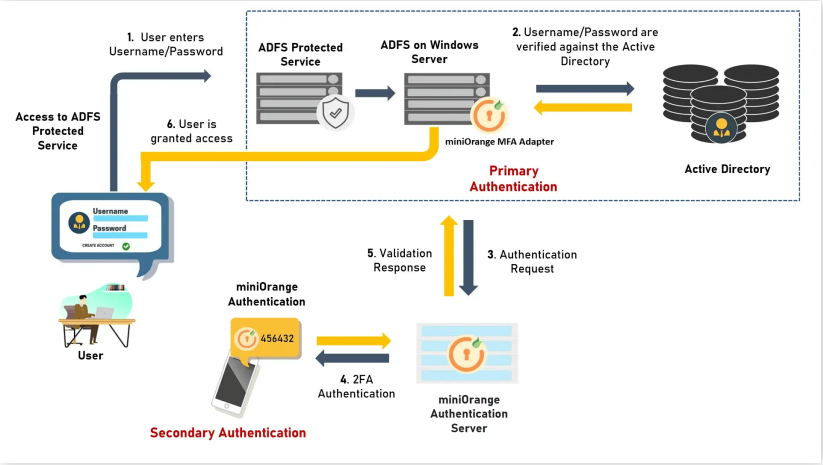
Contents

Request a Demo

Steps to Enable 2FA on top of ADFS Authentication?

The **miniOrange ADFS MFA connector** helps you to enable **Two Factor Authentication (2FA)** for your users to protect the access to **Microsoft Active Directory Federation Services (ADFS)** by adding a **second layer of authentication challenge** to existing username and password of ADFS Deployment. This extra layer prevents the unauthorized person from accessing the resources even if cyber attackers get to know your credentials.

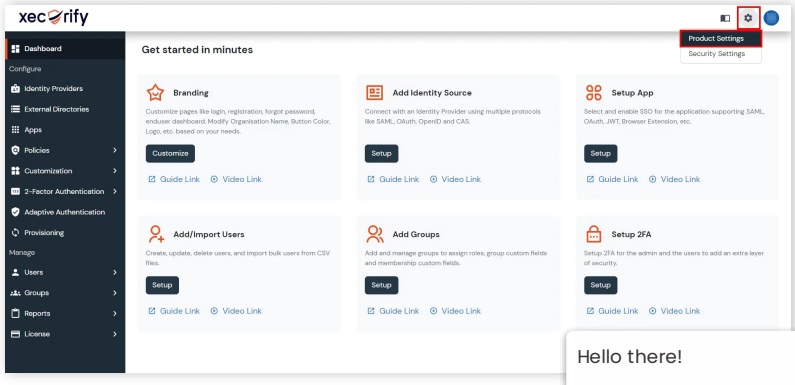
ADFS SSO Authentication Flow with miniOrange MFA Connector:

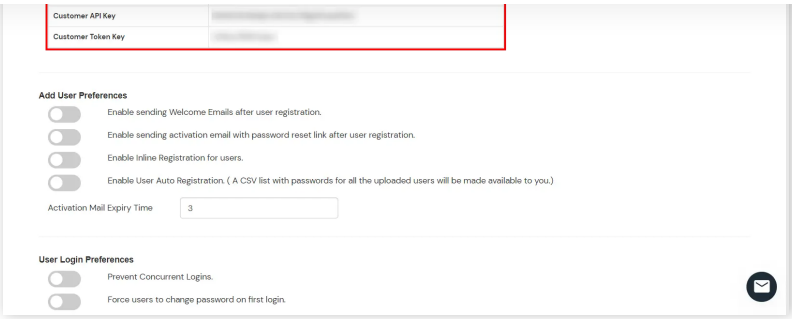


- A user attempts access to ADFS protected service with username / password.
- The username / password is verified against an existing first factor directory (i.e. Active Directory)
- Once the user's first level of authentication gets validated **ADFS sends the confirmation to miniOrange Authentication Server**.
- Now miniOrange Authentication Server asks for a **2-factor authentication challenge** to the user.
- Here user submits the response/code which he receives on his hardware/phone.
- **User response** is checked at miniOrange's Authentication Server side.
- On successful **2nd factor authentication** the user is granted access to login.

Install miniOrange ADFS MFA Adapter

- First, download the miniOrange MFA Adapter.
- Login into miniOrange Admin Console.
- Go to **Product Settings**. Copy **Customer Key** and **Customer API Key**.





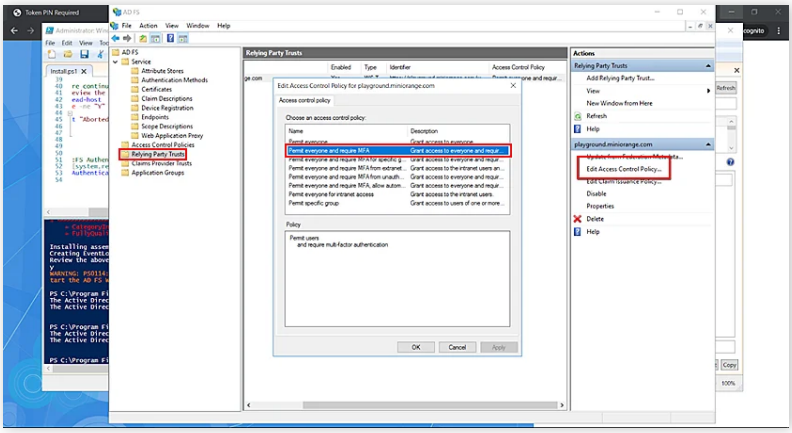
- Add the details like Customer Key and Customer API Key in **Install.ps1** file.

```
Write-Host "Creating required registry keys"
New-Item -Path "HKLM:\SOFTWARE\MFAAdapter" -Force | Out-Null
New-Item -Path "HKLM:\SOFTWARE\MFAAdapter\miniOrangeMFA" -Force  | Out-Null
New-ItemProperty -Path "HKLM:\SOFTWARE\MFAAdapter\miniOrangeMFA" -Name "CustomerID" -Value "<customer-key>" | Out-Null
New-ItemProperty -Path "HKLM:\SOFTWARE\MFAAdapter\miniOrangeMFA" -Name "BaseUrl" -Value "https://login.xecurify.com/moas" | Out-Null
New-ItemProperty -Path "HKLM:\SOFTWARE\MFAAdapter\miniOrangeMFA" -Name "ApiKey" -Value "<Customer API Key>" | Out-Null
New-ItemProperty -Path "HKLM:\SOFTWARE\MFAAdapter\miniOrangeMFA" -Name "IdentityClaims" -Value "http://schemas.microsoft.com/ws/2008/06/id
```

