Azure SAML Security Manager

Live Forms supports the Azure Security Manager for Single Sign On. Users/roles are automatically pulled from Azure AD into Live Forms cloud tenants and on-premise installations. Users are redirected to the Microsoft Azure login screen for authentication.

frevvo recommends using the SAML Security Manager for customers who want to manage users/roles from the Live Forms UI.
On this page:

- Prerequisites
- Configuring the Azure SAML Security Manager
    - Step 1 - Create an Application for Live Forms in Azure
    - Step 2 - Create the Live Forms metadata file
    - Step 3 - Create the Azure Tenant Idp metadata file
    - Step 4 - Create/edit the Azure SAML tenant
    - Step 5 - Logging into a Live Forms Azure SAML Tenant
- Session Timeout
- Embedding Forms/Flows in your website
- Troubleshooting
- Retrieving Custom Attributes from Azure Active Directory in an Azure SAML Tenant
- Using the SharePoint Connector in an Azure SAML Security Manager tenant

Prerequisites

- You will need a valid Microsoft Azure subscription
- The **frevvo.TenantAdmin** and **frevvo.Designer groups** must be specified on your Active Directory server. The group names must be spelled as shown. Upper/lower case may be a factor for Open LDAP systems. These groups are required.
    - Tenant admin users must be assigned to the **frevvo.TenantAdmin** group.
    - Designer users must be assigned to the **frevvo.Designer** group

- Contact the frevvo Customer Success team to schedule your Security Manager configuration.
- frevvo Best Practice recommends that you create a user account in your Active Directory that will house all of your deployed Production forms/flows. This user can be named anything i.e.frevvoProduction but it must be a member of the frevvo.Designer group
- If you want to preserve Applications/Forms/Flows developed in your trial/starter tenant to your desktop, perform these steps **BEFORE** changing the Security Manager. :
    1. Download the Applications/Forms/Flows that you want to preserve to your desktop as a backup. Do this for all Live Forms user accounts that have Applications/Forms/flows that you want to keep.
    2. When the backup of all Applications/Forms/flows is completed, delete the user accounts in your Default Security Manager tenant.
- There are two additional roles in Live Forms - **frevvo.Publisher** and **frevvo.ReadOnly.** These roles are optional.
    - In order to give a user the frevvo.publishers role, create the **frevvo.Publisher** group in your AD and assign users to it. Refer to the Administrator Best Practices for an explanation of this role.
    - In order to give a user the frevvo.ReadOnly role, create the **frevvo.ReadOnly** group in your AD and assign users to it. Following frevvo Best Practice eliminates the need for this role.
- frevvo only supports the Azure Security Manager when Live Forms is running in the tomcat container. Refer to our Supported Platforms for the list of supported/certified Application Servers.

Configuring the Azure SAML Security Manager

Follow these steps listed below to create a Live Forms tenant using the Azure SAML Security Manager:

1. Create an Application for Live Forms in Azure
2. Create the Live Forms metadata file
3. Create the Azure Tenant IDP metadata file
4. Create/edit the Live Forms tenant
5. Log into your Live Forms tenant

Step 1 - Create an Application for Live Forms in Azure

frevvo assumes that customers have someone on staff that can successfully perform this step of the procedure. Information about Live Forms is listed below to help you with this process.

> The Azure global administrator **MUST** create the application for Live Forms in Azure.

If you are familiar with the Microsoft Azure Legacy Portal, review this Microsoft Training Guide before setting up the Azure application for Live Forms.

Click here for some more tips....

> Do not include the curly braces in the URLs discussed below.

1. Login to the Microsoft Azure Management console: https://manage.windowsazure.com or https://portal.azure.com with your Azure global administrator account.
2. Click on the **Azure Active directory** link on the left side of the screen.
3. Click on the **App Registrations** link.
4. Click on the **New application** registration link for creating a new application.
5. Enter the following details:
    a. Name:- Name of your frevvo Azure application
    b. Select who can use this application or access this API
6. **Configure the Redirect URL:**
    a. Cloud Customers should use https://app.frevvo.com:443/frevvo/web/saml/SSO/alias/{t} - replace {t} with name of your frevvo tenant.

    > For example, if you were changing the Security Manager from the Default Security Manager to the Azure SAML Security Manager for a frevvo Cloud tenant named mycompany.com, the REPLY URL would be:
    >
    > https://app.frevvo.com:443/frevvo/web/saml/SSO/alias/mycompany.com

    b. On-premise customers should use http://<server>:<port>/frevvo/web/saml/SSO/alias/{t} - replace <server> with the ip of your server, <port> with the port number (if applicable) and t with the name of your frevvo in-house tenant.

    > For example, if you were changing the Security Manager from the Default Security Manager to the Azure SAML Security Manager for a frevvo in-house tenant named mycompany.com, the REPLY URL would be:
    >
    > https://<server:port>/frevvo/web/saml/SSO/alias/mycompany.com

    c. Click **Register**.
7. Select the frevvo application from the list.
8. Click the **Branding** tab
9. **Configure the Home Page URL:**
    a. Cloud Customers should use https://app.frevvo.com:443/frevvo/web/tn/{t}/login - replace {t} with the name of your frevvo Cloud tenant.

    > For example, if you were changing the Security Manager from the Default Security Manager to the Azure SAML Security Manager for a frevvo Cloud tenant named mycompany.com, the SIGN-ON URL would be:
    >
    > https://app.frevvo.com:443/frevvo/web/tn/mycompany.com/login

    b. On-premise customers should use http://<server>:<port>/frevvo/web/tn/{t}/login - replace <server> with the ip of your server, <port> with the port number (if applicable) and t with the name of your frevvo in-house tenant.

    > For example, if you were changing the Security Manager from the Default Security Manager to the Azure SAML Security Manager for a frevvo in-house tenant named mycompany.com, the SIGN-ON URL would be:
    >
    > https://<server:port>frevvo/web/tn/mycompany.com/login

    c. Click **Save**.
10. Click on the **API Permissions** tab.
    a. Click **Add a Permission.**
    b. Select **Azure Active Directory Graph** from the **Supported legacy APIs** section.
    c. For Application Permissions, select **Read and write directory data (under Directory)**.
    d. For Delegated Permissions, select **Sign in and read user profile (under User) AND Read directory data under (under Directory)**.
    e. Click on the **Grant Permissions** button select "Yes" option and click on the **Save** button.
11. Click on the **Expose an API** tab.
    a. **Configure the Application ID URI:**

i. Cloud Customers should use https://app.frevvo.com:443/frevvo/web/alias/{t} - replace {t} with the name of your frevvo Cloud tenant.

> For example, if you were changing the Security Manager from the Default Security Manager to the Azure SAML Security Manager for a frevvo Cloud tenant named mycompany.com,the AP ID URL would be:
>
> https://app.frevvo.com:443/frevvo/web/alias/mycompany.com

ii. On-premise customers should use http://<server>:<port>/frevvo/web/alias/{t} - replace <server> with the ip of your server, <port> with the port number (if applicable) and {t} with the name of your frevvo in-house tenant.

> For example, if you were changing the Security Manager from the Default Security Manager to the Azure SAML Security Manager for a frevvo in-house tenant named mycompany.com, the AP ID URL would be:
>
> https://<server:port>/frevvo/web/alias/mycompany.com

iii. Click **Save**.

