

ADFS INTEGRATIONS

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security. WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

Limited Warranty - Copyright (c) 2010-2024 RCDevs Security SA. All Rights Reserved.

ADFS integrations

ADFS Federation SSO

Simple Login



Push Login



1. Product Documentation

This document is an installation guide for the OpenOTP Authentication Provider for AD FS 3.0 / 4.0. Hence, the installation or configuration of WebADM, including token registration is not covered in this guide. For installation and usage guides to WebADM refer to the RCDevs WebADM Installation Guide and the RCDevs WebADM Administrator Guide available through the RCDevs' online documentation library.

2. Product Overview

The OpenOTP Authentication Provider for AD FS is a component that integrates the RCDevs OpenOTP one-time password authentication into an Active Directory Federation Services server, adding OpenOTP authentication as a possible MFA option in the AD FS Management tool. RCDevs OpenOTP Authentication Server is a WebApp that is tightly coupled to the RCDevs WebADM application server. The Authentication Provider enables you to use all types of authentication tokens and authentication standards supported by the OpenOTP authentication module. That includes OATH/HOTP, OATH/TOTP, OATH/OCRA, Mobile-OTP, YubiKey, SMSOTP, MailOTP. Software tokens are provided by various publishers and for a variety of platforms including Android and iOS.

3. System Requirements

The OpenOTP Authentication Provider has to be installed on the Windows servers with an AD FS role. Your environment should fulfill the following requirements:

- > Windows 2008 or later.
- > Network access.
- > An instance of WebADM and OpenOTP running in your network.
- > Permanent connection to OpenOTP server's network API.
- > DNS suffix set to match your AD domain.

4. Preliminary Information

Administrative/elevated permissions are necessary on any server to correctly set up and/or change the OpenOTP Authentication Provider's configuration. To correctly set up the provider, please gather the following information. You will need to enter during the installation process:

- > The URI(s)s of the OpenOTP web-service(s) (mandatory).
 - > These URIs are mandatory, due to the client needs to know where the OpenOTP SOAP network API can be reached. They are entered as a comma-separated list. At least one URI is necessary.
- > Your local domain (optional). Needed to force a domain, which is not set as default on the OpenOTP side.
- > A custom login text or tile caption (optional). A text that is displayed on the AD FS login pane.
- > A client ID (optional). An ID to identify this part of your infrastructure to OpenOTP, allowing to modulate OpenOTP's behavior with client policies.
- > A certificate authority (CA) file (optional).
- > A certificate file and the certificate password (optional).
- > A custom settings string (optional).
- > SOAP timeout delay (optional).

Note

OpenOTP plugin for ADFS works for ADFS 3.0 & 4.0 (earlier than Windows server 2008). If you have an older version, you have to update your ADFS Infrastructure.

5. Installation and Configuration

5.1 Installation

In this post, we will assume an existing ADFS infrastructure installed and available. This post will not cover how to set up ADFS. Please refer to the Microsoft documentation and/or the TechNet blog for details about how to install and configure ADFS <u>Microsoft Documentation</u>. For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to WebADM Installation Guide and WebADM Manual to do it.

Note

Before running the MSI file, please make sure your ADFS services are running.

The OpenOTP plugin for ADFS must be installed on every ADFS server. Please download the plugin from the RCDevs Website.

Extract files from the archive on your ADFS server(s) and run the MSI file and click on Next.

🛕 Note

MSI file should be executed with domain admin permissions or local admin permissions. To ensure that you have the required permissions for the installation, you can execute the MSI file through PowerShell executed in "Run As Administrator" mode.



😭 OpenOTP-AP (64 bit) Setup —	Х		
End-User License Agreement	ME		
Please read the following license agreement carefully	lutions		
	_		
RCDEVS OpenOTP-AP LICENSE AGREEMENT	^		
RCDevs OpenOTP Authentication Provider("OpenOTP-AP") Copyright (c) 2010-2019 RCDevs SA, All rights reserved.			
IMPORTANT: READ CAREFULLY: By using, copying or distributing the Software Product you accept all the following terms and conditions of the present OpenID License Agreement("Agreement"). If you do not agree, do not install and use the			
☑ I accept the terms in the License Agreement			
Print Back Next Cano	el		

Consent for End-User License Agreement and click on Next. On the next page, choose your default folder location and click on

Next.

