



Helix™ Security Manager

Secure Your Digital Media Files

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

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.
- **Supports Multiple Devices:** Controls access to content on PCs, PDAs and mobile phones.
- **Supports Multiple Delivery Methods:** Controls access to digital content streamed via the Helix Server or downloaded via an HTTP server.
- **Supports Multiple Media Formats:** Controls access to all formats supported by the Helix Server and HTTP servers.
- **Cross Platform:** Available for Windows, Linux and Solaris.

How Helix Security Manager Works

The 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, the Security Manager enables the following media access process:

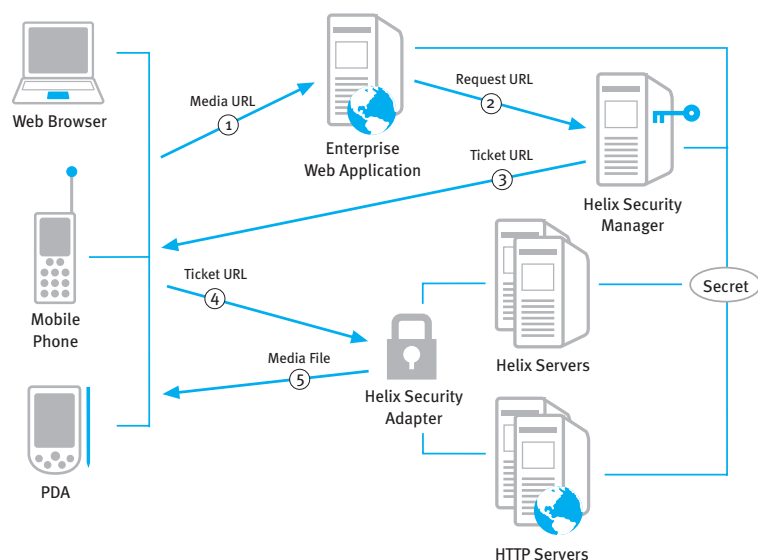
Step 1: The web portal authenticates the end-user for a given request for a Media URL. The web portal allows the end-user access to the Media URL.

Step 2: The portal passes the Media URL to the Helix Security Manager along with parameters governing the access granted.

Step 3: The Security Manager uses a token value to generate a Ticket URL. The Ticket 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 Server or HTTP server for the Media asset using the Secure URL.

Step 5: The request is submitted to the Helix 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.



Feature Specifications

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.

System Requirements

- Media Servers: Helix Server Unlimited v.11; Helix Mobile Server v.11
- HTTP Download Servers: Covalent Enterprise Ready Server 2.4; Apache HTTP Server 2.0
- OS: Windows 2003 Server; Red Hat Enterprise Linux 4; Solaris 8; Solaris 9
- Java Virtual Machine: Sun J2SE SDK 1.4.2

Contact Real Today

To learn more about Helix Security Manager, please contact a Real sales representative at **1-800-444-8011** or visit www.realnworks.com/products/security/hsm/index.html