12. Click the **Certifiates & secrets** tab.
    a. Generate the **Client Secret**. **COPY/SAVE the VALUE in a notepad - you will need this for the frevvo tenant screen. There is only one chance to retrieve the client secret key when you create the application for Live Forms in Azure. Once you leave this screen the value will be hidden.**
13. Click the **Overview** tab.
    a. Copy the **Application ID** into your notepad. This is the value of the Client ID on the frevvo configuration screen.
    b. Copy the **Directory ID** into your notepad. This is the value of the Tenant ID on the frevvo configuration screen.
    Click **Endpoints** at the top of the screen. Copy the Federation Metadata Document URL from the list to your notepad. This is the URL that you will use to generate the Azure metadata

Example of the Federation Metadata Document URL

```
https://login.microsoftonline.com/3d532ac1-a43c-45c7-b0e9-cc814400ca11/fe
derationmetadata/2007-06/federationmetadata.xml
```

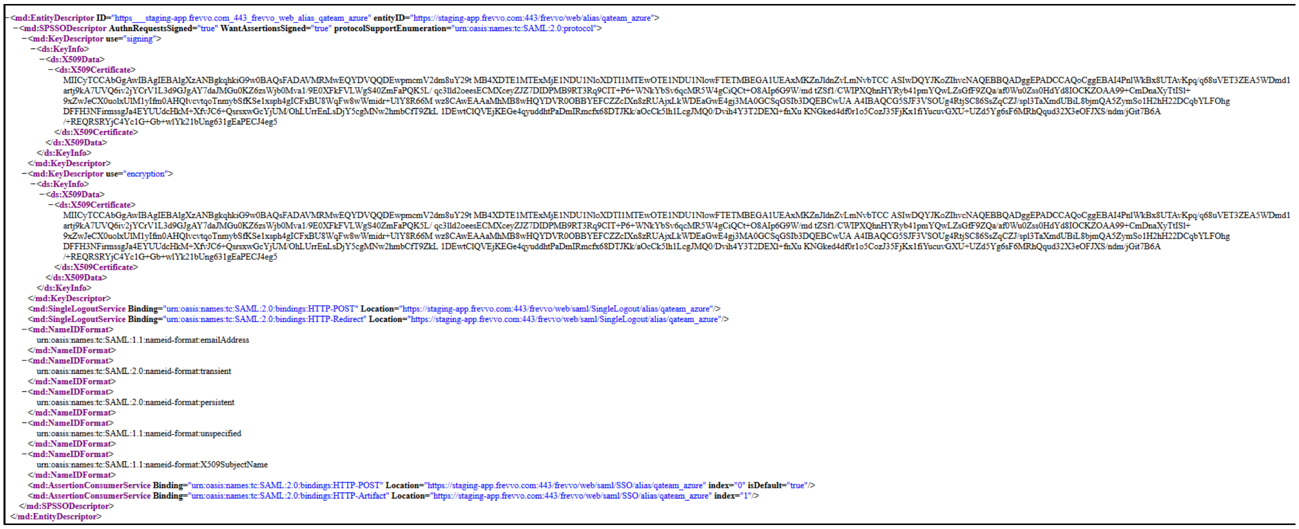
14. Proceed to Step 2 - Create the Live Forms metadata file

> Just a reminder - you will need the **Azure tenant ID, the client id and client secret** for the frevvo application when configuring your Live Forms Azure SAML tenant.

Step 2 - Create the Live Forms metadata file

Follow these steps to generate the frevvo metadata for your Azure SAML tenant. You can do this even if the tenant has not been created yet.

1. Paste this URL into your browsr:
    a. Cloud Customers: https://app.frevvo.com:443/frevvo/web/saml/metadata/alias/{t} - replace {t} with the name of your Live Forms tenant - Ex; azuread
    b. On-premise customers: http://<server>:<port>/frevvo/web/saml/metadata/alias/{t} - replace <server> with the ip of your server, <port> with the port number (if applicable) and t with the name of your frevvo tenant.
2. When the metadata displays, save the page as an xml file.



```
−<md:EntityDescriptor ID="https___staging-app.frevvo.com_443_frevvo_web_alias_qateam_azure" entityID="https://staging-app.frevvo.com:443/frevvo/web/alias/qateam_azure">
  −<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    −<md:KeyDescriptor use="signing">
      −<ds:KeyInfo>
        −<ds:X509Data>
          −<ds:X509Certificate>
             MIICyTCCAbGgAwIBAgIEBAlgXzANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDEwpmcmV2dm8uY29t MB4XDTE1MTExMjE1NDU1NloXDTI1MTEwOTE1NDU1NlowFTETMBEGA1UEAxMKZnJldnZvLmNvbTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI4Pn1WkBx8UTAvKpq/q68uVET3ZEA5WDmd1
             artj9kA7UVQ6iv2jYCrV1L3d9GJgAY7daJMGu0KZ6zsWjb0Mva1/9E0XFkFVLWgS40ZmFaPQK5L/ qc3lld2oeesECMXceyZJZ7DIDPMB9RT3Rq9CIT+P6+WNkYbSv6qcMR5W4gCiQCt+O8AIp6G9W/md tZSf1/CWIPXQhnHYRyb41pmYQwLZsGfF9ZQa/af0Wu0Zss0HdYd8IOCKZOAA99+CmDnaXyTtISl+
             9xZwJeCX0uolxUlM1yIfm0AHQlvcvtqoTnmybSfKSe1xsph4gICFxBU8WqFw8wWmidr+UlY8R66M wz8CAwEAAaMhMB8wHQYDVR0OBBYEFCZZcIXn8zRUAjxLkWDEaGwE4gj3MA0GCSqGSIb3DQEBCwUA A4IBAQCG5SJF3VSOUg4RtjSC86SsZqCZJ/spl3TaXmdUBiL8bjmQA5ZymSo1H2hH22DCqbYLFOhg
             DFFH3NFirmssgJa4EYUUdcHkM+XfvJC6+QsrsxwGcYjUM/OhLUrrEnLsDjY5cgMNw2hmbCfT9ZkL 1DEwtCIQVEjKEGe4qyuddhtPaDmIRmcfx68DTJKk/aOcCk5lh1LcgJMQ0/Dvih4Y3T2DEXl+fnXu KNGked4df0r1o5CozJ35FjKx1fiYucuvGXU+UZd5Yg6sF6MRhQqud32X3eOFJXS/ndm/jGit7B6A
             /+REQRSRYjC4Yc1G+Gb+w1Yk21bUng631gEaPECJ4eg5
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    −<md:KeyDescriptor use="encryption">
      −<ds:KeyInfo>
        −<ds:X509Data>
          −<ds:X509Certificate>
             MIICyTCCAbGgAwIBAgIEBAlgXzANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDEwpmcmV2dm8uY29t MB4XDTE1MTExMjE1NDU1NloXDTI1MTEwOTE1NDU1NlowFTETMBEGA1UEAxMKZnJldnZvLmNvbTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI4Pn1WkBx8UTAvKpq/q68uVET3ZEA5WDmd1
             artj9kA7UVQ6iv2jYCrV1L3d9GJgAY7daJMGu0KZ6zsWjb0Mva1/9E0XFkFVLWgS40ZmFaPQK5L/ qc3lld2oeesECMXceyZJZ7DIDPMB9RT3Rq9CIT+P6+WNkYbSv6qcMR5W4gCiQCt+O8AIp6G9W/md tZSf1/CWIPXQhnHYRyb41pmYQwLZsGfF9ZQa/af0Wu0Zss0HdYd8IOCKZOAA99+CmDnaXyTtISl+
             9xZwJeCX0uolxUlM1yIfm0AHQlvcvtqoTnmybSfKSe1xsph4gICFxBU8WqFw8wWmidr+UlY8R66M wz8CAwEAAaMhMB8wHQYDVR0OBBYEFCZZcIXn8zRUAjxLkWDEaGwE4gj3MA0GCSqGSIb3DQEBCwUA A4IBAQCG5SJF3VSOUg4RtjSC86SsZqCZJ/spl3TaXmdUBiL8bjmQA5ZymSo1H2hH22DCqbYLFOhg
             DFFH3NFirmssgJa4EYUUdcHkM+XfvJC6+QsrsxwGcYjUM/OhLUrrEnLsDjY5cgMNw2hmbCfT9ZkL 1DEwtCIQVEjKEGe4qyuddhtPaDmIRmcfx68DTJKk/aOcCk5lh1LcgJMQ0/Dvih4Y3T2DEXl+fnXu KNGked4df0r1o5CozJ35FjKx1fiYucuvGXU+UZd5Yg6sF6MRhQqud32X3eOFJXS/ndm/jGit7B6A
             /+REQRSRYjC4Yc1G+Gb+w1Yk21bUng631gEaPECJ4eg5
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://staging-app.frevvo.com:443/frevvo/web/saml/SingleLogout/alias/qateam_azure"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://staging-app.frevvo.com:443/frevvo/web/saml/SingleLogout/alias/qateam_azure"/>
    −<md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </md:NameIDFormat>
    −<md:NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:transient
    </md:NameIDFormat>
    −<md:NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
    </md:NameIDFormat>
    −<md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </md:NameIDFormat>
    −<md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
    </md:NameIDFormat>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://staging-app.frevvo.com:443/frevvo/web/saml/SSO/alias/qateam_azure" index="0" isDefault="true"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://staging-app.frevvo.com:443/frevvo/web/saml/SSO/alias/qateam_azure" index="1"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

3. We will need to copy the entire metadata from this file to the Azure SAML Security Manager configuration screen.
4. Metadata must be generated for each Azure SAML tenant. Each tenant will have a unique URL.

Step 3 - Create the Azure Tenant Idp metadata file

Follow these steps:

1. Browse the Federation Metadata Document URL that you copied to your notepad when creating the Azure application for Live Forms. It is located on the **Endpoints** tab in your frevvo Azure application.

Example of Federation Metadata Document URL from Endpoints

