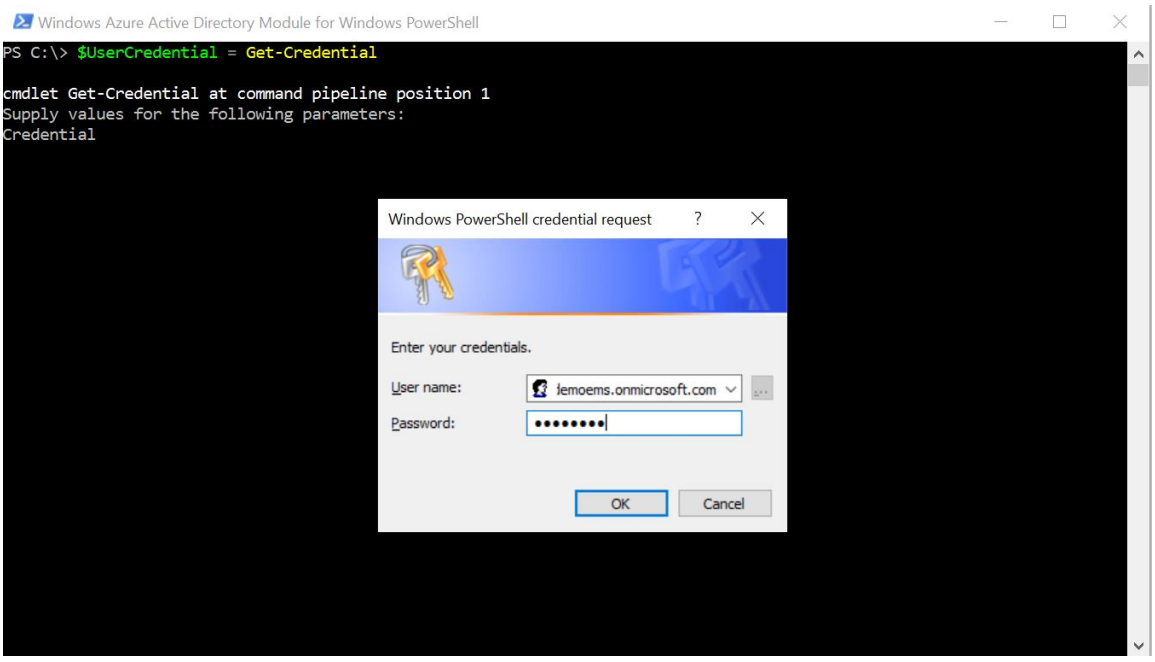
Implementing Single Sign-On

When accessing cloud based application and services, Federated Identity, which is commonly referred to as Single sign-on, means being able to access all of the applications and resources that end customer organizations need to do business, by signing in only once using a single user account. Once signed in, users can access all of the applications they need without being required to authenticate (e.g. type a password) a second time.

Single Sign-on is achieved with the Federation of the end customers Active Directory Federation Services (ADFS) infrastructure with their Azure Active Directory tenant.

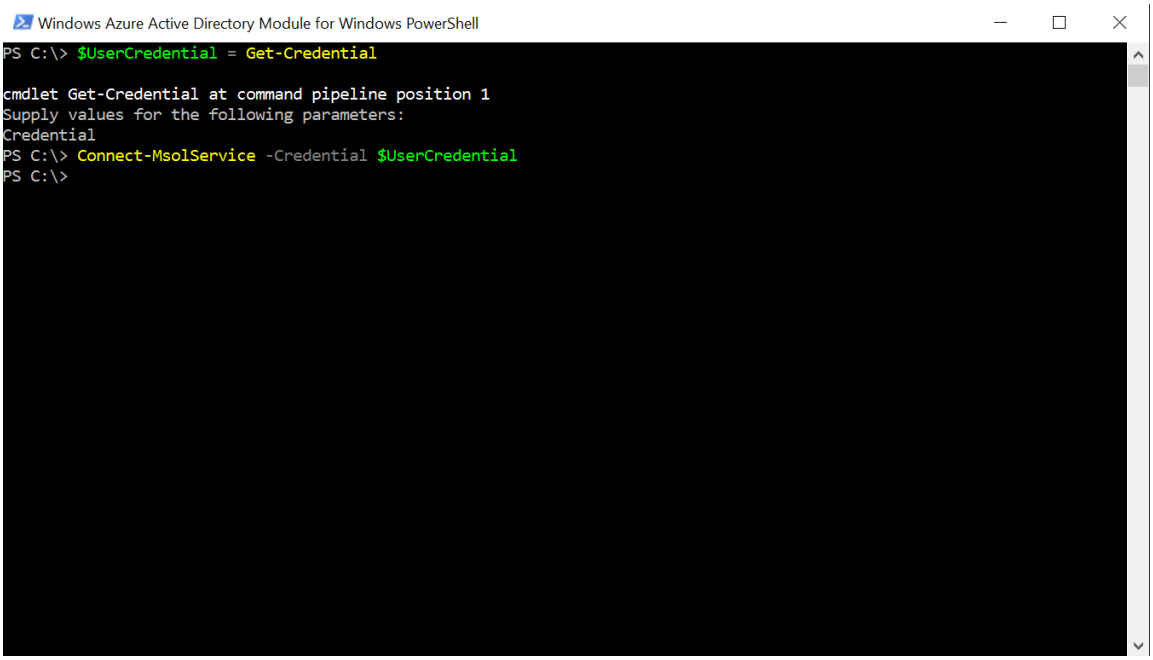
In this example, SSO is being enabled on the ADFS server for the domain **contoso.com** which has been previously added and verified to the Azure AD tenant.

