MobileID Authentication Provider for ADFS - Quick Guide

Table of Contents

This is a quick tutorial how to setup an Active Directory Federation Service (ADFS) external authentication provider which authenticates end users with Mobile ID.

References:

- https://github.com/MobileID-Strong-Authentication/mobileid-enabler-adfs
- https://github.com/MobileID-Strong-Authentication/mobileid-enabler-adfs/blob/main/doc/mobile_id_microsoft_adfs_solution_guide_v1_3.pdf

Windows Server 2022

For this tutorial we use a Windows Server 2022 instance from Amazon Elastic Compute Cloud (Amazon EC2). This *instance* is a virtual server in the AWS Cloud. With Amazon EC2, you can set up and configure the operating system and applications that run on your instance.

Step 1: Create Windows Server Instance

Create a new Amazon Machine Image (AMI) Windows Server instance

If you are not familiar with Amazon EC2, please read https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/EC2_GetStarted.html

- Select `Microsoft Windows Server 2022 Base (Datacenter edition)` as Amazon Machine Image (AMI)
- Select instance type. I recommend `t3.large`
- Create a VPC, enable Auto Public IP
- Create a SecurityGroup and make sure your source IP address is whitelisted in the INBOUND RDP rule
- Create an associate an Elastic IP Address (EIP) and make sure this IP address is whitelisted on the Mobile ID Firewall. Select "allow dissassociate".
- Click the "Connect" Button, select "RDP client" and download the remote desktop file to your Desktop
- Click "Get password", select your key pair and write down the Windows password

Note: You can anytime stop or start an instance, which helps to keep costs low. Only run the instance when it is really used.

Connect to the Windows Server instance

- On your Desktop, start the Remote Desktop Client and load the RDP Profile
- In the RDP Client, adjust the Screen Resolution
- In the RDP Client, select your local drive (gain access to local files)
- Save the changes to your local remote desktop file
- Connect to the Windows Server and login with the password retrieved in step above

Basic Windows configuration

- Adjust the Timezone of your Windows Server
- Set Region Format to "German (Switzerland)"

- Open Server Manager -> Local Server: Disable IE Enhanced Security Configuration
- Copy file from your local disk to the Windows Server's `C:\Users\Administrator\Downloads`. You need at least these files:
  - `YourMobileIdKeyFile.p12` - Mobile ID Account Key File (PFX/PKCS#12 format)
  - `midadfs_setup_*.exe` - Latest Installer Binary from GitHub
  - `myconfig*.xml` - Your MobileID ADFS configuration file (samples can be found on GitHub)
  - Swisscom Root Certificates
    - `Swisscom_Root_CA_2.cer` (Source)
    - `Swisscom_Root_CA_4.cer` (Source)
- `Get-RemoteSSLCertificate.ps1` - Optional PowerShell Script to test an SSL connection to a remote host (e.g. to the Mobile ID server)

Verify the connectivity to Mobile ID API

You can either use Internet Explorer to try to connect to `https://mobileid.swisscom.com` (which should return a 404/PageNotFound) or you can use the PowerShell Script as shown below.

PowerShell - Please run as Administrator

```
cd "C:\Users\Administrator\Downloads\"
$cert=(.\Get-RemoteSSLCertificate.ps1 mobileid.swisscom.com)
Set-Content mobileid.swisscom.com.cer -Encoding Byte -Value $cert.Export('Cert')
```

Get-RemoteSSLCertificate.ps1

```
[CmdletBinding()]
param (
    [Parameter(Mandatory=$true)]
    [string]
    $ComputerName,

    [int]
    $Port = 443
)

$Certificate = $null
$TcpClient = New-Object -TypeName System.Net.Sockets.TcpClient
try {

    $TcpClient.Connect($ComputerName, $Port)
    $TcpStream = $TcpClient.GetStream()

    $Callback = { param($sender, $cert, $chain, $errors) return $true }

    $SslStream = New-Object -TypeName System.Net.Security.SslStream -ArgumentList @($TcpStream, $true,
$Callback)
    try {

        $SslStream.AuthenticateAsClient('')
        $Certificate = $SslStream.RemoteCertificate

    } finally {
        $SslStream.Dispose()
    }

} finally {
    $TcpClient.Dispose()
}

if ($Certificate) {
    if ($Certificate -isnot [System.Security.Cryptography.X509Certificates.X509Certificate2]) {
        $Certificate = New-Object -TypeName System.Security.Cryptography.X509Certificates.X509Certificate2 -
ArgumentList $Certificate
    }

    Write-Output $Certificate
}
```

Check if the file `mobileid.swisscom.com.cer` exists, if it exists it means the connectivity worked. Also check if the certificate is valid (open the file).