OpenOTP-AP (64 b	it) Setup		R	Devs
Select the way you	want features to be insta	alled.	\sim	security solutions
Click the icons in the	e tree below to <mark>c</mark> hange th	e way features	will be installed.	
	enOTP-AP (64 bit)	Full insta	all	
		This feat hard driv subfeat subfeat hard driv	ture requires 10 ve. It has 1 of 1 ures selected. Ti ures require 417 ve.	KB on your ne OKB on your
Location: C	: \Program Files \RCDevs \(rovider \	OpenOTP Auther	ntication	Browse
Reset	Disk Usage	Back	Next	Cancel

On this page, you have to configure one of your WebADM servers URL. If you are running a WebADM cluster, then both OpenOTP URLs should be automatically retrieve in the Auto mode. If your OpenOTP URL(s) can not be automatically retrieve, then configure URL(s) manually like below :

RCDevs OpenOTP-AP (64 bit) Setup
Configuration 1/5 Setup server URLs, default domain, login text and dient ID
Auto O Manual <u>W</u> ebADM URL:
https://192.168.4.20 Configure
Server URL: (mandatory)
https://192.168.4.20:8443/openotp/
additional Server URL: (optional)
https://192.168.4.21:8443/openotp/
Login Text: (optional)
Work Resources
Loading Text: (optional)
Check your phone if push login is enabled for your account
<u>Client ID: (optional)</u>
ADES 🕤
Back Next Cancel

Click Next. On the next page, every configuration is optional. If you'd like to use a client certificate for enhanced security, please use this next screen to provide the detail. Clicking on the information marks (i) will provide additional help during the installation procedure.

🖟 RCDevs OpenOTP-AP (64 bit) Setup			×
Configuration 2/5			Dove
Setup security using a PKI.			security solutions
The following settings are generally They are applicable only if you have step.	not required. set the Server L	JRL with HTTPS in	the previous
Certificate Authority File: (optional)			
C:\Users\yoann\AppData\Local\Ter	np\1\ca.crt		Ð
Certificate File: (optional)			
		(Ð
Certificate Password: (optional)			
		0	
Confirm Password:			
<u> </u>			
	Back	Next	Cancel
	Back	Next	Cancel

The next page allows you to configure failover with OpenOTP, SOAP request timeout and UPN Mode. Keep the default configuration if you are not sure of what you need. Click on **Next** and **Install**.

Here you may set up a custom settings string for your WebADM and OpenOTP configuration (This setting is deprecated since WebADM client policies). Furthermore, you may change the default SOAP service timeout. If two server URLs are defined in server URL, you can optionally configure a request routing policy (i.e. the server selection policy). There are three policies available:

- > Ordered: The first server is always preferred. When it does not respond, the second server is used.
- > Balanced: The server is chosen randomly for each request. When it does not respond, the other is used.
- Consistent: The server selection depends on the user ID. A request for one specific user is also always routed to the same server. If it does not respond, the other server is used. Click Next when you are done and afterward Install.

RCDevs OpenOTP-AP (64 bit) Setup	×
Configuration 3/5	
Setup preferences for this machine.	RCDEVS security solutions
The following settings are for advanced configurations. You should keep the default values here.	
SOAP <u>T</u> imeout: (Default 30)	
30	0
Server Selection Policy: (optional)	
Ordered (Default)	~ 🛈
Back	Next Cancel

On the next page, you can configure a custom message when users need assistance. For example:



On the next screen, you are prompted to provide the ADFS WAP IP address(es) and the ADFS absolute URI which can be returned by the following PowerShell command:



The checkbox Send the service provider ID as the Client ID to OpenOTP can be used to return to OpenOTP, a unique value per service provider in order to create and match a dedicated client policy for each service provider configured with ADFS. If no unique identifier can be retrieve for a service provider, then the default Client ID value configured in step 1/5 is sent to OpenOTP. This feature is supported over WS-Federation, SAML and OpenID implementations. The ADFS absolute URI is mandatory as soon as you are using SAML and per service provider identifier.



Click **Next** to continue the setup.

伊 OpenOTP-AP (64 bit) Setup	- ×
Ready to install OpenOTP-AP (64 bit)	RCDevs
Click Install to begin the installation. Click Back to revie installation settings. Click Cancel to exit the wizard.	w or change any of your
Back	Install Cancel

Installation is near complete. At the end of the installation of ADFS plugin, you will have a message like below:

mportant	
Please enter your ADFS SPN User	SID
This configuration is needed for ADFS	S 4.0
In order to retrive the SID of your SPN	l user:
1. Open CMD 2. Run the command bellow :	
wmic useraccount where (name='SPN	V_USER' and domain='SPN_DOMAIN') get sid
	Ignore Ok

You need to provide the SID of your ADFS service account. On my side, the command will be:

C:\Users\administrateur>wmic useraccount where (name='svc_adfs' and domain='SUPRCDEVS') get sid SID

S-1-5-21-2556788148-2650686732-506205049-1105

🛕 Important Note

The previous command should be executed through Windows Command Prompt and not with PowerShell.

