****

Integrating ADFS/Office 365

with DoubleClue via SAML



# Introduction

This guide provides the instructions of how to configure Microsoft Active Directory Federation Services (ADFS) server and DoubleClue Enterprise Management (DCEM), so that ADFS Applications, like Office 365, use DoubleClue multi-factor authentication (MFA). This can be achieved by using the Security Assertion Markup Language (SAML) XML framework.

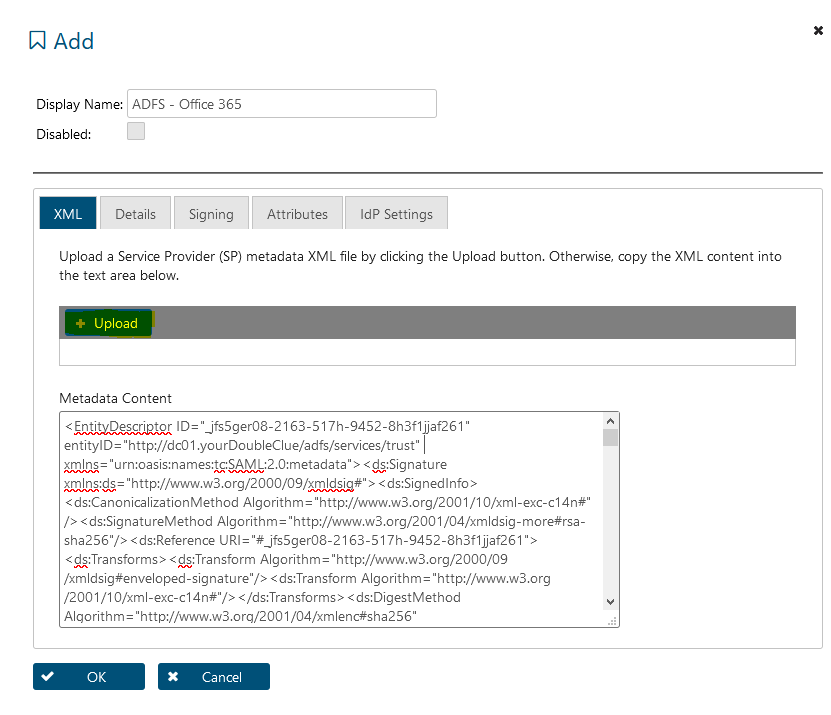
Requirements:

* Installation of ADFS 3.0+.
* DCEM 2.2.1+

# Scenario

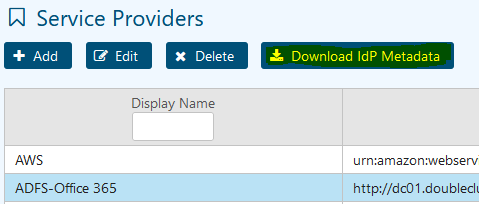
* Users connect to Applications such as Office 365 or Web-OutLook via ADFS
* ADFS acts as a SAML Service Provider (SP)
* DoubleClue acts as a SAML Identity Provider (Idp)
* DoubleClue retrieves credentials form an internal Database, Active Directory or Azure AD

# Configuring DCEM for ADFS

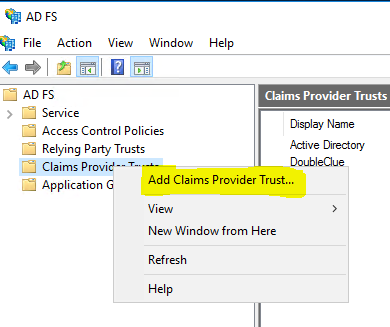
1. Download the ADFS meta data. Go to:   
     
   [**https://*your-adfs-address*/FederationMetadata/2007-06/FederationMetadata.xml**](https://your-adfs-address/FederationMetadata/2007-06/FederationMetadata.xml)  
     
   Replace "*your-adfs-address*" with the address of your ADFS server, e.g: adfs.hws-group.de. The store the metadata file on your machine.
2. Log in to DCEM and navigate to the main menu point “SAML” and choose “Service Providers”.
3. Add a new Service Provider and choose a custom template.
4. Choose a display name and click on “Upload” in the XML tab and choose the file you downloaded in step 1. The content will then be automatically displayed in the field below.
5. Save the configuration and close the dialog by clicking on “OK”.

