SAML 2.0 Setup

Alloantibody Exchange

Exchange of Configuration Information

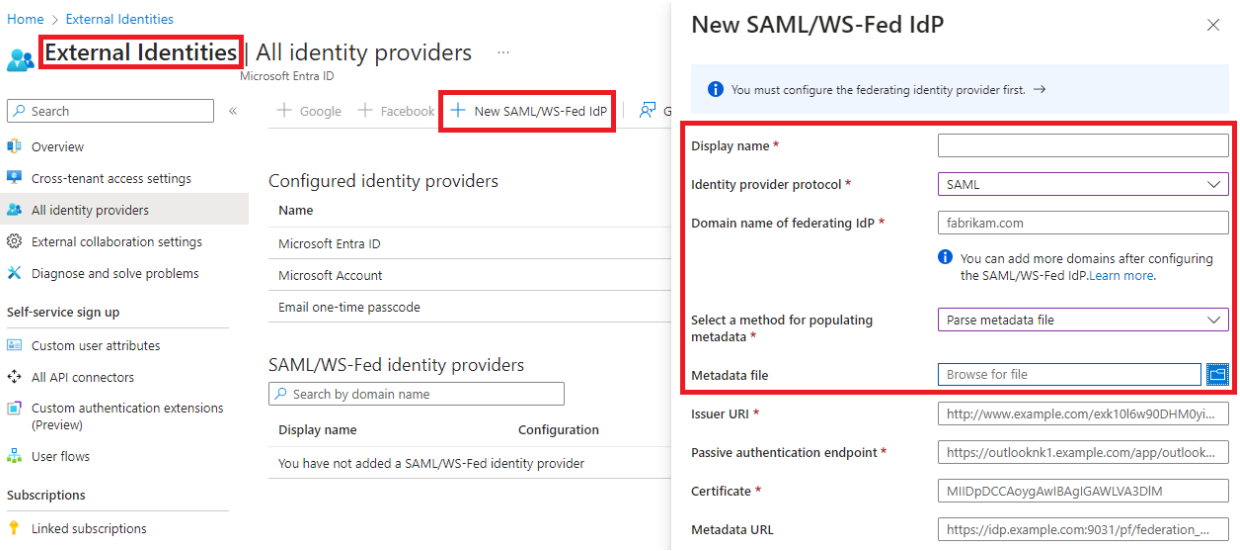
SAML 2.0 Configuration Settings Exchange	
Alloantibody Exchange Provides…	Health System Provides…
SAML 2.0 Metadata - Available at alloantibody.org as a URL. (Ref 1, Step 2)	SAML 2.0 Metadata URL - Required for input into Microsoft Entra Id - External Identities. The metadata URL automatically updates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

Notes:

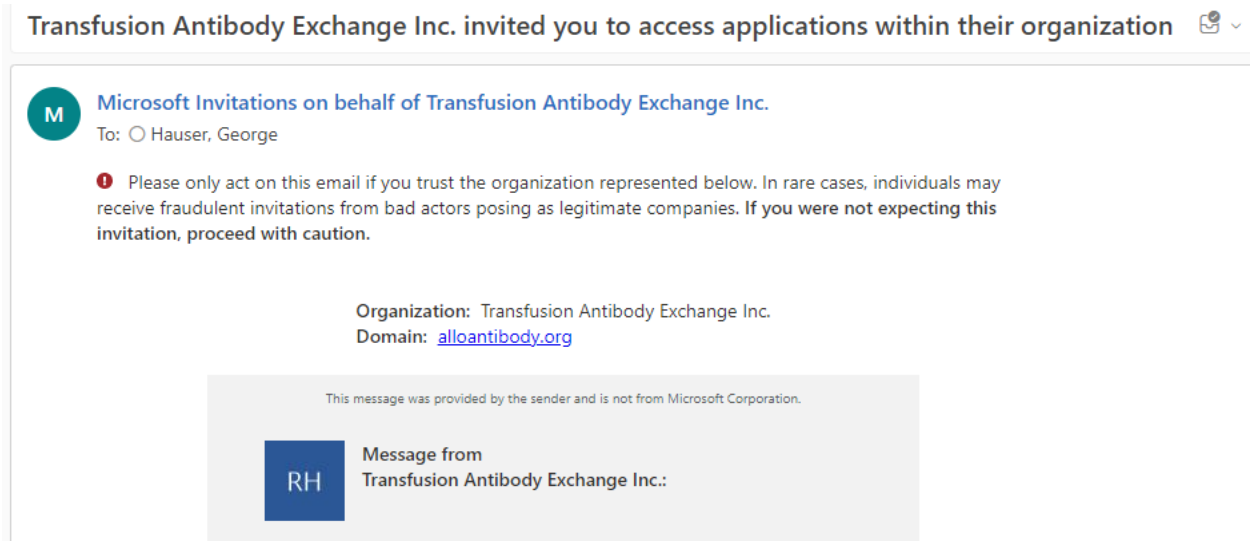
1. The Alloantibody Exchange will check if the new trust relationship with the identity provider has a matching “Domain name of federating IdP” and “Passive authentication endpoint”. If they do not, the health system must add a DNS TXT record. (Ref 1, Step 1)

Examples of matched and unmatched. The domain name is “fabrikam.com”	
Match	Do not match
`https://fabrikam.com`	`https://fabrikamconglomerate.com/adfs`
`https://sts.fabrikam.com/adfs`	`https://fabrikam.com.uk/adfs`

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



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.



References

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