



ADFS & OPENOTP

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.

Copyright (c) 2010-2017 RCDevs SA. All rights reserved.

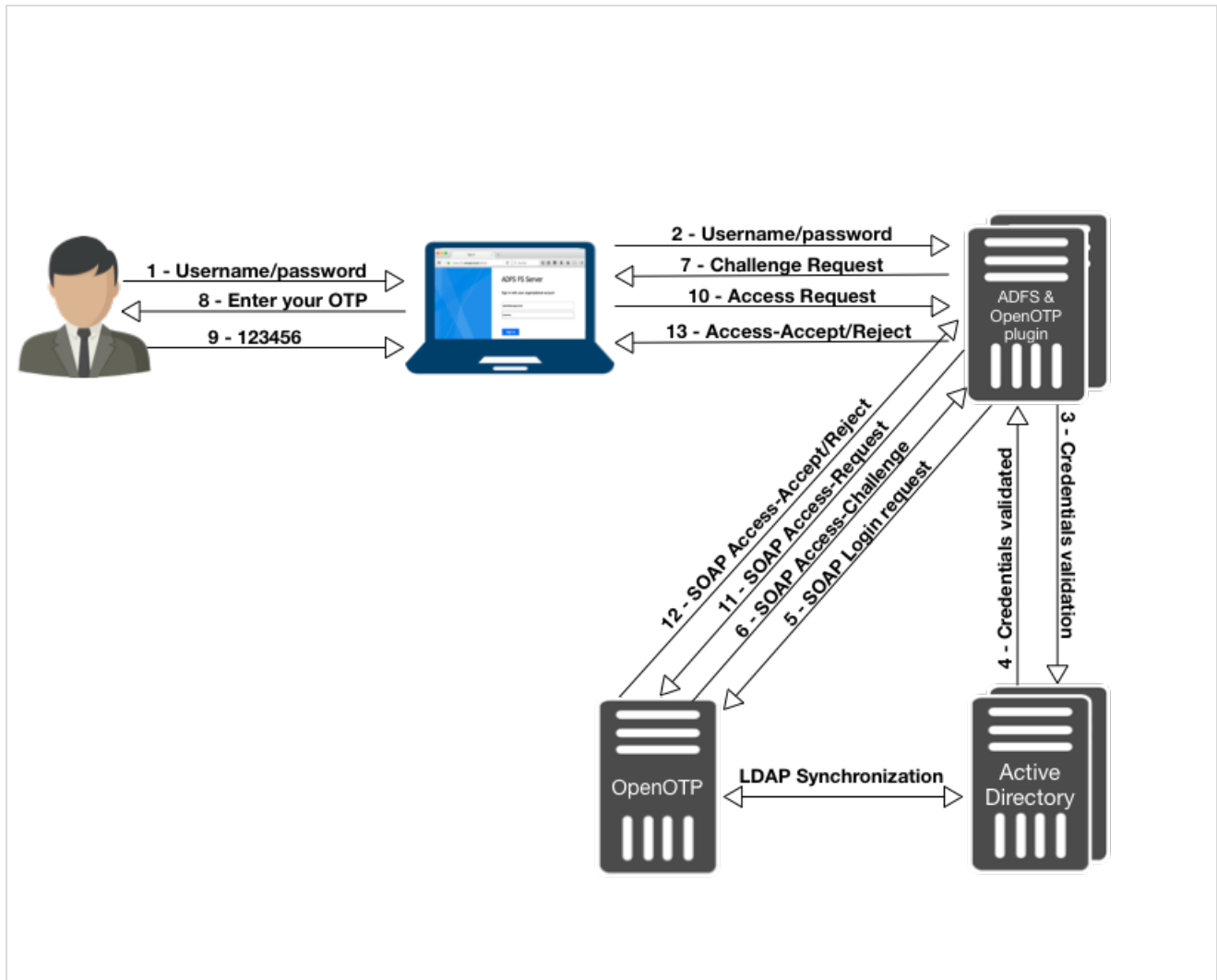
<http://www.rcdevs.com>

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

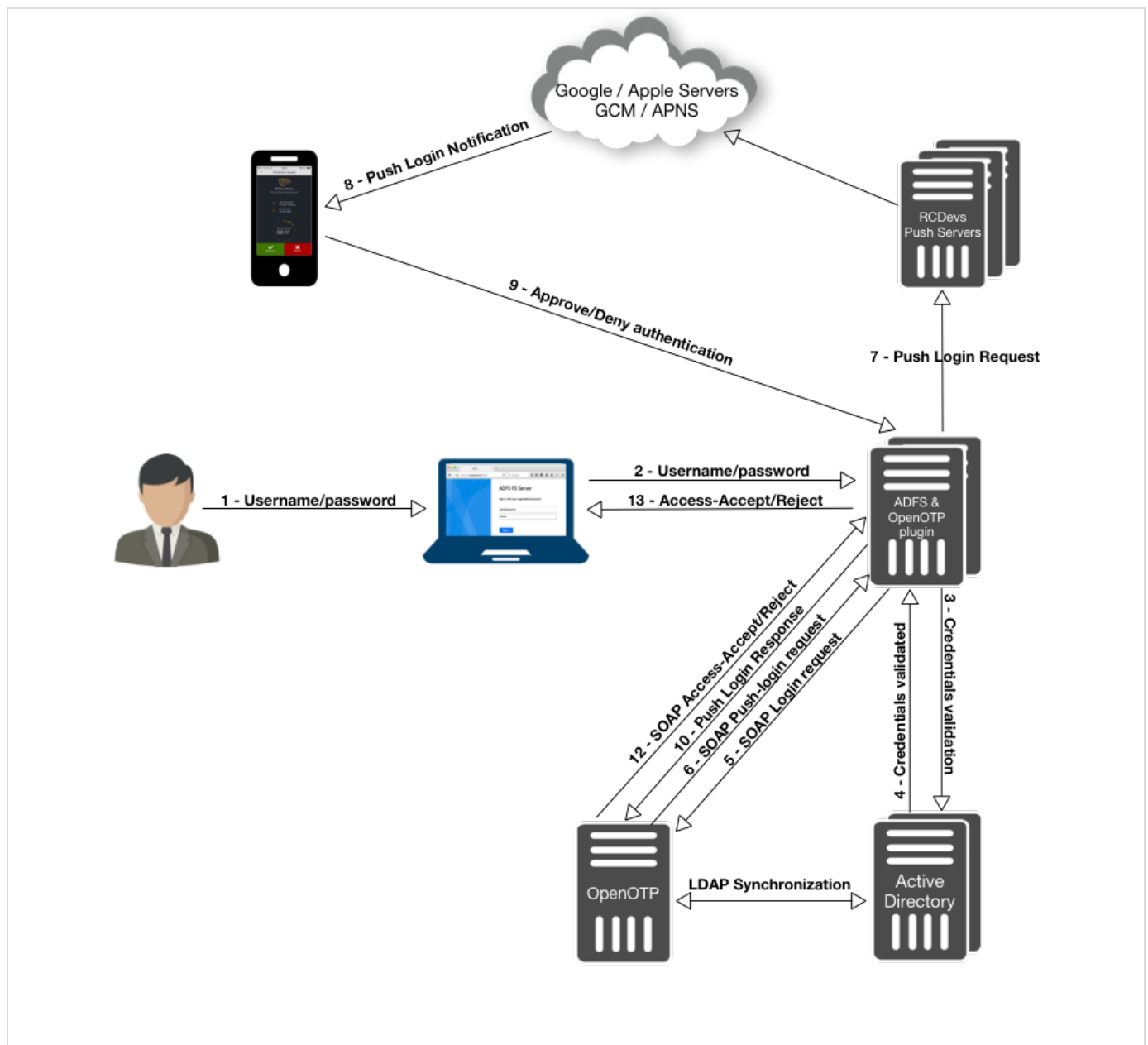
Limited Warranty

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

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 setup the provider, please gather the following information. You will need to enter during the installation process:

- › The URI(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 setup ADFS.

Please refer to the Microsoft documentation and/or the TechNet blog for details about how to install and configure ADFS [Microsoft | TechNet](#). 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

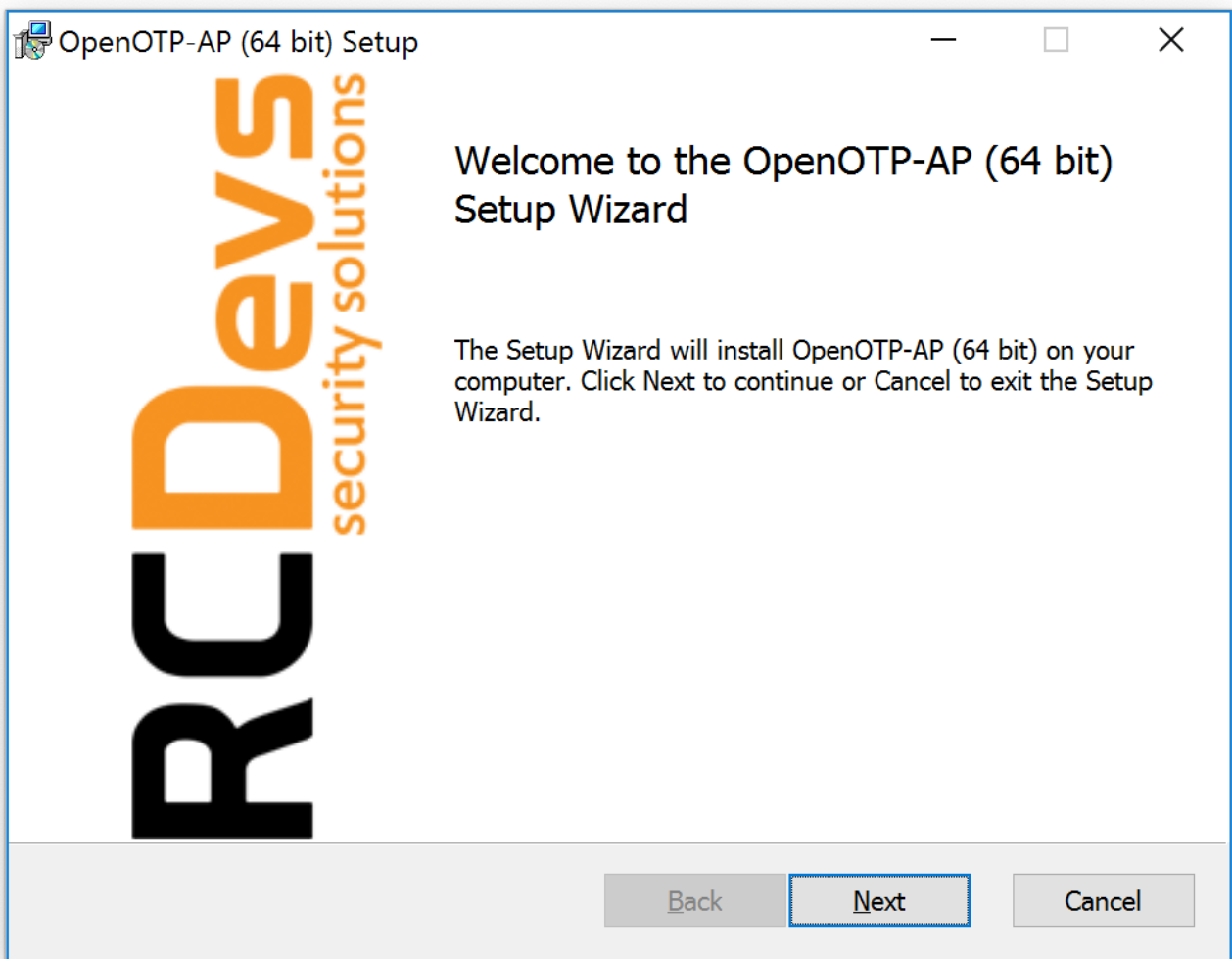
Before running the MSI file, please stop your ADFS services.

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**.