```
https://login.microsoftonline.com/fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2/Federation
Metadata/2007-06/FederationMetadata.xml
```

2. Save all the metadata returned as an xml file. We will need to copy the entire metadata from this file to the Azure SAML Security Manager configuration screen.

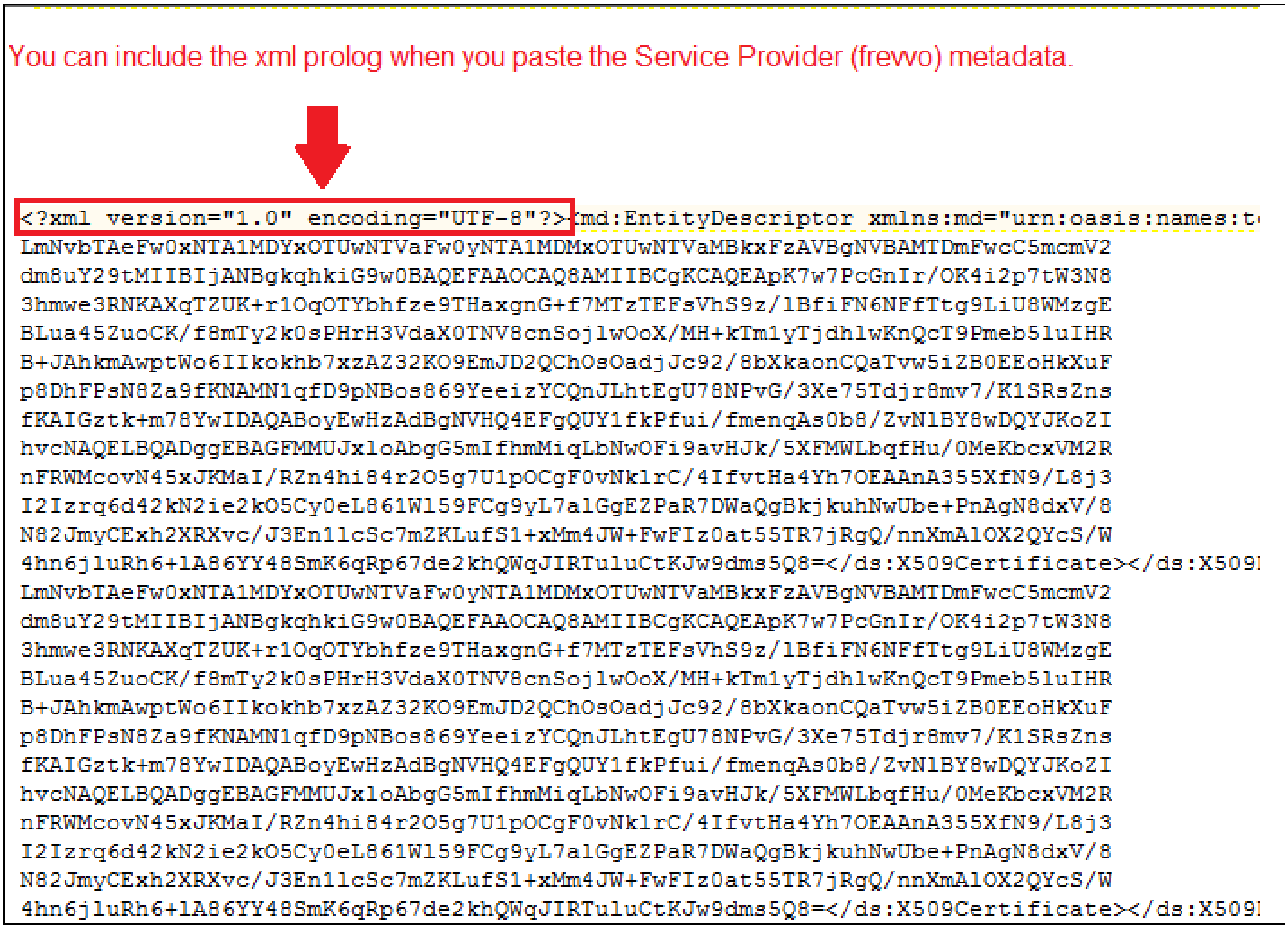
Step 4 - Create/edit the Azure SAML tenant

To successfully create a Live Forms tenant using the Azure SAML Security manager, you will need the following:

- Live Forms metadata file
- The Azure SAML tenant Idp metadata file
- Attribute mapping information
- The Azure tenant ID, the client id and client secret key that are created as part of registering the frevvo application.

Live Forms cloud customers, migrating your tenant to the Azure SAML Security Manager, will make the changes via the Edit Tenant screen. Once accessed, follow these steps beginning with step 3.

1. Log onto Live Forms as the superuser (on-premise) or the tenant admin (cloud).
2. Access the Add Tenant (on-premise) or Edit Tenant (cloud) screen.
3. Select Azure SAML Security Manager from the Security Manager Class dropdown.
4. Copy the Service Provider (frevvo) metadata into the Service Provider field. You can include the xml prolog when you paste the Service Provider (frevvo) metadata.

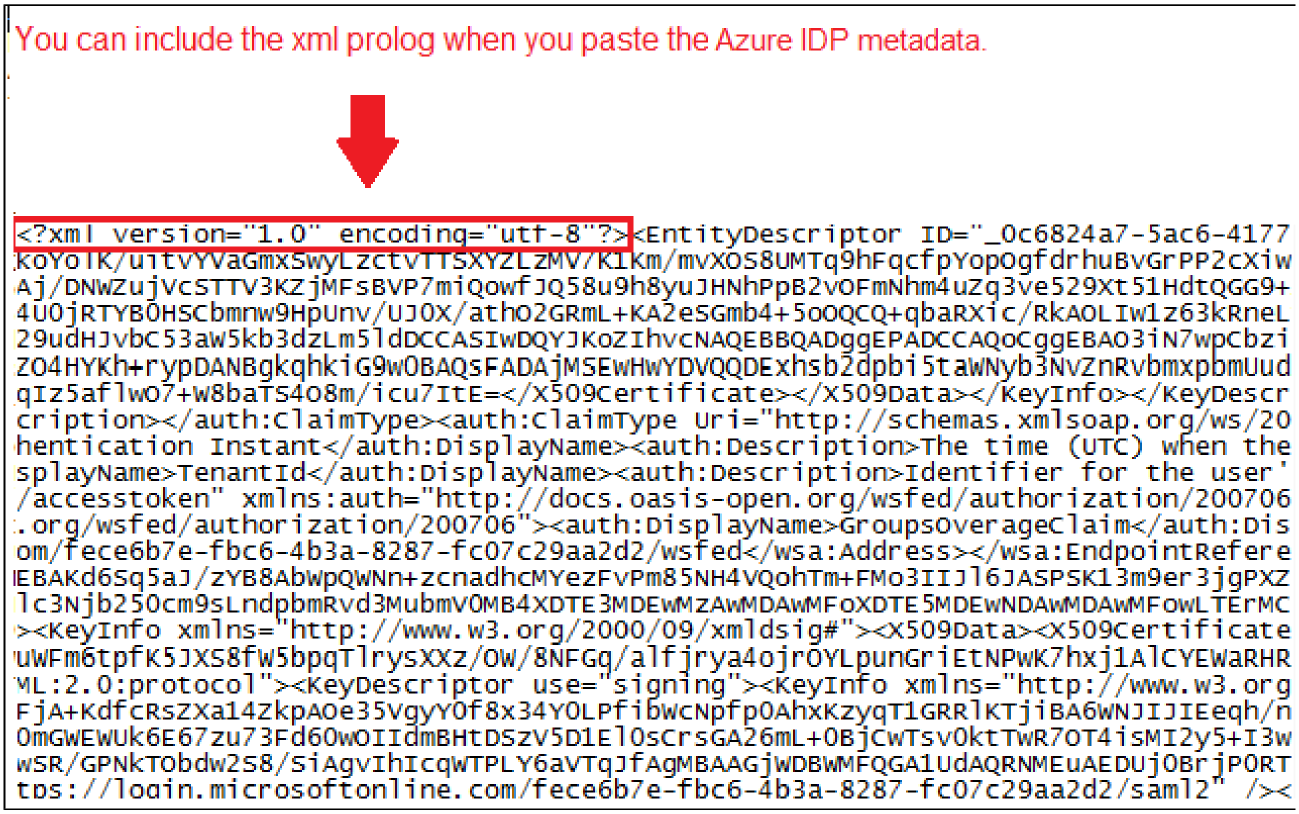


You can include the xml prolog when you paste the Service Provider (frevvo) metadata.

