



## **HELIX MOBILE SESSION MANAGER USER'S GUIDE**

Revision Date: August 14, 2009

RealNetworks, Inc.  
PO Box 91123  
Seattle, WA 98111-9223s  
U.S.A.

<http://www.real.com>  
<http://www.realnexus.com>

©2009 RealNetworks, Inc. All rights reserved.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of RealNetworks, Inc.

Printed in the United States of America.

Helix, the Helix Logo, Real, the Real "bubble" (logo), RealJukebox, RealOne, Real-rTV, RealArcade, RealAudio, RealDownload, RealNetworks, RealPix, RealPlayer, RealPresenter, RealProducer, RealProducer Plus, RealPoducer Pro, RealProxy, RealPublisher, RealSites, RealSystem, RealText, RealVideo, Rhapsody, ra/ve, SureStream, The Future is Real, TurboPlay, and Xing are trademarks or registered trademarks of RealNetworks, Inc.

Other product and corporate names may be trademarks or registered trademarks of their respective companies.

# CONTENTS

INTRODUCTION	1
Conventions Used in This Book	1
1 HELIX MOBILE SESSION MANAGER INSTALLATION	3
Installing and Configuring Helix Mobile Session Manager	3
Installing the Plug-in	3
Installing the License	4
Configuring the Plug-in	4
Setting Basic Helix Mobile Session Manager Parameters	5
Enabling Helix Mobile Session Manager	5
URL Parameter Keywords	5
2 EVENTS AND ACTIONS	7
Session Events	7
Event Types	8
SessionStart Event	8
Play Event	9
Pause Event	9
Resume Event	9
SessionStop Event	9
GeneralError Event	10
Actions	10
Actions List	10
Action Names	11
Action Types	11
ExternalAuth Action	12
ExternalAuthServer Variable	12
ConnectionTimeout Variable	13
ResponseTimeout Variable	13
DefaultAction Variable	13
Log Action	14
Allow Action	14
Deny Action	14
External Authorization Servers	15

3	EXTERNAL MESSAGING	17
	External Authorization Requests.....	17
	Client IP .....	17
	Url .....	18
	Log.....	18
	HTTP Response.....	18
	Action .....	18
	Message .....	19
	Client Session Management.....	19
	Session Management Configuration .....	19
	Realm.....	19
	Port.....	20
	Username .....	20
	Password.....	20
	AuthenticationType.....	20
	HTTP Request to Modify a Client Session .....	21
	sessionmanagement .....	21
	clientids.....	21
	HTTP Response.....	21
	Media Player Disconnect Behavior.....	22
4	AUTHORIZATION LOGS	23
	Logging Configuration.....	23
	AuthLogging .....	23
	AuthLogFileName .....	24
	LogRollSize .....	24
	TemplateFormat .....	24
	Reason for Termination .....	24
	LogServerStart.....	25
	IntervalLogging .....	25
	IdleLogging.....	26
	Authorization Logs .....	26
	Log Type.....	26
	SERVERSTART .....	27
	SESSIONSTART .....	27
	PLAY .....	27
	PAUSE.....	27
	RESUME.....	27
	SESSIONSTOP.....	28
	INTERVALLOG .....	28
	Logging Time .....	28
	URL.....	28

Response Code .....	29
Client IP Address .....	29
Client Identification .....	29
Streaming Times.....	29
Play and Pause Times .....	29
Allowance Codes.....	30
External Authorization Codes.....	30
Template Output .....	31
Termination Codes.....	31
A ENCODED URLS .....	33
Unreserved URL Characters.....	33
Reserved URL Characters .....	34



# INTRODUCTION

This document explains how to configure and use the Helix Mobile Session Manager component of Helix Mobile Server.

## Conventions Used in This Book

The following table explains the typographic conventions used in this book.

Notational Conventions	
Convention	Meaning
<b>emphasis</b>	Bold text is used for in-line headings, user-interface elements, URLs, and e-mail addresses.
<i>terminology</i>	Italic text is used for technical terms being introduced in a given manual or other document, and to lend emphasis to generic English words or phrases.
syntax	This font is used for file names, directory names, code examples (excerpted or in whole), or command-line instructions.
<b>syntax emphasis</b>	Bold syntax character formatting is used for program names and to emphasize specific syntax elements.
<i>variables</i>	Italic text denotes variables. Substitute values appropriate for your system.
[ ]	Square brackets indicate optional values. As a rule, when you use these optional values, you do not include the brackets themselves.
choice 1 choice 2	Vertical pipes separate values you can choose between.
...	Ellipses indicate nonessential information omitted from examples.
“ ”	Curly (“smart”) quotation marks are used for direct quotations, to call out words or phrases that are being used to mean something other than what they mean in everyday English, and to enclose chapter titles and section headings in cross-references.



## HELIX MOBILE SESSION MANAGER INSTALLATION

For Helix Mobile Server, Helix Mobile Session Manager validates access to media clips and broadcasts. This chapter explains how to install and configure Helix Mobile Session Manager on each Helix Mobile Server.

### Installing and Configuring Helix Mobile Session Manager

The following sections explain how to install, verify, and configure Helix Mobile Session Manager.

#### Installing the Plug-in

Follow the next procedure to install Helix Mobile Session Manager.