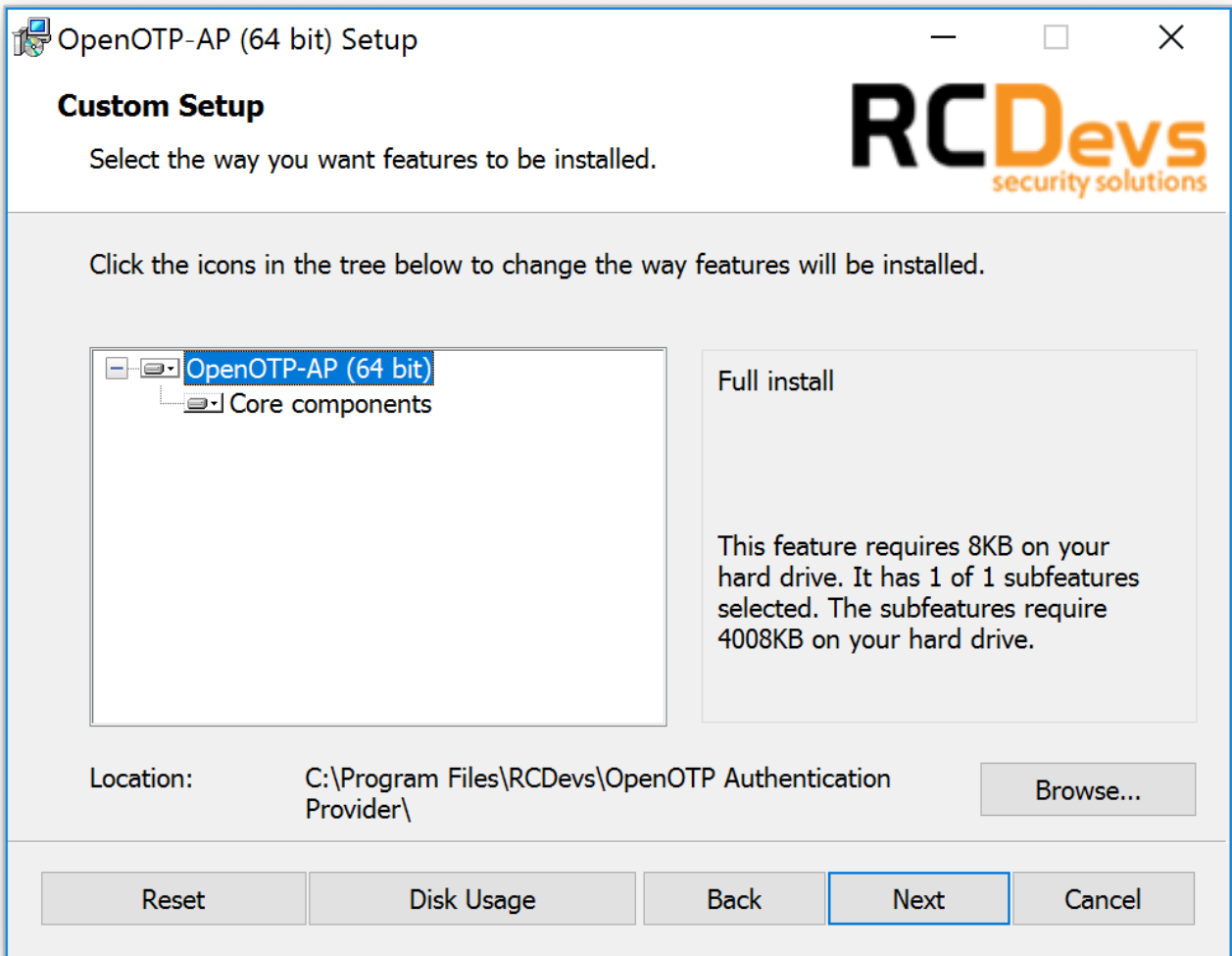
Note

MSI file should be run with domain admin rights. To be sure that you have the good permissions, you can execute the MSI file through PowerShell in “Run As Administrator” mode.






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




On this page, you have to configure the OpenOTP SOAP URL(s). Your WebADM SOAP endpoint should be:

<https://your-web-adm-ip-address-or-dns-name:8443/openotp/>. You can also configure a message for the end-user login page. Click on **Next**.


 OpenOTP-AP (64 bit) Setup

Configuration 1/4


Setup server URLs, default domain, login text and client ID




Server URL: (mandatory)




Additional Server URL: (optional)



Client ID: (optional)



Login Text: (optional)




Back

Next

Cancel

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 question marks (?) will provide additional help during the installation procedure.

 OpenOTP-AP (64 bit) Setup

✕

RCDevs
security solutions

Configuration 2/4
Setup security using a PKI.

The following settings are generally not required.
They are applicable only if you have set the Server URL with HTTPS in the previous step.

Certificate Authority File: (optional)

?

Certificate File: (optional)

?

Certificate Password: (optional)

?

Confirm Password:

Back

Next

Cancel

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



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. 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 afterwards **Install**.

Configuration 4/4

Setup preferences for this machine.



The following settings are for advanced configurations.
You should keep the default values here.

Settings String: (optional)



SOAP Timeout: (Default 20)



Server Selection Policy: (optional)



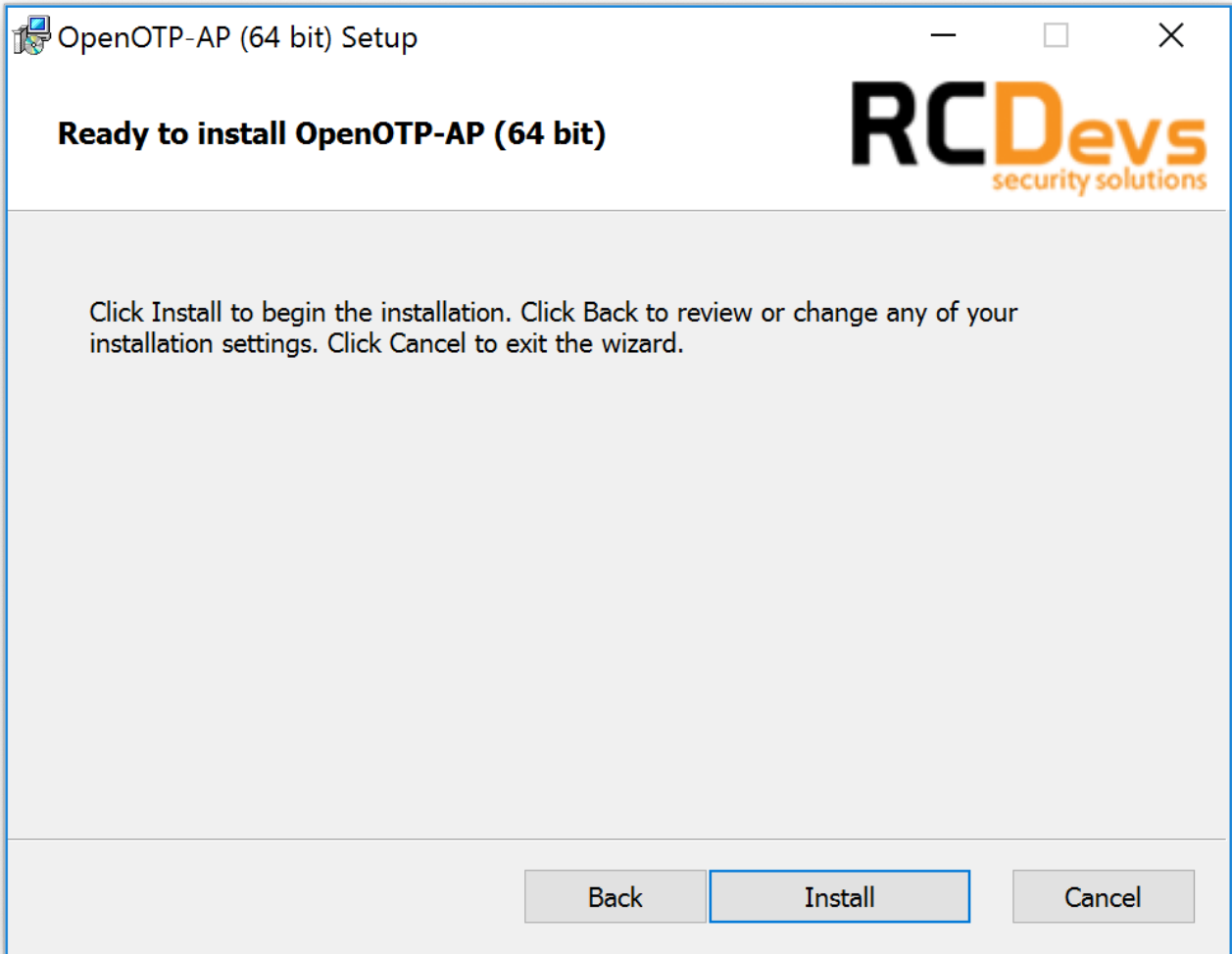
UPN Mode: (optional)