In case you are using Managed Service Account, the above command will not give you the SID and you might need to use Get-AdServiceAccount command instead on your AD domain controller. In this example the service account is "adfs\$":

PS C:\Users\Administrator.SUPRCDEVS> Get-ADServiceAccount -identity svc_adfs\$
DistinguishedName : CN=svc_adfs,CN=Managed Service Accounts,DC=support,DC=rcdevs,DC=com
Enabled : True
Name : svc_adfs
ObjectClass : msDS-GroupManagedServiceAccount
ObjectGUID : c8cc36ac-4a81-4973-bcba-f23e59f7f50d
SamAccountName : svc_adfs\$
SID : S-1-5-21-2556788148-2650686732-506205049-1105
UserPrincipalName :



🛕 Important Note

The previous command should be executed through PowerShell and not with Windows Command Prompt.

On the next screen, you have to register the OpenOTP service in your ADFS instance. The registration should be done only once per ADFS instance. Click on Yes if it's the first time you install OpenOTP ADFS plugin. For the others, ADFS servers in the same instance, click on No. ADFS services should be running during the registration.



Note

After provider registration, ADFS services will be automatically restarted.



On the next screen, click on **Finish** and the installation is done.



🛕 Plugin installation

Repeat this procedure on every ADFS servers! The registration of the plugin must be done only once.

6. ADFS Configuration for Multi-Factor Authentication

In this documentation, we enable OpenOTP Multi-Factor authentication on the default ADFS login page. This page is disabled by default. Have a look to <u>Technet Microsoft</u> to enable the default ADFS login page. With ADFS 4.0 on <u>Windows Server 2019</u>, the <u>PasswordLess</u> feature is now available. That involves you can login on ADFS by just providing the Username and the OTP. The username provided must match a valid account in the AD.

6.1 Configuration for ADFS 3.0

Now, we will configure the ADFS server(s) to have multi-factor authentication. For this, go on Windows Server Manager, click on Tools and ADFS Management.

2	Server Manager	_ 0 ×
Server N	Manager + AD FS •	Kanage Tools View Help
Dashboard Local Server All Servers	SERVERS All servers 1 total	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers
AD DS	Server Name IPv4 Address Manageability	AD FS Management
🐴 AD FS	WIN-RDP 192 168 3 59 Online - Performance counters not	ADSI Edit
DNS DNS	THE REF TELEVISION OF THE PEROTHER COUNCES FOR	Computer Management

9	AD FS
File Action View Window Help Image: State	
 AD FS Service Trust Relationships Authentication Policies 	AD FS Overview AD FS provides single-sign-on (SSO) access for client computers. Learn More Configuring Trust Relationships Configuring Authentication Policies Troubleshooting AD FS AD FS Help

On the ADFS Management page, right click on Authentication Policies and click on Edit Global Multi-factor Authentication...

Ŵ	AD FS
File Action View Window	Help
🧇 🏟 🖄 📰 🛿 🖬	
AD FS	Authentication Policies
Service Trust Relationships	Authentication Policies Overview
Authentication Policies	
E	dit Global Primary Authentication ation and multifactor authentication settings globally
Ed	dit Global Multi-factor Authentication
Vi	iew Window from Here
R	efresh
н	łelp
	Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure global and custom primary authentication settings.

On the next page, you will find a new option available in the additional authentication methods named "RCDevs OpenOTP Authentication Provider". Check the box of this option and click on Ok.

Edit Global Authentication Policy	x		
Primary Multi-factor			
Configure multi-factor authentication (MFA) settings.			
Users/Groups			
MFA is required for the following users and groups:			
AD\Domain Admins	<u>A</u> dd		
AD\Domain Users	Remove		
During			
Devices MEA is required for the following devices:			
Unregistered devices			
Registered devices			
Locations			
MFA is required when accessing applications from the following locations:			
Extranet			
Intranet			
Select additional authentication methods. You must select at least one of the following methods to enable MFA:			
Certificate Authentication			
RCDevs OpenOTP Authentication Provider			
What is multi-factor authentication?			
OK Cancel	Apply		

Your ADFS server is now configured with OpenOTP for ADFS plugin. In order to use it, your relaying party must be configured for multi-factor authentication.

