Single Sign-On with SAML 2.0 and OAuth 2.0

User Guide

Copyright

When using and applying the information generated by Kronos SaaShr, Inc. products, customers should ensure that they comply with the applicable requirements of federal and state law, such as the Fair Labor Standards Act. Nothing in this Guide shall be construed as an assurance or guaranty that SaaShr products comply with any such laws.

Published by Kronos SaaShr, Inc., a UKG Company

3040 Route 22 West, Suite 200, Branchburg, NJ 08876

Phone: 908-722-9952; Fax: 908-722-2153

Support: 1-800-394-HELP (1-800-394-4357)

Publish Date: February 28, 2022 11:59:12 AM

Table of Contents

Single Sign-On with SAML 2.0 and OAuth 2.0 User Guide 4
Configuring Single Sign-On SAML 2.0 5
SP Initiated SSO Example - How It Works 8
Sample SAML Response 8
E-Signatures 9
Errors 10
Multi-Tenant IDP (Partner Resellers Only) 10
Support for Google SSO on Mobile App 11
Active Directory, ADFS, and Azure with SAML 2.0 13
How to Set Up a Federation with the System using ADFS 2.0 13
Importing or Uploading the ADFS Certificates 13
Multiple X.509 Certificates 14
Manual Process (Not recommended) 14
Configuring Relying Party Trust Information 15
Recommended Option: Importing the Service Provider Data into ADFS 15
Manually Entering the Relying Party Information 16
Claim Rules 17
Configuring Single Sign-On OAuth 2.0 19
Configuring OAuth 2.0 19
Differences Between SAML 2.0 and OAuth 2.0 22
SAML 2.0 Flow 22
OAuth 2.0 Flow 23

Single Sign-On with SAML 2.0 and OAuth 2.0 User Guide

Single sign-on (SSO) is a user authentication process that permits a user to enter a username and password once per session to access multiple applications. A designated application provided by an **Identity Provider (IdP)** must authenticate the user. The applications that rely on the IdP to authenticate users are known as **Service Providers (SP)**. The system supports Identity Provider-initiated and Service Provider Single Sign-On using the HTTP POST binding.

Configuring Single Sign-On SAML 2.0

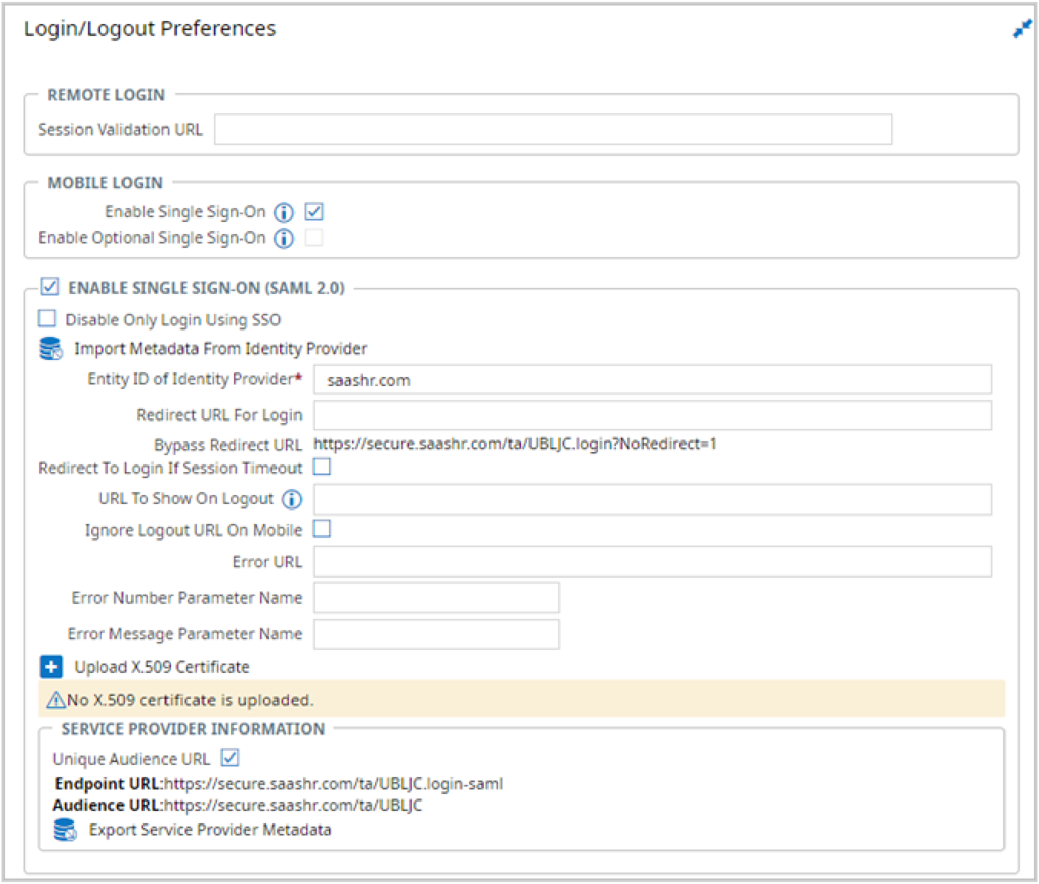
To configure Single Sign-On SAML 2.0, follow these steps:

1. To implement SAML, an X.509 certificate is needed (which may be self-signed). The certificate uploaded to the company must directly correspond to the private key used to sign the SAML responses.

   > **Note:** An option to import metadata from the identity provider is available. If you choose to import the metadata, this certificate will be included. This is the preferred approach for obtaining the X.509 certificate. If this is not possible, you will need to obtain the X.509 certificate from the identity provider directly.

2. The **Enable Single Sign-On (SAML 2.0)** option within the **Login/Logout Preferences** widget will need to be enabled.

   - **UKG Ready™ Partners**: This is done by navigating to **Maintenance > Companies > All System Companies**, clicking the **Edit Company** icon and checking **Enable Single Sign-On (SAML 2.0)** within the **Login/Logout Preferences** widget.
   - **UKG Ready™ Customers**: This is done by navigating to **Global Setup > Company Setup** and navigating to the **Login Config** tab (or adding the Login/Logout Preferences widget to any tab) and checking **Enable Single Sign-On (SAML 2.0)** within the **Login/Logout Preferences** widget.



Login/Logout Preferences

REMOTE LOGIN

Session Validation URL

MOBILE LOGIN

Enable Single Sign-On ☑

Enable Optional Single Sign-On □

☑ ENABLE SINGLE SIGN-ON (SAML 2.0)

□ Disable Only Login Using SSO

Import Metadata From Identity Provider

Entity ID of Identity Provider* saashr.com

Redirect URL For Login

Bypass Redirect URL https://secure.saashr.com/ta/UBLJC.login?NoRedirect=1

Redirect To Login If Session Timeout □

URL To Show On Logout

Ignore Logout URL On Mobile □

Error URL

Error Number Parameter Name

Error Message Parameter Name

Upload X.509 Certificate

⚠No X.509 certificate is uploaded.

SERVICE PROVIDER INFORMATION

Unique Audience URL ☑

Endpoint URL:https://secure.saashr.com/ta/UBLJC.login-saml

Audience URL:https://secure.saashr.com/ta/UBLJC

Export Service Provider Metadata

3. To enable identity providers to begin SSO configuration on their side, you'll need to provide them with specific service provider information. You will need to send the Endpoint URL and Audience URLs to the identity provider.

   The **Service Provider Information** section of the **Login/Logout Preferences** widget contains the endpoint URLs and audience URLs.

   Here are some examples of the endpoint URL format:

   - US: https://secure.saashr.com/ta/company.login-saml
   - EU: https://secure.workforceready.eu/ta/company.login-saml
   - AUS: https://secure.workforceready.com.au/ta/company.login-saml

   The **Unique Audience URL** checkbox determines if a company id is included in the audience URL.

