Clearlogin - SAML Apps

In This Article

Overview

If an application supports SSO using SAML, you can federate the application with Clearlogin.

If you are unable to find your app in the catalog, you can create a custom SAML app below.

> **SAML** apps require a tight integration with the SSO application and Clearlogin. Additionally, each application vendor implements the SAML protocol in different ways. However, with that said, we will try to cover all of the possible settings required for a successful integration.

Steps to Add a SAML App

- Sign into the **Clearlogin Admin Console:** https://admin.clearlogin.com
- In the left navigation bar, browse to: **Apps**
- Click on the **New App Connection** button
- At the bottom of the page in the **Custom Connections** section, select the **SAML** App

- Using the below tables as a reference to enter the required information, and then select **Create SAML App**
- After saving the SAML application, the summary page will contain the public portion of the signing certificate, which needs to be imported into the SAML application.

The below table describes the different properties included in the signing certificate. To view the specifics of the signing certificate created by Clearlogin for your SAML application, paste it into this certificate decoder: https://www.sslshopper.com/certificate-decoder.html

Certificate Property	Description
Common Name	This will be the URL to your Clearlogin tenant. Ex: https://companyName.clearlogin.com
Organization	Clearlogin
Locality	Westfield
State	New Jersey
Country	US
Validity Period	3 Years
Issuer	https://companyName.clearlogin.com, Clearlogin
Serial Number	A randomly generated ID

SAML APP Connector Settings

General Settings

Setting Name	Description
Display Name	This name will be shown at the bottom of the app tile in the user's dashboard.
Icon	Upload a custom image file, which will be used in the app tile in the user's dashboard.
Accepted Access Tags	Bookmark apps support multiple access tags to allow different sets of users access to the web site. Choose the access tags that you would like to allow access to this App Connection. • If you leave this blank then all users will be given access. • If you choose Nobody, then it will not be shown on the user dashboard. For more information on Access Tags, refer to the **Clearlogin Applications** article.
MFA Access Tags	SAML apps can be configured with per-application MFA. This means a user will need to go through the MFA process when they click on the app tile in the user dashboard. Choose the access tags that you would like to trigger an MFA prompt. • If you leave this blank, all users will be prompted for MFA. • If you choose Nobody, then no users will be prompted for MFA. For more information on Access Tags, refer to the **Clearlogin Applications** article.
MFA Duration	The length of time to wait after a user has launched an app to prompt for MFA. • 24 Hours (default)

URL Settings

Setting Name	Description
Login URL (ACS)	This URL is specific to, and provided by, the SAML application. It is known as the Service Provider ACS (Assertion Consumer Service) URL, and is the URL Clearlogin will send the SAML Assertion (token) to.
Logout URL (SLO) (Optional)	This URL is specific to, and provided by, the SAML application. It is known as the Service Provider SLO (Single Log Out) URL, and is the URL that users can navigate to for terminating their session in the SAML application.
App URL Override (Optional)	For SP-Initiated login fill in this value with your Service Provider's URL that will begin the SSO process by sending a SAML Request to Clearlogin. Leave this blank for IdP-Initiated login and Clearlogin will send a SAML Response directly to the Login URL.

Audience

Setting Name	Description
Audience Restriction	If necessary, this URL is specific to, and provided by, the SAML application. If it is not necessary, leave it blank, and Clearlogin will fill this field first with the Audience from the SAML request and second from the Login URL (ACS).
NameID Value	This is the primary identifier for the username included in the SAML assertion (token). Attribute Placeholders can be used within this field. • Default is the user's email address in their Clearlogin User Profile: {{cl.email}}

NameID Format	This is the supported format that the SAML application (Service Provider) expects the NameID to follow. Clearlogin supports the following NameID formats: • Use Request Format (default) - Clearlogin expects the SAML application to provide the NameID format • urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified • urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress • urn:oasis:names:tc:SAML:2.0:nameid-format:persistent • urn:oasis:names:tc:SAML:2.0:nameid-format:transient
SAML Namespace	Determines the SAML namespace to use in the signed XML Assertion document. Most SAML applications support the SAML 2 namespace. If so, it is recommended to change the drop-down to SAML2. Otherwise, leave it with the default SAML namespace. • SAML (default) • SAML2

Attributes

Attributes are the keys and their associated values that you would like to include in the data sent for authentication. Attribute Placeholders can be used within the value field. See the below SAML Attribute Placeholder Examples section for attribute placeholder examples.

Setting Name	Description
Add Attribute	Use the add attribute button to add a new attribute using a Key/Value pair. The key will be the attribute's name, and the value would be the attribute's value. If you don't add any attribute placeholders, the following are used by default from the user's Clearlogin User Profile: • Name: {{cl.name}} • Email: {{cl.email}}
Attribute Format	Indicates to the application how to interpret the attribute names. • urn:oasis:names:tc:SAML:2.0:attrname-format:basic (default) • urn:oasis:names:tc:SAML:2.0:attrname-format:uri • urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Minify XML	Enable this setting to compress the size of the XML sent by Clearlogin to the application. Do not enable this setting if the SAML application does not support XML compression. • Enabled • Disabled (default)