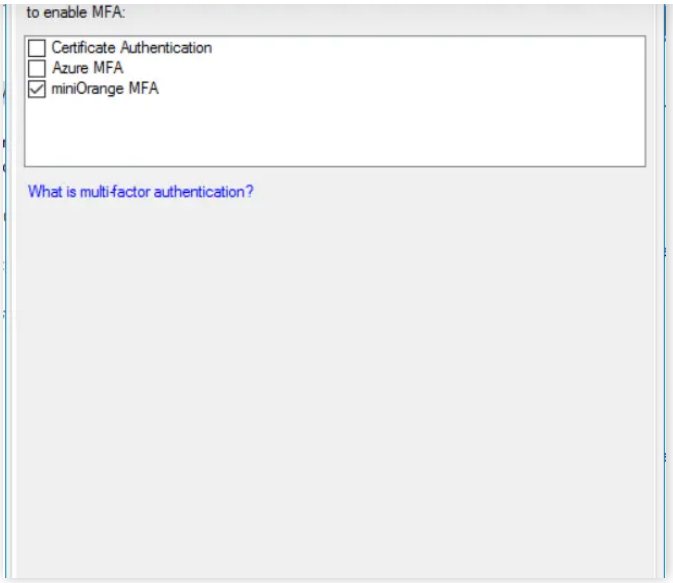
- Run the **Install.ps1** file on ADFS server in administrator mode.
- Press **Y** to continue registration.

```
Installing assemblies into the GAC
Creating EventLog source
Review the above and Press Y continue and register the Authentication Adapter. CTRL-C to exit
Y
WARNING: PS0114: The authentication provider was successfully registered with the policy store.  To enable this provider, you must res
tart the AD FS Windows Service on each server in the farm.

PS C:\Program Files\Ayushi\RadiusAuthenticationAdapter> net stop adfssrv
The Active Directory Federation Services service is stopping.
The Active Directory Federation Services service was stopped successfully.


PS C:\Program Files\Ayushi\RadiusAuthenticationAdapter> net start adfssrv
The Active Directory Federation Services service is starting.
The Active Directory Federation Services service was started successfully.
```

- Restart the ADFS service using the following command:
  - Net stop adfssrv
  - Net start adfssrv
- Edit the access control policy for the already added **Relying Party Trust** or any **Application Group** and select **Permit everyone and require MFA** to enable mfa after login.

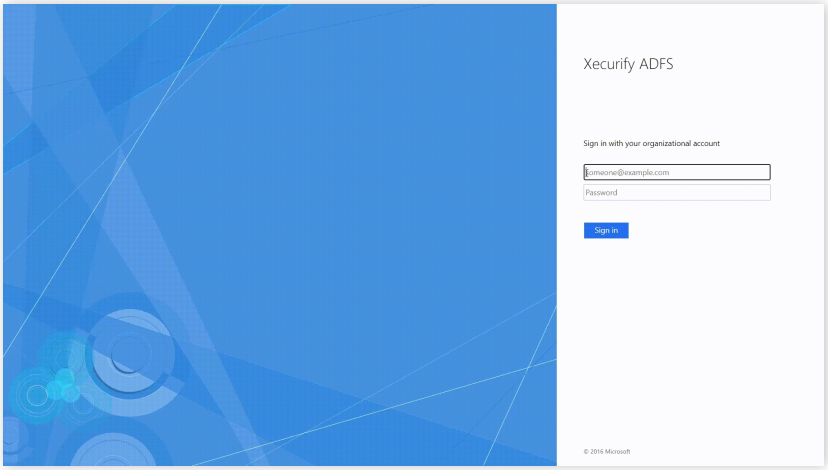


- Go to **Authentication methods** > **Edit Multi Factor Authentication** and select **miniOrange MFA**. Apply the settings.



User Experience

After entering the username and password into the AD FS login, user will be prompted for 2 factor method which is already configured for the user or set as default by the admin. Once the 2 factor gets authenticated, the user gets signed in.



Steps to Unregister

- Open Powershell on ADFS server in administrator mode.
- Use the command to Unregister the adapter:

```
Unregister-AdfsAuthenticationProvider -Name "miniOrangeADFSMFA"
```

- Restart the adfs service using the following command:
  - Net stop adfssrv
  - Net start adfssrv

You have successfully enabled the Two-Factor Authentication (2FA) by using miniOrange ADFS MFA Connector.

External References

- Two-Factor Authentication - 2FA, What is 2FA & How 2FA work?
- Single Sign-On (SSO) for Pre-Integrated Apps | SAML SSO | OAuth SSO | 2FA | Provisioning
- IDP Setup Guides - miniOrange Identity Server