xtendx®
corporate media solutions

simplex Security Options

Securing content access

contact xtendx:

support@xtendx.com

Table of Content

Introduction

This document presents the different methods of controlling user access to customer video content & metadata.

Standard Authentication Methods

IP Whitelisting

On the application level - and for private clouds on server level - xtendx allows for white- or blacklisting of specifiable IP ranges.

Such rules can be activated for backend-, frontend- and feed/API entrypoints.

Geoblocking

Geoblocking is an IP White- or Blacklisting by region. It allows for regional control of video content delivery even when a CDN (Content Delivery Network) is used. The most important usecase are regionally specific visual/audio/content licenses.

Login & Password

The following basic options exist per project:

- Same Password for all Users
- Same Login & Password for all Users
- Individual Logins & Passwords

Integrative Authentication Methods

LDAP

What stands for Lightweight Directory Access Protocol is a solution for long user lists that can be handed to xtendx over a secure channel. The list contains columns “Username”, “Password”, “Group” (optional). In simplex Pro for each video project, access can be granted/revoked to users and/or groups.

The advantage is easy control of who can access which project. The disadvantage is that the list is static and when a user should be added, changed or removed, a new list import is required.

SAML2

As opposed to LDAP, with SAML2 (Security Assertion Markup Language) the users login credentials are not stored on simplex side but on the customers identity provider (ADFS, OAuth, PingFederate, etc.). This is a Single Sign On Method.

The user - upon visiting a specific video link - gets redirected to and authenticated by the customer's identity provider server and returns to simplex with a specific token containing only Username and Group. With that, the user does not even have to type any password or username, he is automatically logged in.

This method requires a one time modification on the customer's identity provider.

Consult the simplex SAML2 documentation for further informations.

Single Access Token

Single Access Token (SAT) Authentication is a way to control access to specific video projects by installing a token generator on the customer Content Management System. The embedded videos are being appended with those generated tokens. Any such video link has a lifetime defined by the token lifetime after which the link will be unusable.

This allows customers to limit viewership of video projects to the authorized audience of their respective CMS (sub) sites.

With SAT, maliciously extracted URL from the CMS source code will be unusable for third parties.

Consult the simplex SAT documentation for further informations.