PingOne Office 365 Deployment

The following guide outlines the steps required to configure the PingOne Office 365 application (available in the Application Catalog) to enable single sign-on (SSO) for users from an Active Directory based Identity Provider solution to Microsoft Office 365. Although the Microsoft guides for setting up Office 365 and the Active Directory environment are comprehensive this guide captures the required elements and emphasizes areas that can be problematic.

Support Matrix

Client	Support level	Exceptions
Web-based clients such as Exchange Web Access and SharePoint Online	Supported	None
Rich client applications such like Lync, Office Subscription, CRM	Supported	None
Email-rich clients such as like Outlook and ActiveSync	Supported	None
Diagnostic tools, such as MSODAL, Exchange Connectivity Test	Not supported	None

Requirements

You will need the following components for SSO to Office 365 through PingOne:

- Microsoft Active Directory Domain Controller
    - The domain must be the same as the domain you register with Office 365 (see below).
    - Follow Microsoft's directions on the specifications for this machine.
- PingOne AD Connect
    - Windows Server 2008 or Windows Server 2008 R2 with IIS 7.0 or 7.5.
    - AD Connect can be installed on the Active Directory Domain Controller or on IIS joined to the same domain as above.
- Windows Server for Directory Synchronization
    - Follow Microsoft's directions on the specifications for this machine but it is recommend a machine with a least 4gb be used.
    - The server must be joined to the same domain as above.
- Windows Server for Microsoft Online Services Module for Windows Powershell
    - Installing Microsoft Online Services Module for Windows Powershell on the same server as the Directory Synchronization tool is not recommended. The install of Microsoft Online Services Module for Windows Powershell requires Microsoft Online Services

Sign-In Assistant. Unfortunately the Directory Synchronization tool also tries to install the Microsoft Online Service Sign-In Assistant and it will fail if a newer version is detected.
    - This server does not need to be joined to the same domain as above.

Naming Infrastructure

- A valid domain name is required that can be validated as part of the Office 365 registration.
- Access to domain registrar to set the TXT flag in the host file so that Microsoft can validate the domain.

Office 365 Demo Account

- Sign up for the 'Midsize business and enterprise' trial. The 'Small business' plan DOES NOT support federation or Active Directory Synchronization.
- http://www.microsoft.com/en-us/office365/free-office365-trial.aspx

Office 365 Configuration

To add a domain to Office 365 follow these steps:

- Click Management → Domains
- Click "Add a domain"
- Enter a domain, click Next.
- Verify the domain using the instructions appropriate for you domain registrar.
- Select the appropriate services.
- Configure the DNS records on the domain registrar for other services.
- Note, do not make the new domain the primary domain for the Office 365 account. When using the Set-MsolDomainAuthentication command to set the domain as a federated domain an error will occur if the domain is the default domain.

PingOne Office 365 Application Configuration

The PingOne setup is quite straightforward:

- Setup the Office 365 application from the Application Catalog.
- Make note of the values provided on the Office 365 Federation Settings step including the certificate.
- On the attribute mapping step map:
    - userPrincipalName → subject
    - objectGUID → guid
- Complete the setup and add the application to the relevant groups on the group membership page.

Enabling Single Sign-On

Enabling Single Sign-On is a multistep process involving the use of the Microsoft Online Services Directory Synchronization tool to sync Active Directory with the Office 365 account as well as using the Microsoft Online Services Module for Windows Powershell to enable federation and provide federation settings for the Office 365 account. It's highly recommend that you follow the Microsoft guides with the PingOne specific amendments mentioned below.

Useful Information:

- Overview on Office Federation: http://technet.microsoft.com/en-us/library/hh967628.aspx
- SSO Road Map: http://technet.microsoft.com/en-us/library/hh967643.aspx

Microsoft's Single Sign-On Road Map (follow above link)

