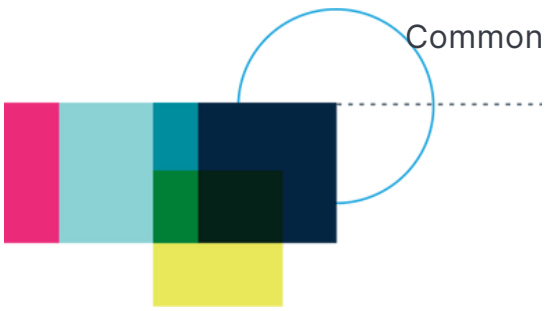
Thought INDUSTRIES

Product Documentation:

Single Sign-On

Table of Contents



Common Terminology

Terminology	Understanding
Single Sign-On or SSO	An authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems
Security Assertion Markup Language or SAML 2.0	Security Assertion Markup Language 2.0 is an open standard for exchanging authentication and authorization data between parties
OpenID Connect or OIDC	OpenID Connect is an authentication layer on top of the OAuth 2.0 authorization framework
JSON Web or JWT Token	JSON Web Token are Tokens designed to be compact, URL-safe, and usable in a web-browser Single Sign-On (SSO) context
Identity Provider or IdP	A system entity that issues authentication assertions in conjunction with a Single Sign-On (SSO)
Service Provider or SP	A system entity that receives and accepts authentication assertions in conjunction with a Single Sign-On (SSO)
Metadata	A standards-based XML document that describes a SAML-enabled system. Metadata is typically provided for both SPs and IdPs.
Application Programming Interface or API	An application programming interface (API) is a way for two or more computer programs to communicate with each other.
Panorama	Thought Industries functionally that allows you to easily license, customize, rebrand, and distribute content across multiple instances

Understanding Single Sign-On

Single Sign-On (SSO) is a mechanism that allows you to authenticate users in your systems and subsequently tell Thought Industries that the user has been authenticated. The user is then allowed to access Thought Industries without being prompted to enter separate login credentials.

At the core of SSO is a security mechanism that allows Thought Industries to trust the login requests it gets from your systems. Thought Industries only grants access to the users you have authenticated.

Thought Industries supports three different types of SSO:

Security Assertion Markup Language 2.0 (SAML 2.0)
SAML 2.0 enables web-based, cross-domain SSO, which helps reduce the administrative overhead of distributing multiple authentication tokens to the user.

OpenID Connect (OIDC)
OIDC allows a range of parties, including web-based, mobile and JavaScript clients, to request and receive information about authenticated sessions and end users.

JSON Web Token (JWT)
JWT claims are typically used to pass identity of authenticated users between an identity provider and a service provider, or any other type of claims as required by business processes.

Use Case Information

The simplest use case for SSO is to allow the user to login once and access Thought Industries without re-entering authentication factors. This could be in the form of an admin looking to login and create content, report on learners, or manage the systems' day to day activity. However, in most cases it is used for learners to access Thought Industries so they can partake in the educational content you have provided with ease.

If configured correctly, SSO can be used to do the following:

Authenticate Login

- Create learner and admin accounts on initial sign in request
- Authenticate access from different systems

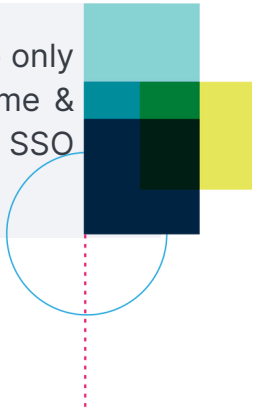
Control Access

- Provision content to the learner directly
- Replace content access
- Directly provide correct access to associated Panorama Instances
- Replace Panorama access

Store Data

- Store optional data fields on user records
- Update learner and admin user records

Note: If implementing SSO after your site is active or live, It is advised to only have one method of authentication. Users who currently use a username & password login in Thought Industries directly should be migrated to your SSO approach.



Prerequisites

- Thought Industries will only act as the SP to receive and accept authentication.
- When setting up SSO, you must supply your own IdP compliant with SAML 2.0, OIDC or JWT.
- When setting up SSO you must have access to an administrative resource supporting the specific SSO solution of SAML 2.0, OIDC or JWT.
- User testing and quality assurance must be performed by an administrative resource supporting the specific SSO solution of SAML 2.0, OIDC or JWT.
- If configuration of SSO is at a Panorama level then you must create a custom Panorama, dedicated to this client, hosting the SSO configuration as to not impact any other Panorama/clients or configurations at the main platform level.
- Panorama can be configured to support SAML 2.0, OIDC or JWT. However, Thought Industries only supports one SSO setup per Panorama.

Common SSO Providers	
Microsoft Azure	Active Directory Federation Services
Okta	Salesforce
OneLogin	JumpCloud
AuthO	Ping

Standard Single Sign-On Settings

SSO settings allow you to control where learners are directed at key moments within Thought Industries. For example, when a learner is registering, you can redirect them to your external registration portal, and then use SSO to send them back to Thought Industries after registration.

The standard SSO settings consist of the following options:

- External Login URL
- Account Logout URL
- External Register URL
- Account Settings Redirect Link

Additional SSO settings options include:

- SSO Subscription
- External eCommerce URL

External Login URL

This is an optional URL you can fill in if you want all learners to log in via SSO. Filling this in will redirect the Thought Industries login page to the URL you specify. It is expected the user will login on the external page, and then you will send their information back to Thought Industries as part of an SSO process, at which point the user will be signed into Thought Industries.

You can use {{returnTo}} in the URL and Thought Industries will automatically fill in what URL the learner should be returned to after they have logged in. For example:

http://www.example.org/sign_in?return_to={{returnTo}}&from=TI

Account Logout URL

Similar to the External Login URL, if you would like all learners to log out via SSO, fill in this URL field. You can use {{returnTo}} in the URL and Thought Industries will automatically fill in what URL the learner should be returned to after they have logged in. For example:

http://www.example.org/logout?return_to={{returnTo}}&from=TI

External Register URL

This is an optional URL you can fill in if you want all learners to register externally. This will redirect both the free registration page and the checkout page if the user is signed out. It is expected the user will register or log in on the external page, and then you will send their information back to Thought Industries as part of an SSO process, at which point the user will be signed into Thought Industries. You can use {{returnTo}} in the URL and Thought Industries will automatically fill in what URL the learner should be returned to after they have registered or logged in. This is particularly important for this endpoint as we will specify a returnTo URL that will put the learner back into the checkout flow. For example:

http://www.example.org/register?return_to={{returnTo}}&from=TI

Account Settings Redirect Link

This is an optional URL you can fill in if you want all learners to update their email address, name, and other profile information externally. You can use {{returnTo}} in the URL and Thought Industries will automatically fill in what URL the learner should be returned to after they have updated their profile. For example:

http://www.example.org/update_profile?return_to={{returnTo}}&from=TI

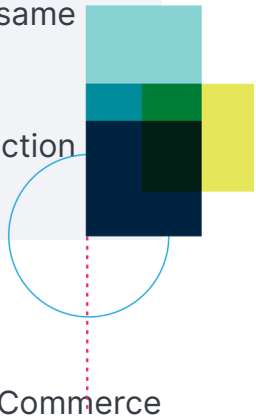
Additional SSO settings:

SSO Subscription

This is an optional selection. SSO Subscription will allow you to provision a subscription to the learners that login via your configured SSO. The subscription must first be created in the eCommerce section of the Thought Industries platform to be applied upon login.

Note: SSO Subscription will not follow the standard subscription process so while it may have purchase terms in eCommerce, it won't follow the same functional outcomes.

Unlike a purchasable subscription, this option will not have any transaction outcome. It is simply a method of providing content to the learners.



External eCommerce URL

This is a URL you can fill in when using the option of 3rd party/external eCommerce instead of the native options. The URL used will redirect learners to this location when they go to checkout after filling their cart within Thought Industries. The transaction will take place outside of the Thought Industries platform and, in most use cases, you will use SSO to provision the content back to the learners. You can include {{cart}} in the URL and it will be substituted with URI-encoded JSON cart item information. The URI-encoded JSON cart item information is used to help map purchasable items in the external eCommerce vendor of choice.

http://www.example.org/cart?cart={{cart}}

SAML 2.0 Settings

SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end user) between a SAML authority, named an Identity Provider, and a SAML consumer, named a Service Provider.

