Integración con Office365

saml2, manual, desarrollador

Azure Active Directory es una solución en la nube global de administración de identidades de Microsoft. Ayuda a proteger el acceso a aplicaciones locales y en la nube, incluidos los servicios en línea como Office 365 | .

La integración de Office 365 | con el proveedor de identidad de la Universidad de Huelva se realiza en dos fases:

1. Federación del dominio en AzureAD
2. Configurar el Idp de la Universidad de Huelva para proveer los atributos que necesita Office365
3. Provisión de usuarios

Federación del dominio en AzureAD

1. En una máquinas windows instalamos la PowerShell y módulo para Azure AD
2. Arrancamos el PowerShell y usamos el comando `Connect-MsolService` para conectarnos a AzureAD e introducimos las credenciales del administrador del AzureAD

```
Connect-MsolService
```

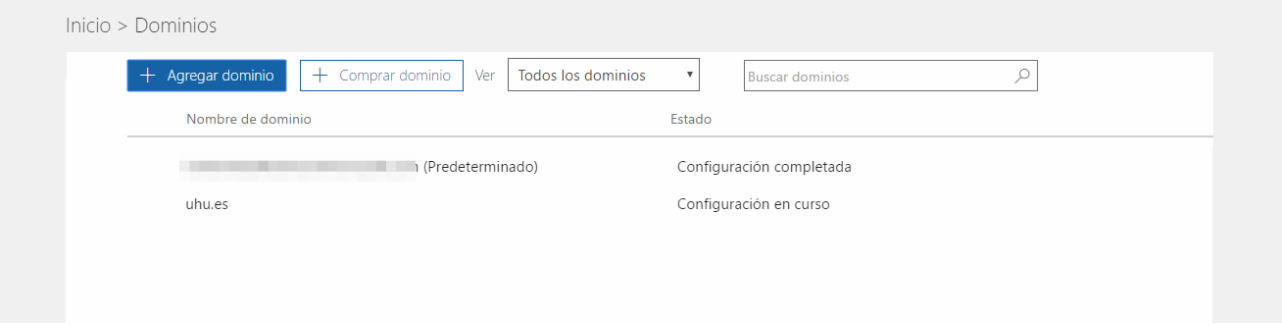
3. Usamos el comando `New-MsolDomain` para crear el nuevo dominio a federar, en este caso `uhu.es`:

```
New-MsolDomain -Name uhu.es -Authentication Federated
```

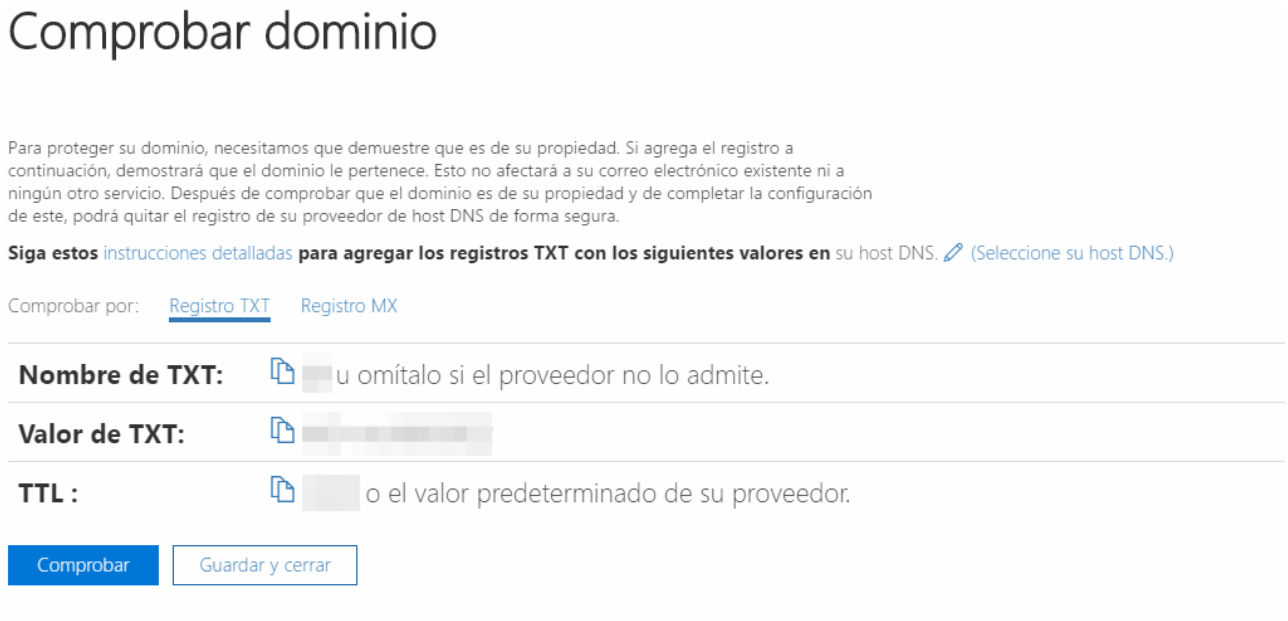
4. A continuación usamos el comando `Get-MsolDomainVerificationDns` para indicarle a AzureAD cómo queremos que compruebe el dominio. En nuestro caso será mediante registros de texto (`-Mode DnsTxtRecord`) introducimos en el DNS responsable del dominio a federar:

```
Get-MsolDomainVerificationDns -DomainName uhu.es -Mode DnsTxtRecord
```

