CROSSMATCH™

DigitalPersona®

Altus Office 365 Deployment Guide

Published: April 10, 2017 (v1.0)

Table of Contents

Scope

This document covers deployment and configuration of Altus STS with an Office 365 Federated Domain, and connection to an on-premise Altus AD Server. Active Directory users will be synchronized to Azure AD via Azure AD Connect, and users will gain access to the enterprise's SaaS applications.

Prerequisites

The following prerequisites should be satisfied prior to continuing with deployment.

- Public domain name – This must be the same domain name registered with Office 365 tenant.
- SSL certificate – Either a wildcard certificate for the public domain name, or one for the specific host name that will be used for STS.
- Office 365 Tenant – An Office 365 subscription with at least the Pro Plus plan.
- Administrator Account – An Office 365 Global Administrator account is required in order to change the tenant from Manage mode to Federation mode.
- Azure Active Directory Sync tool – The AAD Sync tool must be configured to use UPN as the On premise attribute to Azure AD username, and the source Anchor should be objectGUID.
- Altus Server – An Altus AD or Altus LDS Server must be installed and licensed.
- Users – Users need to be enrolled with the Altus Server.
- STS – Preconfigured Altus STS and all required components for STS. Ensure that you are able to open the STS Metadata page by navigating to the following URL: https://<External_Host_Name>/dpsts/wsfed/metadata

Configure Federation for Office 365 tenant

1. On the system which has AAD Sync installed, install the Azure AD PowerShell Module.

   Download the *Azure Active Directory Module for Windows PowerShell (64-bit***)** from (http://go.microsoft.com/fwlink/p/?linkid=236297), and click *Run* to launch the installer package.

2. Perform the following steps to configure your Azure AD domain as a Federated domain:

   a. Start a Windows PowerShell session.

   b. Import the MSOnline mode by typing *Import-Module MSOnline*

   c. Connect to the online service by typing *Connect-MSolService*

   d. Enter the Global Administrator credentials for an account that is not within the federated domain.

   e. Verify if the domain name is listed by executing the following command. Get-MsolDomain you should be able to see the domain listed which required to be federated.

f. To convert the domain to a federated domain, execute a *Set* command with the following parameters, replacing the highlighted elements with your domain name and STS FQDN.

Set-MsolDomainAuthentication

-DomainName domain.com

-Authentication Federated

-ActiveLogOnUri
https://sts.domain.com/DPActiveSTS/ActiveSecurityTokenService.svc/mixed/username/

-IssuerUri https://sts.domain.com/dpsts

-LogOffUri https://sts.domain.com/dpsts/wsfed

-MetadataExchangeUri
https://sts.domain.com/DPActiveSTS/ActiveSecurityTokenService.svc/mex

-PassiveLogOnUri https://sts.domain.com/dpsts/wsfed

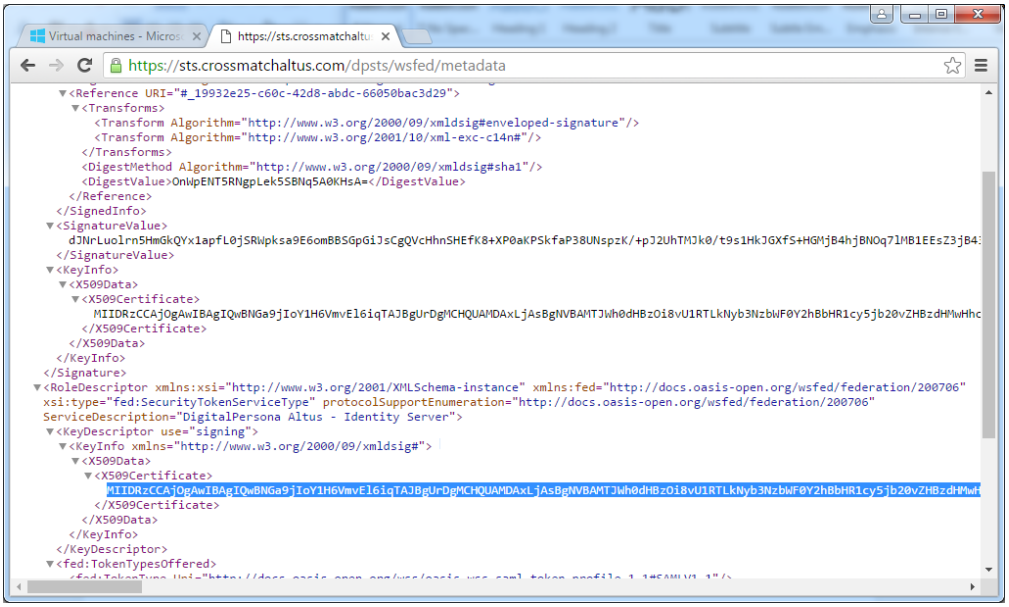
-PreferredAuthenticationProtocol WSFED

-SigningCertificate CertficateValue "

Example

Set-MsolDomainAuthentication -DomainName qamfa.com -Authentication Federated -ActiveLogOnUri https://sts.qamfa.com/DPActiveSTS/ActiveSecurityTokenService.svc/mixed/username/ -IssuerUri https://sts.qamfa.com/dpsts -LogOffUri https://sts.qamfa.com/dpsts/wsfed -MetadataExchangeUri https://sts.qamfa.com/DPActiveSTS/ActiveSecurityTokenService.svc/mex -PassiveLogOnUri https://sts.qamfa.com/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==

g. To specify the correct signing certificate value, navigate to your STS metadata page and copy the string representation of the signing certificate.



Turn off Federation

If you wish to turn *off* the Federation and switch back to the Managed domain, run the following script with the option *Managed*

Set-MsolDomainAuthentication -DomainName domain.com -Authentication Managed

Troubleshooting

1. If the STS login page displays on the server hosting STS, but not externally, the bindings need to be verified on IIS to make sure they contain the correct certificate. The STS certificate needs to be selected.
2. Logging can be enabled on the DPActiveSTS website by including the following 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 post federation, the below site can be used-

   https://testconnectivity.microsoft.com/
4. You should clear out any previous tokens or sessions and start afresh after Federation. Examples include signing out of any MS-Office application and Deleting user sign-in information from Skype.