OpenOTP User Activation

All accounts where authentication will be handled by OpenOTP must be activated. Look the following <u>How-To to activate an</u> account.

6.2 Configuration for ADFS 4.0

Now, we will configure the ADFS server(s) to have multi-factor authentication. For this, go on Windows Server Manager, click on Tools and ADFS Management.

kanager 🔤			– 🗆 ×
Server M	anager • Dashbo	ard 🛛 😴 I 🚩 Manage 🔽	ols View Help
 Dashboard Local Server All Servers AD CS AD DS AD FS DNS File and Storage Services ▷ 	WELCOME TO SERVER M QUICK START WHAT'S NEW LEARN MORE ROLES AND SERVER GR Roles: 5 Server groups: 1	Configure this local serve Configure this local serve Add roles and features Add other servers to manag Create a server group Coups Servers total: 1	Active Directory Administ Active Directory Domain Active Directory Domain Active Directory Module Active Directory Sites an Active Directory Users an AD FS Management ADSI Edit Certification Authority Component Services Computer Management Defragment and Optimi Disk Cleanup DNS Event Viewer Group Policy Management iSCSI Initiator Local Security Policy Microsoft Azure Services ODBC Data Sources (32-

On the ADFS Management page, under Service right click on Authentication Methods and click on

Edit Multi-factor Authentication Methods.

AD FS	Authentication Methods		Actions
Service Attribute Stores Authentication Mark Certificates Claim Descripti Device Registra Endpoints Scope Descripti Web Applicatio Access Control Pol Relying Party Trust: Claims Provider Trusts	Authentication Methods Ove Edit Primary Authentication Methods Edit Multi-factor Authentication Methods View > New Window from Here Refresh Help Extranet Forms Authentic	rview vds and multifactor authentication vds ring to access applications that use AD w to configure settings for primary ration. Edt	Authentication Methods Edit Primary Authentication Methods Edit Multi-factor Authentication Meth View New Window from Here Image: Refresh Help
Application Groups	Microsoft Pass Intranet Forms Authenti Windows Auth Microsoft Pass Multi-factor Authentication M You can use options below to configure setting Authentication Methods Not configured	ont Authentication cation, mitication. ont Authentication ethods gs for multi-factor authentication methods. Edit	

On the next page, you will find a new option available in the additional authentication methods named

RCDevs OpenOTP Authentication Provider. Check the box of this option if it's not already checked and click Apply.

nim an -	Multifactor							
nmary								
Select to enal	additional auth ble MFA:	nentication meth	lods. You r	nust select a	at least o	ne of the fo	ollowing m	lethods
Cer	rtificate Auther	ntication						
	ure MFA	TP Authenticativ	on Provider					
	Devs Openo I		ni Fiovidei					
What is	s multi-factor a	uthentication?						

Relaying parties configured for MFA authentication can now use OpenOTP for ADFS plugin.

6.3 Windows Hello For Business

In order to be able to use OpenOTP authentication for Windows Hello for Business devices registrations, you need to execute the following command through PowerShell on your primary ADFS server :

Set-MsolDomainFederationSettings -DomainName <DOMAIN NAME> -SupportsMfa \$true

Adapt the command with your domain name. On my side it is :

Set-MsolDomainFederationSettings -DomainName SUPRCDEVS -SupportsMfa \$true

Windows Server 2019 brings some changes to ADFS. Two of these are especially interesting for use cases with OpenOTP:

- External Authentication Providers as Primary authentication method : OpenOTP can now be used as the first authentication factor, allowing you to not expose AD password as the first factor. Furthermore, since OpenOTP ADFS plugin can validate both AD password and a 2nd factor, it can be configured as primary authentication provider.
- > Password Authentication as additional Authentication : You can optionally change the default authentication flow from surname + password followed by OTP, to username + OTP followed by password. In that scenario, the second factor is the AD password. This is especially useful for preventing the AD account from being locked due to a brute force attack on the password of a leaked username.