5. Como resultado, este comando nos devolverá el nombre del resgistro que tenemos que añadir, su valor y el TTL.
6. Accedemos al portal de office 365 como administrador. Nos posicionamos en la opción `configuración`, `dominios`. Pulsamos sobre el dominio creado:



7. En el paso `comprobación del dominio` pulsamos sobre el botón de `confirmar`.



8. Si todo ha salido bien pasará directamente a la pestaña configuración de los servicios.
9. Desde la Powershell podemos comprobar que el dominio ya ha sido verificado ejecutamos lo que se indica a continuación y esperamos que el valor de **Status** sea `verified` y el del campo **Authentication** valga `Managed`:

```
Get-MsolDomain
```

10. Antes de continuar, es necesario obetener los siguientes datos:

Nombre	**Descripción**	**Valor**
DomainName	Nombre del dominio	uhu.es
FederationBrandName	some colspan (note the double pipe)	
MetadataExchangeUri	Uri para obtener los metadados del IDP	
ActiveLogOnUri	Uri para iniciar el proceso de logon pasivo	https://idpnew.uhu.es/idp/saml2/idp/SSOService.php
PassiveLogOnUri	Uri para iniciar el proceso de logon pasivo	https://idpnew.uhu.es/idp/saml2/idp/SSOService.php
SigningCertificate	Certificado para firmar las aserciones	
IssuerUri	EntityID de idp	https://idp.uhu.es/idp/
LogOffUri	Uri para iniciar el proceso de logoff	https://idpnew.uhu.es/idp/saml2/idp/SingleLogoutService.php
PreferredAuthenticationProtocol	Protocolo para hacer la autentificación	SAMLP

1. A continuación usamos el comando `Set-MsolDomainAuthentication` para asociar los valores antes indicados a AzureAD

```
$domainname = "uhu.es"
$logoffuri = "https://idpnew.uhu.es/idp/saml2/idp/SSOService.php"
$passivelogonuri =
"https://idpnew.uhu.es/idp/saml2/idp/SingleLogoutService.php"
$cert =
$issueruri = "https://idp.uhu.es/idp"
$protocol = "SAMLP"
$metadataexchangeuri =
$brandname=

Set-MsolDomainAuthentication -DomainName $domainname -
FederationBrandName $brandname -Authentication Federated -
MetadataExchangeUri $metadataexchangeuri -ActiveLogOnUri
$activelogonuri -PassiveLogOnUri $passi
velogonuri -SigningCertificate $cert -IssuerUri $issueruri -LogOffUri
$logoffuri -PreferredAuthenticationProtocol $protocol
```

2. Para comprobar que ya ha sido federado ponemos Get.MsolDomain y ebn el campo Authentication pondrá federated

Configurar del Proveedor de Identidad

El proveedor de identidad de la Universidad de Huelva se basa en SimpleSAMLphp. Los pasos que se han dado son:

1. En el fichero `config/config.uhu` añadimos la localización de los metadatos de azuead

```
    'metadata.sources' => array(
        array('type' => 'flatfile'),
        array('type' => 'flatfile', 'directory' => 'metadata/azuread'),

    ),
```

2. Configuramos el módulo metarefresh,`config/config_metarefresh`, para que obtenga periódicamente los metadatos de azuread. Estos datos se encuentran localizados en https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml

```
'azuread' => array(
       'cron'     => array('daily'),
       'sources'  => array(
            array(
                 'src' =>
'https://nexus.microsoftonline-p.com/federationmetadata/saml20/federati
onmetadata.xml',
```

.

