

WS-Fed Example

Steps

Attribute definition

First of all, will be mandatory to create two new attributes

- User principal name
- AD SID

<input type="checkbox"/>	Name	ShortName	Oid	OpenID name	Radius ...	Value
<input type="checkbox"/>	Filter	Filter	Filter	Filter	Filter	Filter
<input type="checkbox"/>	Full name	Fullname	urn:oid:2.16.840.1.113730.3.1.241	full_name		
<input type="checkbox"/>	Given Name	GivenName	urn:oid:2.5.4.42	given_name		
<input type="checkbox"/>	Organizational unit	OU	urn:oid:2.5.4.11	ou		
<input type="checkbox"/>	Phone	TelephoneNumber	urn:oid:2.5.4.20	phone		
<input type="checkbox"/>	Role & group membership	memberOf	urn:oid:1.3.6.1.4.1.5923.1.5.1.1	meber_of		
<input type="checkbox"/>	Session ID	SessionId	urn:oid:1.3.6.1.4.1.22896.3.1.1	session_id		
<input type="checkbox"/>	Session key	SessionKey	urn:oid:1.3.6.1.4.1.22896.3.1.2			
<input type="checkbox"/>	Surname	Surname	urn:oid:2.5.4.4	family_name		
<input type="checkbox"/>	Birth Date	custom:birthDate	urn:oid:1.3.6.1.4.1.22896.3.1.1515	birthDate		attributes{"birthDate"}
<input type="checkbox"/>	Cliente	custom:Cliente	urn:oid:1.3.6.1.4.1.22896.3.1.1552	Cliente		attributes{"Cliente"}
<input type="checkbox"/>	Language	custom:language	urn:oid:1.3.6.1.4.1.22896.3.1.1518	language		attributes{"language"}
<input type="checkbox"/>	Manager	custom:manager	urn:oid:1.3.6.1.4.1.22896.3.1.1554	manager		attributes{"manager"}
<input type="checkbox"/>	oficina	custom:oficina	urn:oid:1.3.6.1.4.1.22896.3.1.1551	oficina		attributes{"oficina"}
<input type="checkbox"/>	Picture	custom:picture	urn:oid:1.3.6.1.4.1.22896.3.1.1516	picture		attributes{"picture"}
<input type="checkbox"/>	Internal id	custom:rid	urn:oid:1.3.6.1.4.1.22896.3.1.1553	rid		attributes{"rid"}
<input checked="" type="checkbox"/>	AD SID	custom:sid	http://schemas.microsoft.com/ws/2008/06/identity/claims#primarysid	sid		attributes{"sid"}
<input type="checkbox"/>	SSH Public key	custom:ssh_key	urn:oid:1.3.6.1.4.1.22896.3.1.1517	ssh_key		attributes{"ssh_key"}
<input checked="" type="checkbox"/>	User principal name	custom:upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims#upn	upn		attributes{"upn"}

Displayed rows: 23



Bear in mind, that those attributes have to be retrieved from the appropriate system:

System objects

user based on user

Properties

System attribute

System attribute	Direction	Soffid attribute	
objectClass	←	"user"	
givenName	↔	firstName	
cn	→	fullName	
sn	↔	lastName	
relativeBaseDn	←	"cn=Users"	
department	↔	primaryGroup	
sAMAccountName	→	userName	
mail	↔	emailAddress	
userPrincipalName	→	attributes{"upn"}	
objectSid	→	attributes{"sid"}	

Test

Triggers

And those attributes have to be defined in the object metadata:

Object type :

Description :

Use textual index :

<input type="checkbox"/>	Code	Label	Data type	Built-in type
<input type="checkbox"/>	Filter	Filter	Filter	Filter
<input type="checkbox"/>	createdByUser	Created by	User	Yes
<input type="checkbox"/>	createdDate	Created on	Date and time	Yes
<input type="checkbox"/>	modifiedByUser	Modified by	User	Yes
<input type="checkbox"/>	modifiedDate	Modified last on	Date and time	Yes
<input type="checkbox"/>	birthDate	Birth Date	Date	No
<input type="checkbox"/>	picture	Picture	Photo	No
<input type="checkbox"/>	ssh_key	SSH Public key	String	No
<input type="checkbox"/>	language	Language	String	No
<input type="checkbox"/>	oficina	oficina	Custom object	No
<input type="checkbox"/>	Cliente	Cliente	Custom object	No
<input type="checkbox"/>	rid	Internal id	Number	No
<input type="checkbox"/>	manager	Manager	User	No
<input type="checkbox"/>	sid	AD SID	String	No
<input type="checkbox"/>	upn	User principal name	String	No