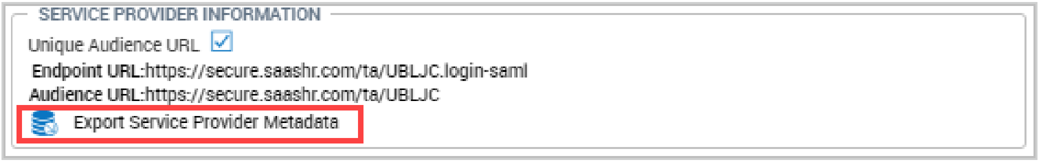
   The Audience URL contains the company domain and the company short name when the **Unique Audience URL** option is checked. Here are some examples:

   - US: https://secure.saashr.com/company
   - EU: https://secure.workforceready.eu/company
   - AUS: https://secure.workforceready.com.au/company

   If not checked, the company domain alone is used for all client companies. Here are some examples:

   - US: https://secure.saashr.com
   - EU: https://secure.workforceready.eu
   - AUS: https://secure.workforceready.com.au

4. After the Unique Audience URL is set appropriately, the information can be manually set at the IdP's site or imported by the IdP from an XML file. To generate an XML file containing the required data, click on the **Export Service Provider Metadata** icon. If the identity provider cannot import an XML file, the information is available in the Service Provider Information section of the Login/Logout Preferences widget and can be manually entered at the IdP site.



SERVICE PROVIDER INFORMATION

Unique Audience URL ☑

Endpoint URL:https://secure.saashr.com/ta/UBLJC.login-saml

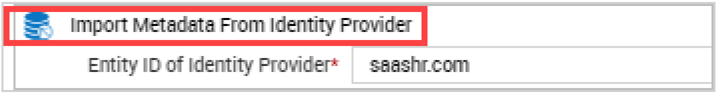
Audience URL:https://secure.saashr.com/ta/UBLJC

5. Configure additional settings.

   - **Redirect URL For Login**: This is the Single Sign-On Service URL provided by the Identify Provider. This is required for SP-Initiated SSO for login links within emails to work.

> **Note:** After this is configured, all users will be redirected upon accessing the login page. This setting should be configured with active users in mind who may be redirected to different pages than they would normally see when logging in. It is recommended that this is configured after SSO is completely configured on both the SP and IdP sides.

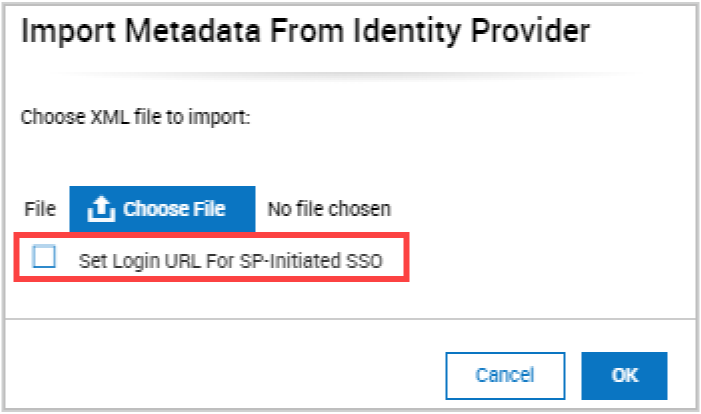
- **Bypass Redirect URL:** This is the URL that will be used for direct logins to the system, without requiring authentication from an external Identify Provider.
- **URL To Show On Logout**: This will be the URL that displays when users log out.
- **Session Validation URL**: This is only needed for older versions of SSO and is used for remote login.
- **Enable Single Sign-On (SAML 2.0)**: Checking this option will enable the options shown below.
- **Import Metadata From Identity Provider:** Clicking on the import icon enables you to import data provided by the Identity Provider, including the Entity ID, Redirect URL For Login and the X.509 Certificate.



Import Metadata From Identity Provider

Entity ID of Identity Provider* saashr.com

- **Set Login URL For SP-Initiated SSO:** This setting overrides the Redirect URL For Login setting with the URL imported from the metadata.



Import Metadata From Identity Provider

Choose XML file to import:

File Choose File No file chosen

□ Set Login URL For SP-Initiated SSO

- **Entity ID of Identity Provider:** The entity ID of your Identity Provider.
- **Error URL:** This will redirect users when there is a problem with logging in through SAML.
- **Error Number Parameter Name:** The error name will be appended to the query string of the error URL if parameter numbers for the message are specified here.
- **Error Message Parameter Name:** The error message and error number will be appended to the query string of the error URL if parameter names for the message and number are specified here.
- **Upload X.509 Certificate:** This is used to upload the X.509 certificate, provided by the IdP into the system.

SP Initiated SSO Example - How It Works

1. User clicks on a login link from an email.

2. User is redirected to the login redirect URL with RelayState appended as a query string parameter. For example, the URL is:

   https://login-redirect-url?RelayState=2g53i5g32523rfghdf.

3. Identity Provider creates a SAML response with the POST message body consisting of:

   ```
   SAMLResponse=response&RelayState=2g53i5g32523rfghdf
   ```

   and posts it back to the system at the endpoint URL:

   - US: https://secure.saashr.com/ta/company.login-saml, or
   - EU: https://secure.workforceready.eu/ta/company.login-saml, or
   - AUS: https://secure.workforceready.com.au/ta/company.login-saml.

4. After verifying the SAML response, the user is redirected to the appropriate first page based on the value of RelayState.

Sample SAML Response

The following is a sample SAML response, which contains the following placeholders:

- [[IDP_ENTITY_ID]] -> The Entity ID of the Identity Provider
- [[COMPANY_SHORT_NAME]] -> The short name of your company
- [[USERNAME]] -> Username of a valid employee from the company