► **To install Helix Mobile Session Manager:**

1. Unpack the archive provided by RealNetworks.
2. Into a convenient directory on the Helix Mobile Server machine, copy Helix Mobile Session Manager:

Helix Mobile Server on Windows:      `sessmgr.dll`

Helix Mobile Server on Linux or UNIX: `sessmgr.so`

3. Move the Helix Mobile Session Manager library to the Plugins directory of Helix Mobile Server.
4. For Linux or UNIX, grant execute permission to the Helix Mobile Session Manager library. For example:  
`chmod 755 sessmgr.so`

## Installing the License

Helix Mobile Session Manager requires a license file available from RealNetworks. Using Helix Mobile Session Manager with an existing server installation may require that you install an updated license file for Helix Mobile Server.

Once you receive the necessary license file or files, copy them to the License subdirectory under the Helix Mobile Server installation directory. If a license is a replacement file, remove the older version of the file. Then restart Helix Mobile Server.

**For More Information:** Check with your RealNetworks representative for information about licensing requirements.

**Warning!** Do not make any changes to a license file. Doing so disables the product.

## Configuring the Plug-in

The following procedure explains how to configure Helix Mobile Session Manager.

1. Navigate to the Helix Mobile Server installation directory.
2. Back up the configuration file for Helix Mobile Server (`rmserver.cfg`), and then open it in a text editor.
3. To the end of the configuration file, add a DAUCPlugin list:

```
<!-- DAUC Plugin -->  
<List Name="DAUCPlugin">  
  ...Helix Mobile Session Manager lists and variables...  
</List>
```
4. In the DAUCPlugin list, configure the variables as described in the following sections:
  - “Setting Basic Helix Mobile Session Manager Parameters” on page 5 explains how to enable the Helix Mobile Session Manager plug-in and set basic features.
  - Chapter 2 beginning on page 7 explains how to configure Helix Mobile Session Manager to take certain actions when specific events occur, such as a streaming session starting.

- “Session Management Configuration” on page 19 explains how to configure the Helix Mobile Session Manager plug-in to accept the session management directives described in Chapter 3.
  - “Logging Configuration” on page 23 explains how to set the variables that control the output logging information.
5. Save the configuration file.
  6. Restart Helix Mobile Server to put the the new settings into effect.

## Setting Basic Helix Mobile Session Manager Parameters

The following sections describe the basic configuration parameters for Helix Mobile Session Manager. Most parameter are standalone variables that you add to the DAUCPlugin list of the Helix Mobile Server configuration file. Some features require the addition of sublists, however. The following provides an example of the basic Helix Mobile Session Manager parameters:

```
<List Name="DAUCPlugin">
  <Var Enabled="1"/>
  <List Name="URLKeywords">
    ...URL keywords defined...
  </List>
  ...additional elements...
</List>
```

### Enabling Helix Mobile Session Manager

To enable Helix Mobile Session Manager to authorize URL requests, set the Enabled variable to the value 1. If you set this attribute to 0 (zero), the Helix Mobile Session Manager plug-in passes through all requests without validating them.

### URL Parameter Keywords

The URLKeywords list configures the keywords that you add to URLs to cause Helix Mobile Session Manager to take certain actions when allowing the session. The LogIntervalKeyword affects Helix Mobile Session Manager operation:

```
<List Name="DAUCPlugin">  
  ...other Helix Mobile Session Manager variables...  
  <List Name="URLKeywords">  
    <Var LogIntervalKeyword="li"/>  
  </List>  
</List>
```

**For More Information:** See “IntervalLogging” on page 25 for an explanation how you use the log interval keyword in a URL.

## EVENTS AND ACTIONS

This chapter explains how to configure Helix Mobile Session Manager to take specific actions when specific session events occur. For example, the Helix Mobile Session Manager plug-in may first notify an external server when a client requests a streaming session.

**For More Information:** You define events within the DAUCPlugin list of the Helix Mobile Server configuration file. For details, refer to “Configuring the Plug-in” on page 4.

## Session Events

The Events list within the DAUCPlugin list configures the various types of events that may occur during any RTSP streaming session, such as the session set-up, a pause in streaming, and ending the session. Each type of event is defined once within the configuration file, as shown in the following example:

```
<List Name="DAUCPlugin">  
  ...general plug-in configuration elements...  
  <List Name="Events">  
    <List Name="SessionStart">  
      ...actions to perform when the session is set up...  
    </List>  
    <List Name="Play">  
      ...actions to perform when a session begins to stream...  
    </List>  
    <List Name="Pause">  
      ...actions to perform on a session pause...  
    </List>  
    <List Name="Resume">  
      ...actions to perform on a resume from a pause or seek...  
    </List>  
    <List Name="SessionStop">  
      ...actions to perform when a session stops...  
    </List>
```

```

<List Name="GeneralError">
    ...actions to perform when a general error occurs...
</List>
</List>
...log configuration elements...
</List>

```

## Event Types

The following sections explain the types of events that Helix Mobile Session Manager can monitor.

### SessionStart Event

A SessionStart event occurs when a media player connects to Helix Mobile Server to request a streaming session. For clients that do not already have an SDP file, the event typically occurs during the RTSP DESCRIBE transaction. For clients that have an SDP file, the event typically occurs during the RTSP SETUP phase. Any required validation of the URL occurs at this time.