Signing Certificate Properties

Setting Name	Description
Digest Method	This is the hash algorithm used to generate the digital signing certificate, which is used to sign the XML SAML assertion (token) for authentication. If you change the digest method you will need to generate a new certificate in Clearlogin and update the SAML application with the new certificate. • SHA256 (default) • SHA1 (not recommended)
Canonicalization Algorithm	The standard used when generating the digital signing certificate. It is recommended to leave this at the default unless the SAML application does not support the #WithComments properties. • http://www.w3.org/2001/10/xml-exc-c14n#WithComments (default) • http://www.w3.org/2001/10/xml-exc-c14n#

Additional Settings

Setting Name	Description
Debug App	Enables or disabled debug logging. Enable this to view logs for troubleshooting purposes. • Enabled • Disabled (default)
Enabled	This will enable or disable the app. When it's disabled, it will not show on the user dashboard. • Enabled (default) • Disabled
Admins Only	When selected, only user accounts assigned the admin role will see the app on the user dashboard. • Enabled • Disabled (default)
Hide on Dashboard	When selected, the app will be hidden from the user dashboard. • Enabled • Disabled (default)

SAML Attribute Placeholder Examples

In addition to hard coded values, you can use the below example Attribute Placeholders to populate fields with information from the authenticating user.

Expand to view examples for each attribute placeholder type.

These are the available placeholders for attributes in your Clearlogin tenant account.

Attribute Placeholder	Description
{{tenant.domain}}	Your configured domain name.
{{tenant.account_id}}	Your configured Account ID.

These are the available placeholders for Clearlogin User Profile attribute placeholders.

Attribute Placeholder	Description
{{cl.email}}	The user's email address
{{cl.username}}	The user's username
{{cl.name}}	The user's name
{{cl.first_name}}	The user's first name
{{cl.last_name}}	The user's last name
{{cl.role}}	The user's Clearlogin role
{{cl.access_rules}}	The user's Access Rules
{{cl.avatar_url}}	URL to the user's Clearlogin avatar

{{cl.tenant_domain}}	The user's configured domain name
{{cl.lockout}}	Whether the user is locked out
{{cl.openid_uid}}	The user's OpenID user id
{{cl.transient}}	A random unique identifier
{{cl.persistent}}	A calculated per-user unique identifier
{{cl.last_sign_in_at}}	Date last signed in at
{{cl.last_sign_out_at}}	Date last signed out at
{{cl.ossmosis_user_id}}	The user's Ossmosis user id. Defaults to Clearlogin username/email.

These are some of the available placeholders for user attributes provided by your Active Directory (LDAP) identity sources.

Attribute Placeholder	Description
{{ldap.mail}}	The user's email address
{{ldap.sAMAccountName}}	The user's username
{{ldap.userPrincipalName}}	The user's user principal name (UPN)
{{ldap.uid}}	The user's login id
{{ldap.cn}}	The user's canonical name
{{ldap.gn}}	The user's given name (first name)
{{ldap.sn}}	The user's surname (last name)
{{ldap.dn}}	The user's distinguished name
{{ldap.distinguishedName}}	The user's distinguished name
{{ldap.memberOf}}	The user's groups
{{ldap.ou}}	The user's organizational unit
{{ldap.lastLogon}}	Timestamp of the user's last login
{{ldap.lastLogoff}}	Timestamp of the user's last logout
{{ldap.pwdLastSet}}	Timestamp of when user's password was last set
{{ldap.accountExpires}}	Timestamp of when user's account will expire
{{ldap.badPwdCount}}	Count of bad password attempts
{{ldap.badPasswordTime}}	Timestamp of last bad password attempt
{{ldap.objectGUID}}	Unique identifier for an object
{{ldap.objectSid}}	Binary value that specifies the security identifier

---

These are based on the default attributes for Clearlogin Directory.

Attribute Placeholder	Description
{{cld.email}}	The user's email address
{{cld.username}}	The user's username
{{cld.name}}	The user's name
{{cld.groups}}	The user's groups

{{cld.avatar_url}}	The user's avatar URL
{{cld.password_reset_required}}	Whether password reset is required

---

Attribute Filters

These filters can be applied to force an operation on the attribute.

Filter	Description
Base64.encode64	Sends the Base64-encoded version of an attribute Ex: {{cl.email | Base64.encode64}}
strip_domain	Strips the domain from an attribute Ex: {{cl.email | strip_domain}}
lowercase	Forces an attribute to lowercase Ex: {{cl.email | lowercase}}

Transform Rules

Transform Rules allow you to define custom placeholder policies that take a placeholder input and transform it into a different placeholder (or value) output. A Transform Rule will check to see if a placeholder matches one or more conditions, and if conditions are matched, then the Transform Rule will change the placeholder type and/or placeholder value defined by the rule.

A common example is to transform a user's group membership into a specific role within a SAML application. Clearlogin knows the user is a member of the group, but the application doesn't care. The application is only concerned with the user's role assignment within the application.

Lets say George is a member of the Financial Admins group. When George authenticates with the company's financial application he is given the Admin role within the application. This is because the transform rule converted George's group membership into the Admin role of the application.

Transform Rule Settings

Setting Name	Description
Display Name	The name of the transform rule
Placeholder Name	The name of the placeholder used to call the rule. If left empty, the Display Name will be used.
Transform Conditions	One or more conditions that must be met to transform the incoming attribute placeholder into a different value or another attribute placeholder. **IF** this **Attribute Placeholder** meets the **Condition** of this **Value**, then output this **Value** or **Placeholder.** Available Conditions • Contain • Not Contain • Equal • Not Equal