CROSSMATCH™

DigitalPersona®

SSO for Office 365

Azure Cloud Hosted with On Premise AD

LDS Solution Deployment Guide

Published: June 19, 2017 (v2.2)

Table of Contents

Scope

This document covers configuration of a Federated Domain in Azure. Active Directory users will be synchronized to Azure AD via Azure AD Connect, DigitalPersona LDS & STS is configured in Azure Classic to gain access to office 365.

Customer Prerequisite Steps: General

Prior to a session with the DigitalPersona Solution Engineer, the customer should ensure that the following procedures have been completed.

1. You will need a Microsoft Azure subscription and an Office 365 subscription with federation capability.
2. An Office 365 Global Administrator account is required for changing the tenant from Manage mode to Federation mode
3. Have access to either a wildcard SSL certificate for the public domain name, or an SSL certificate for the specific host name that will be used for the DigitalPersona Secure Token Service (STS).

Customer Preparation Steps: In Azure Management Portal

4. Access the Azure Classic Management Portal (https:\\manage.windowsazure.com) with your Microsoft Azure account.
5. Create an Azure Classic virtual network (VNet). Ensure that the VNet is in the same region where domain services are supported. For more information, see the following webpage. https://azure.microsoft.com/en-us/updates/active-directory-ds-new-regions/
6. Enable Domain Services. This step will take from 30 to 60 minutes. Make sure to select your domain name for the DNS DOMAIN NAME OF DOMAIN SERVICES option. If domain services is already enabled in the existing Azure Subscription, provide information about the domain name used.
7. *(For Solution Engineer)* Go to step 10. If possible, validate or have the customer show you the existing settings

   By default, the registered Office 365 domain name will be listed when enabling domain services. It is recommended to use the same on premise domain name as this will be in line with your on premise domain services.

   For further details, see this webpage. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-getting-started-enableaadds

   Note: Once the domain is activated two IP addresses will be allocated from the selected VNet for the domain services.

8. Verify that the *AAD DC Administrators* group has been created in Azure Active Directory.

   This Group contains the list of all domain admin accounts. Users who are added to the group will be domain admins for the Azure cloud domain services. A user who is a member of this account will be required when configuring the DigitalPersona solution.
   For further information, see this webpage.

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-getting-started-create-group

This group should be created when domain services are enabled. It can also be created manually if necessary.

9. Add the IP address generated with Domain Services in to the existing Virtual Network DNS Settings.

   For further information, see the section on *DNS Servers* on this webpage.

   https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-portal-classic

   Create a Windows server 2012 R2 Datacenter or Windows server 2016 Virtual Machine with any preferred size. For Region/Affinity Group/Virtual Network, use the virtual network used by the domain services.

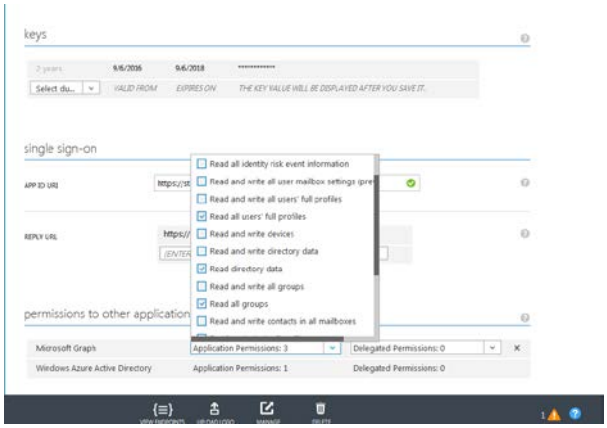
   For further information, see this webpage.

   https://docs.microsoft.com/en-us/azure/virtual-machines/windows/classic/tutorial

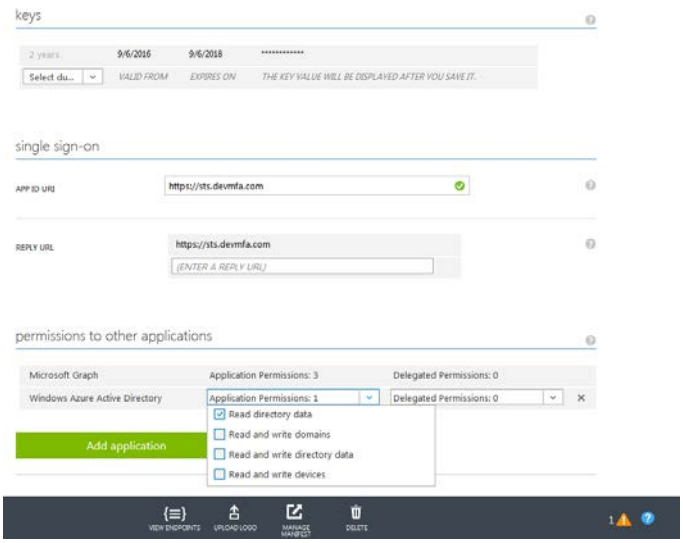
10. Create a new Azure AD application.