The SessionStart event can include a Blocking variable set to 0 (no blocking, the default) or 1 (blocking). If blocking is enabled, the stream does not start until the actions defined for the SessionStart event have been carried out:

```

<List Name="SessionStart">
    <Var Blocking="1"/>
    <List Name="Actions">
        ...defined actions...
    </List>
</List>

```

The primary purpose for blocking is to delay the stream until an external server authorizes the session (see “ExternalAuth Action” on page 12). The following table summarizes what happens during an external authorization when blocking is enabled, and when blocking it is disabled.

**SessionStart Activity with Blocking and External Authorization**

Blocking Mode	Upon the Initial Client Request	If Session is Allowed by External Server	If Session is Denied by External Server
Enabled (Blocking="1")	Stream does not play.	Stream begins to play.	No playback begun. User disconnected.
Disabled (Blocking="0")	Stream begins to play.	No change. Stream continues to play.	Stream stops playback. User disconnected.

**Note:** A Blocking variable added to the configuration syntax for an event type other than SessionStart is ignored.

### Play Event

A play event occurs when the RTSP PLAY is issued. Monitoring this event is useful if you need to keep accurate measurements for server-side play and pause times.

### Pause Event

This event occurs when the media client issues an RTSP PAUSE request, and Helix Mobile Server pauses the session stream.

**Tip:** When a user seeks through a media timeline, the action is treated as a pause and a resume, in which the stream is resumed at a different point in the media timeline.

### Resume Event

This event occurs when the media client issues an RTSP PLAY request to resume a paused session.

**Tip:** Defining Log actions for Pause and Resume events is useful for determining pause times in a prepaid scenario. If you log each play and resume event, you can determine from the log records how long the user paused the stream.

**For More Information:** See “Log Action” on page 14 and “Play and Pause Times” on page 29.

### SessionStop Event

The SessionStop event is triggered when the session terminates. The session may end for a number of reasons. The SessionStop event does not differentiate between these types of session ending events:

- The media client issued a RTSP TEARDOWN message.
- Helix Mobile Server terminated the stream for any reason, such as a session management command to end the stream. (See Chapter 3.)
- The media client is unresponsive and Helix Mobile Server ended the stream after the RTSP timeout expired.

## GeneralError Event

Helix Mobile Session Manager issues a general error when a significant problem occurs during a session. Conditions that may cause a general error event include the following:

- Necessary session parameters are missing or corrupted.
- Helix Mobile Session Manager configuration contains syntax errors.
- The server is out of memory.
- The external authorization server returned an error code outside of the HTTP 200 error range.
- The server could not initiate or maintain the stream.
- The Helix Mobile Session Manager plug-in could not communicate with the server.

**Note:** If an attempt to contact an external authorization server fails because of a timeout, the timeout is recorded in the log file in the external authorization codes (see “External Authorization Codes” on page 30). This situation is **not** recorded as a general error.

**Tip:** The RTSP session may continue after a general error event. If the error stops the session, Helix Mobile Session Manager generally triggers a SessionStop event. That may not occur, however, depending on the type and severity of the error.

## Actions

When a defined event occurs, one or more actions can take place. For example, on a SessionStart event, Helix Mobile Session Manager may contact an external server to verify the access. Based on the server's response, it may then allow or deny the access.

### Actions List

For each event type, an Actions list defines which actions occur. Each action is configured within a sublist of the Actions list, as shown in the following abstract example:

```

<List Name="DAUCPlugin">
  <List Name="Events">
    <List Name="SessionStart">
      <Var Blocking="1"/>
      <List Name="Actions">
        <List Name="Action_1">
          ...first action to perform on this event...
        </List>
        <List Name="Action_2">
          ...second action to perform on this event...
        </List>
        ...additional actions to perform...
      </List>
    </List>
  </List>
</List>

```

## Action Names

Action names, such as Action\_1, are user-definable. Within a single Actions list, the actions must have unique names, such as Action\_1, Action\_2, and so on. The action names do not have to be unique across event types. For example, the SessionStart event and the Pause event can both have Action\_1 and Action\_2 elements within their respective Actions lists.

Helix Mobile Session Manager carries out actions in sequence, based on the alphanumeric order of the action names. For instance, Action\_1 is performed before Action\_2, even if Action\_1 is configured after Action\_2 in the Actions list. Note that names are sorted on a character-by-character basis. This means that Action\_10 would occur before Action\_2.

## Action Types

Within each action element, variables define the type of action, along with any configuration information required to carry out the action:

```

<List Name="Action_1">
  <Var Type="action_type"/>
  ...additional action variables...
</List>

```

The action type can be one of the following:

- ExternalAuth – Contact an external server (see page 12).

- Allow – Allow the event (see page 14).
- Deny – Deny the event (see page 14).
- Log – Write a log file entry (see page 14).

## ExternalAuth Action

The ExternalAuth action posts the event information to an HTTP server. The server's reply instructs Helix Mobile Session Manager on further actions to take. The ExternalAuth action can occur more than once for each event. For example, on a SessionStart event, Helix Mobile Session Manager may contact two external servers, one to validate the request, and one to update a customer service database.