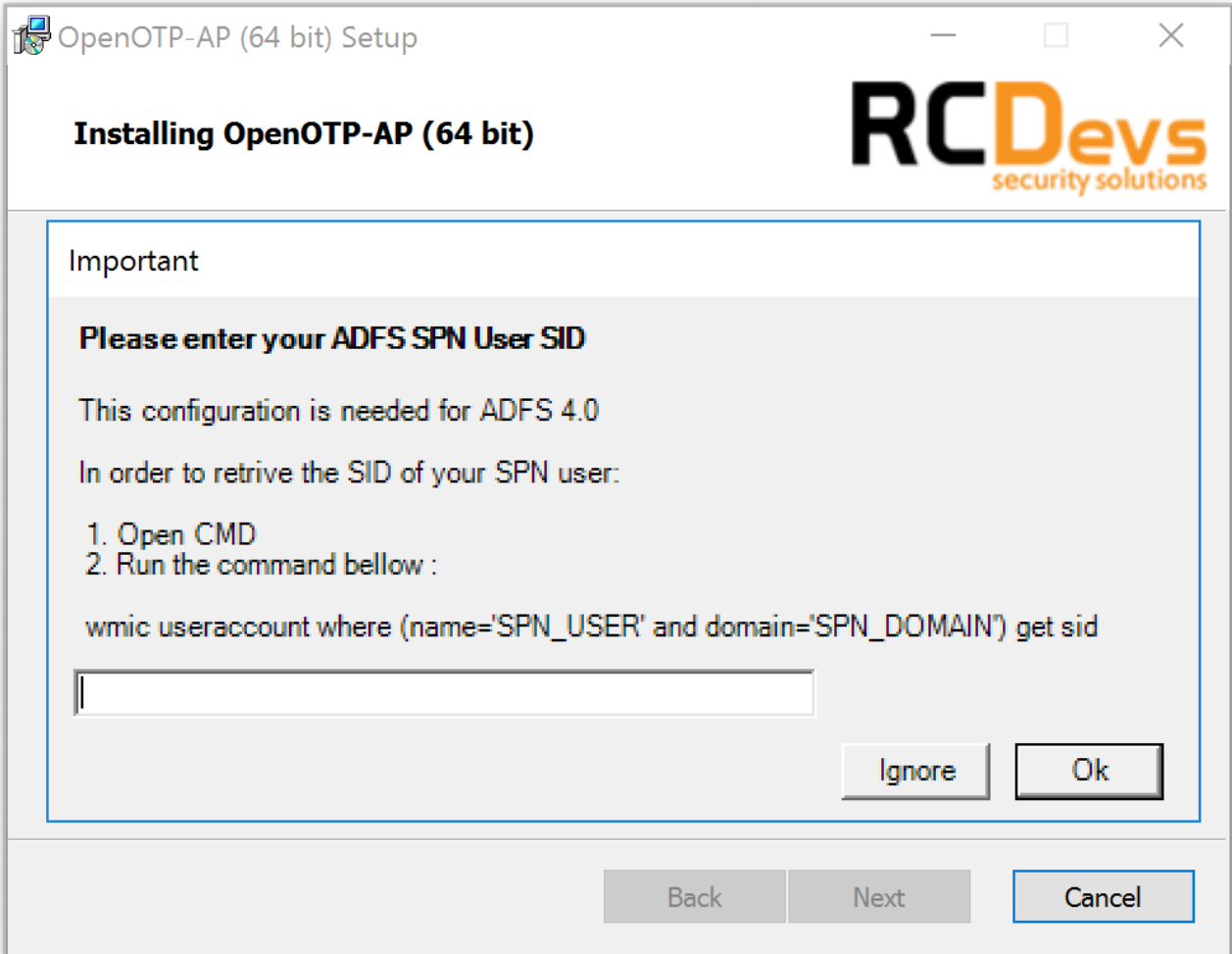
Back

Next

Cancel

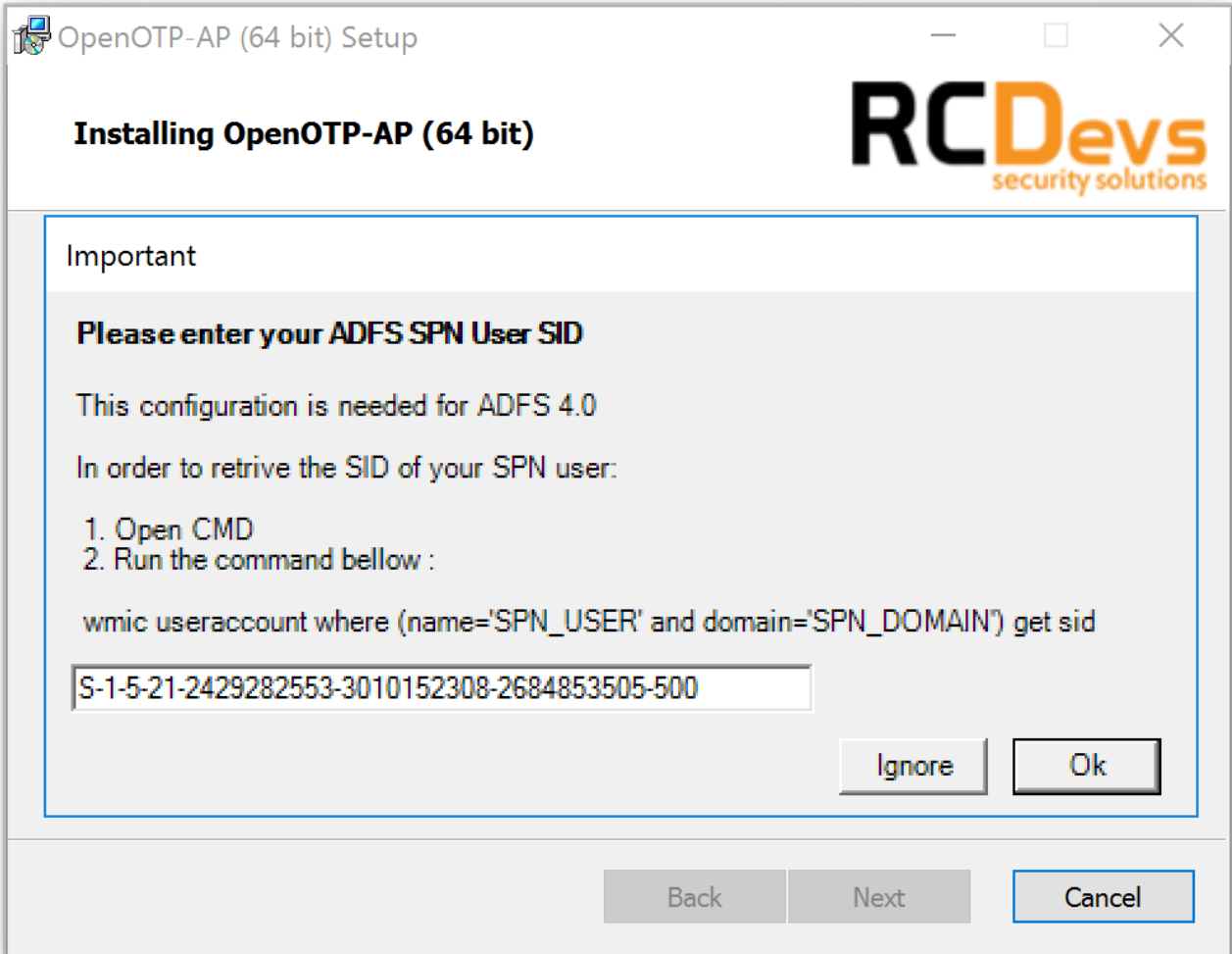


Installation is near complete. At the end of the installation of ADFS plugin, you will have a message like below:



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

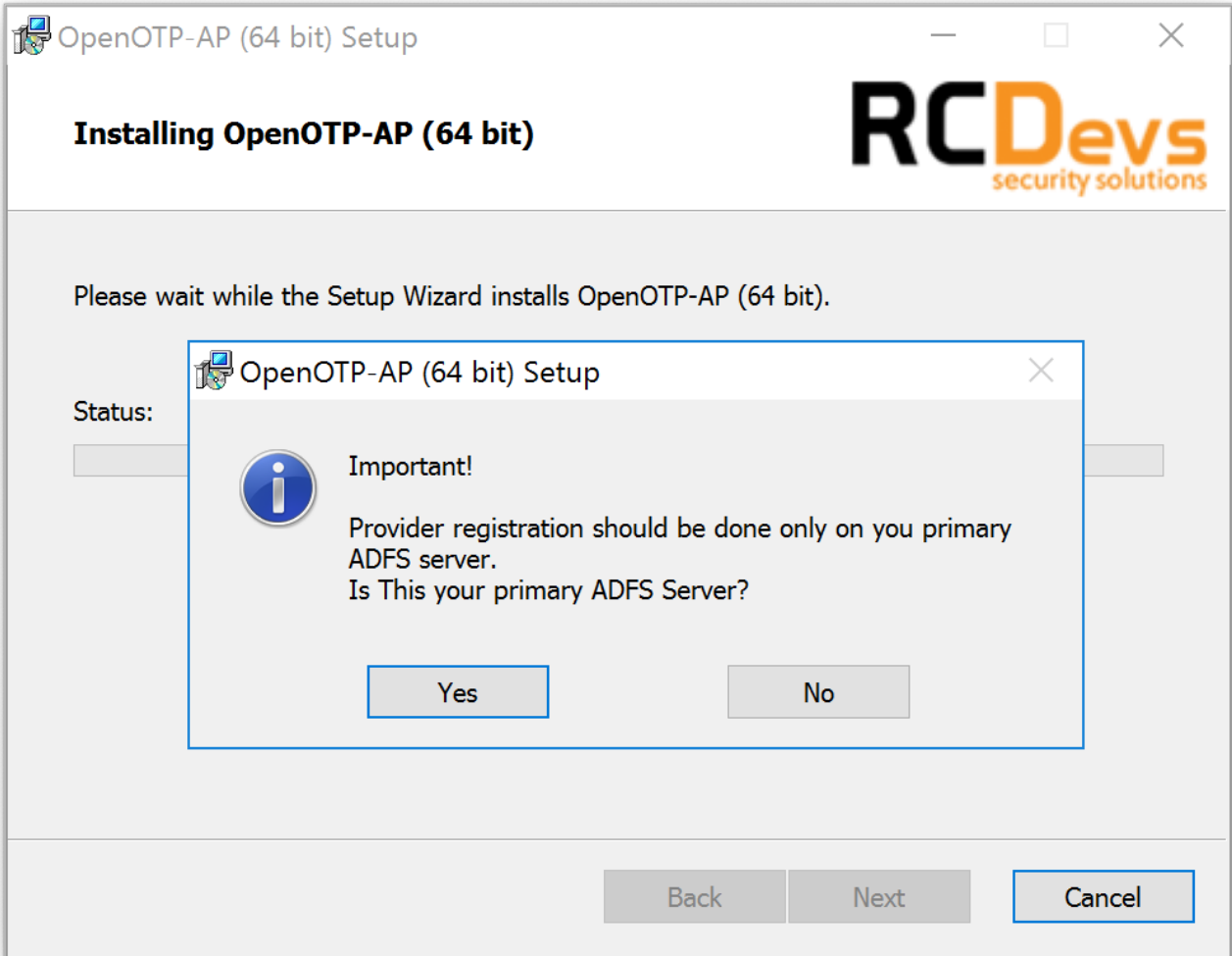
```
C:\Users\administrateur>wmic useraccount where (name='administrator' and  
domain='RCDEVS') get sid  
SID  
S-1-5-21-2429282553-3010152308-2684853505-500
```



Important Note

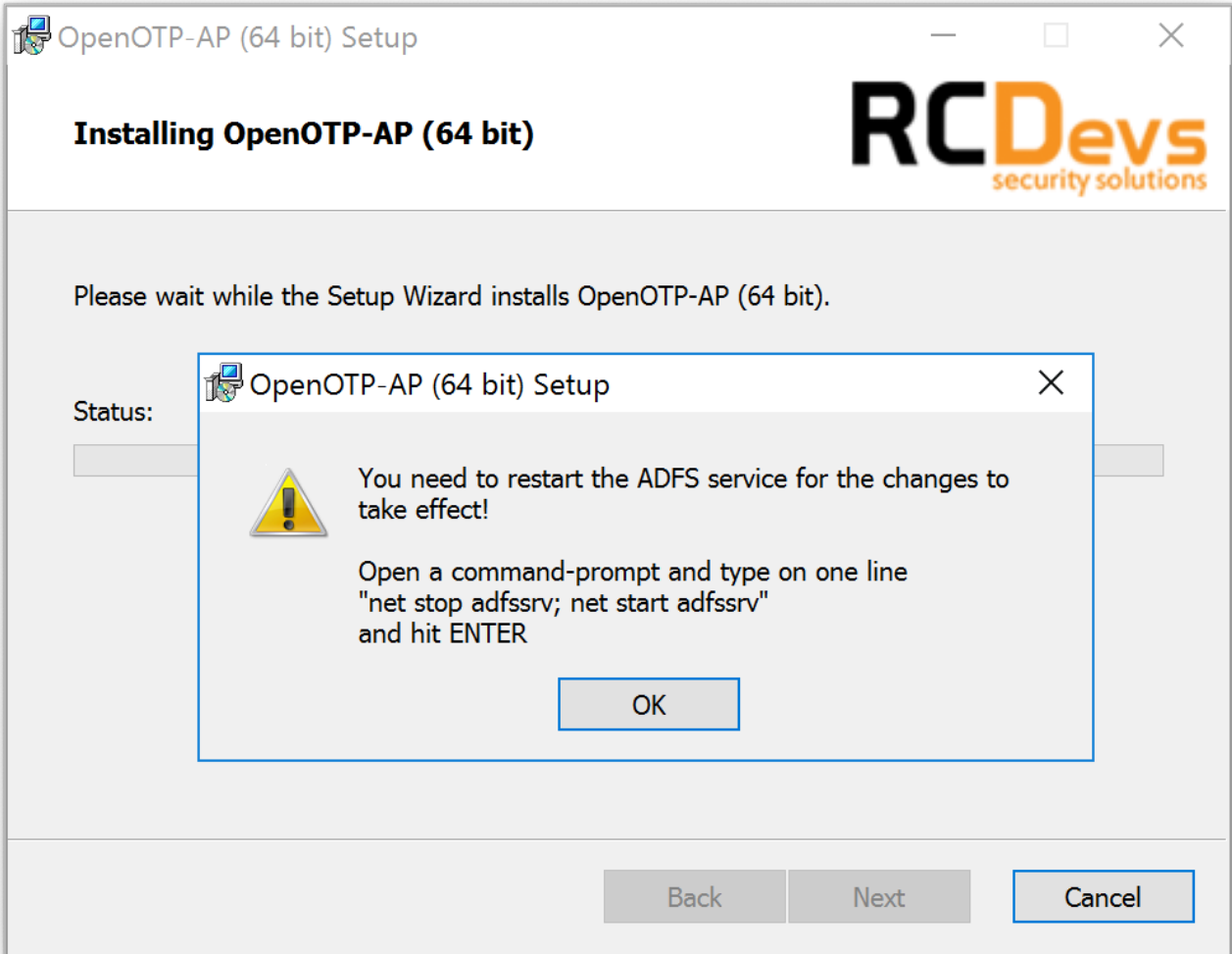
The previous command should be executed through Windows Command Prompt and not with Powershell.