WARNING – When creating the application, it is important to make note of the *Client ID* and *Client* Key values, because these will be needed later by the DigitalPersona Solutions Engineer, but will no longer be visible after about 15 minutes. *If these values are not saved, the Azure AD application will need to be recreated.*

a. Create a new application within your Azure AD, and select the option to add an application that your organization is developing.
b. Enter a custom name and select *Web* Application as the Type.
c. On the *App* properties screen, enter the fully-qualified sign-on URL and App ID URI for the application.
d. On the application *Configuration* screen, create a new 2-year key for the application and copy it as soon as it is generated.
e. Add the following permissions to the *Microsoft Graph* application.
   - Read all user's full profile
   - Read directory data.
   - Read all groups



f. Add the following permissions to the *Windows Azure Active Directory.*
   - Application Permission: Read directory data
   - Delegated Permissions: Sign in and read user profile



Customer Prerequisite Steps: On premise Domain Controller

1. SSL certificate – Import either a wildcard certificate for the public domain name, or an SSL certificate for the specific host name that will be used for the DigitalPersona Secure Token Service (STS).
2. Install and configure *Azure Active Directory Sync*.

   If this has already been setup, skip this step.
3. Install the *Azure AD PowerShell Module* on the same server where *AAD Connect* is installed. This will be required for converting the existing managed domain to a federated domain. If this has already been installed, skip this step.

Solution Engineer's Steps: Azure Portal

1. Verify the correct configuration of Azure VM, Vnet, Domain services & Web Application as described in previous sections.
2. Check if LDAP Services are responding to a valid AAD DC Administration account. You can use any LDP tool to check the binding.
3. Check DNS services. Run *Nslookup* and verify that the required name resolution is working as expected.
4. Make sure a *global admin* user is available in the *AAD DC Administrators* group.
5. Ensure that the VM provided in Azure has been created on the *Classic* portal and is domain joined to the Azure Domain services. You should be able to log in to this VM using the global admin user in the AAD DC administrator group.
6. Check the sync status between the Azure cloud and the Domain Controller.

Solution Engineer's Steps: VM in Azure Cloud

1. Login as a global admin user.
2. Import the SSL certificate provided by the customer.
3. Copy the following DigitalPersona packages to the VM.
    - DigitalPersona LDS server, DigitalPersona LDS Administration Tools, DigitalPersona Extended Server Policy Module (ESPMS) and the DigitalPersona Web Management Components.
4. Install each component and configure according to instructions in the DigitalPersona Administrator Guide for the LDS solution. When installing the *Web Management* Components, use the *Express Configuration* option, and on the *Directory Access account* page select *Skip this page*.
5. After successful configuration, open the *IIS Manager* and navigate to the *Application Pools* section.
    - Right-click on the *DigitalPerosnaLdsPoolV4* application and select *Advanced Settings*.
    - Scroll down to the *Identity* tab under the *Generate Process Model Event Log* entry.
    - Select the global admin user provided by the customer.
6. Update the *web.config* file for Passive STS with the Azure application details created by the customer in the previous section. The path to the file is – *C:\Program Files\DigitalPersona\Web Management Components\DP STS\DPPassiveSTS \web.config*
   In the <*AltusConfirm*> section, insert the required information in the following fields.
    - **AzureTenantId=***"<domainname>"*
    - **AzureClientId=***"<Client Id key from Azure>"*
    - **AzureClientKey=***"<Client Key from Azure>"*

   Example:

```
<AltusConfirm AuthSvcUri="https://sts.<domainname>/DPWebAUTH/DPWebAuthService.svc"
  PolicySvcUri="https://sts.<domainname>/DPWebPolicies/DPWebPolicyService.svc"
  ClaimSvcUri="https://sts.<domainname>/DPWebClaims/DPWebClaimsService.svc"
  AzureTenantId="<domainname>"
  AzureClientId="98f58100-18a9-450b-94c0-62c63eb1593c"
  AzureClientKey="oJ9UUn34sVagsdfgXdfgsdyd5FzyEot/JpdU1GZ34Y=" />
```

Customer Federation Steps

On the system where *AAD Sync* and the *Azure AD PowerShell Module* are installed, perform the following steps to configure your Azure AD domain as a Federated domain.
WARNING: Federation generally takes between 15 and 90 minutes. During this time access to all Office 365 apps will be unavailable.

1. Start a Windows PowerShell session.
2. Import the MSOnline mode by entering the following cmdlet.

   Import-Module MSOnline

3. Connect to the online service by executing the following cmdlet.

   Connect-MSolService

4. Enter the Office 365 administrator username and password.
5. Verify that the domain name is listed by executing the following cmdlet.

   Get-MsolDomain -domain <domainname>

   You should be able to see the name of the domain that you will be federating.