The configuration syntax for the ExternalAuth action indicates which server to contact, specifies a default action to take if no response is received, and sets the appropriate server timeouts:

```
<List Name="Action_1">
  <Var Type="ExternalAuth"/>
  <Var ExternalAuthServer="EventTracker01"/>
  <Var ConnectionTimeout="30"/>
  <Var ResponseTimeout="15"/>
  <List Name="DefaultAction">
    <Var Name="Deny|Allow"/>
    <Var Message="message on Deny action"/>
  </List>
</List>
```

**For More Information:** The section “External Authorization Requests” on page 17 explains the syntax of the HTTP POST that Helix Mobile Session Manager sends to the external authorization server, as well as the syntax of possible responses.

## ExternalAuthServer Variable

The ExternalAuthServer variable provides a user-defined name of the authorization server to contact. This name must match a server name in the configuration file's ExternalAuthServers list, which defines the server's address, HTTP port, and so on.

**For More Information:** See “External Authorization Servers” on page 15.

## ConnectionTimeout Variable

The ConnectionTimeout variable sets the number of seconds that Helix Mobile Session Manager waits to establish a connection to the external server. If Helix Mobile Session Manager cannot open a socket, it applies the default action that is configured for the event. The default value for ConnectionTimeout is 30 seconds.

**For More Information:** Connection timeouts are recorded in the log file. See “External Authorization Codes” on page 30.

## ResponseTimeout Variable

The ResponseTimeout variable sets the number of seconds that Helix Mobile Session Manager waits for the external server to respond after the connection has been established. If there is no response after this time elapses, Helix Mobile Session Manager carries out the default action configured for the event. The default value for ResponseTimeout is 15 seconds.

**For More Information:** Response timeouts are recorded in the log file. See “External Authorization Codes” on page 30.

## DefaultAction Variable

The DefaultAction list determines the action to take if the external server does not respond. For example, if a validation server does not respond before the ResponseTimeout expires, Helix Mobile Session Manager may deny the access and respond to the user with a message:

```
<List Name="DefaultAction">
  <Var Name="Deny"/>
  <Var Message="We are sorry. This clip cannot be streamed."/>
</List>
```

**For More Information:** See the sections “Allow Action” on page 14 and “Deny Action” on page 14 for more information about possible default actions.

## Log Action

The Log action generates a log entry that records the event. It can occur at any time as Helix Mobile Session Manager carries out actions for an event. If the Log action is not included, the event is not logged. The Log action requires no additional variables:

```
<List Name="Action_3">  
  <Var Type="Log"/>  
</List>
```

**For More Information:** See Chapter 4 for information about enabling logging and reading the log file format.

## Allow Action

The Allow action allows the event to occur. It is typically defined as the DefaultAction of a complex action, such as ExternalAuth. It requires no additional variables:

```
<List Name="DefaultAction">  
  <Var Type="Allow"/>  
</List>
```

## Deny Action

The Deny action denies the request. It can include a Message value up to 4096 bytes long. This text is returned to the media client as an RTSP SET\_PARAMETER message:

```
<List Name="DefaultAction">  
  <Var Type="Deny"/>  
  <Var Message="message"/>  
</List>
```

**Note:** After a Deny action, the only remaining action that can occur for the event is a Log action. Any other defined actions that follow the Deny action are ignored.

## External Authorization Servers

The variables that define the connection information for external authorization servers occur within the ExternalAuthServers list of the DAUCPlugin list:

```
<List Name="DAUCPlugin">
  ...general plug-in configuration elements...
  <List Name="Events">
    ...events and actions...
  </List>
  <List Name="ExternalAuthServers">
    <List Name="server_1">
      ...first set of external authorization server configuration variables...
    </List>
    <List Name="server_2">
      ...second set of external authorization server configuration variables...
    </List>
    ...additional authorization servers...
  </List>
  ...log configuration elements...
</List>
```

Separate sublists configure each authorization server's address and port. An external authorization action refers to the server by the list name. For example:

```
<List Name="ExternalAuthServers">
  <List Name="EventTracker01">
    <Var Server="authorization.example.com"/>
    <Var Port="8080"/>
    <Var Path="/media/authorization.pl"/>
  </List>
  ...
</List>
```

The following table describes the variables used to configure each external authorization server.

**External Authorization Server Variables**

Attribute	Value	Description
Server	IP Address   DNS Name	Address of the external authorization server to contact. If Helix Mobile Session Manager must go through a proxy, set the Server value to the proxy server address. Do <b>not</b> include a protocol value such as http://.
Port	0-65535	The HTTP port of the host server or proxy. The default is 80.
URL	path	The path needed to execute the appropriate logic for obtaining the authorization action. This information is appended to the host and port information.

## EXTERNAL MESSAGING

This chapter describes how Helix Mobile Session Manager contacts external authorization servers to receive instructions about handling a session event. It also explains how to configure Helix Mobile Session Manager to receive HTTP directives to terminate a stream.

### External Authorization Requests

When Helix Mobile Session Manager requests authorization for an event from an external server, it passes information to the server in an HTTP POST. The POST message provides information about the client and the requested URL using a series of name and value pairs. Each name and value combination is written to a new line, as shown in the following example:

*...POST header information...*

```
ClientIP=IP_address  
Url=URL  
Log=log_record
```

**Note:** Reserved characters within the *IP\_Address*, *URL* and *log\_record* values are URL-encoded as noted in Appendix A.

