mini@range

+1 978 658 9387 🛛 🕲 Login

Login **Q** Search

Contact Us

Products V Solutions V Pricing Resources V Partners

Contents

Overview

Install miniOrange ADFS MFA Adapter

User Experience

Steps to Unregister

External References

Request a Demo

IAM / Steps to Enable 2FA on top of ADFS Authentication

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.

xec ∕rify			IC 🗢 🔵
Deshboard	Get started in minutes	Product Settings Security Settings	
dentity Providers	Branding	Add Identity Source	Setup App
External Directories	Customize pages like login, registration, forgot password,	Connect with an identity Provider using multiple protocols	Select and enable SSO for the application supporting SAML,
III Apps	enduser dashooard. Modiry Organisation Name, Button Color, Logo, etc. based on your needs.	ike SAML, Gauth, OpenD and CAS.	CANIER, JWI, Browser Extension, etc.
Policios	Customize	Setup	Setup
Customization	> Z Guide Link Video Link	Z Guide Link Video Link	Z Guide Link Video Link
2-Factor Authentication	•		
Adaptive Authentication			
Provisioning	Add/Import Users	Add Groups	Setup 2FA
Aanago	Greate, update, delete users, and import bulk users from CSV files.	Add and manage groups to assign roles, group custom fields and membership custom fields.	Setup 2FA for the admin and the users to add an extra layer of security.
L Users	Setup	Setup	Settup
t Groups			
📋 Reports	> D Guide Link Video Link	2 Guide Link Video Link	🖾 Guide Link 💿 Video Link
E License	>		
			Hello there!
			Need Help? We are right here

	+1 978 658 9387 Login Q
mini@range	Products V Solutions V Pricing Resources Partners Free Trial Contact Us
	Add User Preferences Enable sending velocine Emails after user registration. Enable sending activation email with password reset link after user registration. Enable sending activation for users. Enable user Auto Registration (A GSV list with passwords for all the uploaded users will be made available to you.) Activation Mall Expiry Time User Login Preferences Prevent Concurrent Logins. Force users to change password on first login.
	 Add the details like Customer Key and Customer API Key in Install.psi file. write-Host "Creating required registry Keys" New-Item-Path "NKLK'SOFTWARE WrAdagter"-Force Out-Null New-Item-Path "NKLK'SOFTWARE WrAdagter"-Informage#A" -Force Out-Null New-ItemProperty -Path "NKLK'SOFTWARE WrAdagter Viniformage#A" -Name "Customer D" -Value "customer-Keys" Out-Null New-ItemProperty -Path "NKLK'SOFTWARE WrAdagter Viniformage#A" -Name "Customer D" -Value "customer-Keys" Out-Null New-ItemProperty -Path "NKLK'SOFTWARE WrAdagter Viniformage#A" - Name "Customer D" -Value "customer-Keys" Out-Null New-ItemProperty -Path "NKLK'SOFTWARE WrAdagter Viniformage#A" - Name "IdentityClaims" -Value "http://Schemas.microsoft.com/vs/2008/06/ide
	 Run the Install.ps1 file on ADFS server in administrator mode. Press Y to continue registration.
	Installing assemblies into the GAC Creating Eventugg source Review the above and Press Y continue and register the Authentication Adapter. CTRL-C to exit WARNING: PSDI31- 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\Vyushi\RadiusAuthenticationAdapters net stop adfssrv The Active Directory Federation Service is stopping He Active Directory Federation Service is stopping successfully. PS C:\Program Files\Vyushi\RadiusAuthenticationAdapters net start adfssrv The Active Directory Federation Service is storpten successfully. PS C:\Program Files\Vyushi\RadiusAuthenticationAdapters net start adfssrv The Active Directory Federation Service is storpten 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
	<image/>
	• Go to Authentication methods > Edit Multi Factor Authentication and select miniOrange MFA. Apply the settings.
	Hello there! Need Help? We are right here!

	+1 978 658 9387 🕲 Login 🔍	
mini@range	Products - Solutions - Pricing Resources - Partners Free Trial Contact Us	
	to enable MFA: Azure MFA miniOrange MFA What is multi-factor authentication?	

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.

Xecurify ADFS
Sign in with your organizational account
rassword Sign in
© 2016 Microsoft

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