6. Convert the domain to a federated domain by executing the *Set-MsolDomainAuthentication* cmdlet with the parameters shown below, replacing the highlighted elements with your domain name and STS FQDN.
   Also specify the signing certificate value, which you can find by navigating to your STS metadata page and copying the string representation of the signing certificate.

   The STS Medata data URL is *https://sts.MyDomain.com/dppassivests/wsfed/metadata*

   Set-MsolDomainAuthentication

   -DomainName <domainname>

   -Authentication Federated

   -ActiveLogOnUri https://sts.<domainname>/DPActiveSTS/ActiveSecurityTokenService.svc/mixed/username/

   -IssuerUri https://sts.<domainname>/dpsts

-LogOffUri https://sts.<domainname>/dpsts/wsfed

-MetadataExchangeUri https://sts.<domainname>/DPActiveSTS/ActiveSecurityTokenService.svc/mex

-PassiveLogOnUri https://sts.<domainname>/dpsts/wsfed

-PreferredAuthenticationProtocol WSFED

-SigningCertificate CertficateValue "

Example

Set-MsolDomainAuthentication -DomainName <domainname> -Authentication Federated -ActiveLogOnUri https://sts.<domainname>/DPActiveSTS/ActiveSecurityTokenService.svc/mixed/username/ -IssuerUri https://sts.<domainname>/dpsts -LogOffUri https://sts.<domainname>/dpsts/wsfed -MetadataExchangeUri https://sts.<domainname>/DPActiveSTS/ActiveSecurityTokenService.svc/mex -PassiveLogOnUri https://sts.<domainname>/dpsts/wsfed -PreferredAuthenticationProtocol WSFED -SigningCertificate MIIDADCCAeigAwIBAgIQQCbMQ9s9YYRHa3UFMY/1CDANBgkqhkiG9w0BAQ0FADAYMRYwFAYDVQQDDA1zdHMucWFtZmEuY29tMB4XDTE3MDMwNjIyMjAzMVoXDTE4MDMwNjIyMjAzMVowGDEWMBQGA1UEAwwNc3RzLnFhbWZhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOceGDySSTdtYAw26oGfWXB1sapJ0xi1OTnHIZiwtzgpgRu9vwpTxRE/SI5NqE53T+txba+bS2tsy80mCnPFMUqnAZ70CFrqkFgaxDid1Sx4APXNFwCyUgKBQ8aGIPz79WVzwCEvnIofXbS6GC6YJm3tj0F7RBU3P0Q5MCdHe6FNn9XtKq9vHbA3Oq+jW+xdoAn/kbBxbBBXOpiNuDs1dW932Rk3KP1wvz1Uz46UZ0w5tT6dPYclstaLdaikdhqNY35/Bz6bA9xUFIju5HKv75n/5jlTaOcHfMybb7D4rSHUVaCk6a7FnCOAfycNQ5XqPeentcCYYxm+LLgGGoWbhscCAwEAAaNGMEQwEwYDVR0lBAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFJyTuGnlHjsMWCDNQ4hKBRwq5QUlMA4GA1UdDwEB/wQEAwIFIDANBgkqhkiG9w0BAQ0FAAOCAQEA47qrxXZIIfyufs1aTEAQeMXVeGGnDUv22b5TpXl4aUsjP8D4fIguXQrzw3Zz7UcS+tvt+k0nkPKOtAINdc33LJUcThv11wkZwrB0Y5WZ/1tXW4qntYwpVsAIXeb/PEQhsx02NHgVopbXINh10RNzg5HxCLBqgIWL4WkMv+HDb/7lTwQdgPFmRS7LeeuDkrVmWqzWDaHlmlpnM2N7ZK7SnScVgppxtEsjyxFryimf9kyzeJrYggOvbJCGvf/IkFg35IS2F+mgqKEvsQO4+F1kIqOspZZgWBHNDdQv0iSRLn2EXp4Oi0NWdAd7J8Mp7KtBibID5To0vhRj+F8YARGZOQ==

Customer Steps to Turn off the Federation

If at some point, it is necessary to turn off the federation and switch back to a Managed domain, you can run the following cmdlet with the option *Managed*.

Set-MsolDomainAuthentication -DomainName domain.com -Authentication Managed

Troubleshooting Steps

1. If the STS login page displays on the server that is hosting STS, but does not display externally, verify the bindings in IIS Manager and make sure that the correct SSL certificate is selected.
2. Logging can be enabled on the DPActiveSTS website by including the following element in its *web.config* file.

   <sharedListeners>

```
    <add initializeData="C:\dptrace\TracingAndLogging-server.svclog"
    type="System.Diagnostics.XmlWriterTraceListener" name="xml" />
  </sharedListeners>
```

3. For troubleshooting any application connectivity issues after federation, you can use the *Remote Connectivity Analyzer* at *https://testconnectivity.microsoft.com/*.
4. You should clear out any previous tokens or sessions and start fresh after Federation. For example, sign out of any MS-Office applications and delete user sign-in information from Skype.