In many cases the SAML 2.0 configuration in Thought Industries requires only a few key pieces of information to set up basic authentication. Please note that the IdP may require more in-depth configuration in order to meet the needs of your integration. These configurations may include attribute mappings, encrypted assertions, and other settings as needed. Configuration can differ from IdP to IdP and it is best advised to refer to your IdP documentation for advanced configuration.

The following settings should be retrieved from your IdP, and can often be found in the administration console (if applicable) or extracted from the IdP metadata XML of your provider. In your instance settings, specify the following options under the SAML 2.0 section under Single Sign-on. These options are available at a main site level, and can be overridden at the Panorama level as needed.

The SAML 2.0 settings consist of the following options:

- IdP Single Sign-On URL
- IdP Single Logout URL
- IdP X.509 Certificate
- Download SP Metadata

Advanced SAML 2.0 Options Include:

- Sign Requests
- Allow Unencrypted Assertions
- Force Re-Authentication

Other Considerations:

- Assertion Consumer Service (ACS) URL
- Entity ID

IdP Single Sign-On URL

This is the endpoint that is dedicated to handling SAML transactions and the location we are receiving the payload from. Thought Industries supports SP-initiated SSO using the HTTP-REDIRECT binding.

http://www.example.org/sso/saml

IdP Single Logout URL

Single logout is not currently supported, but you may still enter this value here for future use. In most use cases the Account Logout URL is used as a redirect instead.

http://www.example.org/slo/saml

IdP X.509 Certificate

This is a PEM formatted certificate that will be used to sign SAML communicate with your IdP, also known as the public key certificate from the IdP. This is required for security purposes in order to validate authentication requests and that acknowledge that the user is coming from the expected IdP. The X.509 Certificate should be entered in PEM format with a header.

This certificate can be found within the Thought Industries SP Metadata. If you have to type it in manually please see IdP X.509 Certificate Sample below.

Note: The IdP X.509 Certificate should always start with the following "**——BEGIN CERTIFICATE——**".

If it does not, you can format the X.509 certificate with an external tool such as https://www.samltool.com/format_x509cert.php or other available tools.

IdP X.509 Certificate Sample

-----BEGIN CERTIFICATE-----
MIIDgzCCAmqgAwIBAgIBADANBgkqhkiG9w0BAQ0FADBbMQswCQYDVQQGEwJ1czEL
MAkGA1UECAwCVVMxGzAZBgNVBAoMElRob3VnaHQgSW5kdXN0cmllczEiMCAGA1UE
AwwZd3d3LnRob3VnaHRpbmR1c3RyaWVzLmNvbTAeFw0xNzA3MTIyMDEyNTBaFw0y
NzA3MTIyMDEyNTBaMFsxCzAJBgNVBAYTAnVzMQswCQYDVQQIDAJVUzEbMBkGA1UE
CgwSVGhvdWdodCBJbmR1c3RyaWVzMSIwIAYDVQQDDBl3d3cudGhvdWdodGluZHVz
dHJpZXMuY29tMIIBIzANBgkqhkiG9w0BAQEFAAOCARAAMIIBCwKCAQIArqB4whkc
URE1DhmsxwBUdY4epWE3KWI6kEmhdtDg1GJo0Bmkt5SU/1Yawja4YvxvR82hpcjk
o+bXJdo3T44Lwq9Y8NQA6DKSZ3duvvx50gUhD3y66ka0AmlayyGDegtHwjz7Px6Q
orRg5aEUMFGGnNZ0AA0+sW0skbfVZsJ+wV5EU8VsXmgqL8mhH8squWXZCOCY+/8M
KW7f1Lf7qBrERRLmVZpgQklx7v8/hxU8K9CMQJR95YG5rLYQjBm1oseaMZmYp2pK
5bKyJCuKiu7nF2eYSnxIAZZKA7Xw1gZRYvnOGguip0yvyHuZMCRmLdg8Fl6Yi4/h
5C1Z/asj1e459/ECAwEAAaNQME4wHQYDVR0OBBYEFNkdMQ/bCwVR0dtyrohqCtZ3
XhmTMB8GA1UdIwQYMBaAFNkdMQ/bCwVR0dtyrohqCtZ3XhmTMAwGA1UdEwQFMAMB
Af8wDQYJKoZIhvcNAQENBQADggECAD4J7tQHK/pkoO5KNrMz/K/rN36cCJ+AP6eK
2Y/WmtC/0WsRuw7DQSTXNLo6CDVi0N8drzF0X9TfpU9LKqlqMNJ8GahyRjNjjHGC
13ET39V/rKUlU4KgiP6MyB5Oqus0u49lpeEPBokUVegH+VLFSxUzWwvVQD9D4j1g
vgYRS9fWAcEihtYUdJyZlOpAQenlw4POrZozk528LEoAupRPjkR6JcqbjoVWeAn7
R+jis+59pbyZJTtmnJFVagyJmqwEE171yU86Eo4TpBmXXwN/fdJA3qr+UKPHgALH
Lfu/UBsugSE3wb5o7BUD1T1xqf1t7JKkuKMKjFxTJm13vC+C4yGc
-----END CERTIFICATE-----

Download SP Metadata

Once the IdP X.509 Certificate has been added to your SSO settings, you will also need to register Thought Industries as a SP within the IdP. This process is different for each provider, but generally you will need the SP metadata information. You can obtain this file by clicking "Download SP Metadata" from the SSO settings page.

Show Advanced

Advanced SAML 2.0 Options:

Advanced Settings

There are several advanced options available and enabling them will depend on the support from your IdP. Check with your provider to determine if any of these options are required or desirable. You can view these options by clicking "Show Advanced" from the SSO settings page.

Sign Requests

This will enable signed requests and validate response signatures. This option may not be supported by all IdPs.

Allow Unencrypted Assertions

When enabled, encrypted assertions are required by default. This option may not be supported by all IdPs.

Force Re-authentication

When enabled, forces re-authentication of learners even if the learner has a SSO session with the IdP. This option may not be supported by all IdPs.

Other Considerations:

Assertion Consumer Service (ACS) URL

The endpoint that receives HTTP-POST bindings from the IdP.

Main Site: https://www.example.org/access/saml/consumer

Panorama: https://www.example.org/access/saml/consumer/client-slug

Entity ID:

Unique identifier for your Thought Industries instance service.

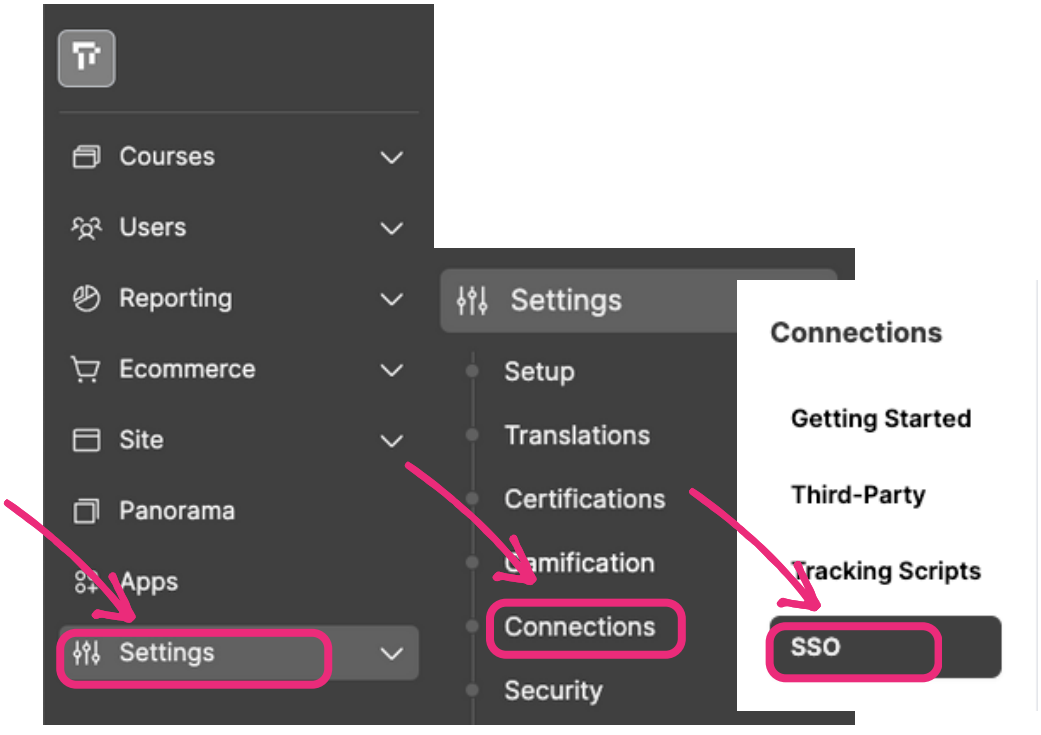
Main Site: https://www.example.org/access/saml/metadata

