What end-user information is passed to Kaltura when using eCDN?

Last Modified on 08/06/2020 5:32 pm IDT

When an end-user accesses Mediaspace and plays back a video, the end-user makes 4 connections:

1. To your SSO system (If applicable).
2. To the Kaltura CDN for widgets, player objects, related files, etc.
3. To Kaltura MediaSpace for the actual MediaSpace web application.
4. To the Kaltura Edge Server (KES) for playback of the video assets. The KES then passes the request back to Kaltura's CDN which contains the video asset unique IDs and video segment number.

The end-user data that is sent to the Kaltura cloud in that scenario is as follows:

1. SSO Attributes that you choose to send to the end-user from your SSO system. The user then POSTs it to Kaltura's Mediaspace server who then validates it prior to allowing the user access. These attributes would typically include firstname, lastname, email address, role, and any groups. This is the nature of SSO so that you only send what info you want, and no passwords or sensitive data is passed to our system.
2. The end-user external (public) IP address. If accessing via an office or central datacenter, it would be their public IP address.
3. The end-user Internal IP address when using an eCDN hub-spoke topology. Kaltura uses the end-user Internal IP address to form a "mapping" between the external and internal IP address to identify which sub-office the end-user is located in. Again, picture a hub-spoke topology where multiple offices internet traffic all flows through a central datacenter before reaching the Internet. If you don't have this hub-spoke topology and all offices have independent Internet connections, then Kaltura only needs the external(public) IP address to "enable" the eCDN component.
4. End-user browser information (no different than a typical webpage session).