

---

# Connecting Office 365

## Introduction

You can use an Identity Provider defined into Soffid to connect to Office 365. You only need to register the Office 365 metadata into a Soffid Service Provider and register the Identity Provider Metadata into your Office 365.

At this tutorial Soffid explain how to connect to Office 365 using PowerShell.

## Step By Step

### Attribute definition

Review the attribute definition to check if it will be necessary to add the Required attributes.

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-saml-idp>

### Attribute sharing policies

Review the attribute sharing policies to add the required attributes.

### Option 1

Soffid will be in charge of creating users in Office 365.

1. First of all, you need to configure your **Identity Provider**, in that case, we configure Soffid as Identity Provider.

### Identification

IdP type :

publicID :

Name :

Organization :

contact :

### Login rules

User regular expression :

Login hint script :

Identity provisioning script :

### Session management

Session timeout (secs) :

oAuth Session timeout (secs) :

SSO Cookie name :

SSO Cookie domain :

Ask for consent :  Yes  No

### Advanced authentication

Allow user to recover passwords :  Yes  No

Allow users to self-register :  Yes  No

Register identities identified by external IdPs :  Yes  No

### Service configuration

Metadata : 

```
<EntityDescriptor entityID="https://idppoc.soffid.com/asn"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:si="http://www.w3.org/2001/XMLSchema-instance">
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:
protocol urn:oasis:names:tc:SAML:2.0:protocol">
```

### Network

Host Name :

Standard port :

Disable SSL :  Yes  No

### Authentication

Always ask for credentials :  Yes  No

Authentication methods

	First aut	Password	Kerbero	External	OTP	Email	SMS	PIN	Certific	FIDO
Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerbero	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OTP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PIN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Profiles

Filter

OpenidProfile
SAML1ArtifactResolutionProfile
SAML1AttributeQueryProfile
SAML2ArtifactResolutionProfile
SAML2AttributeQueryProfile
SAML2ECPPProfile
SAML2SSOProfile

Displayed rows: 7

2. Then, you need to configure the **Service provider**. It will be mandatory to copy the Metadata of Office 365 into the Service Configuration.

### Identification

Type :

publicID :

Name :

### Login rules

Allow impersonations :

UID Script :

Yes  No

### Service configuration

Metadata : 

```
</X509Data></KeyInfo></KeyDescriptor><SingleLogoutService Binding="urn:oasis:
names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://login.microsoftonline.co
m/login.srf"/><NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAd
dress</NameIDFormat><NameIDFormat>urn:mace:shibboleth:1.0:nameid-identifier</
NameIDFormat><NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspe
cified</NameIDFormat><NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-form
at:transient</NameIDFormat><NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid
-format:persistent</NameIDFormat><AssertionConsumerService Binding="urn:oasis:
names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://login.microsoftonline.co
m/login.srf" index="0" isDefault="true"/><AssertionConsumerService Binding="urn:
oasis:names:tc:SAML:2.0:bindings:HTTP-POST:SimpleSign" Location="https://login.m
icrosoftonline.com/login.srf" index="1"/><AssertionConsumerService Binding="urn:
oasis:names:tc:SAML:2.0:bindings:PAOS" Location="https://login.microsoftonline.co
m/login.srf" index="2"/></SPSSODescriptor><Extensions><alg:DigestMethod Algori
thm="http://www.w3.org/2000/09/xmldsig#sha1"/><alg:SigningMethod Algorithm=
"http://www.w3.org/2000/09/xmldsig#rsa-sha1"/></Extensions></EntityDescriptor>
```

3. You need to configure an Office 365 agent:

<https://bookstack.soffid.com/books/connectors/page/how-to-configure-the-office-365-agent>

## Option 2

The Active Directory will be in charge of creating users in Office 365.

1. You need to create the attribute *immutableId* in the agent configuration

System objects

account based on account

Properties

System attribute	Direction	Soffid attribute
objectClass	←	"user"
relativeBaseDn	←	"cn=Users"
sn	→	accountDescription
cn	→	accountDescription
"U"	→	type
List list = new LinkedList(); list.add(sAMAccountName);	→	ownerUsers
sn	←	accountDescription
cn	←	accountDescription
sAMAccountName	↔	accountName
immutableId	→	attributes{"immutableId"}

Test

If you fetch the Soffid object, Soffid will display this new attribute

System objects

account based on account

Properties

System attribute

objectClass		
relativeBaseDn		
sn		
cn		
"U"		
List list = new LinkedList(); list.add(sAMAccountName);		
sn		
cn		
sAMAccountName		accountName
immutableId		attributes{"immutableId"}

Name: frank

accountDescription Frankaaa Sinatra

accountName frank

attributes{"immutableId"} F0gzUlySRU6zIDnFoRgF9g==

ownerUsers [frank]

type U

Status: success

4/19/23, 9:57:20 AM INFO BEGIN Initalize Active Directory agent  
ActiveDirectoryDemoLab

4/19/23, 9:57:20 AM INFO ActiveDirectoryDemoLab: Fetching main domain for

Accept Load into Soffid database

Account: frank Test expression Synchronize now Fetch system raw data Fetch Soffid object

2. You must add a UID Script in the Office 365 Service Provider

## Identification

Type :	SAML
Identifier :	urn:federation:MicrosoftOnline
Name :	Office365

## Login rules

Allow impersonations :	Target application URL
UID Script :	<pre>System.out.println("Guessing immutable id for " + id + "/" + userName); for (account: serverService.getUserAccounts(id, "ActiveDirectoryDemoLab")) {     if (account.attributes["immutableId"] != null)         return account.attributes["immutableId"]; } </pre>
Ask for consent :	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Roles required to login :	Roles required to login
System where an enabled account is required :	