```
<?xml version="1.0" encoding="UTF-8"?>md:EntityDescriptor xmlns:md="urn:oasis:names:t
LmNvbTAeFw0xNTA1MDYxOTUwNTVaFw0yNTA1MDMxOTUwNTVaMBkxFzAVBgNVBAMTDmFwcC5mcmV2
dm8uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApK7w7PcGnIr/OK4i2p7tW3N8
3hmwe3RNKAXqTZUK+r1OqOTYbhfze9THaxgnG+f7MTzTEFsVhS9z/lBfiFN6NFfTtg9LiU8WMzgE
BLua45ZuoCK/f8mTy2k0sPHrH3VdaX0TNV8cnSojlwOoX/MH+kTm1yTjdhlwKnQcT9Pmeb5luIHR
B+JAhkmAwptWo6IIkokhb7xzAZ32KO9EmJD2QChOsOadjJc92/8bXkaonCQaTvw5iZB0EEoHkXuF
p8DhFPsN8Za9fKNAMN1qfD9pNBos869YeeizYCQnJLhtEgU78NPvG/3Xe75Tdjr8mv7/K1SRsZns
fKAIGztk+m78YwIDAQABoyEwHzAdBgNVHQ4EFgQUY1fkPfui/fmenqAs0b8/ZvNlBY8wDQYJKoZI
hvcNAQELBQADggEBAGFMMUJxloAbgG5mIfhmMiqLbNwOFi9avHJk/5XFMWLbqfHu/0MeKbcxVM2R
nFRWMcovN45xJKMaI/RZn4hi84r205g7U1pOCgF0vNklrC/4IfvtHa4Yh7OEAAnA355XfN9/L8j3
I2Izrq6d42kN2ie2kO5Cy0eL861W159FCg9yL7alGgEZPaR7DWaQgBkjkuhNwUbe+PnAgN8dxV/8
N82JmyCExh2XRXvc/J3En1lcSc7mZKLufS1+xMm4JW+FwFIz0at55TR7jRgQ/nnXmAlOX2QYcS/W
4hn6jluRh6+lA86YY48SmK6qRp67de2khQWqJIRTuluCtKJw9dms5Q8=</ds:X509Certificate></ds:X509
```

```
LmNvbTAeFw0xNTA1MDYxOTUwNTVaFw0yNTA1MDMxOTUwNTVaMBkxFzAVBgNVBAMTDmFwcC5mcmV2
dm8uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApK7w7PcGnIr/OK4i2p7tW3N8
3hmwe3RNKAXqTZUK+r1OqOTYbhfze9THaxgnG+f7MTzTEFsVhS9z/lBfiFN6NFfTtg9LiU8WMzgE
BLua45ZuoCK/f8mTy2k0sPHrH3VdaX0TNV8cnSojlwOoX/MH+kTm1yTjdhlwKnQcT9Pmeb5luIHR
B+JAhkmAwptWo6IIkokhb7xzAZ32KO9EmJD2QChOsOadjJc92/8bXkaonCQaTvw5iZB0EEoHkXuF
p8DhFPsN8Za9fKNAMN1qfD9pNBos869YeeizYCQnJLhtEgU78NPvG/3Xe75Tdjr8mv7/K1SRsZns
fKAIGztk+m78YwIDAQABoyEwHzAdBgNVHQ4EFgQUY1fkPfui/fmenqAs0b8/ZvNlBY8wDQYJKoZI
hvcNAQELBQADggEBAGFMMUJxloAbgG5mIfhmMiqLbNwOFi9avHJk/5XFMWLbqfHu/0MeKbcxVM2R
nFRWMcovN45xJKMaI/RZn4hi84r205g7U1pOCgF0vNklrC/4IfvtHa4Yh7OEAAnA355XfN9/L8j3
I2Izrq6d42kN2ie2kO5Cy0eL861W159FCg9yL7alGgEZPaR7DWaQgBkjkuhNwUbe+PnAgN8dxV/8
N82JmyCExh2XRXvc/J3En1lcSc7mZKLufS1+xMm4JW+FwFIz0at55TR7jRgQ/nnXmAlOX2QYcS/W
4hn6jluRh6+lA86YY48SmK6qRp67de2khQWqJIRTuluCtKJw9dms5Q8=</ds:X509Certificate></ds:X509
```

5. Copy the metadata from the Azure tenant IDP file previously created and paste it into the Identity Provider field.



You can include the xml prolog when you paste the Azure IDP metadata.

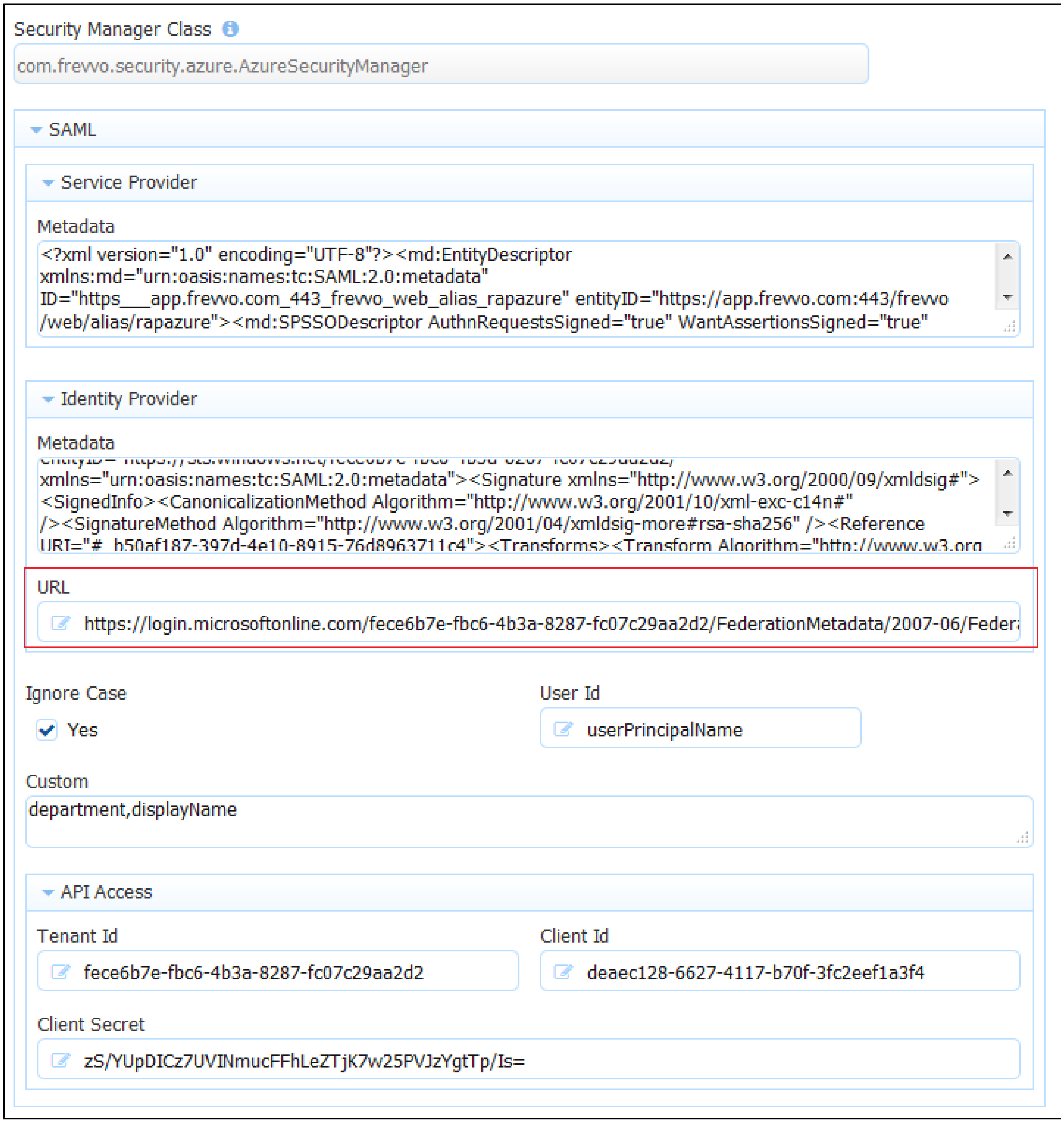
```
<?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID="_0c6824a7-5ac6-4177
koYoIK/uitvYVaGmxSwyLzctvTTSXYZLzMV/K1Km/mvXOS8UMTq9hFqcfpYopOgfdrhuBvGrPP2cXiw
Aj/DNWZujVcSTTV3KZjMFsBVP7miQowfJQ58u9h8yuJHNhPpB2vOFmNhm4uZq3ve529Xt51HdtQGG9+
4U0jRTYB0HSCbmnw9HpUnv/UJOX/athO2GRmL+KA2eSGmb4+5oOQCQ+qbaRXic/RkAOLIw1z63kRneL
29udHJvbC53aW5kb3dzLm5ldDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAO3iN7wpCbzi
ZO4HYKh+rypDANBgkqhkiG9w0BAQsFADAjMSEwHwYDVQQDExhsb2dpbi5taWNyb3NvZnRvbmxpbmUud
qIz5aflwO7+W8baTS4o8m/icu7ItE=</X509Certificate></X509Data></KeyInfo></KeyDescr
cription></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/20
hentication Instant</auth:DisplayName><auth:Description>The time (UTC) when the
splayName>TenantId</auth:DisplayName><auth:Description>Identifier for the user'
/accesstoken" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706
.org/wsfed/authorization/200706"><auth:DisplayName>GroupsOverageClaim</auth:Dis
om/fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2/wsfed</wsa:Address></wsa:EndpointRefere
EBAKd6Sq5aJ/zYB8AbwpQWNn+zcnadhcMYezFvPm85NH4VQohTm+FMo3IIJl6JASPSK13m9er3jgPXZ
lc3Njb250cm9sLndpbmRvd3MubmV0MB4XDTE3MDEwMzAwMDAwMFoXDTE5MDEwNDAwMDAwMFowLTErMC
><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certificate
uWFm6tpfK5JXS8fW5bpqTlrysXXz/OW/8NFGq/alfjrya4ojrOYLpunGriEtNPwK7hxj1AlCYEWaRHR
ML:2.0:protocol"><KeyDescriptor use="signing"><KeyInfo xmlns="http://www.w3.org
FjA+KdfcRsZXa14ZkpAOe35VgyYOf8x34YOLPfibWcNpfp0AhxKzyqT1GRRlKTjiBA6WNJIJIEeqh/n
OmGWEWUk6E67zu73Fd60wOIIdmBHtDSzV5D1ElOsCrsGA26mL+0BjCwTsvOktTwR7OT4isMI2y5+I3w
wSR/GPNkTObdw2S8/SiAgvIhIcqWTPLY6aVTqJfAgMBAAGjWDBWMFQGA1UdAQRNMEuAEDUjOBrjPORT
tps://login.microsoftonline.com/fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2/saml2" /><
```

6. Enter the Federation Metadata Document URL that you copied from **Endpoints** in your frevvo Azure application. The URL is needed to handle Signing key rollover in Azure Active Directory. This URL is polled and refreshes the Azure IDP metadata every 3 hours. The new metadata is stored and automatically used as backup in case the URL is not accessible.

    Example of Federation Metadata Document URL

    ```
    https://login.microsoftonline.com/fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2/FederationMetadata/2007-06/FederationMetadata.xml
    ```

7. Check the **Ignore Case** checkbox if you are using LDAP for authentication and you want Live Forms to ignore the case stored in LDAP systems for users/roles. The field is checked by default. Refer to the Mixed or Upper case User Names topic for more information.
8. Enter the User Id. This should be the User property name that identifies the user. A typical value is userPrincipalName, givenname etc.
9. Custom attributes can be mapped by typing the attribute **names** in the Custom field separated by a comma.
10. Enter the following information in the API Access section.
    - a. Enter the Azure tenant identifier into the tenant Id field. This can be obtained by viewing the endpoint Urls listed when you click **View Endpoints** in your frevvo Azure application.
    - b. Enter the client id and client secret key that were created as part of registering the frevvo application into the respective fields.



Security Manager Class

com.frevvo.security.azure.AzureSecurityManager

SAML

Service Provider

Metadata

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https___app.frevvo.com_443_frevvo_web_alias_rapazure" entityID="https://app.frevvo.com:443/frevvo
/web/alias/rapazure"><md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
```