- Step 1: Prepare for Single Sign-On
    - http://technet.microsoft.com/en-us/library/jj151786.aspx
    - Determine whether your environment is ready for Office 365 by using OnRamp. Instructions can be found here:
        - http://technet.microsoft.com/en-us/library/jj993929.aspx
        - The tool will indicate whether the Active Directory Domain Controller is ready for synchronization and will point out any issues (e.g. schema problems).
    - Install the Microsoft Online Services Sign-In Assistant on the Windows Powershell server.
        - http://www.microsoft.com/en-us/download/details.aspx?id=39267
    - Use the Role Management tool (Server Manager → Features → Add Feature) to install .NET 3.5.1 on the Directory Synchronization server and the Windows Powershell server.
- Step 2: Deploy Active Directory Federated Services 2.0
    - Skip this step.
- Step 3: Installing Windows Azure Active Directory Module for Windows PowerShell
    - http://technet.microsoft.com/library/jj151815.aspx
    - This document walks through the Powershell commandlets required to enable federation. Since AD Connect is the IDP solution ADFS configuration is not required. There are a few alternative commands that need to be executed.
    - Download the Windows Azure Active Directory Module for Windows PowerShell (AdministrationConfig-en.msi) to the PowerShell server.
    - http://technet.microsoft.com/en-us/library/jj205461.aspx
    - In this document p 'Add a domain' and proceed to 'Convert a domain'. This is because adding a domain depends on having an ADFS context established which is not required in this scenario.
    - Convert a Domain
        - Complete steps 1 through 3.
            - When entering credentials the Microsoft Office 365 administration credentials must be provided. They will be in the format <username>@<domain>.onmicrosoft.com
        - Ignore step 4 & 5.
        - Instead use the following 'Set-MsolDomainAuthentication' and 'Set-MsolDomainFederationSettings' commands along with the parameters provided by the PingOne Office 365 APS application to supply PingOne Federation Settings to the Office 365 account.
            - `Set-MsolDomainAuthentication -DomainName <YOUR DOMAIN> -Authentication federated -IssuerUri <PROVIDED> -LogOffUri <PROVIDED> -ActiveLogOnUri <PROVIDED> -PassiveLogOnUri <PROVIDED>`

              Example:

              ```
              Set-MsolDomainAuthentication -DomainName myoffice365domain.com -Authentication federated -IssuerUri
              ```

```
http://pingone.com/adconnect/3dee1243-79a6-4536-bb5e-82df93c7bf06 -
LogOffUri https://connect365.pingone.com/365/passive/sign-
out/bWRwcm9kcHJvdg -ActiveLogOnUri
https://connect365.pingone.com/365/active/sign-in/bWRwcm9kcHJvdg -
PassiveLogOnUri https://connect365.pingone.com/365/passive/sign-
in/bWRwcm9kcHJvdg
```

- `Set-MsolDomainFederationSettings -DomainName <YOUR DOMAIN> -FederationBrandName <YOUR DOMAIN> -IssuerUri <PROVIDED> -LogOffUri <PROVIDED> -MetadataExchangeUri  <PROVIDED> -ActiveLogOnUri <PROVIDED> -PassiveLogOnUri <PROVIDED>`

  Example:

```
Set-MsolDomainFederationSettings -DomainName myoffice365domain.com
-FederationBrandName myoffice365domain.com -IssuerUri
http://pingone.com/adconnect/3dee1243-79a6-4536-bb5e-82df93c7bf06 -
LogOffUri https://connect365.pingone.com/365/passive/sign-
out/bWRwcm9kcHJvdg -MetadataExchangeUri
https://connect365.pingone.com/365/mex/bWRwcm9kcHJvdg -
ActiveLogOnUri_https://connect365.pingone.com/365/active/sign-
in/bWRwcm9kcHJvdg -PassiveLogOnUri
https://connect365.pingone.com/365/passive/sign-in/bWRwcm9kcHJvdg
```

- `Set-MsolDomainFederationSettings -DomainName <YOUR DOMAIN> -SigningCertificate "CERTIFICATE CONTENTS"`

  Example:

```
Set-MsolDomainFederationSettings -DomainName <YOUR DOMAIN> -
SigningCertificate
"MIIE5TCCA82gAwIBAgIRALbSpY9ypzszBq90SG/+yE4wDQYJKoZIhvcNAQEFBQAwQT
ELMAkGA1UEBhMCRlIxEjAQBgNVBAoTCUdBTkRJIFNBUzEeMBwGA1UEAxMVR2FuZGkgU
3RhbmRhcmQgU1NMIENBMB4XDTEyMDcxMzAwMDAwMFoXDTEzMD

...shortened for space...

pJO91Ky8MoOMpQWdUmCe0TwndEMssDk73KxyeQ1bAEMPs5hMsQTm11/n6dQTnRitlv4
j980TzpFY6eK7f5TaVEX65vUDNzVRvepcwHgUpSPC/VInZtI2VDKTD+TwTUj+5VjOc3
0WoJLI4U9Q6Rep+5Zb"
```