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="RNPWBRGOGEZZYSLKZKTKUKOIAXPJNQRAMOWCSIPH" IssueInstant="2013-03-03T19:07:11.975Z" Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
[[IDP_ENTITY_ID]]</saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="#RNPWBRGOGEZZYSLKZKTKUKOIAXPJNQRAMOWCSIPH">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml samlp"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>Pq/3GDC3zbxiO9ek/J//SYHY840=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>a12twr1ip873lGjM76VfnGBJCG13J99N/ef28Pc8lnb81xCb8KcmClcvSqLtEAs0J8BF+ZuqYsZ1
```

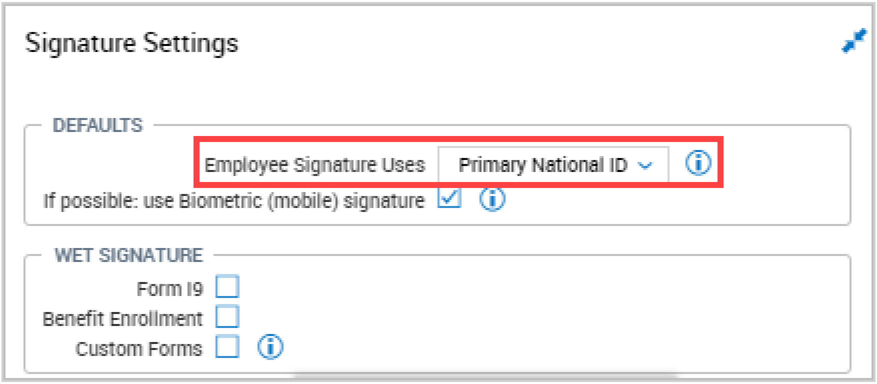
```
EkpSbGMAEph6dbhE5XkfjSyBwhVWFS0OlOo/RJsaXi85E8Q9DJzmSRaadYr9CMom59TAHfVUrKAv
kk/wEt4SyTJnuUKdMAU=</ds:SignatureValue>
 </ds:Signature>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
 </samlp:Status>
 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="KLEPEIPQAFALFWJEWYWJJYUCQGKQOLYMRVSXEACB" IssueInstant="2013-03-03T19:07:11.975Z" Version="2.0">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">[[IDP_ENTITY_ID]]</saml:Issuer>
  <saml:Subject>
   <saml:NameID>[[USERNAME]]</saml:NameID>
   <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2013-03-03T19:10:11.975Z" Recipient="https://secure.saashr.com/ta/
[[COMPANY_SHORT_NAME]].login-saml"/>
   </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2013-03-03T19:04:11.975Z" NotOnOrAfter="2013-03-03T19:10:11.975Z">
   <saml:AudienceRestriction>
    <saml:Audience>https://secure.saashr.com</saml:Audience>
   </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2013-03-03T19:07:11.975Z">
   <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRe
f>
   </saml:AuthnContext>
  </saml:AuthnStatement>
 </saml:Assertion>
</samlp:Response>
```

E-Signatures

Depending on your requirements and configuration, employees may need to sign documents electronically within the system. The passwords that employees provide to the IdP may not be the same as the passwords for the system. The Electronic Signature Uses field can be configured to allow users to electronically sign a document using a field other than their password. To avoid confusion when electronic signatures are required, it is recommended that this field be configured to something other than **Password**.

The **Electronic Signature Uses** field can be found in the **Signature Settings** widget, typically on the **Global Policies** tab under **Company Settings > Global Setup > Company Setup**.



Signature Settings

DEFAULTS

Employee Signature Uses: Primary National ID

If possible: use Biometric (mobile) signature ☑

WET SIGNATURE

Form I9 □

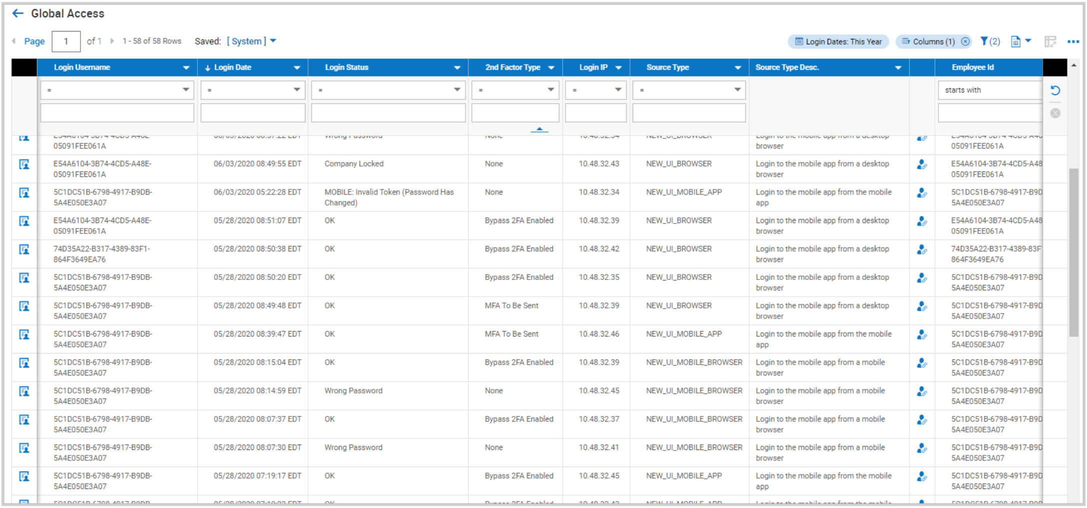
Benefit Enrollment □

Custom Forms □

Errors

When logged in to the system, you can find more detailed error messages for SAML 2.0 when you go to the **System Events** report under **Company Settings > System > Events** and search for events where source starts with SAML 2.0. When there's an issue with the SAML 2.0 response itself, errors will have a source of SAML 2.0 Response.

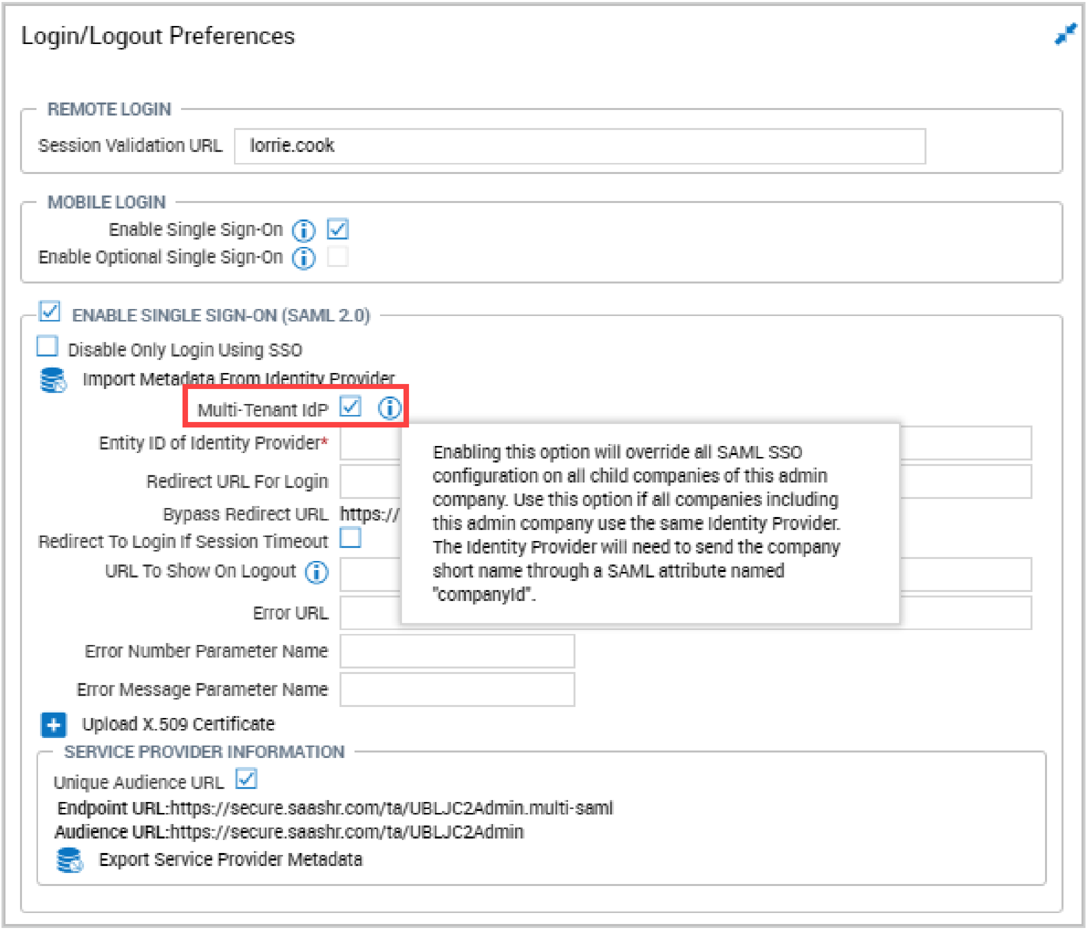
If the SAML 2.0 response is processed successfully but there's an issue with the username used, you can find the related error when you view login attempts on the Global Access report under **My Info > My Reports > System Reports > System Utilities > Global Access**.



Login Username	↓ Login Date	Login Status	2nd Factor Type	Login IP	Source Type	Source Type Desc.		Employee Id
=	=	=	=	=	=			starts with
05091FEE061A						browser		05091FEE061A
E54A6104-3B74-4CD5-A48E-05091FEE061A	06/03/2020 08:49:55 EDT	Company Locked	None	10.48.32.43	NEW_UI_BROWSER	Login to the mobile app from a desktop browser		E54A6104-3B74-4CD5-A48 05091FEE061A
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	06/03/2020 05:22:28 EDT	MOBILE: Invalid Token (Password Has Changed)	None	10.48.32.34	NEW_UI_MOBILE_APP	Login to the mobile app from the mobile app		5C1DC51B-6798-4917-B9D 5A4E050E3A07