Note: There are also other critical connectivity requirements such as `ldap.swissdigitcert.ch`. Refer to PDF Table 1.

Step 2: Install AD Domain

PowerShell - Please run as Administrator

```
$secpass=ConvertTo-SecureString "pass@word1" -AsPlainText -Force
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
import-module ADDSDeployment
Install-ADDSForest -DomainName "contoso.intern" -InstallDNS -SafeModeAdministratorPassword $secpass
```

This will ask you to reboot the System.

Step 3: Install ADFS

The ADFS Service will run in the context of a GMSA Account. Create a GSMA Account:

PowerShell - Please run as Administrator

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
New-ADServiceAccount FsGmsa -DNSHostName adfs1.contoso.intern -ServicePrincipalNames http/adfs1.contoso.intern
```

For ADFS to work, we need a Certificate. The following lines create a self signed certificate with the required `Subject Name` and `Subject Alternative Names`.

PowerShell - Please run as Administrator

```
$selfSignedCert = New-SelfSignedCertificate -DnsName adfs1.contoso.intern,enterpriseregistration.contoso.intern,
adfs1.contoso.intern -CertStoreLocation cert:\LocalMachine\My
$certThumbprint = $selfSignedCert.Thumbprint
dir Cert:\LocalMachine\My
```

Install the self-signed certificate to have the required trust:

- Run `mmc.exe`
- Add snap-in Certificates (Computer)
- Go to "Certificates">"Personal">"Certificates"
- Right-click on `adfs1.contoso.intern` and select export
- Double-click the exported adfs1.contoso.intern.cer and install it to "Local Machine"

Install ADFS Federation:

PowerShell - Please run as Administrator

```
Install-WindowsFeature -IncludeManagementTools -Name ADFS-Federation
Import-Module ADFS
Install-AdfsFarm -CertificateThumbprint $certThumbprint -FederationServiceDisplayName "Contost ADFS Test" -
GroupServiceAccountIdentifier "contoso.intern\FsGmsa$" -FederationServiceName "adfs1.contoso.intern"
Set-AdfsProperties -EnableIdpInitiatedSignonPage $true
```

In the internal DNS Service of AD, configure the following A Record and a CNAME. Please replace the IP accordingly!

PowerShell - Please run as Administrator

```
$ipAdress = "10.0.0.25"
Add-DnsServerResourceRecordA -Name "adfs1" -ZoneName "contoso.intern" -AllowUpdateAny -IPv4Address $ipAdress -
TimeToLive 01:00:00
Add-DnsServerResourceRecordCName -Name "enterpriseregistration" -HostNameAlias "adfs1.contoso.intern" -ZoneName
"contoso.intern"
```

- Open Edge Browser and visit: https://adfs1.contoso.intern/adfs/ls/IdpInitiatedSignon.aspx
- Add this site to the "trusted sites" list.
- View the site's certificate details and click "Install Certificate", select "Local Machine"

At this point we have the basic ADFS Demo Setup (without MID/ADFS Authentication Provider) completed.

Step 4: Add Test User

- Run "Server Manager" -> "Tools" -> "Active Directory Users and Computers"
- Go to "contoso.intern" -> Users -> right-click and select "New -> User"
    - Set First- and Last name
    - Set User logon name
    - Click next
    - Set password and only select "Password never expires"
    - Finish
- Double-click User and select "Telephones"-register
- Set Mobile +41791288731. It also works in the format "+41-79 128 87 31". This number is a CA4 Mobile ID Test User (auto-responding).

Step 5: Install MID/ADFS Enabler

- Run `midadfs_setup_*.exe` (as admin)

Check Logs in Event Viewer and in `C:\Program Files (x86)\MobileIdAdfs\v1.3\inst`

Make sure, the it became available in ADFS Management Console:

PowerShell - Please run as Administrator