Displayed rows: 34

Attribute sharing policies

Define the proper attribute policy

Policy :

Condition

Attributes

<input type="checkbox"/>	Attribute	Action	Condition
<input type="checkbox"/>	Filter	Filter	Filter
<input type="checkbox"/>	AD SID	Allow	ANY
<input type="checkbox"/>	User principal name	Allow	ANY

Displayed rows: 2

Service Provider

Identification

Type : WS-Federation
Identifier : https://xxx.owa.demo.soffid.net/owa/
Name : owa - ws-fed

Login rules

Allow impersonations : Target application URL
UID Script : Script to compute the user name to pass to the target application
Ask for consent : Yes No
Roles required to login : Roles required to login
System where an enabled account is required :

WS-Federation

Response URL : https://xxx.owa.demo.soffid.net/owa/
Response URL

Undo Apply changes

Configure Exchange

Finally, you must configure the Exchange.

- 1.- Upload the SAML certificate to the certificate repository
- 2.- Search for the thumbprint of the certificate:

```
Set-Location Cert:\LocalMachine\Root; Get-ChildItem | Sort-Object Subject
```

```
Administrator: Windows PowerShell
PS Cert:\LocalMachine\Root> Set-Location Cert:\LocalMachine\Root; Get-ChildItem | Sort-Object Subject

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\Root

Thumbprint                               Subject
-----
7F88CD7223F3C913018600461A886005A385017 CN=Microsoft Authenticode(tm) Root Authority, O=MSFT, C=US
06F1AA330B927                             2 CN=Microsoft ECC Product Root Certificate Authority 2018, O=Microsoft Corporation, L=Redmond, S=W...
31F9FC8BA3805                             4 CN=Microsoft ECC TS Root Certificate Authority 2018, O=Microsoft Corporation, L=Redmond, S=Washin...
A43489159A520                             9 CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright (c) 1997 Microsoft Corp.
3B1EFD3A66EA2                             5 CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
8F43288AD272F                             E CN=Microsoft Root Certificate Authority 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
CDD4EEAE6000A                             2 CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com
92B46C76E1305                             5 CN=Symantec Enterprise Mobile Root for Microsoft, O=Symantec Corporation, C=US
BE36A4562FB2E                             6 CN=Thawte Timestamping CA, OU=Thawte Certification, O=Thawte, L=Durbanville, S=Western Cape, C=ZA
18F7C1FCC3090                             5 OU="NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.", OU=VeriSign Time Stamping Service Root, OU="Ver...
4F65566336DB6                             4 OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
742C3192E607E                             2 OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
245C97DF7514E                             5 OU=Copyright (c) 1997 Microsoft Corp., OU=Microsoft Time Stamping Service Root, OU=Microsoft Corp...
```

- 3.- From the Exchange Management Shell, run:

```
Set-OrganizationConfig -AdfsIssuer https://gbr.idp.demo.soffid.net/profile/wsfed `
-AdfsAudienceUri "https://gbr.owa.demo.soffid.net/owa/","https://gbr.owa.demo.soffid.net/ecp/" `
-AdfsSignCertificateThumbprint "XXXXXXXXXXXXXXXXXXXX"
```

```
Set-OWAVirtualDirectory -Identity "OWA (Default Web Site)" -AdfsAuthentication $true `
  -BasicAuthentication $false -DigestAuthentication $false -FormsAuthentication $false `
  -WindowsAuthentication $false
```

```
Set-ECPVirtualDirectory -Identity "ECP (Default Web Site)" -AdfsAuthentication $true `
  -BasicAuthentication $false -DigestAuthentication $false -FormsAuthentication $false `
  -WindowsAuthentication $false
```

```
net stop was /y
```

```
net start w3svc
```

The server must be up to date. Otherwise WS-Fed will reject the response

Revision #8

Created 27 September 2023 06:39:31

Updated 16 January 2025 08:20:20