E54A6104-3B74-4CD5-A48E-05091FEE061A	05/28/2020 08:51:07 EDT	OK	Bypass 2FA Enabled	10.48.32.39	NEW_UI_BROWSER	Login to the mobile app from a desktop browser		E54A6104-3B74-4CD5-A48 05091FEE061A
74D35A22-B317-4389-83F1-864F3649EA76	05/28/2020 08:50:38 EDT	OK	Bypass 2FA Enabled	10.48.32.42	NEW_UI_BROWSER	Login to the mobile app from a desktop browser		74D35A22-B317-4389-83F 864F3649EA76
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 08:50:20 EDT	OK	Bypass 2FA Enabled	10.48.32.35	NEW_UI_BROWSER	Login to the mobile app from a desktop browser		5C1DC51B-6798-4917-B9D 5A4E050E3A07
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 08:49:48 EDT	OK	MFA To Be Sent	10.48.32.39	NEW_UI_BROWSER	Login to the mobile app from a desktop browser		5C1DC51B-6798-4917-B9D 5A4E050E3A07
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 08:39:47 EDT	OK	MFA To Be Sent	10.48.32.46	NEW_UI_MOBILE_APP	Login to the mobile app from the mobile app		5C1DC51B-6798-4917-B9D 5A4E050E3A07
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 08:15:04 EDT	OK	Bypass 2FA Enabled	10.48.32.39	NEW_UI_MOBILE_BROWSER	Login to the mobile app from a mobile browser		5C1DC51B-6798-4917-B9D 5A4E050E3A07
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 08:14:59 EDT	Wrong Password	None	10.48.32.45	NEW_UI_MOBILE_BROWSER	Login to the mobile app from a mobile browser		5C1DC51B-6798-4917-B9D 5A4E050E3A07
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 08:07:37 EDT	OK	Bypass 2FA Enabled	10.48.32.37	NEW_UI_MOBILE_BROWSER	Login to the mobile app from a mobile browser		5C1DC51B-6798-4917-B9D 5A4E050E3A07
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 08:07:30 EDT	Wrong Password	None	10.48.32.41	NEW_UI_MOBILE_BROWSER	Login to the mobile app from a mobile browser		5C1DC51B-6798-4917-B9D 5A4E050E3A07
5C1DC51B-6798-4917-B9DB-5A4E050E3A07	05/28/2020 07:19:17 EDT	OK	Bypass 2FA Enabled	10.48.32.45	NEW_UI_MOBILE_APP	Login to the mobile app from the mobile app		5C1DC51B-6798-4917-B9D 5A4E050E3A07

Multi-Tenant IDP (Partner Resellers Only)

At the Partner Admin Company Level, the Multi-Tenant IDP option is available. When enabled, the SAML 2.0 Configuration becomes global and all child companies of the Admin company use the same IDP provider. When this option is enabled, the identity provider needs to send the company short name through a SAML 2.0 attribute named companyId.



Login/Logout Preferences

REMOTE LOGIN

Session Validation URL: lorrie.cook

MOBILE LOGIN

Enable Single Sign-On ☑

Enable Optional Single Sign-On □

☑ ENABLE SINGLE SIGN-ON (SAML 2.0)

□ Disable Only Login Using SSO

Import Metadata From Identity Provider

Multi-Tenant IdP ☑

Entity ID of Identity Provider*

Redirect URL For Login

Bypass Redirect URL: https://

Redirect To Login If Session Timeout □

URL To Show On Logout

Error URL

Error Number Parameter Name

Error Message Parameter Name

Upload X.509 Certificate

Enabling this option will override all SAML SSO configuration on all child companies of this admin company. Use this option if all companies including this admin company use the same Identity Provider. The Identity Provider will need to send the company short name through a SAML attribute named "companyId".

SERVICE PROVIDER INFORMATION

Unique Audience URL ☑

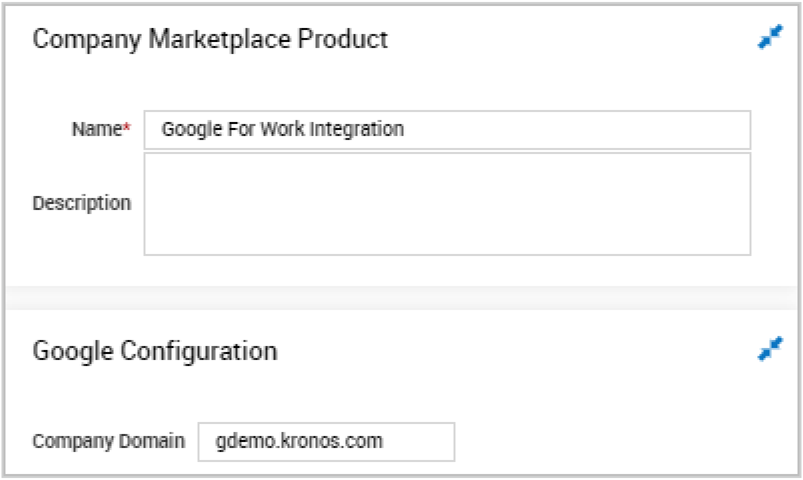
Endpoint URL:https://secure.saashr.com/ta/UBLJC2Admin.multi-saml

Audience URL:https://secure.saashr.com/ta/UBLJC2Admin

Export Service Provider Metadata

Support for Google SSO on Mobile App

Users utilizing the Mobile App can now authenticate with Google SSO (Single Sign On). This option requires that companies have installed and are using the Google Cloud (formerly called Google for Work) Integration Marketplace product. The Google domain and the Company Domain configured in the Marketplace must match. Locate the product under **Company Settings > Marketplace > Marketplace Setup**. Look for the product under the Installed tab and click the edit icon.



Company Marketplace Product

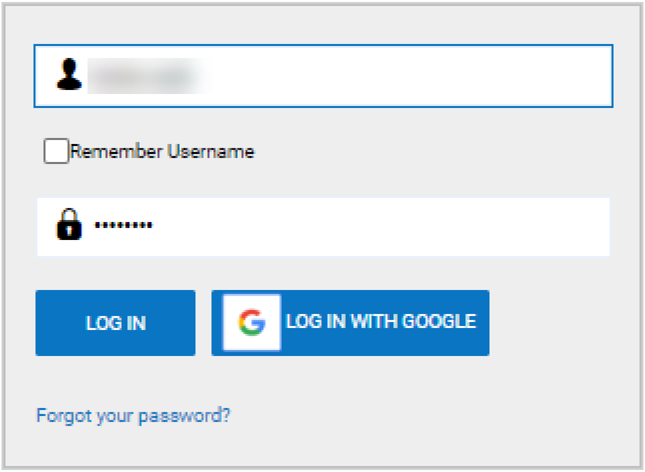
Name*: Google For Work Integration

Description