#### Client IP

Helix Mobile Session Manager extracts the ClientIP value from the IP packets or the RTSP headers. Because this may be, in some cases, the address for a proxy or NAT firewall, the ClientIP value is not a reliable means for the external authorization server to validate the client.

**Tip:** RealNetworks recommends that the external server identify clients through URL parameters present in the log record.

**For More Information:** For information about logging, refer to Chapter 4.

### Url

The URL value is the URL requested by the media player without the protocol designation (typically `rtsp://`), the server address, or any port value. Query string parameters appended to the URL are included, however.

### Log

The Log value is a log entry for the event. The external authorization server can use this log to identify the user, either through the IP address or from query string parameters in the request URL.

**Note:** This log record is not written to Helix Mobile Session Manager log file. If a Log action is defined for the event (see “Log Action” on page 14), Helix Mobile Session Manager writes a new log record to the file *after* the external authorization server responds with an Allow or Deny action.

**For More Information:** Chapter 4 explains the field values in a log record.

## HTTP Response

The external authorization server instructs Helix Mobile Session Manager to allow or deny the request by returning a valid HTTP POST response. This message includes one or more name and value pairs in the message body:

*...POST header information...*

```
Action=Default|Allow|Deny  
Message=message
```

### Action

The Action value can be one of the following:

Default	Perform the default action configured for Helix Mobile Session Manager.
Allow	Allow the action.
Deny	Disallow the action.

## Message

The Message name and value pair are required only if Action=Deny. The message, which can be up to 4096 bytes in any character set, provides the reason for the denial. It is passed to the client as an RTSP SET\_PARAMETER message and logged in the extauth message field of the log file (see “External Authorization Codes” on page 30).

Reserved characters within the *message* value must be URL-encoded as noted in Appendix A. For example:

```
Message=Prepaid%20credit%20expired.%20Please%20check%20account.
```

## Client Session Management

Using an HTTP POST, an external server may contact Helix Mobile Session Manager to terminate a session immediately. The POST message must identify the clients by including the appropriate client\_ID values extracted from log entries.

### Session Management Configuration

Helix Mobile Session Manager must be configured to accept session management directives from external servers. The SessionManagement list within the DAUCPlugin list defines the configuration elements:

```
<List Name="DAUCPlugin">
  ...additional configuration elements...
  <List Name="SessionManagement">
    <Var Realm="server.realm"/>
    <Var Port="port"/>
    <Var Username="name"/>
    <Var Password="password"/>
    <Var AuthenticationType="basic|digest"/>
  </List>
  ...additional configuration elements...
</List>
```

### Realm

The Realm specifies the Helix Mobile Server security realm in which a user name and password for session management are defined. A security realm is typically the server name and realm name separated by a period. This convention may vary, however.

**Note:** A valid realm must be specified even if basic authentication is used.

**For More Information:** For information about defining a user name and password, refer to the authentication chapter of *Helix Mobile Server Administration Guide*.

## Port

The Port value sets the port that Helix Mobile Session Manager uses to listen for session management directives. Do **not** use the Helix Mobile Server HTTP port (typically port 80). Helix Mobile Session Manager does not bind to the socket on Helix Mobile Server start-up. Rather, it binds to the port upon receiving the first media request.

**Tip:** If you have a multi-homed Helix Mobile Server machine that accepts media requests on only one IP address, for example, Helix Mobile Session Manager claims the HTTP port only for that address.

## Username

The Username value indicates the user name defined in the authentication realm for use with session management. Names are case-sensitive.

## Password

The Password value provides the password for the user name defined in the authentication realm for session management. Passwords are case-sensitive.

## AuthenticationType

The AuthenticationType variable specifies either basic or digest. The digest value is recommended because it provides encryption for the log-in credentials. Using basic security transmits log-in credentials as clear text, which is recommended only if the server does not support digest.

**Tip:** Session Management requests can be proxied through an SSL-enabled VIP or proxy that communicates to the unsecure network over HTTPS, then proxies those requests to Helix Mobile Server over HTTP.

**For More Information:** For background on basic and digest authentication, see <http://www.faqs.org/rfcs/rfc2617.html>.

## HTTP Request to Modify a Client Session

To disconnect one or more clients, the external server sends an HTTP POST request that includes a comma-separated list of the client IDs within an XML structure. For example:

*...POST header information...*

```
<sessionmanagement version="1">
  <clientids>ID_1,ID_2,ID_3</clientids>
</sessionmanagement>
```

**Note:** On a valid disconnect request, Helix Mobile Server terminates the stream immediately by sending the media client an RTSP BYE message. It does not wait for an RTSP TEARDOWN message from the client.

### sessionmanagement

The required sessionmanagement element defines the root-level of the XML structure. The version parameter is required. Only version 1 of the session management protocol is currently supported.

### clientids

The required clientids element provides the comma-separated list of client IDs. The element value can be up to 8000 bytes, which is approximately 100 client IDs.

**For More Information:** For information about the client\_ID value, refer to “Client Identification” on page 29.

## HTTP Response

In response to an HTTP directive from an external server, Helix Mobile Session Manager returns an HTTP response. This response contains an XML-formatted list of the actions taken with the client. For example:

```
<response>
  <clientid="ID_1" result="1"/>
  <clientid="ID_2" result="0"/>
  ...
</response>
```

A result code of 1 indicates that the action was successful. The result code 0 means failure, which can occur if the specified client ID did not exist (the user

disconnected before the action could take place, for example), or Helix Mobile Session Manager could not carry out the action because of an error.