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.

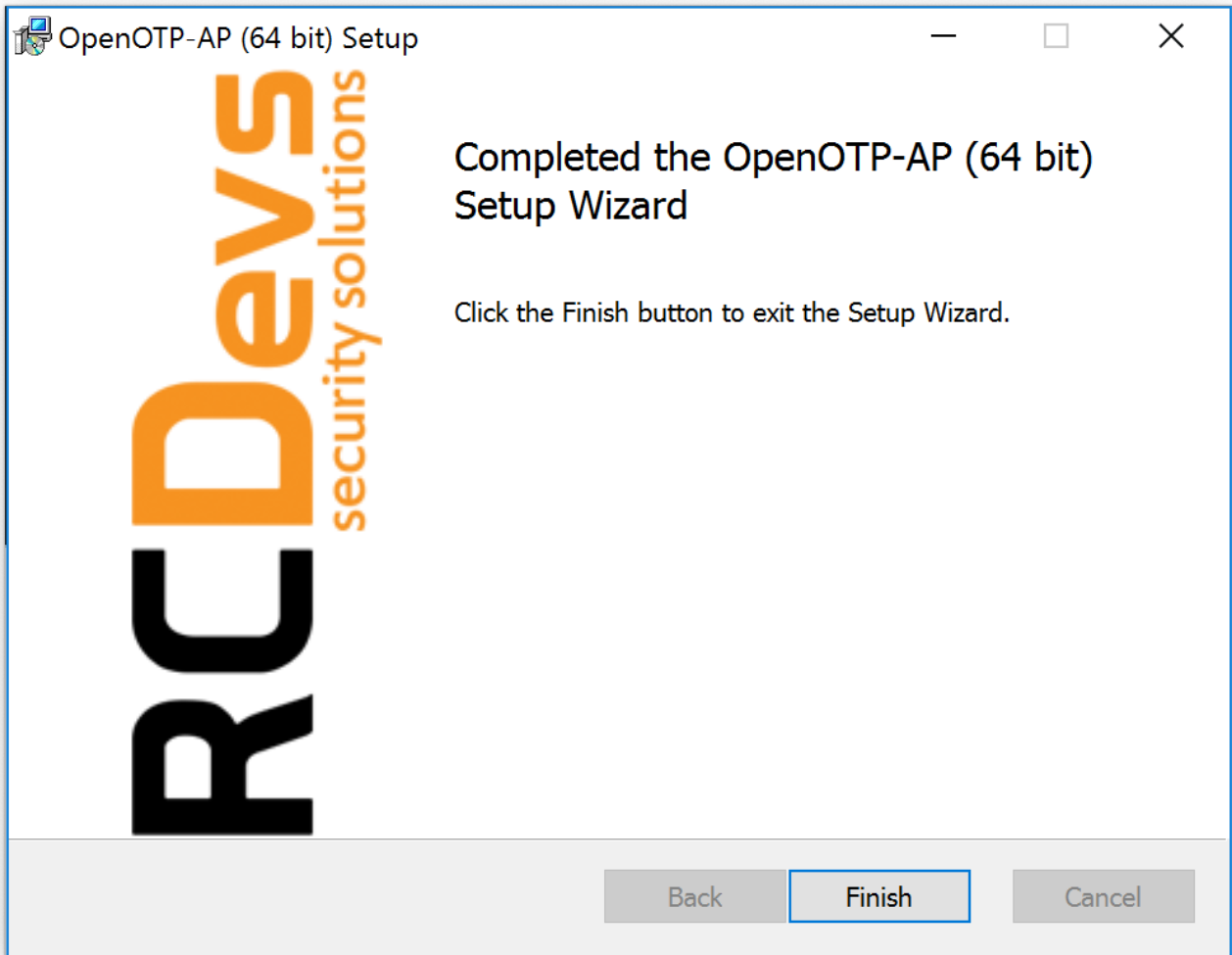


Note

Don't forgot to restart ADFS services when your installation is done.



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



⚠ Plugin installation

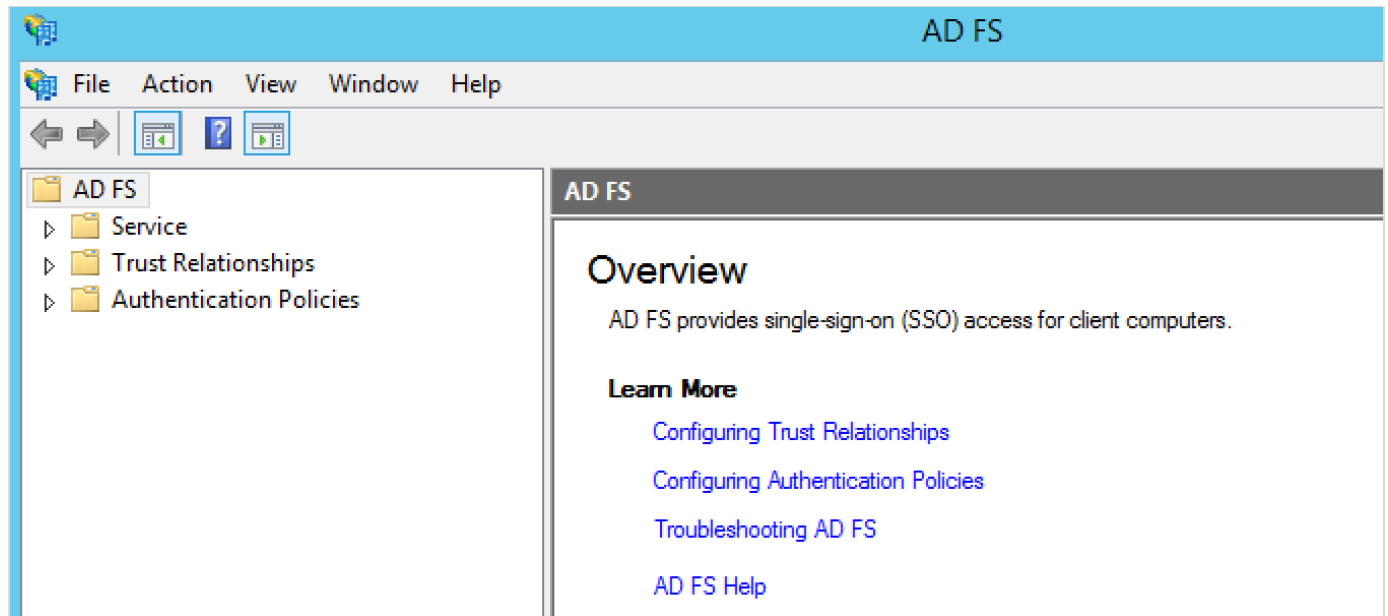
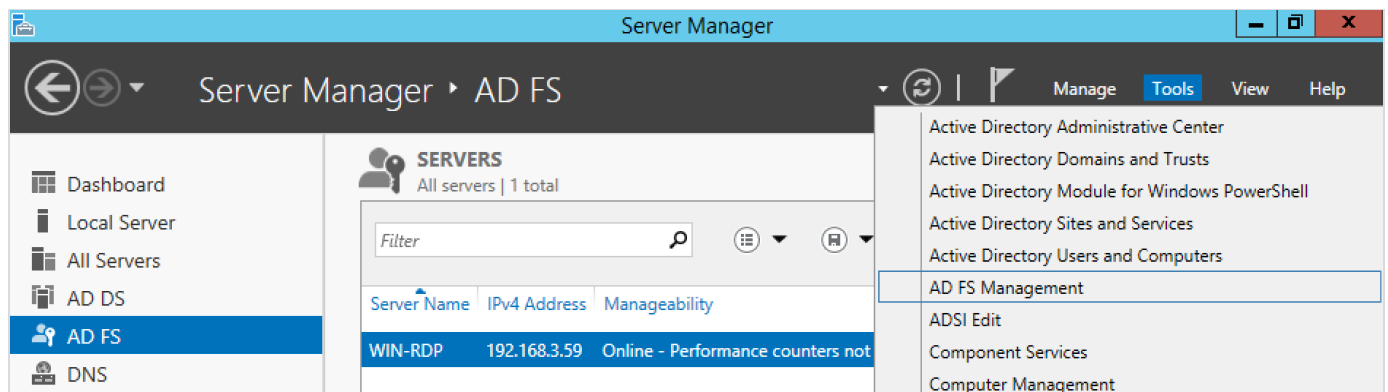
Repeat this procedure on every ADFS servers!

6. ADFS Configuration for Multi-Factor Authentication

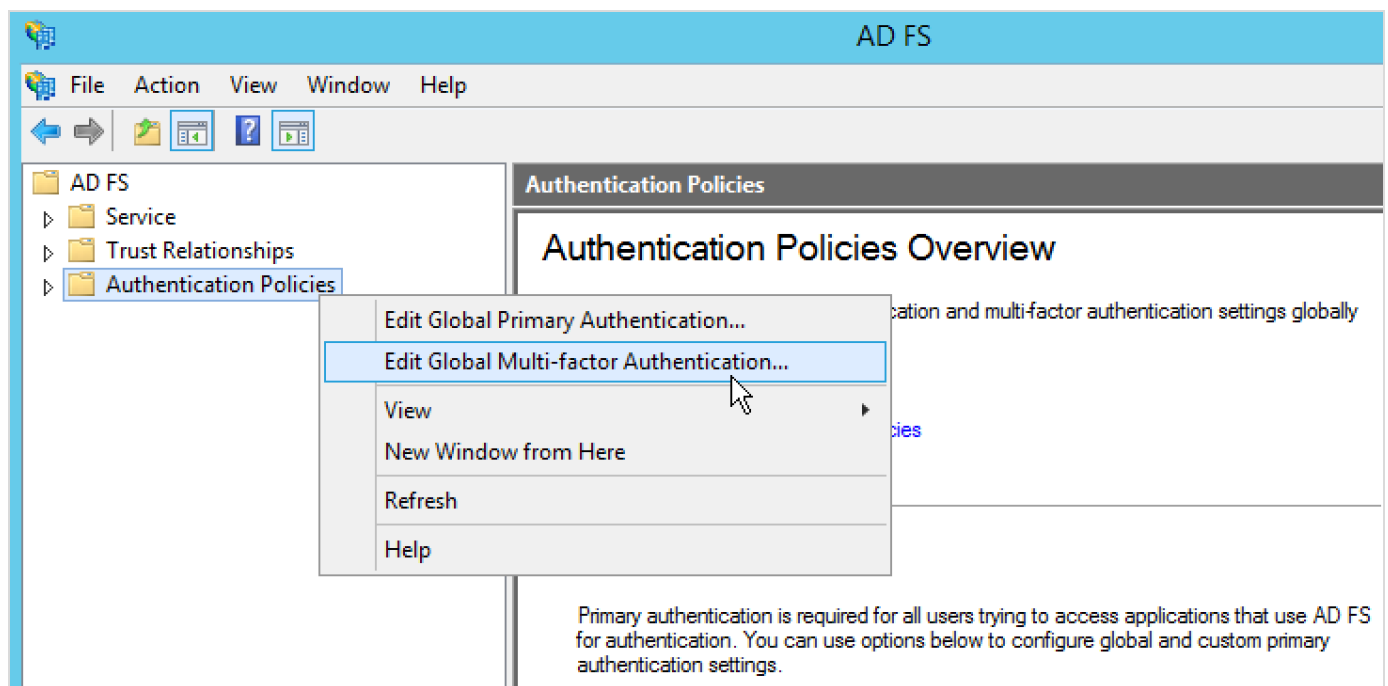
In this documentation, we enable OpenOTP Multi-Factor authentication on the default ADFS login page. This page is disabled by default. Have a look to [Technet Microsoft](#) to enable the ADFS login page.