3. Según se indica en el apartado **Atributos requeridos** del documento Utilizar un proveedor de identidad SAML 2.0 para implementar el inicio de sesión único, limitaremos los atributos a mandar a `Issuer`,`ImmutableID` y `IDPEmail`, estableceremos su formato a

`urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified`, marcaremos al atributo `ImmutableID` como NameID y estableceremos su formato a `urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified`:

```
'attributes' => array ('Issuer','ImmutableID','IDPEmail'),
'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified',
'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent',
'simplesaml.nameidattribute' => 'ImmutableID',
```

4. Indicaremos el algoritmo con el que se firmarán las aserciones, estableceremos que los logout deben ir firmados y que las aserciones no irán cifradas (tal y como se indica en el apartado Requisitos del bloque de firma del documento Utilizar un proveedor de identidad SAML 2.0 para implementar el inicio de sesión único:

```
'signature.algorithm'=> 'http://www.w3.org/2000/09/xmldsig#rsa-sha1',
'redirect.sign' => true,
'redirect.validate' => false,
'assertion.encryption' => false,
```

5. Por último usamos el `authproc` para establecer los filtros necesarios para obtener las atributos solicitados
6. El fichero final sería:

```
'azuread' => array(
    'cron'          => array('daily'),
    'sources'       => array(
        array(
            'src' =>
'https://nexus.microsoftonline-p.com/federationmetadata/saml20/federati
onmetadata.xml',
        'template' =>  array(
                'tags' => array('azuread'),
                'attributes' => array
('Issuer','ImmutableID','IDPEmail'),
        'attributes.NameFormat' =>
'urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified',
        'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent',
        'simplesaml.nameidattribute' => 'ImmutableID',
                'signature.algorithm'=>
'http://www.w3.org/2000/09/xmldsig#rsa-sha1',
        'redirect.sign' => true,
                'redirect.validate' => false,
                'assertion.encryption' => false,
                'authproc' => require(__DIR__ .
'/rules/azuread/main.php'),
        ),
        ),
    ),
```

```
    'expireAfter'    => 60*60*24*2, // Maximum 2 days cache time.
    'outputDir'     => 'metadata/azuread/',
    'outputFormat' => 'flatfile',
),
```

7. El `InmutableID` lo obtenemos a partir del atributo `eduPersonPrincipalName` de la siguiente forma

```
return array(
    'class' => 'core:PHP',
    'code' => '
        if (empty($attributes["eduPersonPrincipalName"]) ||
$attributes["eduPersonPrincipalName"][0] === FALSE) {
        $mesg = "Error while provisioning InmutableID:
eduPersonPrincipalName required, not presented";
        SimpleSAML_Logger::error($mesg);
                throw new SimpleSAML_Error_Exception($mesg);
        }

        $eppn = $attributes["eduPersonPrincipalName"][0];
        $chunks = str_split(md5($eppn), 4);
        $attributes["employeeNumber"][0] = vsprintf("%s%s-%s-%s-%s-
%s%s%s", $chunks);
    ',
);
```

Provisión de usuarios shadow en AzureAD

Una vez federado el dominio y configurado nuestro Idp, pasamos a crear cuentas en AzureAD para comprobar que todo funciona correctamente.

1. Creamos la cuenta del usuario prueba@uhu.es ponemos:

```
PS C:\Users\Usuario\Desktop> New-MsolUser -UserPrincipalName
prueba@uhu.es -ImmutableId 32e23dsce-2sdsd9-8238-3710-60bfb2ddss4e4 -
DisplayName "Usuario prueba uhu" -FirstName Prueba -LastName UHU -
UsageLocation "ES"

Password UserPrincipalName  DisplayName                isLicensed
-------- -----------------  -----------                ----------
         prueba@uhu.es      Usurio pruaba uhu          False
```

2. Nos conectamos a http://potal.office.com e introducimos las credenciales de usuario, nos redireccionará al idp en donde acabaremos de introducir nuestra clave
3. El usuario accederá al portal pero, al no tener asociada licencia, no podrá descargar ni usar los productos de microsoft. Para ver las licencias que podemos asociar usamos el comando `Get-MsolAccountSku`:

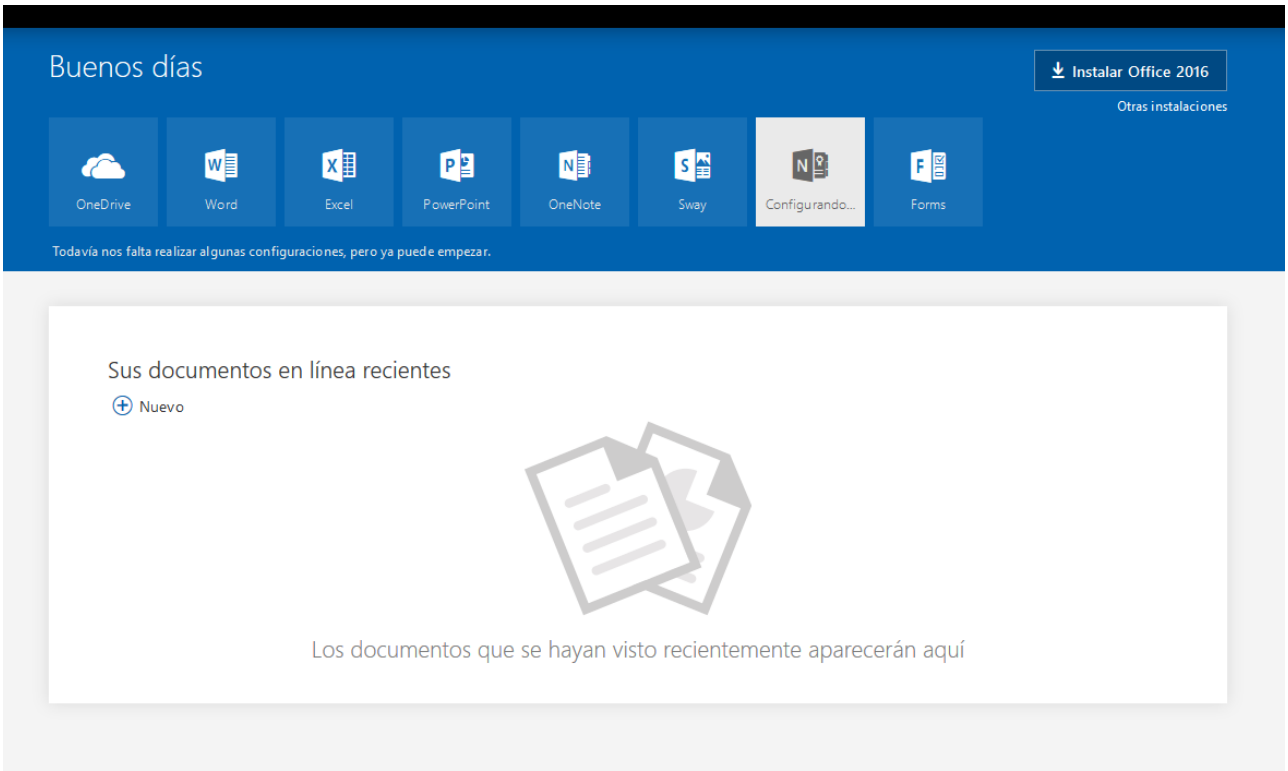
```
PS C:\Users\Usuario\Desktop> Get-MsolAccountSku
```

```
AccountSkuId                                    ActiveUnits WarningUnits
ConsumedUnits
------------                                    ----------- ------------ -
------------
universidadhuelva:OFFICESUBSCRIPTION_FACULTY 33000        0
0
universidadhuelva:OFFICESUBSCRIPTION_STUDENT 120000       0
0
universidadhuelva:STANDARDWOFFPACK_FACULTY   34000        0
0
universidadhuelva:STANDARDWOFFPACK_STUDENT   130000       0
0
```

4. Para asociar licencias al usuario creado ejecutamos:

```
PS C:\Users\Usuario\Desktop> Set-MsolUserLicense -UserPrincipalName
prueba@uhu.es -AddLicenses universidadhuelva:OFFICESUBSCRIPTION_FACULTY
```

5. Si nos volvemos a conectas a http://portal.office.com e introducimos las credenciales de usuario, debería aparecer una pantalla similar a la siguiente en la que tendremos los productos asociados a la licencia



From:
https://ayudame.uhu.es/docs/ - **Documentación Servicio de Enseñanza Virtual**

Permanent link:
https://ayudame.uhu.es/docs/doku.php/sso/manuales/office365

Last update: **2018/07/17 07:43**