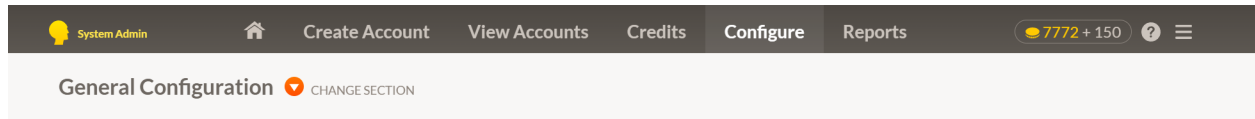


How to setup Microsoft Azure SAML2 SSO

In order to use our SAML SSO integration, you will first need to reach out to [The Conover Company](#) and request access to this feature.

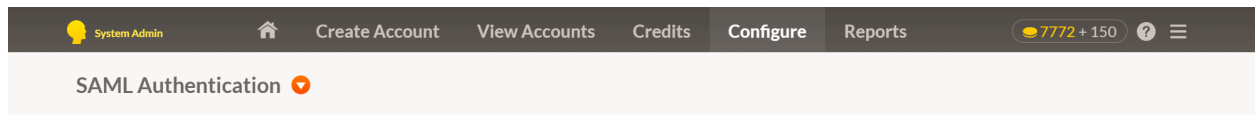
Once enabled, you will have access to a Configuration Option.



Configuration

Platform	Programs	Other
General Configuration	Anger Management	Community Resources Correlations
Email Configuration	Anxiety Management	Course Correlations
SAML Authentication	Bullying Prevention	
	Functional Skills System	
	MECA System	
	Personal Responsibility	
	Success Profiler	
	Workplace Readiness	

When you select the option, all of the information you need to create the SAML2 connection will be present on the screen.



Editing SAML configuration

Instructions

1. Log into your Identity Provider (IdP) and create a new SAML app.
2. Your IdP will require several configuration options. The table below lists the values you need to enter into your IdP.

Reply URL / Assertion / Destination/ Recipient URL	https://staging.conovercompany.com/users/saml/auth
Audience URL	https://staging.conovercompany.com/users/saml/metadata
Sign on URL	https://staging.conovercompany.com/users/saml/auth
Relay State	https://staging.conovercompany.com/
Name ID / Application Username / Unique User Identifier	EmailAddress
Certificate fingerprint encoding algorithm	SHA256
SSO Bookmark Link <small>Visiting this link will initiate the sign-in flow with your Identity Provider</small>	https://staging.conovercompany.com/conover/auth/saml

3. Identity Providers create a certificate for every application. We need a **certificate fingerprint** encoded with SHA256 algorithm. If the identity provider doesn't provide such fingerprint, use OpenSSL command line tools to generate it:
`openssl x509 -text -noout -in /path/to/certificate.cert -fingerprint -sha256`
The certificate fingerprint looks like this: F1:20:A9:91:A8:ED:F2:7E:EC:1B...

SSO target URL / Login URL *	<input type="text" value="https://login.microsoftonline.com/a9c9b6f1-823f-4d7c-9442-dfdd1f2eb75c/saml2"/>
Certificate fingerprint (SHA256) *	<input type="text" value="9C:19:CD:5E:D6:EE:D7:77:01:6A:CE:20:DD:AC:7B:BC:44:2B:D9:35:CD:39:61:1B:A2:06:57:BD:A9:0F:A"/>
IdP Issuer/Identifier URL *	<input type="text" value="https://sts.windows.net/a9c9b6f1-823f-4d7c-9442-dfdd1f2eb75c/"/>

[Save SAML authentication settings](#)

Here are some sample screens from our integration with Microsoft Azure so you can see where we put each URL.

Basic SAML Configuration



Save | Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default



[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default



[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.



Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.



Attributes & Claims ...

[+ Add new claim](#) [+ Add a group claim](#) [≡ Columns](#) | [🔗 Got feedback?](#)

Required claim

Claim name	Value	
Unique User Identifier (Name ID)	user.mail [nameid-format:emailAddress]	...

Additional claims

Claim name	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	...

⌵ Advanced settings (Preview)

We require the email address to be sent as the Unique User Identifier. We were forced to edit the value to make sure only the email address was sent. This was probably due to us using a trial version of Azure that was not completely setup with our domain name.

SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save
 New Certificate
 Import Certificate
 Got feedback?

Status	Expiration Date	Thumbprint
Active	9/29/2025, 11:40:42 AM	B9E1A10B702C583A31DD54C6BFCA68072A5ECC85

Signing Option

Signing Algorithm

Notification Email Addresses

cvolkman@conovercompany.com

Sign SAML assertion

SHA-256

Make certificate active

Base64 certificate download

PEM certificate download

Raw certificate download

Download federated certificate XML

Delete Certificate

There is an issue with the way Azure generates its thumbprints. Do not use Azure's SHA256 thumbprint. What you need to do is download the PEM certificate and generate your own SHA256 thumbprint.

You can either use OpenSSL Command Line

```
openssl x509 -text -noout -in /path/to/certificate.cert -fingerprint -sha256
```

Or this website can also help you generate the proper thumbprint.

<https://www.samltool.com/fingerprint.php>

The certificate fingerprint looks like this: F1:20:A9:91:A8:ED:F2:7E:EC:1B...

Conover Online Test | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

<<

Upload metadata file Change single sign-on mode Test this application Got feedback?

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://staging.conovercompany.com/users/saml/metadat
Reply URL (Assertion Consumer Service URL)	https://staging.conovercompany.com/users/saml/auth
Sign on URL	Optional
Relay State (Optional)	https://staging.conovercompany.com/
Logout Url (Optional)	Optional

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.mail

3

SAML Certificates

Token signing certificate

Edit

Status	Active
Thumbprint	B9E1A10B702C583A31DD54C6BFCA68972A4ECCB5
Expiration	9/29/2025, 11:40:42 AM
Notification Email	cvolkman@conovercompany.com
App Federation Metadata Url	https://login.microsoftonline.com/a9c9b6f1-823f-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) (Preview)

Edit

Required	No
Active	0
Expired	0

4

Set up Conover Online Test

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/a9c9b6f1-823f-...
Azure AD Identifier	https://sts.windows.net/a9c9b6f1-823f-4d7c-9442...
Logout URL	https://login.microsoftonline.com/a9c9b6f1-823f-4d

5

Test single sign-on with Conover Online Test

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

Once all of the options are filled in, the information that you need to insert into Conover Online will appear in setup 4.