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.



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



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

Primary Multi-factor

Configure multi-factor authentication (MFA) settings.

Users/Groups
MFA is required for the following users and groups:

AD\Domain Admins
AD\Domain Users

Add...
Remove

Devices
MFA is required for the following devices:

☐ Unregistered devices
☐ Registered devices

Locations
MFA is required when accessing applications from the following locations:

☐ Extranet
☐ Intranet

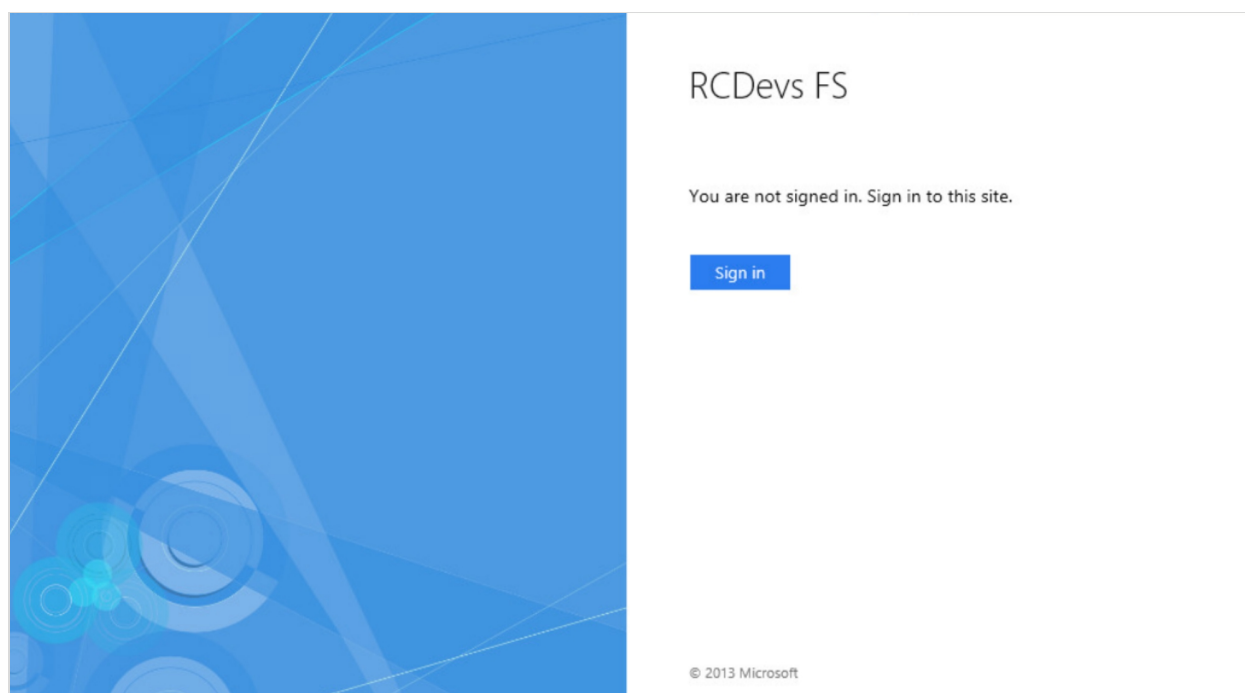
Select additional authentication methods. You must select at least one of the following methods to enable MFA:

☐ Certificate Authentication
☒ RCDevs OpenOTP Authentication Provider

[What is multi-factor authentication?](#)

OK Cancel Apply

Your ADFS server is now configured with OpenOTP. You can go on your ADFS login page:



Click on **Sign in** button, enter your credentials and click on **Sign in**.

Connexion

Non sécurisé | <https://win-rdp.ad.rcdevs.com/adfs/ls/idpinitiatedsignon>

WIN-RDP.ad.rcdevs.com

Connexion avec votre compte professionnel

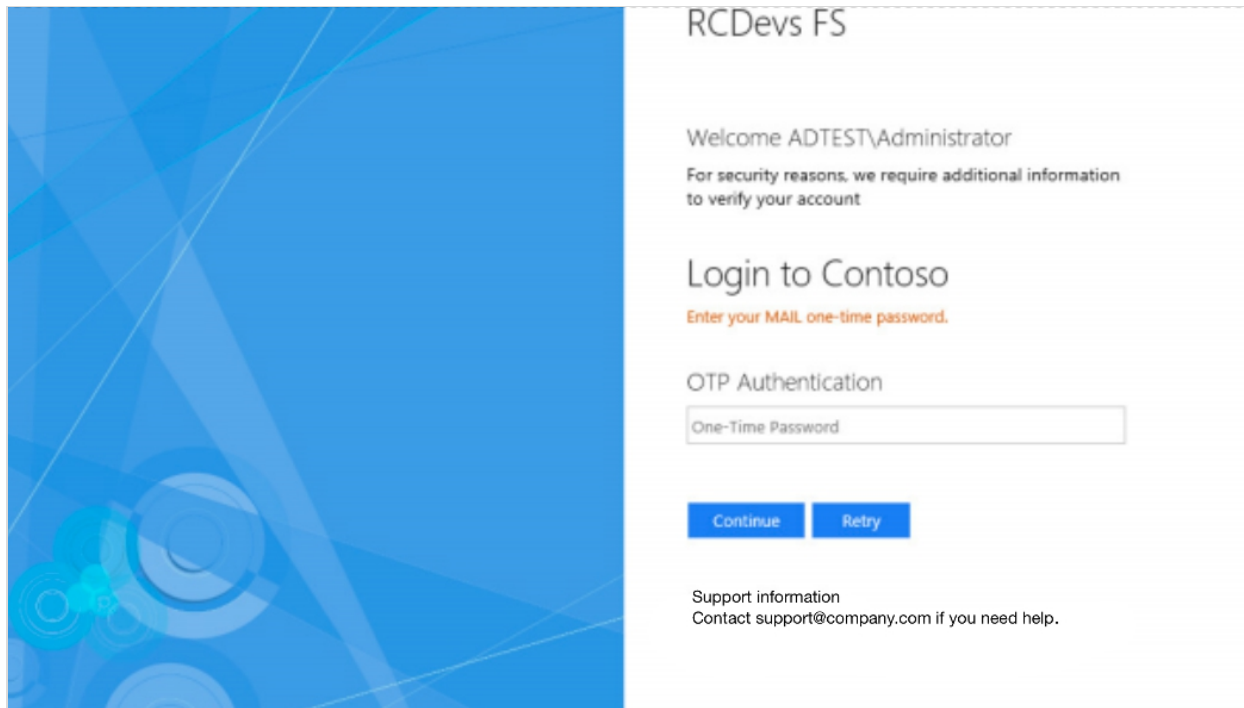
AD\Administrateur

.....

Sign in

© 2013 Microsoft

On the next page, an OTP will be asked.



🚩 OTP Policy

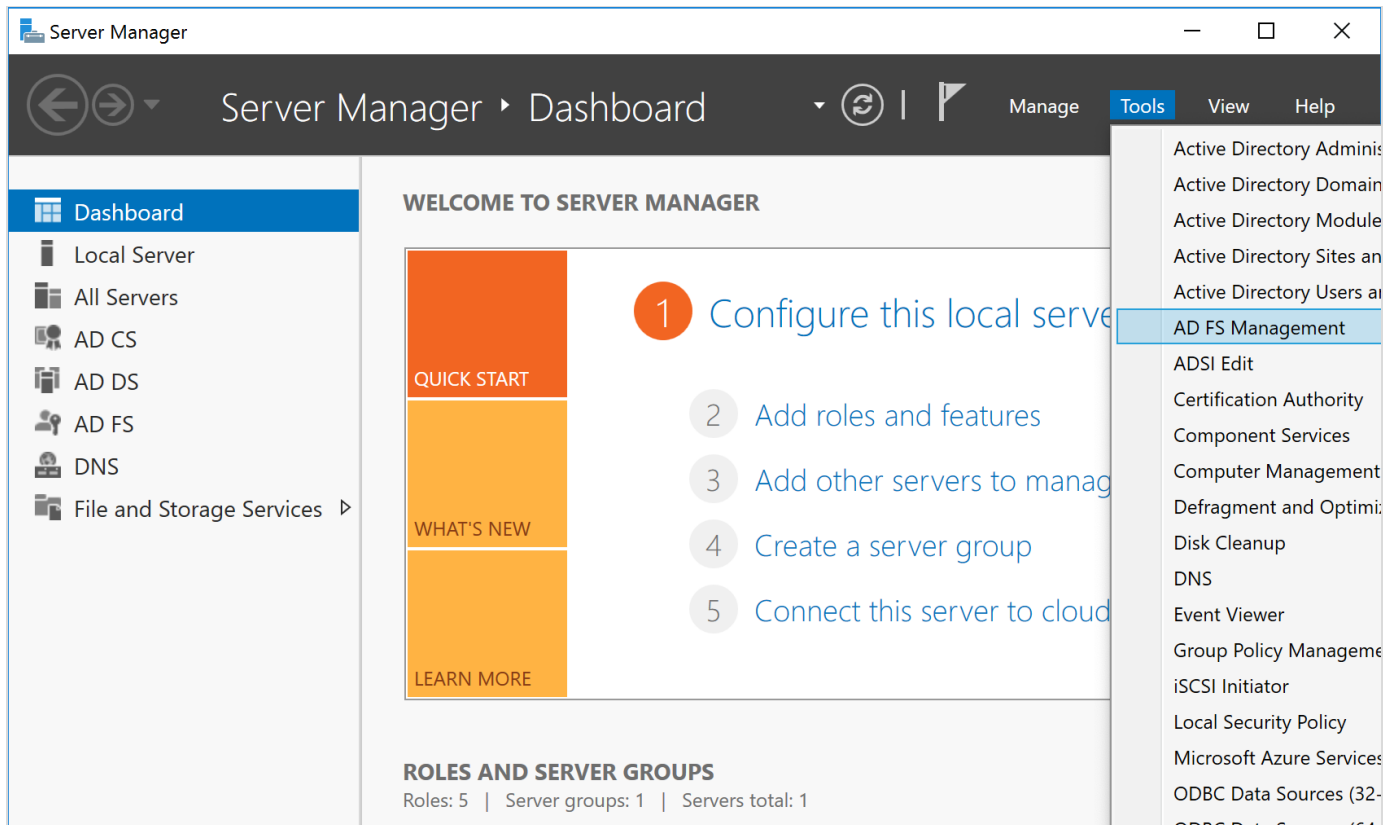
Here, AD FS was configured so that OpenOTP is the only option for a secondary factor, and OpenOTP is configured to require an OTP sent by mail to the user only. Enter your secondary factor to complete the test.