```
Get-AdfsAuthenticationProvider -Name MobileID13
```

Enable MFA in ADFS, Run "Server Manager" -> "Tools" -> "AD FS Management"

- AD FS Management: AD FS -> Service -> Authentication Methods -> Edit Mulit-factor Authentication Methods -> Select "Mobile ID Authenticator v1.3"
- AD FS Management: AD FS -> Relying Party Trusts -> Add Relying Party Trust...
- Select "Claims aware"
- Select "Enter data about the relying party manually"
- Display name "mobileid.ch"
- Select only "Enable support for the SAML 2.0 WebSSO protocol" and set value https://mobileid.ch
- Next, add https://mobileid.ch as Relying party trust identifier!
- Next, select "Permit everyone and require MFA"
- Once finished, open it again and go to "Endpoints"-tab and edit the SAML endpoint to set Binding to "Redirect" (to https://mobileid.ch)

Load the MID/ADFS configuration file:

PowerShell - Please run as Administrator

```
cd "C:\Program Files (x86)\MobileIdAdfs\v1.3"
.\import_config.ps1 "C:\Users\Administrator\Downloads\myConfig*.xml"
```

Important: A restart is usually required!

Example `myConfig*.xml` content:

```
<?xml version="1.0" encoding="utf-8" ?>
<appConfig>
  <mobileIdClient
    AP_ID = "mid://adfs-dev.swisscom.ch"
    SslKeystore = "LocalMachine"
    SslCertThumbprint = "19CB073F974729D9FEC8CB1A0C50866886FCDEBA"
    SslRootCaCertDN = "CN=Swisscom Root CA 2, OU=Digital Certificate Services, O=Swisscom, C=ch"
    DtbsPrefix = "ADFS Demo:"
    SecurityProtocolType = "Tls12"
  />
</appConfig>
```

```
<?xml version="1.0" encoding="utf-8" ?>
<appConfig>
 <mobileIdClient
    AP_ID = "mid://adfs-dev.swisscom.ch"
    SslKeystore = "LocalMachine"
    SslCertThumbprint = "19CB073F974729D9FEC8CB1A0C50866886FCDEBA"
    SslRootCaCertDN = "C=CH, O=Swisscom, OID.2.5.4.97=VATCH-CHE-101.654.423, OU=Digital Certificate Services,
CN=Swisscom Root CA 4"
    DtbsPrefix = "ADFS Demo:"
    SecurityProtocolType = "Tls12"
  />
</appConfig>
```

Step 6: Setup MID Certs

- Right-click your SSL Client certificate file
  - Install PFX
  - Local Machine
  - Click Next twice
  - passphrase ***
  - click Next and finish

Only if AP Client Cert is self-signed, do this:

- Run `mmc.exe`
  - Add/Remove Snap-in..., select Certificates
    - snap-ins panel, click Add > Computer account
    - click Next, Finish
  - Local Computer; right-click Trusted People,
    - navigate to All Task, then Import..., this opens the
    - Certificate Import Wizard; Clicks Next, locates the PFX file in File to Import, Next, enter passphrase: ***
    - clicks Next twice, Finish

IMPORTANT: Always run `mmc.exe` as Administrator to import the certs into `LocalMachine` (the certmgr.msc imports to `CurrentUser` only)

Configure trust to Swisscom Root CA 2 (or CA 4):

- navigate to
  - Trusted Root Certificate Authority
  - Right-click Certificates, select All Tasks, Import...
  - select the file *.crt containing the Swisscom Root CA 2 and/or Swisscom Root CA 4
  - Next twice, Finish, confirm Yes on the Security Warning "You are about to install a certificate from a certificate authority (CA) claiming to represent: ... Thumbprint (sha1): ..." Click OK.

PowerShell - Please run as Administrator