Panorama: https://www.example.org/access/saml/metadata/client-slug

SAML 2.0 Configuration

Configure the Thought Industries Settings

1. Navigate to site settings from the admin menu.
    a. Select the Connections options.
        i. Select the SSO option.
2. Within the standard SSO settings, configure External Login URL, Account Logout URL, External Register URL and Account Settings Redirect URL as required.
3. Click the Arrow icon next to SAML 2.0 settings to open up the menu.
4. Retrieve the information from your IdP to configure the IdP SSO URL and IdP Single logout URL as required.
5. Manually enter or copy and paste the IdP X.509 Certificate into the provided text box. This information will be gained during Configuring the Identity Provider settings during step below.
6. Select Download SP Metadata.
    a. You will be presented with the XML file. Right-click and select Save As and save the XML to your computer. This will be uploaded into the IdP SSO solution.



Configuring the Identity Provider Settings

Example Identity Provider Configuration

Salesforce as an IdP

1. Enable Salesforce as a SAML IdP
   a. In the quick find box, enter Identity Provider, then select Identity Provider.
   b. Click enable Identity Provider.
   c. Select a certificate from the dropdown menu.
   d. Save your changes.
2. Enter the IdP settings needed in the configure the Thought Industries settings step into Thought Industries
   a. IdP Single Sign-On URL
   b. IdP Single logout URL as required.
   c. IdP X.509 Certificate
3. Add the configuration information from Thought Industries to Salesforce:
   a. ACS URL: https://www.example.org/access/saml/consumer
   b. Entity ID: https://www.example.org/access/saml/metadata

More Information and in depth steps can be found from Salesforce documentation Salesforce as an Identity Provider or Prerequisites for Integrating Service Providers with SAML

JumpCloud as an IdP

1. Go to user authentication > SSO.
   a. Click (+) to configure a new application.
   b. Select the custom SAML app button
2. Upload the Thought Industries XML metadata
   a. This will automatically populate required connector fields
      i. ACS URL: https://www.example.org/access/saml/consumer
      ii. Entity ID: https://www.example.org/access/saml/metadata
3. Set the SAML SubjectNameID format to SAML 2.0 Unspecified
4. Set the signature algorithm to SHA256
5. Set sign assertion
6. Click activate to save and activate the connector. A public certificate and private key pair are generated
7. Download the public certificate and private key pair.

More Information and in depth steps can be found from Jumpcloud documentation Configuring the SAML 2.0 Connector

Note: The IdP examples above are in the form of generalized steps and further configuration may be required, optional or in your best interest depending of the IdP of choice.

Please use the best practices, documentation and guidance of the IdP vendor to configure correctly based on your use case.

SAML 2.0 Attribute Mapping

Thought Industries supports the following attributes that can be mapped from your IdP. The attributes and attribute names returned in the authentication request will vary depending on the IdP. The attribute names you place in the system are case sensitive and must fully adhere to the IdP configuration. Check with your IdP to determine the available attributes and attribute names.

**Required Every Payload*

†Required for Panorama Access via SSO

Attribute	Understanding
First Name*	First name of the user being signed in
Last Name*	Last name of the user being signed in
Email*	Email address of the user being signed in
Role	The role of the user, e.g. “admin”, “student”, “client-manager” etc. Can be a built-in Thought Industries role or a custom role
iMis ID	iMis ID needed for iMis integration to enable you to bring the learning site and member engagement into the iMis solution
Client by ID †	The unique identifier of the Panorama the user should belong to. The ID can be found from the management interface URL in Panorama *Example: /learn/manager/panorama/66667fe3-2cc9-4bbd-a2e2-2e2bfabf253f* † Client ID, SKU, or Slug required for panorama access via SSO

Attribute	Understanding
Client by SKU †	The unique identifier of the Panorama the user should belong to. The SKU can be added in Thought Industries from the management interface. Location: Panorama > Settings > Primary - SKU † Client ID, SKU, or Slug required for panorama access via SSO
Client by Slug †	The unique identifier of the Panorama the user should belong to. The ID can be found from the Panorama landing page URL in Panorama *Example: https://www.example.org/example* † Client ID, SKU, or Slug required for panorama access via SSO
Student Licenses by ID †	The ID of the Panorama sublicense the user should have access to as a learner. The ID can be found in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - License ID † Learner Roles: Student License ID or SKU required for panorama access via SSO
Student Licenses by SKU †	The sku of the Panorama sublicense the user should have access to as a learner. The SKU can be added in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - SKU † Learner Roles: Student License ID or SKU required for panorama access via SSO
Manager Licenses by ID †	The ID of the Panorama sublicense the user should have access to as a Panorama admin or custom role. The ID can be found in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - License ID † Manager Roles: Manager License ID or SKU required for panorama access via SSO

Attribute	Understanding
Manager Licenses by SKU †	The sku of the Panorama sublicense the user should have access to as a Panorama admin or custom role. The SKU can be added in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - SKU † Manager Roles: Manager License ID or SKU required for panorama access via SSO
Active Licenses by ID	Attached to the Sublicense Separation feature in the Thought Industries platform. Allows you to set what is the Active/Main licenses if Users have more than one
Licenses by SKU, Deprecated	It is deprecated and no longer recommended. Please specify using Student Licenses or Manager Licenses instead
Courses by Slug	The unique slug identifier of the course the user has access to. A slug is the part of the URL after "/learn/course/" *Example: /learn/course/example*
Courses by SKU	The unique SKU identifier of the course the user has access to. The SKU can be added in Thought Industries from the management interface Location: Courses > All Courses > Selection > Design - SKU
Learning Paths by Slug	The unique slug identifier of the course(the user has access to. A slug is the part of the URL after "/learn/learning-path/" *Example: /learn/learning-path/example*
Bundles by Slug	The unique slug identifier of the subscription the user should be given access to. A slug is the part of the URL after "/bundle/" *Example: /bundle/example*

Attribute	Understanding
Salesforce Contact ID	The contact ID is a number Salesforce uses to uniquely identify a contact object.
Salesforce Account ID	The account ID is the number Salesforce uses to uniquely identify an account object
Learner Ref1 - 10	Any arbitrary information to be stored on the user. Can be used for any arbitrary information, e.g. student ID, company name, etc
Language	Identifier used to enable a learner's preferred language
Replace Course Access?	Revoke access to any content not specified in either courses or learning paths
Replace License Access?	Revoke access to any licenses not specified in either student licenses or manager licenses
Tiered Subscription?	Use if you have a subscription system where a user is upgrading or downgrading between subscriptions. Specify which single subscription the user has access to with bundles by slug and it will replace any existing subscription. Leave blank to remove subscription
License Course SKUs	Microsoft Endpoint Configuration Manager, formerly System Center Configuration Manager endpoint configuration option. Add course skus an admin role is to be provisioned access to. They will be able to see reports for these pieces of content, and learners attached to this the user will automatically gain access to these pieces of content

Attribute	Understanding
Parent License SKU	Microsoft Endpoint Configuration Manager, formerly System Center Configuration Manager endpoint configuration option. Add SKUs of a parent license, used to create a nested hierarchy of levels
Clear Cart?	When a learner adds items to the cart but the transaction is external, use this attribute to clear cart upon return
Dual Role?	This attribute is a field that is required to tell the Thought Industries that the user logging in is a dual role. When a dual role user logs in (regardless of role) the payload should include dualRole: true. This does not need to be sent for non-dual role users, only those users that have an active dual role

Important Note: We recommend including External Customer IDs in your SSO configuration to allow for easier account management via SSO. Management of external IDs is the sole responsibility of the your IdP administrator. These values must be unique to users in your IdP (e.g. employee ID) and will be passed in the payload for all learners. It is recommended not to use email as the external ID as emails can change.