## **Media Player Disconnect Behavior**

When you disconnect a session in which the stream uses the RealNetworks RDT packet format, the server notifies RealPlayer that the stream is no longer available. RealPlayer immediately stops playing the stream and logs session statistics. It does not provide any indication to the user, however, that the session was disconnected.

The RTP format does not provide RTP-based media players with notification that the stream has terminated. Therefore, RTP-based media players go into a communication or rebuffering state when the session stops. They may log statistics differently:

- Some media players receiving RTP packets, such as RealPlayer and PacketVideo Player, time out after approximately 20 seconds and log session statistics.
- Other RTP-based media players, such as Motorola players, do not time out a terminated session. Instead, they log statistics only after the viewer shuts down the player or requests another stream. This may result in statistics not being written to the log for a considerable time after the session ends.

## AUTHORIZATION LOGS

This chapter explains how to configure the logging parameters for Helix Mobile Session Manager. It also explains the structure of the log data.

### Logging Configuration

The LogOutput list of the DAUCPlugin list configures Helix Mobile Session Manager logging parameters:

```
<List Name="DAUCPlugin">  
  ...additional configuration elements...  
  <List Name="LogOutput">  
    <Var AuthLogging="0|1"/>  
    <Var AuthLogFileName="path/file_name"/>  
    <Var LogRollSize="MB"/>  
    <Var TemplateFormat="format"/>  
    <Var LogServerStart="0|1"/>  
    <Var IntervalLogging="0|1"/>  
    <Var IdleLogging="0|1"/>  
  </List>  
</List>
```

**For More Information:** See “Configuring the Plug-in” on page 4 for information about editing the Helix Mobile Session Manager configuration.

### AuthLogging

The AuthLogging parameter turns logging on or off for Helix Mobile Session Manager. The default value is 1, which enables logging. Set this parameter to 0 to disable logging entirely.

**Note:** To generate logs for a certain type of media session event, you must configure a Log action for that event. For more information, see “Log Action” on page 14.

## AuthLogFileName

The AuthLogFileName parameter sets the path and base file name of the log files created by Helix Mobile Session Manager. The log is a text file typically stored in the Logs subdirectory beneath the Helix Mobile Server installation directory. You can specify an absolute path, or a relative path from the directory used to start Helix Mobile Server. The following example sets a relative path from the Helix Mobile Server main installation directory:

```
<Var AuthLogFileName="Logs/dauc.log"/>
```

Each log file automatically receives a timestamp of the file creation time in the format YYYYMMDDHHMMSS. For example, a log created on January 24, 2008, at 4:56.13 P.M. looks like this:

```
dauc.log.20080124165613
```

## LogRollSize

The LogRollSize parameter sets the maximum size of the Helix Mobile Session Manager log file in Megabytes (MB). Helix Mobile Server creates a new log file once the current file reaches this size.

## TemplateFormat

The TemplateFormat variable allows you to customize the authorization log with client session information stored in the Helix Mobile Server registry. You can add any number of server registry variables to the template format.

**For More Information:** Refer to the chapter on advanced logging in *Helix Mobile Server Administration Guide*, as well as the chapter on client properties in *Helix Mobile Server Configuration and Registry Reference*.

### Reason for Termination

As an example of using the TemplateFormat variable, you can set a value of %Client.\*.ReasonForTermination% to record why the server terminated the stream:

```
<Var TemplateFormat="%Client.*.ReasonForTermination%"/>
```

**For More Information:** The section “Termination Codes” on page 31 explains the meaning of the possible termination values.

## LogServerStart

Set to its default value of 1, the LogServerStart parameter causes Helix Mobile Session Manager to generate a log entry on the first media player access following a Helix Mobile Server restart. The default value of 0 turns off the logging of server start-up events.

**For More Information:** See “Authorization Logs” on page 26.

## IntervalLogging

A value of 1 for the IntervalLogging parameter enables Helix Mobile Session Manager to write multiple log records at regular intervals for certain streaming sessions. These interval logs are written, however, only if the request URL includes a log interval query string parameter that sets the logging frequency.

The log interval parameter value is in seconds, with 10 as the minimum and 60 as the recommended value. A value of 60, for example, causes Helix Mobile Session Manager to write a new authorization log entry every minute. This value is passed to Helix Mobile Session Manager through the request URL. This enables different sessions to have different logging intervals as needed:

```
rtsp://helixserver.example.com/video.rm?li=60
```

**Tip:** Interval logs are useful for determining a user’s remaining time in a prepaid billing situation. The log entry indicates how long the viewer has played the stream. Once the viewer’s prepaid time expires, the system can disconnect the user as described in “Client Session Management” on page 19.

**For More Information:** The log interval parameter (li in the preceding example) is user-definable. See “URL Parameter Keywords” on page 5.

## IdleLogging

The IdleLogging variable is used only with interval logging. If set to the default value of 0, IdleLogging suspends the interval logs during periods in which the media player is assumed not to be playing the media, such as during a viewer-initiated pause. If this variable is set to a value of 1, interval logging continues during idle playback times.

**For More Information:** For information about how authorization logs report idle time, refer to “Play and Pause Times” on page 29.

