



# Integration of ADFS with DoubleClue as a Multi-Factor Authentication (MFA) Provider



## 1. Introduction

This guide is intended for users of *Microsoft ADFS* who would like to add *DoubleClue* authentication as a second factor to ADFS authenticated logins for Web Applications.

### Requirements:

- Installation of ADFS 4 on a Windows Server.
- DoubleClue Enterprise Management (DCEM) installation with an imported set of users from the same Active Directory instance of the Domain Controller that the ADFS Server uses.

⚠ Please note: DCEM uses REST Web-Services for communications; so ideally, it is to be installed in the same internal network as the ADFS Server.

## 2. Setting up the ADFS MFA Provider Plugin

DoubleClue can be set up as a secondary factor to ADFS logins via a specially built MFA Provider Plugin, which communicates with a running instance of DCEM.

Copy the folder “adfs” from “DcemInstallation” to somewhere on your ADFS server.

### 2.1 Configuration

First, you need to set up the configuration file.

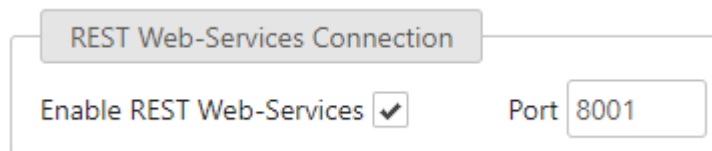
1. Inside the “adfs” folder you just copied, open the file “dcAdfsMfaProvider\_config.json” with a text editor of your choice. The contents of this file should be like the following:

```
{
  "restApiUrl": "https://dcem_server:8001/dcem/restApi/as",
  "restOperatorName": "RestServicesOperator",
  "restPassword": "test",
  "restConnectionTimeout": 5000,
  "messageResponseTryDuration": 1,
  "messageResponseMaxTries": 120
}
```

2. Modify the value of “restApiUrl” to an accessible URL of the REST services of your DCEM installation. The format of this should be:

<Base URL of DCEM server>:<REST port number>/dcm/restApi/as


You can find the REST port number by logging into DCEM and navigating to the main menu item “System”, sub menu “Cluster Configuration”. Here you will find the settings for the REST connection.



3. If you changed the credentials of the DCEM REST services operator, you will need to modify the values of “restOperatorName” and “restPassword” as well. You can find the values of these by logging into DCEM and navigating to the main menu item “Administration”, sub menu “Operators”. Search for the Operator whose Role is “RestServices”.
4. Optionally, you may modify the other configuration settings to your liking.
  - restConnectionTimeout: How much time to wait (in milliseconds) for a successful connection to the REST service before firing a timeout.
  - messageResponseTryDuration: How much time to wait (in seconds) between pings of message statuses.
  - messageResponseMaxTries: How many times a message is pinged before showing a timeout error.
5. Save and close the file.

## 2.2 MFA Provider Plugin Installation

1. Open Windows PowerShell in Administrator mode.
2. Navigate to the setup folder using “cd”.
3. Run “.\Install.ps1”
4. Wait for the setup to finish (it may take about a minute to complete).

 Please note: The setup will restart the ADFS service, so make sure to run it at a time when it is safe for the service to be down for a few seconds.

If everything is set up correctly, whenever a user tries to login via ADFS, a secondary screen will appear afterwards asking the user to acknowledge a code with their DoubleClue App. Secure Messages sent to users’ devices use the “adfs.login” template.

If you want to make further changes to the text resources or the configuration file, you will need to run this setup again for the changes to take effect. Please retain your copy of the installation files for possible future use.

## 2.3 Text Resources (Optional)

In “adfs/resources”, you can find text files for English (“en.txt”), German (“de.txt”) and French (“fr.txt”). These will be used as resources for displayed text during the authentication with DoubleClue.

You may modify them as you like to fit your company’s needs. You can also add new languages by simply adding more text files and using the same keys. Any new text files need to be named with their respective Culture Codes. You can find a full list of Microsoft supported Culture Codes at <https://msdn.microsoft.com/en-us/library/hh441729.aspx>

Changes will take effect only after having reinstalled the MFA Provider Plugin. If this does not work, it may be necessary to restart the entire server, and then reinstall the Plugin again. Unfortunately, this is a limitation of ADFS, and currently there is no other known solution for it.

## 2.4 Changing the Identity Claim (Optional)

By default, the DoubleClue MFA provider will identify DoubleClue users by their “SAM-Account-Name” (a.k.a. Windows Account Name), so make sure to import users from LDAP into DCEM using this property as their Login ID.

If, however, this is changed for some reason, it is possible to change which property the MFA provider uses to identify users so that it matches the imported set in DCEM.

To do this, open “regedit” and browse to:

“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DcAdfsMfaProvider”

Inside is a String key called “LoginAttribute”. Its value can be changed to one of the following:

- <http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname>
- <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn>
- <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>
- <http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid>

Unfortunately, ADFS only supports one of these four options as identity claims to MFA Providers, so it is currently not possible to use other attributes.

Changes will take effect only after having restarted ADFS. If this does not work, it may be necessary to restart the entire server, and then restart ADFS again. Unfortunately, this is a limitation of ADFS, and currently there is no other known solution for it.