All users must have their own unique External Customer ID to ensure access to that user's account.

OpenID Connect Settings

OIDC is an authentication layer on top of the OAuth 2.0 authorization framework. It allows Thought Industries to verify the identity of the End-User based on the authentication performed by an Authorization Server.

The following settings should be retrieved from your IdP, and can often be found in the administration console (if applicable) or automatically discovered by providing a well-known URL. Configuration can differ from IdP to IdP and it is best advised to refer to your IdP documentation for advanced configuration. In your instance settings, specify the following options under the OIDC section under SSO. These options are available at a main site level, and can be overridden at the Panorama level as needed.

There are two ways to begin OIDC configuration in Thought Industries, Discovery and Manual Setup.

Discovery Options Include:

- Use Well-Known Endpoint Toggle
- Well-Known Endpoint

The Manual OIDC settings consist of the following options:

- Issuer
- Authorization Endpoint
- Token Endpoint
- User Info Endpoint
- End Session Endpoint
- Signing Algorithm

Other Considerations:

- Client ID
- Client Secret
- Authorization Parameters

Use Well-Known Endpoint Toggle - Yes

If your IdP supports the use of well-known endpoints, you should turn this toggle on. This will remove the Manual options provided and instead provide the steps for automatically discovering information about your OIDC provider. This option may not be supported by all OIDC Authorization Servers

Well-Known Endpoint

This Endpoint will be able to automatically discover endpoint configuration from your IdP. This URL must contain .well-known and likely ends with .well-known/openid-configuration. To initiate discovery, enter the well-known URL of your OIDC authorization server.

https://example.org/.well-known/openid-configuration

Once the URL is entered, click Discover. If successful, the results of the discovery will be displayed. If not, ensure the well-known URL is correct and try again.

Discover

Note: Using the Discovery option and Well-Known Endpoint is the recommended way to configure OpenID Connect in Thought Industries.

If the endpoint is unable to be discovered, you will receive a notification stating the following:
Unable to Discover
Please ensure the well-known endpoint is correct and try again. If the issue persists, you can disable 'Use Well-Known Endpoint'.

Use Well-Known Endpoint Toggle - No

To manually enter Authorization Server information, toggle Use Well-Known Endpoint off.

Manual OIDC Options:

The values for these settings should be retrieved from your Authorization Server, and can often be found in the administration console.

Issuer

The Issuer identifier for the IdP of the authorization response. An Issuer identifier is a case sensitive URL.

https://example.org/

Authorization Endpoint

This Endpoint handles authentication and authorization of a user.

https://example.org/o/oauth2/v2/auth

Token Endpoint

This Endpoint is used to obtain an access token from the authorization endpoint.

https://example.org/token

User Info Endpoint

This Endpoint is a protected resource that, when presented with an Access Token, returns authorized information about the End-User. It is optional and used for fetching additional claims after authorization.

https://example.org/v1/userinfo

End Session Endpoint

This Endpoint is optional and is used for logging the learner out of the OpenID Connect Authorization Server.

https://example.org/v1/userinfo

Signing Algorithm

This dropdown is a selection to verify the JWT returned by the Token Endpoint. The options are RS256 or HS256. It defaults to the RS256 algorithm, an asymmetric algorithm that uses a private key to sign a JWT and a public key for verification of that signature. HS256 is a symmetric algorithm that shares one secret key between the identity provider and your application. The same key is used to sign a JWT and allow verification of that signature.

Other Considerations:

Creating a Client

Each Authorization Server can support more than one Client. We recommend creating a Client specific to your Thought Industries instance. When creating the Client on your Authorization Server, you will likely be asked for "Redirect URI" sometimes referred to as "Callback URI".

Note: Redirect URI or Callback URI should be added in the following format:
https://example.org/access/openId/callback

If configuring Panorama-specific SSO settings it will be in the following format.
https://example.org/access/openId/callback/client-slug

Client ID

After creating the Client in your Authorization Server, you should be given a Client ID. This is the public identifier for the client that is required for all OIDC flows.

Client Secret

After creating the Client in your Authorization Server, you should be given a Client Secret. The Client Secret is used to exchange an authorization code for a token.

Authorization Parameters

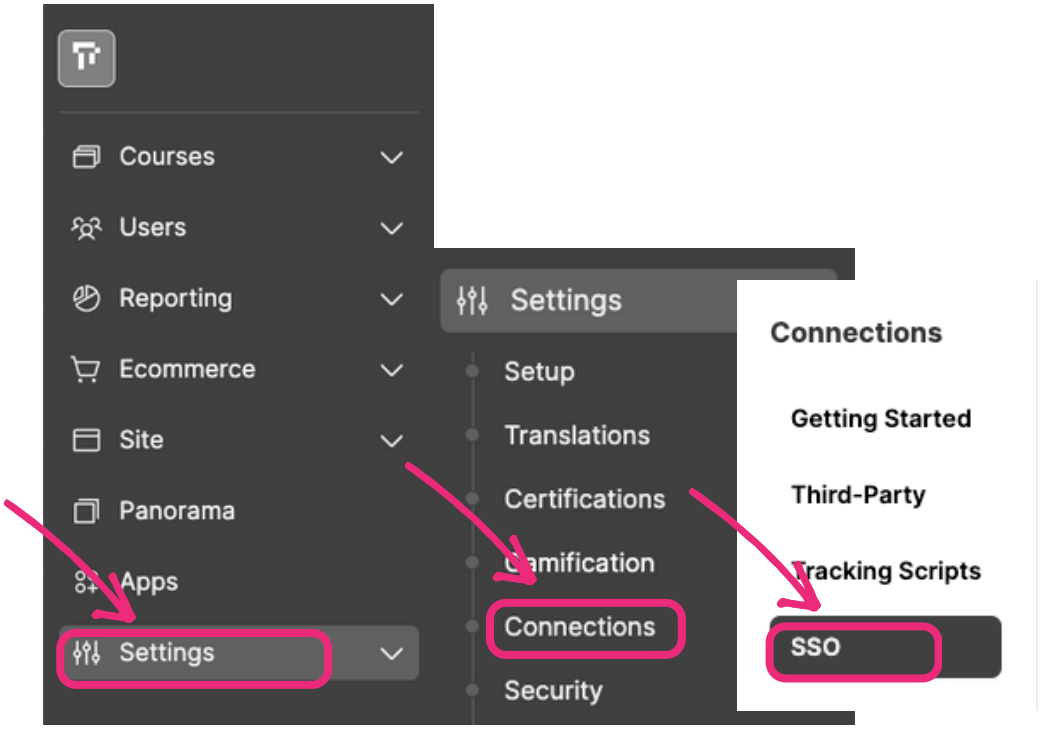
Authorization Parameters are used to configure the Authorization step of OIDC. Each Authorization Server can have slightly different Authorization Parameters, but the common ones are outlined below. You can also add your own Authorization Parameters.

Parameters	Understanding
response_mode	The Response Mode determines how the Authorization Server returns result parameters from the Authorization Endpoint. Thought Industries supports form_post, query, and fragment Response Modes. If not specified, this will default to "query".
response_type	The Response Type request parameter informs the Authorization Server of the desired authorization processing flow. Typically, this is "code" which informs the Authorization Server to return an Access Token. If not specified, this will default to "code".
scope	Scope(s) determine what end-user information is made available to Thought Industries. You can separate multiple scopes with spaces. "openid" is the most typical scope, alongside "email" and "profile". If supported by your Authorization Server, we recommend setting this to "openid email profile". If not specified, this will default to "openid".

