

Active Directory

YellowfinSAML bridgeActive DirectoryAD FS

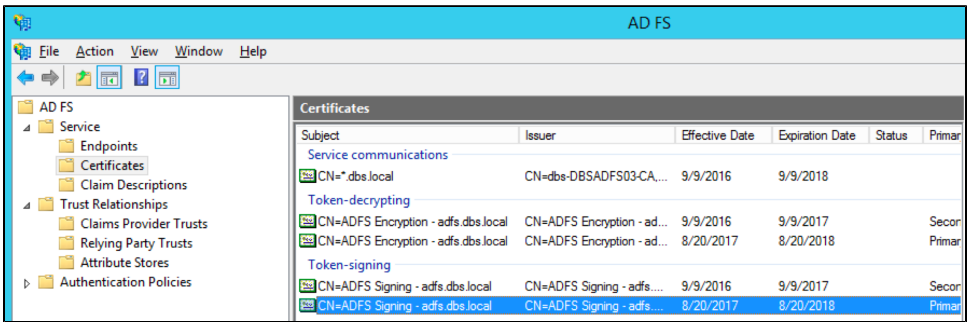
AD FS

YellowfinSAMLAD FS .cer**onelogin.saml.properties**

onelogin.saml2.idp.x509cert =MIIC2DCCAcCgAwIBAgIQfdRAAWmWko1IsimA004o3TANBgkqhki...

AD FS

1. AD FS



- 2. **View Certificate**
- 3. **Details**
- 4. **Copy to file**
- 5. **onelogin.saml2.idp.x509cert**

Yellowfin SAML BridgeAD FS

Yellowfin SAML Bridges**samlbridge/metadata.jsp**URL<http://yellowfin:8080/samlbridge/metadata.jsp>

AD FSURL**samlbridge/WEB-INF/classes/onelogin.saml.properties**

onelogin.saml.propertiesAD FS**YellowfinRelying Party Trust**

AD FS[https://technet.microsoft.com/en-us/library/adfs2-help-how-to-add-a-relying-party-trust\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/adfs2-help-how-to-add-a-relying-party-trust(v=ws.10).aspx)

- 1. AD FS**Trust RelationshipRelying Party TrustAdd Relying Party Trust Wizard**
- 2. **Import data about the relying party published online or on a local networkFederation metadata address (host name or URL)URLYellowfin SAML Bridge metadata.jspURL<http://yellowfin:8080/samlbridge/metadata.jsp> onelogin.saml.propertiesIDonelogin.saml2.sp.entityid**

Add Relying Party Trust Wizard

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.

< Previous Next > Cancel

3. Select Data Source

Add Relying Party Trust Wizard

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name:

< Previous Next > Cancel

4. onelogin.saml.propertiesSSO URL

onelogin.saml2.idp.single_sign_on_service.url = <https://adfs.local/adfs/ls/IdpInitiatedSignon.aspx?loginToRp=Yellowfin>

5. I do not want to configure multi-factor authentication settings for this relying party trust at this timeNext

6. Permit all users to access this relying partyNext

7. AD FSYellowfin SAML Bridge

SAMLAD FSName ID

Name ID**onelogin.saml.properties**

onelogin.saml2.sp.nameidformat = urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

AD FSName ID

AD

1. Add RuleSent LDAP Attributes as ClaimsLDAP
2. SAML Bridge
3. SAML Bridge
4. YellowfinIDID
5. User-Principal-NameE-Mail-Addresses

Edit Rule - Email

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:
Email

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	E-Mail Address
	Given-Name	Given Name
	Surname	Surname
▶	Employee-ID	uid
*		

View Rule Language...

OK

Cancel

6. SAML BridgeADSAML Bridge **web.xmlacs.jsp**

ID

1. Add RuleTransform an Incoming Claim
2. Incoming claim typeE-Mail Address

3. Outgoing claim typeName IDIDOutgoing name ID formatIDEmailonelogin.saml.propertiesonelogin.saml2.sp.nameidformat

Edit Rule - name id

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:
name id

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

View Rule Language... OK Cancel

SSOIdpInitiatedSignOnPage

AD FS 2.0SAMLIDPSSOIdpInitiatedSignOn.aspxSAMLAD FS 2.0YellowfinWeb SSOreplying party:PR

URLonelogin.saml.properties

```
onelogin.saml2.idp.entityid = https://<ADFS domain name>/adfs/ls/IdpInitiatedSignon.aspx?loginToRp=<RP>

onelogin.saml2.idp.single_sign_on_service.url = https://<ADFS domain name>/adfs/ls/IdpInitiatedSignon.aspx?loginToRp=<RP>
```

<PR>AD FS YellowfinSAML Bridge

IdpInitiatedSignOn.aspx<https://msdn.microsoft.com/en-au/library/ee895361.aspx>

SAML bridge

Bridge