# ADFS Configuration

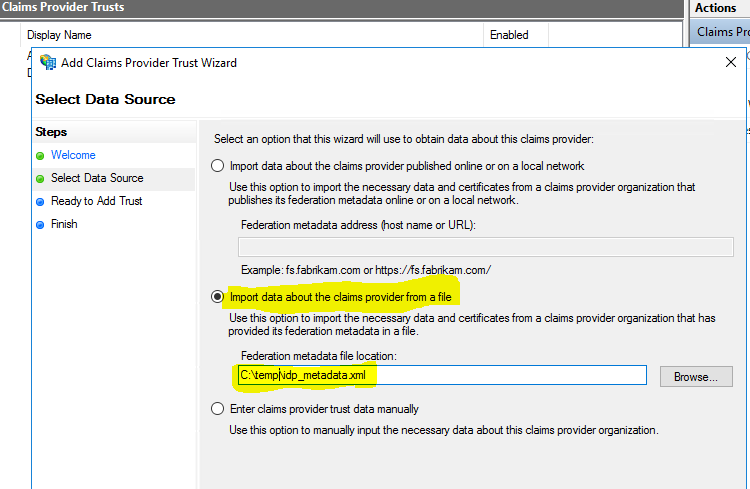
1. Log into DCEM, go to the main menu point “SAML” and choose “Service Providers”.



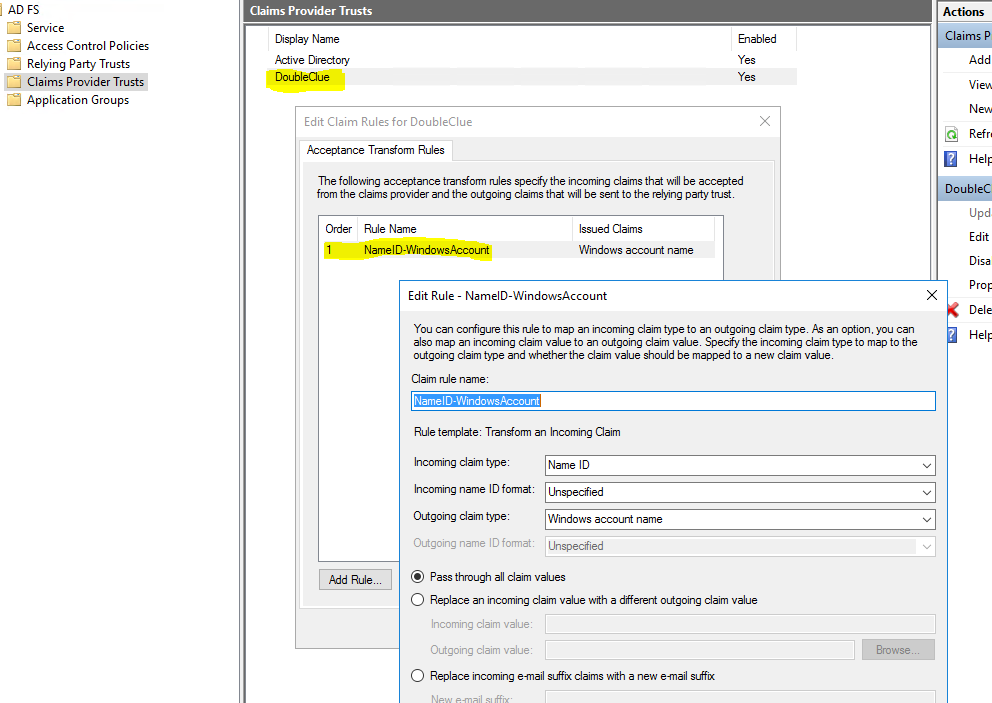
1. Click on “Download IdP Metadata” and download both, the ‘Certificate’ and the DCEM ‘Metadata’.
2. Open the ADFS Management Console and add a “Claims Provider Trust”.