🚩 OpenOTP User Activation

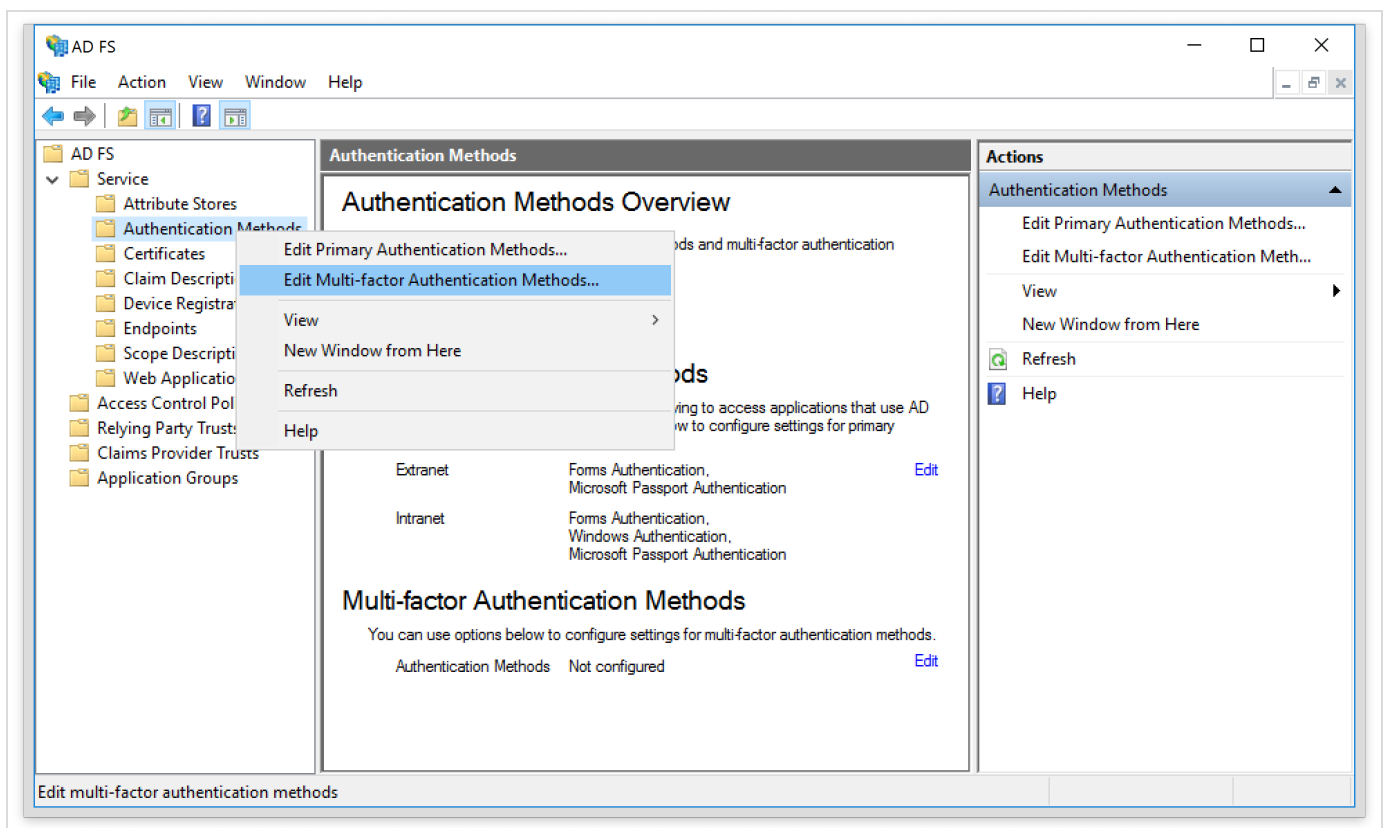
Your account should be activated for OpenOTP. Look the following How-To to activate an account: [OpenOTP User Activation](#). A Token has to be enrolled on the user account before testing OTP authentication.

6.2 Configuration for ADFS 4.0

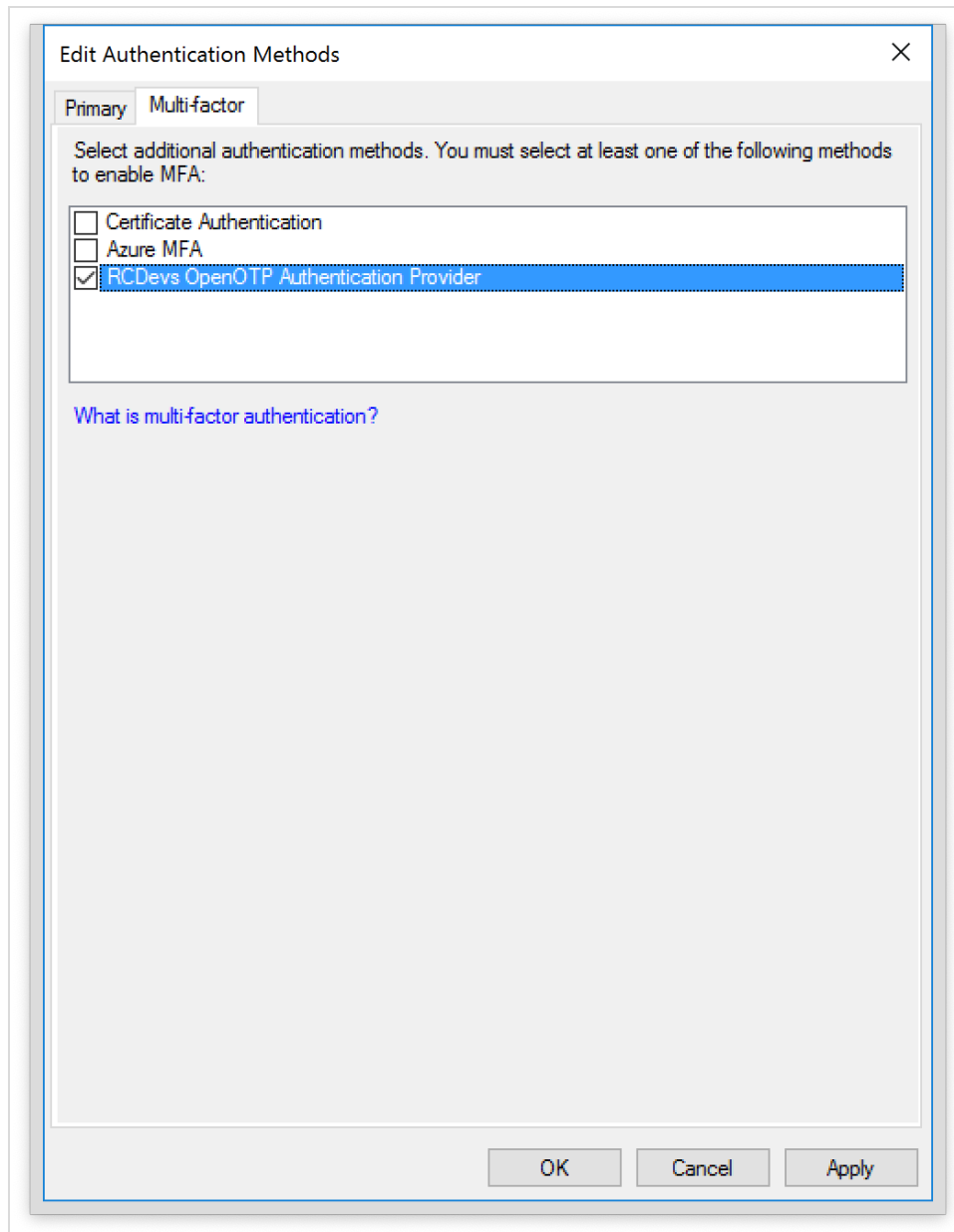
Now, we will configure the ADFS server(s) to have multi-factor authentication. For this, go on Windows Server Manager, click on Tools and ADFS Management.



On the ADFS Management page, under **Service** right click on **Authentication Methods** and click on **Edit Multi-factor Authentication Methods**.

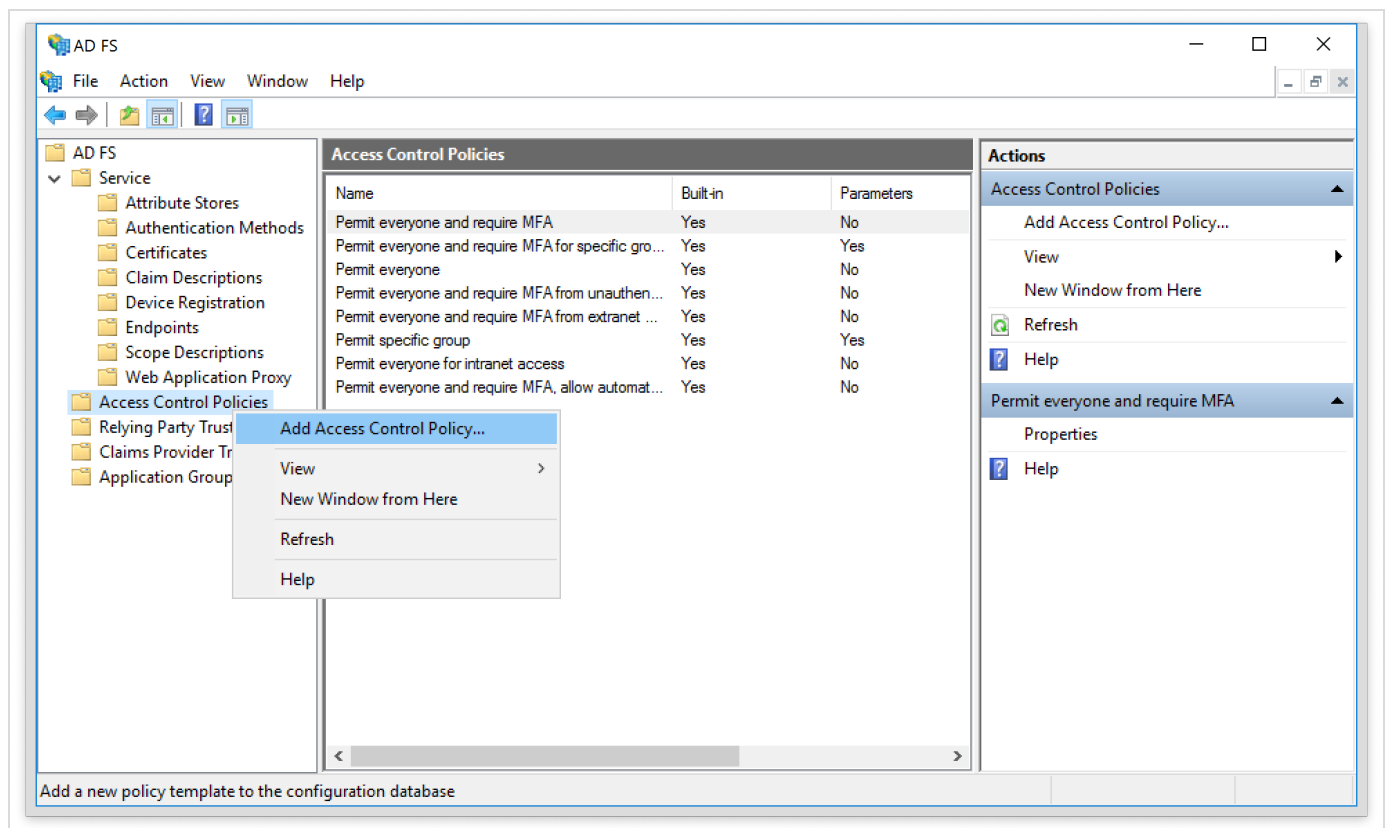


On the next page, you will find a new option available in the additional authentication methods named **RCDevs OpenOTP Authentication Provider**. Check the box of this option and click on OK.



Multi-factor policies at the ADFS level will now contact RCDevs plugin for MFA authentication.

We will now create a Multi-Factor policy called `OpenOTP`. Right click on Access Control Policies under the ADFS management console and then click `Add Access Control Policy`.



Name your Access Control Policy, on my side **OpenOTP** and click on **Add** button to configure the policy. On my side, I will allow every user and require a multi-factor authentication.