Google Configuration

Company Domain: gdemo.kronos.com

Additionally, users can only log in using their company's Google For Work (Google Cloud) user account. Consumer accounts will not work. Users need to have their primary email address set as their Google For Work (Google Cloud) address to use this functionality.



Active Directory, ADFS, and Azure with SAML 2.0

This section is provided for the convenience of our users who use Microsoft ADFS and/or Azure for SSO. It is not intended to be used for a complete deployment, troubleshooting, or configuration guide. For technical support regarding these Microsoft products, a wealth of information is available at Microsoft and other sites, including:

- https://docs.microsoft.com
- https://techcommunity.microsoft.com
- https://msdn.microsoft.com
- Integrating SAML support with ADFS

How to Set Up a Federation with the System using ADFS 2.0

Two steps are required to set up a federation between ADFS 2.0, the IdP, and the system, which is a trusted resource in this scenario. You will need to obtain an X.509 certificate and establish a trust relationship between the system and the ADFS 2.0 server.

In this scenario, the user enters the URL for the system in a browser or clicks a link from an email. When the system receives the request, it checks the request to determine if the user has been authenticated. If the authentication data is present, the user can access the system and is redirected back to the URL that they were initially attempting to access.

If the authentication data is not present, the request is redirected to an ADFS server for authentication. The system includes the X.509 certificate in any requests to authenticate the user. If the X.509 certificate is valid, the user is asked to login through ADFS. If authenticated, the request is redirected back to the original URL.

For all pieces to work correctly in this scenario, you must complete two steps.

1. Obtain the certificate from the ADFS side and import it or upload it to the system.
2. Import data about the system into ADFS. ADFS requires this step when configuring a Relying Party Trust.

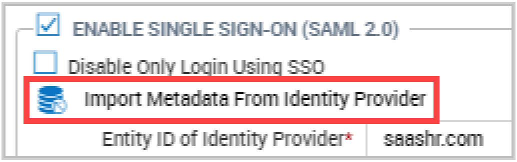
Importing or Uploading the ADFS Certificates

To set up the certificate on the ADFS side, you can use a self-signed certificate generated by ADFS or use a different certificate. Two approaches can be used.

The recommended approach requires fewer manual steps. In this approach, the certificate is contained in the metadata XML file. The metadata can be downloaded from https://<server>/federationmetadata/2007-06/federationmetadata.xml, where <server> is the ADFS server.

The metadata must then be imported to the system in the Enable Single Sign-On (SAML 2.0) section:

- **UKG Ready™ Partners**: This is done in the **Login/Logout Preferences** widget in the **Company Information** page.
- **UKG Ready™ Customers**: This is done in the **Login/Logout Preferences** widget in the **Global Setup** > **Company Information** page.



☑ ENABLE SINGLE SIGN-ON (SAML 2.0)

□ Disable Only Login Using SSO

Import Metadata From Identity Provider

Entity ID of Identity Provider* saashr.com

Multiple X.509 Certificates

Multiple X.509 certificates can be uploaded, and as a result, a new certificate can be uploaded alongside a soon-to-expire certificate to allow a simpler transition from the old certificate to the new one.

Expired or duplicate certificates cannot be uploaded, and a warning displays if a duplicate is uploaded. When a certificate is no longer valid, it is automatically removed after 15 days. Certificates display in a table for better readability.

An option to **Replace Existing Certificates** is available when importing metadata. When enabled, importing metadata deletes the existing certificate(s) and replaces it with the one from the metadata.

Expired certificates are hidden by default, and they can be shown when the **Show Expired Certificates** checkbox is enabled. This checkbox is only visible when the company has any expired certificates. The **Valid To** date displays in red for expired certificates.

