



---

## **Release Notes:**

**Helix Mobile Server 11.1.7**

**Helix Mobile Gateway 11.1.7**

January 15, 2008

©RealNetworks, Inc. All rights reserved.

RealAudio and RealVideo are registered trademarks of RealNetworks, Inc. in the United States of America and other countries.

Basic Server, Basic Server Plus, Real Broadcast Network, RBN, RealDeveloper, RealProducer, RealMedia, RealNetworks, RealPix, RealPlayer, RealPlayer Plus, RealPublisher, RealServer, RealSystem, RealText, the Real Bubble and the RealNetworks Media Type logotypes are trademarks of RealNetworks, Inc. in the United States of America and other countries.

RealFlash is a trademark of Macromedia, Inc. and RealNetworks, Inc. in the United States of America and other countries.

Macromedia, the Macromedia logo, and Flash are registered trademarks of Macromedia, Inc. in the United States of America and other countries.

All other trade names, trademarks or registered trademarks are trade names, trademarks or registered trademarks of their respective companies.

## **RealNetworks**

2601 Elliott Avenue  
Seattle, Washington 98121  
Phone: (206) 674.2700  
Fax: (206) 674.2699  
[www.real.com](http://www.real.com)

## Table of Contents

1.	VERSION INFORMATION.....	2
2.	HARDWARE/SOFTWARE REQUIREMENTS.....	3
3.	WHAT'S NEW IN THIS RELEASE .....	3
4.	NEW SINCE 11.1.2 GA RELEASE .....	3
5.	DOCUMENTATION ADDITIONS .....	9
5.1	Security Updates.....	9
5.2	Operating System Configuration Changes.....	9
5.3	Memory Allocation .....	9
5.4	File Descriptor Settings.....	9
5.5	RHEL4 .....	9
5.6	Solaris 8 and Solaris 9.....	10
5.6.1	Solaris settings of soft and hard limits for SLTA .....	10
5.7	Solaris 8 and Solaris 9 Patch Recommendations.....	11
5.8	RHEL4 Kernel Configuration Recommendations.....	11
5.9	PSTACK Installation.....	11
5.10	Windows Registry Update.....	12
5.11	Cross Version Plug-in Compatibility.....	12
5.12	RTPLive Legacy Mode Support .....	12
5.13	Reduced Startup Delay Configuration.....	12
6.	FIXES SUPPLIED IN THIS RELEASE.....	13
6.1	Listed Issues Fixed as part of v11.1.7.....	13
7.	FIXES SUPPLIED IN PREVIOUS RELEASES .....	15
7.1	Listed Issues Fixed as part of v11.1.6.....	15
7.2	Listed Issues Fixed as part of v11.1.5.....	18
7.3	Listed Issues Fixed as part of v11.1.4.....	19
7.4	Listed Issues Fixed as part of v11.1.3.....	20
7.5	Listed Issues Fixed as part of v11.1.2.....	22
7.6	Listed Issues Fixed as part of v11.1.1.....	24
8.	KNOWN ISSUES.....	26
8.1	Windows Media Player 11 With Helix Server.....	26
8.2	MDP and QuickTime playback of mobile content .....	28
8.3	Alternate Mount Point.....	28
8.4	Broadcast Redundancy .....	28
8.5	Content Distribution .....	28
8.6	3GP Compliance.....	28
8.7	Admin System.....	29
8.8	Content Browser .....	29
8.9	Delayed Shutdown .....	29
8.10	General .....	29
8.11	Java Monitor.....	29
8.12	Redundancy and HTTP with Windows Media Content.....	29
8.13	Multicasting of Windows Media Content.....	29
8.14	Logging.....	30
8.15	Multicast .....	30
8.16	Proxy.....	30
8.17	Rate Adaptation .....	30
8.18	Reduced Startup Delay .....	30
8.19	SNMP.....	30
8.20	Windows Media Support (non-WMP 11 related).....	30
8.21	Stopping SLTA results in Segmentation Fault .....	30
8.22	Crash Avoidance Issues (CAs).....	30
8.23	Handset Specific Issues.....	31
9.	CHECKSUM.....	32

## 1. Version Information

Release: Helix Mobile Server 11.1.7 and Helix Mobile Gateway 11.1.7

Version: 11.1.7.3406

Build: servproxyall-122007-10598

Release Status: General Availability

Products: Helix Mobile Server, Helix Mobile Gateway

Files:

Windows Server and Gateway Software:

mbrs1117-ga-win32.zip  
mbgw1117-ga-win32.zip

Linux Server and Gateway Software:

mbrs1117-ga-linux-rhel4.tar.gz  
mbgw1117-ga-linux-rhel4.tar.gz

Solaris 8, Solaris 9, and Solaris 10 Server and Gateway Software:

mbrs1117-ga-solaris-8.tar.gz  
mbgw1117-ga-solaris-8.tar.gz

Documentation:

HelixMobileServerAdmin.pdf  
HelixMobileServerConfig.pdf  
HelixMobileProxyAdmin.pdf  
HelixMobileProxyConfig.pdf

Note: not all files are distributed with all distributions.

## 2. Hardware/Software Requirements

Supported Platforms:

- Redhat Enterprise Linux 4
- Solaris 8
- Solaris 9
- Solaris 10
- Windows 2003 Server

Additional information about platform configuration recommendations for operating systems and hardware available at:

[http://www.realnetworks.com/resources/contentdelivery/server/recommended\\_platforms.html](http://www.realnetworks.com/resources/contentdelivery/server/recommended_platforms.html)

## 3. What's New in This Release

3.1 No New functionality has been added to this release.

## 4. New Since 11.1.2 GA Release

### 4.1 Alternate Mount Point

#### Feature Overview

The Alternate Mount Point feature will provide an alternate (or backup) path to the Real System Content directory as existing currently in the Server.

#### 4.1.1 Use Cases

##### 4.1.2 Performance enhancement

Performance of the server could be enhanced by allowing high demand content to reside locally, whilst lower demand content can reside on a file server, configured as the alternate (backup) content directory.

##### 4.1.3 Content fail-over

In a scenario where the user configures both main and alternate Content directories as a network device, the alternate can be used as a back-up if the main directory is unavailable.

##### 4.1.4 Content authoring

Having a backup Content Mount Point will allow the user to author content URLs without having to change the URL when content is moved to alternate location.

#### 4.1.5 Theory of Operation

The ability to search an alternate (or backup directory) is achieved by allowing additional Mount Points to be created with the same name, but different base paths. Additionally, each of the file systems sharing the same Mount Point will be assigned a Mount Point search order. This search order will determine the sequence in which the server will look for content in the additionally configured file systems.

#### 4.1.6 Interoperability

- **Network and Network Technologies Compatibility**

This feature may be configured to use a Local or Network file system. A choice of Networked File System will invoke the Asynchronous File System features, which are platform specific to each of the supported server platforms.

- **Component/Feature interoperability**

This section refers to areas where this feature will or not be interoperable. In addition, areas in which the feature is interoperable, but specific behavior needs to be called out will be noted as well.

- Content Browsing – Supported for both main and alternate Mount Points
- View Source – Supported for both main and alternate Mount Points, See *Section 3.16*
- Data types – All currently supported data types will be supported.
- Aliasing – Supported.
- Live Archiving – Not supported, see *Section 3.17*
- Cdist – Supported, see *Section 3.15*
- Logging – Standard and custom, will not be affected.
- SDPGen – This Mount Point will not be affected. SDPGen needs to follow the same login as for file system Mount Points when finding a file.
- ASXgen – This Mount Point will not be affected
- Ramgen – This Mount Point will not be affected
- Smilgen - This Mount Point will not be affected
- Live/On-demand switching, this feature will continue to work as previously designed

#### 4.1.7 Functional Behavior

##### 4.1.7.1 Alternate Mount Point(s)

With the implementation of this new feature, the server allows for one or more Mount Points to have the same MountPoint Attribute, but different base paths. The creation of Alternate Mount Points will be supported for all Mount Points listed under FSMount in the rmserver.cfg file. It is recommended that only Mount Points that contain a base path have an Alternate Mount Point configured for them.

##### 4.1.7.1.1 Configuration

Alternate Mount Points will be configured via direct edit of the configuration file.

#### 4.1.8 Mount Point Search Order

To determine the order in which the server will search through the alternate Mount Points, a configuration file variable `<Var MountPointSearchOrder="VAL"/>` will need to be added by the end-user to all additional Mount Points.

##### 4.1.8.1.1 Configuration file editing

The default value for MountPointSearchOrder is 1. If MountPointSearchOrder is omitted, the default value is assumed.

Additional Mount Points will need to have the variable `<Var MountPointSearchOrder="n"/>` added to them in the configuration file see *Section 3.18*.

The end-user will be required to enter a search order (n = search order). The user does not have to number additional file systems sequentially (1,2,3, etc), but may assign higher values to allow for additional file systems to be added later (i.e. 1, 10, 100, etc.).

The end-user may also add this variable to a default Mount Point, and change its search order.

#### 4.1.8.1.1.1 Duplicate Mount Point Search Order

If the end-user has one or more alternate file systems for the same Mount Point and two or more are configured with the same value for the variable *MountPointSearchOrder* the server will only execute a search on the first file system in the list, and ignore the others. This can occur if the end-user creates an alternate file system, and does not include a value (manual edit of the configuration file), the server will assign a default of 1. On server startup if a duplicate Mount Point with the same search order, the server will continue to startup, log an error message, and will ignore the duplicate

### 4.1.9 Process Flow

This section defines the flow of the new feature, as integrated with the legacy functionality.

#### 4.1.9.1 Mount Point Hierarchy

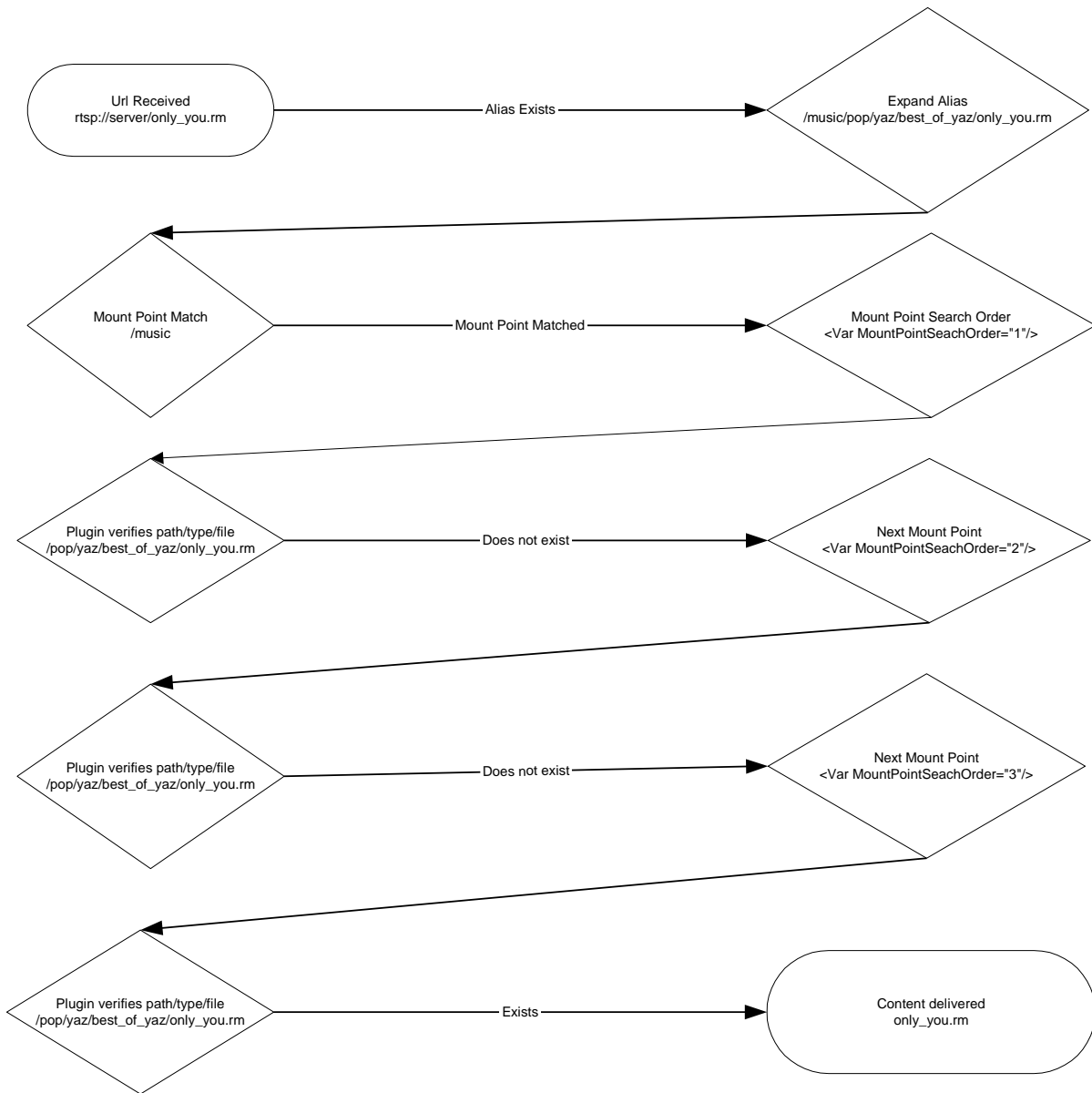
- When the Mount Points are loaded into the system on server startup, they are arranged into a tree, this is for search optimization. When a URL is received, the system will step down the tree and look for the most specific match, if that is not found, the next most specific Mount Point is tested, and this is repeated until “/”.

#### 4.1.9.2 Content Search

- Once the mount point is matched, the path will be verified for the content
- If the content exists, the plug-in associated with the Mount Point will take over verification and delivery.
- If the content does not exist, the next Mount Point in order (if configured) will be searched
- If the content exists, the plug-in associated with the Mount Point will take over verification and delivery.
- If the content does not exist, the next Mount Point in order (if configured) will be searched. This continues for the number of Alternate Mount Points configured for that Mount Point.
- If the content exists, the plug-in associated with the Mount Point will take over verification and delivery.
- When the search through all Alternate Mount Points is exhausted, and the content is not found, the system will then attempt to find the content on the next step up the tree see *Section 3.12 Mount Point Hierarchy*, above.

#### 4.1.10 Example

- The following example (flowchart on the next page) uses the configuration file variables shown in *Section 3.19*, below.  
url: rtsp://server/onlyyou.rm



#### 4.1.11 Content Caching

Content Caching (CDist) will be supported by this feature.

Currently, we have a configuration variable "UseContentDistribution" for each Mount Point which can be set by selecting "Cacheable by Content Subscribers" checkbox on Server Setup > Mount Points page.

- **Publisher**

When a server is acting as a Content Publisher, for each CDist rule it will receive a request for content from Content Caching Subscriber. The "UseContentDistribution" values of Mount Point on Publisher don't have any affect with respect to AMP. If the Mount Point on Publisher is having AMPs, the content will be searched on each AMP until content is found or the AMP list exhausts. If content is not found on any of the Publisher's AMPs, then it will fallback to Publisher's root mount point and check the subdirectory structure. If found, stream the content to Subscriber; otherwise, give an error.

- **Subscriber**

Currently, the "UseContentDistribution" flag is used by a Content Caching Subscriber to make a decision on whether or not to go to publisher if the content is not found locally. And this behavior would be changed as follows with respect to AMP. When a server is configured as a Content Caching Subscriber, and there are multiple Mount Points with the same name, they will be searched for content first. If content is not found on any of the Subscriber's Mount Points, then it should fallback to root and search subdirectory structure for the content. If still content is not found then we will check "UseContentDistribution" flag of the Mount Point having Highest Priority Search Order. If this flag is set, then we will be fetching the content from Publisher when content is not found in local cache. For example, if we have following mount point configuration:

```
MountPoint: "/music/"
BasePath: C:\Program Files\Real\Helix Server\Content\audio
MountPointSearchOrder=1
UseContentDistribution=1
```

```
MountPoint: "/music/"
BasePath: C:\Program Files\Real\Helix Server\Content\audiovideo
MountPointSearchOrder=2
UseContentDistribution=0
```

Here Highest Priority Search Order is "1". So, the first Mount Point's "UseContentDistribution" value will be used to decide whether or not go to Publisher to fetch the content. In above case, it will go to Publisher. "UseContentDistribution" value of other mount points will not matter.

#### 4.1.12 View Source

When there are multiple Mount Points with the same name, *View Source* and *Hide Paths* will be applied as a group, to all Mount Points with the same name.

#### 4.1.13 Live Archiving

When Live Archiving is enabled, the Server will attempt to save the broadcast to a file on the default path associated with the Mount Point selected. If that Mount Point is not available, the system will not attempt to write to the Alternate Mount Point associated for that Mount Point, and the attempt will fail.

#### 4.1.14 Configuration File

The following configuration variable is added to the rmserver.cfg (default.cfg) file on system install.

```
<!-- Local File System; Media -->
  <List Name="RealSystem Content">
    <Var ShortName="pn-local"/>
    <Var MountPoint="/Music"/>
    <Var BasePath="/home/server11/Content"/>
    <Var MountPointSearchOrder="1"/>
    <Var UseContentDistribution="0"/>
  </List>
<!-- Local File System; Media -->
  <List Name="RealSystem Content Alternatel">
    <Var ShortName="pn-network"/>
    <Var MountPoint="/Music"/>
    <Var BasePath="/mnt/fileserver1/Content"/>
    <Var MountPointSearchOrder="2"/>
    <Var UseContentDistribution="0"/>
  </List>
<!-- Local File System; Media -->
  <List Name="RealSystem Content Alternate2">
    <Var ShortName="pn-network"/>
    <Var MountPoint="/Music"/>
    <Var BasePath="/mnt/fileserver2/Content"/>
    <Var MountPointSearchOrder="3"/>
    <Var UseContentDistribution="0"/>
  </List>
...
</List>
```

#### 4.1.15 Variable Name

Name	Type	Range	Default	Description
MountPointSearchOrder	string	1 to 256 bytes	1	Must be a positive integer, greater than 0

- **Duplicate List Name**

The List Name of the Mount Point is the only means by which the server can differentiate between Mount Points. Upon startup, the server will parse the rmserver.cfg file if more than one Mount Point shares the same List Name, the server will continue to startup, log an error message, and will ignore the original, using the last one in the list.

#### 4.1.16 Default Configuration Files

The following Mount Points located within the 'FSMount' section of the default "rmserver.cfg" and "default.cfg" files will be modified to include `<Var MountPointSearchOrder="1"/>`.

- Name="RealSystem Content"
- Name="RealSystem Secure Content"
- Name="CapExProfiles"

#### 4.1.17 Notes

- Upon making manual changes to the configuration file, a server restart is required for these changes to take effect.
- Whenever the Mount Points are re-parsed the sever will validate that both the Mount Point Search Order and Mount Point Descriptions are unique for a group of Mount Points and log an error to the error log.
- When this feature is used to back up static content, the back up must mirror the original content. Different content with the same filename can cause errors, and should be avoided.

## 5. Documentation Additions

### 5.1 Security Updates

Please review the recent Security Update and Incident Report. The most recent posting can be reviewed by visiting <http://www.service.real.com/help/faq/security>

### 5.2 Operating System Configuration Changes

#### 5.3 Memory Allocation

The Helix Mobile Server and Proxy consume memory on a per-client basis. The amount of memory consumed will vary, according to the nature of the presentation streamed to each. Memory is allocated by using the `-m #` command line flag at startup, where `#` is the amount of memory to allocate, in megabytes. For example, starting the server with the command `Bin/rmserver rmserver.cfg -m 512` would allocate 512 megabytes of memory to the server process.

Memory allocation limits of Helix Server and Proxy:

- Solaris: 4GB
- Linux/i386: ~2.8GB
- Windows: 2 GB (the OS is limited to 2 GB also)

About Memory-Mapped I/O

Since the server uses memory-mapped I/O that is not counted as part of this `-m` shared memory segment, additional memory should be reserved for mapped I/O. Not doing so may result in a significant performance penalty. The amount of memory needed for memory-mapped I/O varies with the number of clips being played and the bit rate of those clips. Generally reserving about 30% of the system memory for memory-mapped I/O is a good rule of thumb, but when setting this variable, one should monitor the system performance and watch for sudden changes in performance such as page faults.

#### 5.4 File Descriptor Settings

RealNetworks recommends increasing the default file descriptor setting for your Solaris and Linux servers. File descriptors are heavily used by the server, for each file read, each open socket, etc. The recommended number of file descriptors to set is 65537 for each CPU. Therefore, on a dual processor machine you would set the value to 131074, and on a quad processor machine you would set it to 262148.

### 5.5 RHEL4

1. Examine system fd limit and ensure it meets or exceeds the recommended minimum:

```
$ cat /proc/sys/fs/file-max
```

If it doesn't, increase it by editing the file `/etc/sysctl.conf` (all file edits will require root access) and adding:  
`fs.file-max = number_of_desired_file_descriptors`

2. Edit as root `/etc/security/limits.conf` and add the lines:

```
*      soft      nofile      number_of_desired_file_descriptors
*      hard      nofile      number_of_desired_file_descriptors
```

3. Edit `/etc/pam.d/login` and add the following line:

```
session required pam_limits.so
```

4. Edit `/etc/pam.d/sshd` and add the following line:

```
session required pam_limits.so
```

## 5.6 Solaris 8 and Solaris 9

1. examine system fd limit and ensure it exceeds the recommended minimum:

```
$ ulimit -Hn
```

If it doesn't, increase it by editing the file `/etc/system` (all file edits will require root access) and adding:

```
set rlim_fd_max=number_of_desired_file_descriptors
```

### 5.6.1 Solaris settings of soft and hard limits for SLTA

Soft Limits:

Before 11.1.x release, SLTA used to start fine with a soft limit of 256 on the file descriptors on Solaris. However, there was a change after that which requires the soft limit to be set to at least 512 on the file descriptors, on Solaris. This can be done in the following two ways:

1. Through shell command "ulimit"  
`ulimit -Sn 512`

Please note that this setting would be applicable for only the shell from which this command is executed. If you exit the shell and start a new one, then you need to execute the above command again, before starting SLTA.

2. Changing the system wide settings by adding the following line to `/etc/system`:  
`set rlim_fd_cur=512`

Please note that this change requires the super user permissions and a reboot. Once changed, this limit would be applicable for all the shells invoked.

Hard Limits:

Minimum for SLTA operation is 512 and any setting beyond this is up to the administrators based on the ability that they would like to give their users to adjust the soft limits. However, if SLTA is used on the same machine

where the Helix Server/Helix Proxy is installed, then the hard limits recommended in section 5.4 should be followed and hold good for SLTA operation.

## 5.7 Solaris 8 and Solaris 9 Patch Recommendations

Testing at RealNetworks has shown some instability of Solaris 8 and 9 operating systems related to high levels of UDP usage. Sun has provided and recommends the following patch in order to address this situation.

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57728-1>

This patch is not necessary unless the operating systems experience kernel panic messages related to the UDP module.

## 5.8 RHEL4 Kernel Configuration Recommendations

Testing at RealNetworks has shown some instability on Red Hat Enterprise Linux 4. This instability is manifested as "kernel panics" related to "out of memory and no killable processes". This is partially because the 11.0.1 release of the Helix Mobile Server and Helix Mobile Gateway has a larger memory footprint than previous releases. Because of the 1 gigabyte (default) kernel virtual memory limitation on 32-bit systems with less than 4G RAM, we are recommending application of the 4G/4G patch set:

linux-2.6.0-4g4g.patch  
linux-2.6.8-4g4g-backout.patch  
linux-2.6.9-4g4g-hugemem-warning.patch  
linux-2.6.9-net-b44-4g4g.patch  
linux-2.6.9-4g4g-noncacheable.patch

Note: This should only be necessary in cases where there will likely be enough player load on the server that memory usage would exceed 1 gigabyte. If the server is started with a memory flag setting of less than 1 gigabyte (`-m 1024`), this patch solution will not be required.

To install the Linux kernel patches, do the following steps:

Download the kernel-2.6.9-5.0.5.EL.i686 kernel from <http://rhn.redhat.com>; you can find it by searching for "kernel" under "Packages"

Please refer to your Linux documentation regarding updating your Linux kernel  
During the configuration step of your kernel update, make the following changes:

Under "Processor type and features" change the following:

Select "4 GB kernel-space and 4 GB user-space virtual memory support"

Select "Symmetric multi-processing support"

Deselect "Virtual Kernel Preemption"

Under "High Memory Support (65GB)", select "4GB"

Save the configuration, and compile and install the kernel

## 5.9 PSTACK Installation

There are known stability issues on Solaris and Linux systems running Helix Mobile Server and Helix Mobile Gateway which don't have pstack installed. Pstack is installed and configured on Solaris by default, however if you are running RHEL4, you will need to install and configure pstack for reliable Helix Mobile Server and Helix Mobile Gateway operation. You find the pstack package by searching for "pstack" under Packages at <http://rhn.redhat.com>. Please refer to your Linux documentation for instructions on installing or updating package files.

## 5.10 Windows Registry Update

When running the Helix Server and Helix Proxy on Windows, it will be necessary to increase the Default Send Buffer size in the operating system. To do this you will need to add a value to your Windows Registry.

Launch the Registry Editor from the Start→Run... option by typing the `regedt32.exe` command

Traverse through the tree to the following branch:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters

Add a new DWORD Value to the key called `DefaultSendWindow` and set that value to `32767` (decimal).

Restart your Windows 2003 Server machine.

This change will prevent poor QOS for clients connecting to live broadcasts over TCP.

## 5.11 Cross Version Plug-in Compatibility

Plug-ins are not binary-compatible between v9/v10 and v11 on Linux due to changes in compiler versions. The plugins need to be recompiled with the updated build environment to be useful.

## 5.12 RTPLive Legacy Mode Support

A new configuration variable has been added to fix an issue with live streams using RTP which caused sync, and other QOS issues. The variable is `<Var RTPLiveLegacyMode="1"/>`. When this flag is set to 1, RTP transport forces initial RTPtime and sequence to be 0. After a PAUSE, sequence will be the last sequence number of RTP packet plus 1 and RTPtime will reflect the elapsed time between the PAUSE and PLAY request (i.e. RTPtime is offset only at the initial PLAY request). This is in accordance with 3GPP specifications

## 5.13 Reduced Startup Delay Configuration

It is possible to increase the limit on RSD packet buffer queue duration through the following configuration variable:

```
<List Name="LiveReducedStartupDelay">  
  <Var MaxDurationOfRSDPacketBufferQueue="90"/>  
</List>
```

The default value for this is 70 seconds and the units are in seconds. The above section is not present by default in the configuration. It needs to be added manually and the value adjusted accordingly.

## 6. Fixes Supplied in this Release

### 6.1 Listed Issues Fixed as part of v11.1.7

- **180778 Bind to port X fails when broadcasting live stream**  
When live encoding using "Push, Account Based Authentication" the Helix Server reports in rterror.log:  
05-Oct-2006 14:15:44.UNKNOWN tmp1gpln(4032): Bind to port 50001 failed.  
The above-described condition has been fixed.
- **187598 SLTA experiences problems with file descriptors / ulimit**  
Before 11.1.x release, SLTA used to start fine with a soft limit of 256 on the file descriptors on Solaris. However, there was a change after that which requires the soft limit to be set to at least 512 on the file descriptors.  
This can be done in the following two ways:
  1. Through shell command "ulimit" `ulimit -Sn 512`  
Please note that this setting would be applicable for only the shell from which this command is executed. If you exit the shell and start a new one, then you need to execute the above command again, before starting SLTA.
  2. Changing the system wide settings by adding the following line to /etc/system:  

```
set rlim_fd_cur=512
```

  
Please note that this change requires the super user permissions and a reboot. Once changed, this limit would be applicable for all the shells invoked.  
  
Additionally, if the soft FD limit at the SLTA start-up time is less than 512, the application will return an error message: `Insufficient soft fd limit found. Please increase the soft fd limit up to minimum of 512.`  
(See section 5.6.1 for more details on this topic.)
- **192013 Helix Server does not restart the service from a restart in Server Admin Page**  
Restarting server from within the Server Admin results in the service stopping. The expected behavior would be for the server to restart. The Windows services manager log indicates that the application has unexpectedly stopped. This issue has been reported on Windows 2003 with SP2. The problem does not occur if the service pack is not installed.  
The above-described condition has been corrected.
- **197224 Surestream-aware splitting setting interferes with live 3gp**  
Under specific conditions if the SureStream Aware splitting is enabled for live 3gp, the server reports faulty message: `"tmp1gpln(27670): The packets' timestamps are incorrect for path/rtpencoder/xyz.sdp, the buffering of packets is disabled."` No functional issues however were associated with this error message.  
The above-described condition has been corrected. The error message is displayed only when appropriate.
- **198373 Crash Avoidance in broadcast reception plugin cause 3gp live feeds to drop**  
Under specific conditions if crash avoidance occurs in the broadcast reception plugin, it will cause the edge receiver to drop all live feeds. The edge receiver must then be restarted in order to restore service.  
The above-described condition has been corrected.

- **198652 Disconnected players not removed from registry**  
 A player streaming live content will not be removed from the registry upon disconnect. The issue was related to incorrect accounting in a server's plugin.  
 The above-described condition has been corrected. The count is now decremented as expected.
- **199221 SLTA Pull encoding stops playback after about 1 minute and 26 seconds**  
 The STLA session stops unexpectedly after about one and a half minute. Restarting the STLA session results in the same behavior as mentioned. This specific issue occurs if the SLTA is ran on Windows 2003 Server platform. It is not present on Solaris or Linux.  
 The above-described condition has been corrected. SLTA session continues through the duration of the content or until stopped by the user.
- **199915 SLTA Splitting / can result in server failures when redundancy is used**  
 When splitting is configured to redistribute "/" as the PathPrefix, problems can occur when redundancy is used. The server redistributes both the *"/broadcast/"* feeds as well as the *"/redundant/"* feeds that are on the transmitter server. As a result, multiple redundant feeds were created which caused instability.  
 The above-described condition has been corrected. Unnecessary multiple redundant feeds are no longer generated.
- **201509 ConnectionID Zero (0) remains in registry**  
 When pulling a client registry dump it has been noticed that ConnectionID "0" remains with details about the last failure to play. It has been determined that the problem was caused by the way in which 404 and 401 error connections were being accounted for. Although not affecting any of the functionality, the registry value has raised unnecessary concerns.  
 The above-described condition has been corrected.
- **203850 Server responds with incorrect value for Range as Range:npt=0- after receiving PLAY**  
 In the response message to PLAY, the server is sending back the Range Header as Range: npt=0- . This is happening only when client sends PAUSE, and then a PLAY. Under normal circumstances, the server should respond with the Range Header with the exact range of the RTP Data Packets being sent by it.  
 eg. Range: npt=8.16-31.02.  
 The above-described condition has been corrected. Proper range is now being returned.
- **204575 Poor performance was seen if the stream has more than 1 audience ( surestream )**  
 Attempting to stream a live broadcast using Back-Channel Multicasting with Helix Server results in poor video and audio quality and the stream frequently hangs even under low load conditions.  
 The above-described condition has been corrected. Performance under this specific setup is now at the expected level.
- **204606 Stopping SLTA results in segmentation fault**  
 When stopping the SLTA with Ctl-C, it ends with a segmentation fault. No core dump is generated and restarting the SLTA does not present any adverse effects.  
 The above-described condition has been corrected. SLTA no longer generates a segmentation fault when stopped.
- **205066 Poor performance of Video On Demand Content compounded by multiple Crash Avoidances**  
 Under specific conditions continuous CA's have been observed when trying to use the server with following configuration:
 
  - High capacity disk attached by NFS to the edge server
  - The edge server also contains local content
  - Helix Server is configured to use the Alternative Mount Point by looking on the local disk for content (set in config file as pn-local) and if it doesn't exist check the NFS drive (set in config file with pn-network for Async).

- RealMedia content

The above described condition has been fixed. The server no longer generates Crash Avoidance instances.

- **205780 Memory Leak resulting in a restart from every few days to once a month**

Under specific load conditions a relatively small memory leak has been observed. At 60 concurrent players, connecting and disconnecting at typical mobile rates (about 1-3 minutes per watch), memory usage increases about 60 MB / day. Depending on usage and memory reserved for the server, the server runs out of memory every few days to every month, auto restarting and disconnecting all players. The memory leak is independent on the content used. It was seen on on-demand only and live only servers. Memory usage increases only when players connect and disconnect. When no players are connected, memory usage stays flat.

The above described condition has been fixed.

## 7. Fixes Supplied in Previous Releases

### 7.1 Listed Issues Fixed as part of v11.1.6

- **135783 NMS does not receive the Server start trap**

In a particular test it was discovered that the NMS was not receiving the ServerStart trap. A simplified procedure requires configuring the server for SNMP and setting the ServerStart trap to 1. Next, start both the master and the server. As a result, the expected trap is not received by NMS.

The above described condition has been fixed. The trap is now being received as expected.

- **149366 Multiple "couldn't lookup session for channel <0x1>" errors**

A session with an SLTA stream has revealed significant number of these error messages. Such would occur when the SLTA stream was split through the proxy and the proxy's Live Splitting Transport was set to "Always use TCP."

The above-described condition has been corrected.

- **171671 Choppy playback of audio/video MRC file with MDP enabled on Helix Proxy 11.1**

Under certain circumstances it has been observed that while MDP is enabled on the proxy, playback of MRC content is choppy. The actual problem occurs at about 3 minutes of playback.

The above described condition has been corrected. During the investigation it has been determined that the issue was not caused by MDP, but due to generation of empty rate manager logs. The latter had an impact on MDP, which in turn resulted in choppy playback.

- **176345 Lingering connections when streaming Windows Media content through Apache Server as a proxy**

The hung connections can be seen in 'rss' and 'netstat' and the java monitor. All show specific requests for Windows Media content that are not timing out. A high number of the connections are over HTTP/Port 80.

The above-described condition has been corrected.

- **17802 Mention of MSQL support on Helix Server for user authentication in docs**

The documentation cites an example of setting playback restriction using msql. This method is no longer supported.

The Server Admin and Configuration guides have been updated accordingly. References to msql have been removed.

- **178626 ASXGEN does not incorporate query variables into URL response**

Under certain conditions the query variable as present in the original request is not included in the returned URL. For example:  
Use an http client (such as wget) to request an asxgen url that includes query parameters such as:

```
http://localhost:8080/asxgen/media.wmv?varname=varvalue
```

Open or otherwise view the result of asxgen and observe that the URL returned in the asx file does not include the query variables that were present in the request. e.g.:

```
mms://localhost:1755/media.wmv
```

The above-described behavior has been corrected.

- **180467 Firewall chapter misses HTTP port for remote profile retrieving**  
The firewall chapter of the Helix Server Administration Guide should include the need to open TCP port 80 (HTTP) for outgoing connections originating at the Helix Server aimed at handset manufacturer's device capability profile servers in the Internet.  
The pdf documents on page 117 of the Mobile Proxy Admin Guide, and page 278 of Mobile Server Admin Guide now include the previously missing information.
- **180935 Redundant Publisher Failover does not function**  
When configuring a Helix Server to be a subscriber, it is possible to add in multiple Publisher servers to a specific path for the subscriber to look for content on. This means should a publisher server fail the subscriber servers have a redundant option to fallback to and look for content. However, testing has revealed that this does not work.  
The above described condition has been corrected. Please note that the expected behavior applies only if the publisher server is not responding. This implementation does dictate that the subscriber checks the publisher and fails over if the content or the server is not available.
- **181142 Incorrect reporting of SNMP Memory OID usage**  
SNMP Memory Usage OID reports incorrect values after 2 GB of memory allocation. The OID is a 32-bit integer, so when it hits its maximum value of (2147483648), it begins to report a negative value.  
The above-described behavior has been corrected.
- **183232 MOV/MP4 files fail at 2mins 10 seconds via HTTP**  
When streaming a MOV file with a QuickTime client, if it cannot get the data by UDP the client falls back to getting the data via HTTP. Under certain conditions it has been observed that when this fallback occurs and a stream is played from the Helix server using HTTP, the playback stops at 2mins 10seconds.  
Workaround: Set the KeepAlive value to 60 seconds in the server configuration file:  

```
<Var KeepAliveInterval="60"/>
```
- **185750 Content browsing feature doesn't work through administrator User Interface**  
While trying to browse the content of "/" or any other mount point using admin UI, the server doesn't respond to the request and file contents of the mount point are not displayed to the user.  
The above described condition has been corrected. Content browsing feature from within the administrator user interface is now working as expected.
- **185973 Listname parse error message is logged on wrong file**  
In the Helix Server Version 11.x builds, the checking for dot in List Names is missing. As a result the Registry contains an invalid entry (a tree node without a name) as below.

```

MediaDelivery
|
---UserAgentProfiles
|
---Default
|
---
```

This happens only if List Name ends with a dot. Because dot is considered as field separator, an empty field is added to Registry.

- **186671 Admin UI does disallows users to add Alternate Mount Points**  
 Since the Helix Server 11.1.2GA, a new feature called Alternate Mount Point has been added. However at the time of the release, this feature was not configurable through the Administrator User Interface.
- **187050 Transmitter re-announces Encoder feed to Receiver after Encoder stops**  
 It has been observed that an Edge server is listing a live encoder stream as being available but is in fact not. What appears to happen is that the Transmitter re-announces an encoder feed to the Receiver server after the encoder was stopped.
- **187617 Templatized Logging HTTPPost fails when DNS is used**  
 When using Templatized Logging to post information to a HTTP server, it has been observed that this fails when the Destination used contains a DNS name rather than a IP address. The server does not appear to even make a HTTP attempt to the server.  
 The failure was due to the fact that the host name was not being resolved correctly. The server was parsing the URL to obtain the host name but it was not resolving it before using to connect to the socket. The above described condition has been corrected.
- **188873 Message: "select error in main loop" during server restart**  
 During certain conditions following a server (service) restart, while streaming Windows Media content, the server begun to exhibit high CPU usage with only one to two users being connected. The rmemlog file showed instances of the aforementioned error message. This error occurs on Windows platform only. The above described condition has been corrected.
- **190250 Crash Avoidance Loop causes server to generate 2GB RSS logs and reports errors**  
 Under specific conditions while server is experiencing Crash Avoidance loop, the error log increases in size to 2GB. Eventually, the rss log error (27) File too large begins to occur as well.
- **192658 Live RTP: Server sends duplicate RTP packets causing reported packet loss of 16777215 (0xfffff)**  
 Under certain conditions, if a client is disconnected in the first three or four seconds, the packet loss logged would be 0x00ffffff. If there was any packet loss, the right value would get reported.  
 The issue is related to the fact that the player is the one sending this particular packet value. As a preventive measure, the server has been modified to set the packet loss value to 0 every time it receives the invalid value from the player.
- **195633 Fast-forwarding Windows Media stream containing markers results in long pauses**  
 While streaming a Windows Media video file (containing markers) from the Helix Server and skipping to the marker through an embedded player or simply fast forwarding, the user will experience pausing at 91% for the length of time the user fast forwarded to before the playback continues.
- **196821 Lingering Windows Media encoder connections**

Under certain conditions, once a player disconnects from a stream, the Windows media encoder connection continues to be attached to the server. Since this is a pull-type connection, it is expected that the encoder connection is dropped once the player disconnects.

The above-described condition has been corrected. The encoder connection drops shortly after the player disconnects from the server.

- **199219 Helix Mobile Server and Gateway experience memory leaks while streaming 3gp content**  
Under certain conditions a memory leak occurs in the server if x-wap-profiles are used in RTSP requests. Depending on the amount of RAM, the server will eventually run out of memory and restart.  
The above-described condition has been corrected. Issue was related to server's failure in releasing of memory resources.
- **199300 Accessing live content from MobiTV via Helix Proxy stops streaming after 2 minutes**  
Streaming via the helix proxy to a variety of handsets fails after 2 minutes for no apparent reason. The issue does not occur when streaming to a desktop client or Palm-based handsets.  
The above-described condition has been corrected.
- **199593 Proxy injects source IP into RTSP conversation**  
Under a specific setup conditions where the proxy is behind a VIP or on a private network, the injection of the source IP (non-routable address) by the proxy results in handset's failure to contact the proxy and the RTCP RR reports never reaching their intended destination – the origin server.  
The above-described condition has been corrected.
- **199593 Support of SNMP to v2 does appear to be reflected in the MIB browser**  
It has been discovered that although the SNMP is set to v2, the MIB browser shows v1 traps.  
The above-described condition has been corrected. Both v1 and v2 traps are now sent and correctly reported in the MIB browser.
- **200258 Incorrect values reported in proxy's java monitor for live/split client connections**  
Under specific conditions it has been observed that the proxy java monitor incorrectly reports bandwidth usage when doing live split streaming. For example, when pulling a 50kbps live stream using a mobile handset, it will only report 480 bits/second. Additionally, the splitting import value is showing as zero.  
The above-described condition has been corrected. The bandwidth for non-RealPlayer clients was incorrectly calculated, resulting in false data being displayed in the java monitor.
- **202781 Stopping encoder feeds on the origin server ends all encoder feeds on the edge server**  
Under specific conditions where encoders are configured to connect to the origin server, terminating one of these would result in drop of the remaining streams at the edge server. The issue occurs only when the servers are configured for multicast splitting.  
The above-described condition has been corrected.
- **203686 SNMP v2 trap sent by Helix server/proxy needs to contain a 0 before the trap number**  
In SNMP v2 traps, the second variable binding, the SNMPTrapOID should include a 0 between the Enterprise and the specific trap number. Absence of the zero causes the MIB Browsers to show the v2 traps incorrectly.  
The above-described condition has been corrected.

## 7.2 Listed Issues Fixed as part of v11.1.5

- **180778 Bind to port X failed when live broadcasting**  
When live encoding using "Push, Account Based Authentication" the Helix Server reports in rmerror.log:

05-Oct-2006 14:15:44.UNKNOWN tmp1gpln(4032): Bind to port 50001 failed.

It appears to show that when an encoder connects if the ports are in use then the server attempts to bind to them and then falls back to the next free port range continuing before finding a free range available. The above-described behavior has been corrected.

- **184743 H264/MOV, H264/MP4 videos stutter when content is from non-HMP**  
264/MOV or H264/MP4 content created on a number of 3rd party encoders (e.g. Mac with Final Cut Pro, QuickTime Pro, Popwire Encoding tool) plays poorly from Helix Server with default install settings (MDP disabled) to QT player.  
The above-described condition has been corrected. The issue was related to timestamps being read incorrectly.
- **190741 Windows Media HTTP connections log entries written on two lines rather than one**  
Helix Server logs Windows Media client requests over 2 lines instead of one. This makes it impossible to parse with log parsing tools as the line breaks are placed incorrectly in the middle of the entry.  
The above-described behavior has been corrected. The logs are now written correctly to the access file.
- **193716 SLTA generates a core dump file on certain invalid files**  
Certain invalid files will cause the SLTA to stop and generate a core file. While such files can be easily identified and removed, it is desired that the SLTA does not quit because of an invalid file in the playlist.  
The above-described condition has been corrected. The SLTA will now skip an invalid file and proceed to the next one in the playlist.
- **193935 SLTA 3GP feed degrades after few hours of streaming**  
Under certain conditions after streaming for about two to seven hours a MPEG4 or AMR-NB file, the quality of the feed unexpectedly degrades. After analyzing this issue it seems that the problem is with SLTA while looping the content file for streaming.  
The above-described behavior has been corrected. The feed no longer degrades as initially reported.

### 7.3 Listed Issues Fixed as part of v11.1.4

- **157648 Proxy fails to timeout and terminate invalid connection attempts**  
Under certain conditions Helix Proxy would not correctly terminate invalid connection attempts. Resulting in what is commonly referred to as lingering connections.  
Helix Proxy now correctly terminates invalid connection attempts.
- **169887 "Default" UAP used even when the User-Agent matches another normally disabled) UAP**  
An MDP User-Agent Profile with a specific UserAgent matching string that is normally disabled (hasUseMediaDeliveryPipeline=0) is not used if the connecting client enables MDP with Helix-Adaptation or 3GPP-Adaptation. Instead, the "Default" UAP is used.  
Helix Proxy no longer uses the default UAP when the matching UserAgent has UseMediaDeliveryPipeline=0.
- **180152 Bad quality when using unhinted 3GPP content with SLTA**  
Simulated live broadcasts that used unhinted 3GPP content as its source would result in a poor video experience for end users.  
Unhinted 3GPP content will now stream correctly when used as a source for SLTA.
- **183554 SMIL File with RealText and RealPix causes CA when using UDP**  
Smil files that contained both RealText and RealPix elements would not stream correctly from Helix Server via UDP.

Smil files that contain RealText and RealPix elements will now correctly stream from Helix Server via UDP.

- **Helix Mobile Server runs out of memory with 2000 clients and 200 live streams**  
Under a specific set of load circumstances Helix Server would run out of memory and restart. Corrective measures have been included in Helix Server 11.1.4.  
It is now possible to support varying load scenarios with Helix Server.
- **188627 HTTP Delivery to WM client fails**  
Helix Server would fail to stream content to Windows Media clients when the content was located in an http deliverable directory.  
Helix Server will now correctly stream content stored in an http deliverable directory to Windows Media Clients.
- **189199 Java Monitor Bandwidth Usage field does not display Bandwidth Served to QuickTime Player for 3GPP live broadcasts**  
When playing a 3GPP live stream to a Quicktime player, Helix Server's Java Monitor Bandwidth Usage field does not count the bandwidth.  
Helix Server now properly displays bandwidth usage when QuickTime clients are connect to a live 3GPP session.
- **190327 Frequent buffering occurs when MDP is enabled on HP 11.1.3**  
Frequent buffering occurred when MDP was enabled on Helix Proxy 11.1.3. Resulting in choppy audio and pixilated video.  
Enabling MDP on Helix Proxy no longer results in frequent rebuffering or poor QOS for end users.
- **190609 Imprecise error message**  
Helix Server 11.x does not support 3GPP Rel.6 files which have been encoded with the "Progressive Download" profile. When trying to stream such a file, the server refuses and prints out the following error:

```
***07-Mar-2007 08:15:12.604 tmlgpln(3928): This server(proxy) does not support 3GPP files with a major brand of 3gr6.
```

While technically correct this message did not provide sufficient information for system administrators to take corrective action. Additional text has been added to the message to ensure that streaming server administrators can correct the cause on their own. The following is an example of the new error message:

```
***07-Mar-2007 08:15:12.604 tmlgpln(3928): This server(proxy) does not support 3GPP files with a major brand of 3gr6 (Progressive Download profile). Please use only files that are encoded with the "Streaming Server profile (include hint tracks)". See 3GPP TS 26.244, Rel-6.
```

## 7.4 Listed Issues Fixed as part of v11.1.3

- **173113 RTP Timestamp Computation Selection" does not function with Helix Mobile Server or Proxy**  
Under certain conditions while in " Legacy RTP Timestamp Computation Selection" mode, the server would fail to properly calculate the RTP time stamp. The issue manifests itself after repeated fast-forward, rewind, and pause operations.  
The above-described behavior has been corrected. The Legacy mode for RTPS time is now functioning as expected. To configure the server to use Legacy RTP time stamp for a specific player please add the following section to server configuration file:

```
<List Name="LegacyRTPTimestampComputationUserAgentStrings">
  <Var Item_1="PlayerUserAgentString"/>
</List>
```

- **173204 Surestream files playback fails on Nokia handset with MDP enabled on Helix Proxy 11.1**

At approximately 43 seconds into playback of a surestream clip, the following message appears on the client: "Memory full close some applications?" The issue occurs while MDP functionality is enabled. The Client Profile for the micro core player of the Nokia handset is missing in the capex section of the default proxy configuration file. As a result, the proxy may be using the incorrect client's buffer size. Adding the missing section under capex corrects usage of NokiaR1M.rdf profile. This has resolved both display of the aforementioned error message and playback of the surestream file. This setting is present in the server's configuration file under the capex section and the same is now present in the proxy's configuration file. For reference the missing section is:

```
<List Name="Client8">
  <Var UserAgent="RealMedia Player/mc"/>
  <Var URI="file://profiles/NokiaR1M.rdf"/>
</List>
```

- **178520 Backchannel Multicast does not fail over**

In a situation where a client connects to Helix Server for Backchannel multicast, the server is not sending PLAY response. As a result the player is not failing over to next selected transport and times out. The above-described condition has been corrected. The server now sends the PLAY response at the appropriate time so that the failover is successful. This fix is applicable to backchannel multicast only.

- **181297 Watch Log Transmitting via TCP Breaks when Receiving Service Temporarily Down**

When Helix Server 11 is configured to regularly send a Watch log via TCP to a remote Log Processing service, it works fine. However, if the remote server becomes unavailable then even after it is restored, log transmitting is not restored and Helix Server must be restarted in order to resume log transmitting. The above-described condition has been corrected. Connection sockets between the server and the remote service are now properly maintained and transmitting of the logs resumes as expected.

- **184340 Invalid RTSP clients in registry cause incorrect real-time statistics reporting**

And when a player connects to a redundant live stream via a receiver, and if the encoder suddenly becomes unavailable, the player's registry entry is not cleared and the player count is not getting decremented on the receiver. Specifically, what happens is that during this particular time the receiver server is sending a REDIRECT request to the connected client and the client is tearing down the existing connection and sending a new OPTIONS request followed by the DESCRIBE. The receiver is not responding to this DESCRIBE request and it is this second client connection attempt that is causing hung registry entry. The initial connection however is getting cleaned up as expected. The above-described condition has been corrected.

- **185748 Server exhibits Heartbeat Failure; fails to restart**

During a heartbeat failure, the server uses "pstack" (on a Linux Red Hat Enterprise 4 platform) on the controller Process ID to receive stack traces of all the pthreads. The pstack invokes gdb, attaches a binary to the controller Process ID and runs the gdb command to print the stack traces of all the threads. However, the particular gdb version would hang during the process, resulting in eventual 100% usage of the CPU. A manual kill of the gdb and the server processes is required in order to recover from this state. The above-described condition has been corrected. Solution includes avoidance of the condition under which the server process is trapped when gdb process is rendered unresponsive.

- **187510 Server stops sending post-seek packets of sparse data streams (timestamp delivery ones)**

After a seek operation, the event which start time is before the seek point, and end time is after the seek point, does not launch. The above-described condition has been corrected. The events are launching as expected.

- **187816 Live streams drop at the edge servers**  
Under certain conditions in encoder -> transmitter --(multicast)-> edge server setup, the live stream would suddenly become unavailable. A restart is necessary in order to correct the issue. However, this results in dropping all of the client connections.  
The above-described behavior in the specific scenario as outlined has been corrected. The end result was caused by a Crash Avoidance instance. Addressing the condition leading to the CA has resulted in streams no longer being dropped at the edge servers.

## 7.5 Listed Issues Fixed as part of v11.1.2

- **121899 RBS encodes do not show source IP address.**  
Unavailability of the source IP address prevents identification of (remote) host encoders. This becomes critical in managing significant number of concurrent encoders and in case of troubleshooting problems with the encoded streams.  
The above-described condition has been corrected. The server now properly displays source IP address of RBS encoders.
- **132494 Misleading error messages logged for ANY LatencyMode (True Live) streams**  
The error message: "Low latency streaming is not licensed in this server. Stream being reverted to normal latency mode" is seen in all latency configurations (low, moderate & normal) with and without servers which have the LowLatencyLive (True Live) feature enabled. Expected results:  
  
Expected Results:  
When the server has the license with LLL enabled, no errors are written to the rmerror log file when the encoder uses Normal, Moderate or Low settings  
  
When the server has the license with LLL disabled, no errors are written to the rmerror log file when the encoder uses Normal settings  
  
When the server has the license with LLL disabled, an error message is written to the rmerror log file when the encoder uses Moderate or Low settings  
  
The above-described condition has been corrected. The log entries are being made as expected.
- **143204 Windows Media Client requests are logged incorrectly**  
The server incorrectly reports a status code of 0 rather than the expected 200  
The above-described condition has been corrected. The server properly logs the expected status code.
- **166738 Status 404 (file not found) errors not logged in access log from QuickTime player**  
The server's rmerror log file reports "Error retrieving URL" message. The log should include proper status code, which in this case is 404.  
The above-described condition has been corrected. The server properly logs the expected status code.
- **170865 Unexpected 408 errors - Connection refused, too many connections**  
Under certain load conditions the proxy would enter an erroneous condition causing it to report client connections count exceeding that of the license file.  
The above-described condition has been corrected. The proxy no longer enters a state causing it to report an invalid client count.
- **175954 Helix Server Configuration Guide error**  
The example of a variable setting on page 156 is incorrect:

Shows: <Var Disable3GPPKeyframeDetection="1">  
Should be: <Var Disable3GPPKeyframeDetection="1"/>

The Server Configuration Guide has been updated with the appropriate correction.

- **175190 Incorrect SNMP MIB values returned**

The incorrect values are returned with the following variables:

```
hsUDPTransports (.1.1.5 & .1.1.6)
hsPercentCPUUsage
clientRequests
clientRequestsSuccessCount
clientsLeaving.
```

The above-described condition has been corrected.

- **176500 Server does not release connections, triggers Crash Avoidance and restarts**

A race condition with the Administration UI Server Monitor was causing the server not to release connections.

This issue has been fixed.

- **177358 Cannot redirect output of the master command to a log file**

Commands such as `./Bin/master master.cfg > master.log` would not capture output as expected. The resulted files contained no data.

This issue has been fixed. The output redirection now functions as expected.

- **177553 Server statistics for Free Pages Outstanding & Overhead becomes inaccurate under certain conditions**

Negative values for Memory Allocation Overhead appear in the rss logs. In the case of allocation of big pages of size more than 1 MB, free page outstanding was not getting decremented and hence the observed behavior.

The fix corrects the above mentioned counter and all related calculations are now correct.

- **177728 Server leaves RTSP session open, and unresponsive after issuing Server Alert in response to bad DESCRIBE request**

Under certain conditions the TCP connection is still active, but the server is non-responsive to further RTSP requests.

The above-described condition has been corrected.

- **180912 RMERROR.LOG shows UNKNOWN instead of milliseconds for each entry**

The date timestamp is missing the milliseconds and puts UNKNOWN instead. This should be filled in with the number of milliseconds or nothing if not supported.

This issue has been fixed. The server now logs expected values.

- **182056 HTTP Content-length of ZERO causes client connection failure**

Server is treating Content-Length Zero in HTTP header as an invalid value. The result is a client connection failure and a Crash Avoidance on the server.

The above-described condition has been corrected.

- **182153 Strange URL recorded in RMACCESS.LOG precedes a failed client playback**

The URL in question has the following syntax: `miicache/{IPADDRESS}:554/conv-test/02/longfile.3gp` or this `rtsp://{IPADDRESS}:554/conv-test/02/longfile.3gp`. This issue was caused by faulty client disconnect handler. It has been corrected and the logs now reflect the expected URL.

- **183958 When using RDT as the transport to stream mp4/3gp files, seek fails beyond certain time**  
Around 4 minutes 30 seconds the failure manifests itself in a form of a video freeze, however audio continues to play fine.  
This issue has been fixed. The above described condition no longer appears.

## 7.6 Listed Issues Fixed as part of v11.1.1

- 151545 SDP files in sub-folder of `/rtpenodersdp/` fail to be primed on server  
The behavior was initially determined as by design. New implementation now allows for priming of sub folders of the `/rtpenodersdp/` directory.
- 154092 Windows Media client connections show multiple "New players" in server's log file  
This is by design. Windows Media Players establish and then tear down two RTST connections to the same server on port 554 before attempting MMS connection on port 1755.
- 155842 Startup.log doesn't contain date/time when server was started  
Issue has been resolved. The logs now contain startup time and date.
- 159274 Content accessed from Helix or Windows Server using MMS protocol fails to stream via Helix Proxy  
Problem has been caused by truncation of MMS response from the Player on the proxy. Issue is fixed.
- 165119 Windows Media content streams audio only when accessed via HTTP  
Problem was caused by the server reading stream number in decimal rather than in hex. This has been fixed.
- 165813 Helix Mobile Client rebuffers when streaming from Server v11  
Problem was caused by variations in units of measurement used by various mobile clients. Addition of a new configuration variable "LinkCharMultiplier" to the User Agent corrects the behavior.
- 166333 URL Alias function fails with live rtp content  
Issue was related to the URL aliasing literally replacing an alias of i.e. "/t0" with original value for mount point of i.e. "/", resulting in a link of `"/rtpenoder/live.sdp"` passed to the rest of the system.
- 166361 Proxy keeps connection open to Helix Server for Windows Media content  
Playing windows media content resulted in a leak, which then caused the connections to remain in an open state. This has been resolved.
- 166673 Unable to play from Windows Media server WM content via Helix Proxy using RTSP  
Problem was related to proxy's failure to parse control lines inside an SDP file. This has been fixed.
- 166694 MMS server response forwarded to client through proxy is truncated – client disconnects  
This has been corrected. Truncation no longer occurs and therefore the clients do not get disconnected.
- 167254 Server Crash Avoidance caused by DESCRIBE method on Solaris 10 platform  
Issue due to difference in how Solaris 10 vs other Unix systems handle certain function calls. Issue has been fixed.

- 167421 Missing date and time from the startup.log  
Problem with missing time and date stamp have been corrected.
  
- 167431 Server erroneously allows two Helix Mobile Producer connections on the same port range  
The Server now recognizes the different IP address that the sdp comes from and creates a separate stream objects for each. This enables having multiple encoders using the same port address but without conflicts. This functionality however has some limitations. For example, if the encoders are behind the same NAT server, they would appear to have the same IP address. Thus, if there's more than one encoder behind a NAT-Server, then if both try to use the same port, the server would not be able to differentiate between the different streams and would just send all incoming packets as part of the same outgoing stream.
  
- 167761 Authentication failure when using NTLM features of the Server  
Problem was due to a broken functionality. Issue has been resolved.
  
- 168133 SLTA stops at end of 3GPP (mpeg4 & amrnb) hinted content created with Helix Mobile Producer  
Problem caused by incorrect internal messaging indicating stream failure rather than stream completion. This has been resolved.
  
- 170686 Windows Media video playback from Helix Server 11.1 fails on certain SunOS 5.8 machines  
Problem caused by outdated patch level. To correct the problem ensure that the latest patches are applied to the Solaris 5.8 operating system.
  
- 171329 Server 11.1 generates Crash Avoidance every couple of minutes or less  
Problem was caused by streaming unhinted 3gpp2 content encoded with QCELP codec for the audio stream. This codec is currently not supported by the Helix Server. Fix consists of the server returning an error code 415 (Invalid File).
  
- 175062 Very large memory allocation in mobile RSD live  
Issue caused by an outdated memory management code. This has been fixed.

## 8. Known Issues

Below is a summary of known issues in functional and stability areas of the Helix Mobile Server 11.1.3 and Helix Mobile Gateway 11.1.3.

### 8.1 Windows Media Player 11 With Helix Server

Windows Media Player 11 no longer requests media using the MMS protocol. When it encounters an MMS URL for on-demand or live content on Helix Server, the player attempts to access the clip in the following order:

1. The player first requests the stream over HTTP, issuing an HTTP request in one of two possible ways:
  - If the MMS URL explicitly contains an MMS port number, the player directs the HTTP request toward that port on Helix Server. In this case, the request fails because Helix Server does not listen for HTTP requests on its MMS port. The standard port used for MMS on Helix Server is 1755.
  - If the MMS URL does not provide a port number, the player directs the HTTP request toward Helix Server port 80. If Helix Server uses port 80 for HTTP, the request succeeds and the server delivers the stream as cloaked MMS. If the server does not use port 80 for HTTP, however, the request fails.
2. If the HTTP request fails, the player sends an RTSP request to Helix Server port 554, the standard RTSP port. This request always fails regardless of the RTSP port that Helix Server uses. This is because Helix Server does not support the streaming of Windows Media content over RTSP.

#### Supporting Windows Media Player 11

You can update your streaming media system to provide Windows Media Player 11 with an alternate HTTP URL whenever it requests an MMS URL. The HTTP URL will contain the appropriate Helix Server port number for the player's HTTP request. Once the player makes the HTTP connection, Helix Server delivers the stream as HTTP-cloaked MMS.

Note that the HTTP connection used to deliver cloaked streams to Windows Media Player 11 is **not** managed the same as HTTP requests from browsers. You therefore do **not** need to add the mount points under which the Windows Media content resides to the HTTPDeliverable list in the Helix Server configuration file. The content is delivered only to the media player, and is protected against browser caching and user download.

Updating your system requires the following actions:

- Modify an existing Helix Server configuration value for the ASXgen utility. This causes Helix Server to provide an alternate HTTP URL to any Windows Media Player that requests an MMS URL.
- Update any .asx files linked to Web pages to include an alternate HTTP URL.

#### Modifying ASXgen

ASXgen is a Helix Server utility for launching Windows Media Player from a Web page link. Helix Server is configured with a mount point named /asxgen/, which you add to a Web page link for Windows Media content. For example:

```
<a href="http://helixserver.example.com:8080/asxgen/video.wmv">Play Windows Media</a>
```

When Helix Server receives an HTTP request that contains the /asxgen/ mount point, it sends a MIME stream that causes the browser to launch Windows Media Player. This MIME stream instructs the player to contact Helix Server on its MMS port, and explicitly provides the MMS port number (typically 1755). To support Windows Media Player 11 for on-demand and live streams, you configure ASXgen to provide an alternate HTTP URL along with each MMS request. This alternate URL includes the actual HTTP port number used by Helix Server. After the initial MMS URL returned by ASXgen fails, Windows Media Player 11 requests the stream using the alternate HTTP URL.

- To configure ASXgen to Support Windows Media Player 11:

1. Using any text editor, open the Helix Server configuration file (rmserver.cfg). This file resides in the Helix Server main installation directory.

2. Find the ASXgen configuration list and variables:

```
<List Name="ASX File Generator">
<Var ShortName="pn-asxgen"/>
<Var MountPoint="/asxgen"/>
<Var HaveAltHTTPURL="0"/>
</List>
```

3. Enable the HaveAltHTTPURL variable by setting its value to 1:

```
<Var HaveAltHTTPURL="1"/>
```

**Note:** Beginning with Helix Server maintenance release 11.1.2, the HaveAltHTTPURL variable is enabled by default.

4. Save and close the configuration file. A Helix Server restart or a "kill -HUP `cat ./Logs/rmserver.pid`" command is required unless the modification is done through the Admin page (see below).