1. Open **Windows Azure Active Directory for Windows PowerShell** and enter the following command:
   `$UserCredential = Get-Credential`
2. When prompted, enter the credentials with Office 365 Global Administrator permissions to the end customer's subscription and select OK.



3. Enter the following command to initiate a connection to the Office 365 subscription:

```
Connect-MsolService -Credential $UserCredential
```



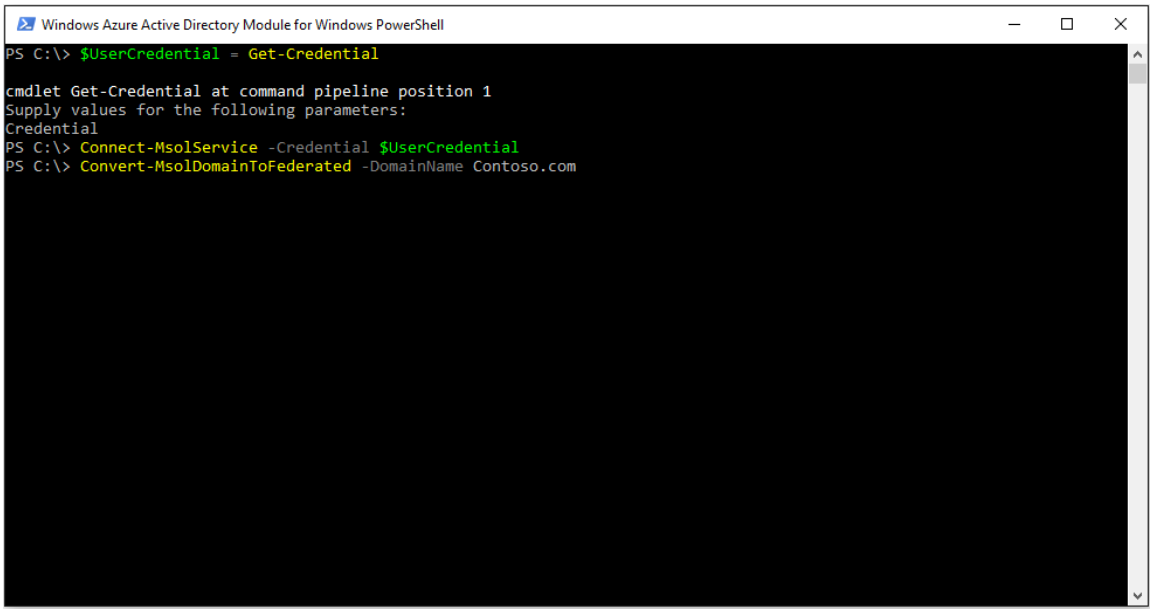
4. Run the following command to convert the specified domain from Managed authentication to Federated authentication:

   `Convert- MsolDomainToFederated -DomainName <Domain Name>`

   Example:

   `Convert- MsolDomainToFederated -DomainName Contoso.com`

   In this example, SSO federation with the Azure AD tenant is configured for the domain **contoso.com**.



5. Run the following command to verify the end customer Federation status:

   ```
   Get-MsolDomain
   ```

   This will detail all of the domains in the end customers Azure AD Tenant and the authentication model associated with each domain.
   In the example, the domain **contoso.com** has now had SSO enabled as shown by its Federated authentication status.
   All users logging into Microsoft online services with a @contoso.com username will now be required to authenticate against the on-premises ADFS infrastructure.