## Authorization Logs

The following syntax illustrates the fields included in each log entry generated by Helix Mobile Session Manager. Each entry is written to a single line in the log file:

```
log_type [log_time] URL response_code IP_address client_ID [client_start]
client_duration play_time pause_time [allowance_code allowance_message]
[extauth_code extauth_message] [template_output]
```

The following is a side-by-side comparison of these field names with an actual log entry:

log_type	PAUSE
[log_time]	[20/Nov/2008:22:13:02 -0800]
URL	kane.3gp
response_code	1
IP_address	192.168.128.129
client_ID	15
[client_start]	[20/Nov/2008:22:12:56 -0800]
client_duration	6
play_time	6
pause_time	0
[allowance_code allowance_message]	[0 No Error]
[extauth_code extauth_message]	[2 Allowed response]
[template_output]	[0]

## Log Type

The log\_type entry indicates the type of authorization log. The following log types are supported.

**SERVERSTART**

Server has restarted and all previous streaming sessions have been closed. In this log entry, most logging fields other than the current time field record the value 0 or UNKNOWN. For example:

```
SERVERSTART [20/Nov/2008:22:12:56 -0800] UNKNOWN 2 UNKNOWN -1
[UNKNOWN -0800] 0 0 0 [0 No Error] [0 No Error] []
```

**Note:** This log entry is written on the first media client access attempt following the server restart.

**For More Information:** For Helix Mobile Session Manager to write this type of log entry, the LogServerStart variable must be enabled. See “LogServerStart” on page 25.

**SESSIONSTART**

New streaming session initiated. For example:

```
SESSIONSTART [20/Nov/2008:22:12:56 -0800] kane.3gp 1 192.168.128.129 15
[20/Nov/2008:22:12:56 -0800] 0 0 0 [0 No Error] [2 Allowed response] [0]
```

**PLAY**

Server has begun to send the stream. For example:

```
PLAY [20/Nov/2008:22:12:56 -0800] kane.3gp 1 192.168.128.129 15
[20/Nov/2008:22:12:56 -0800] 0 0 0 [0 No Error] [2 Allowed response] [0]
```

**PAUSE**

Streaming session paused. For example:

```
PAUSE [20/Nov/2008:22:13:02 -0800] kane.3gp 1 192.168.128.129 15
[20/Nov/2008:22:12:56 -0800] 6 6 0 [0 No Error] [2 Allowed response] [0]
```

**For More Information:** The section “Play and Pause Times” on page 29 explains how Helix Mobile Session Manager logs the amount of time that a user has viewed a clip.

**RESUME**

Streaming session resumed from a pause. For example:

```
RESUME [20/Nov/2008:22:13:19 -0800] kane.3gp 1 192.168.128.129 15
[20/Nov/2008:22:12:56 -0800] 23 6 17 [0 No Error] [2 Allowed response] [0]
```

## SESSIONSTOP

Streaming session ended. For example:

```
SESSIONSTOP [20/Nov/2008:22:13:54 -0800] kane.3gp 1 192.168.128.129 15  
[20/Nov/2008:22:12:56 -0800] 58 41 17 [0 No Error] [2 Allowed response] [0]
```

## INTERVALLOG

An interval log. For example:

```
INTERVALLOG [20/Nov/2008:22:18:19 -0800] kane.3gp?li=60 1 192.168.128.129 18  
[20/Nov/2008:22:18:19 -0800] 60 0 0 [0 No Error] [2 Allowed response] [0]
```

Note the following about interval logs:

- Interval logging must be enabled for each Helix Mobile Session Manager through the IntervalLogging parameter, which is described in the section “IntervalLogging” on page 25.
- A logging interval parameter (for example, li=60) is passed in the URL query string to set the frequency of the interval logs. If the parameter is not included, no interval logging occurs.

## Logging Time

The [log\_time] field indicates the time at which Helix Mobile Session Manager logged the entry according to the server clock. For a server start-up log, the logging time is the time the server received the first media player request following a server restart.

The logging time entry uses the following format, in which TZ is the server's time zone offset from Coordinated Universal Time (Greenwich Time):

```
[dd/Mmm/yyyy:hh:mm:ss TZ]
```

For example:

```
[31/Oct/2008:13:44:32 -0800]
```

## URL

The URL field lists the URL in its encoded format. It includes the URL path, file name, and any query string parameters. The request protocol (typically rtsp://), server address, and port number are omitted.

## Response Code

The `response_code` field lists the action that Helix Mobile Session Manager took in response to the URL request:

- 0 request not validated
- 1 request allowed
- 2 request rejected
- 3 interval log (allowance already granted)

## Client IP Address

The `client_IP` field records the IP address of the media player making the request. This address is gathered from the source address field of the request IP packets. The IP address may therefore belong to a proxy or a NAT firewall, rather than a specific media client.

## Client Identification

The `client_ID` field records the unique integer assigned to each client connection by Helix Mobile Server. The numbers start with 1 and increment by 1 for each new connection. After a server restart, the `clientID` values restart again at 1.

**Tip:** You specify these client IDs to disconnect specific sessions. See “Client Session Management” on page 19.

## Streaming Times

The `[client_start]` field records the time according to the server clock that streaming began. The format is the same as the `[log_time]` field:

`[dd/Mmm/yyyy:hh:mm:ss TZ]`

The `client_duration` field records an integer that indicates the total number of seconds that the client has been connected to the stream since the `[client_start]` time began. For a streamed clip or broadcast, this value includes any time that the viewer paused the stream.

