Note that content by Rachael Stavchansky starts at Security features for HLS streams using Wowza CDN on Akamai. The Fastly content was added later.

Wowza Player, Wowza GoCoder SDK, & the technology powering the Ultra Low Latency service in Wowza Streaming Cloud will no longer be available August 31, 2021. Learn more.

Security features in Wowza Streaming Cloud

Originally Published on 08/29/2018 | Updated on 03/23/2021 12:13 pm PDT

The Wowza Streaming Cloud™ service provides a range of security features that allow you to protect the delivery of and access to a stream as it moves from camera or source encoder to the transcoder, from the transcoder to a stream target, and from the stream target to a player. You can also limit access to playback based on geographic location or by using AES-128 encryption or token authorization. Slightly different security features are available for Wowza Streaming Cloud HLS streams that run through Wowza CDN on Fastly stream targets and streams that run through Wowza CDN on Akamai stream targets. Ultra low latency streams also have access to a subset of security features.

This article outlines which security features are available for different types of streams. It also points to step-by-step instructions for implementing the security features using the Wowza Streaming Cloud REST API or the Wowza Streaming Cloud user interface.

Contents

Security features for HLS streams using Wowza CDN on Fastly

The following features are available to secure an HLS stream that uses Wowza CDN on Fastly stream targets in Wowza Streaming Cloud.

User authentication for source connection on Fastly

User authentication for HLS streams provides a secure connection from the source encoder or camera into the ingest origin server and prevents third parties from connecting to and altering your stream. When user authentication is enabled on a push stream, Wowza Streaming Cloud requires the source encoder or camera to use a username and password associated with the stream to establish a connection. You can set the username and password values, or you can have Wowza Streaming Cloud generate values for you. You can also configure user authentication on a pull stream so that the source encoder or camera uses values set on the encoder side to connect to a live stream or transcoder in Wowza Streaming Cloud.

See these articles to configure user authentication for streams using Wowza CDN on Fastly targets:

- Manage user authentication for HLS streams with the Wowza Streaming Cloud REST API
- Manage user authentication for HLS streams in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

SSL for playback on Fastly

After Wowza Streaming Cloud transcodes (or passes through) encoded live source video, it passes the video stream through stream targets. Those targets deliver the stream to viewers, such as through a hosted webpage or a direct playback URL.

Secure Socket Layer (SSL) can provide secure and encrypted HTTPS connections as a stream moves through the network connections from stream targets to playback destinations. When a specific stream target property is enabled, Wowza Streaming Cloud uses SSL to establish a handshake for encrypting HTTP connections. For streams using Wowza CDN on Fastly targets, you can choose to deliver streams to players for playback using SSL and require the player client to use HTTPS for playback.

Encrypting connections between servers and clients using SSL and HTTPS prevents data from being intercepted and manipulated in transit and prevents third parties from altering a stream as it moves between servers. As of 2018, certain browsers warn users against websites with content served over unsecured HTTP connections. Configuring SSL for your HLS streams can help secure streams and avoid browser warnings.

See these articles to configure SSL playback for streams using Wowza CDN on Fastly targets:

- Manage HLS playback over SSL for Wowza CDN on Fastly with the Wowza Streaming Cloud REST API
- Manage HLS playback over SSL for Wowza CDN on Fastly in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

Geo-blocking for playback on Fastly

Geo-blocking through Wowza Streaming Cloud allows you to selectively allow or block access to Wowza CDN on Fastly stream targets to control where a stream can be viewed. You can use geo-blocking to specify which countries or regions are allowed or which countries or regions are blocked. You can also allow streaming at specified IP addresses even if they're within a blocked location.

See these articles to configure geo-blocking for streams using Wowza CDN on Fastly targets:

- Geo-block Wowza CDN on Fastly stream targets with the Wowza Streaming Cloud REST API
- Geo-block Wowza CDN on Fastly stream targets in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

Token authentication for playback on Fastly

Token authentication protects streams using Wowza CDN on Fastly targets by requiring a token, which is hashed and appended to the playback URL, for viewer access. You can use token authentication to make a stream playback URL unavailable after a certain length of time, to limit access to approved IP addresses, to provide content to paying viewers only, or to apply other restrictions. Token authentication prevents playback URLs from being shared by unauthorized links or player hijacking attacks.