- You can verify the federation settings using the following command:

```
Get-MsolDomainFederationSettings -DomainName <YOUR DOMAIN>
```

- Step 4: Verify Additional Domains
  - Follow this step if necessary for the given environment.
- Step 5-9: Setup Active Directory synchronization
  - Prepare for the installation: http://technet.microsoft.com/en-us/library/jj151831.aspx
  - Login to the Office 365 portal, activate synchronization and download the Directory Synchronization tool to the Directory Synchronization server:
    - Click Admin in the Office 365 portal header.
    - Click Users from the left pane.
    - Click the link next to ‘Active Directory synchronization’ near the top of the page.

        - Under Step 3: 'Activate Active Directory synchronization' click Activate.
            - Activating Active Directory synchronization can take up to 24 hours.
        - Under Step 4: 'Install and configure the Directory Synchronization' tool click Download.
    - Run the Directory Synchronization tool (dirsync) -- it will take approximately 20 minutes on on adequate hardware. The Directory Synchronization tool installs the following components:
        - Directory Synchronization
        - Identity Lifecycle Manager 2007
        - Microsoft SQL Server Express 2008
        - Microsoft Online Services Sign-In Assistant
    - Once the installation is complete the assistant will proceed to synchronize Active Directory with the Office 365 account.
        - http://technet.microsoft.com/en-us/library/jj151771.aspx
        - For the Microsoft Online Services Credentials enter the Office 365 administration account credentials.
        - If necessary configure the Exchange hybrid deployment.
    - Return to the Office 365 portal and verify that users have been synced.
    - Before SSO is possible activate one or more synced users for SSO
        - Click Admin in the portal header.
        - Click Users from the left pane.
        - On the Users page, select the checkbox next to the user or users that require activation, and then click Activate synced users.
- Step 10: Single Sign-On will now be enabled!
    - Initiate SSO from the Cloud Desktop: https://desktop.connect.pingidentity.com/clouddesktop/<cloud desktop domain>/ by selecting the Office 365 application;
    - Initiate SSO directly using the initsso url: https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<saasid>&idpid=<idpid>;
    - Or, SSO from Microsoft using the URL: http://login.microsoftonline.com/ and then enter the username (userPrincipalName). Another link will be provided for SSO.

Active Profile Authentication

Active profile authentication requires one additional parameter in the federation settings that are set using the 'Set-MsolDomainFederationSettings' command. That parameter is -ActiveLogOnUri and is already included in the ''Set-MsolDomainFederationSettings' instructions above (step 3).

For active profiles, authentication is not handled through a browser. For this reason it is important for AD Connect to use a trusted certificate for the SSL binding. If the certificate is not trusted authentication will simply not work.

Once PingOne Office 365 configuration is complete a user can set up additional clients (Lync, Outlook, Sharepoint, Office) and use active profile authentication to authenticate with Office 365, verify their license and activate these applications. However, before a user can use these clients and services an Administrator does need to add several DNS records for some of the Office 365 services (Lync Online, Exchange Online and Sharepoint Online). Instructions on where to find this information in your Office 365

account can be found here: http://office.microsoft.com/en-us/office365-suite-help/gather-the-information-you-need-to-create-office-365-dns-records-HA104028359.aspx?CTT=5&origin=HA102851099

Follow these steps to get additional clients downloaded, configured and activated for use with Office 365:

- Single Sign-On into Office 365.
- On the Office 365 dashboard, under Resources click Downloads
- Depending on the license you will see different options on the Downloads page. Assuming you have an E3 license you will be able to download Microsoft Office Professional Plus, Microsoft Lync and a setup utility to setup and configure Office desktop apps.
- Installing Microsoft Office Professional Plus (assumes E3 Microsoft Office 365 license):
    - In section 1, select your language and version then click Install.
    - Save the MicrosoftOffice.exe installer.
    - Once the download has completed run the installer (will require Administrator privileges).
    - Once the installation is complete you will be prompted to install Microsoft Online Services Sign In Assistant. This service is required in order to verify the Office 365 subscription.
    - Install Microsoft Online Services Sign In Assistant. If installation fails see the troubleshooting section.
    - Once the Microsoft Online Services Sign In Assistant has installed, another service will run to verify your Office 365 subscription. It will run through some configuration until it prompts you to complete the setup. Once you do this it will then open another dialog and prompt you for your Microsoft Online Service ID. Enter the credentials of a user with a valid Office 365 license.
    - Once your Microsoft Office 365 license has been verified Microsoft Office setup is complete.
- Installing Microsoft Lync (assumed E1/E3 Microsoft Office 365 license):
    - In section 2, select your language and version then click Install.
    - Save the LyncSetup.exe installer.
    - Once the download has completed run the installer (will require Administrator privileges).
    - Microsoft Lync will start automatically once installation is complete. You will be prompted to enter your Microsoft Online Service ID. You will then be prompted again for your password.
- Configuring your Office desktop apps (assumes E1/E3 Microsoft Office 365 license):
    - In section 3, click Set up.
    - A dialog will prompt you to Run the Office365DesktopSetup.
    - Enter your Microsoft Online Service ID. You'll then be prompted to sign into your domain.
    - Enter your AD Connect credentials.
    - The Microsoft Office 365 desktop setup with then check your system configuration (this can take some time)
    - Once the initial system check has been completed you will be prompted to continue the configuration and installation of updates for your desktop applications (Outlook, Sharepoint and Lync).
    - Once the configuration and installation of updates is complete you will be prompted to restart the computer.
    - Once the computer restarts and you login the Microsoft Office 365 desktop setup will resume and check your system configuration again.
    - Upon completion there will be some additional manual configuration for Microsoft Outlook.
    - Open Microsoft Outlook.
    - Proceed through the setup wizard and select to configure an Email account.
    - Enter your Microsoft Office 365 email address if it has not already been entered.

- You will be prompted to authenticate.
- Setup will complete and will sync with Microsoft Exchange Online.

Troubleshooting

- If the command `Set-MsolDomainAuthentication` generates the following error:

```
Set-MsolDomainAuthentication : You cannot remove this domain as the default dom
ain without replacing it with another default domain. Use the the Set-MsolDomai
n cmdlet to set another domain as the default domain before you delete this dom
ain.
```

  This means the domain being set for federation in already the primary domain. Go into the Office 365 portal and set a different domain as the primary domain.
  - Above Admin Overview click the Organization Name.
  - On the Window that pops up click Edit.
  - Pick a different Primary Verified Domain

- If the installation of the Directory Synchronization tool fails check the Event Viewer.
  - One cause of failure is that the Microsoft Online Service Sign-In Assistant is already installed.
  - If the Directory Synchronization tool needs to be uninstalled it might be necessary to log off first and then login again.
  - If the Directory Synchronization tool is really slow the server probably lacks sufficient RAM.

- If SSO fails at Microsoft with the error: Your organization could not sign you in to this service
  - Verify the SAML1.1 contains the expected userPrincipalName (SCIM.userName) and objectGUILD (SCIM.externalId).
  - Verify the federation settings using the command: `Get-MsolDomainFederationSettings -DomainName <YOUR DOMAIN>`

- If after the installation of Microsoft Office Professional Plus the Microsoft Online Services Sign In Assistant fails to install with the error: “The Microsoft Online Services Sign In Assistant has experience an error. The error must be resolved before your subscription for this product can be verified. To retry subscription verification, first resolve error message 800704DD or try to manually install the Microsoft Online Services Sign In Assistant....” you will need to manually install the Microsoft Online Services Sign In Assistant. Go to http://www.microsoft.com/en-us/download/details.aspx?id=39267 to download the installer.

  Once install is complete you will need to relaunch the service to verify your Office 365 license. Details on how to do that can be found here: http://office.microsoft.com/en-ca/word-help/reactivate-subscription-license-by-using-osaui-exe-HA102053194.aspx

- If active profile authentication fails for Microsoft Lync or Microsoft Exchange (Outlook) clients verify that the necessary DNS records have been added to your DNS. For details see: http://office.microsoft.com/en-us/office365-suite-help/gather-the-information-you-need-to-create-office-365-dns-records-HA104028359.aspx?CTT=5&origin=HA102851099