## Service configuration

Metadata :	<pre>&lt;EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:alg="urn:oasis:names:tc:SAML:metadata:alg:support" ID="_d8c4e4ae- 1a04-4f10-b193-a8e89f71e462" entityID="urn:federation:MicrosoftOnline"&gt; &lt;Signature xmlns="http://www.w3.org/2000/09/xmldsig#"&gt; </pre>
------------	---

```
System.out.println("Guessing immutable id for " + id + "/" + userName);
for (account: serverService.getUserAccounts(id, "ActiveDirectoryDemoLab")) {
    if (account.attributes{"immutableId"} != null)
        return account.attributes{"immutableId"};
}
```

# PowerShell

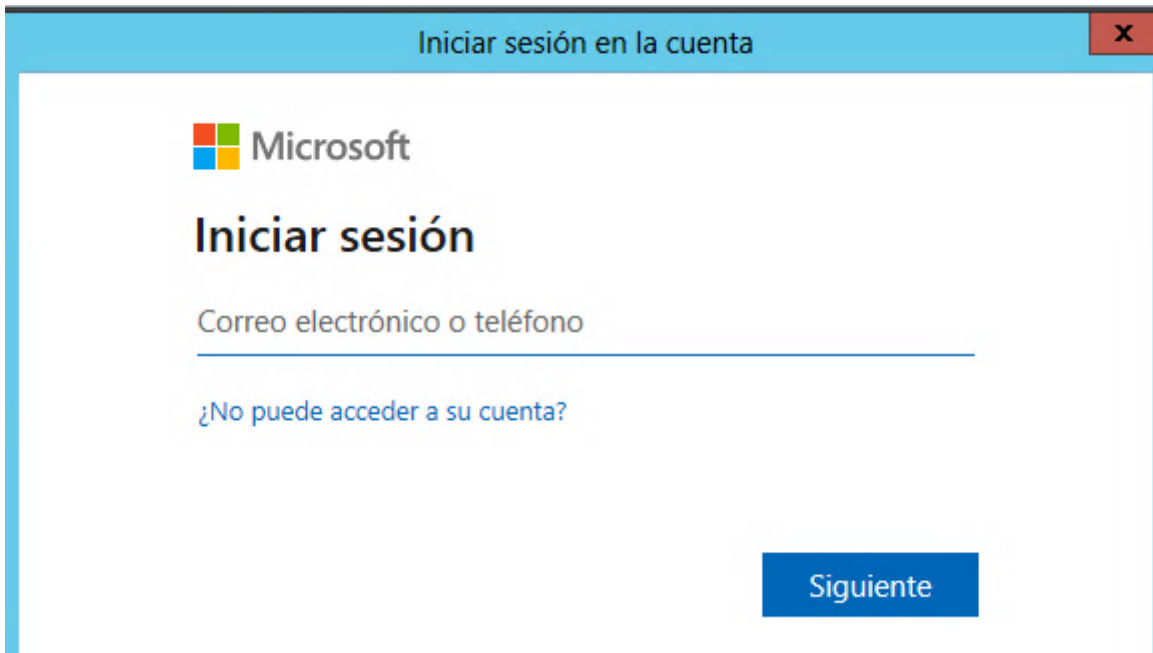
If necessary you can install the Azure AD module for Windows PowerShell

```
Install-Module MSOnline
```

Then you can connect to the service

```
Connect-MsolService
```

When you executed the connect method, a new window will open to login Microsoft in as an administrator domain user.



Once you have logged in, you could execute some commands to configure the connection to Office 365:

- **Register-PSRepository -Default:** registers a PowerShell repository
- **Get-MsolDomain:** displays the registered domains in Azure Active Directory.
- **GetMsolDomainFederationSettings:** get the settings for a federated domain
- **Set-MsolDomain -Name <YOUR\_DOMAIN> -isdefault:** set as default one domain
- **Set-MsolDomainAuthentication -DomainName <YOUR\_DOMAIN> - Authentication federated:** set as federated a specific domain.

In order to connect to Office 365, one can use the following script:

```
$dom = "<Your demain>"
$BrandName = "<Your company>"
$LogOnUrl = "https://<Your Soffid IdP>/profile/SAML2/POST/SSO"
$LogOffUrl = "https://<Your Soffid IdP>/profile/SAML2/POST/SLO"
$ecpUrl = "https://<Your Soffid IdP>/SAML2/POST/PAOS"
$MyURI = "<Your Soffid IdP>"
$MySigningCert = "<Your certificate in Base64>";
# "MII GaDCCBVCgAwIBAgIQAWdkq9pxzP/bK+MIym5y5zANBgkqhkiG9w0BAQsFADBeMQswCQY....
$Protocol = "SAML"

# To enable
Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName $BrandName -Authentication
Federated -PassiveLogOnUri $LogOnUrl -SigningCertificate $MySigningCert -IssuerUri $MyURI -LogOffUri
$LogOffUrl -PreferredAuthenticationProtocol $Protocol
```

```
# To disable
```

```
# Set-MsolDomainAuthentication -DomainName $dom -Authentication Managed
```

---

<https://docs.microsoft.com/en-us/powershell/module/cimcmdlets/?view=powershell-7.2>

<https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-msonlinev1?view=azureadps-1.0#install-the-azure-ad-module>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-saml-idp>

---

Revision #14

Created 27 September 2021 13:45:12

Updated 27 September 2023 06:34:26