See these articles to configure token authentication for streams using Wowza CDN on Fastly targets:

- Protect a Wowza CDN on Fastly stream target with token authentication using the Wowza Streaming Cloud REST API
- Protect a Wowza CDN on Fastly stream target with token authentication in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

AES-128 encryption for playback on Fastly

AES-128 encryption protects streams using Wowza CDN on Fastly targets by requiring devices to provide a matching key before a stream can be played. Wowza Streaming Cloud uses the external method of AES-128 encryption. When you use the external method, encryption keys are delivered to devices from an external URL.

See these articles to configure AES-128 encryption for HLS streams using Wowza CDN on Fastly targets:

- Secure HLS streams with AES-128 external encryption using the Wowza Streaming Cloud REST API
- Secure HLS streams with AES-128 external encryption in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

Security features for HLS streams using Wowza CDN on Akamai

The following features are available to secure an HLS stream that uses Wowza CDN on Akamai stream targets in Wowza Streaming Cloud.

User authentication for source connection on Akamai

User authentication for HLS streams provides a secure connection from the source encoder or camera into the ingest origin server and prevents third parties from connecting to and altering your stream. When user authentication is enabled on a push stream, Wowza Streaming Cloud requires the source encoder or camera to use a username and password associated with the stream to establish a connection. You can set the username and password values, or you can have Wowza Streaming Cloud generate values for you. You can also configure user authentication on a pull stream so that the source encoder or camera uses values set on the encoder side to connect to a live stream or transcoder in Wowza Streaming Cloud.

See these articles to configure user authentication:

- Manage user authentication for HLS streams with the Wowza Streaming Cloud REST API
- Manage user authentication for HLS streams in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

Secure ingest for transfer from transcoder to Wowza CDN

Secure ingest allows you to secure a stream with a query parameter as it passes from the transcoder to the Wowza CDN for delivery over HLS. When Wowza CDN on Akamai ingests the stream from the transcoder, it requires the query parameter for processing. This prevents third parties from overriding the contents of your stream with unwanted content.

To configure secure ingest using the REST API, see Send streams securely to Wowza CDN on Akamai with the Wowza Streaming Cloud REST API.

To enable secure ingest for a Wowza CDN stream target in the user interface, see Add a Wowza CDN on Akamai target for HLS playback.

SSL for transfer from transcoder to stream target and playback

After Wowza Streaming Cloud transcodes (or passes through) encoded live source video, it sends a stream to geographically distributed servers called stream targets. Those targets then deliver the stream to viewers, such as through a hosted webpage or a direct playback URL. Wowza Streaming Cloud uses the HTTP protocol to make these two outbound network transfers.

Secure Socket Layer (SSL) can provide secure and encrypted HTTPS connections as a stream moves through the network connections from transcoder to stream targets and from stream targets to playback destinations. When specific stream target properties are enabled, Wowza

Streaming Cloud uses SSL to establish a handshake for encrypting HTTP connections. You can either choose to deliver streams from transcoders to targets using SSL or to deliver streams to players for playback using SSL, or both. You can also require the player client to use HTTPS for playback.

Encrypting connections between servers and clients using SSL and HTTPS prevents data from being intercepted and manipulated in transit and prevents third parties from altering a stream as it moves between servers. As of 2018, certain browsers warn users against websites with content served over unsecured HTTP connections. Configuring SSL for your HLS streams can help secure streams and avoid browser warnings.

See these articles to configure SSL playback for HLS streams:

- Manage HLS playback over SSL for Wowza CDN on Akamai with the Wowza Streaming Cloud REST API
- Manage HLS playback over SSL for Wowza CDN on Akamai in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

Geo-blocking for playback on Akamai

Geo-blocking through Wowza Streaming Cloud allows you to selectively allow or block access to Wowza stream targets to control where a stream can be viewed. You can use geo-blocking to specify which countries or regions are allowed or which countries or regions are blocked. You can also allow streaming at specified IP addresses even if they're within a blocked location.

See these articles to configure geo-blocking for HLS streams:

- Geo-block stream targets with the Wowza Streaming Cloud REST API
- Geo-block Wowza CDN on Akamai stream targets in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

Token authorization for playback on Akamai

Token authorization protects streams by requiring a token, which is hashed and appended to the playback URL, for viewer access. You can use token authorization to make a stream playback URL unavailable after a certain length of time, to limit access to approved IP addresses, to provide content to paying viewers only, or to apply other restrictions. Token authorization prevents playback URLs from being shared by unauthorized links or player hijacking attacks.