Add Access Control Policy

Name:

OpenOTP

Description:

Permit access if any of the following rules are met:

Add

Edit

Remove

☐ Require users to provide credentials each time at sign-in

OK

Cancel

Rule Editor

×

Permit

☐ everyone

☒ users

☐ from specific network

☐ from specific groups

☐ from devices with specific trust level

☐ with specific claims in the request

☒ and require multi-factor authentication

Except

☐ from specific network

☐ from specific groups

☐ from devices with specific trust level

☐ with specific claims in the request

Permit users
and require multi-factor
authentication

OK

Cancel

Add Access Control Policy

Name:
OpenOTP

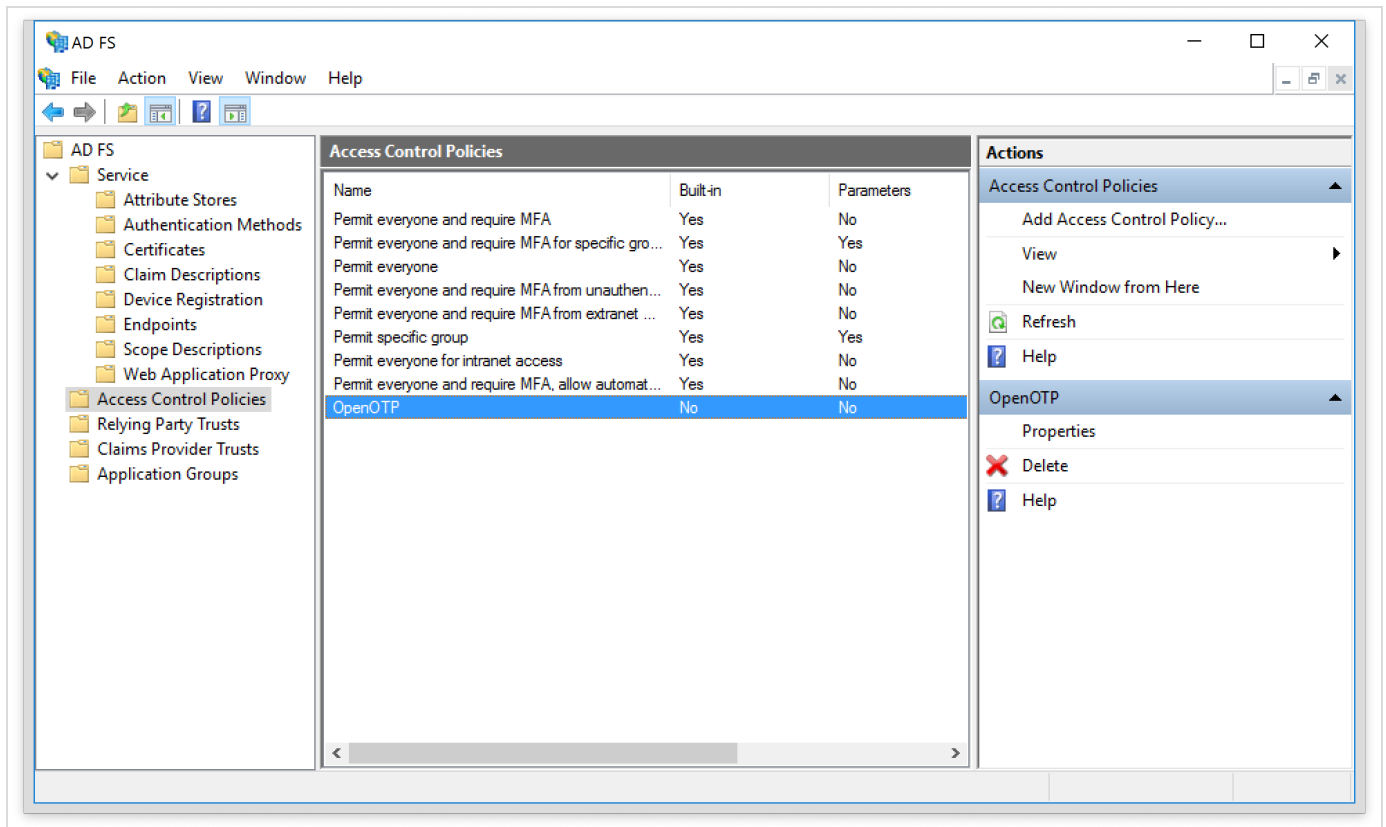
Description:

Permit access if any of the following rules are met:

Permit users
and require multi-factor authentication

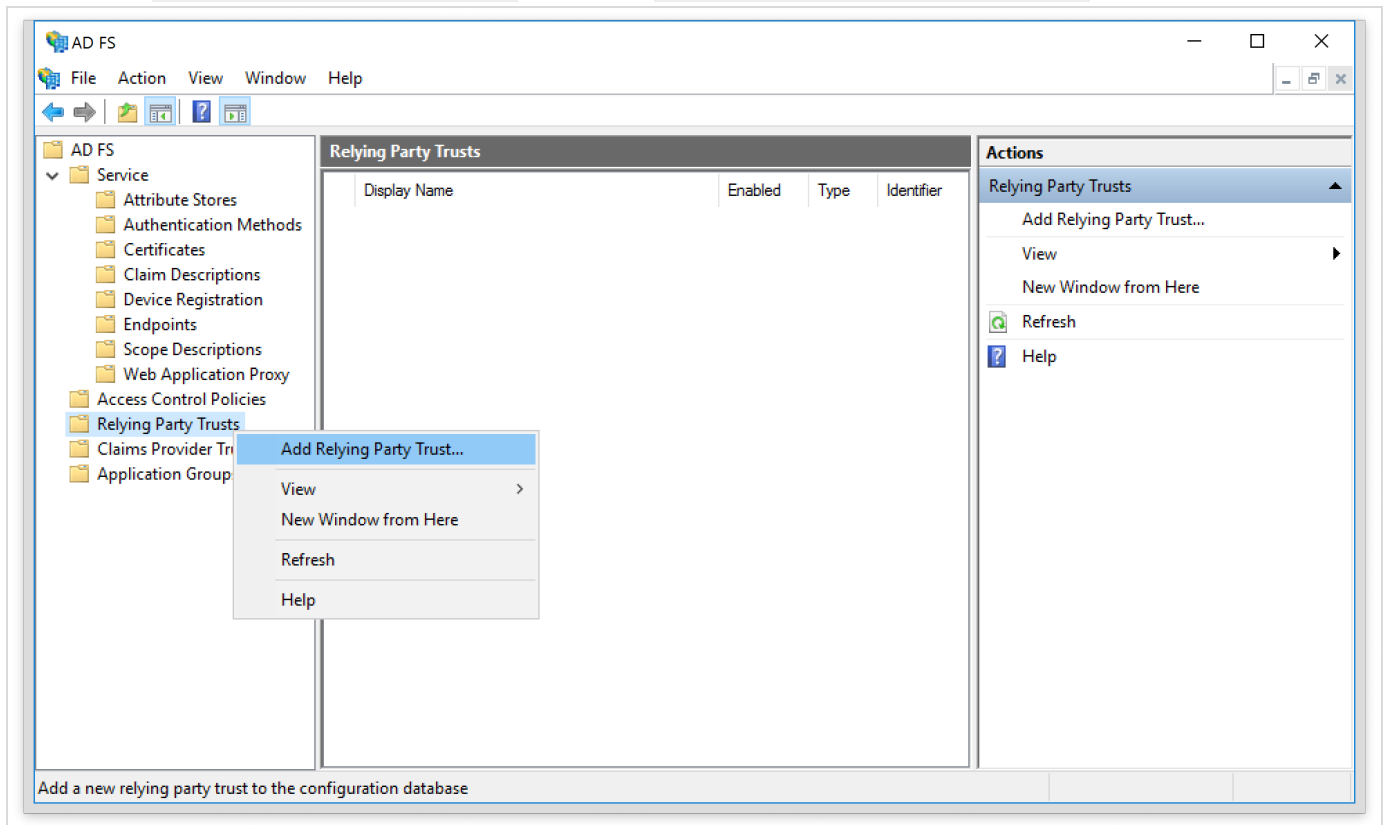
☒ Require users to provide credentials each time at sign-in

This part is done, you can click on **OK**.



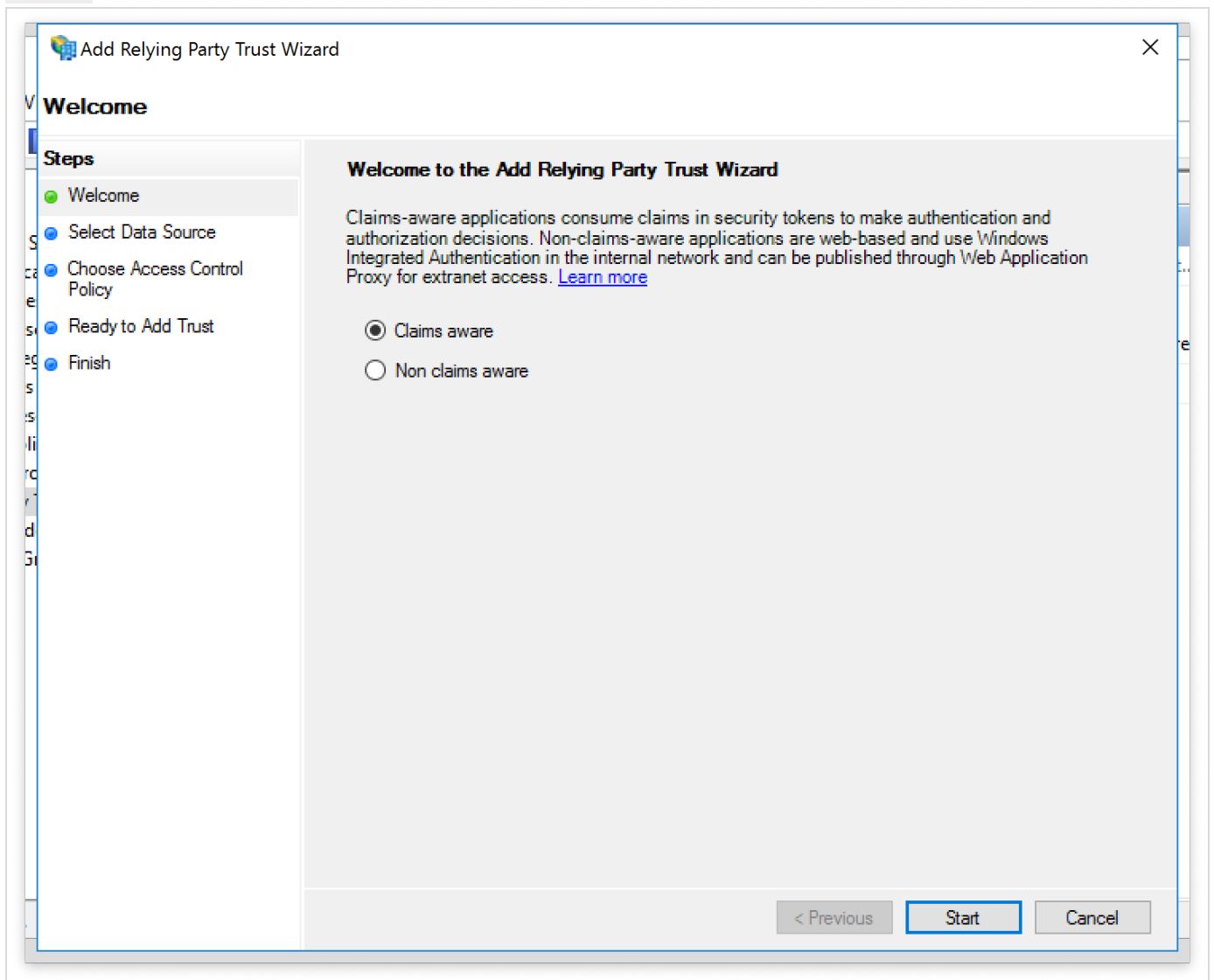
We will now configure a relying party trusts on the ADFS to apply our policy to the default ADFS login page (https://ADFS_INSTANCE_NAME/adfs/ls/idpinitiatedsignon)

Right click on **Relying Party Trusts** and click on **Add Relying Party Trusts**.



You are now in **Relying Party Trusts** Wizard. On the first page, select the option **Claims aware** and then click

Start .



On the next screen, you have to select the data source. Choose the 3rd option to configure the data source manually and click

Next .

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.


Federation metadata file location:

☒ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

On the next screen, name your Relying Party and click on **Next** :

 Add Relying Party Trust Wizard

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Enter the display name and any optional notes for this relying party.

