

SAML 2.0 Setup

Alloantibody Exchange

Exchange of Configuration Information

<u>SAML 2.0 Configuration Settings Exchange</u>	
<u>Alloantibody Exchange Provides...</u>	<u>Health System Provides...</u>
SAML 2.0 Metadata - Available at alloantibody.org as a URL . (Ref 1, Step 2)	SAML 2.0 Metadata URL - Required for input into Microsoft Entra Id - External Identities. The metadata URL automatically updates the certificates as they expire. (See Ref 1, Step 3.)
Required attributes and claims are listed in the Ref 1, Step 2 tables .	

Notes:

1. The Alloantibody Exchange will check if the new trust relationship with the identity provider has a matching "Domain name of federating IdP" and "Passive authentication endpoint". If they do not, the health system must add a DNS TXT record. (Ref 1, Step 1)

Examples of matched and unmatched. The domain name is "fabrikam.com"	
Match	Do not match
<code>https://fabrikam.com</code>	<code>https://fabrikamconglomerate.com/adfs</code>
<code>https://sts.fabrikam.com/adfs</code>	<code>https://fabrikam.com.uk/adfs</code>

2. The Alloantibody Exchange will register the health system's metadata URL in Azure as shown.

The screenshot shows the Microsoft Entra ID External Identities console. The 'External Identities' tab is selected, and the 'All identity providers' view is active. A '+ New SAML/WS-Fed IdP' button is highlighted. The configuration form for the new IdP is shown, with the following fields:

- Display name *
- Identity provider protocol * (SAML)
- Domain name of federating IdP * (fabrikam.com)
- Select a method for populating metadata * (Parse metadata file)
- Metadata file (Browse for file)
- Issuer URI * (http://www.example.com/exk10l6w90DHM0yi...)
- Passive authentication endpoint * (https://outlooknk1.example.com/app/outlook...)
- Certificate * (MIIDpDCCAoygAwIBAgIGAWLVA3DIM)
- Metadata URL (https://idp.example.com:9031/pf/federation_...)

3. Guest users will be sent an invitation. If you are asked to create a new password, stop the process and contact george.hauser@alloantibody.org. This may require communication with your directory administrator.

The screenshot shows an email invitation from Transfusion Antibody Exchange Inc. The email content is as follows:

Transfusion Antibody Exchange Inc. invited you to access applications within their organization

M Microsoft Invitations on behalf of Transfusion Antibody Exchange Inc.
To: Hauser, George

i Please only act on this email if you trust the organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Organization: Transfusion Antibody Exchange Inc.
Domain: alloantibody.org

This message was provided by the sender and is not from Microsoft Corporation.

RH Message from Transfusion Antibody Exchange Inc.:

References

1. <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/direct-federation>