Identity Provider

Metadata

```
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference
URI="#_b50af187-397d-4e10-8915-76d8963711c4"><Transforms><Transform Algorithm="http://www.w3.org
```

URL

https://login.microsoftonline.com/fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2/FederationMetadata/2007-06/Feder

Ignore Case

☑ Yes

User Id

userPrincipalName

Custom

department,displayName

API Access

Tenant Id

fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2

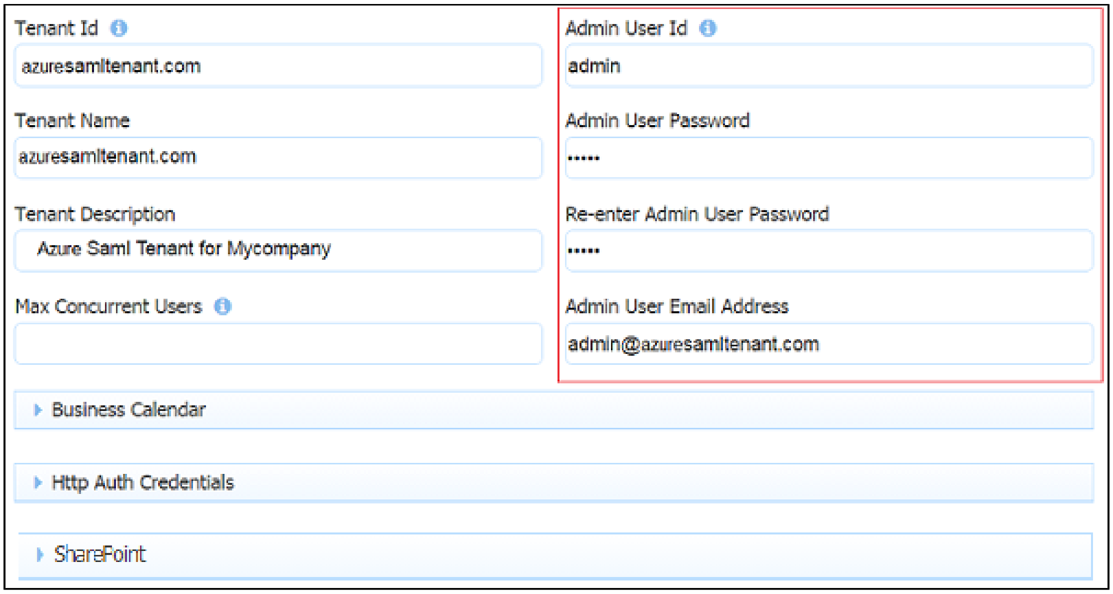
Client Id

deaec128-6627-4117-b70f-3fc2eef1a3f4

Client Secret

zS/YUpDICz7UVINmucFFhLeZTjK7w25PVJzYgtTp/Is=

11. Configure a tenant admin account. This account does not require Azure SAML authentication. This tenant admin can log directly into Live Forms providing a default security manager backdoor.
    a. The tenant admin id, password and email fields are required.
    b. When this tenant admin performs a form based login i.e. /frevvo/web/login, the password entered on this screen is used for authentication. This is also the URL used by the API.
    c. If the tenant based login url is used i.e. /frevvo/web/tn/{t}/login then the Azure SAML login is used.



Tenant Id
azuresamltenant.com

Tenant Name
azuresamltenant.com

Tenant Description
Azure Saml Tenant for Mycompany

Max Concurrent Users

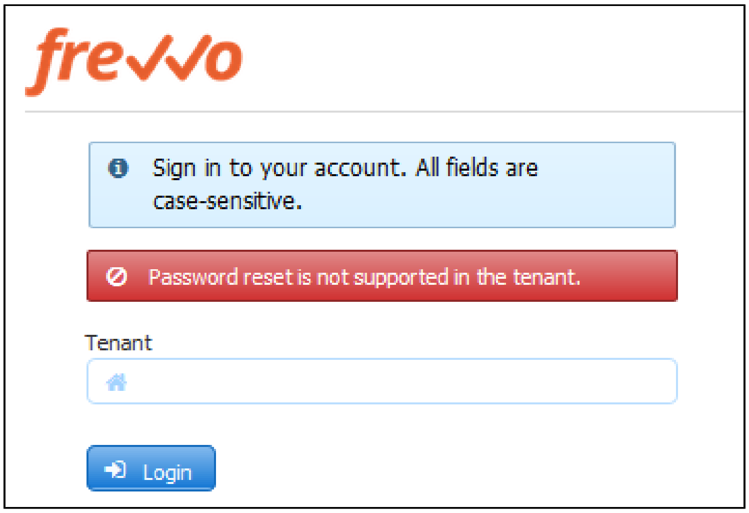
Admin User Id
admin

Admin User Password
•••••

Re-enter Admin User Password
•••••

Admin User Email Address
admin@azuresamltenant.com

The forgot password function works for an Azure SAML tenant admin user. For all others, it will display the error message about not being supported for the tenant.