6.4.1 ADFS OpenOTP Plugin as Primary Authentication Method

To configure ADFS OpenOTP plugin as primary authentication method, open the ADFS Management console, expand Service folder and click on Authentication methods, configure ADFS Authentications Methods > Primary Authentication Methods > Edit and enable the setting Allow additionnal authentication provider as primary :

Edit Authentication Methods	×
Primary Additional	
Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in. If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication. Learn more about Azure MFA (Multi-Factor Authentication).	
Extranet	
Forms Authentication Certificate Authentication Device Authentication Microsoft Passport Authentication	
Intranet	
Forms Authentication Windows Authentication Certificate Authentication Device Authentication Microsoft Passport Authentication	
Allow additional authentication providers as primary	
Azure MFA authentication methods will not be available until an Azure Active Directory tenant is configured. Learn More	
To use device authentication as a primary authentication method, you need to configure device registration.	
OK Cancel Apply	

Click Ok button and edit again Primary Authentication Methods. As ADFS OpenOTP plugin is already installed, you should now see RCDevs OpenOTP Authentication Provider available.

elect	authentication methods. By selecting more than one authentic	ation method, you enable
sers to	have a choice of what method to authenticate with at sign in	
lister and	and a difficult and the anti-entire models of its and sites of the difficult its and the second sites of the second site of the second sites of the second site of the second sites of the	an Alman al a Cau dh
uthent	ated windows authentication method is specified, it appears a tication method on browsers that support Integrated Windows	authentication.
earn r	nore about Azure MFA (Multi-Factor Authentication).	
Extran	let	
F	orms Authentication	
	ertificate Authentication	
	Device Authentication	
	licrosoft Passport Authentication	
L	CDevs OpenOTP Authentication Provider	
Intran	et	
٧N	Vindows Authentication	~
	ertificate Authentication	
	Device Authentication	
	ficrosoft Passport Authentication	
L	CDevs OpenOTP Authentication Provider	×.
	and a second	
Allo	w additional authentication providers as primary	
	zure MEA authentication methods will not be available until	an Azure Active
U D	lirectory tenant is configured. Learn More	diff Editor Houro
A T	o use device authentication as a primary authentication metho	od, you need to configure
d	evice registration.	

Enable it for access you want to protect with OpenOTP :



You can now try to perform a login with PasswordLess authentication.

P Note

The following screenshots are coming from another instance of ADFS. Don't take into account the ADFS URL and UPN value use for that login example

YORCDevs Sign in administrateur@yorcdevs.com	
Next	

Click Next button:

OpenOTP Authentication Provid: x + YORCDevs VORCDevs Work Resources Continue Retry Image: Retry			YO_ADFS19	P	our relâcher votre souris, appuyez sur : Control
OpenOTP Authentication Provid: x + □	II 🖪	∢ ↔ 🖸 🙆 🔍	\$ A	0	
	OpenOTP	Authentication Provid × +			- 0 ×
VORCDevs Work Resources Continue Retry	← → C	yoadfs19.yorcdevs.com/a	dfs/ls/idpinitiatedsignon?client-request-id=7a888	aeb-1226-4f01-0200-008	0010000f9 🕁 😁 :
			YORCDevs Work Resources Continue Retry		
		6			
© 2018 Micro					© 2018 Microso
電 ク 財 🩋 🔚 💺 🤽 👩 🛛 🛛 ヘ 空 da ERG 317 PM に	- 0	H; 🛋 🖿 📕	Q, 👩		ヘ 記 de ENG 3:17 PM FR 4/3/2020 □

Click **Continue** button and OpenOTP plugin will call OpenOTP server for authentication :

II E	→ ↔ 🖬	0	4 4		0			
OpenOTP	Authentication Provid	× +					-	o ×
 	🗑 yoadfs19.yon	cdevs.com/a	dfs/ls/idpinitiated	dsignon?client-request-id=7a888aeb	-1226-4f01-0200-0	0080010000f9	\$	0 :
			YORCDO Work Enter your T OTP Aut	evs Resources TOKEN password thentication we Password Continue Retry				
							6 Z	018 Microso
م I	H 健 🖡	-	0, 🌍			^ 틷 4	ENG 3:18	
							FK 4/3/2	020

Provide the OTP and you are logged in.

6.4.2 LDAP Password as Additional Authentication Method

To configure LDAP password as second factor, open the ADFS Management console, expand Service folder and click on

Authentication methods, configure

ADFS Authentications Methods > Additional Authentication Methods > Edit and enable the setting Forms Authentication :



Apply the configuration.

Now, all policies requiring additional factor or MFA will ask for User LDAP password as 2nd factor.