```
dir Cert:\LocalMachine\Root\ |? Subject -Like "*Swisscom*"
```

Give ADFS Service Account the required access to the client certificate
If winhttpcertcfg is not in the path, you might find it in C:\Program Files (x86)\Windows Resource Kits\Tools\.
If you do not already have the WinHttpCertCfg.exe tool on your Windows Server, download and install it: https://www.microsoft.com/en-us/download/details.aspx?id=19801

Please change the subject (in the example below it is `adfs-dev.swisscom.ch`) according to your own client certificate subject.

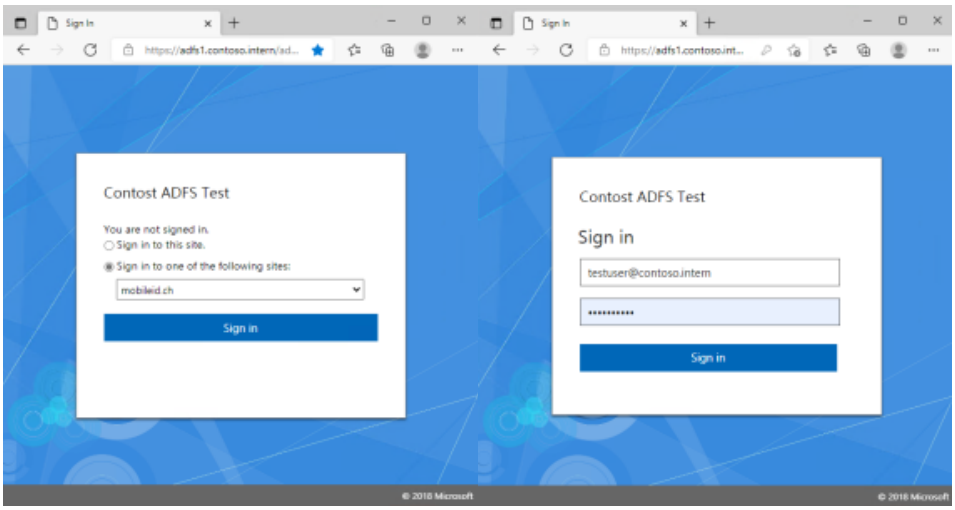
PowerShell - Please run as Administrator

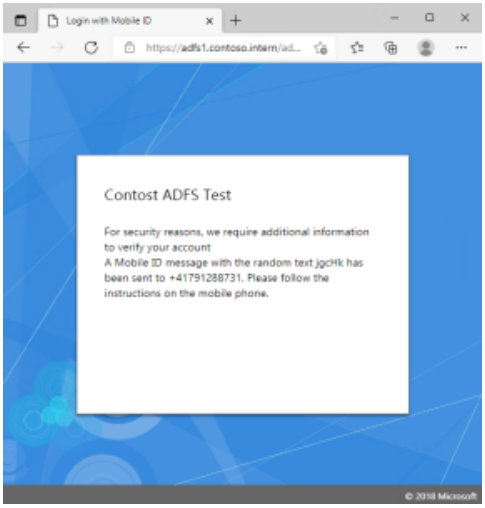
```
cd 'C:\Program Files (x86)\Windows Resource Kits\Tools'
.\winhttpcertcfg.exe -g -c LOCAL_MACHINE\My -s adfs-dev.swisscom.ch -a contoso\\fsgmsa$
```

Step 7: Login with MID

Finally, open the Internet Browser (Ms Edge) and visit: https://adfs1.contoso.intern/adfs/ls/IdpInitiatedSignon.aspx

You should be able to select mobileid.ch and then enter the test user credentials. This should invoke a Mobile ID authentication request to the phone number configured for this test user.





Troubleshooting

Connectivity Test

PowerShell - Please run as Administrator
`Invoke-WebRequest http://aia.swissdigicert.ch/sdcs-rubin4.crt`

Miscellaneous

PowerShell - Please run as Administrator

```
Get-AdfsProperties
Get-AdfsAuthenticationProvider –Name MobileID13

dir Cert:\LocalMachine\Root\ |? Subject -Like "*SwissSign*"
dir Cert:\LocalMachine\Root\ |? Subject -Like "*Swisscom*"

dir Cert:\LocalMachine\My
dir Cert:\LocalMachine\TrustedPeople

dir Cert:\CurrentUser\My
```

Wireshark Filter

```
(ip.dst == 195.65.194.58) || (ip.src == 195.65.194.58)
```

Trace Logging Configuration

PowerShell - Please run as Administrator

```
New-EventLog -LogName Application -Source MobileId
New-EventLog -LogName Application -Source MobileId.WebClient
New-EventLog -LogName Application -Source MobileId.Adfs
New-EventLog -LogName Application -Source MobileId.Adfs.AuthnAdapter
```

Add MobileID Log entries to `C:\Windows\ADFS\Microsoft.IdentityServer.ServiceHost.exe.config`
Ensure read access to log file, e.g. `C:\temp\*.log`
Note: A reboot will be required!

PowerShell - Please run as Administrator

```
Set-AdfsProperties -AuditLevel verbose
```

CMD.EXE- Please run as Administrator

```
C:\Windows\System32\wevtutil sl "AD FS Tracing/Debug" /L:5
```

Righ-click on "Applications and Service Logs" -> "View" -> "Show Analytic and Debug Logs"

Update Root CA Certificate List

PowerShell - Please run as Administrator

```
md C:\temp\certs
CertUtil –generateSSTFromWU C:\temp\certs\RootStore.sst
$file=Get-ChildItem -Path C:\temp\certs\Rootstore.sst
$file | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root\
```