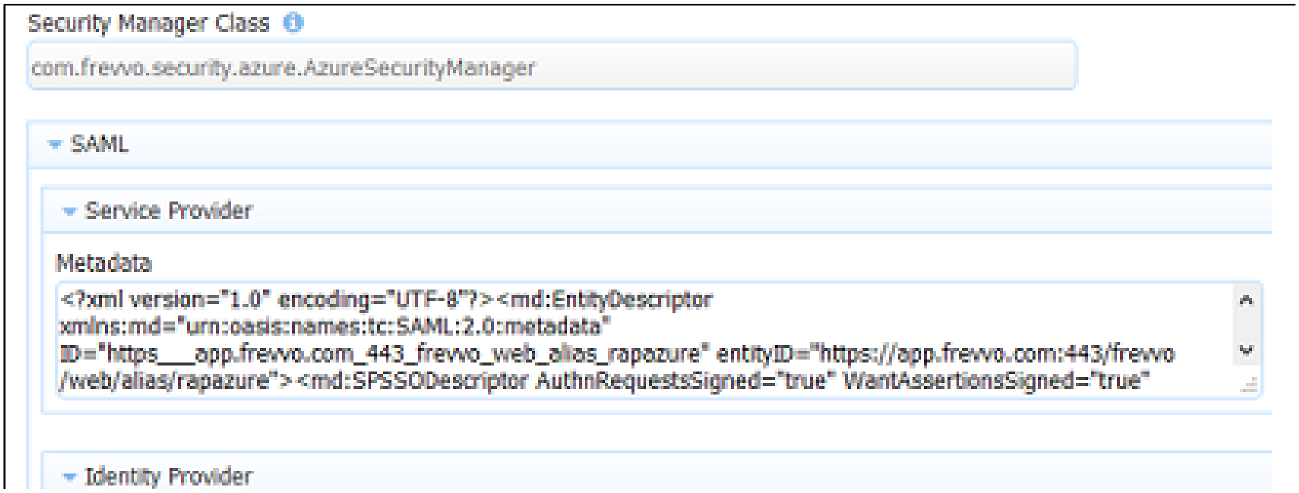


Sign in to your account. All fields are case-sensitive.

Password reset is not supported in the tenant.

Tenant

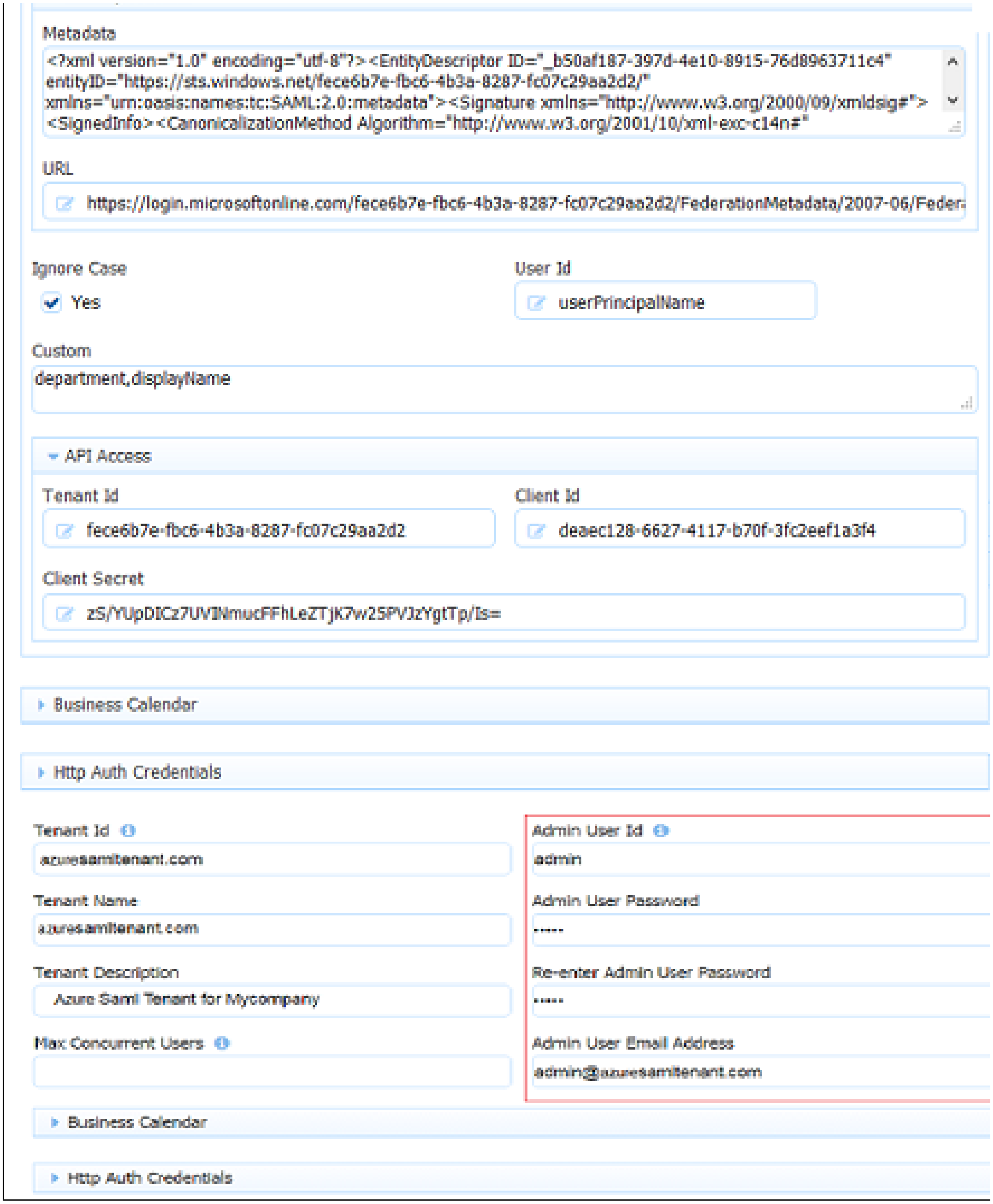
12. Configure the Business Calendar for your tenant. The Live Forms escalation feature will use this calendar to calculate deadlines and send notification and reminder emails.
13. Enter HTTP Auth credentials if required. Credentials for external secure web services accessed by the forms and flows in your tenant can be specified in this section.
14. Click Submit.



Security Manager Class
com.frevvo.security.azure.AzureSecurityManager

Metadata

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https___app.frevvo.com_443_frevvo_web_alias_rapazure" entityID="https://app.frevvo.com:443/frevvo
/web/alias/rapazure"><md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
```



Metadata