## Play and Pause Times

The `play_time` value is an integer that indicates the total number of seconds that the media player has played the clip. The `pause_time` value is an integer

that records the number of seconds that the media player has paused the stream. Together, the `play_time` and `pause_time` values equal the `client_duration` time.

**Note:** Time spent rebuffering a stream is recorded in the `play_time` value. Excessive stream rebuffering may therefore result in recorded play times that are larger than actual.

## Allowance Codes

The `allowance_code` and `allowance_message` fields record one of the codes and messages described in the following table.

**Allowance Codes and Messages**

Code	Default Message	Meaning
0	Session Not Ended Yet	Session streaming normally.
3	Internal Error	Helix Mobile Session Manager experienced an error processing the request. The plug-in may not have received certain necessary values from the server or may be out of memory.
7	Disconnected	Client was disconnected using the session management methods described in Chapter 3.

## External Authorization Codes

The `extauth_code` and `extauth_message` fields record a code and message describing the action that occurred if Helix Mobile Session Manager forwarded the URL to an external authorization server. Codes 100 and higher indicate errors in operation.

**External Authorization Codes and Messages**

Code	Message	Meaning
1	<i>default response</i>	External authorization server responded with its default action.
2	<i>allow response</i>	External authorization server responded with an Allow action.
3	<i>deny response</i>	External authorization server responded with a Deny action.

(Table Page 1 of 2)

**External Authorization Codes and Messages (continued)**

Code	Message	Meaning
101	Connection failed	Connection to the external authorization server was rejected, possibly due to an incorrect IP address or port, or misconfiguration of the external authorization server.
102	Connection timed out	Not able to connect to the external authorization server before the connection timeout period elapsed. This time is set by the ConnectionTimeout parameter, as described in the section “ConnectionTimeout Variable” on page 13.
103	Internal Error	An error occurred when processing data during an external authorization request.
104	Cannot read from server	Connection to the external authorization server succeeded, but Helix Mobile Session Manager could not read from the socket.
105	Extauth server timed out	External authorization server did not respond before the configured timeout was reached. This maximum response time is set by the ResponseTimeout parameter on streaming servers, as described in the section “ResponseTimeout Variable” on page 13.
300-599	<i>dynamic message</i>	External authorization server returned a non-200 HTTP response, indicating an error in the connection attempt. In this case, Helix Mobile Session Manager takes the default action for the user.

(Table Page 2 of 2)

**Template Output**

The [template\_output] field records the template output defined by the TemplateFormat variable of the Helix Mobile Session Manager configuration. Typically, this field reports a termination code as described in the section “Termination Codes” on page 31.

**For More Information:** The section “TemplateFormat” on page 24 explains the TemplateFormat variable.

**Termination Codes**

A code of 0 in termination logs (log\_type value of 2) indicates that the client disconnected the session. A non-zero termination code means that the session

manager terminated the stream. This termination code results from adding the error codes listed in the table “Allowance Codes and Messages” on page 30 to the reauthorization codes listed in the table “External Authorization Codes and Messages” on page 30.

To ensure that each possible combination of the error code and reallocation code produces a unique result, the allowance code value is multiplied by 65536. Therefore, the formula for generating the termination code is the following:

$$\text{Termination Code} = [\text{Allowance Code} * 65536] + \text{Reallowance Code}$$

The following table lists the termination codes, showing which combination of error code and reallocation code each termination code represents.

**Termination Codes**

Termination Code	Default Error Message	Code	Reallowance Message	Code
0	Session Not Yet Ended	0	n/a	0
196608	Internal Error	3	n/a (reallocation not available)	0
196609	Internal Error	3	<i>default response</i>	1
196610	Internal Error	3	<i>allow response</i>	2
196611	Internal Error	3	<i>deny response</i>	3
196709	Internal Error	3	Connection failed	101
196710	Internal Error	3	Connection timed out	102
196711	Internal Error	3	Internal Error	103
196712	Internal Error	3	Cannot read from server	104
196713	Internal Error	3	Extauth server timed out	105
196908-197207	Internal Error	3	<i>dynamic message</i>	300 - 599
458752	Disconnected	7	n/a (reallocation not available)	0

## ENCODED URLS

This appendix explains the reserved and unreserved characters that can be passed in a URI.

**For More Information:** See  
<http://www.faqs.org/rfcs/rfc2396.html>.

## Unreserved URL Characters

The following table lists the unreserved characters you can pass to URL Processor.

**Unreserved Characters**

Description	Character
apostrophe	'
asterisk	*
exclamation point	!
hyphen	-
left parenthesis	(
lowercase letters	a-z
numerals	0-9
period	.
right parenthesis	)
tilde	~
underscore	_
uppercase letters	A-Z

## Reserved URL Characters

The following table lists the reserved characters used only as delimiters, typically for query string parameters. You can pass one of these characters as text by using its hex-encoded value.

Description	Character	Hexadecimal Value
“at” sign	@	%40
ampersand	&	%26
colon	:	%3A
comma	,	%2C
dollar sign	\$	%24
equals sign	=	%3D
forward slash	/	%2F
plus sign	+	%2B
question mark	?	%3F
semicolon	;	%3B
space		%20