> **Note:** If all certificates are expired, the **Show Expired Certificates** checkbox is always enabled and all expired certificates are always shown.

Manual Process (Not recommended)

As an alternative, the certificate can be downloaded directly by logging into the ADFS server.

1. Start the Microsoft Management Console.

   You will need to run the Microsoft Management Console (MMC) program by clicking on **Start**, then selecting **Run** and entering “MMC”.

2. Start the Certificate Snap-in Wizard.

   Click on the **File** menu option and select **Add/Remove Snap-in…** Then select **Certificates** and click on **Add**.

3. Specify where to get the file.

   After the Certificate Snap-in wizard starts, select **Computer account** and click the **Next** button.

   Since you are pulling the file from the local system, select **Local computer,** then click the **Finish** button and then click **OK**.

4. Select the certificate.

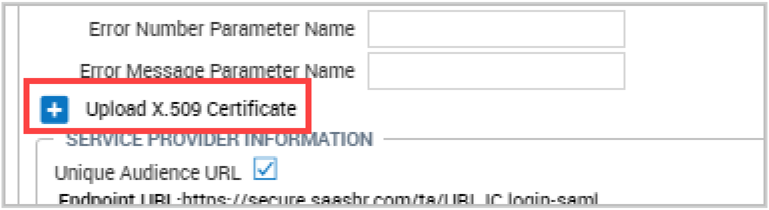
   Expand **Console Root\Certificates (Local Computer)\Personal\Certificates**. Select the X.509 certificate by right-clicking on it. Select **All Tasks**, then click **Export** and then click **Next**.

   Choose **No, do not export the private key option**, then click **Next**.

   Choose the **Base-64 encoded x.509(.CER)** option, then click **Next**.

   Enter a file path and name then click the **Next** button.

You should see a pop-up reading **The export was successful**, and you can click OK, then save and upload the exported file into the system using the **Upload X.509 Certificate** option.



Error Number Parameter Name

Error Message Parameter Name

Upload X.509 Certificate

SERVICE PROVIDER INFORMATION

Unique Audience URL ☑

Endpoint URL:https://secure.saashr.com/ta/URL.IC.login-saml

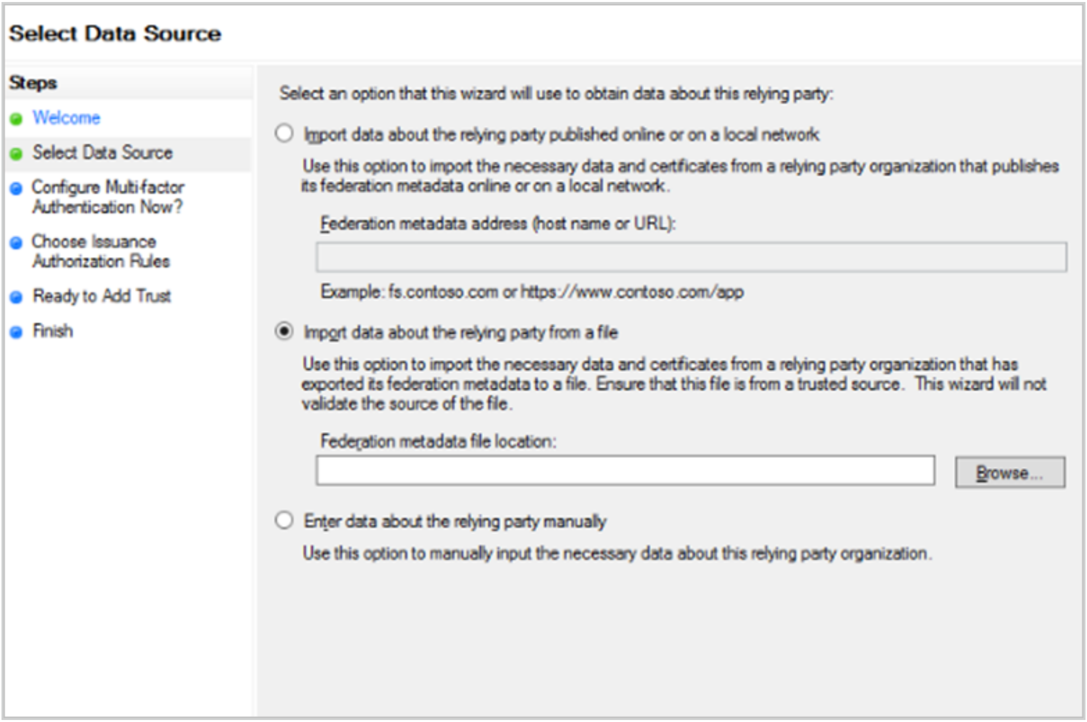
Configuring Relying Party Trust Information

The ADFS 2.0 Management snap-in will be used to configure Relying Party Trust Information. From that tool, you can navigate to **ADFS 2.0 > Trust Relationships > Relying Party Trusts**. You'll need to right-click on **Relying Party Trusts** and select **Add Relying Party Trust**.

A wizard will start. Click the **Start** button. Two options are available, an import and manual text entry. The import option is recommended. Manual entry should only be used if your IdP cannot import the data from a file. This is not the case with ADFS.

Recommended Option: Importing the Service Provider Data into ADFS

If you have exported service provider metadata from the **Login/Logout Preferences** widget, you can upload the file. Within the **Relying Party Trust** wizard, choose **Select Data Source** and upload the file using the **Import data about the relying party from a file** option.



Select Data Source

Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

For **Display** name, enter any name (for example, **Trusted Resource**) and click the **Next** button.

Manually Entering the Relying Party Information

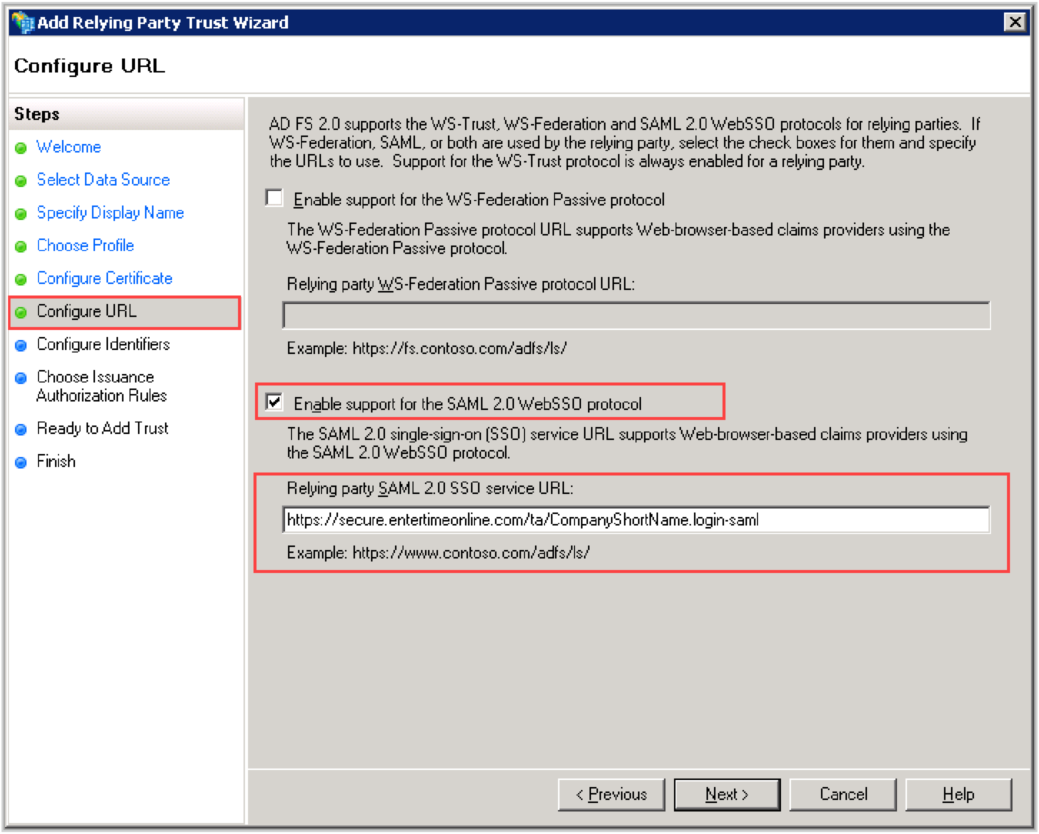
If your IdP cannot import a file, the alternative is to choose **Enter data about the relying party manually** option and click the **Next** button.

You'll need to step through each of the sections in the **Relying Party Trust** wizard.

1. In the **Specify Display Name** section, enter any name for **Display** (for example, **Trusted Resource**) and click the **Next** button.

2. For the **Choose Profile** section, select **AD FS 2.0 profile** and click the **Next** button.

3. For the **Configure Certificate** section, click the **Next** button as the system does not support a token encryption certificate.



Configure URL

AD FS 2.0 supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

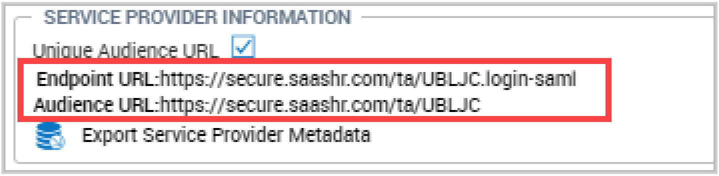
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://secure.entertimeonline.com/ta/CompanyShortName.login-saml

Example: https://www.contoso.com/adfs/ls/

