsuccessful, a ✖ is displayed.

Note: Channels selected by the Director override receiver groups setting, allowing display of any channel on the network.

Setting the Homepage

You can set the homepage on Exterity receivers. This enables the browser on any receiver in the network to be configured with a new homepage. If you want the receiver(s) to access portal functions, enter the Portal URL in the Homepage field.

To set the homepage:

1   Open the Receivers page.

2   Use the Name and Location column list ordering or search functions to help find the receiver(s).

3   Select the required receiver(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose Set Homepage.

5   Click Apply to display the following window:
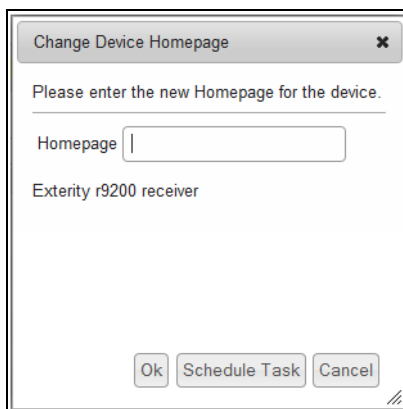
Figure 34   *Setting the homepage*

Enter the URL of the required homepage and click Ok. Refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option. Enter the URI as follows:

- AvediaServer Portal - <server ip address>/portal, for example: 10.8.100.168/portal

- Web page - http://www.xyz.com, for example: http://www.exterity.com

6   Confirm the Name entry for the device steps through the following sequence:

   a. Homepage change scheduled
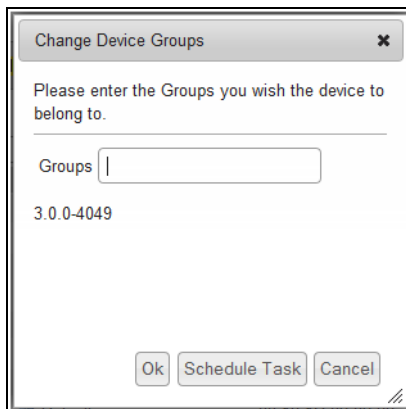
   b. Homepage change in progress

c. Name and ✅

The ✅ mark indicates the operation has been successful and is complete. Click show device specific details and confirm that the Channel is correct. If unsuccessful, a ✖ is displayed.

Setting Groups

You can change the group membership setting on Exterity receivers.

To set the group membership:

1 Open the Receivers page.

2 Use the Name and Location column list ordering or search functions to help find the receiver(s).

3 Select the required receiver(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4 Click the Action drop-down list and choose Set Groups.

5 Click Apply to display the following window:

Figure 35 *Setting Groups*

6 Enter a comma-separated list for the group membership. Enter all, or leave blank if you want to set membership to all groups. Ensure there are no spaces in the comma separated list.

7 Click Ok to continue or refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

8 Confirm the Name entry for the device steps through the following sequence:

a. Groups change scheduled

b. Groups change in progress

c. Name and ✅

The ✅ mark indicates the operation has been successful and is complete. Click show device specific details and confirm that the Groups value is correct. If unsuccessful, a ✖ is displayed.

Changing the Splash Screen

The splash screen can be configured to be displayed on the connected TV when the receiver is turned on. This process uploads the splash screen image file to the receiver using the AvediaServer TFTP server. You can specify the image to be displayed and the image file you want to use must be saved on the TFTP server.

Note: Ensure that the TFTP Server address is configured correctly and that the TFTP server is running. Refer to "Setting a Device TFTP Server Address" on page 29 for more information.

To set the splash screen:

1   Open the Receivers page.

2   Use the Name and Location column list ordering or search functions to help find the receiver(s).

3   Select the receiver(s) by clicking the Select check box. If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose Set Splash Screen.

Click Apply and the following window is displayed:
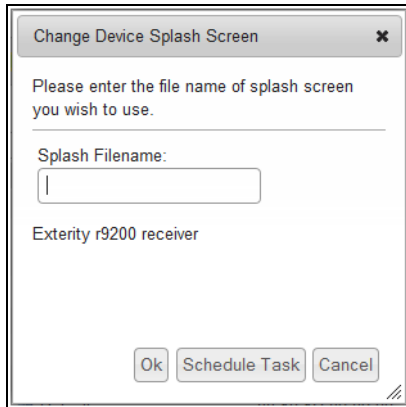
Figure 36   *Setting the splash screen*

5   Enter the filename for the splash screen you want to use.

6   Click Ok to continue or refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

7   Confirm the Name entry for the device steps through the following sequence:

a. Splash screen change scheduled

b. Splash screen change in progress

c. Name and ✅

The ✅ mark indicates the operation is successful and complete. If unsuccessful, a ✖ is displayed.

Setting the Volume

You can set the audio output level from Exterity receivers. You can specify a value between 0 (min volume) and 40 (max volume) or mute the output.

To set the volume:

1   Open the Receivers page.

2   Use the Name and Location column list ordering or search functions to help find the receiver(s).

3   Select the receiver(s) by clicking the Select check box. If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose Set Volume.

5   Click Apply to display the following window:
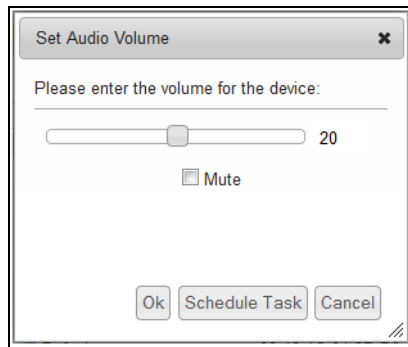
Figure 37   *Setting the Volume*

6   Click and drag the slider it to the value you want to use. To mute the output, click the Mute checkbox.

7   Click Ok to continue or refer to "Scheduling Tasks" on page 42 for more information about the Schedule Task option.

8   Confirm the Name entry for the device steps through the following sequence:

   a.   Volume change scheduled

   b.   Volume change in progress

   c.   Name and ✅

The ✅ mark indicates the operation has been successful and is complete. If unsuccessful, a ✖ is displayed.

Scheduling Tasks

This section shows you how to create and manage scheduled or immediate tasks. Tasks are created using the Actions drop-down list on any of the four device view pages: All Devices, New Devices, AvediaStream, and Receivers.

The process of scheduling a task for a later time is an extension of the process for immediate execution, and is the same for all actions except IR Assistant. Scheduling tasks can help you manage the processes of maintaining the IPTV network and take advantage of capabilities such as setting all receivers in a defined location to display a particular channel at a specified time.

Note: All actions except IR Assistant can be configured as a scheduled event.

Once created, the Scheduled Tasks page allows you to confirm the tasks are scheduled as required and lists completed, immediately executed, and scheduled tasks.

The section is divided as follows:

•   Creating Scheduled Tasks

•   Managing Scheduled Tasks

Creating Scheduled Tasks

This section shows how to create a scheduled task. Any task can be scheduled as a once only event, or repetitively at daily, weekly, or monthly intervals.

This section describes the following procedures:

•   Creating and Executing a Task

•   Schedule a Daily Recurring Task

•   Schedule a Weekly Recurring Task

•   Schedule a Monthly Recurring Task

Creating and Executing a Single Task

Scheduling a single event enables you to implement a non-recurring process such as for example, upgrading device firmware at a time which minimizes service disruption. The procedure requires that you select the device(s), select the action, and either execute it immediately, or define a time and date. Adding event names and descriptions help you manage multiple events.

To schedule a single task:

1   Open a device view page – for example, the Receivers page.

2   Use the Name and Location column list ordering or search functions to help find the device(s).

3   Select the required device(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4   Click the Action drop-down list and choose, for example, Set Channel.

5   Click Apply.

Figure 38 *Setting the channel*

6   Select the channel as described in "Setting a Channel" on page 38.

7   Click Schedule Task to display the Schedule Dialog window. The default schedule is Once.
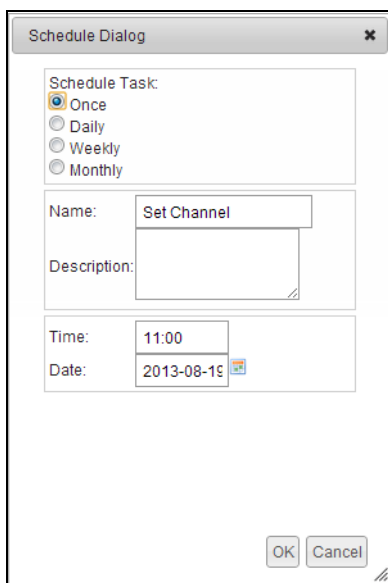
Figure 39 *Scheduled Task Dialog*

8 You can enter a Name and Description to help identify the task when it is listed on the Scheduled Tasks page. To do so:

   a. Click the Name checkbox and enter a name.

   b. Click the Description checkbox and enter a description.

9 Enter the required time for the task to be executed. You can specify the time in 24 hour clock format.

10 Click the calendar icon beside the Date field and select the required date.
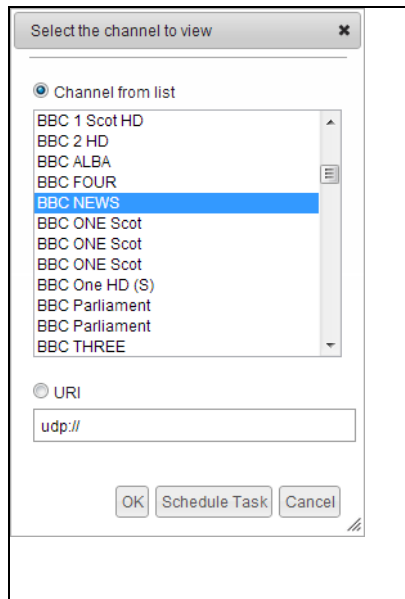
Figure 40 *Selecting the Date and Time*

11 Click OK to complete the entry.

12 Confirm the Name entry for the device displays Channel change scheduled.

13 Click Scheduled Tasks and confirm the entry is now listed in the table.

Scheduling a Daily Recurring Task

You can Schedule a daily recurring event to establish a regular task, such as setting all receivers to a regular broadcast on a daily, or every 2nd, 3rd day and so on, or as required. The procedure requires that you select the device(s), select the Action, and define a start date, end date, and the daily recurrence. Adding Event Names and Descriptions help you manage multiple events.

To schedule a daily recurring task:

1 Open a device view page – for example, the Receivers page.

2 Use the Name and Location column list ordering or search functions to help find the device(s).

3 Select the required device(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4 Click the Action drop-down list and choose Set Channel.

5 Click Apply to display the following window:

Figure 41 *Selecting the channel*

6   Select the channel as described in "Setting a Channel" on page 38.

7   Click Schedule Task. The Schedule Dialog window is displayed:
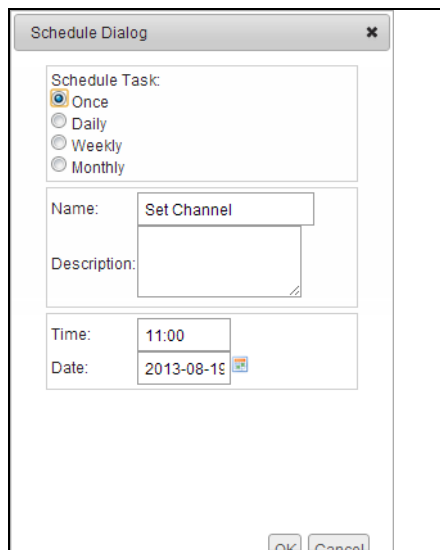
Figure 42 *Setting the schedule*

8   Click Daily and the Time, Start Date, End Date and Every fields are added to the Schedule Dialog window.

9   You can enter a Name and Description to help identify the task when it is listed on the Scheduled Tasks page. To do so:

     a.   Click the Name checkbox and enter a name.

     b.   Click the Description checkbox and enter a description.

10   Enter the required time for the task to be executed. You can specify the time in hours, minutes and seconds.

11   Click the Start Date calendar icon and select the required start date.

12   Click the End Date calendar icon and select the required finish date. Do not check the end date checkbox if you want to ensure the task repeats as scheduled until reconfigured.

Figure 43 *Setting a daily schedule*

13 Enter the required value in the Every field – for example enter '1' for daily repeat, '2' for every 2nd day, and so on.

14 Click Ok to complete the entry.

15 Confirm the Name entry for the device displays Channel change scheduled.

16 Click Scheduled Tasks and confirm the entry is now listed in the table.

Scheduling a Weekly Recurring Task

Scheduling a weekly recurring event enables you to establish a regular task such as setting all receivers to a regular broadcast on any day of the week. The procedure requires that you select the devices, select the action, and define a start date, end date, and the required day(s). Adding Event Names and Descriptions help you manage multiple events.

To schedule a weekly recurring event:

1 Open a device view page – for example, the Receivers page.

2 Use the Name and Location column list ordering or search functions to help find the device(s).

3 Select the required device(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4 Click the Action drop-down list and choose Set Channel.

5 Click Apply to display the following window:
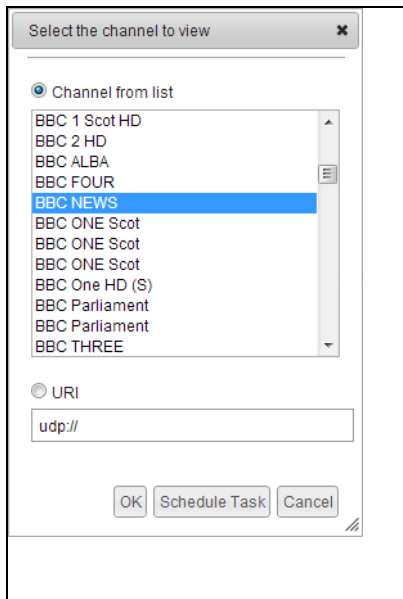
Figure 44 *Selecting the channel*

6   Select the channel as described in "Setting a Channel" on page 38.

7   Click Schedule Task. The Schedule Dialog window is displayed:
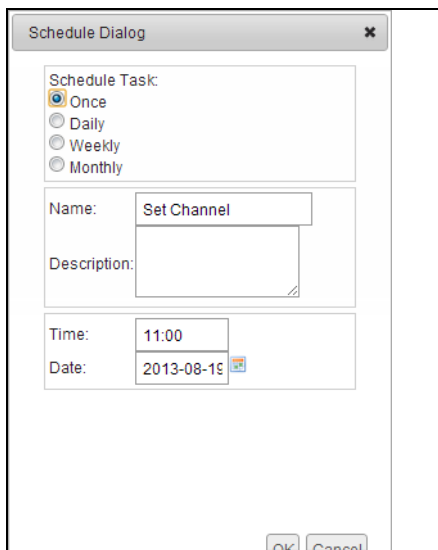
Figure 45 *Setting the schedule*

8   Click Weekly and the Time, Start Date, End Date fields and Day checkboxes are added to the Schedule Dialog window.

9   You can enter a name and description to help identify the task when it is listed on the Scheduled Tasks page. To do so:

a.   Click the Name checkbox and enter a name.

b.   Click the Description checkbox and enter a description.

10   Enter the required time for the task to be executed. You can specify the time in hours, minutes and seconds.

11   Click the Start Date calendar icon and select the required start date.

12   Click the End Date calendar icon and select the required finish date. Do not check the end date checkbox if you want to ensure the task repeats as scheduled until reconfigured.

Figure 46 *Setting a weekly schedule*

13 Select the day, or days, required.

14 Click Ok to complete the entry.

15 Confirm the Name entry for the device displays *Channel change scheduled*.

16 Click Scheduled Tasks and confirm the entry is now listed in the table.

Scheduling a Monthly Recurring Task

Scheduling a monthly recurring event enables you to establish a regular task such as setting all receivers to a regular broadcast on a specified date of every month. The procedure requires that you select the devices, select the action, and define a start date, end date, and the required date. Adding event names and descriptions help you manage multiple events.

To schedule a monthly recurring event:

1 Open a device view page – for example, the Receivers page.

2 Use the Name and Location column list ordering or search functions to help find the device(s).

3 Select the required device(s). If, after filtering, the list contains only the required devices, select All from the Select drop-down list.

4 Click the Action drop-down list and choose Set Channel.

5 Click Apply.

Figure 47 *Setting the channel*

6   Select the channel as described in "Setting a Channel" on page 38.

7   Click Schedule Task:

Figure 48 *Setting the schedule*

8   Click Monthly and the Time, Start Date, End Date and the On the – of the month fields are added to the Schedule Dialog window.

9   You can enter a name and description to help identify the task when it is listed on the Scheduled Tasks page. To do so:

 a. Click the Name checkbox and enter a name.

 b. Click the Description checkbox and enter a description.

10 Enter the required time for the task to be executed. You can specify the time in hours, minutes and seconds.

11 Click the Start Date calendar icon and select the required start date.

12 Click the End Date calendar icon and select the required finish date. Do not click the end date checkbox if you want to ensure the task repeats as scheduled until reconfigured.
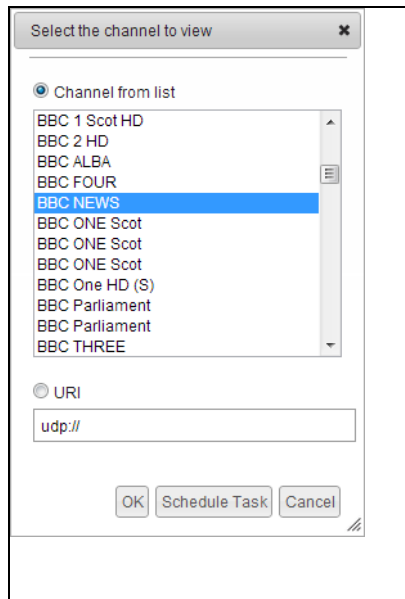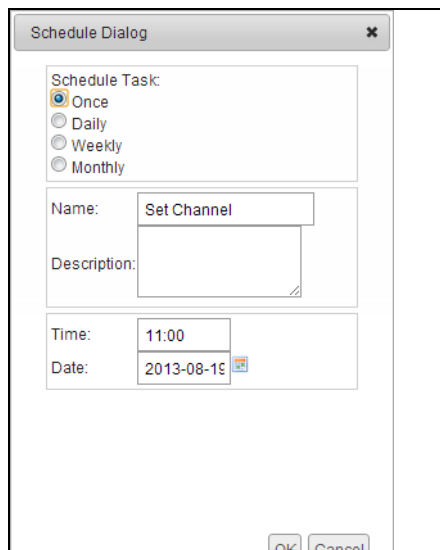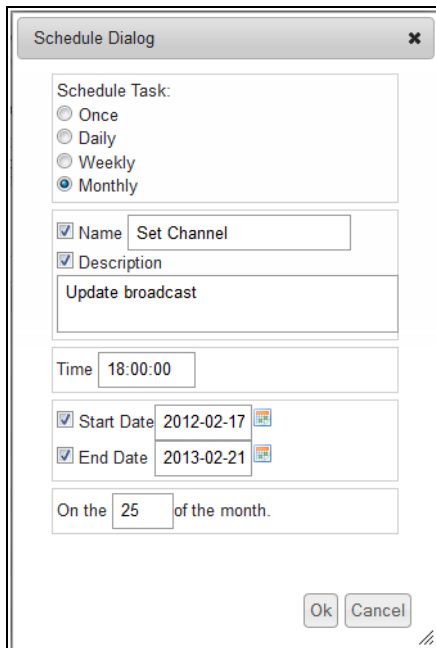
Figure 49 *Setting a monthly schedule*

13 Enter the required date in the month.

14 Click Ok to complete the entry.

15 Confirm the Name entry for the device displays *Channel change scheduled*.

16 Click Scheduled Tasks and confirm the entry is now listed in the table.

Managing Scheduled Tasks

This section shows you how to manage scheduled tasks. Any tasks created as scheduled tasks from the Actions list on the device view pages, All Devices, AvediaStream and Receivers are listed in the table on the Scheduled Tasks page. The table lists all tasks, both pending and completed.

Figure 50 *Scheduled Tasks Page*

Scheduled Tasks Page Layout and Functions

This section describes the highlighted areas of the Scheduled Tasks Page shown in Figure 4.

Action

The Action panel allows you to delete or cancel tasks in the table. You can apply the functions to one or more selected tasks.

Action	Cancel Task(s) ▼	Apply	Delete All

- Action drop-down list and Apply button – Allows you to perform the cancel and delete functions.

- Delete Task(s) removes the selected task(s) from the table. It can be applied to completed, scheduled, and canceled tasks.

- Cancel Task(s) cancels the selected scheduled task(s) but does not remove it/them from the table.

- Delete All button - Allows you to clear the Scheduled Tasks, deleting all current entries in the list.

Select and Column Functions

Select and Column Functions allow you to globally select or deselect tasks, order the list by the heading title and to search for a specific value in a table column. For example, to order the list by name, click Task Name. To invert the order press Task Name again. The default list order is Execution Time.

Job ID	Status	Execution Time	Task Name	Description	Device Name	Location	Address	Target MAC
\<search\>	\<search\>	\<search\>	\<search\>	\<search\>	\<search\>	All ▼	\<search\>	\<search\>
6	Complete	2012-04-20 17:29:58	Set Channel		Support-02-syncleft	Support	10.8.100.210	00:18:1C:01:3D:53

Figure 51 *Task List column headings*

- **Job ID** – Displays the task as a Job ID. A unique Job ID is assigned to each task when it is created. Click Job ID to order the list by ID. To find tasks by Job ID, enter the ID in the column \<search\> field and click anywhere on the page to initiate the search. A Job ID may be listed more than once in the table:

  - For more than one device – Indicates that a specific task is to be/has been applied to more than one device.