OpenID Connect Configuration

Configure the Thought Industries Settings

1. Navigate to site settings from the admin menu.
    a. Select the Connections options.
        i. Select the SSO option.
2. Within the standard Single Sign-On settings, configure External Login URL, Account Logout URL, External Register URL and Account Settings Redirect URL as required.
3. Click the Arrow icon next to OpenID Connect settings to open up the menu.
4. Retrieve the information from your IdP to configure either the Discovery Endpoints or Manual Endpoints as required.
5. Add the Client ID and Client Secret retrieved from your IdP.
6. Add Authorization Parameters as required



Configuring the Identity Provider Settings

Example Identity Provider Configuration

OneLogin as an IdP

1. To connect your OIDC-enabled app to OneLogin, you must:
   a. Add an OIDC app to your company app catalog.
   b. Provide users with access to the app in OneLogin.
2. Access your OneLogin administration portal and select Apps.
3. Select Add App to add a new app.
   a. Search for “OpenId Connect” or “oidc” then select the OpenId Connect (OIDC) app
4. Name the app "Thought Industries" or an appropriate name for your learning site and click Save.
5. On the Configuration tab, enter the Redirect URI that your app uses as the callback endpoint. This is where OneLogin sends the authentication response and ID token.
6. On the SSO tab, copy the Client ID and Client Secret values and use these in your Thought Industries.

More Information and in depth steps can be found from OneLogin Docs
Connect an OIDC enabled app

JumpCloud as an IdP

1. You must set up a project in the Google API Console to obtain credentials and set a redirect URI
2. Obtain OAuth 2.0 credentials
   a. Go to the Credentials page.
   b. Click the name of your credential or the pencil icon. Your client ID and secret are at the top of the page
3. Set a redirect URI
   a. Go to the Credentials page.
   b. In the client IDs section of the page, click a credential.
   c. View or edit the redirect URIs.
   d. If there is no client IDs section on the Credentials page, then your project has no OAuth credentials. To create one, click Create credentials.
4. To simplify implementations and increase flexibility, OIDC allows the use of a "Discovery document,
   a. To use Google's OIDC services, you should use Well-Known Endpoint In Thought Industries https://accounts.google.com/.well-known/openid-configuration

More Information and in depth steps can be found from Google Docs
Using OAuth 2.0 to Access Google APIs

Note: The IdP examples above are in the form of generalized steps and further configuration may be required, optional or in your best interest depending of the IdP of choice.

Please use the best practices, documentation and guidance of the IdP vendor to configure correctly based on your use case.

OpenID Connect Mapping

Thought Industries supports the following attributes that can be mapped from your IdP. The attributes and attribute names returned in the authentication request will vary depending on the IdP. The attribute names you place in the system are case sensitive and must fully adhere to the IdP configuration. Check with your IdP to determine the available attributes and attribute names.

**Required Every Payload*

†Required for Panorama Access via SSO

Attribute	Understanding
First Name*	First name of the user being signed in
Last Name*	Last name of the user being signed in
Email*	Email address of the user being signed in
Role	The role of the user, e.g. “admin”, “student”, “client-manager” etc. Can be a built-in Thought Industries role or a custom role
iMis ID	iMis ID needed for iMis integration to enable you to bring the learning site and member engagement into the iMis solution
Client by ID †	The unique identifier of the Panorama the user should belong to. The ID can be found from the management interface URL in Panorama *Example: /learn/manager/panorama/66667fe3-2cc9-4bbd-a2e2-2e2bfabf253f* † Client ID, SKU, or Slug required for panorama access via SSO

Attribute	Understanding
Client by SKU †	The unique identifier of the Panorama the user should belong to. The SKU can be added in Thought Industries from the management interface Location: Panorama > Settings > Primary - SKU † Client ID, SKU, or Slug required for panorama access via SSO
Client by Slug †	The unique identifier of the Panorama the user should belong to. The ID can be found from the Panorama landing page URL in Panorama *Example: https://www.example.org/example* † Client ID, SKU, or Slug required for panorama access via SSO
Student Licenses by ID †	The ID of the Panorama sublicense the user should have access to as a learner. The ID can be found in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - License ID † Learner Roles: Student License ID or SKU required for panorama access via SSO
Student Licenses by SKU †	The sku of the Panorama sublicense the user should have access to as a learner. The SKU can be added in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - SKU † Learner Roles: Student License ID or SKU required for panorama access via SSO
Manager Licenses by ID †	The ID of the Panorama sublicense the user should have access to as a Panorama admin or custom role. The ID can be found in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - License ID † Manager Roles: Manager License ID or SKU required for panorama access via SSO

Attribute	Understanding
Manager Licenses by SKU †	The sku of the Panorama sublicense the user should have access to as a Panorama admin or custom role. The SKU can be added in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - SKU † Manager Roles: Manager License ID or SKU required for panorama access via SSO
Active Licenses by ID	Attached to the Sublicense Separation feature in the Thought Industries platform. Allows you to set what is the Active/Main licenses if Users have more than one
Courses by Slug	The unique slug identifier of the course the user has access to. A slug is the part of the URL after "/learn/course/" *Example: /learn/course/example*
Courses by SKU	The unique SKU identifier of the course the user has access to. The SKU can be added in Thought Industries from the management interface Location: Courses > All Courses > Selection > Design - SKU
Learning Paths by Slug	The unique slug identifier of the course the user has access to. A slug is the part of the URL after "/learn/learning-path/" *Example: /learn/learning-path/example*
Bundles by Slug	The unique slug identifier of the subscription the user should be given access to. A slug is the part of the URL after "/bundle/" *Example: /bundle/example*
Salesforce Contact ID	The contact ID is a number Salesforce uses to uniquely identify a contact object

Attribute	Understanding
Salesforce Account ID	The account ID is the number Salesforce uses to uniquely identify a account object
Learner Ref1 - 10	Any arbitrary information to be stored on the user. Can be used for any arbitrary information, e.g. student ID, company name, etc
Replace Course Access?	Revoke access to any content not specified in either courses or learning paths
Replace License Access?	Revoke access to any licenses not specified in either Student Licenses or Manager Licenses
Tiered Subscription?	Use if you have a subscription system where a user is upgrading or downgrading between subscriptions. Specify which single subscription the user has access to with bundles by slug and it will replace any existing subscription. Leave blank to remove subscription
License Course SKUs	Microsoft Endpoint Configuration Manager, formerly System Center Configuration Manager endpoint configuration option. Add course skus an admin role is to be provisioned access to. They will be able to see reports for these pieces of content, and learners attached to this the user will automatically gain access to these pieces of content
Parent License SKU	Microsoft Endpoint Configuration Manager, formerly System Center Configuration Manager endpoint configuration option. Add SKUs of a parent license, used to create a nested hierarchy of levels
Clear Cart?	When a learner adds items to the cart but the transaction is external, use this attribute to clear cart upon return

Attribute	Understanding
Dual Role?	This attribute is a field that is required to tell the Thought Industries that the user logging in is a dual role. When a dual role user logs in (regardless of role) the payload should include dualRole: true. This does not need to be sent for non-dual role users, only those users that have an active dual role

Important Note: We recommend including External Customer IDs in your SSO configuration to allow for easier account management via SSO. Management of external IDs is the sole responsibility of the your IdP administrator. These values must be unique to users in your IdP (e.g. employee ID) and will be passed in the payload for all learners. It is recommended not to use email as the external ID as emails can change.

All users must have their own unique External Customer ID to ensure access to that user's account.

JSON Web Token Settings

JWT claims are typically used to pass identity of authenticated users between an identity provider and a service provider, or any other type of claims as required by business processes. Typically, it is an IdP product that will generate the JWT when a user logs in through an application, although it is possible for an individual application to create a JWT itself.

Because of its relatively small size, a JWT can be sent through a URL, through a POST parameter, or inside an HTTP header, and it is transmitted quickly. A JWT contains all the required information about an entity to avoid querying a database more than once. The recipient of a JWT also does not need to call a server to validate the token.

In its compact form, JWTs consist of three parts separated by dots (.), which are:

1. Header
2. Payload
3. Signature

Therefore, a JWT typically looks like the following.

xxxxx.yyyyy.zzzzz or Header.Payload.Signature

The following shows a JWT that has the previous header and payload encoded, and it is signed with a secret:

Header.Payload.Signature

**eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHRlcm5hbEN1c3RvbWVyS
WQiOiIxMjM0NSIsImVtYWlsIjoiYm9iQGV4YW1wbGUuY29tIiwiZmlyc3ROY
W1IjoiQm9iIiwibGFzdE5hbWUiOiJKb25lcyIsInJldHVyblRvIjoiL2xlYXJuLyIsI
nJlZjEiOiJzdHVkZW50aWQiLCJyZWYyIjoiY29tcGFueSBuYW1lIn0.K-
R5Z8dLSk68TcUCvXdxfIHzRXk_1V7naPK40h6xG3c**

Header:

The Header contains metadata about the type of token and the cryptographic algorithms used to secure its contents. You will need specify HS256 as the JWT algorithm in the header of your JWT payload.

```
{
 "alg": "HS256",
 "typ": "JWT"
}
```

Payload:

The Payload contains verifiable security statements, such as the identity of the user and the permissions they are allowed. It is the set of claims or attributes that need to be provided for authentication. When working with JWT claims, you should be aware of the different claim types and naming rules.

Once you have generated the JWT payload, redirect the user along with the payload to the following Thought Industries endpoint:

```
https://mycompany.thoughtindustries.com/access/jwt?jwt=PAYLOAD
```

The payload should be a base64-encoded JSON object and appended to the URL as a query string.

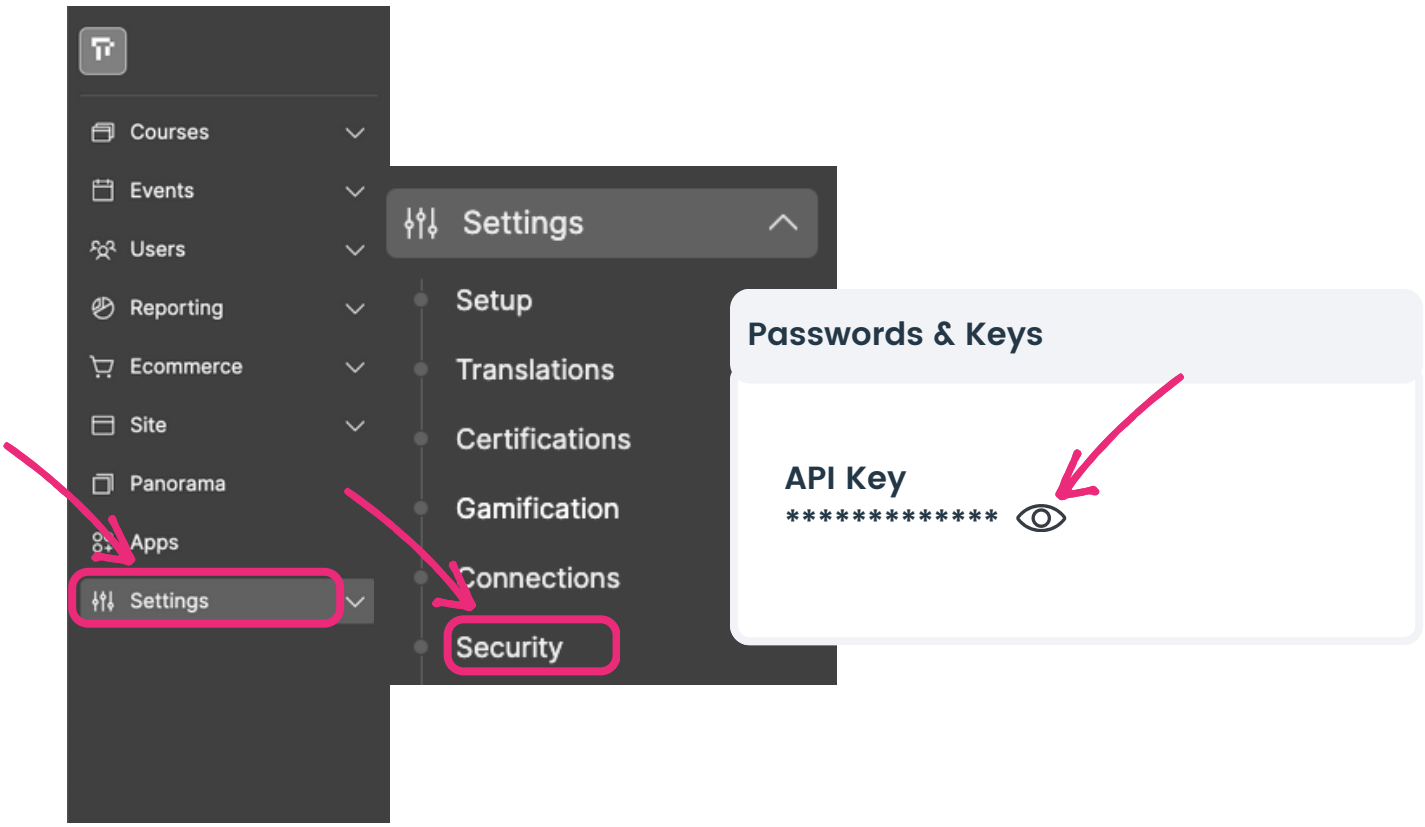
```
{
"externalCustomerId": "12345",
"email": "bob@example.com",
"firstName": "Bob",
"lastName": "Jones",
"returnTo": "/learn/",
"ref1": "studentid",
"ref2": "company name"
}
```

Signature

The Signature used to validate that the token is trustworthy and has not been tampered with. When you use a JWT, you must check its signature before storing and using it. The signature is used to verify that the sender of the JWT is who it says it is and to ensure that the message wasn't changed along the way. To create the signature, the Base64-encoded header and payload are taken, along with a secret, and signed with the algorithm specified in the header.

```
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
secret)
```

You can find your shared secret key by navigating to Settings > Security > Passwords and Keys. From there you will find the key under "API Key." For your protection, you should never share your API keys with anyone. Additionally, as a best practice, we recommend frequent key rotation for API keys. You can have a maximum of two API keys at a time.



JSON Web Token Attribute Mapping

Thought Industries supports the following attributes that can be mapped from your IdP. To perform SSO for a user, you need to send several attributes to Thought Industries as a base64-encoded JSON hash/dictionary. The claims you place in the Payload are case sensitive and must fully adhere to the IdP configuration.

*Required Every Payload

†Required for Panorama Access via SSO

Attribute	Understanding
firstName*	First name of the user being signed in
lastName*	Last name of the user being signed in
email*	Email address of the user being signed in
externalCustomerId	Any unique identifier for the user
iat	The time the token was generated, this is used to help ensure that a given token gets used shortly after it's generated. The value must be the number of seconds since UNIX epoch. We will automatically reject the token if the iat is not within 500 seconds of Thought Industries server time.
courseSlugs	The unique slug identifier of the course the user has access to. A slug is the part of the URL after "/learn/course/" *Example: /learn/course/example*
bundleSlugs	The unique slug identifier of the subscription the user should be given access to. A slug is the part of the URL after "/bundle/" *Example: /bundle/example*

Attribute	Understanding
role	The role of the user, e.g. “admin”, “student”, “client-manager” etc. Can be a built-in Thought Industries role or a custom role
learningPathSlugs	The unique slug identifier of the course the user has access to. A slug is the part of the URL after “/learn/learning-path/“ *Example: /learn/learning-path/example*
replaceCourseAccess	Revoke access to any content not specified in courseSlugs
replaceLearningPathAccess	Revoke access to any content not specified in learningPathSlugs
tieredSubscription	Use if you have a subscription system where a user is upgrading or downgrading between subscriptions. Specify which single subscription the user has access to with bundleSlugs and it will replace any existing subscription. Leave blank to remove subscription
returnTo	URI of page to redirect the user after they have been created. Defaults to the student dashboard
ref1 - ref10	Any arbitrary information to be stored on the user. Can be used for any arbitrary information, e.g. student ID, company name, etc
customFields	Additional arbitrary information to be stored on the user. Can be used for arbitrary information, or in conjunction with other platform functionality
sfContactId	The contact ID is a number Salesforce uses to uniquely identify a contact object

Attribute	Understanding
sfAccountId	The account ID is the number Salesforce uses to uniquely identify a account object
studentLicenseIds †	The ID of the Panorama sublicense the user should have access to as a learner. The ID can be found in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - License ID † Learner Roles: Student License ID or SKU required for panorama access via SSO
studentLicenseSkus †	The sku of the Panorama sublicense the user should have access to as a learner. The SKU can be added in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - SKU † Learner Roles: Student License ID or SKU required for panorama access via SSO
managerLicenseIds †	The ID of the Panorama sublicense the user should have access to as a Panorama admin or custom role. The ID can be found in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - License ID † Manager Roles: Manager License ID or SKU required for panorama access via SSO
managerLicenseSkus †	The sku of the Panorama sublicense the user should have access to as a Panorama admin or custom role. The SKU can be added in Thought Industries from the management interface Location: Panorama > Sublicenses > Selection > General - SKU † Manager Roles: Manager License ID or SKU required for panorama access via SSO

Attribute	Understanding
clientId †	The unique identifier of the Panorama the user should belong to. The ID can be found from the management interface URL in Panorama *Example: /learn/manager/panorama/66667fe3-2cc9-4bbd-a2e2-2e2bfabf253f* † Client ID, SKU, or Slug required for panorama access via SSO
clientSku †	The unique identifier of the Panorama the user should belong to. The SKU can be added in Thought Industries from the management interface Location: Panorama > Settings > Primary - SKU † Client ID, SKU, or Slug required for panorama access via SSO
clientSlug †	The unique identifier of the Panorama the user should belong to. The ID can be found from the Panorama landing page URL in Panorama Example: https://www.example.org/example † Client ID, SKU, or Slug required for panorama access via SSO
replaceLicenseAccess	Revoke access to any licenses not specified in either Student Licenses or Manager Licenses

Important Note: We recommend including External Customer IDs in your SSO configuration to allow for easier account management via SSO. Management of external IDs is the sole responsibility of the your IdP administrator. These values must be unique to users in your IdP (e.g. employee ID) and will be passed in the payload for all learners. It is recommended not to use email as the external ID as emails can change.

All users must have their own unique External Customer ID to ensure access to that user's account.

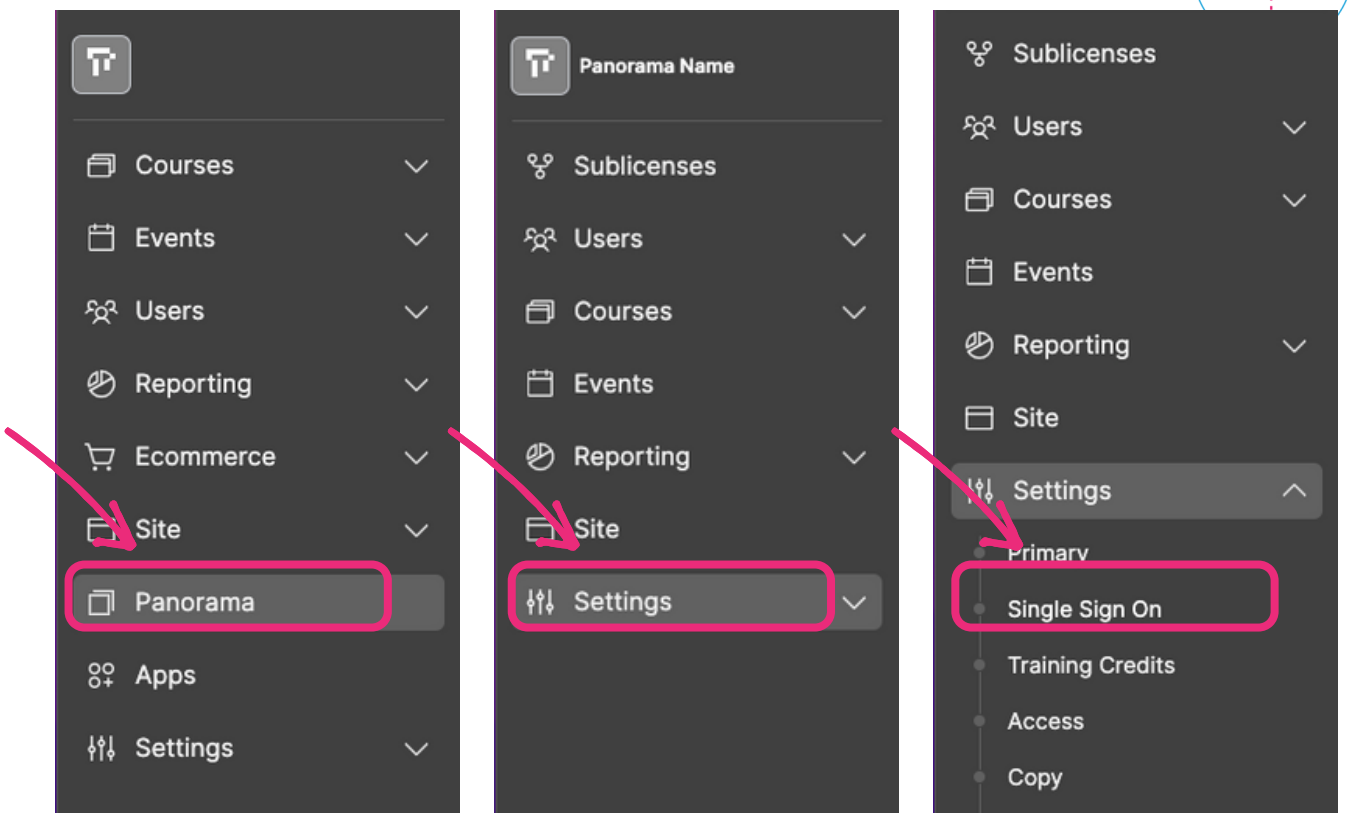
Single Sign-On with Panorama

With Panorama, you can create client portals and sublicenses, which allows for various cohorts to be fully segregated from other cohorts. Each client portal can have their own custom configuration in regards to SSO.

The options available at the main site level for SAML, OIDC or JWT can be overridden at the Panorama level as needed, allowing for multiple IdPs to be configured. Panorama can be configured to support SAML 2.0, OIDC or JWT. However, Thought Industries only supports one SSO setup per Panorama.

The SSO set up location for Panorama is in a different location than the main site and must be configured by going to the following path:
Panorama > Click Panorama/Client Name > Settings > Single Sign-On

Note: If configuration of SSO is at a Panorama level, then you must create a custom Panorama, dedicated to this client, hosting the SSO configuration as to not impact any other Panorama/clients or configurations at the main platform level.



Panorama Considerations for SAML:
Assertion Consumer Service (ACS) URL should be configured as

https://www.example.org/access/saml/consumer/client-slug

Entity ID should be configured as

https://www.example.org/access/saml/metadata/client-slug

Panorama Considerations for OpenID Connect:
Redirect URI or Callback URL should be be configured as

https://example.org/access/openId/callback/client-slug

Panorama Considerations for JWT:
API Keys referenced in SSO cannot be configured at the client level and must be from the main site level. To identify your main site API key, start on your Admin Homepage and go to Settings > Security.

Dual Roles and Single Sign-On

Dual roles are a Thought Industries feature that allows a user to share an email for both a learner and a manager account. When a user is set up in Thought Industries, they can then be turned into a dual role.

Our dual role functionality is supported with SAML 2.0, OIDC, and JWT SSO. A company can specify dualRole during SSO and specify the role alongside access attributes.

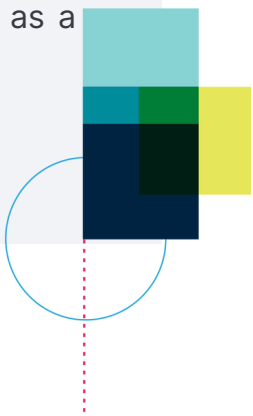
Note: The relationship must be manager/learner, we do not support dual roles that are either manager/manager or learner/learner. When the user next logs in they will be able to switch between their manager and learner accounts seamlessly, allowing them to administer their site and take content without the need for two separate accounts.

Why are dual roles different with SSO?

When a user logs in with SSO, we automatically assume that the user is a learner. This is the default setup with SSO. Our system can support dual role users logging in through SSO, but additional parameters need to be passed for dual role users so that they are correctly recognized by the system and logged in appropriately.

Note: Although the original manager or learner user can be created through SSO, you cannot use SSO to then make that user a dual role. The user must be created as a dual role before they login with SSO for the first time as a dual role user. The dual role can be created one of two ways:

1. From a manager profile manually through the admin interface
2. From either a manager or learner profile via API



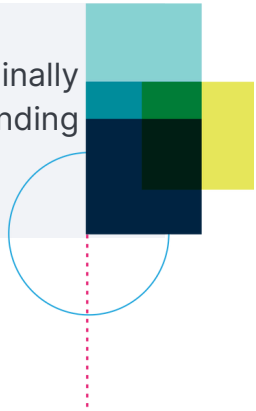
Required Attributes for Dual Role SSO Payloads

Once the dual role user is created you will need to configure your IdP to send the appropriate information for the user when they login. When a dual role user logs in, they must be sent with the role and dualRole attributes every time they login.

Attribute	Understanding
role	This attribute is the name of the role that a user should be placed in when they login. Learner accounts should always be sent in as role: student. Manager accounts should be sent in with the slugified version of the role name. An example would be client-admin rather than Client Admin
dualRole	This attribute is a boolean field that is required to tell the system that the user logging in is a dual role. When a dual role user logs in (regardless of role) the payload should include dualRole: true. This does not need to be sent for non-dual role users, only those users that have an active dual role

If you are using either SAML 2.0 or OIDC, then you will need to map the two attributes from your system that you are using to send these two pieces of information. The attribute names you place in the system are case sensitive and must fully adhere to the IdP configuration. Check with your IdP to determine the available attributes and attribute names.

Note: If you have changed the name of a custom role since you originally created it, then you should confirm the actual slug of the role before sending the attribute.



Common Errors

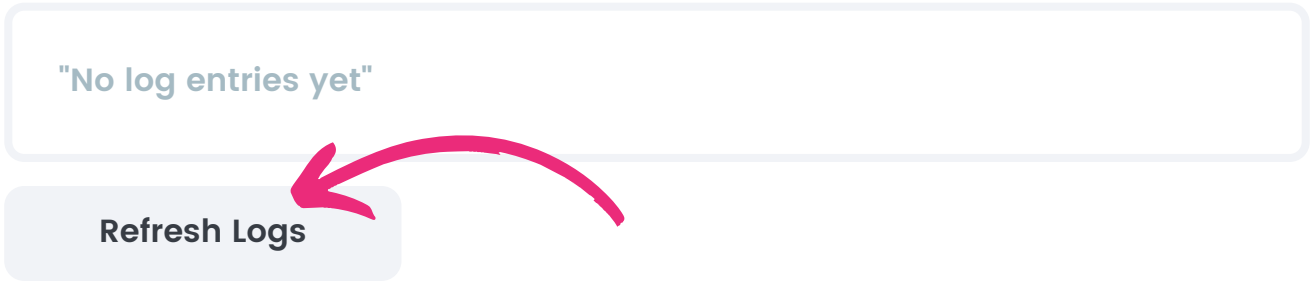
Errors	Understanding
Email already exists	The email exists without a matching external customer ID. Update current user record with that email with external Customer ID that matches the payload via SSO. The system will then sync that user to the account.
Error during SAML authentication	Turn on “Allow Unencrypted Assertions” in Advanced SSO settings.
“Page not found” error	Make sure access point is correctly configured .
No username / user email only	The attribute names you place in the system are case sensitive and must fully adhere to the IdP configuration.
Learner does not log in to Panorama	Panorama attributes such as Client by ID or Student Licenses by ID are unique to Thought Industries and therefore the IdP may need to create or configure custom claim.
Items or Access have been removed	Certain attributes such as Tiered Subscription or Replace License Access will revoke content or learner access if the attribute is blank upon payload send. Always check your attribute matching is correct.
Access is blocked by SSO	When users where created prior to SSO set up, then they may not have an ExternalID mapped. Update the user records ans test again.

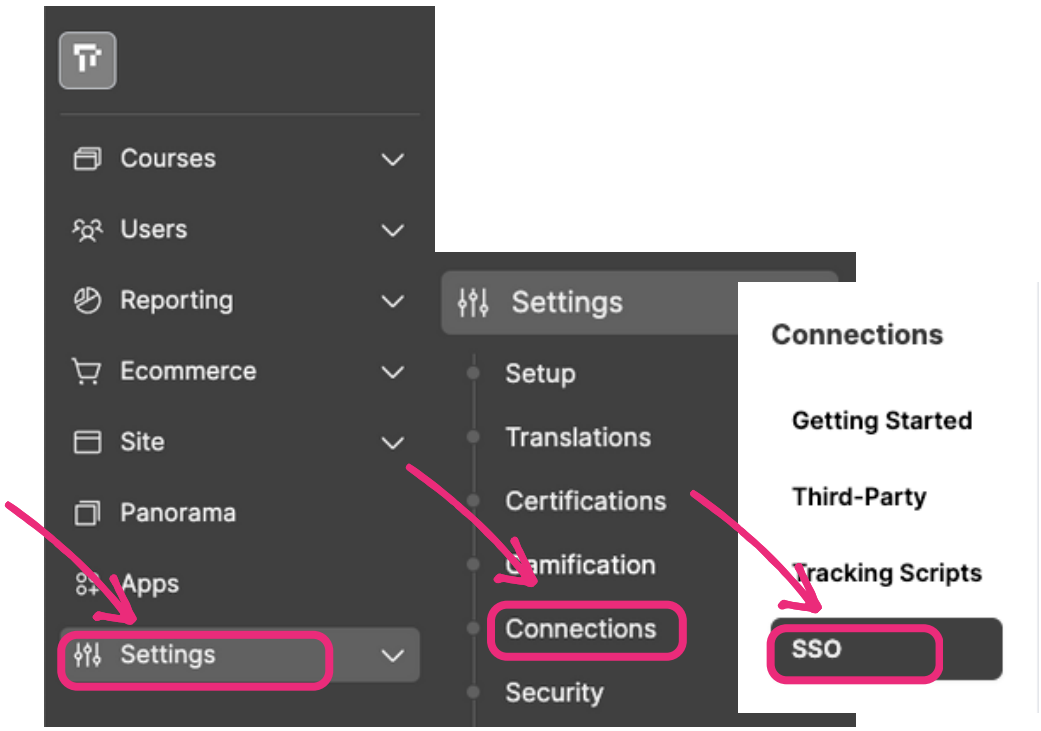
Note: If you have difficulties resolving SSO errors, we suggest you reach out to the administrative resource supporting the specific SSO solution of SAML 2.0, OIDC or JWT. The Thought Industries support team can also offer advice or put you in contact with Thought Industries technical resources by contacting support.thoughtindustries.com.

Single Sign-On Logs

As you test your configuration, it is possible to view error handling in the platform. To turn on logs, you need to navigate to the following path and select Show Logs: Settings>Integrations>SSO>Show Logs

Logs will remain active and you can refresh logs by pressing the Refresh Logs option. We display the past 7 days of activity or the last ~600 responses depending on the frequency of SSO logins.





Single Sign-On Logs Sample


```
{
 "type": "saml",
 "action": "assertionConsumer",
 "ssoBlock": "61c81b3a-3c98-4704-a970-7c01f4debca4",
 "response": {
  "response_header": {
   "version": "2.0",
   "destination": "https://learn.mongodb.com/access/saml/consumer",
   "in_response_to": "_74fa8cede8f6a019cb994af43620a3fb7546c2ba6a",
   "id": "id439820467882245799130277O1"
  },
  "type": "authn_response",
  "user": {
   "name_id": "00uamdfvq5RdTTnzU297",
   "session_index": "_74fa8cede8f6a019cb994af43620a3fb7546c2ba6a",
   "attributes": {
    "email": [
     "bob.hopkins@mongodb.com"
    ],
    "firstName": [
     "Bob"
    ],
    "lastName": [
     "Hopkins"
    ],
    "oktaID": [
     "00uamdfvq5RdTTnzU297"
    ],
    "department": [
     "Online Education Development"
    ],
    "location": [
     "USA_CO"
    ],
    "team": [
     "Developer Relations"
    ],
    "jobCode": [
     "ENG1192"
    ],
    "departmentID": [
     "D28000"
    ],
```


Continued Below

```
"groups": [
"Everyone",
"10gen-eng",
"10gen",
"Employees"
],
"licenseSlug": [
"a641d986-9fe6-4b90-a318-2a14178d2012"
]
}
}
},
"result": {
"valid": true,
"attrs": {
"externalCustomerId": "00uamdfvq5RdTTnzU297",
"firstName": "Bob",
"lastName": "Hopkins",
"email": "bob.hopkins@mongodb.com",
"studentLicenseIds": [
"a641d986-9fe6-4b90-a318-2a14178d2012"
],
"ref4": "00uamdfvq5RdTTnzU297"
}
}
}
```

Powering the Business of Learning

Thought INDUSTRIES