After OpenOTP success login, I'm now prompted for the LDAP password of my account :

				YO_AD	FS19	Pour relâch	er votre souris, app	ouyez sur : Co	ntrol-
11 🖪	2 00 0		0 🔮 4			Ø			
Sign In		× +					-	. 0	×
< → C	₩ voadfs19.v	vorcdevs.com	m/adfs/ls/idpinitiated	lsianon?client-reau	est-id=a9a71021-7090-4a5	9-2200-0080010000	fd 😽	* 0	:
			YORCDe For security to verify yo ← admir 	evs reasons, we requi ur account iistrateur@yorcde	re additional information evs.com I Sign in				
								100 00 10 L L	rrosof
								19 2018 Mi	0.0301

I provide my password and then I'm connected :

11 25	3 ↔ 3 0	4 4	0	
Sign In	× +			- 0 ×
← → C	i yoadfs19.yorcdevs.com/ad	fs/ls/idpinitiatedsignon?client-request-id=a	a9a71021-7090-4a59-2200-008001	0000fd 🕶 🖈 😝 :
		YORCDevs You are signed in. (DP) Sign in to one of the following site: (DP) Sign in Sign out from all the sites that you Sign out from this site. Sign Out	s:	
				© 2018 Microso

6.5 Voice Biometric Authentication through Web Browser

In order to use Voice authentication with ADFS and to provide your VOICE password through the microphone of your computer/laptop and your Web browser, ADFS needs to support some additional HTTP headers (worker-src). By default, we advise to configure the following through PowerShell :

Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue "default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:; worker-src blob:"

You may have a custom ADFS configuration where the HTTP headers values configured are different from the ones previously described. The important part is regarding 'worker-src blob:' which must be added to your existing configuration.

Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue "EXISTING CONFIG"; worker-src blob:"

After enabling it, you can use VOICE authentication through ADFS. You will be prompted for VOICE password as below :

Work Resou	rces
Vocal OTP Authentic	ation
R	lecord
Enter your VOICE passwo Remaining t	ord ime : 81 seconds
Retry	Continue

Click on **Record** button, the microphone is triggered and then provide your VOICE password, and you are logged in. More information on VOICE authentication and registration are available on the following documentation

7. Uninstalling the OpenOTP Authentication Provider

If you ever decide to uninstall the provider, simply re-run the installer and choose **Remove**.

Select th	e operation you v	vish to perforr	n.	ΠĽ	security solution
	Change	r i			
	Lets you change	the way feat	ures are installed.		
	Repair				
	Repairs errors in files, shortcuts,	n the most rec and registry e	ent installation by t ntries.	fixing missing and	d corrupt
	Remove]			
	Removes Open0	DTP-AP (64 bit	:) from your compu	ter.	

8. Troubleshooting

To pinpoint a problem in your ADFS for OpenOTP plugin setup, you can start with the Windows Event viewer: "Applications and Services Logs", enter in "AD FS" folder and then "Admin" logs. Also look at /opt/webadm/logs/webadm.log.

If the provider registration failed, you can manually register OpenOTP Authentication provider by executing the following command through PowerShell. You may need to adjust the version number and the PublicKeyToken of OpenOTP plugin for ADFS.

The command for the registration looks like :

Register-AdfsAuthenticationProvider -TypeName "AuthenticationProvider.AuthenticationAdapter, OpenOTPAuthenticationProvider, version=x.x.x.x, culture=neutral, publicKeyToken=xxxxxxxxx, processorArchitecture=AMD64" -Name "OpenOTPAuthenticationProvider"

In order to figure out the values for PublicKeyToken and version, you can execute the following command :

([system.reflection.assembly]::loadfile("C:\Windows\Microsoft.NET\assembly\GAC_64\OpenOTPAuthentication

Which return :

OpenOTPAuthenticationProvider, Version=1.0.12.0, Culture=neutral, PublicKeyToken=b04a046270ba95d2

🛕 Note

The name folder containing the OpenOTPAuthenticationProvider.dll may change according to the version of the ADFS plugin. Please adapt the path if required. The path below is for 1.0.12.0 version of ADFS plugin.

The registration command is then:

Register-AdfsAuthenticationProvider -TypeName "AuthenticationProvider.AuthenticationAdapter, OpenOTPAuthenticationProvider, version=1.0.12.0, culture=neutral, publicKeyToken=b04a046270ba95d2, processorArchitecture=AMD64" -Name "OpenOTPAuthenticationProvider"

9. Video Demonstration



This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved