

# Helix Security Manager

## Secure Your Digital Media Files

### Enable enterprise web applications to control access to streaming and downloaded media content.

Helix Security Manager leverages ticketed URL technology to integrate managed media access with an enterprise's existing end-user authentication and authorization systems. It controls access to streaming or downloaded content served by Helix Universal Media Server family, Helix Proxy, and Apache or Covalent web servers and proxies.

### Key Benefits

- Integrates Media Servers into Enterprise Web and Mobile Applications**  
 More robust and flexible level of access control than username and password, less complex and easier to deploy than digital rights management (DRM), enables web-based single sign-on security.
- Allows Client-Access Control**  
 Control client connections and disconnect based on business rules.
- Supports Multiple Devices**  
 Controls access to content on PCs, PDAs and mobile phones.
- Supports Multiple Delivery Methods**  
 Controls access to digital content streamed or downloaded via the Helix Universal Media Server or downloaded via an HTTP server.
- Supports Multiple Media Formats**  
 Controls access to all formats supported by the Helix Universal Media Server and HTTP servers.
- Cross-Platform**  
 Available for Windows, Linux and Solaris.

### How Helix Security Manager Works

Helix Security Manager provides media access security and fraud protection by attaching and validating a token hash to each content URL presented by enterprise web applications. The token supports a series of parameters including hash token key timeout and content playback duration (lifetime) to prevent media URLs from being shared in an unauthorized way and to provide better control over media assets. To accomplish this, Helix Security Manager enables the following media access process:

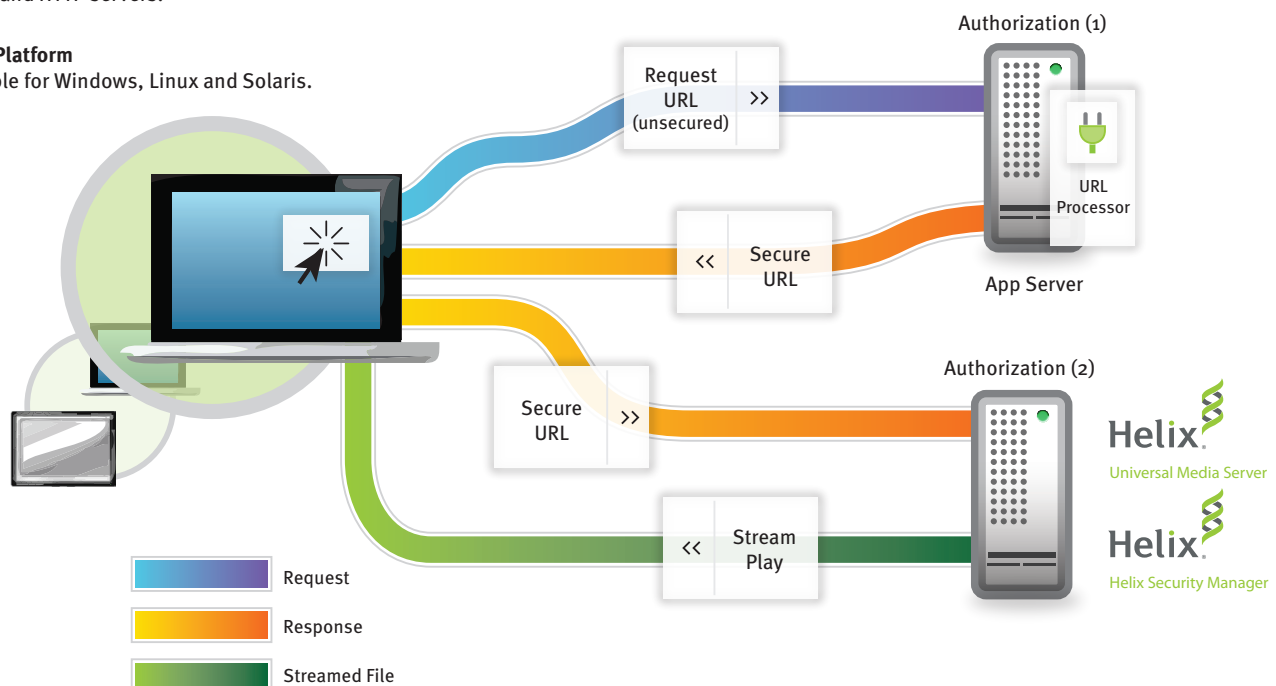
**Step 1:** The web portal authenticates the end-user for a given request for a Media URL.

**Step 2:** The portal passes the Media URL to the backend URL processor along with parameters governing the access granted.

**Step 3:** Helix Security Manager uses a token value to generate a Ticketed URL. The Ticketed URL is returned to the portal and then to the end-user's browser.

**Step 4:** The end-user's browser launches the appropriate media player which makes a request to the Helix Universal Media Server or HTTP server for the Media asset using the Secure URL.

**Step 5:** The request is submitted to the Helix Universal Media Server Security Adapter. The Security Adapter validates the Ticketed URL. If the Ticketed URL validates, and it is not expired, the end-user is delivered the requested media file.



## Product Features

Helix Security Manager consists of two components, Security Manager and Security Adapter.

### Helix Security Manager

- Dynamically generate secure URL media access tickets
- Per-URL Configurable Lifetime
- Per-URL Token Timeout
- Configurable URL Parameters
- MD5 and SHA-1 Message Digest Encryption

### Helix Security Adapter

- Reject unauthorized or expired keys
- Bypass - Allow secure and non-secure content on a single server. Content can either be secured by default and only unsecured content is bypassed by regular expression matching by content location or vice versa.
- External Allowance - Dynamically authenticate unsecured requests directly to the Security Adapter against an external system
- Configurable Error Handling - Handle exceptions by any of the following means:
  - Custom error string
  - Redirect client to alternate HTTP or RTSP resource
  - Dynamically determine which of the above actions to take by invoking an external system
- Logging - Log Authentication attempts into an Authentication Log file
- Log Rolling - Set the log roll size via configuration file
- IP Address Verification - Verifies that the IP Address of the client requesting the secure URL from the Security Manager is the same as client receiving authenticated by the Security Adapter

Note: You will need to purchase additional copies of Helix Security Adapter if you would like to manage more than one media server.

## Specifications

### Helix Security Manager

- Media Servers: Helix Universal Media Server v14 Series
- Operating Systems: Windows Server 2003 and 2008; Linux – Red-Hat Enterprise Linux 5.x; Oracle Solaris 10.x
- Java Virtual Machine: Sun J2SE SDK 1.6.x or later
- Java-EE based application server: Apache Tomcat v6.x or later (recommended), jBoss v5.x or later

### Helix Security Adapter

- Media Servers: Helix Universal Media Server v14 Series or Helix Proxy Server v14 Series
  - Operation Systems: Windows Server 2003 and 2008, Linux – Red-Hat Enterprise Linux 5.x and Oracle Solaris 10.x

## About the Helix Media Delivery Platform

The Helix Media Delivery Platform is an end-to-end streaming media solution for government, education and enterprises that is multi-format, multi-platform, and multi-screen. With Helix Producer, Helix Universal Media Server, Helix Media Library, and Helix Enterprise Player – the core components of the platform – organizations can create, deliver, manage and playback content. Created by RealNetworks, the company that pioneered streaming media in 1995, Helix products provide a high-quality, scalable digital media experience. And with Helix's global customer support team, assistance is just a phone call or email away.

## Contact Us

Contact a Helix Sales Representative at 800.444.8011 or [helix-sales@realnetworks.com](mailto:helix-sales@realnetworks.com). To learn more about the Helix Media Delivery Platform, visit [www.realnetworks.com/helix](http://www.realnetworks.com/helix).