See these articles to configure token authorization for HLS streams:

- Protect streams with token authorization with the Wowza Streaming Cloud REST API
- Protect a Wowza CDN on Akamai stream target with token authentication in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

AES-128 encryption for playback on Akamai

AES-128 encryption protects streams using Wowza CDN on Akamai targets by requiring devices to provide a matching key before a stream can be played. Wowza Streaming Cloud uses the external method of AES-128 encryption. When you use the external method, encryption keys are delivered to devices from an external URL.

See these articles to configure AES-128 encryption for HLS streams using Wowza CDN on Akamai targets:

- Secure HLS streams with AES-128 external encryption using the Wowza Streaming Cloud REST API
- Secure HLS streams with AES-128 external encryption in Wowza Streaming Cloud (Wowza Streaming Cloud user interface)

Security features for ultra low latency streams

The following features are available to secure an ultra low latency stream in Wowza Streaming Cloud during source connection and playback.

User authentication for source connection on pull streams

User authentication for ultra low latency pull streams provides a secure connection from the source encoder or camera into the ingest origin server and prevents third parties from connecting to and altering your stream. A pull stream indicates that Wowza Streaming Cloud pulls your stream from the encoder or IP camera. To configure user authentication for a pull stream, you enable authentication for your source encoder or camera. Wowza Streaming Cloud then uses a source URL you provide to connect to the authenticated source stream and pull it to an origin server for an ultra low latency stream target.

See these articles to configure user authentication for ultra low latency streams:

- Manage user authentication for ultra low latency streams with the Wowza Streaming Cloud REST API
- Manage user authentication for ultra low latency streams in Wowza Streaming Cloud

IP allowlisting for source connection on push streams

For ultra low latency push streams, you can control the connection to an ultra low latency target's origin server by providing a list of IP addresses for trusted sources. Only sources with allowed IP addresses can connect to the ingest origin server, preventing unauthorized sources from connecting to and altering your stream. A push stream indicates that the source encoder or IP camera pushes the stream to Wowza Streaming Cloud.

See these articles to configure IP allowlisting:

- Manage IP allowlisting for ultra low latency streams with the Wowza Streaming Cloud REST API
- Manage IP allowlisting for ultra low latency streams in Wowza Streaming Cloud

SSL for playback

After Wowza Streaming Cloud with Ultra Low Latency receives an ultra low latency stream at an origin server, it sends the stream to playback destinations using a WebSockets (WS) connection. If a backup HLS stream is enabled, the HLS stream moves from the Wowza Streaming Cloud edge server to a playback destination over an HTTP connection. Ultra low latency and backup HLS streams are available over both encrypted WSS and HTTPS connections and unencrypted WS and HTTP connections. To ensure playback over a secure connection for ultra low latency, you can use SSL to embed Wowza Player configured with secure playback URLs into a webpage hosted over HTTPS. These secure playback URLs use SSL to establish a handshake between a server and client to exchange encrypted data over WSS and HTTPS.

Encrypting connections between servers and clients using SSL prevents data from being intercepted and manipulated in transit and prevents third parties from altering a stream as it moves between servers. As of 2018, certain browsers warn users against websites with content served over unsecured HTTP connections. Configuring SSL for playback of ultra low latency streams can help secure your streams and avoid browser warnings.

See these articles to configure secure playback for ultra low latency streams:

- Manage secure playback for ultra low latency streams with the Wowza Streaming Cloud REST API
- Manage secure playback in Wowza Player for Wowza Streaming Cloud ultra low latency streams

Digital rights management

Digital rights management (DRM) technology provides a way, through encryption, for content creators to protect copyrights and unauthorized distribution of their digital media. The Wowza Streaming Cloud REST API provides integration with EZDRM, a third-party digital rights management (DRM) service you can use to protect content from unauthorized viewing.

Currently, Wowza Streaming Cloud supports the following EZDRM key management systems:

- **EZDRM FairPlay Streaming** – Supports HLS playback for content to Apple devices with native support for the HTML 5 player in macOS Safari browsers or Safari 11.3 on iOS.
- **EZDRM Universal** – Supports MPEG-DASH playback for Google Widevine and Microsoft PlayReady devices and platforms using a linked Common Encryption (CENC) key.

See About digital rights management in Wowza Streaming Cloud for more information.

Subscribe

SELECT A LANGUAGE

English ▲

Terms

Privacy

Trademarks

Legal