```
<?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID="_b50af187-397d-4e10-8915-76d8963711c4"
entityID="https://sts.windows.net/fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2/"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
```

URL

https://login.microsoftonline.com/fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2/FederationMetadata/2007-06/Feder

Ignore Case

☑ Yes

User Id

userPrincipalName

Custom

department,displayName

Tenant Id

fece6b7e-fbc6-4b3a-8287-fc07c29aa2d2

Client Id

deaec128-6627-4117-b70f-3fc2eef1a3f4

Client Secret

zS/YUpDICz7UVINmucFFhLeZTjK7w25PVJzYgtTp/Is=

Tenant Id

azuresamltenant.com

Tenant Name

azuresamltenant.com

Tenant Description

Azure Saml Tenant for Mycompany

Max Concurrent Users

Admin User Id

admin

Admin User Password

•••••

Re-enter Admin User Password

•••••

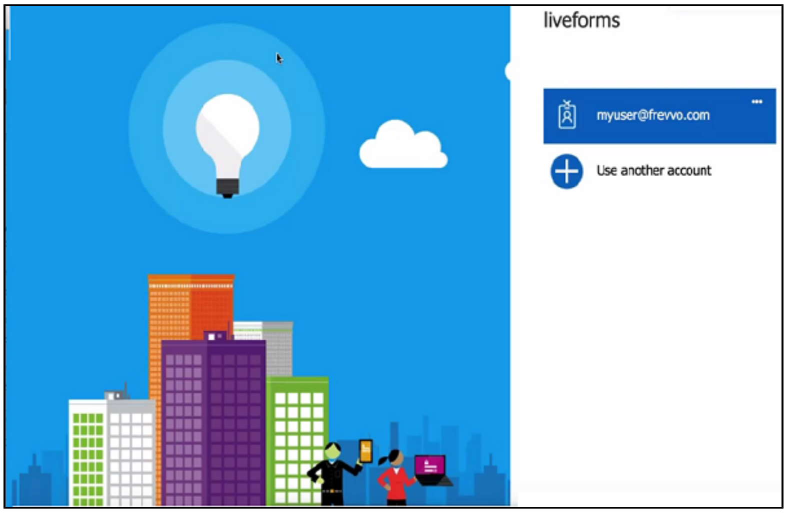
Admin User Email Address

admin@azuresamltenant.com

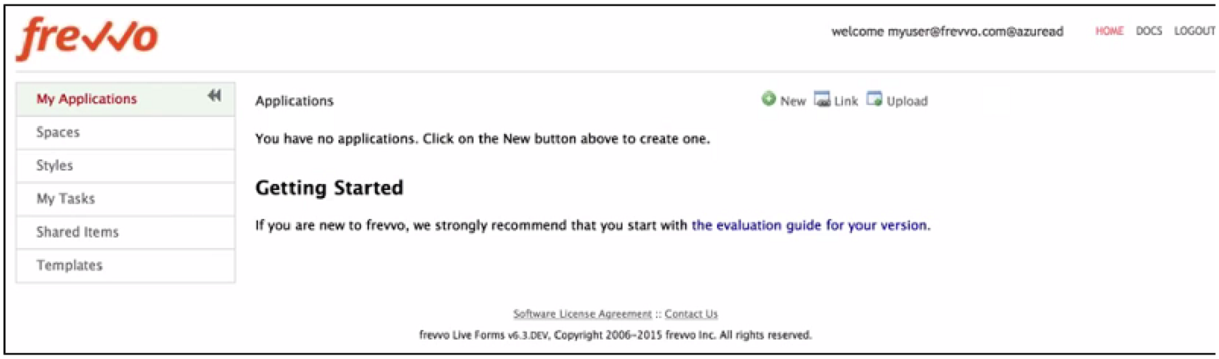
Step 5 - Logging into a Live Forms Azure SAML Tenant

1. Paste this tenant specific URL into your browser:
    a. Cloud Customers: **https://app.frevvo.com:443/frevvo/web/tn/{t}/login -** Replace {t} with the name of your Azure SAML tenant.
    b. On-premise Customers:**http://<server>:<port>/frevvo/web/tn/{t}/login**. Replace <server> and <port> with your server information and t with the name of your Azure SAML tenant.

c. The user is redirected to the Azure login screen.



d. If the user is authenticated, Live Forms screens display depending on the level of authorization specified for the user. Designer users will see the Application Home Page while non-designer users will be directed to their Task List.



You have no applications. Click on the New button above to create one.

Getting Started

If you are new to frevvo, we strongly recommend that you start with the evaluation guide for your version.

Software License Agreement :: Contact Us

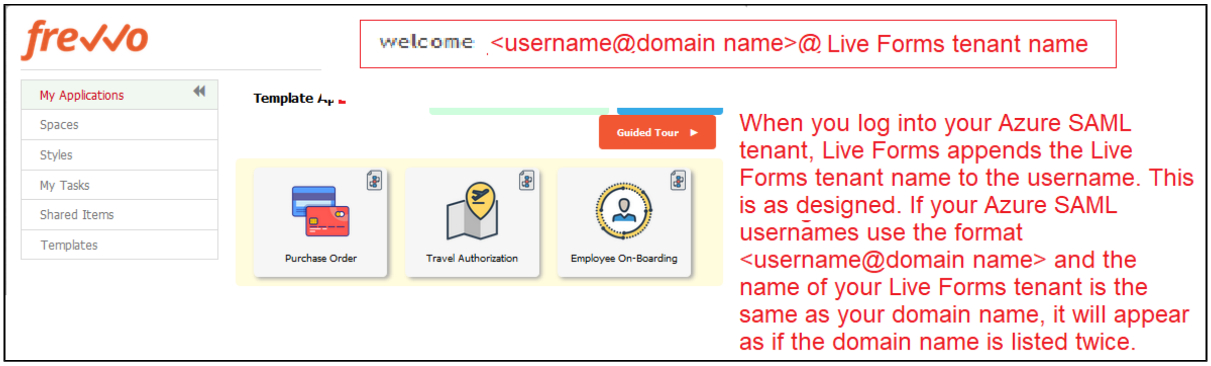
frevvo Live Forms v6.3.DEV, Copyright 2006-2015 frevvo Inc. All rights reserved.

You will see this redirection when logging into a Live Forms space as well.

- Clicking the logout link in Live Forms, logs the user out from Live Forms only.
- When a user logs in to space, the logout link will not be visible in an Azure AD (SSO) tenant.
- When a user logs in to Live Forms (non-space mode), the logout link will be visible in an Azure AD (SSO) tenant.

Logged in User Display in Azure SAML Live Forms tenant

If your Azure SAML userIds are in the format <username>@<domain name>, when you login to Live Forms the Live Forms tenant name is appended to the userId . This is as designed. You will see <username@domain name@frevvo tenant name> as the logged in user at the top of the screen. If your domain name is the same as your Live Forms tenant name, it will appear as if the domain name is listed twice.



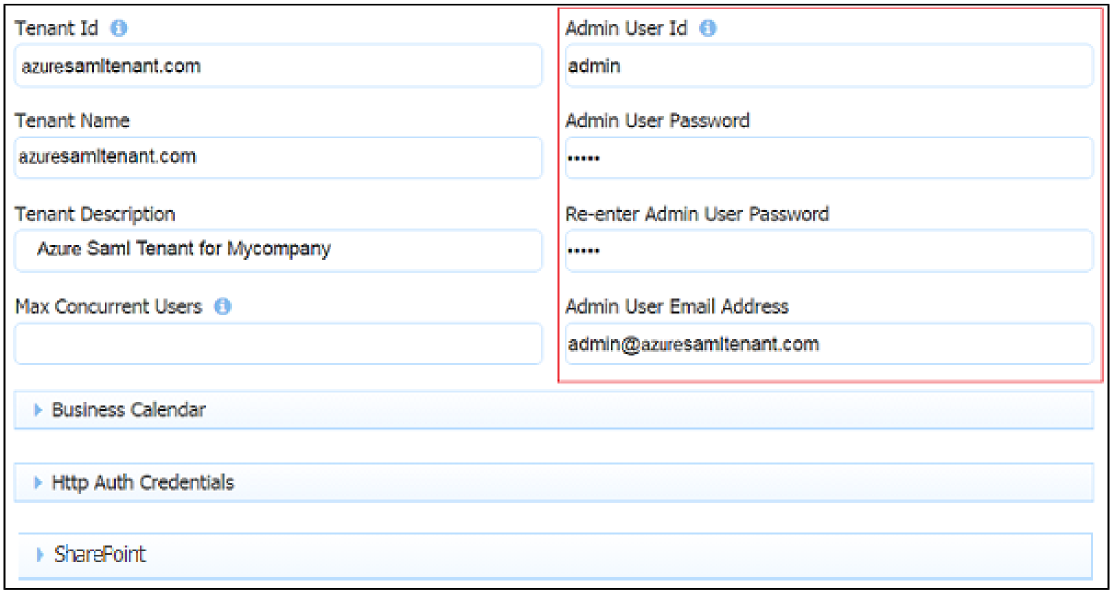
welcome <username@domain name>@ Live Forms tenant name

When you log into your Azure SAML tenant, Live Forms appends the Live Forms tenant name to the username. This is as designed. If your Azure SAML usernames use the format <username@domain name> and the name of your Live Forms tenant is the same as your domain name, it will appear as if the domain name is listed twice.

Azure SAML Tenant backdoor admin user

Just a reminder that the tenant admin account can login directly into Live Forms or use the Azure SAML login.

When you create a new tenant you are prompted to set up a tenant admin user id and password. This tenant admin does not authenticate via your Azure SAML IDP. It only exists in Live Forms. If you experience an issue with your Azure SAML configuration such that you can't login as an Azure SAML authenticated user, this account provides a backdoor you can use to login to your tenant as a tenant admin in order to fix your Azure SAML configuration issue. Only one backdoor tenant admin account is supported.



Tenant Id: azuresamltenant.com

Tenant Name: azuresamltenant.com

Tenant Description: Azure Saml Tenant for Mycompany

Max Concurrent Users:

Admin User Id: admin

Admin User Password: •••••

Re-enter Admin User Password: •••••

Admin User Email Address: admin@azuresamltenant.com

If your tenant originally used the Default Security Manager and then you changed to the Azure SAML Security Manager, this tenant admin account has already been setup. If you have forgotten the password, you can change it by :

- Using the Live Forms Forgot Password? feature for the tenant admin account.
- Logging in as a Azure SAML authenticated tenant admin and changing the password via Manage Users.

What if you do not remember the userid of your original tenant admin? Follow these steps:

1. Login as your authenticated Azure SAML tenant admin
2. Click Manage Users and click the
   edit admin icon.

Session Timeout

Session timeouts are configured in Live Forms and in your Azure SAML IDP. If a user's session ends before the IDP timeout is reached, they will automatically be logged back into Live Forms if they try to access it again. It is recommended that the Live Forms session timeout and the IDP session timeout be configured for the same value.

Embedding Forms/Flows in your website

Embedding forms and flows into your website when using the Azure SAML Security Manager, will work in the following scenarios :

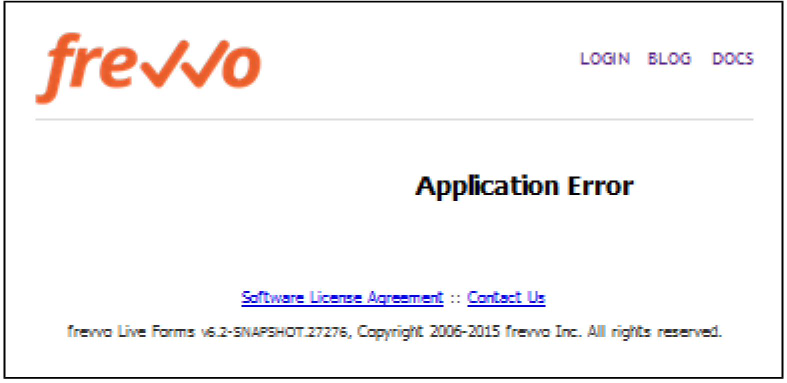
- The visibility of the form is set to Public.
- The visibility of the form is set to Public in Tenant and the user is already authenticated to Azure SAML

> Embedding forms and flows into your website is NOT supported if the the visibility of the form is set to Public in Tenant and the user is NOT already authenticated to Azure SAML. This is because frevvo must direct the user to the IDP login screen and the browser will not allow loading the IDP login page in frevvo's form iframe.

Troubleshooting

Logging into a Azure SAML tenant as (user@Azure SAML tenant name)

Logging into a Azure SAML tenant as (user@Azure SAML tenant name) displays an application error message.



Application Error

Software License Agreement :: Contact Us

frevvo Live Forms v6.2-SNAPSHOT.27276, Copyright 2006-2015 frevvo Inc. All rights reserved.

On-premise customers using the tomcat bundle will see the following entry in the Live Forms error log:

```
Application error processing /frevvo/web/login?null
java.lang.UnsupportedOperationException: null
```

Accessing a Space in a AzureAD tenant on a mobile device will not display a logout button.

Skew error when logging into an Azure tenant

Users logging into a Live Forms Azure SAML tenant may encounter the error "Access Denied. Authorization Required". Examination of the frevvo.log shows the following entry:

```
Response issue time is either too old or with date in the future, skew 60, time
2016-06-01T05:49:25.330Z
```

This error is typically caused by a clock synchronization issue between the SP (frevvo) and the Idp (Azure) or a genuine delay in the connection. If you get this error, you can change the value of the context parameter, **com.frevvo.security.saml.response.skew**, to specify the time in seconds allowed between the SAML request and response to a value greater than the default value of 60 seconds.

Follow the instructions listed in the Installation Tasks chapter to add the parameter.

Login into the Live Forms Azure SAML tenant fails

If the login into your Azure SAML tenant fails and the Live Forms log reports the following error, you may have to edit your Azure SAML tenant to add the metadata URL. T

```
org.opensaml.xml.validation.ValidationException: Signature is not trusted or invalid.
```

The URL is needed to handle Signing key rollover in Azure Active Directory. This URL is polled and refreshes the Azure IDP metadata every 3 hours. The new metadata is stored and used as backup in case the URL is not accessible. Refer to **Step 6** above for the details.

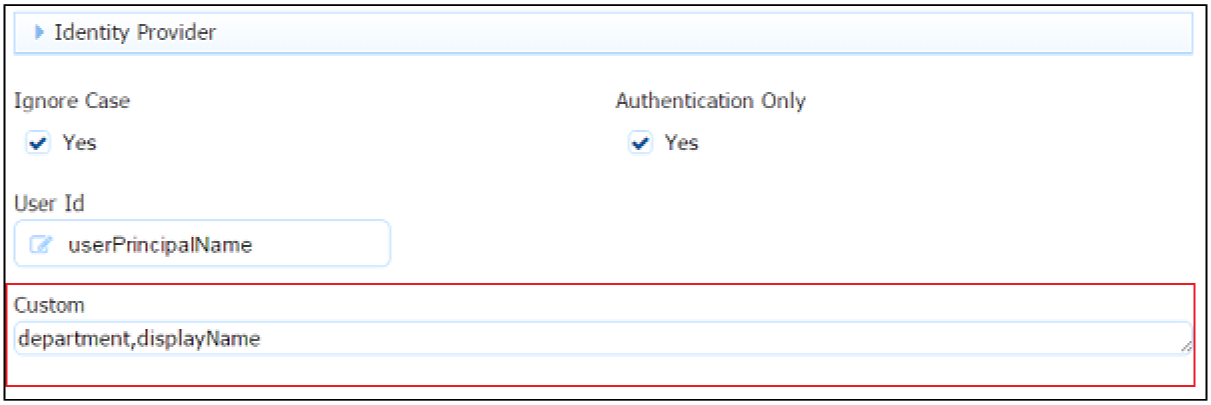
Retrieving Custom Attributes from Azure Active Directory in an Azure SAML Tenant

The Azure AD Graph API allows access to users, groups etc... in Azure AD. User entity attribute data exposed by the API for the logged in user can be pulled into fields in your form/flow with a business rule. If the attribute that you are looking for is not already exposed, you can:

- Sync Azure AD to your in-house AD via the Microsoft provided connector
- Add an extension property

Once the custom attributes are made available, add them to the Custom section of your Azure SAML tenant.

1. Login to your Azure SAML tenant as the as the tenant admin.
2. Click the Edit Tenant link
3. Add the custom attributes to the Custom section as a comma separated list. The image shows the department and displayName attributes listed in the custom attribute section.



Identity Provider

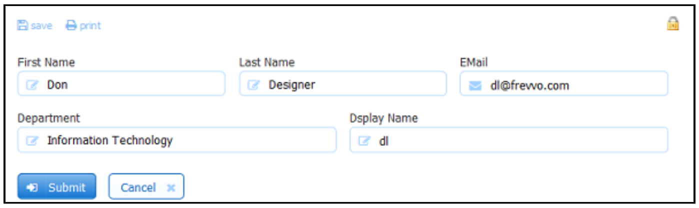
Ignore Case
☑ Yes

Authentication Only
☑ Yes

User Id
userPrincipalName

Custom
department,displayName

4. Design your form/flow with fields to collect the information.
5. Write a business rule to populate the controls with the custom attribute information.



First Name: Don
Last Name: Designer
EMail: dl@frevvo.com
Department: Information Technology
Dsplay Name: dl

Here is an example of a rule that will retrieve the custom attributes, department and displayName, plus the standard attributes, First Name, Last Name and Email address.

```
if (form.load) {
    FirstName.value =
_data.getParameter('subject.first.name'
);
    LastName.value =
_data.getParameter('subject.last.name')
;
    EMail.value =
_data.getParameter('subject.email');
    department.value =
_data.getParameter('subject.department'
);
    displayName.value =
_data.getParameter('subject.displayName
');
}
```

Using the SharePoint Connector in an Azure SAML Security Manager tenant

At least one designer user that is going to be connecting forms/flows to SharePoint with the Save to SharePoint wizard must also be a SharePoint user with the correct privileges to provide consent if your tenant is configured with the Azure SAML Security Manager .