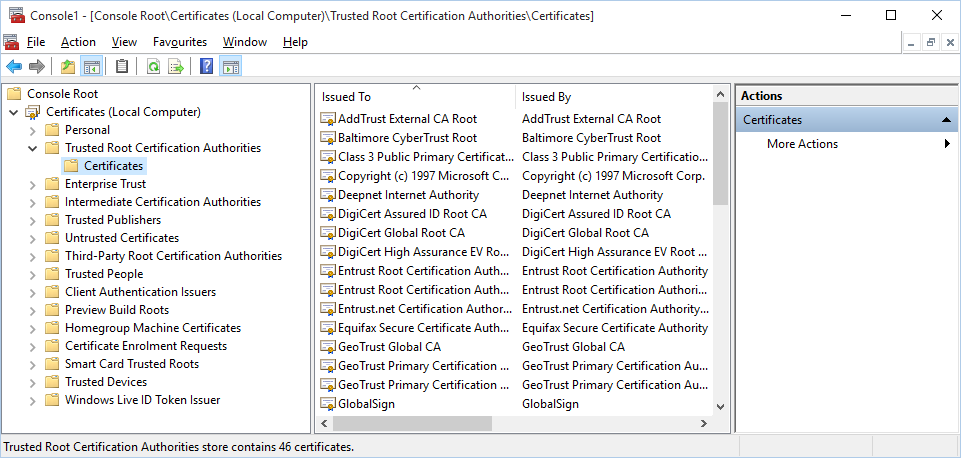
1. Click through the welcome panel till you get to “Select Data Source”.
2. Select “Import data about the claims provider from a file”.



1. Add the DoubleClue IdP metadata file you downloaded in step 1 into the "Federation metadata file location" field and click on “Next”.
2. In next View enter a unique and distinct Display Name, such as “**DoubleClue**” and click on Next.
3. For Office 365 to work with DoubleClue, you also need to add a new claims rule to the DoubleClue claims provider in the ADFS server.



1. Import the DoubleClue IdP CA certificate into the local computer certificate store as a root trusted CA on your ADFS server.



## Configuring ADFS with Power Shell Scripts

Unfortunately, configuring ADFS in the GUI is not enough to setup a Claims Provider Trust. You further need to execute the following commands in the Windows Powershell console of your ADFS Server:

**Set-ADFSClaimsProviderTrust -TargetName "*Claims\_Provider\_Name*" -SigningCertificateRevocationCheck None**

Further, execute the following command for all of your applications which should use DoubleClue as Identity Provider:

**Set-AdfsRelyingPartyTrust -TargetName "*Your-Application*" -ClaimsProviderName @("*Claims\_Provider\_Name*")**

Note:  
The “Claims Provider Name” is the ‘Display Name’ of the Claims Provider Trust. Such as “DoubleClue”.

The “Your-Application” is the Relying Party Trusts Display Name. Such as “Outlook Web App” or “Office 365”.

## Set the Anchor Type Claim

On Windows Server 16 RTM, you can further set the Anchor Type Claim with Powershell. Unfortunately, the powershell attribute to set Anchor Claim Type does not exist in the CTP, and the property cannot be defined using the UI.

If you don’t set the Anchor Type Claim, you will probably get the error:   
*MSIS9642: The request cannot be completed because an id token is required but the server was unable to construct an id token for the current user.*

To avoid this error execute the following Powershell command:

**set-adfsclaimsprovidertrust -targetidentifier yourDoubleClue.de -AnchorClaimType**

**http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname**

Where **“yourDoubleClue.de” is your new Claim Provider Trust name.**