- To make the change from "HaveAltHTTPURL=0" to "HaveAltHTTPURL=1" without any restart can be done through the Helix Administrator page. The setting can be found in "Server Setup/Ports" as "Enable HTTP Fail Over URL for ASXGen" – where it can be changed from "No" to "Yes." Finally clicking on "Apply" enables the new setting.

### Updating ASX Files

If you direct Windows Media Player to MMS streams using ASX files, you can update the files to include an alternate HTTP URL. Simply add a second REF entry to the same content, using an HTTP URL that indicates the Helix Server HTTP port number. For example:

```
<ASX Version = "3.0">
<ENTRY>
<Ref href = "mms://helixserver.example.com:1755/wmvideo.wmv"/>
<Ref href = "http://helixserver.example.com:8080/wmvideo.wmv"/>
</ENTRY>
</ASX>
```

**Note:** Updating ASX files is not required only if the MMS URL in each file does **not** contain an explicit MMS port number and your Helix Server uses port 80 for HTTP connections.

### Using a Proxy

Windows Media Player 11 does not provide an option to use an MMS proxy. Instead, its player preferences contain options to use an HTTP proxy and an RTSP proxy:

- For the HTTP proxy, you can select any HTTP proxy available to you. You cannot use Helix Proxy, however, because Helix Proxy does not proxy any media using HTTP.
- For the RTSP proxy option, you can specify Helix Proxy. Note the following, however:
  - Because Helix Server does not support Windows Media over RTSP, Helix Proxy cannot proxy any Windows Media content residing on Helix Server for Windows Media Player 11. Streams originating from Helix Server can be delivered only by an HTTP proxy as HTTP-cloaked MMS.
  - Helix Proxy can proxy on-demand and live, RTSP-based Windows Media streams originating from a Windows Media Server. However, all streams are delivered in pass-through mode only. Helix Proxy does not cache on-demand clips or split live streams.

## 8.2 MDP and QuickTime playback of mobile content

Any content created with Final Cut Pro and then hinted with QuickTime Pro results in poor playback when streamed from Helix server with MDP enabled. During some tests, it was noticed that the DLSR (Delay Since Last Sender Report) values reported by QuickTime player in RTCP Receiver reports appeared larger than expected. A bug report has been filed with Apple.

A H264 content created with Final Cut Pro and then hinted with QuickTime Pro also results in a poor playback when streamed from Helix server. This is because the encoder doesn't seem to be packetizing the content and the Helix server does not have H264 packetizer. However, H264 content created with Helix Mobile Producer does not exhibit such issues during playback.

## 8.3 Alternate Mount Point

Alternate Mount Point with same (duplicate) List Name does not log an error in Error.log

Alternate Mount Point feature can be configured via the configuration file only. Currently there's no GUI interface for this function.

## 8.4 Broadcast Redundancy

When sending a live feed to the Helix Server, if the filename has multiple dots in it then broadcast redundancy generates multiple alternative files available. This means that one live feed being sent in is duplicated hundreds of times (depending on the number of dots in the original filename).

## 8.5 Content Distribution

If no default "/" Mount exists, Cdist still looks in "/" for files

If no "/" mount point exists in the rmserver.cfg and Cdist is configured, the Content subscriber sends the wrong URL to the Content publisher when looking for content and therefore returns a "404 - File Not Found."

Explanation: The default mount point must always exist in order for the feature to work as designed.

## 8.6 3GP Compliance

Bandwidth of RTCP RR/SR exceeded XXbps limit

Under certain conditions the RTCP sender and receiver reports indicate that the bandwidth limit setting of 5000bps has been significantly exceeded.

Explanation: This would degrade the quality of the stream if there was insufficient capacity in the channel to handle the extra 2 kbps but otherwise would not have any negative impact. The most likely result would be for the rate manager to lower the bit rate if the stream was multi-rate and the player supported rate adaptation. Otherwise, end-users may experience rebuffering. This issue is to be addressed in the next major release.

## **8.7 Admin System**

Clicking on some pages of the Helix Admin System will cause extraneous 404 errors in the server's logs  
Changing the Transmitter Source name in the Admin System requires a server restart for the change to take effect, however the Admin System will not notify the user that this is required. The Quicktime sample clip will not play if the link is clicked in the Admin System.

## **8.8 Content Browser**

Content browsing feature doesn't work through admin UI in version 11.1.2.  
Restricting Content Browsing to specific extensions does not function  
Directories in the Content Browser windows are improperly displayed as files

## **8.9 Delayed Shutdown**

Disabling "Allow New Client Connections" will not keep new clients from connecting when a Delayed Shutdown of the server is in progress.

## **8.10 General**

System time changes of more than a few seconds while the server is running, and particularly while the server is under load can cause severe memory leaks and potentially restarts. This sort of system time change may be triggered by NTP services, daylight savings changes, or simply by manual date/time changes. We recommend disabling these sorts of services on systems running Helix Mobile Server and Helix Mobile Gateway, and that time adjustments be made during server down times, or times of low load.

## **8.11 Java Monitor**

Bandwidth Usage is not recorded for 3GP Live streams being played.

## **8.12 Redundancy and HTTP with Windows Media Content**

"LiveEncoder Redundancy" does not work with Live feeds from Windows Media Encoder (due to the fact that Windows Media Player v11 is now the standard which only allows HTTP connections to Helix server for content).

## **8.13 Multicasting of Windows Media Content**

Starting the multicasting without using Windows Media Encoder causes Crash Avoidance on server. Access with administrative rights is necessary in order to encounter this issue. The following example list the necessary reproduction steps:

1. Configure Windows Media Encoding & Windows Media Multicasting as per the Admin Reference Guide (Page no.180)
2. Click on Broadcasting
3. Click on Windows Media Multicasting.
4. Click on Stop Transmitting Check box.
5. Kill the Windows Media Encoder.
6. Make Enable Broadcast as a Yes & Click on Apply. It will start Transmitting Channel.
7. Again click on the Stop Transmitting Check box.
8. After few seconds the server will generate Crash Avoidance instances.

## 8.14 Logging

Superfluous error message: "couldn't lookup session for channel <0x1>" is getting written to the error log

## 8.15 Multicast

When configuring Scalable Multicast, "VirtualPath" values cannot be numeric only; "2" won't work, but "2a" will.

## 8.16 Proxy

Proxy does not support Caching or Splitting for scenarios where Proxy Routing is used.

## 8.17 Rate Adaptation

When MDP is enabled, and you are using TCP Limirate, the server has a tendency to over send data. The higher the bitrate, the more it will over send. You can compensate for this by increasing the MaxBurst size variable on the server when streaming at higher bitrates until the margin of error is within acceptable limits.

## 8.18 Reduced Startup Delay

Setting the variable "CPUThresholdToDisableRSD" to 100 will roll the value back to the default of 65; 99 is the highest value the system will recognize.

## 8.19 SNMP

The SNMP v1 user name must be set to "public" for traps to function properly

The Trap Interval value has no effect

The Master Agent doesn't return an error message if it is started with an invalid configuration

The Master Agent doesn't return an error message if authentication information is invalid

The Master Agent prints an error when starting without a community string being configured; this error message should be ignored

Setting the trap values for CPU or MaxConnections to zero doesn't disable these traps; you must set them to a value which is high enough that it won't be reached

ServerStart trap is never sent

## 8.20 Windows Media Support (non-WMP 11 related)

Windows Media 9 live streams won't work if hosted from SLTA

Windows Media Player will sometime give an error when attempting to connect to the server using ASXGen

Windows Media Push Splitting fails if setup to use TCP on an IPv6 network

Windows Media streams fail to connect to the Helix Mobile Gateway via an IPv6 network

Windows Media clips will not play properly if clicked on in the Content Browsing window

There are various logging errors, which occur when playing MMS through the Helix Mobile Gateway

## 8.21 Stopping SLTA results in Segmentation Fault

Stopping the SLTA with Ctl-C results with segmentation fault. No other side effects are observed.

## 8.22 Crash Avoidance Issues (CAs)

When using a Parent and Child Proxy routing setup, the Parent proxy CAs on RTSP request.

Adding a Scalable Multicast channel through the Admin System will cause a CA

Requesting a MMS stream through the proxy will cause the proxy to CA

CAs occur on certain types of connection attempts with the Sony Ericsson P900 and the Nokia 6630

## **8.23 Handset Specific Issues**

Sony Ericsson P900 renders 3GP content at the incorrect speed

## 9. Checksum

MD5SUM	File Name
c3f4ef71450b747fa9682ecb5fd8a436	mbgw1117-ga-linux-rhel4.tar.gz
1b3b04d08a0b8b13bd5e360f334b55b7	mbgw1117-ga-solaris-8.tar.gz
919a5a67356015c87f4b263204f02b42	mbgw1117-ga-win32.zip
a0b5abc75e0d73e054ca5754e39a08bb	mbrs1117-ga-linux-rhel4.tar.gz
db410d028789718a42c42b5312c66863	mbrs1117-ga-solaris-8.tar.gz
19cf0471a878705c1a9f191dc5705961	mbrs1117-ga-win32.zip