4. For the **Configure URL** section, check **Enable support for SAML 2.0 Web SSO protocol**. For the **Relying party SAML 2.0 SSO** service URL, enter the Service Provider (SP) URL. This is the Endpoint URL shown in the **Service Provider Information** in the **Login/Logout Preferences** widget.


SERVICE PROVIDER INFORMATION
Export Service Provider Metadata

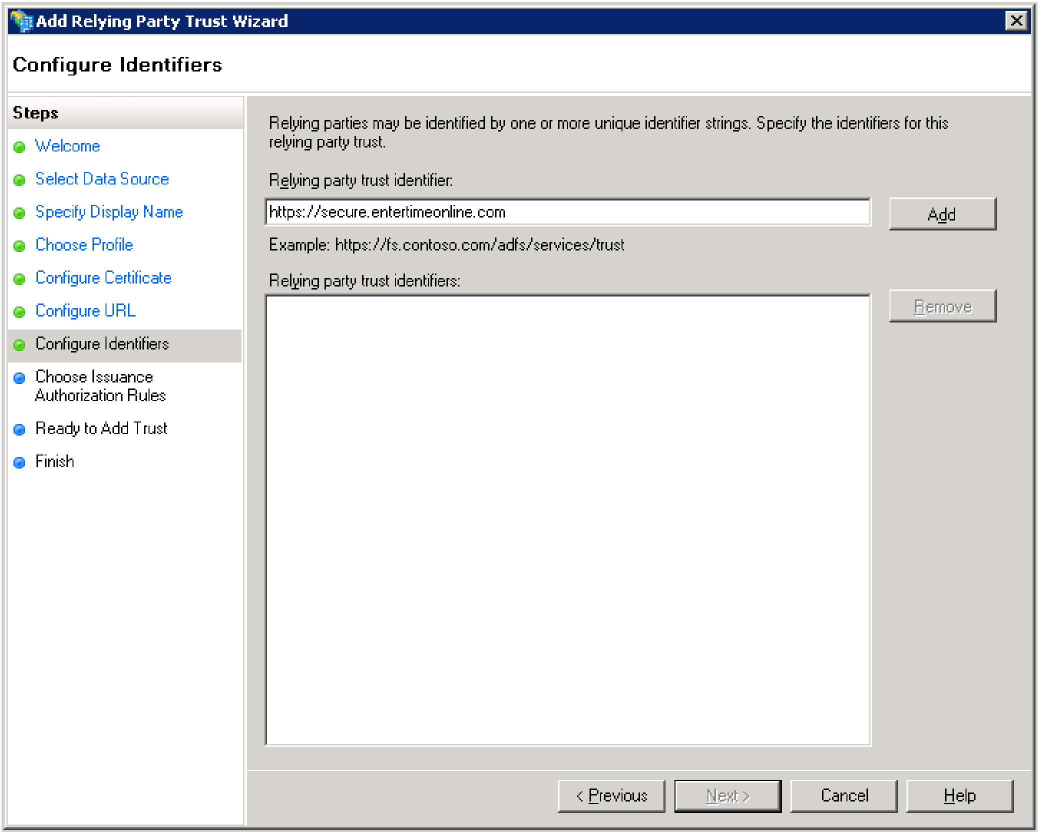
Unique Audience URL ☑

Endpoint URL:https://secure.saashr.com/ta/UBLJC.login-saml

Audience URL:https://secure.saashr.com/ta/UBLJC

5. Click the **Next** button.

6. In the **Configure Identifiers** section, you'll need to enter some system URLs. In the **Relying party trust identifier**, the system's SAML endpoint needs to be entered. This is the Audience URL shown in the **Service Provider Information** in the **Login/Logout Preferences** screen, for example: https://secure2.saashr.com



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier: https://secure.entertimeonline.com

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

7. Click the **Add** button then click the **Next** button.

8. For the **Choose Issuance Authorization Rules** section, select **Permit all users to access this relying party** then click the **Next** button.

9. For the **Ready to Add Trust section**, you can review the configuration on this screen. Once you are satisfied with the information click the **Next** button.

10. Click the **Close** button.

Claim Rules

You should now see a dialog box to add Claim rules to the **Trusted Resource** relying party that was just configured. There is only one claim that needs configuration before sending to the system: Name ID. The next steps show you how to configure this. As with any federation configuration, case sensitivity is critical. Please make sure to use the matching case when configuring the claim names.

1. In the **Trusted Resource Claim** rules click the **Add** button.

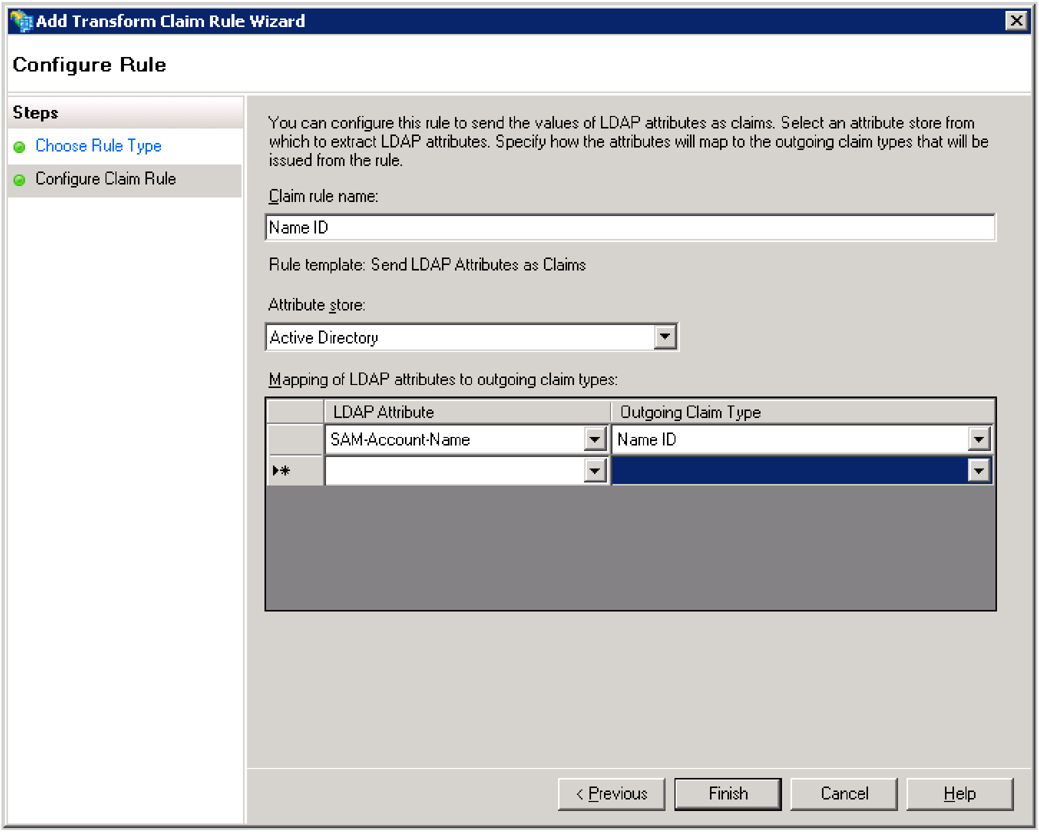
2. For the Claim rule template field, select **Send LDAP attributes as Claims** then click the **Next** button.

3. Enter any name for the Claim rule name, for example, **Name ID.**

4. For the **Attribute store** field, drop down and select **Active Directory**.

5. In the **LDAP Attribute** section, drop down and select **SAM-Account-Name**.

6. In the **Outgoing Claim Type** section, drop down and select **Name ID**.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Name ID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
	SAM-Account-Name	Name ID
▸*		

7. Click the **Finish** button.

8. Click the **OK** button on the Claim rule configuration for **Trusted Resource**.

   Since we have configured this as a SAML assertion we can use the LoginToRP feature with the IDPInitiatedSignon page to get the users signed into ADFS and then redirect them to WFR. Here is an example of this assuming that the ADFS server name is adfs.example.com. The URL would be:

   https://adfs.example.com/adfs/ls/IDPInitiatedSignon.aspx?LoginToRP=https://secure.entertimeonline.com

Configuring Single Sign-On OAuth 2.0

OAuth 2.0 (Open Authorization) provides clients secure delegated access to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials.

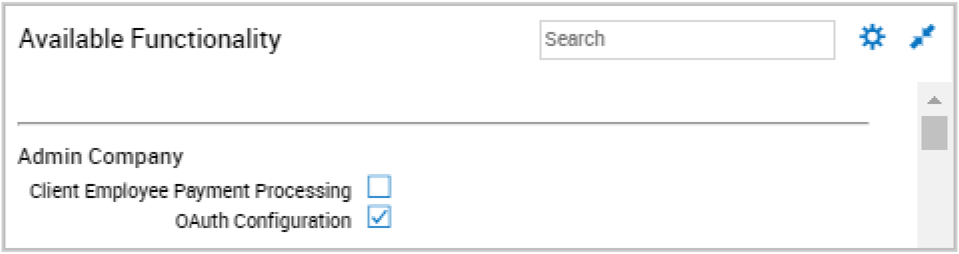
Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth 2.0 essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third-party then uses the access token to access the protected resources hosted by the resource server.

It works by delegating user authentication to the service that hosts the user account and authorizing third-party applications to access the user account. OAuth 2.0 provides authorization flows for mobile devices, as well as web and desktop applications.

> **Note:** For Partners, OAuth 2.0 can be added to Admin and Holding companies, but each client company must be configured individually.

Configuring OAuth 2.0

Enable OAuth 2.0 in the **Available Functionality** widget of your company. Check the OAuth Configuration checkbox, save and then log in as SA. This will make the widget available in Company Setup.