  - For only one device – Indicates that a task is recurring with both completed and scheduled dates and times listed. (Complete and New)

- **Execution Time** – Displays the time set for the task. The time was configured by the task creator. Refer to "Scheduling Tasks" on page 42 for more information. Click Execution Time to order the list by time. To find tasks by time, enter the date and time in the form year-month-date hh:mm:ss in the column \<search\> field and press the Return/Enter key to initiate the search.

- **Task Name** – Displays the task name specified by the task creator. Refer to "Scheduling Tasks" on page 42 for more information. Click Task Name to order the list by task. To find a task by name, enter all or part of the task name in the column \<search\> field and click anywhere on the page to initiate the search.

- **Description** – Displays the task description specified by the task creator. Refer to "Scheduling Tasks" on page 42 for more information. Click Description to order the list by description. To find tasks by description, enter all or part of the task description in the column \<search\> field and click anywhere on the page to initiate the search.

- **Device Name** – Displays the name of the listed device. The device was selected by the task creator. Refer to "Scheduling Tasks" on page 42 for more information. Click Device Name to order the list by name. To find tasks by device name, enter all or part of the device name in the column \<search\> field and click anywhere on the page to initiate the search.

- **Location** – Allows you to filter the events based on the location of the listed devices. Click Location and choose from the drop-down list.

- **Address** – Displays the IP address of the listed device. Click Address to order the list. To find tasks by IP address, enter the IP address in the column <search> field and click anywhere on the page to initiate the search.

- **Target MAC** – Displays the MAC address of the listed device. Click Target MAC to order the list. To find tasks by MAC address, enter the MAC address in the column <search> field and click anywhere on the page to initiate the search.

- **Status** – Displays the execution status of the task:

  - New: Indicates that the task is still pending. A new task is also listed automatically each time a recurring task is completed.

  - Complete: The task has been executed.

  - Canceled: The task has been canceled using the Cancel Task(s) Action on the Scheduled Tasks page.

 - Failed: Indicates that the task was not successfully completed.

Task List

The Task List area displays all pending or completed tasks and associated devices. All items remain in the list until you delete them.

	Job ID	Status	Execution Time	Task Name	Description	Device Name	Location	Address	Target MAC
Select: ▼	<search>	<search>	<search>	<search>	<search>	<search>	All ▼	<search>	<search>
☐	6	New	2012-02-17 18:00:00	Set Channel	Go to News	Exterity r9200 receiver	At TC Desk	10.8.100.147	00:18:1C:01:36:8F
☐	5	Complete	2012-02-17 11:09:52	Factory Reset		Exterity r9200 receiver	At TC Desk	10.8.100.147	00:18:1C:01:36:8F

Figure 52 *Scheduled Task list*

Page Control

The paging step buttons allow you to page through longer lists of tasks. You can also choose to display a greater or lesser number of tasks on a single page by selecting a value from the drop-down list. The default number of devices per page is 10.

|◄ ◄ Page 1 of 1 (1-8 of 8 Scheduled Task(s)) ▼ ► ►|
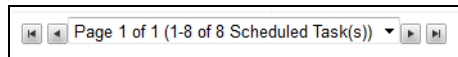
Navigate through the pages by clicking the step forward/back single arrows, or the jump to end/beginning double-arrows.

6 Using the Channel Monitor Application

The Channel Monitor application allows prompt and accurate monitoring of channel status. The list of network channels is built up by listening for SAP announcements from head-end equipment. Additionally, by connecting to the multicast stream of each selected channel in turn, both the presence and integrity of the transport stream encapsulation is determined. Both Multicast RTP and UDP channels are detected.

If a valid stream is not detected on a monitored channel within the specified channel ageing period, the channel is highlighted red in the Channel Monitor application. Channels are highlighted yellow when they have stopped streaming but have not yet reached the full ageing time limit. You can change the channel ageing values on the Director application Configuration page. (Time before marking channel as off-air:)

Channel, stream and source device information is displayed in an orderable and searchable table. The table is split into the Listener (on the left) and the Monitor (on the right):

Figure 53 *Channel Monitor application*

Note: For channels to be added and updated automatically, both the SAP (Session Announcement Protocol) must be enabled by the streaming devices (head-end), and the Channel Listener service must be enabled and running in the AvediaServer System application Services page.

The Channel Monitor function, also located on the System application Services page, must be enabled and running to enable use of the Monitor section of the channel table.

Channel Monitor Page Layout and Functions

This section describes the highlighted areas of the Channel Monitor Page.

Channels and Search

The channels table and search functions allow you to remove channels from the list, turn monitoring on and off, and search within the table contents.

Figure 54 *Channels listing*

- **Search**: Entry field – orders the table by best match to text and numbers within any entry listed in the table. The list is interactively updated as you enter data into the search field.

- **Headings**: You can order the table by clicking on the name of any column heading. Click a column heading again to reverse the order. The order is indicated by the up/down arrows.

- **Channel Name, URI** and **Source Hyperlinks**: You can quickly check the channel content by clicking the Name or URI hyperlinks. Click the Source Name hyperlink to log in to the Web Interface of the channel source device.

Column Headings

The column headings can be used to order the entries in the table by the column heading. For example, to order the table by channel name click Name. To invert the order click Name again. The checkbox allows you to select/deselect all channels in the table.

Listener Headings

- **#** – Displays the channel number assigned at the stream source. The channel number is configured using the AvediaStream Encoder, TVgateway, or Transcoder Web Interfaces which are accessed using the channel Source hyperlink.

- **Name** – Displays the name of the channel.

- **URI** – Displays the channel multicast address and port number.

- **Source Name** – Displays the assigned name of the head-end device which is transmitting this channel.

- **Source Type** – Displays the type of the head-end device which is transmitting this channel, for example, Gateway.

- **Groups** – Displays the channel Group membership.

- **Video PID** – Displays the video packet ID within the channel stream, or audio only if there is no video.

- **Audio PID** – Displays the primary audio packet ID (PID). Only one Audio PID is listed for a channel.

- **Stream ID** – Displays the stream ID of the channel, containing information about its origin and content. It is in the form, originator network id:transport stream id:service id, and is applied to the stream by the originating broadcaster.

- **Last SAP** – Displays the time elapsed since receipt of a channel Session Announcement Protocol (SAP) message.

Monitor Headings

All Monitor parameters display n/a when the channel is not being monitored

- **Scrambling** – Indicates if a channel is scrambled.
- **Bitrate (Mbps)** – The measured bitrate for the channel.
- **Uptime** – The length of time the channel has been streaming. The counter starts from when monitoring starts or when the channel started streaming, whichever is later. Displays n/a when the channel is not monitored or not streaming.
- **Cont Err** – The number of detected continuity errors.
- **TEI Err** – The number of transport errors. A Transport Error Indicator is raised by the demodulation section of a device, such as a TVgateway, to indicate that it was unable to correct an error in the stream.
- **Sync Err** – The number of Sync errors detected.

Channel Details

Each row lists the channel details in accordance with the column headings.

Figure 55 *Channel details*

- **Colour coding** – The channel listing is colour coded according to the channel activity. The Channel Listener must be enabled on the System application Services page. Yellow highlighting is applied when no SAP announcements are received for over 1 minute. Red highlighting is applied after 10 minutes and indicates an inactive channel.
- **Monitoring** – The green timer icon is displayed in the channel row when it has been selected and monitoring enabled.

Page Control

The paging step buttons allow you to page through longer lists of channels. You can also choose how many channels to display on a single page by selecting a value from the Show drop-down list. The default number of channels per page is 10.
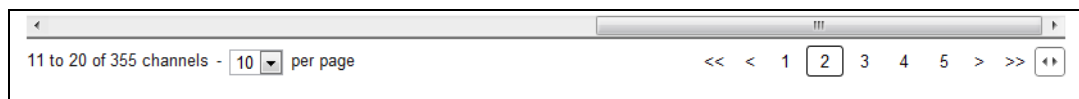
Figure 56 *Page control*

Navigate through the pages by clicking the step forward/back single arrows.

The lower line displays the range of channels from the total currently displayed. If you have filtered the results by entering text in the search field, the lower line displays the range of results from the total number of channels.
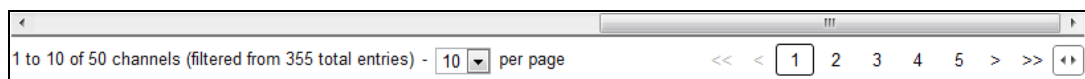
Figure 57 *Page control filtered*

Configuring Channel Monitor Settings

If a valid stream is not detected on a monitored channel within the specified channel ageing period, the channel is highlighted red in the Channel Monitor application. Channels which are no longer streaming, but have not yet reached the configured offline threshold are highlighted yellow. You can change the channel ageing values on the Director application Configuration page. (Time before marking channel as off-air:)

Note: Monitoring of specific channels in the Channel Monitor application is disabled by default.

To configure the Channel Monitoring settings:

1 Start the Director application.

2 Click the Configuration tab.

Figure 58 *Director application - Channel Monitor configuration*

3 Enter a value for Time before marking Channel as off-air. This specifies the time to wait for data before declaring that a channel is not streaming. The default is 2 seconds and the range 1 to 10.

4 Enter a value for the Maximum simultaneous channels the Channel Monitor application can open. The default is 10 and the range is 1 to 150.

5 Enter a value for the Time between channel starts. Channel monitoring is performed in a sequential manner. This specifies the delay between closing one channel and opening the next. The default is 3 seconds and the range 1 to 10.

6 Enter a value for the Bit rate sampling time. This specifies the time used to determine the streaming rate of a channel. The default is 2 seconds and the range 1 to 10.

7 Click Apply.

Managing Channels

The Channel Listener function uses SAP (Session Announcement Protocol) messages to add the announced channel to the list. Channels added using the Channel Announcer application are also listed. The channel details are listed in the individual line items. Using the hyperlinks in the table you can view the channel in your browser (AvediaPlayer desktop) or open the web interface for the channel streaming device to make configuration changes if required.

Channels remain in the list, even when streaming has stopped and SAP messages are not broadcast. Yellow highlighting is applied when the channel activity cannot be determined for over 1 minute. Red highlighting is applied after 10 minutes.

The channel ageing function allows you to quickly identify non-streaming channels by highlighting them in red.

Additional channel details are provided by the Monitor function which can be enabled as required.

This section shows you how to:

- Identify and delete non-streaming channels

- Enable channel monitoring

- Change channel parameters

Identifying and Deleting Non-Streaming Channels

Identifying non-streaming channels allows you to see at a glance if any channels have unexpectedly stopped sending SAP announcements. Channels which are no longer being announced are highlighted red. A channel may have stopped streaming for several reasons, for example:

- It has been deliberately stopped at the head-end.

- It is no longer being broadcast.

To identify and delete non-streaming channels:

1 Start the Channel Monitor application to display all channels.

2 Click Last SAP twice to list the channels by oldest SAP announcement.

3 If required, you can perform additional checks:

- Click the channel Name or URL and confirm the channel is inactive.

- Click the Source hyperlink to launch the device web management interface, log in and confirm that the device is functioning normally.

4 Click the channel to select it and click Delete to remove it from the list.

Enabling/Disabling Channel Monitoring

Channel monitoring provides additional information about a selected channel. It does not use the Channel Monitor Service, but instead opens the channel directly for examination. This can be useful in identifying for example, scrambled channels, channels with the highest bandwidth requirements and those with errors.

To enable/disable channel monitoring:

1 Start the Channel Monitor application.

2 Locate the channel you want to monitor and select it by clicking at the left end of its row in the table.

Figure 59 *Starting the Monitor*

3   Click Start Monitoring.

4   Confirm the 🔄 icon is displayed on the selected channel listing:

Changing Channel Parameters

Parameters such as channel name, group membership, and streaming bitrate are configured by the streaming device. However, the source device is listed for each channel and you can use this to access the device web management interface and make configuration changes if required.

To change channel parameters:

1   Locate the channel of interest in the table.

2   Click the device hyperlink in the Source column. (The type of device is displayed in the Source Type column.)

3   Enter the administrator login and password to access the device's Web Interface

4   Refer to the Exterity AvediaStream Encoder, Transcoder, TVgateway or AvediaServer Administrator Guides to make channel configuration changes as required.

7 Using the Logger Application

AvediaServer is a Linux standard Syslog Server used to log information about the system. Logging information can be used by authorised Exterity service personnel to analyse any installation or performance problems experienced on an AvediaServer.

Other devices such as receivers and encoders can send their own log information to this server. Likewise this server can log information to another syslog server if you have a central log server.

Logs are retained for 7 days and replaced at 24 hour (daily) intervals.

Note: You can configure the syslog server address for all Exterity IPTV devices using the Director application.

This chapter contains the following sections:

- Viewing Logging Information
- Downloading the Log File
- Logging Information to an External Syslog Server
- Using the AvediaServer as a Syslog Server

Viewing Logging Information

To view logging information:

1 Start the Logger application to display the AvediaServer's own log:

Figure 60 *Logger – Local Page*

2 Click Show All.

The following window is displayed with all available log information:

Feb 5 15:36:15 avediaserver-23A4 iSocketListener[22388]: *****removing a086421,720e,ARM_1,udp://239.192.1.33:5000?format=33

Feb 5 15:36:15 avediaserver-23A4 iSocketListener[22388]: *****removing a086421,dca3,BBC World News,udp://239.192.2.33:5000?format=33

Feb 5 15:36:15 avediaserver-23A4 iSocketListener[22388]: *****removing a086421,1039,Euronews,udp://239.192.5.33:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,726e,BBC R Scotland,udp://239.192.8.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,5dcb,BBC Radio 1,udp://239.192.13.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,d137,BBC Radio 2,udp://239.192.14.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,9c59,BBC Radio 4 Ex,udp://239.192.16.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,7f47,BBC ALBA,udp://239.192.2.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,6082,BBC Asian Net.,udp://239.192.3.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,1af2,BBC R n Gaidheal,udp://239.192.9.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,8951,BBC R5SX,udp://239.192.12.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,b60d,BBC Radio 3,udp://239.192.15.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,dd6c,BBC Radio 4,udp://239.192.17.32:5000?format=33

Feb 5 16:02:53 avediaserver-23A4 iSocketListener[22388]: *****removing a086420,fe17,BBC World Sv.,udp://239.192.21.32:5000?format=33

Feb 5 16:11:33 avediaserver-23A4 avedia-EPGd: Bad crc

Feb 5 18:02:19 avediaserver-23A4 iSocketListener[22388]: *****removing a086424,43b0,CITV,udp://239.192.8.36:5000?format=33

Feb 5 18:02:54 avediaserver-23A4 iSocketListener[22388]: *****removing a086424,3b7f,Al Jazeera Eng,udp://239.192.133.36:5000?format=33

Feb 5 18:02:59 avediaserver-23A4 iSocketListener[22388]: *****removing a086422,e761,Food Network,udp://239.192.140.34:5000?format=33

Feb 5 18:02:59 avediaserver-23A4 iSocketListener[22388]: *****removing

Figure 61 *Logger – all log information*

Downloading the Log File

The downloaded log file also contains additional information such as the AvediaServer database in SQL format.

To download the log file:

1 Start the Logger application.

2 Click Local to display the local log and click Download.

(Depending on your browser and its configuration, a pop-up window is presented or the file is downloaded directly to your configured downloads folder.)
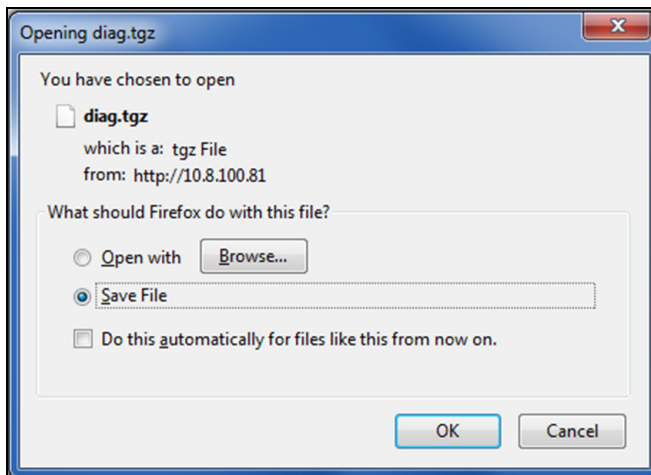
Figure 62 *Logger – Save Log File*

3 Click OK to save the log file to the required destination.

> **Note:** You can also open the log file if you wish to view it immediately. Click Browse to select your .tgz extraction application.

Logging Information to an External Syslog Server

The AvediaServer is configured by default for all logging messages to be saved locally. The default logging is set to Level 7, Debug. However, you can configure different logging levels and save the messages to an external Syslog server.

Note: A Syslog server must already be available for use.

To log information to an external Syslog server:

1 Start the Logger application and click Local.

2 Click the Log remotely checkbox.

3 Enter the IP address of the Syslog Server in the Syslog Server field.

4 Select the logging level from the Level drop-down list. 0-Emergency logs the least amount of data to the Syslog server, 7-Debug the most.
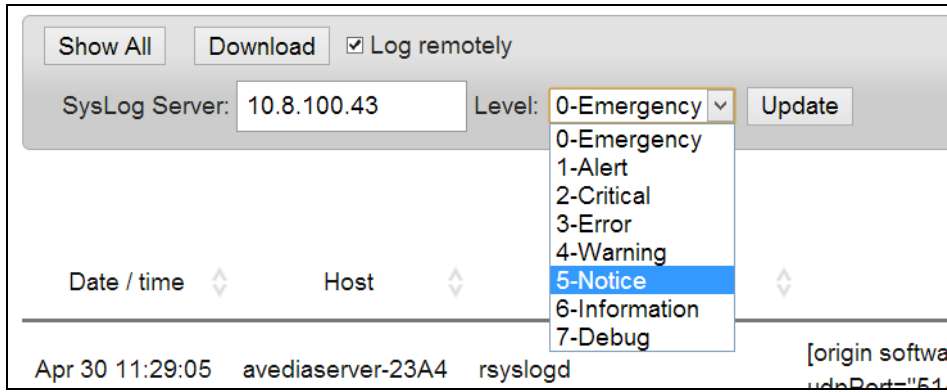
Figure 63 *Logger – Remote Logging*

5 Click Update.

Using the AvediaServer as a Syslog Server

Exterity devices can be configured to use a Syslog Server for storing system log files. You can use the AvediaServer as the Syslog Server: the available Syslog files are then listed on the Logger application Remote page. The filenames are listed for each device using the Syslog server capability of the AvediaServer and you can use the columns and search fields to order the list by Device type, Device Name, IP Address, and to update date and time.

To view a syslog file on the local AvediaServer:

1 Start the Logger application and click Remote.
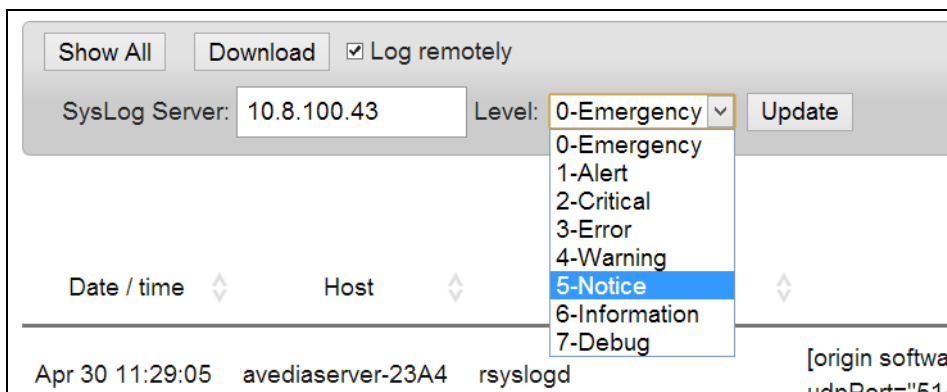
Figure 64 *Logger – Remote Logging*

2 Use the Device filter, column headings or search functions to help you find the required device.

3 Click the device checkbox, select View Syslog from the Action drop-down list and click Apply to view a specific device log:

```
May 9 10:36:47 10.8.100.174 iSocketListener[1116] Deleting AvediaStream e3535
May 9 10:36:57 10.8.100.174 zapper[1233] Zapper string ZAPPER:UPDATE_CHANNELS:
May 9 10:36:57 10.8.100.174 galio Creating channel collection
May 9 10:36:57 10.8.100.174 galio Creating object (0x298AA06C 0x8C 0x298B0A0C 0x7B80066C)
May 9 10:36:57 10.8.100.174 snmpd[8138] Received TERM or STOP signal... shutting down...
May 9 10:36:57 10.8.100.174 admind admin: /etc/init.d/snmpd-utils start
May 9 10:36:57 10.8.100.174 admind snmptrap -c public -v2c 239.255.255.255 " ecConfigChange ecSerialNumber x '00 18 1c 00 00 6e 00 00'
ecConfigChangeText s "updateChannelsList:yes" ecConfigVersion i 63
May 9 10:36:57 10.8.100.174 snmpd[8355] Initialised the table data set!!!!!!!!
May 9 10:36:58 10.8.100.174 snmpd[8355] NET-SNMP version 5.0.8
May 9 10:36:58 10.8.100.174 zapper[1233] parse line error #9 (line 163)
May 9 10:36:58 10.8.100.174 zapper[1233] parse line error #9 (line 163)
May 9 10:42:29 10.8.100.174 iSocketListener[1116] adding a08644b,d813,10.8.100.75,AvediaStream e3535
,02255F,udp://239.192.100.75:5000?format=33,y,n,0,-1,0,1,all
May 9 10:42:57 10.8.100.174 zapper[1233] Zapper string ZAPPER:UPDATE_CHANNELS:
May 9 10:42:57 10.8.100.174 snmpd[8355] Received TERM or STOP signal... shutting down...
May 9 10:42:57 10.8.100.174 admind admin: /etc/init.d/snmpd-utils start
May 9 10:42:57 10.8.100.174 galio Creating channel collection
May 9 10:42:57 10.8.100.174 admind snmptrap -c public -v2c 239.255.255.255 " ecConfigChange ecSerialNumber x '00 18 1c 00 00 6e 00 00'
ecConfigChangeText s "updateChannelsList:yes" ecConfigVersion i 64
May 9 10:42:57 10.8.100.174 galio Creating object (0x298AA06C 0x8C 0x298AFB30 0x7B80066C)
May 9 10:42:57 10.8.100.174 snmpd[8410] Initialised the table data set!!!!!!!!
May 9 10:42:58 10.8.100.174 snmpd[8410] NET-SNMP version 5.0.8
```

Figure 65 *Logger – remote logging*

4   If required, you can save the displayed file for additional analysis using the browser File > Save as... function.

To delete a syslog file on the local AvediaServer:

1   Start the Logger application and click Remote.

2   Use the Device filter, column headings or search functions to help you find the required device(s).

3   Click the checkbox to select the device log file(s) to be deleted.

Figure 66 *Deleting a local log*

4   Select Delete Syslog from the Action drop-down list and click Apply.

8   Using the System Application

This chapter contains the following information:

- Naming the AvediaServer
- Configuring the SNMP Community Strings
- Configuring Network Settings
- Configuring NTP Server and Local Time
- Configuring the AvediaServer Timezone
- Specifying a Fully Qualified Domain Name
- Configuring AvediaServer Services
- Managing AvediaServer and AvediaPlayer Desktop Licences
- Status Monitoring
- Monitoring Content Bandwidth
- Maintaining the AvediaServer

It shows how to use the System application to configure basic settings such as the IP address and time server/time zone of the AvediaServer. AvediaServer Services, used by other AvediaServer applications, are configured in the System application.

The System application also provides maintenance functions for the AvediaServer such as reboot, upgrade, and AvediaServer and AvediaPlayer Desktop licence management. (The Director application is required to carry out maintenance functions on other IPTV devices.) You can also monitor disk space usage and bandwidth consumption of VoD assets and Play/Record channels and carry out maintenance such as upgrades and configuration import/export.
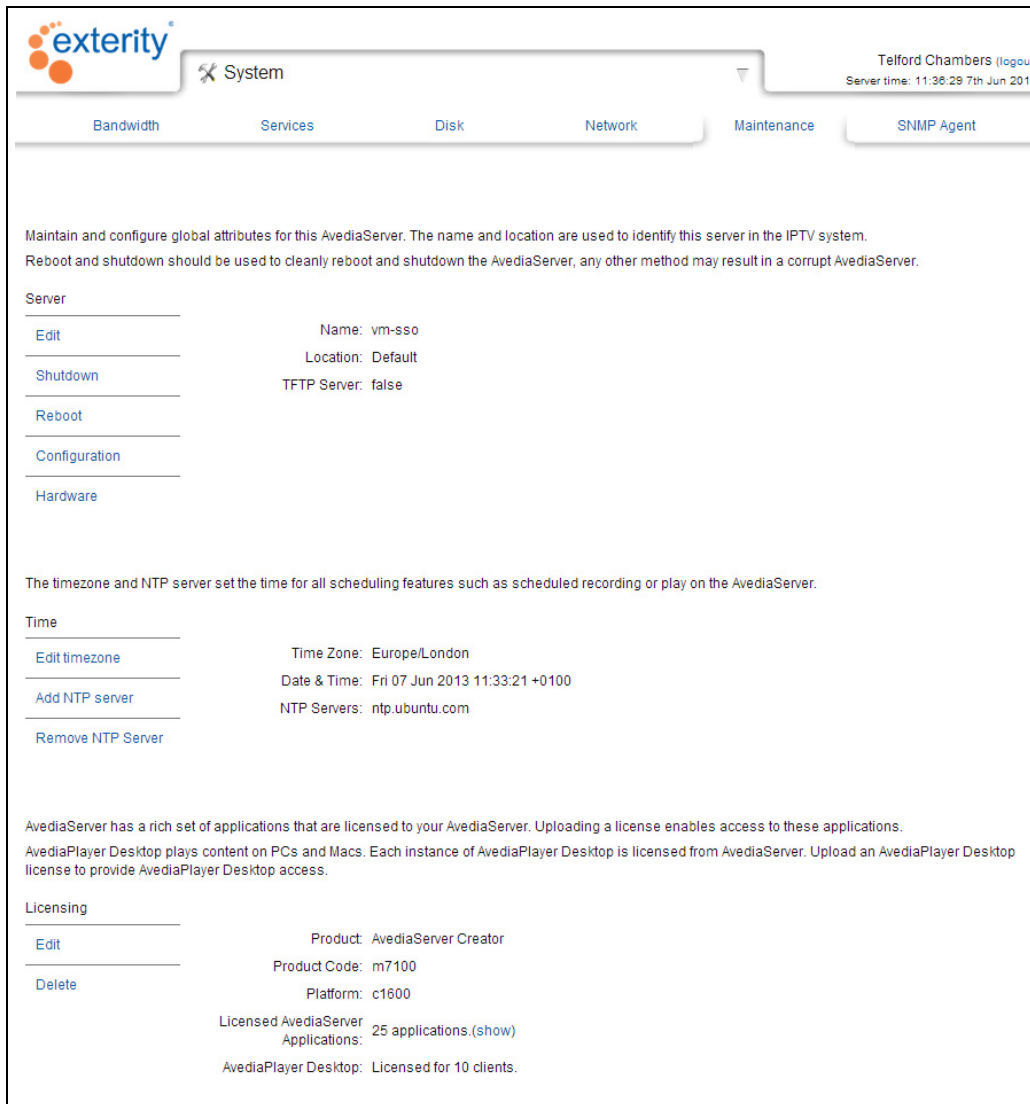
Figure 67 *System – Maintenance Page*

All procedures described in this section assume that you are running the Web Management Interface. The System application is available in all configurations of AvediaServer.

Note: When making changes to settings, click Apply to save your changes before moving to another page or application, otherwise your changes are lost.
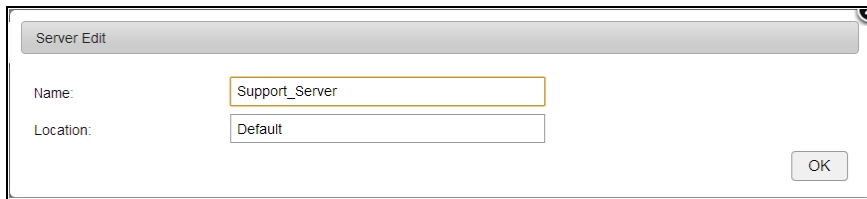
Naming the AvediaServer

The AvediaServer can be assigned a name and location. This name and location can be used to identify the AvediaServer within the AvediaServer Director application. For example, if you specify the location Foyer, the server is listed with Foyer in the location column in the AvediaServer Director AvediaStream page.

The default name assigned to the AvediaServer is its MAC address.

To specify the name and location:

1   Start the System application.

2   Click the Maintenance tab and in the System name section.

3   Click Edit and enter the required values in the Name and Location fields.

Figure 68 *Setting the name and location*
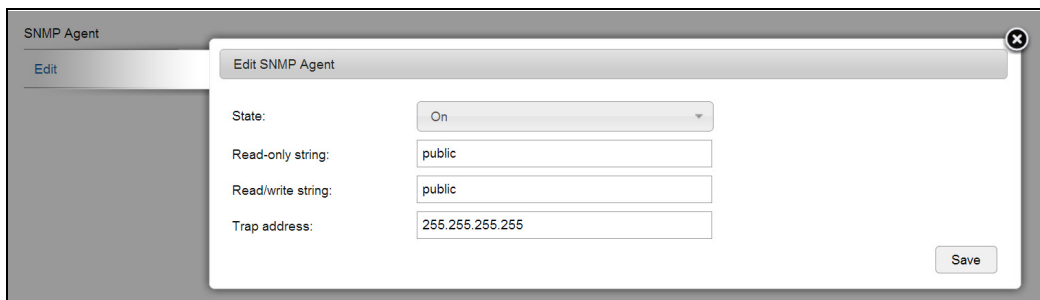
4   Click OK.

Configuring the SNMP Community Strings

With the SNMP agent enabled you can manage the AvediaServer as an independent device on the network. SNMP is used by applications such as the AvediaServer Director application to perform the functions listed. It is also possible to completely disable the use of SNMP.

To configure SNMP community strings:

1   Click the SNMP Agent tab.

2   Click Edit.

Figure 69 *Editing SNMP settings*

3   Enter the required read/write and read-only community strings in the appropriate boxes.

4   Click Save.

To enable/disable SNMP control:

1   Click the SNMP Agent tab.

2   Click Edit.

3   Select On or Off as required from the State drop-down list.

4   Click Save.

Configuring Network Settings

Configuring IP Address Settings

You can configure the server to obtain an IP address automatically using DHCP, or you can specify static addressing information: IP address, subnet mask, and default gateway.

Note: Changes to IP addressing take place immediately on clicking Apply.

By default, the AvediaServer is configured to obtain an IP address using DHCP:
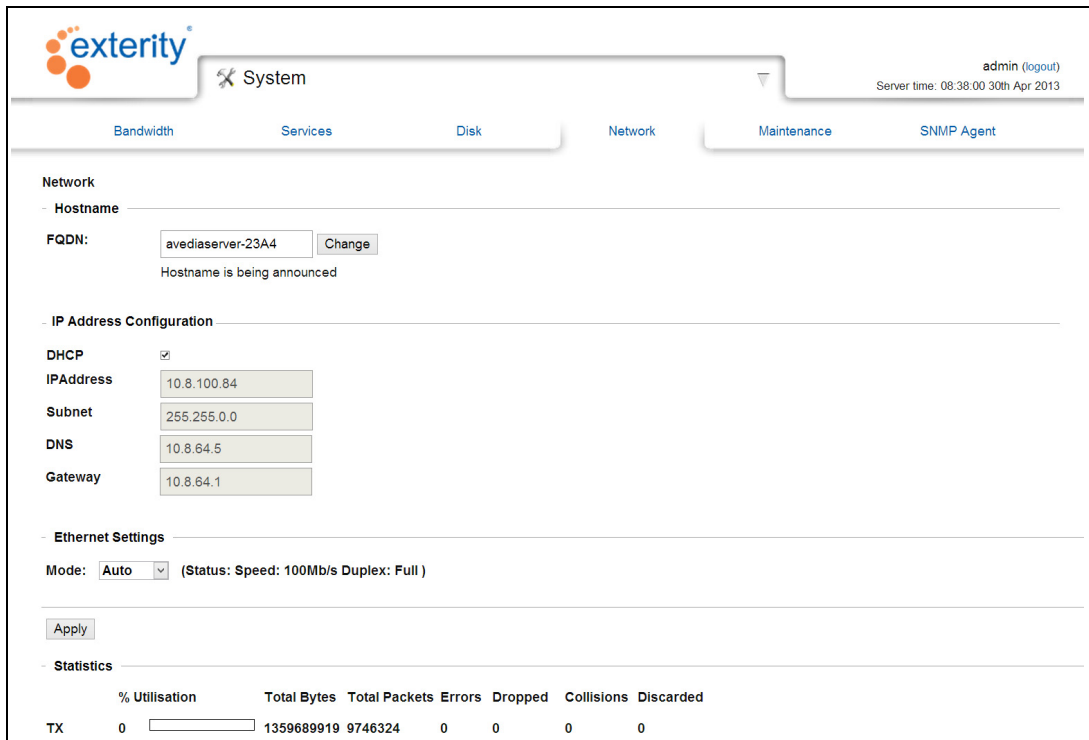
Figure 70 *System – Network Page*

To configure a static IP address:

1 Start the System application.

2 Click Network and in the IP Address Configuration section, deselect the DHCP checkbox.
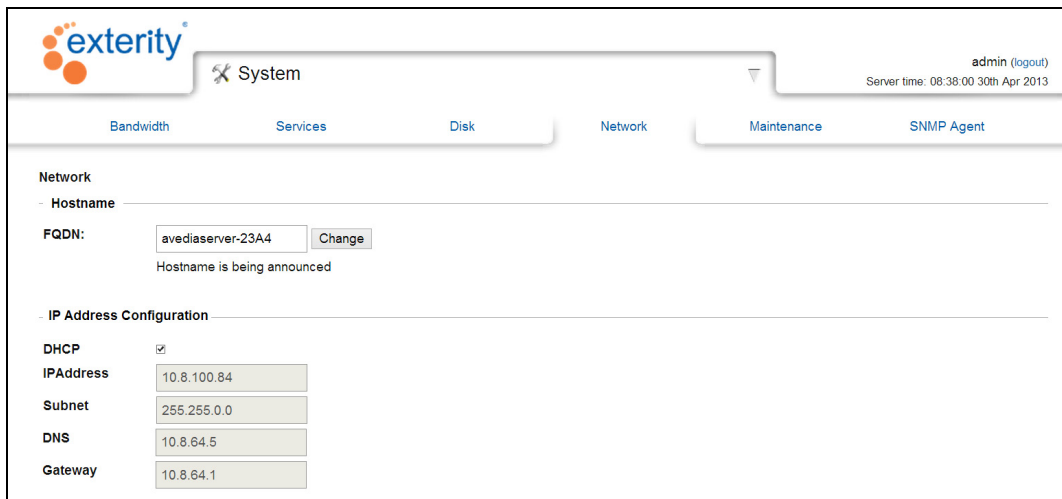
Figure 71 *System – Network Page*

3 Enter the required IP Address, Subnet mask, DNS address and Gateway Address in the appropriate fields.

4 Click Apply.

To configure the AvediaServer to be allocated an IP address dynamically:

1 Start the System application.

2 Click Network and in the IP Address Configuration section, select the DHCP checkbox.

3 Click Apply.

Note: Exterity strongly recommends using a static IP address for the AvediaServer because other Exterity devices rely on this address remaining the same.

Configuring the Ethernet Settings

The AvediaServer Ethernet interface is a 100/1000 port that can be set to either auto-negotiation, 1000FD or 100FD mode. Auto-negotiation is enabled by default.

Note: In order to avoid Ethernet errors, ensure that the server's interface settings match the settings for the network switch port to which the server is connected. This means that either both devices should be configured for auto-negotiation or both devices should be configured for a fixed setting of 1000FD or 100FD. A Gigabit port is essential to ensure full operating performance with VoD, Play and Record functions.

You can view the Ethernet Settings on the Network page:

Ethernet Settings

Mode: Auto   (Status: Speed: 100Mb/s Duplex: Full)
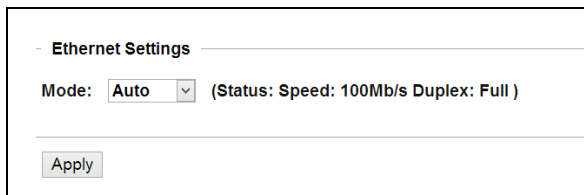
Apply

Figure 72 *System – Ethernet settings*

To enable/disable auto-negotiation:

1   Start the System application.

2   Click Network and in the Ethernet Settings section, choose an option from the Mode drop-down list.

3   Click Apply.

Configuring NTP Server and Local Time

Specifying NTP Servers

You can configure NTP Time Servers on the Maintenance page. The AvediaServer uses these to keep time accurately and adjusts its time accordingly. You must configure one or more NTP Servers to ensure correct operation of the Play and Recorder applications and the guide in the Portal and Player client interfaces.

Note: When DHCP is used and the DHCP server supplies an NTP server address, this server is used in preference to any NTP servers configured using the Web Management Interface. If the DHCP server does not supply an NTP server address, the address must be configured on the Maintenance page.

To add an NTP server:

1   Start the System application and click Maintenance.

2   In the Time menu click Add NTP Server.

3   Enter the IP address of the required NTP server in the Server address field.

Edit timezone   Time Zone: Europe/London

Add NTP server   Add NTP Server

Remove NTP Server   Server address: 10.8.64.100

Add

Figure 73 *System – adding an NTP Server*

4   Click Add.

5   Add additional servers if required.

6   Confirm the NTP Servers have been added by clicking the *NTP Server: x servers show* hyperlink to view the added IP addresses.

To remove an NTP server:

1   Start the System application.

2   Click Maintenance and in the Time section, click Remove NTP Server.
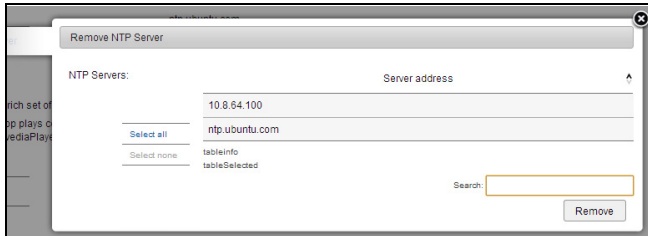
Figure 74   *System - removing an NTP Server*

3   Select the NTP Server to be deleted.

4   Click Remove.

Configuring the AvediaServer Timezone

The AvediaServer has a real-time clock that is persistent over reboots and power downs. Maintaining accurate synchronisation with local time is vital to ensure correct operation.

Caution: Changing the time zone automatically reboots the AvediaServer causing interruption to Play channels and current VoD sessions. Therefore, ensure that you configure the time zone before scheduling any content.

To configure the time zone of the AvediaServer:

1   Start the System application.

2   Click Maintenance and in the Time section click Edit timezone.
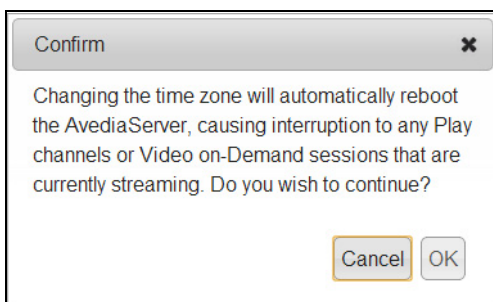
Figure 75   *Changing time zone advisory message*

3   Click OK to continue or Cancel.

4   If OK, select the option from the Time Zone drop-down list that best suits the location of the AvediaServer.
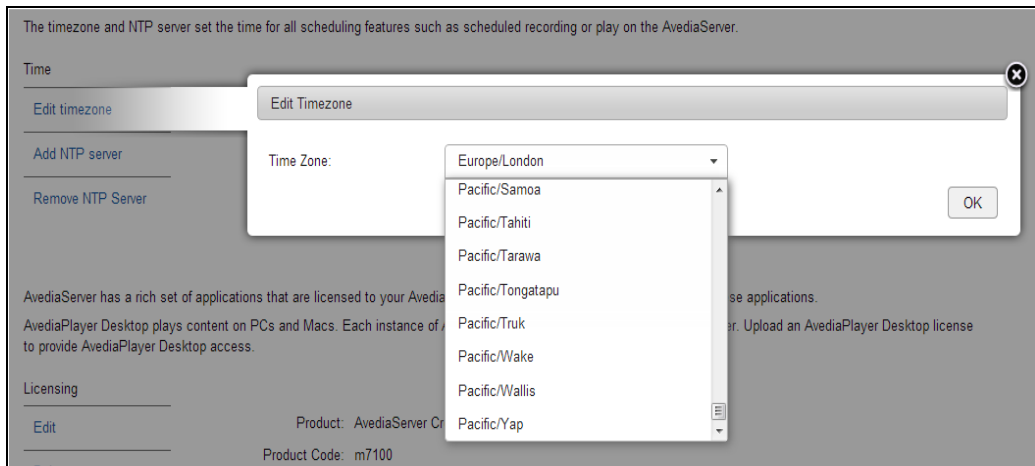
Figure 76 *Selecting a new time zone*

5   Click OK to apply the selected time zone setting.

Specifying a Fully Qualified Domain Name

A Fully Qualified Domain Name (FQDN) for the AvediaServer is one of the elements required to enable Single Sign On (SSO) and secure (https) communication with the AvediaServer.

To specify a fully qualified domain name for the AvediaServer:

1   Start the System application.

2   Click Network.

Figure 77 *FQDN required*

3   Enter the domain name required in the FQDN field, for example:
    `avediaserver-cb1a.exterity.local`

4   Click Change. The name is applied with messages "Hostname changed" and "Hostname being announced" to indicate successful completion.

Figure 78 *Hostname announced*

Refer to "Configuring for Secure Server Access" on page 110 and "Configuring for Single Sign-on Operation" on page 112 to complete SSO and/or secure communication with the AvediaServer.

Configuring AvediaServer Services

The applications configured for the AvediaServer specify the Services available. Each application supplies one or more Services and they are used by the application to perform its function. They can be enabled or disabled on the System application Services page.

Note: The default Services configuration should not be changed unless you want to enable/disable specific AvediaServer functions.

Start the System application and click the Services page:
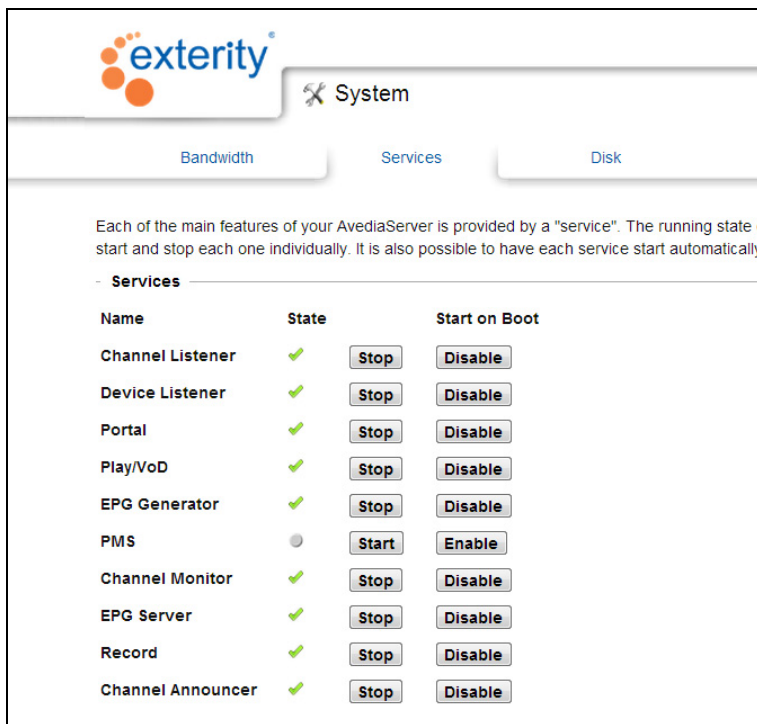
Figure 79 *System – Services Page*

The licence Type is shown in the Product licence section. The status of all available services is displayed in the Services section. Refer to Table 7 on page 73 for detailed information about each Service.

The default setting is for all Services to start on boot.

AvediaServer services status is shown by a simple traffic light icon that has 3 states:

Indicates that the Service is running without any errors.

Indicates that the Service is not running. The administrator has deliberately stopped the Service, or an error has occurred.

Indicates that start on boot is disabled and the Service is not running.

Starting and Stopping Services

To start a service:

1   Start the System application.

2   Click Services and click Start next to the Service you wish to start.

3   Confirm the State turns to   , indicating the Service has started.

To stop a service:

1   Start the System application.

2   Click Services and click Stop next to the Service you wish to stop.

3   Confirm the State turns to ✖ if Start on Boot is enabled or ⬤ if Start on Boot is disabled.

Configuring Services to Start on Boot

You can configure services to start automatically when you start the AvediaServer. You can also disable services from starting on boot.

To enable a service to start on boot:

1   Start the System application.

2   Click Services and click Enable next to the Service you wish to enable. The button changes to Disable.

3   The Service is now configured to start automatically the next time you boot the AvediaServer.

To disable a service from starting on boot:

1   Start the System application.

2   Click Services and click Disable next to the Service you wish to disable. The button changes to Enable.

3   The Service is now configured to remain off until manually enabled the next time you boot the AvediaServer.

Note: Changing the Start on Boot status of a Service does not immediately turn it on or off. The status only changes on the next AvediaServer reboot.

Services in Detail

Table 7   Service name and function

Service Name	Function
Device Listener	Device Listener automatically discovers devices for use throughout the IPTV system. When disabled, no new devices can be detected and device list pages are not updated. Refer to "Managing Devices" in the *AvediaServer IPTV System Administrator's Guide* for more information.
Channel Listener	Channel Listener function uses SAP (Session Announcement Protocol) messages to generate a list of channels for all applications. When disabled, the list is not updated.
EPG Generator	The EPG generator creates EIT tables for the play channels so that they can appear as part of the aggregated EPG.
Scheduled Play/VoD	Enables/disables the play and video-on-demand (VoD) functionality used by the Play and Video on Demand applications.
EPG Server	The EPG (Electronic Program Guide) combines EIT (Event Information Table) data for the various content sources on the IPTV network, providing a consolidated program guide. Enables/disables the EPG server. When disabled, no EPG information is available.
Portal	Enables/Disables the Portal Client Interface and AvediaPlayer Desktop functions.
PMS	Enables/disables the AvediaServer interface to a Property Management System (PMS).

Table 7 Service name and function
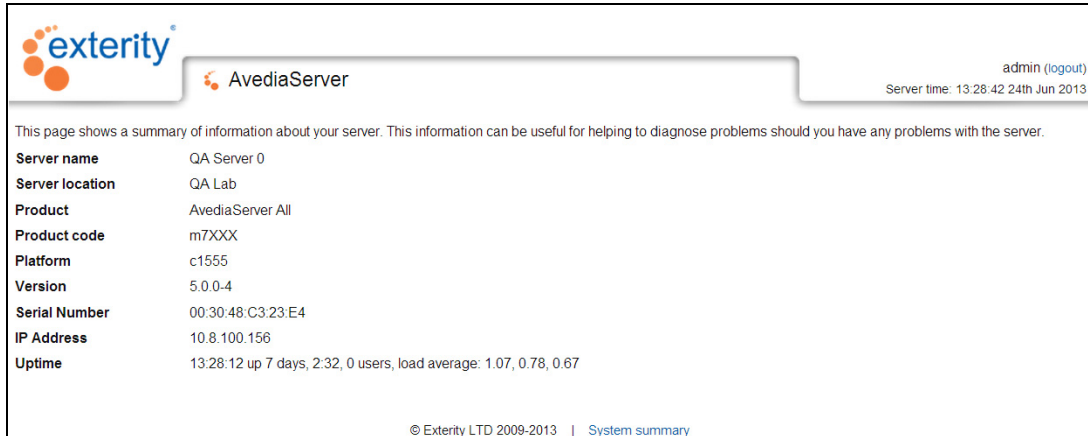
Service Name	Function
Record	When enabled, allows the scheduled recording of content. If disabled, recording capabilities are globally withheld.
Channel Monitor	When enabled, you can selectively view additional channel information on the Channel pages in the Director application.
Channel Announcer	SAP Announcements are used by Exterity Receivers and Servers for channel discovery. Channel Announcer sends SAP announcements for channels created in the Play application and channels configured in the Channel Announcer application. This is also useful for third party channels that do not use SAP Announcements.

Managing AvediaServer and AvediaPlayer Desktop Licences

The AvediaServer licence enables the AvediaServer applications in accordance with the purchased software. Each AvediaServer is supplied with 10 preinstalled floating licences for the AvediaPlayer Desktop.

Determine Installed Licences

To determine the AvediaServer licence type, click the System summary link at the bottom of the AvediaServer Home screen.

Figure 80 *Reviewing installed licences*

The installed AvediaPlayer Desktop licence is listed in the Product code line as follows:

Product Code and Product

- avsrv-m7100 — AvediaServer IPTV Director Software
- avsrv-m7200 — AvediaServer IPTV Producer Software
- avsrv-m7300 — AvediaServer IPTV Creator Software

Platform

- avsrv-c1510 — AvediaServer c1510 Hardware Platform
- avsrv-c1555 — AvediaServer c1555 Hardware Platform
- avsrv-v1600 — AvediaServer Virtual Platform

Managing licences

The AvediaServer licence enables the specified applications only for the MAC address of the AvediaServer chassis, or if a VM installation, on the configured MAC address of the virtual machine. When purchased as an AvediaServer chassis and software combination the licence is preinstalled and no further action is required. If the AvediaServer software is installed on a virtual machine, or if you are upgrading your licence, refer to "Installing Licences", below.

Additional purchased licences can be installed from the supplied USB memory stick and are added to the10 preinstalled licences. The floating licences can be reserved by any suitable PC or Mac and are released when the application is closed.

Installing Licences

AvediaServer licences or additional AvediaPlayer Desktop licences are installed on the server by uploading the licence details from the supplied USB device using the admin computer. The licence file on the USB device is in the form: <AvediaServerLicence_SalesOrder.txt> or <DesktopPlayerLicence_SalesOrder.txt> where "SalesOrder" is the text string of the Exterity sales order code. Each licence is locked to an AvediaServer.

To install licences:

1 Start the System application.

2 Insert the USB Licence stick into a port accessible by your PC/browser.

3 Click Maintenance and click Edit in the Licensing section of the page.

4 Select AvediaServer or AvediaPlayer Desktop from the Licence type drop-down list. (The AvediaServer licence must be uploaded first, you cannot upload the AvediaPlayer Desktop licence(s) without an in-place AvediaServer licence.

5 Click Choose File and use the Windows Explorer window to navigate to the licence file on the memory device. When located click Open.
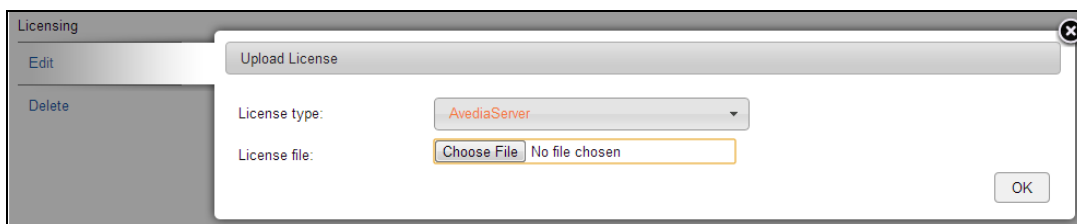
Figure 81 *Licence Type Selection*

6 Click OK to add the licence.

Note: Following the licence installation (either AvediaServer or AvediaPlayer Desktop) the AvediaServer reboots.

7 Confirm the AvediaServer licence has been installed by clicking the 'show' hyperlink to display the list of enabled applications.

8 Check the number of AvediaPlayer Desktop licences has been incremented correctly.
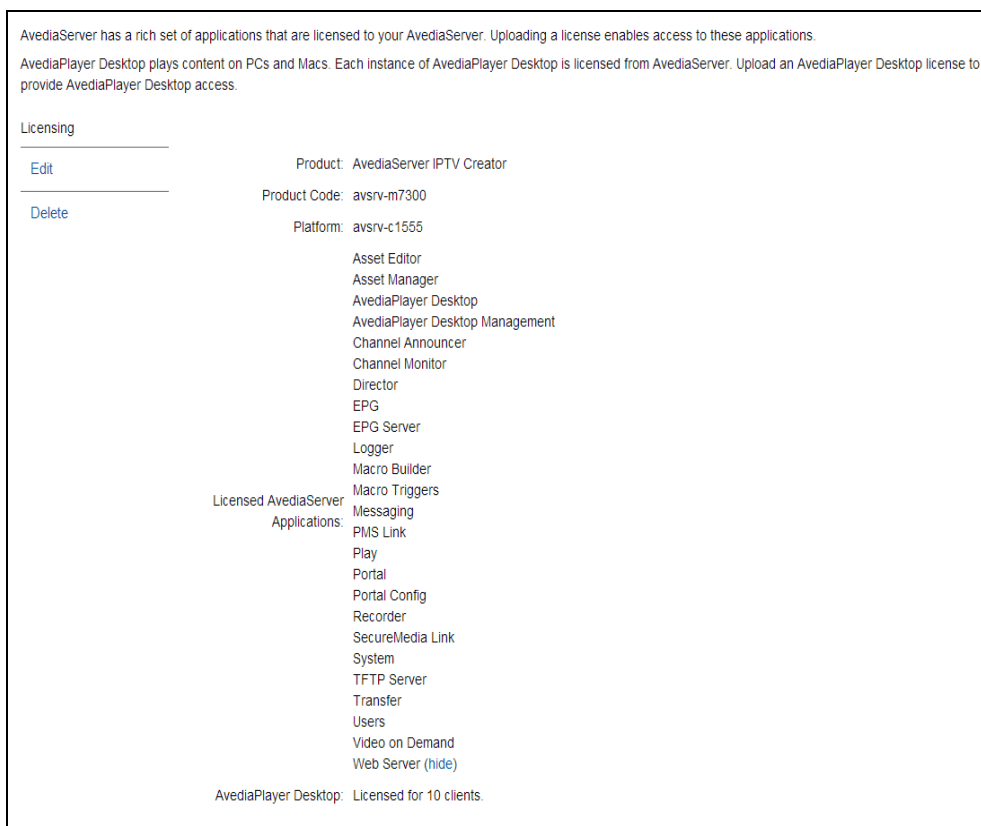
Figure 82 *Showing enabled applications*

Status Monitoring

This section explains how to check the operating status of the AvediaServer. It contains the following sections:

- Viewing AvediaServer Details
- Viewing Hardware Information
- Viewing Network Status
- Viewing RAID Status

Viewing AvediaServer Details

You can view the basic AvediaServer details at any time by clicking the System summary page as shown in Figure 9:
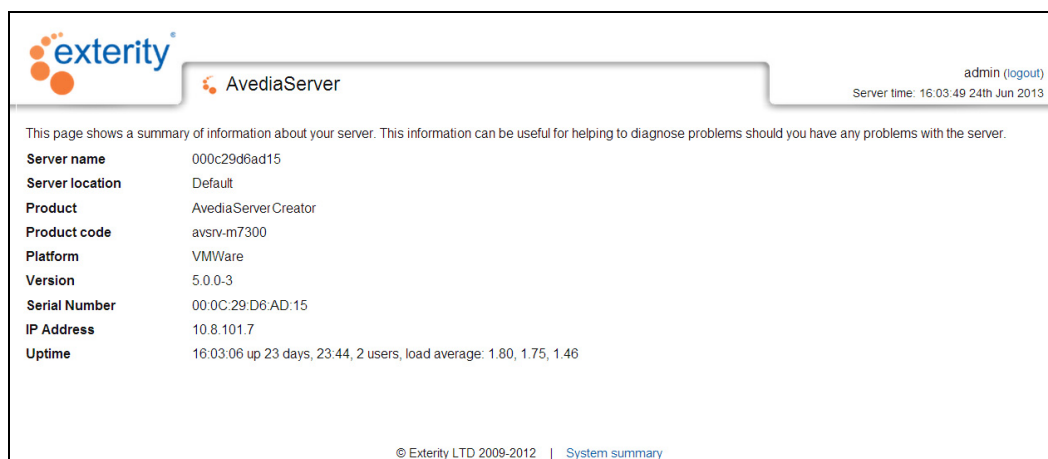
Figure 83 *AvediaServer – System Summary Page*

The following information is displayed:

- **Server name** – Name of the AvediaServer. Refer to "Naming the AvediaServer" on page 65 for more information.

- **Server location** – Location of the AvediaServer. Refer to "Naming the AvediaServer" on page 65 for more information.

- **Product** – The AvediaServer Software Title (Application Bundle).

- **Product code** – The AvediaServer Software Code

- **Platform** – The AvediaServer chassis model or virtual machine information.

- **Version** – The currently installed AvediaServer firmware version.

- **Serial Number** – The MAC address of the AvediaServer eth0 port or as assigned in the virtual machine installation.

- **IP Address** – The IP address assigned to the AvediaServer, either configured statically or assigned by DHCP. Refer to "Configuring Network Settings" on page 66 for more information.

- **Uptime** – The length of time since the last power-on or reboot, number of users, and load average statistics.

- **Desktop Users** – Indicates the number of available AvediaPlayer Desktop licences.

    Note: You can also configure the AvediaServer to log specific information about its performance using the Logger application. Refer to Chapter 7, "Using the Logger Application" for more information.

Viewing Hardware Information

To view hardware information for the AvediaServer:

1 Start the System application.

2 Click Maintenance and click Hardware Info Show in the Server Details section:

```
#### Network Interface Configuration ####
eth0     Link encap:Ethernet  HWaddr 00:30:48:7c:c0:2a
         inet addr:10.8.100.153  Bcast:10.8.255.255  Mask:255.255.0.0
         inet6 addr: fe80::230:48ff:fe7c:c02a/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:291018818 errors:0 dropped:0 overruns:0 frame:0
         TX packets:10624886 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:2160552695 (2.0 GB)  TX bytes:1983825880 (1.8 GB)
         Base address:0x2000 Memory:d8020000-d8040000


eth1     Link encap:Ethernet  HWaddr 00:30:48:7c:c0:2b
         UP BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:
```

Figure 84 *System – Hardware Information*

Viewing Network Status

The Statistics section of the Network page provides an indication of the bandwidth being used by the network interface.

Start the System application and click Network to view the Statistics in the lower half of the page. The AvediaServer automatically updates the statistics without the need to refresh the page.

	% Utilisation	Total Bytes	Total Packets	Errors	Dropped	Collisions	Discarded
TX	4.1	1361165938	9759822	0	0	0	0
RX	0.1	3694624904	1857417602	0	0	0	0

Statistics

Figure 85 *System – Network Statistics*

Note: If the channels are streaming, the bandwidth being used by the network indicates this; a standard definition (SD) TV channel typically uses 4Mbps of network bandwidth and a radio channel uses approximately 200kbps.

Viewing RAID Status

The AvediaServer c1555 chassis supports multiple disks configured in a RAID array, which ensures that no data is lost in the event of a disk failing. This capability is not supported on the c1510 chassis and the RAID page is not displayed in the AvediaServer menu.

Note: A RAID array of disks is used for content storage, which typically applies to AvediaServers used for Play and Record.

Due to implementation differences, the c1550 and c1555 chassis RAID reporting pages differ.

Checking the c1550

To check the status of the RAID array on the c1550 chassis:

1   Start the System application and click Disk:

```
RAID Status

Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]

md0 : active raid5 sdb1[0] sdd1[2] sdc1[1]

      625137152 blocks level 5, 64k chunk, algorithm 2 [3/3] [UUU]


unused devices: <none>
/dev/md0:
          Version : 00.90.03
    Creation Time : Thu Apr 29 16:14:52 2010
       Raid Level : raid5
       Array Size : 625137152 (596.18 GiB 640.14 GB)
    Used Dev Size : 312568576 (298.09 GiB 320.07 GB)
     Raid Devices : 3
    Total Devices : 3
  Preferred Minor : 0
      Persistence : Superblock is persistent

      Update Time : Thu Feb  9 09:17:39 2012
            State : clean
   Active Devices : 3
  Working Devices : 3
   Failed Devices : 0
    Spare Devices : 0


           Layout : left-symmetric
       Chunk Size : 64K


             UUID : f121f3b6:50119e03:a20ddd0c:66c16573 (local to host avediaserver-8968)
           Events : 0.108


    Number   Major   Minor   RaidDevice State
       0       8       17        0      active sync   /dev/sdb1
       1       8       33        1      active sync   /dev/sdc1
       2       8       49        2      active sync   /dev/sdd1

Disk Layout:
sda -> pci-0000:00:1f.2-scsi-0:0:0:0
sdb -> pci-0000:00:1f.2-scsi-1:0:0:0
sdc -> pci-0000:00:1f.2-scsi-2:0:0:0
sdd -> pci-0000:00:1f.2-scsi-3:0:0:0
```

Figure 86 *AvediaServer c1550 chassis RAID page*

2   Check that the last characters in the third line of information look like [UUU], as shown below:

Each 'U' relates to an individual disk in the RAID array. In the above example, there are five disks in the array.

If an underscore is displayed (for example, [U_U]), one of the disks is faulty and has been removed from the RAID array.

3   Further down the page, check the number of RAID Devices. If all the disks are working properly, the information is as follows:

If the number of total devices is less than the number of RAID Devices (for example, Total Devices = 4 and RAID Devices = 5), a disk(s) in the array is faulty and has been removed from the RAID array.

```
Disks missing from the RAID array
```

A disk could be missing from the array because it has physically been removed from the server or it could be logically removed from the array because of some other problem (for example, read/write errors resulting in the RAID software deciding not to use the disk and removing it from the RAID array).

If you discover there is a disk missing, please contact support for assistance. For more information, refer to Chapter 13, "Troubleshooting".

Caution: Hard disks must not be removed from the server unless guided by and instructed to so by the System Integrator or Exterity support. Removing a disk from an active RAID array can result in the loss of all data on the array and physical damage to the disk.

Checking the c1555

To check the status of the RAID array on the c1555 chassis:

1 Start the System application and click Disk:

```
RAID Status


Unit   UnitType  Status        %RCmpl  %V/I/M  Stripe  Size(GB)  Cache  AVrfy
--------------------------------------------------------------------------------
u0     RAID-5    OK            -       -       256K    13038.4   RiW    ON


VPort Status        Unit Size       Type  Phy Encl-Slot     Model
--------------------------------------------------------------------------------
p0    OK            u0   1.82 TB    SATA  0   -             Hitachi HUA722020AL
p1    OK            u0   1.82 TB    SATA  1   -             Hitachi HUA722020AL
p2    OK            u0   1.82 TB    SATA  2   -             Hitachi HUA722020AL
p3    OK            u0   1.82 TB    SATA  3   -             Hitachi HUA722020AL
p4    OK            u0   1.82 TB    SATA  4   -             Hitachi HUA722020AL
p5    OK            u0   1.82 TB    SATA  5   -             Hitachi HUA722020AL
p6    OK            u0   1.82 TB    SATA  6   -             Hitachi HUA722020AL
p7    OK            u0   1.82 TB    SATA  7   -             Hitachi HUA722020AL



Unit      UnitType  Status        %RCmpl  %V/I/M  VPort Stripe  Size(GB)
--------------------------------------------------------------------------------
u0        RAID-5    OK            -       -       -     256K    13038.4
u0-0      DISK      OK            -       -       p0    -       1862.63
u0-1      DISK      OK            -       -       p1    -       1862.63
u0-2      DISK      OK            -       -       p2    -       1862.63
u0-3      DISK      OK            -       -       p3    -       1862.63
u0-4      DISK      OK            -       -       p4    -       1862.63
u0-5      DISK      OK            -       -       p5    -       1862.63
u0-6      DISK      OK            -       -       p6    -       1862.63
u0-7      DISK      OK            -       -       p7    -       1862.63
u0/v0     Volume    -            -       -       -     -       13038.4
```

Figure 87 *System Disk (c1555)*

2 Figure 87 shows a fully operational c1555 chassis RAID array. The status is listed in the summary line at the top of the table, in this example, it is shown as OK.

3 A disk problem is reported as DEGRADED. This is shown in the summary line and in the table listing as shown in Figure 14. This indicates a failure. In this example disk u0-5 in port p2 has developed a problem.

Note: The RAID system ensures that no data is lost due to a single disk failure. However the system cannot withstand an additional failure without compromising performance. You should report this as soon as possible to your support contact.

Caution: Hard disks must not be removed from the server unless instructed to by the System Integrator or Exterity support. Removing a disk from an active RAID array can result in the loss of all data on the array.

```
RAID Status

Unit  UnitType  Status
----------------------

Unit  UnitType  Status        %RCmpl  %V/I/M  Stripe  Size(GB)  Cache  AVrfy
------------------------------------------------------------------------------
u0    RAID-5    OK            -       -       256K    13038.4   RiW    ON

VPort Status        Unit Size     Type  Phy Encl-Slot    Model
------------------------------------------------------------------------------
p0    OK            u0   1.82 TB   SATA  0   -            Hitachi HUA722020AL
p1    OK            u0   1.82 TB   SATA  1   -            Hitachi HUA722020AL
p2    OK            u0   1.82 TB   SATA  2   -            Hitachi HUA722020AL
p3    OK            u0   1.82 TB   SATA  3   -            Hitachi HUA722020AL
p4    OK            u0   1.82 TB   SATA  4   -            Hitachi HUA722020AL
p5    OK            u0   1.82 TB   SATA  5   -            Hitachi HUA722020AL
p6    OK            u0   1.82 TB   SATA  6   -            Hitachi HUA722020AL
p7    OK            u0   1.82 TB   SATA  7   -            Hitachi HUA722020AL


Unit      UnitType  Status        %RCmpl  %V/I/M  VPort Stripe  Size(GB)
------------------------------------------------------------------------------
u0        RAID-5    DEGRADED      -       -       -     256K    13038.4
u0-0      DISK      OK            -       -       p0    -       1862.63
u0-1      DISK      OK            -       -       p1    -       1862.63
u0-2      DISK      OK            -       -       p2    -       1862.63
u0-3      DISK      OK            -       -       p3    -       1862.63
u0-4      DISK      OK            -       -       p4    -       1862.63
u0-5      DISK      DEGRADED      -       -       -     -       1862.63
u0-6      DISK      OK            -       -       p6    -       1862.63
u0-7      DISK      OK            -       -       p7    -       1862.63
u0/v0     Volume    -            -       -       -     -       13038.4
```

Figure 88 *Disk Failure (c1555)*

Subsequent disk failures result in the system reporting INOPERABLE. As shown in Figure 88, 2 disks are DEGRADED resulting in an INOPERABLE status. In this condition, recording and playback is not possible.

```
RAID Status

Unit  UnitType  Status
----------------------

Unit  UnitType  Status          %RCmpl  %V/I/M  Stripe  Size(GB)  Cache  AVrfy
------------------------------------------------------------------------------
u0    RAID-5    OK              -       -       256K    13038.4   RiW    ON

VPort Status          Unit Size      Type  Phy Encl-Slot    Model
------------------------------------------------------------------------------
p0    OK              u0   1.82 TB   SATA  0   -            Hitachi HUA722020AL
p1    OK              u0   1.82 TB   SATA  1   -            Hitachi HUA722020AL
p2    OK              u0   1.82 TB   SATA  2   -            Hitachi HUA722020AL
p3    OK              u0   1.82 TB   SATA  3   -            Hitachi HUA722020AL
p4    OK              u0   1.82 TB   SATA  4   -            Hitachi HUA722020AL
p5    OK              u0   1.82 TB   SATA  5   -            Hitachi HUA722020AL
p6    OK              u0   1.82 TB   SATA  6   -            Hitachi HUA722020AL
p7    OK              u0   1.82 TB   SATA  7   -            Hitachi HUA722020AL


Unit       UnitType  Status          %RCmpl  %V/I/M  VPort Stripe  Size(GB)
------------------------------------------------------------------------------
u0         RAID-5    INOPERABLE      -       -       -     256K    13038.4
u0-0       DISK      OK              -       -       p0    -       1862.63
u0-1       DISK      DEGRADED        -       -       -     -       1862.63
u0-2       DISK      OK              -       -       p2    -       1862.63
u0-3       DISK      OK              -       -       p3    -       1862.63
u0-4       DISK      OK              -       -       p4    -       1862.63
u0-5       DISK      DEGRADED        -       -       -     -       1862.63
u0-6       DISK      OK              -       -       p6    -       1862.63
u0-7       DISK      OK              -       -       p7    -       1862.63
u0/v0      Volume    -               -       -       -     -       13038.4
```

Figure 89 *Chassis Inoperable (c1555)*

Monitoring Content Bandwidth

The System application provides a summary of the bandwidth consumption of content to and from the server. The bandwidth requirement of channels created in the Play application and configured to reserve bandwidth is also listed.

Note: Recording bandwidth is limited to a maximum of 200MB.

*Figure 90* *AvediaServer System Application – Bandwidth Page*

The table summarises maximum, reserved, used and available bandwidth for the recording and play functions on the AvediaServer. In the Streams section you can view more details for the individual channels listed by their category.

Click Refresh to update the information when required.

Maintaining the AvediaServer

This chapter describes the AvediaServer maintenance procedures. It contains the following sections:

- Importing and Exporting AvediaServer Configurations

- Upgrading the AvediaServer

- Rebooting the AvediaServer

- Shutting Down the AvediaServer
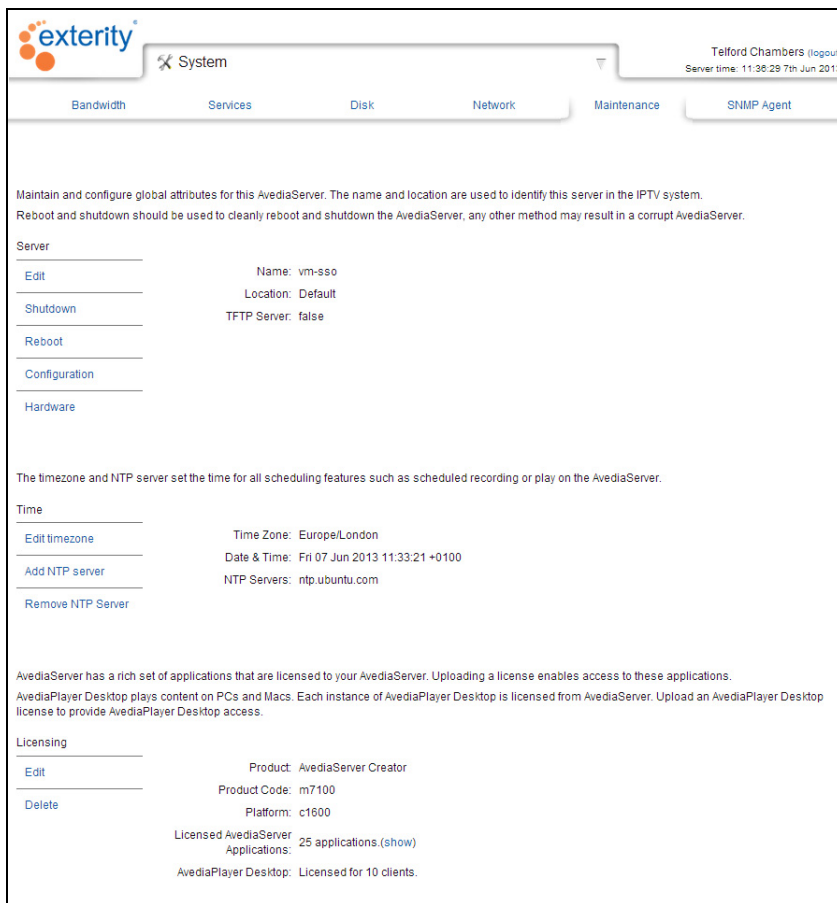
Figure 91 *System – Maintenance Page*

Importing and Exporting AvediaServer Configurations

You can export and import the AvediaServer configuration allowing you to save a specific setup for reference, or to replicate the settings on another AvediaServer. You can use a saved configuration of the AvediaServer immediately after installation to return it to a known state at any time. The configuration file is exported in the format <as_specified.tar.gz>.

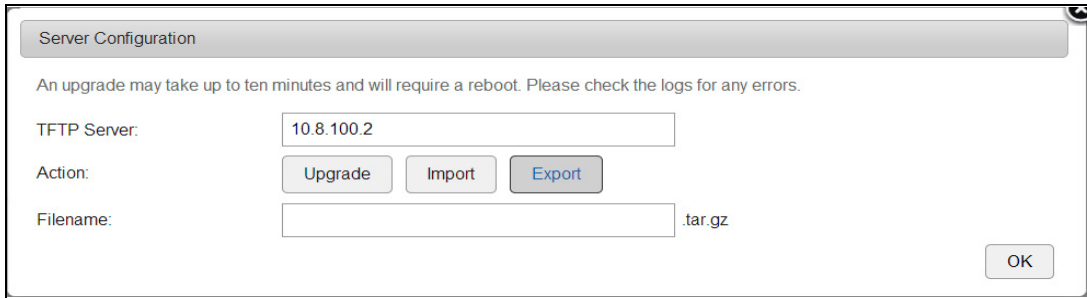The settings for the parameters listed in Table 8 are included in the configuration.

Table 8 Applications and pages in Configuration Import/Export

Application	Page Tab	Comment
Asset Manager	Genres	
	Groups	Only those added manually
	Tariff	
	Content Ageing	
AvediaPlayer Desktop Management	Configuration	Logo and configuration
Channel Announcer	Channel Announcer	
Channel Monitor	Channel Monitor	
Director	Devices	Only manually added devices (if found)
	Scheduled Tasks	
	Configuration	
EPG Server	Summary	EPG Listening Port
	XML import	XMLTV and tv anytime files
	XML assignment	
Logger	Local	Only remote settings
MacroBuilder	Macros	
MacroTriggers	Macro Triggers	
Messaging	Message	
Play	Schedule	
	EPG Generator	
PMS Link	Configuration	
	Tariff	
Portal Config	Settings	
	Display	
	Backgrounds	
	Buttons	
	Channel Genres	
	Localisation	
SecureMedia Link	SecureMedia Link	
System	Maintenance	
	SNMP Agent	
TFTP Server	TFTP server	
Transfer	Transfer hosts	
Users	User Accounts	
	Profiles	
	LDAP	
	Access Control	
	Permissions	
Video on Demand	VoD Assets	
	Servers	
	Cluster	
Web Server	Config	

To export a configuration:

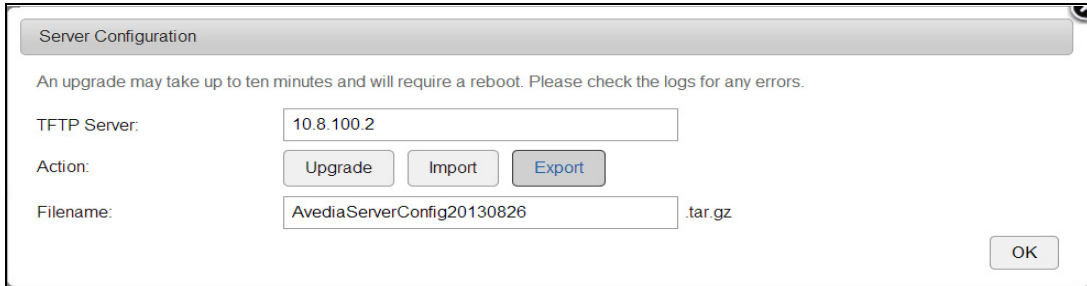1   Start the System application and click Maintenance.

2   In the Server section click Configuration, then Export.

Figure 92 *Server Configuration upgrade/import/export*

3   Enter the IP address and path of the TFTP Server/ folder in the TFTP Server field.

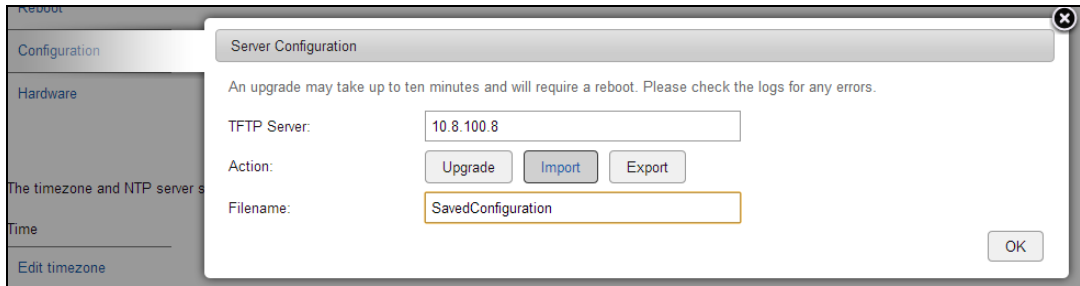4   Enter a suitable name for the exported file.

Figure 93 *Configuration export specified*

5   Click OK.

6   Confirm the exported file in the specified location.

To import a configuration:

1   Start the System application and click Maintenance.

2   In the Server section click Configuration, then Import.

Figure 94 *Importing a configuration*

3   Click Import.

4   Enter the IP address and path of the TFTP Server/ folder in the TFTP Server field.

5   Enter the name of the file to be imported.

6   Click OK to import the configuration settings.

Upgrading the AvediaServer

Upgrading an Exterity AvediaServer from a version prior to 3.0.1 is complex and involves a complete installation of the operating system. For more information, contact your System Integrator.

For version 3.0.1 or later, you can perform an upgrade using the maintenance page.

To upgrade the AvediaServer:

1   Place the new AvediaServer release file (avedia-server-install-x.y.z.tar.gz) in the root directory in a known remote TFTP server location.

Note: Exterity does not recommend upgrading an AvediaServer using the its own TFTP Server application as the source for the installation file.

2   Start the System application and click Maintenance.

3   In the Server section, click Configuration.
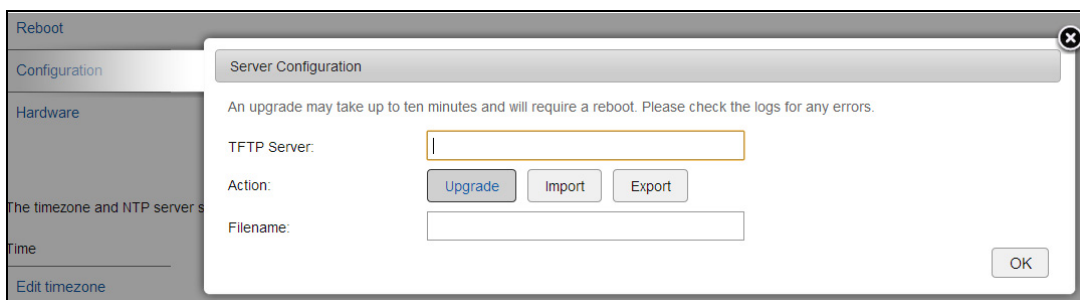
4   Enter the IP address of the remote TFTP server in the TFTP Server field.

5   Enter the name of the new firmware <abc123.tar.gz> file in the Upgrade Filename field.

6   Click Upgrade, then OK.

The AvediaServer may require more than 10 minutes and may restart more than once to complete the upgrade process. When completed, you should check the services page (System > Services) to confirm the configuration is as required.

Note: Following upgrade, you should restart your browser to ensure browser caching does not affect the information displayed.

Rebooting the AvediaServer

To reboot the AvediaServer:

1   Start the System application and click Maintenance.

2   In the Server section, click Reboot.

Shutting Down the AvediaServer

Caution: The AvediaServer must be shut down using only the process described; do not simply remove power to the chassis.

To shut down the AvediaServer:

1   Start the System application and click Maintenance.

2   In the Server section, click Shutdown.

9 Using the TFTP Server Application

This section describes how to configure and use the TFTP Server application. Exterity devices use TFTP to download firmware upgrades and other files such as IR and serial configuration files. The firmware and configuration files are hosted on a TFTP server, and the Exterity device downloads the appropriate file from the TFTP server.

You can establish a folder structure in the TFTP Server application to help manage multiple devices and file types. Uploads and downloads to other IPTV system devices must always be carried out from the TFTP Server root directory. "Managing Files on the TFTP Server" shows you how to use the TFTP Server page functions.

In addition to configuring the TFTP Server application, you must also specify the TFTP server address and port on each device to enable the transfer of firmware and configuration files. The TFTP server address can be configured using the device admin web interface; however the AvediaServer Director application allows you to configure single or multiple devices simultaneously.
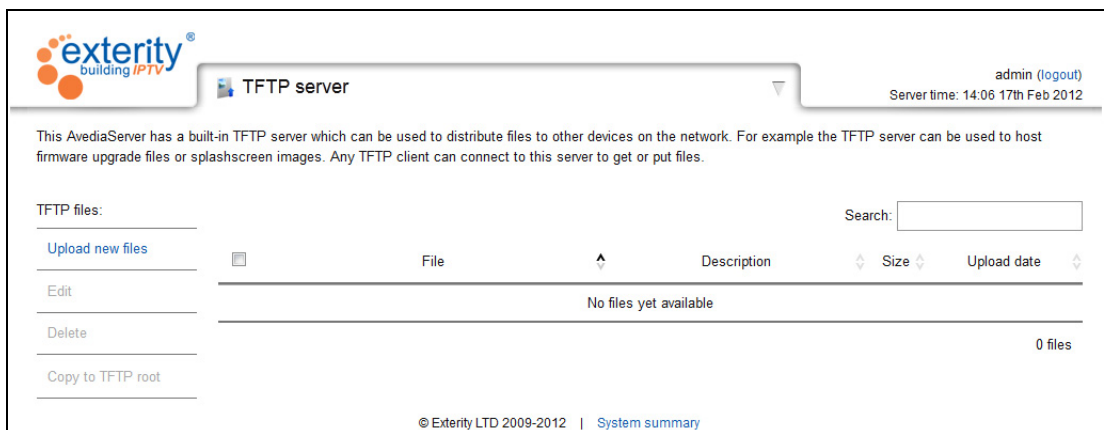
Figure 95 *TFTP Server Page*

Managing Files on the TFTP Server

The TFTP Server application allows you to manage files such as device firmware, device settings and splash screen images. You can create a directory structure to help organise multiple device and file types.

When transferring files to a device, for example during a firmware upgrade, the files must be made available in the TFTP Server root folder. Similarly, any files transferred from a device are placed in the TFTP Server root.

This section describes the following procedures:

- Uploading Files to the TFTP Server
- Editing Files in the TFTP Server Directories
- Copying Files to and from TFTP root

Uploading Files to the TFTP Server

This section shows how to upload items such as device firmware files to the required directory on the TFTP Server. You can also upload and uncompress ZIP archives, preserving their directory structure.
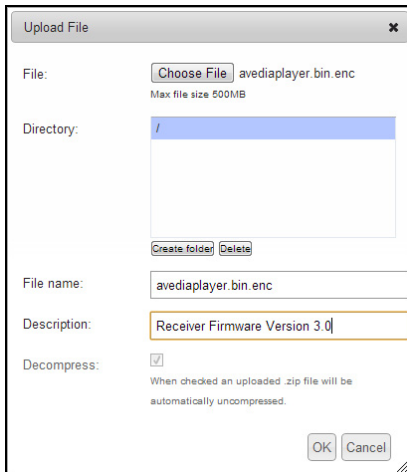
To upload files to the TFTP server:

1   Start the TFTP Server application to display the page shown in Figure 5.

2   Click Upload New Files:
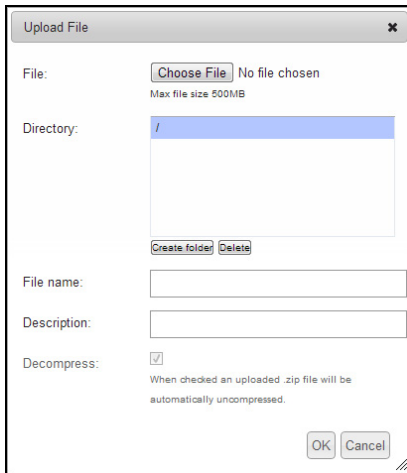
Figure 96   *Preparing for upload*

3   Click Choose File and locate and select the file you want to upload. Confirm the required file is correctly listed in the File: field.

4   If required, add a description for the file.

Figure 97   *Adding a description for the selected file*

5   Press OK to upload the file to the TFTP root directory, or to upload the file to a folder, first select the required folder in the Directory list.

6   If a suitable folder is not listed, click Create folder and enter the required name in the Create Folder window. Then select the directory and click Ok.
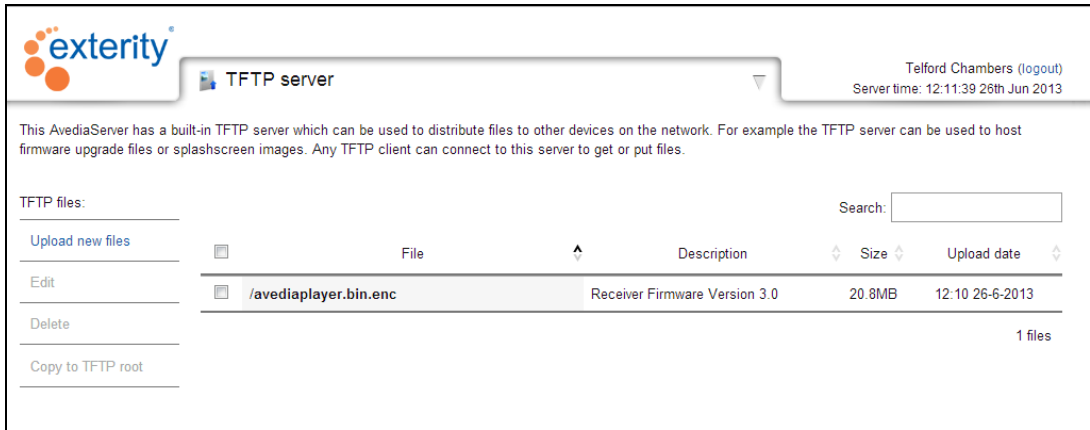
Figure 98 *File listing*

The file is now listed on the TFTP Server page. Note that the full path in shown (with respect to the root folder). The filename is shown in bold.
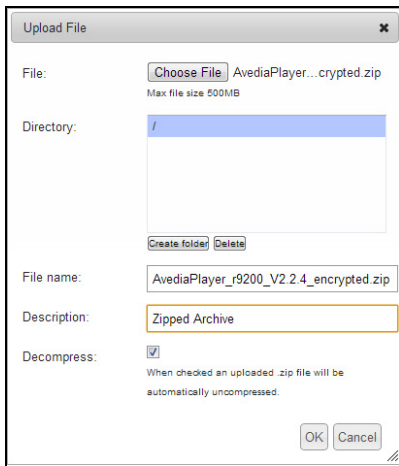
Figure 99 *Uploading a zipped archive*

7   To upload a zip archive and preserve its directory structure, select the Decompress check box in the Upload File window.

8   Select the required destination, add a description and click Ok.
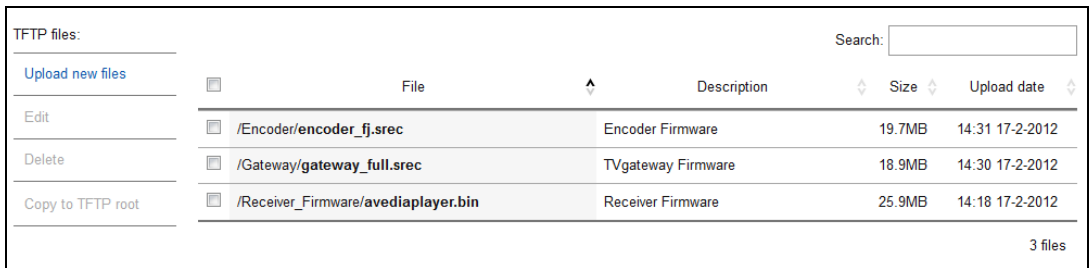

Figure 100 *Preserved folder structure*

9   The archive is uploaded and uncompressed. The directory structure and contents are maintained. Please note that you cannot overwrite files of the same name and the contents of a file of the same name on the ftp server are preserved and any transfer attempt ignored.

10   The Description is applied to all files in the upload. If required, you can edit the description for each listed file as described in "Editing Files in the TFTP Server Directories".

Editing Files in the TFTP Server Directories

You can edit, move, or delete any file and directory listed in the TFTP Server application.

To edit and move a listing on the TFTP Server:

1   Click the check box for the file you want to edit.

2   Click Edit.
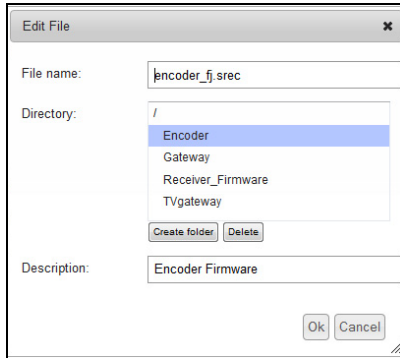
Figure 101   *Editing a listed item*

3   You can edit the file name, the file location and its description. Only one file can be edited at a time.

- **Name** - Edit the text as required.

- **Location**

  - To move the file to a different directory, select it in the Directory: list.

  - To move the file to a new directory, click Create folder.

  - To move the file to a new folder within an existing folder, first select the existing folder before clicking Create folder.

- **Description** - Enter a new file description.

- **Delete** - To delete a folder and all its contents select it in the Directory: list and click Delete.

4   Click Ok when you have made all required changes.

To delete a file from the TFTP Server:

1   Click the check box for the file you want to delete. Select additional files if required.

2   Click Delete.
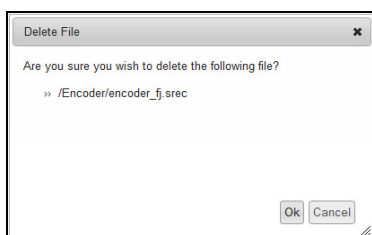
Figure 102   *Delete file confirmation*

3   Confirm the selection and click Ok to delete the file.

4   The file is removed from the listing.

5   To delete all TFTP Server content, click the check box at the top of the column to select all items and click Delete.

Copying Files to and from TFTP root

Exterity devices are configured to access the root folder of the specified TFTP server address. To transfer a file to another device it must therefore first be placed in the root directory of the TFTP Server application.

To copy a file to the TFTP root directory:

1   Select the file you want to make available in the root directory.

Figure 103 *Selecting the required file*

2   Click Copy to TFTP root.

3   The file is copied to the TFTP root directory and the TFTP Server list is updated to show the new listing, including an updated Description field detailing the original file location. Ensure the required files are available in the TFTP root directory prior to starting a Director application action such as upgrading firmware.

Figure 104 *File copied to Root*

Note: The TFTP Server root directory can contain as many files as required. A warning window appears if files of the same name are about to be overwritten by the Copy to TFTP root process.

Similarly, files transferred from a device, such as configuration files, are placed in the root directory. If required, you can manually add a description.

10 Using the Users Application

This section describes configuration of specific capabilities for users, or groups of users, who have access to the AvediaServer using the Web Management Interface.

The functions described in this section are accessed from the Users application and are available in all configurations of AvediaServer.

The AvediaServer User account management allows you to configure specific user and group accounts, their associated profiles, and the capabilities of each profile. User accounts and profiles can be added, edited, and deleted. You cannot however delete or edit the base admin account and profile. If Active Directory has been implemented in the organisation, you can use the LDAP Groups function to assign profiles to user groups without creating specific named accounts for each individual user. Users can use their domain credentials to log in.

In addition, the content available to users, or groups of users, can be managed using the Exterity Groups mechanism. By assigning a group to a profile, only the channels and VoD assets in the group are available to users assigned to the profile. The combination of assigning groups and user accounts to a profile allows you to filter the content available to users according to their login.

This section describes the following procedures:

- Changing the Admin Account
- Managing Profiles
- Managing User Accounts
- Configuring LDAP Access
- Managing Active Directory User Group Accounts
- Managing API Access to the AvediaServer
- Specifying Default Content Sharing Permissions
- Configuring for Secure Server Access
- Configuring for Single Sign-on Operation
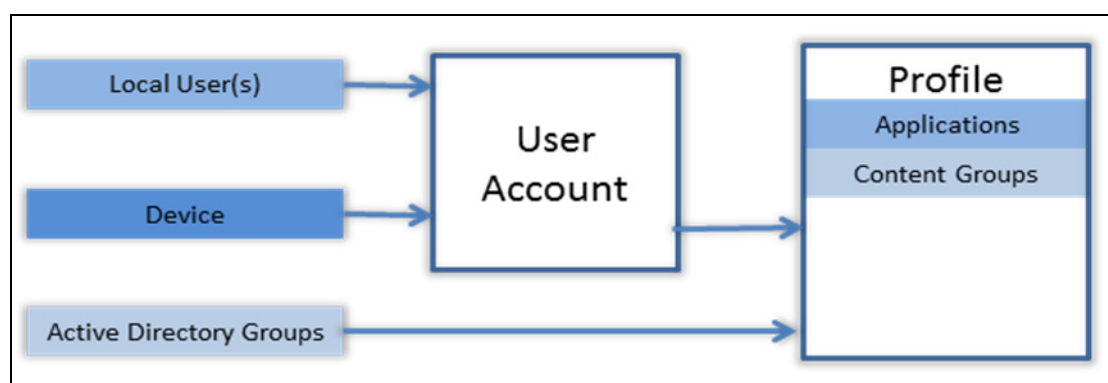
Figure 105 *Users overview*

Changing the Admin Account

By default, a username/password pair of admin/labrador is required to gain access to the Web Management Interface and the Admin Interface. The admin password can be changed by the administrator, as required.

To change the admin password:
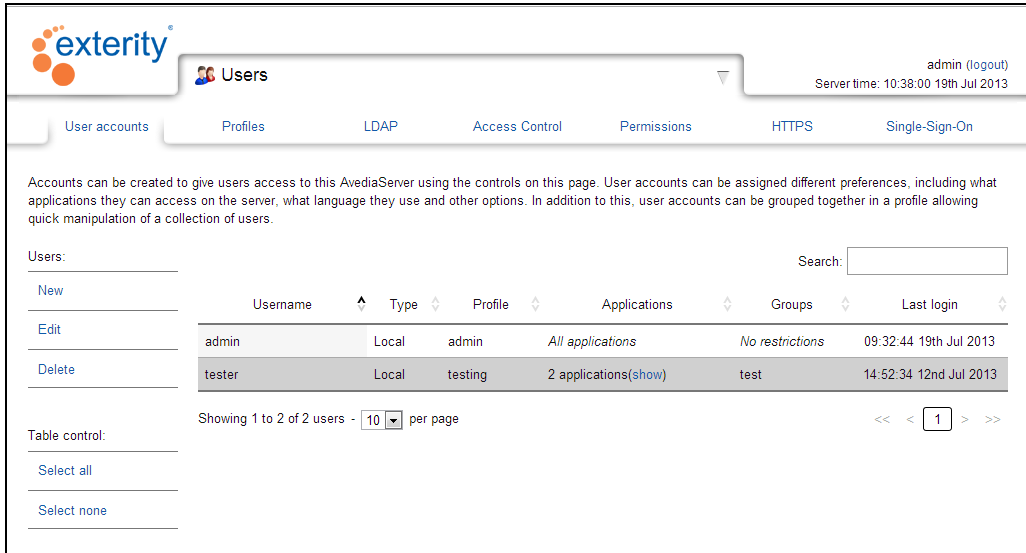
1 Start the Users application.

2 Click User accounts:

Figure 106 *Users – User Accounts Page*

3 Click the admin line in the table to highlight it and click Edit.
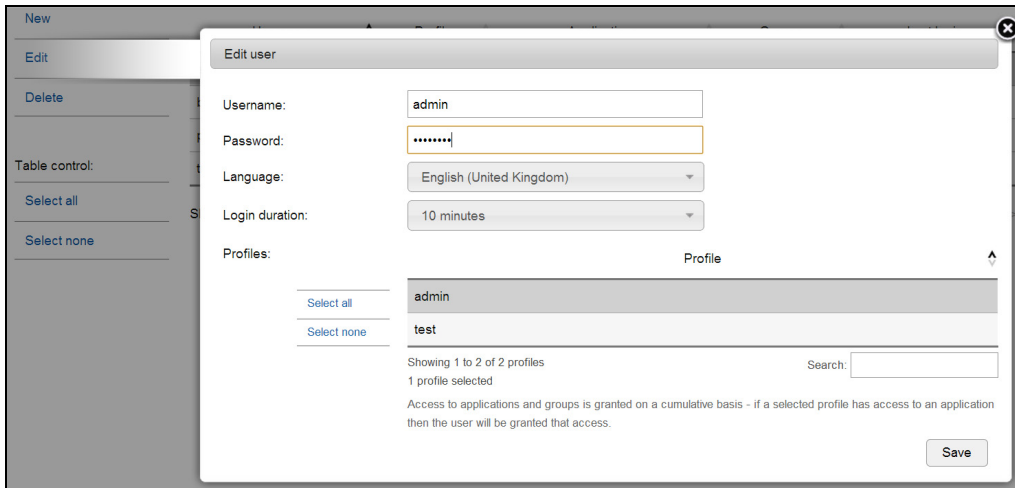

Figure 107 *Users – Changing the admin password*

4 Enter the new password in the Password entry field.

5 If required, select the preferred language from the drop-down list.

6 Select a different Login duration from the drop-down list if you want to change it from the default of 10 minutes. Extending the duration allows for a longer period of inactivity before being automatically logged out, up to a maximum of 1 month.

7 Click Save.

Managing Profiles

Each user must have an associated profile. If a profile is not assigned, the user account has no capability and access to the AvediaServer is blocked when log in is attempted. Each profile you create can enable any permutation of the 24 profile functions.

Start the Users application and select the Profiles tab:

Figure 108 *Users – Profiles page*

Each profile listed in the Profile column has the following attributes:

|	
Profile:	Name of the profile. Only the admin profile is available when first installed, but additional profiles can be created. The admin profile cannot be removed.
Applications:	Lists the number of applications enabled in the profile. All applications are available in the admin profile. Click (show) to view the applications enabled. Table 3 on page 5 provides a brief description of each available application.
Groups:	Shows the Exterity content group membership of the profile. Groups are used to filter content to control availability. No restrictions indicate the profile has not been assigned to a group and all content is available. All content is also available to the 'all' group. A profile can be a member of more than one group; click (show) to view more.
Used by:	
Users	Lists the number of users assigned to the profile
AD groups	Lists the names or number of the Active Directory Groups assigned to the profile

Creating, Editing, and Deleting Profiles

You can create as many profiles as you need to make the specific application and Exterity content Groups available to match each user, or user group requirements. Once created, any profile can be edited and/or deleted as required. The admin profile cannot be removed.

Note: When new applications are added following an AvediaServer upgrade, any profile previously configured with all applications enabled must have the new applications added manually.

To create or edit a profile:

1   Start the Users application.

2   Click the Profiles tab to display the current profiles list as shown in Figure 108.

3   Click New or click on the profile you want to change to select it, and click Edit.
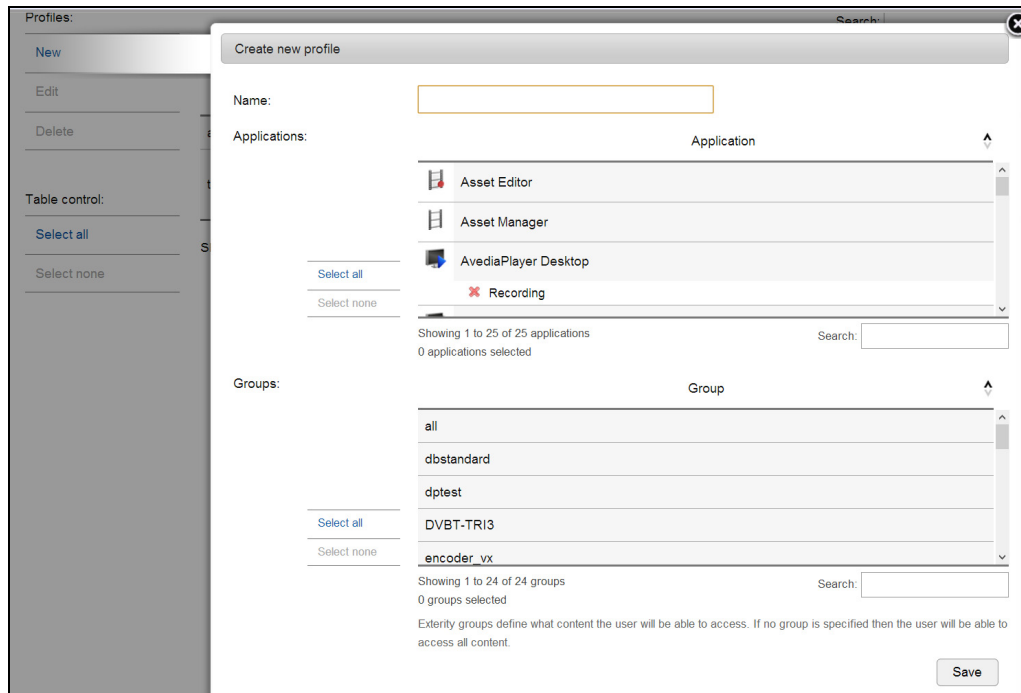
Figure 109   *Users – creating a new profile*

4   Enter or edit the name for the profile in the Name field.

5   Select the application(s) by selecting those required from the Application table. You can select as many as required. Use Select all or Select none as required.

Note: Some applications have additional options. When selected, the optional function is also enabled, as indicated by a green tick   . To disallow the optional function, click on the optional function to display a red cross   .

6   Add the channel Group(s) to the profile by selecting them from the Group table. Use Select all or Select none as required. (Channel Group 'all' enables all content.)

7   Save your changes, or click X in the top right corner to cancel.

Deleting a Profile

Any profile, except the admin profile, can be deleted unless one or more users are assigned to it. A user account has no capabilities without being assigned to a profile, therefore you cannot delete a profile without first deleting any user or user group account, or assigning it to a different profile. Refer to "Managing User Accounts" on page 99 for more information.

To delete a profile:

1   Start the Users application.

2   Click the Profiles tab to display the current profiles list as shown in Figure 108.

3   Click the profile to select it and click Delete.

If a user account is still assigned to the profile, the following message is displayed:
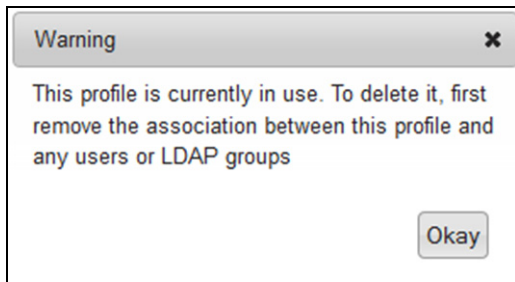
Figure 110 *User profile in use warning*

Profile Functions

The following section lists and briefly describes the applications listed on the profiles page. When an application is enabled as part of a named profile, the application is available to all assigned users. By selecting or deselecting individual applications you can enable the capabilities best suited to each user, or groups of users.

For more detailed information about each application refer to the relevant AvediaServer Administrator's Guide. The Applications and guides are listed in the Chapter 3, "AvediaServer Applications and Documentation".

Applications

The applications available depend on the licence configuration of the AvediaServer. All are detailed below:

- **Asset Manager** – Enables/disables access to the Asset Manager application. Any media or content imported into the AvediaServer is known as an asset. Assets can be offered as Video on Demand (VoD) content and are the building blocks of the Play application.

- **Asset Editor** – Enables/disables access to the Asset Editor application. Any AvediaServer content, or specified sections, can be downloaded. Editing tools also allow you to set the start and end points of a clip visually.

- **AvediaPlayer Desktop** – Enables/disables use of the AvediaPlayer Desktop client. The AvediaServer has AvediaPlayer Desktop application built-in. The AvediaPlayer Desktop application allows clients to view content, and if the user/profile combination is so configured, create recordings from the available channel content. Recording capability can be enabled/disabled.

- **AvediaPlayer Desktop Management** – Enables/disables ability to specify the login requirements for the AvediaPlayer Desktop client.

- **Channel Announcer** – Enables/disables access to the Channel Announcer application. The IPTV system uses SAP announcements to broadcast the availability of a channel. The Channel Announcer application allows you to configure streams from sources that cannot generate SAP announcements.

- **Channel Monitor** – Enables/disables access to the Channel Monitor application, allowing prompt and accurate monitoring of a channel status. The list of the channels on the network is built up by listening for SAP announcements from head-end equipment.

- **Director** – Enables/disables access to the AvediaServer Director application. The AvediaServer Director application is provided with all AvediaServer configurations and allows administrators, or users with administrator level access, to control and manage the IPTV system from anywhere on the network.

- **EPG Recording** – Enables/disables recording capability from the Guide displayed on an AvediaPlayer receiver Portal Client Interface when the receiver has been assigned to a device profile.

- **EPG Server** – Enables/disables access to the EPG Server application. The EPG Server listens for EPG information from a TVgateway or any other EPG source and makes that information available on the network for EPG display on connected devices. If no EPG source is available, an imported XML file can be used to provide the information.

- **Logger** – Enables/disables access to the Logger application. AvediaServer uses the Linux standard syslog to log information about the system. Logging permanently logs events.

- **Macro Builder** – Enables/disables access to the Macro Builder application. The Macro Builder application forms part of the triggered responses capability of the AvediaServer. The Macro Builder application allows you to specify an action, or sequence of actions, carried out in response to a triggering event.

- **Macro Triggers** – Enables/disables access to the Macro Triggers application. The Macro Builder application allows you to specify an action, or sequence of actions, carried out in response to a triggering event.

- **Messaging** – Enables/disables access to the Messaging application. The Messaging application allows you to push messages to all or a subset of AvediaPlayer receivers in the IPTV network which then display that message at the bottom of the Portal page for the specified period of time.

- **Play** – Enables/disables access to the Play application. The Play application allows you to construct channels from assets or playlists, scheduling the content in the order required, and multicast these onto the IPTV network.

- **PMS Link** – Enables/disables access to the Property Management System (PMS) Link application. The Property Management System Link application provides AvediaServer compatibility with two proprietary systems, Otrum Global and FIAS (Fidelio Interface Application Specification).

- **Portal Recording** – Enables/disables recording capability of the currently viewed channel when it has been selected using the Portal Client Interface.

- **Portal Config** – Enables/disables access to the Portal Config application. The Portal Config application is used to configure the Portal Client Interface. AvediaServer Portal provides a customised client interface targeted at Exterity Receivers providing the user with a simple but powerful interface to access live or recorded video and audio, and where enabled, create recordings. This interface is referred to as the Portal Client Interface.

- **Recorder** – Enables/disables access to the AvediaServer Recorder application. The AvediaServer Recorder application allows you to create scheduled or continuous recordings of any channel content available on the IPTV system.

- **SecureMedia Link** – Enables/disables access to the SecureMedia Link application. Exterity utilise the SecureMedia encryption scheme to offer encrypted content to users.

- **System** – Enables/disables access to the System application. The System application allows you to configure the basic settings such as IP address and time server/time zone of the AvediaServer, configure AvediaServer Services used by other AvediaServer applications, and provides maintenance functions such as reboot, factory default reset, upgrade, and AvediaPlayer Desktop licence management.

- **TFTP Server** – Enables/disables access to the TFTP Server application. The TFTP Server application enables the Director application actions such as device firmware upgrades and settings upload/download.

- **Transfer** –You can configure how a recording is managed on its completion including transfer to other AvediaServers.

- **Users** – Enables/disables user access to the Users application. The Users application allows the administrator to configure specific capabilities for users, or groups of users, who have access to the AvediaServer using the Web Management Interface.

- **Video on Demand** – Enables/disables access to the Video on Demand (VoD) application. The Video on Demand (VoD) application allows you to make content available for on demand viewing and specify the use of other AvediaServers to supply additional content or to provide additional load capacity for the same content.

- **Web Server** – Enables/disables the use of the AvediaServer Web Server application. The Web Server application allows you to host a simple webpage on the AvediaServer.

Managing User Accounts

There are two basic types of account, admin and user. You can create and delete user accounts as required. The core admin user account and profile cannot be modified or deleted. You can however, create a user account with the admin profile.

All other accounts are considered user accounts, even when all applications and functions are enabled. This allows you, the system administrator, to closely control the capabilities available to specific users. Refer to "Managing Active Directory User Group Accounts" on page 102 for more information about configuring user groups from Active Directory.

As profiles define the capabilities available to a user, an account without an assigned profile has no capability. By default, freshly created accounts or profiles have no enabled applications. Likewise, profiles are not automatically assigned to new individual or group user accounts. These must be manually configured. Create profiles for a specific user prior to creating the account. A user can be a member of more than one profile.

This section describes the following:

- Creating or Editing a User Account

- User Login

- Deleting a User Account

Figure 111 *Users – User accounts page*

Creating or Editing a User Account

To add/modify a user account:

1 Start the Users application and click the User accounts tab.

2 Click New or select a user account and click Edit:
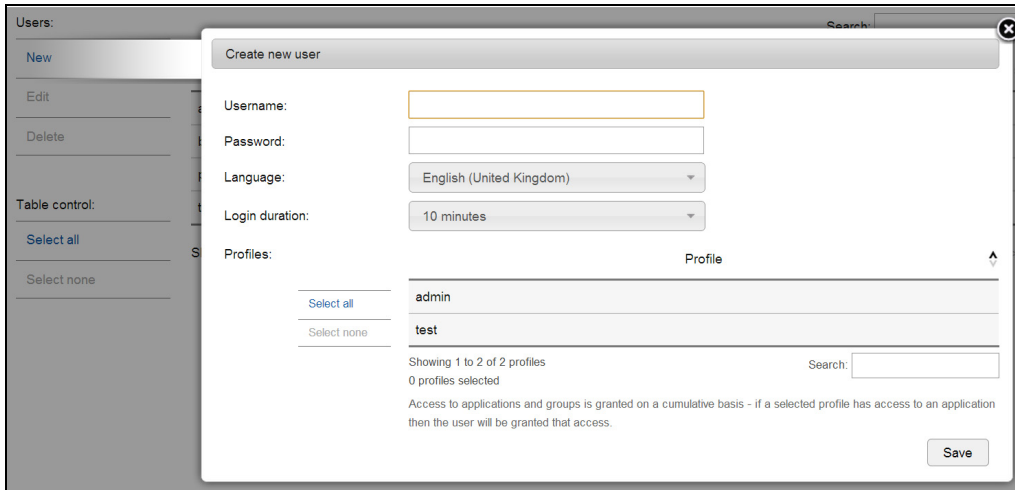
Figure 112 *Users – User account configuration*

3   Enter or revise the user name and password in the Username and Password fields.

4   If required, select the preferred language from the Language drop-down list.

5   Select a different login duration from the drop-down list if you want to change it from the default of 10 minutes. Extending the duration allows for a longer period of inactivity before being automatically logged out.

6   Select the required profile(s) from the Profile list. You can select more than one to build the capability you require for the account.

7   Click Save to save your changes.

User Login

The user can now log into the Avedia Server using the assigned user name and password:

Figure 113 *Logging in to the server*

Deleting a User Account

To delete a user account:

1   Start the Users application and click the User accounts tab.

2   Click to select the required user account and click Delete.

Configuring LDAP Access

If Active Directory has been implemented in the organisation, users and their passwords are already organised by functional groups. You can make use of this information and its structure using the LDAP (Lightweight Directory Access Protocol) feature.

With LDAP authentication configured and enabled, the Active Directory information is used to allow users access to AvediaServer applications using their own domain name and login. The applications are determined by the profile assigned to each Active Directory group, so users can access only the applications enabled by the assigned profile.

For example, in an education environment, teachers and students are likely to be in two distinct groups. By using the accessed data you can assign a play only profile to the student group, whilst allowing teachers more extensive capabilities with different, or combinations of profiles. Setting up an AvediaServer user account for every user is not required, only the Active Directory Group.
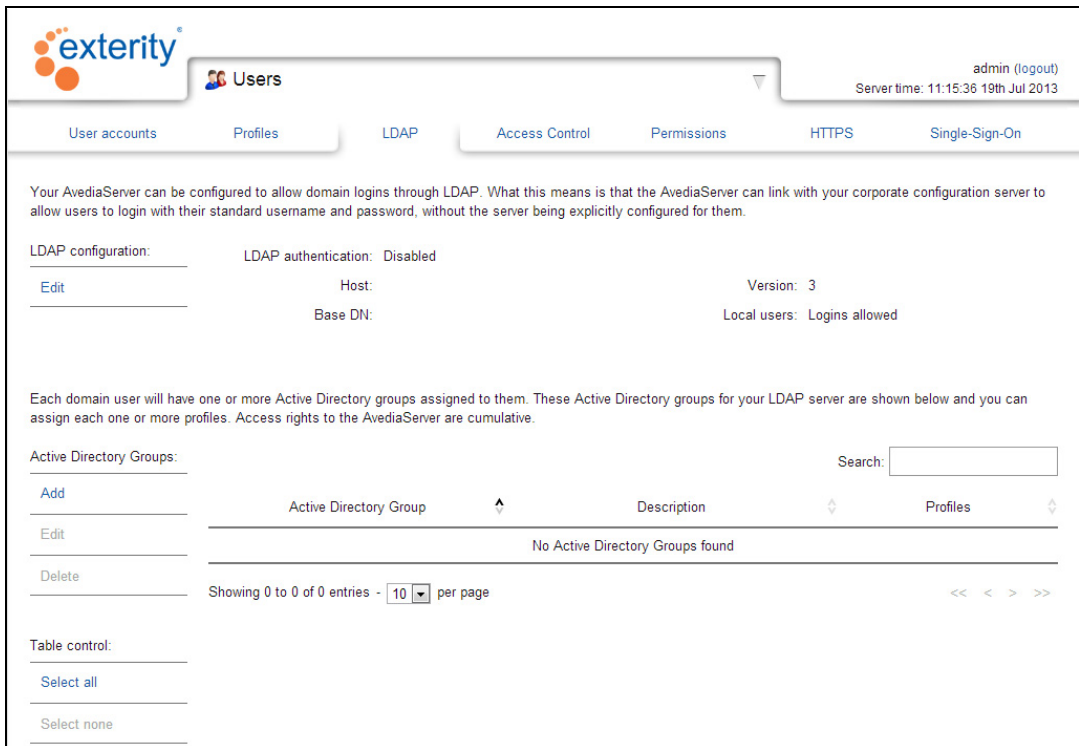
Figure 114   *Users – LDAP configuration page*

The following information is required for configuration:

•   The IP address of the Active Directory host.

•   The Base DN (Domain Name) of the directory entries. The Base DN is typically derived from the organisation name and domain name.

•   The version of LDAP in operation on the Host.

To configure LDAP access:

1   Start the Users application and click the LDAP tab.

2   Click Edit in the LDAP configuration section:

Figure 115 *Users – LDAP configuration*

Note: An LDAP login with administrator rights is required for the configuration for the server to obtain the full list of Active Directory Groups.

3   Click Enable for LDAP authentication.

4   Enter the IP address of the Active Directory host in the Host field.

5   Enter the Base Domain Name in the Base DN field.

6   Enter the LDAP version in use in the Version field (normally 3).

7   Click Allow access or Disallow access for Local users. Disallow access restricts login to 'admin' and configured Active Directory group members.

8   Enter your domain login in the Username field.

9   Enter your domain password in the Password field.

10 Click Save to apply the configuration and access your Active Directory.

11 Confirm the LDAP page displays the configured information.

Note: If unsuccessful, an error message is displayed.

Managing Active Directory User Group Accounts

Whilst names and members are defined by the Active Directory, configuring AvediaServer group accounts is similar to the process for individual user accounts. As profiles define user capability, any account without an assigned profile has no function. A user group can be a member of more than one profile.

Due to the limitations of Active Directory, not all AD groups are listed if the directory exceeds 1000 entries. With the help of an active directory browser you can use the Add AD Group function to identify and specify Active Directory groups not displayed in the main list.

This section describes the following:

•   Adding and Removing Active Directory User Groups

•   Configuring an AD Group User Account

Adding and Removing Active Directory User Groups

You can use the Add AD Group function if a required Active Directory user group is not listed. Due to paging limitations of the Active Directory system the AvediaServer can only display the first 1000 Active Directory Groups. Reducing the number of displayed groups through use of the search base and/or filter functions allows selection of the required Active Directory Groups.
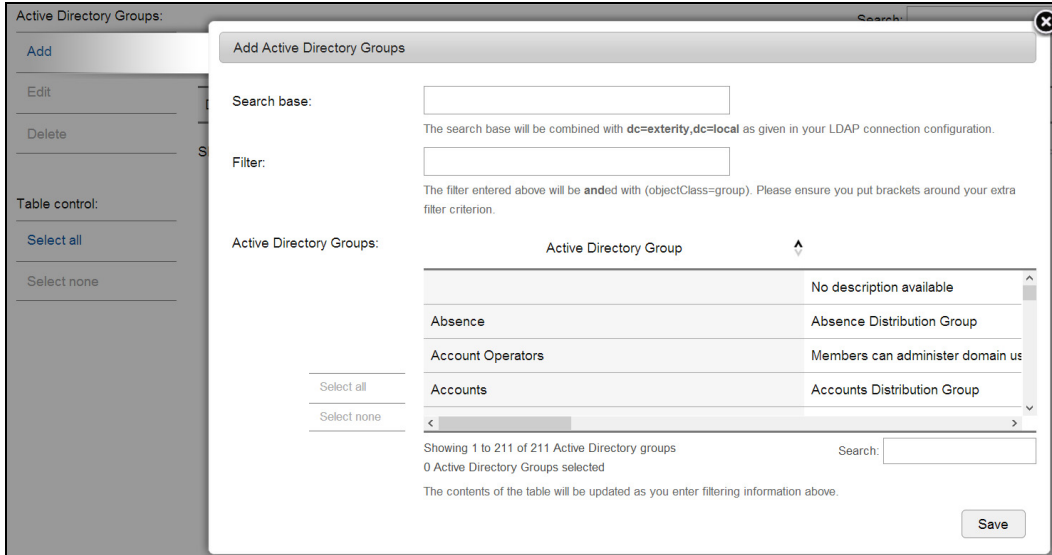
Note: An Active Directory browser may also be required to identify the required search parameters.

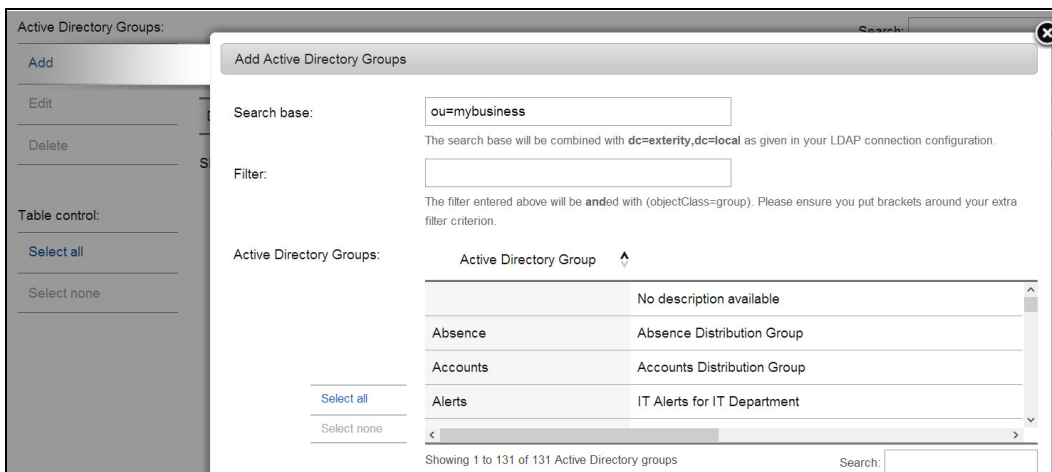To add an AD User Group to the AvediaServer List:

1   Start the Users application and click the LDAP tab.

2   Click Add in the AD Groups section:

Figure 116 *Users – LDAP add AD groups*

3   Enter the required Active Directory search criteria in the Search base field. For example:

- Search base: ou=mybusiness

- Filter: cn=AvediaServerLdapTest

Figure 117 *Users – search criteria*

Note: The search base is already configured with the Base DN specified during the access configuration.

4   Enter additional filtering information as required to help locate the AD Group.
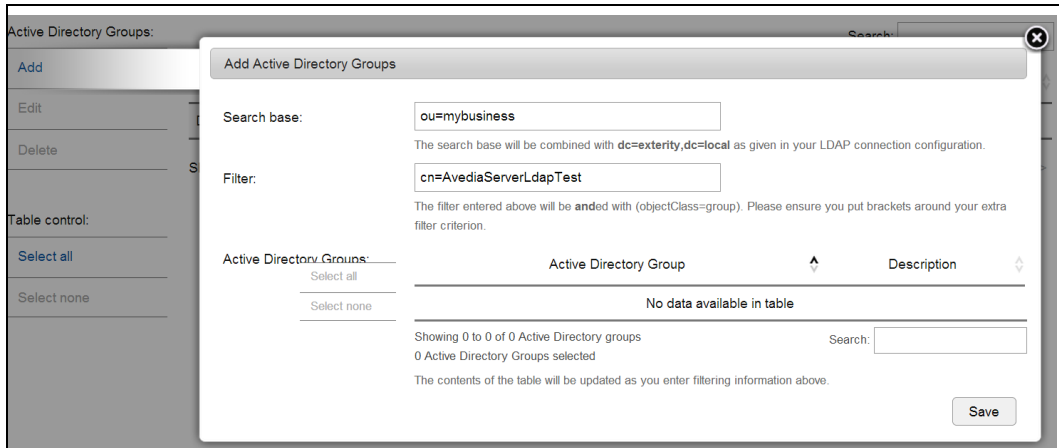
Figure 118 *Users – additional AD search information*

5   Click to select the group(s) you want to add and click Save to add the group(s) to the AD Groups list.

Note: Like all user accounts, the Active Directory Group must be assigned to a Profile to enable capability.
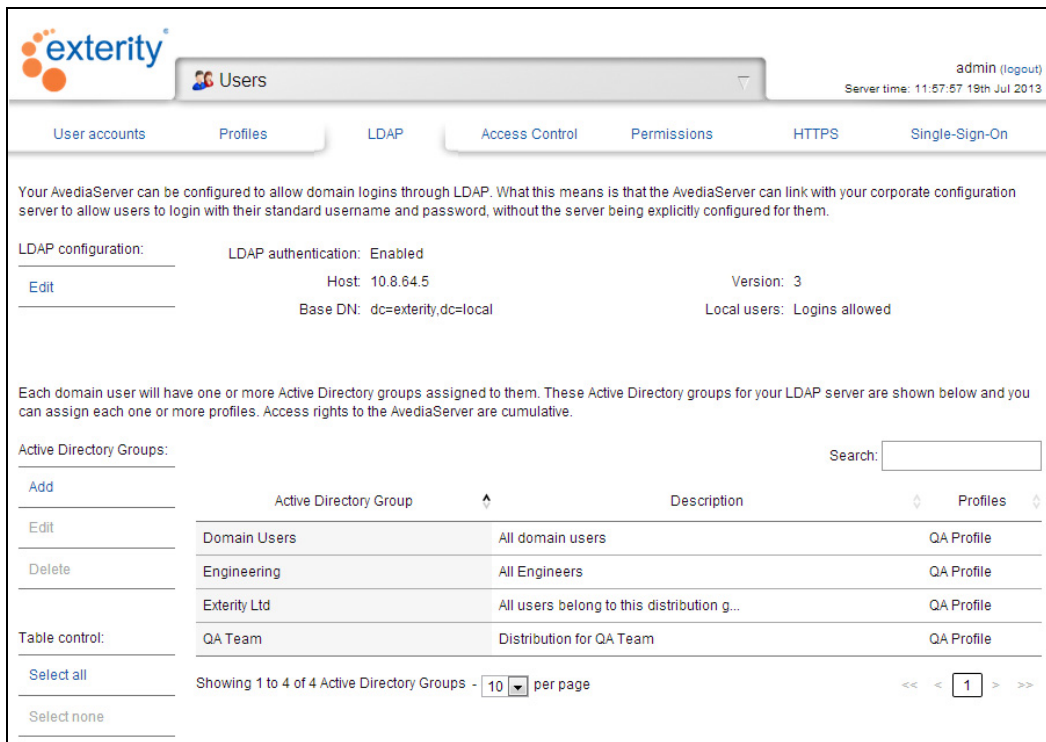

Figure 119 *Users – AD groups populated*

To remove an AD User Group from the AvediaServer List:

1   Start the Users application and click the LDAP tab.

2   In the AD Groups section, select the Active Directory Group(s) you want to delete.

3   Click Delete.

Note: The AD Group is deleted only from the AvediaServer list.

Configuring an AD Group User Account

After you have specified profiles and their associated applications, and selected the required Active Directory groups, you can assign each AD group to the appropriate profile.

To configure an AD Group account:

1   Start the Users application and click the LDAP tab. When the Active Directory access has been configured correctly, the AD Groups list is populated, similar to that shown in Figure 120.

2   Click the AD Group in the list you want to configure and click Edit:
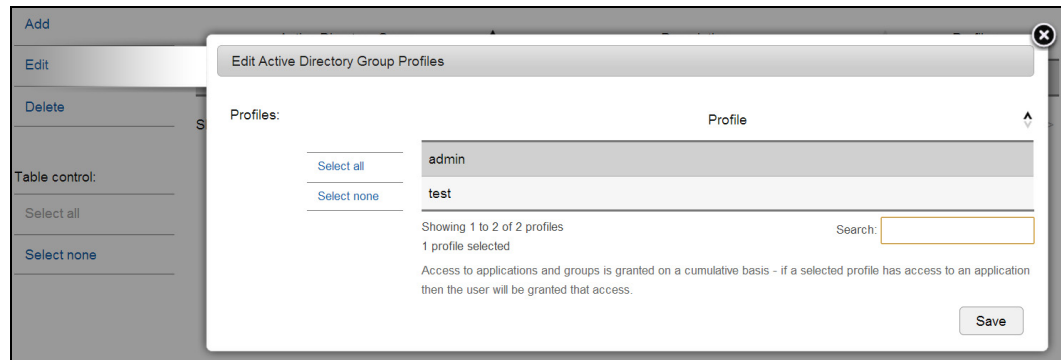
Figure 120   *Users – editing an AD group*

3   Select the profile(s) required for the AD group and click Save.

4   Confirm the AD Group displays the required profile(s) in the Profiles column.

Each user within the specific Active Directory Group now has access to the AvediaServer with capabilities and limitations determined by their assigned profile(s).

Managing AvediaServer Access Control

The Access Control page provides a method of specifying the AvediaServer functions available to all, or to specified devices only. The API (Application Programming Interface) documentation published for the AvediaServer shows how to access server functions using the defined command list.

You can manage access to functions globally in the Device Access table, or on an individual basis in the API access control list. Capabilities available to the device are managed using the user/profile combinations. Devices must be assigned to a username and associated profile as described in "Managing Profiles" on page 95 and "Managing User Accounts" on page 99.

You can globally manage access using the Device Access table. In the default setting, all discovered devices are allowed access and assigned to the admin user account and profile. This allows a user to initiate an instant recording by pressing Record on their AvediaPlayer receiver Remote Control handset or clicking the AvediaPlayer Desktop record button. Recording duration is specified by repeatedly pressing record to add 30 minute increments. (The AvediaServer portal IP address must be specified in the AvediaPlayer receiver home page field.)

To manage access for devices on an individual basis such as your computer or other access device, its IP address or MAC address must be registered in the API access control list. API commands sent from unregistered sources are ignored by the AvediaServer.
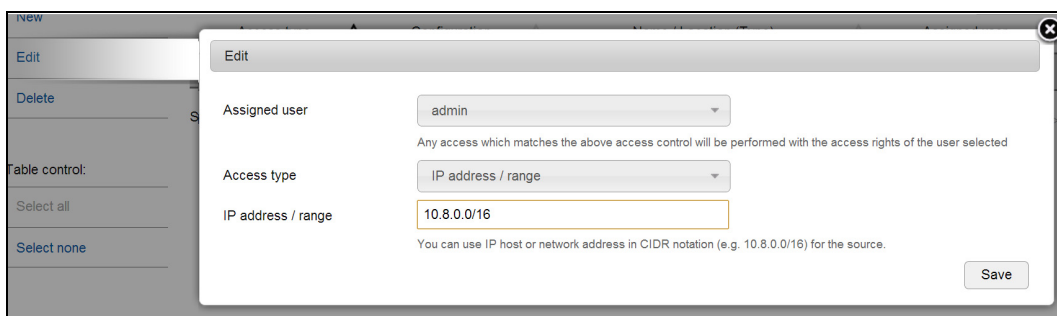
To manage access from discovered devices:

1   Start the Users application.

2   Click Access Control.

Figure 121   *Users – Access Control*

3   Select the entry you want to edit.

4   Click Edit in the API access control list.

Figure 122   *Users – editing access control*

5   To globally exclude all devices click No and click Save.

6   To assign all devices to a specific user account click Yes and select an account from the Assigned user drop-down list.

Note: You must create a user account and profile for the functions you want to make available. (Refer to "Managing Profiles" on page 95).

To configure an API access control list entry:

1   Start the Users application.

2   Click Profiles and create a profile for each user account you want to add and specify the required AvediaServer applications (refer to "Managing Profiles" on page 95).

3   Click User Accounts and create an account for each unique API user (refer to "Managing User Accounts" on page 99).

4   Click Access Control.

5   Click New to specify API access for an IP address or a device:
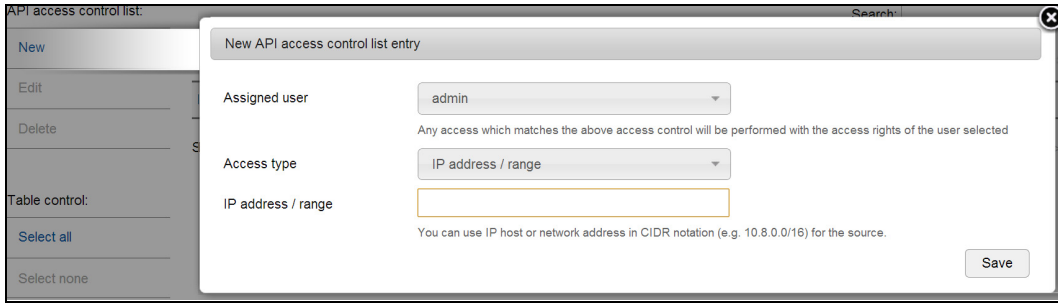
Figure 123 *Users – specifying API access*

You can add an entry based on an IP host or network address in CIDR notation (e.g. 10.8.0.0/16) for the source or select a device from those available.

To add a device:

1 Select a username you created in Step 3 above from the Assigned user drop-down list.

   a. Select Device from the Access type drop-down list.

   b. Click the device you want to add in the displayed list:
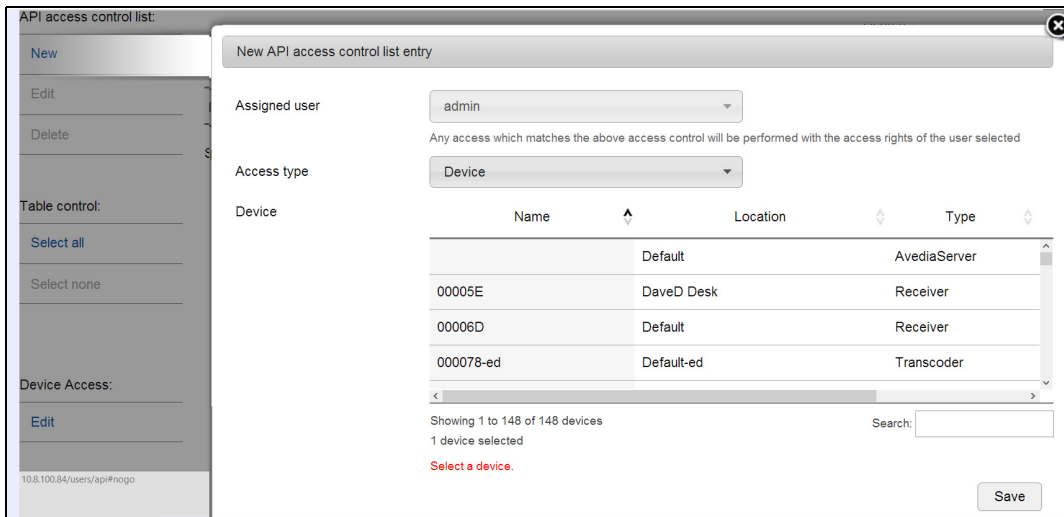
Figure 124 *Users – Adding a device*

   c. Click Save.

2 The device, its details and the Assigned user are displayed in the access control list.

To add an entry using IP addressing:

1 Select a username you created in Step 3 above from the Assigned user drop-down list.

   a. Select IP address / range from the Access type drop-down list.
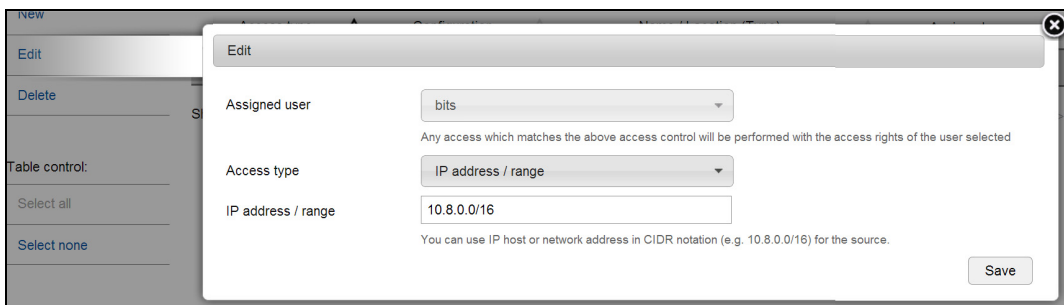
Figure 125 *Users – Adding an entry using IP addressing*

b. Enter the IP address (in CIDR notation) of the device in the IP address / range entry field.

c. Click Save.
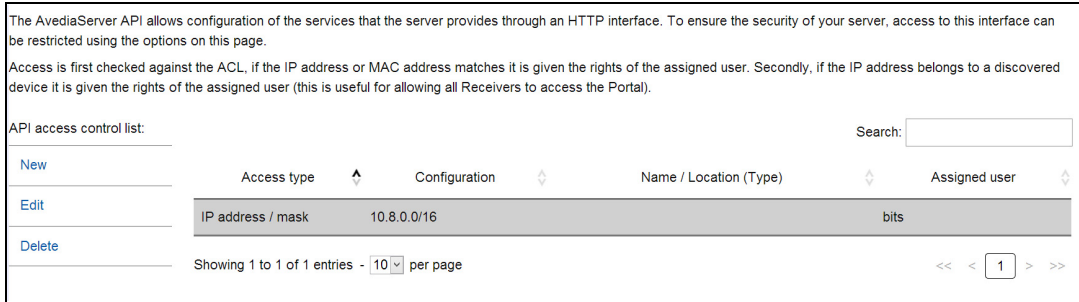
Figure 126 *Users – IP address and assigned user*

2   The IP address and the Assigned user are displayed in the access control list.

Specifying Default Content Sharing Permissions

You can specify the default permissions for content sharing between users. You can configure permissions to be applied when users share the same profile (Profile), and permissions to be applied when they have different profiles (Other). The default permissions for Profile and Other is write.

The selectable permissions allow the following capability:

*   None – no access to non-owned content.

*   Read – allows read-only access to non-owned content. Can play back, schedule or create a playlist but cannot edit or delete.

*   Write – allows content to be read, copied and deleted.

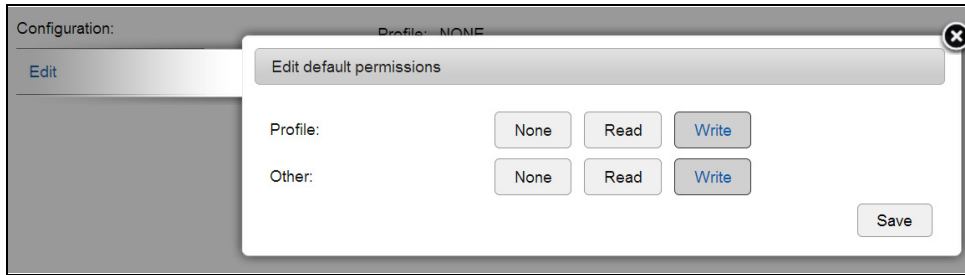**Note:** The content owner always has write permission.

To specify content sharing permissions:
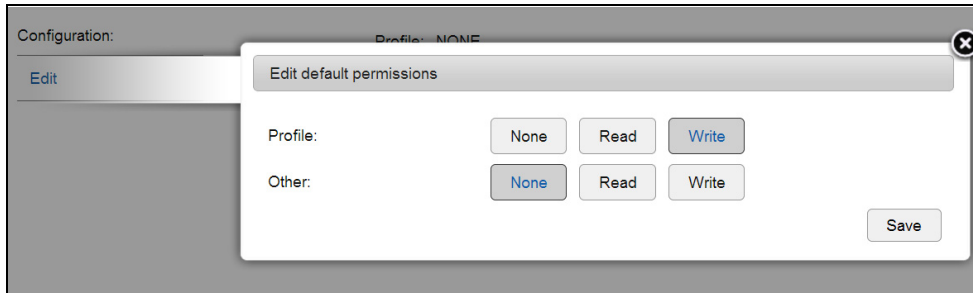
1   Start the Users application and click Permissions:
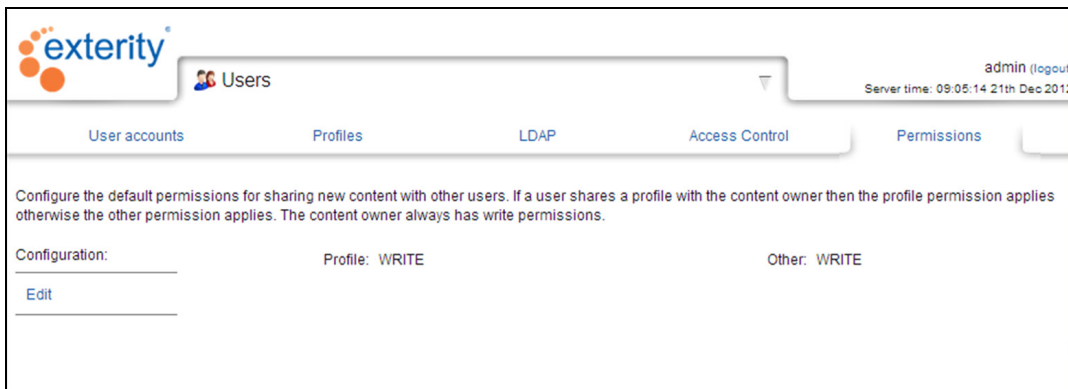
Figure 127 *Users – Content Sharing Permissions*

2   Click Edit.

3   Click None, Read or Write for the required permission for the shared profile.

Figure 128 *Users – Content Sharing Permissions*

4   Click None, Read or Write for the required permission when the profile is not shared.

Figure 129 *Users – Content Sharing Permissions*

In this example, users with a common profile can view content owned by each other, but users with different profiles cannot access each other's content.

5   Click Save to save your changes, or X to cancel.

Configuring for Secure Server Access

HTTPS access can be configured to provide secure communication between users and the AvediaServer. A valid SSL certificate matching the Domain Name of your AvediaServer must be uploaded. The Fully Qualified Domain Name (FQDN) is configured on the Network page of the AvediaServer System application. Refer to "Specifying a Fully Qualified Domain Name" on page 71 in Chapter 10, "Using the Users Application".

Only one certificate and private key pair may be uploaded at any one time. Uploading another pair replaces any already uploaded.

Before enabling secure operation you must configure an FQDN as described in "Specifying a Fully Qualified Domain Name" on page 71 and have a prepared SSL certificate available in a location such as the admin computer.
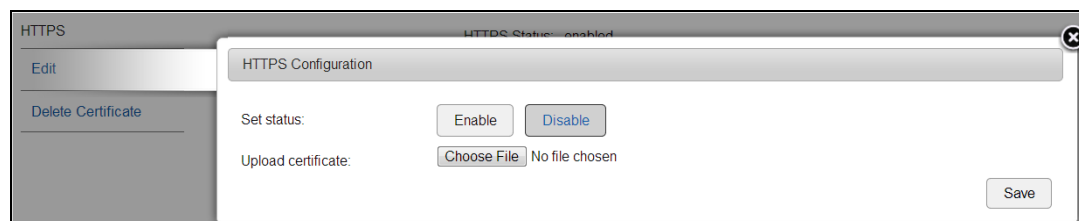
To enable secure access:
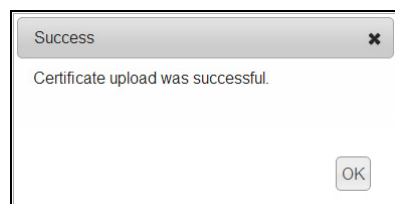
1   Start the Users application and click HTTPS.
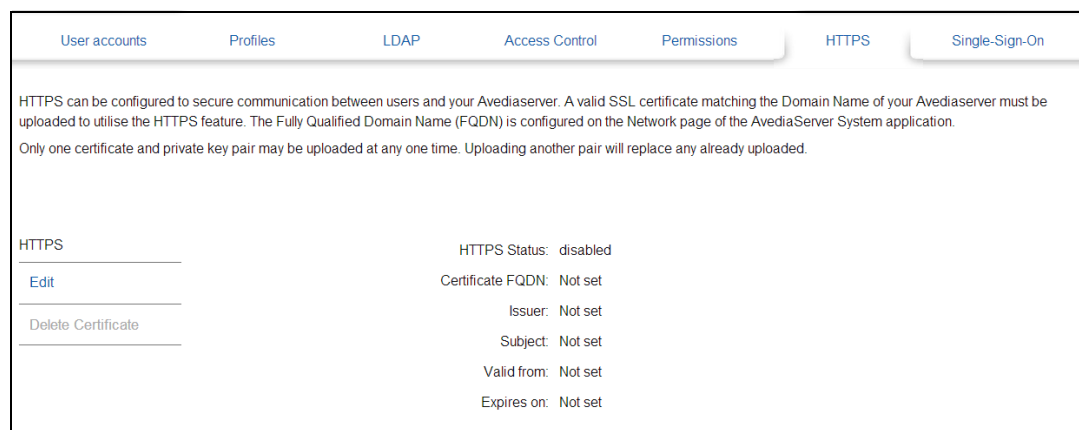
Figure 130 HTTPS disabled

2   In the HTTPS section click Edit.

Figure 131 Specifying the SSL Certificate

3   Click Choose File and locate the SSL Certificate file, of the form <abc123.pem>.

4   Click Save.

Figure 132 Certificate successfully uploaded

HTTPS

Edit

Delete Certificate

HTTPS Status: enabled
Certificate FQDN: avediaserver-cb1a.exterity.local
Issuer: Exterity Ltd
Subject: Exterity Ltd
Valid from: 2013-06-26 15:43:31
Expires on: 2014-06-26 15:43:31

© Exterity LTD 2009-2012 | System summary

Figure 133 *HTTPS access enabled*

5   When successfully configured, the HTTPS page is updated with the details of the FQDN and SSL Certificate.

6   With access enabled you can no longer log into the AvediaServer Web Interface using its IP address in your browser. To login, the browser must used the configured domain name. (For example, https://avediaserver-308e.domain.local)

Note: To load an SSL certificate file and enable HTTPS access simultaneously in the HTTPS Configuration window, choose the SSL Certificate file and click Enable before clicking Save.

Configuring for Single Sign-on Operation

The purpose of Single Sign-on (SSO) is to detect users who are logged onto their local domain and allow them automatic log in to the AvediaServer or AvediaPlayer Desktop, without additional user name and password entry. SSO applies only to the AvediaServer and AvediaPlayer Desktop interfaces. Accessing the interfaces of other devices such as an AvediaPlayer r9200 receiver requires login credentials. SSO is only supported by Windows operating systems.

Note: Single Sign-on requires familiarity with, and the configuration of several IP system tools. The procedures describe only the configuration of the AvediaServer Single Sign-on function.

Kerberos provides the required infrastructure to enable SSO. Refer to www.kerberos.org for more information. Additional user environment tools and configurations are required to enable this capability:

Note: AvediaServer SSO is only supported for Windows operating systems.

- The AvediaServer must have a Fully Qualified Domain Name (FQDN). Refer to "Specifying a Fully Qualified Domain Name" on page 71.

- Active Directory must be implemented in the organisation, with users and their passwords already organised by functional groups. Refer to "Managing Active Directory User Group Accounts" on page 102 for more information.

- The AvediaServer must be part of the Active Directory Domain.

- The AvediaServer must be a user in the Active Directory Domain.

- Kerberos must be enabled in the browsers used to access the AvediaServer and AvediaPlayer Desktop.

- A Keytab file must declare the AvediaServer as a service and map the domain account to the http service on the AvediaServer. The file is uploaded by the AvediaServer during the configuration process. Refer to Windows Server Support Tools for more information.

Caution: When Single Sign-on is enabled, the AvediaServer Web Interface is no longer accessible using the user name/password login screen. Without admin level access, SSO cannot be disabled. You must ensure an Active Directory user, or user group is configured in the enterprise Active Directory and is configured with an administrator level profile in the AvediaServer Users application. Refer to the previous sections in this chapter which describe the configuration of user accounts, specifying capabilities in a profile, and integration with Active Directory groups.

To load the keytab file:
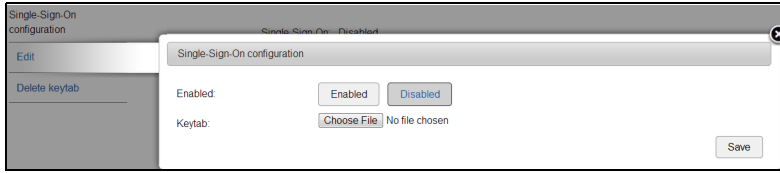
1 Start the Users application and click Single Sign-on.

Figure 134   Single Sign-on Page

2   Click Edit.

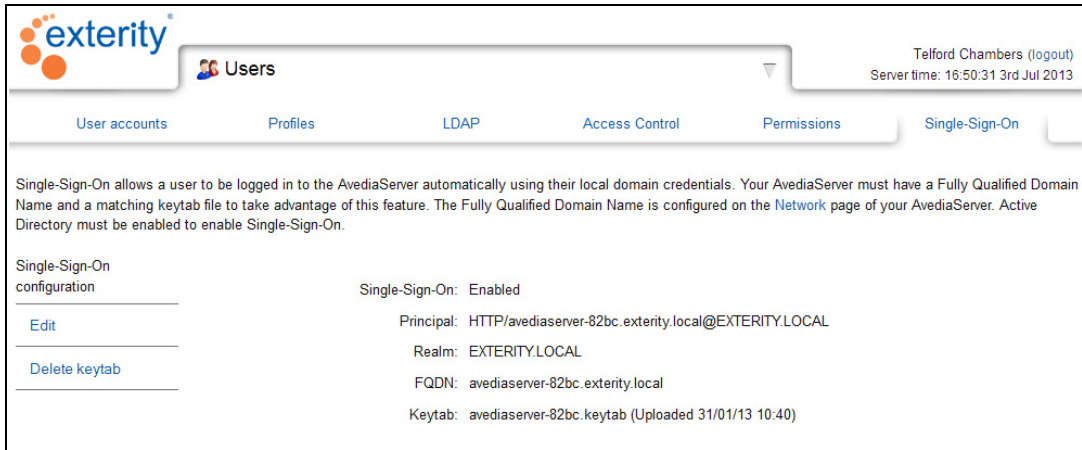3   Click Choose File and select the Keytab file.

Figure 135   *Selecting the Keytab file*

4   Click Save.

To enable single sign-on:

1   Start the Users application and click Single Sign-on.

2   Ensure a Keytab file has been uploaded as described above.

3   Click Edit, then Enabled.

4   Click Save.

Figure 136   *Single Sign-on enabled*

5   Confirm the Single Sign-on status is Enabled.

A   Support and Contact Information

Technical Support for Exterity products is provided by authorised Systems Integrators and Resellers. Please contact your Systems Integrator or Reseller with any support issues.