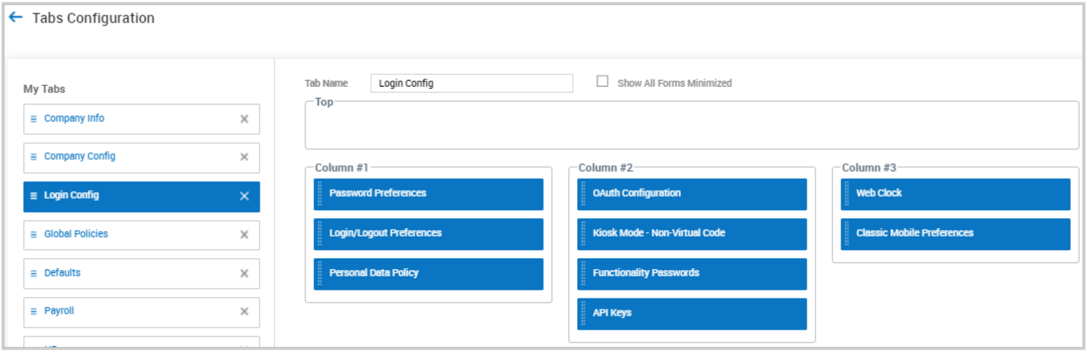


Admin Company

Client Employee Payment Processing □

OAuth Configuration ☑

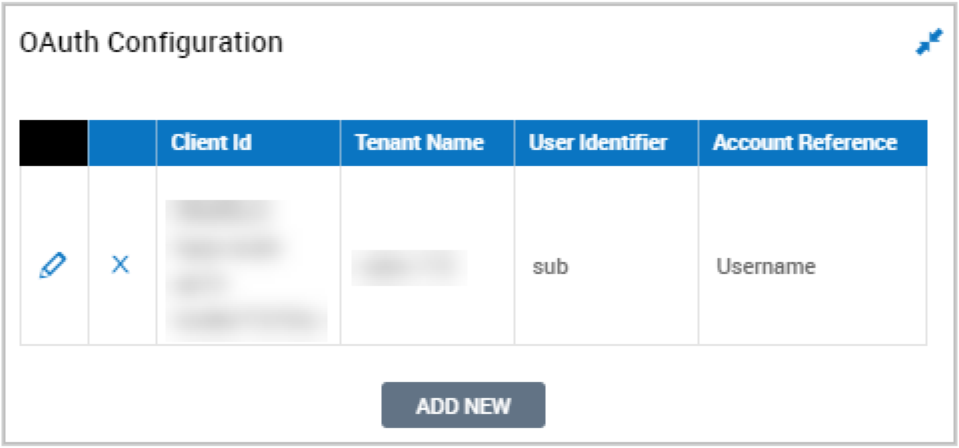
Navigate **to Company Settings > Global Setup > Company Setup**. From **Edit Tabs**, locate and drag the OAuth Configuration widget to the tab of your choice and save.



Tab Name: Login Config

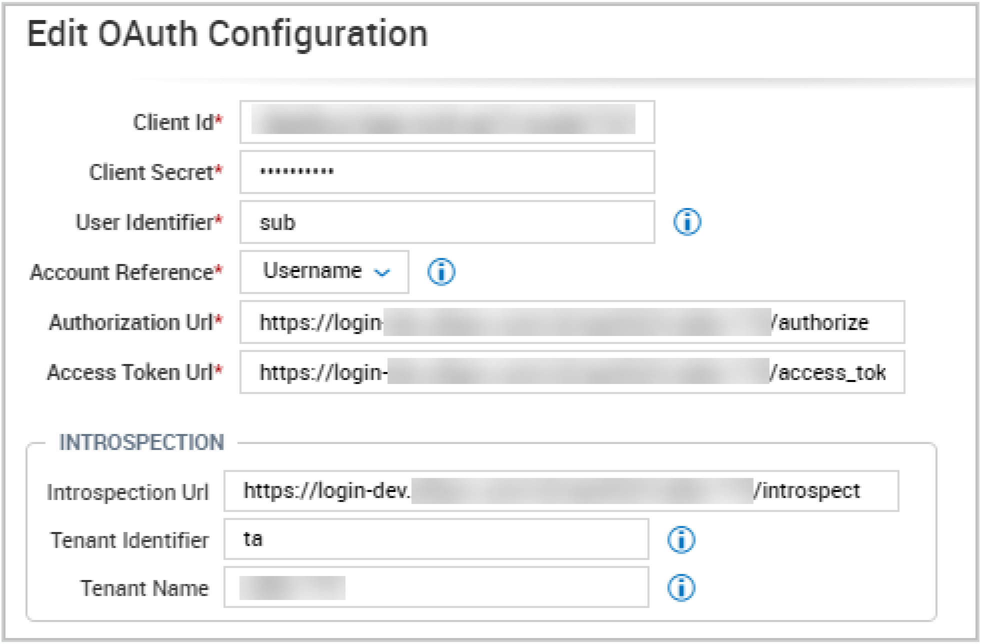
□ Show All Forms Minimized

From the widget, select Add New to create a new tenant.



OAuth Configuration

		Client Id	Tenant Name	User Identifier	Account Reference
✎	×	[redacted]	[redacted]	sub	Username



Edit OAuth Configuration

Client Id*	[redacted]
Client Secret*	••••••••••
User Identifier*	sub
Account Reference*	Username
Authorization Url*	https://login[redacted]/authorize
Access Token Url*	https://login-[redacted]/access_tok

INTROSPECTION

Introspection Url	https://login-dev.[redacted]/introspect
Tenant Identifier	ta
Tenant Name	[redacted]

With the exception of the **Account Reference** fields, the remaining fields will come from the authorization server. There are multiple OAuth vendors available. Once you have chosen one and have set up your account, the vendor will provide you with the information you need to complete this widget.

- **Client ID**: This is a required field and the ID will be generated by the authorization server.
- **Client Secret**: This is a required field and acts as a password.
- **User Identifier**: This is a required field. This identifier is the name of the standard field (claim) that identifies the subject (user) of the Access Token. It is used to identify the system user account in our system.
- **Account Reference**: This is a required field. You can select Account ID, Employee ID, External ID, or Username. This is used to match the user account information to the User Identifier value from the Access Token.
- **Authorization URL**: The authorization URL generated for your company from the authorization server.
- **Access Token URL**: The access token URL generated for your company from the authorization server.

- **Introspection URL**: The introspection URL generated for your company from the authorization server.

- **Tenant Identifier**: The name of the standard field (claim) that identifies the tenant (company) of the Introspection Token.

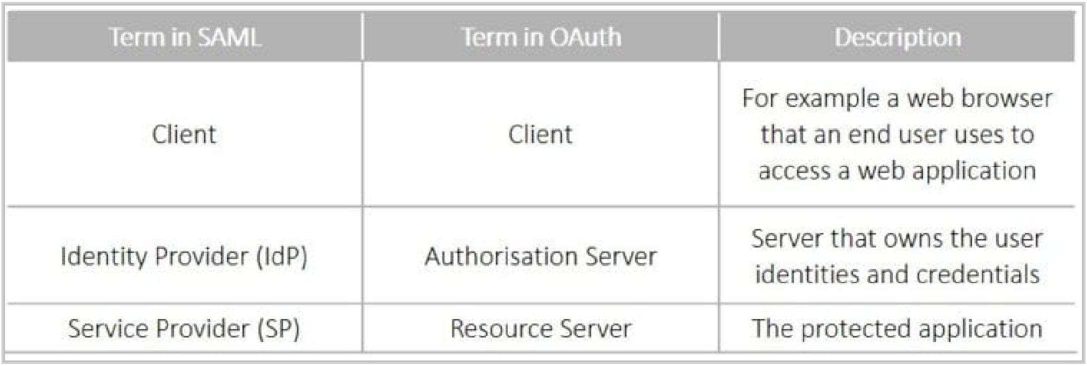
- **Tenant Name**: The expected value of the tenant. It should be matched to the Tenant Identifier value from the Introspection Token.

Differences Between SAML 2.0 and OAuth 2.0

You can use SAML 2.0 or OAuth 2.0 for Single Sign-On authorizations. Consider these differences between the two options.

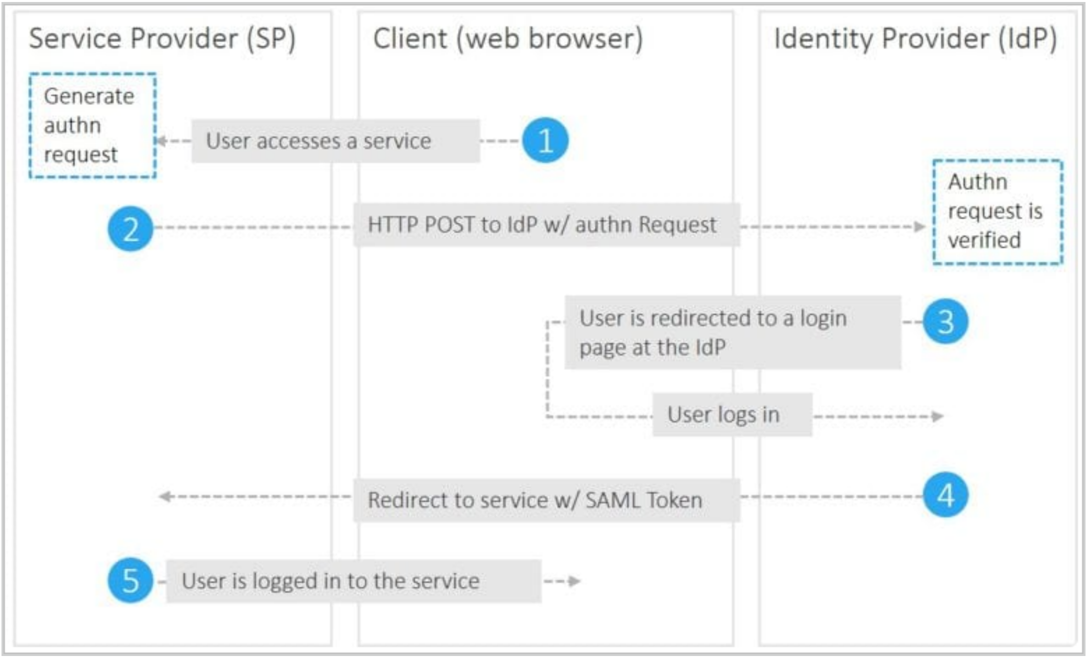
- OAuth 2.0 is primarily built for mobile environments.
- SAML 2.0 is more geared for desktop environments.

Also, be aware of the different definitions for the same terms between the two options.

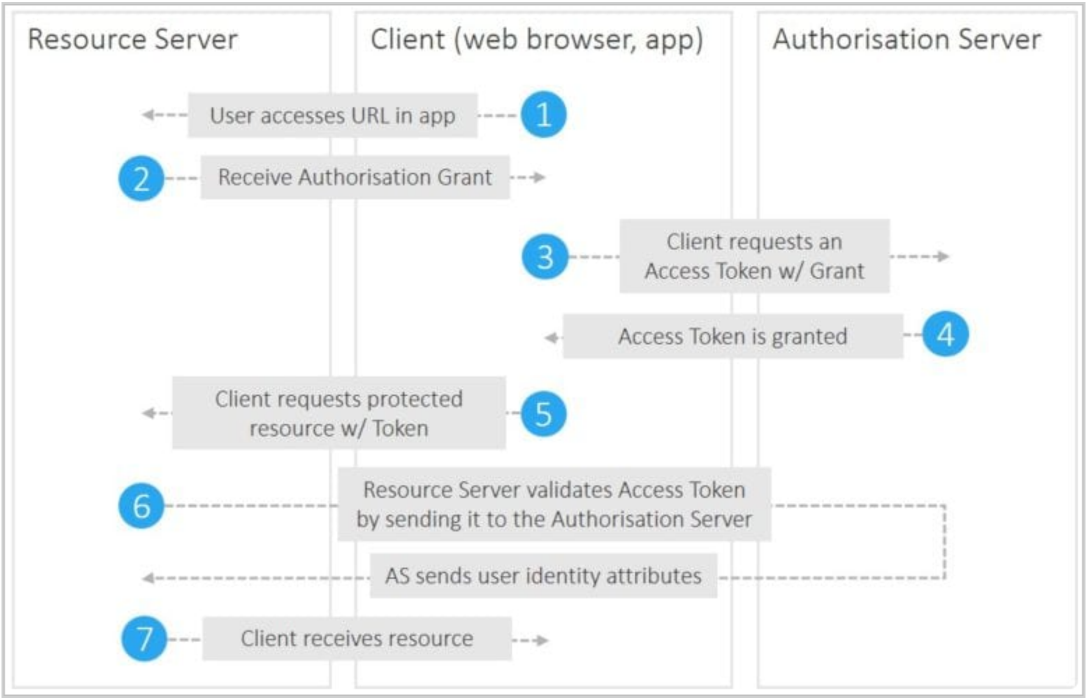


Term in SAML	Term in OAuth	Description
Client	Client	For example a web browser that an end user uses to access a web application
Identity Provider (IdP)	Authorisation Server	Server that owns the user identities and credentials
Service Provider (SP)	Resource Server	The protected application

SAML 2.0 Flow


Service Provider (SP)
Client (web browser)
Identity Provider (IdP)
Generate authn request
User accesses a service
1
2
HTTP POST to IdP w/ authn Request
Authn request is verified
User is redirected to a login page at the IdP
3
User logs in
Redirect to service w/ SAML Token
4
5
User is logged in to the service

OAuth 2.0 Flow


Resource Server
Client (web browser, app)
Authorisation Server
1
User accesses URL in app
2
Receive Authorisation Grant
3
Client requests an Access Token w/ Grant
4
Access Token is granted
5
Client requests protected resource w/ Token
6
Resource Server validates Access Token by sending it to the Authorisation Server
AS sends user identity attributes
7
Client receives resource