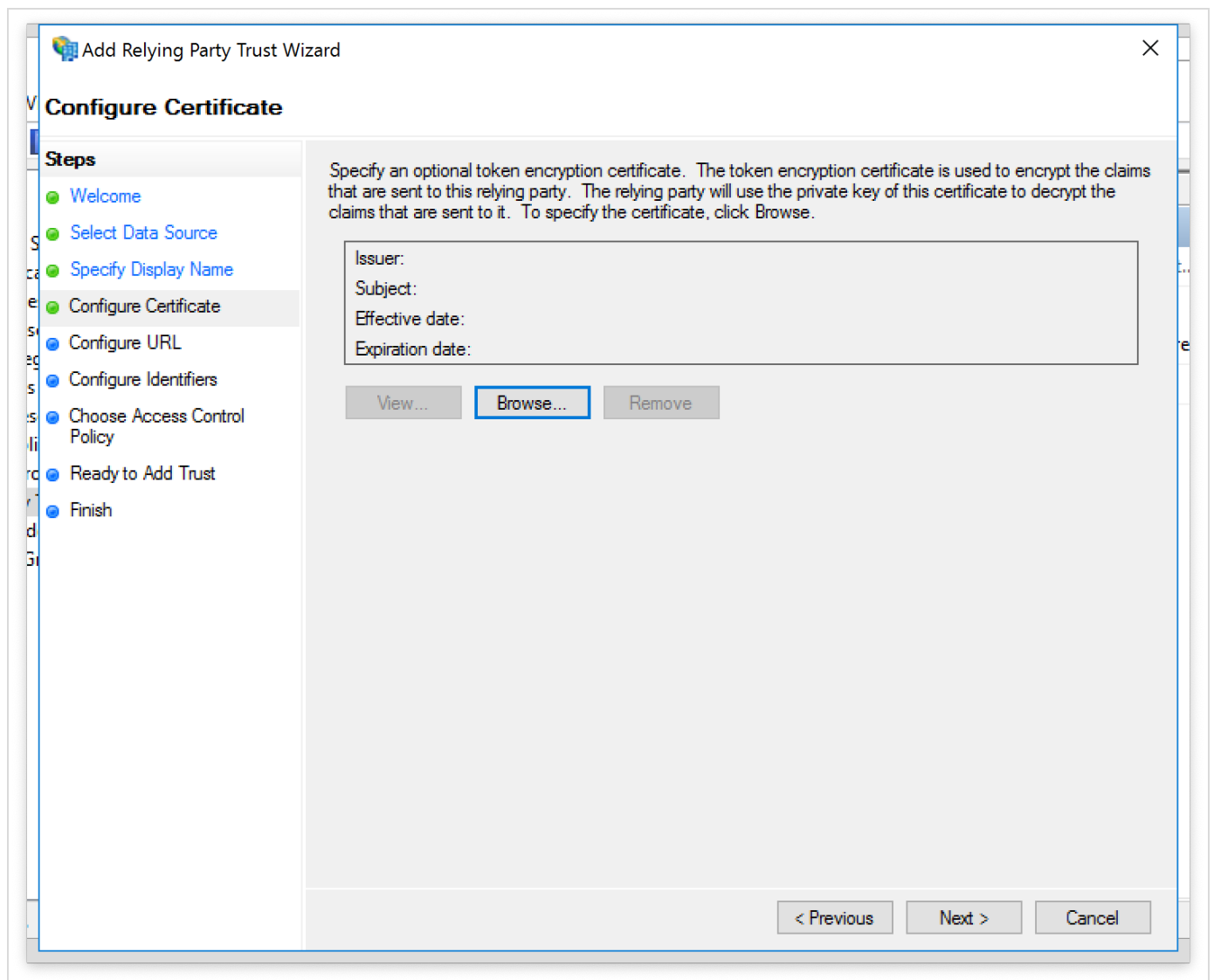
Display name:

MyIDP

Notes:

< Previous **Next >** Cancel

The next configuration page is optional. If required configure it and click on **Next**.



On the next page, select **Enable support for the SAML 2.0 WebSSO protocol** and configure your URL according to your ADFS server and click on **Next**.

Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: `https://fs.contoso.com/adfs/ls/`

☒ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

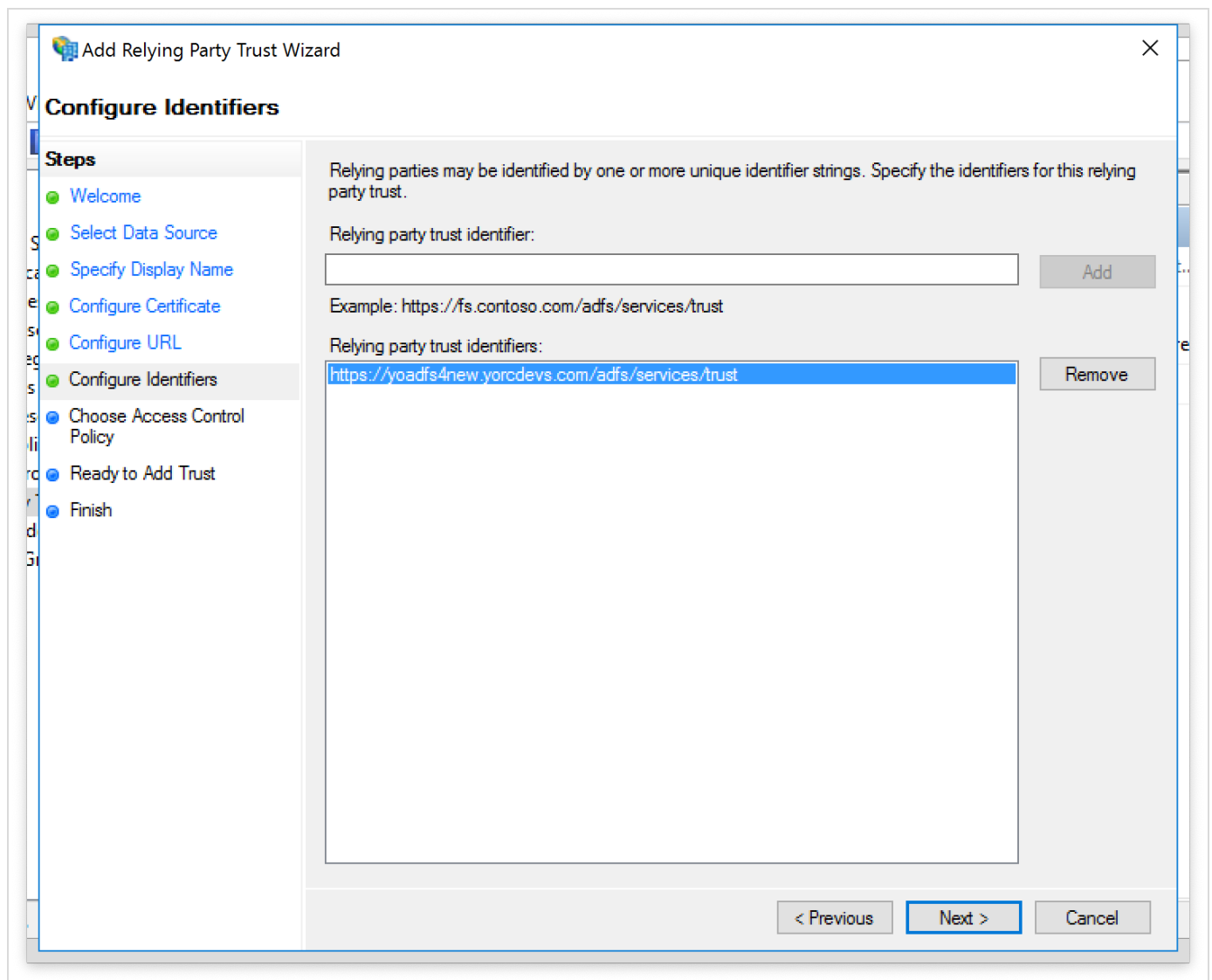
Relying party SAML 2.0 SSO service URL:

`https://yoadfs4new.yorcdevs.com/adfs/ls/`

Example: `https://www.contoso.com/adfs/ls/`

< Previous Next > Cancel

On the next screen, you have to configure your Identifier. Configure your Identifier, click **Add** and **Next**.



On the next configuration page, you have to choose an access control policy. I have previously created a policy called **OpenOTP** so I choose this one:

Add Relying Party Trust Wizard

Choose Access Control Policy

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy**
- Ready to Add Trust
- Finish

Choose an access control policy:

Name	Description
OpenOTP	
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require multi-factor authentication.
Permit everyone and require MFA for specific group	Grant access to everyone and require multi-factor authentication for specific groups.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require multi-factor authentication for extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require multi-factor authentication from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require multi-factor authentication, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.

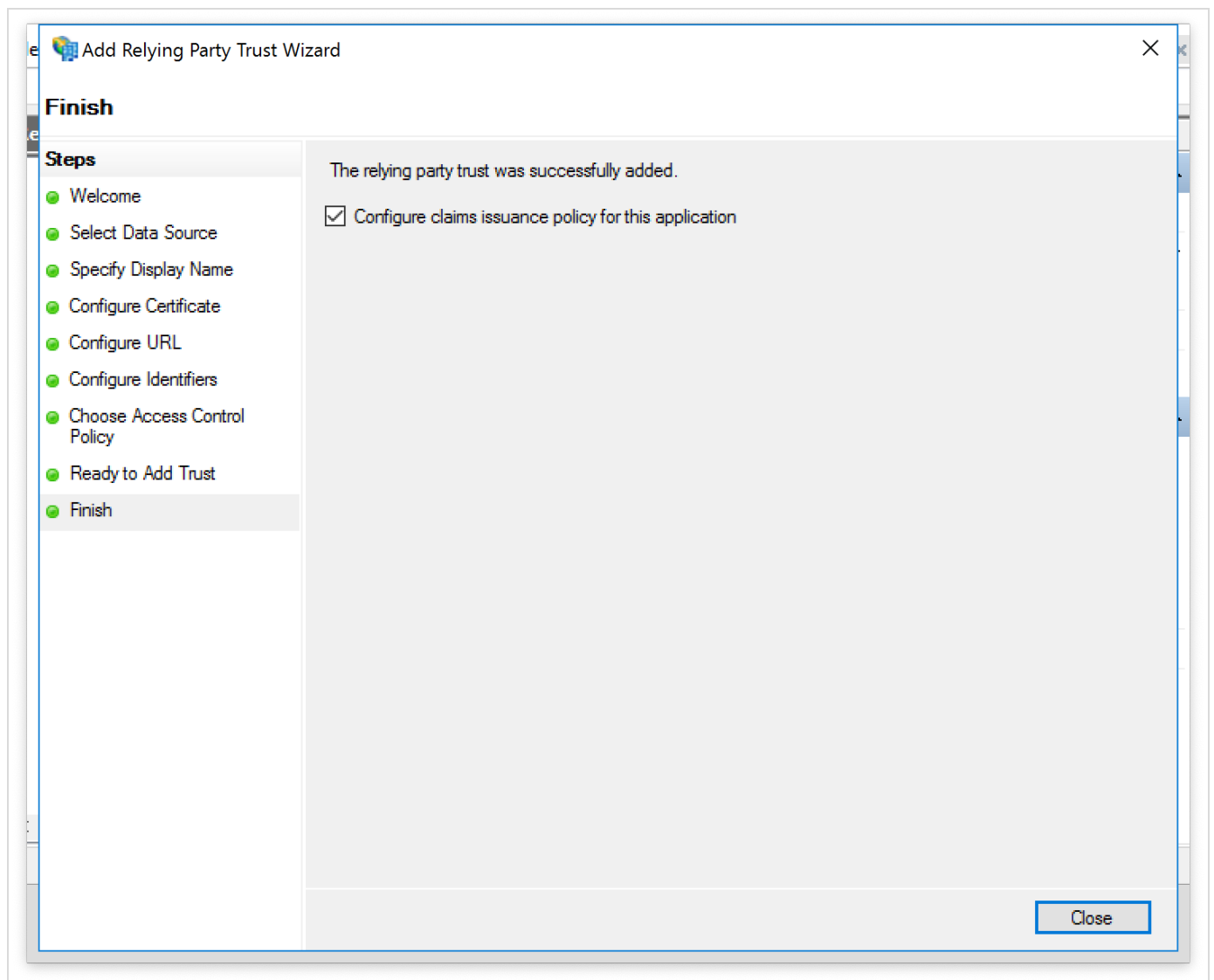
Policy

Permit users and require multi-factor authentication

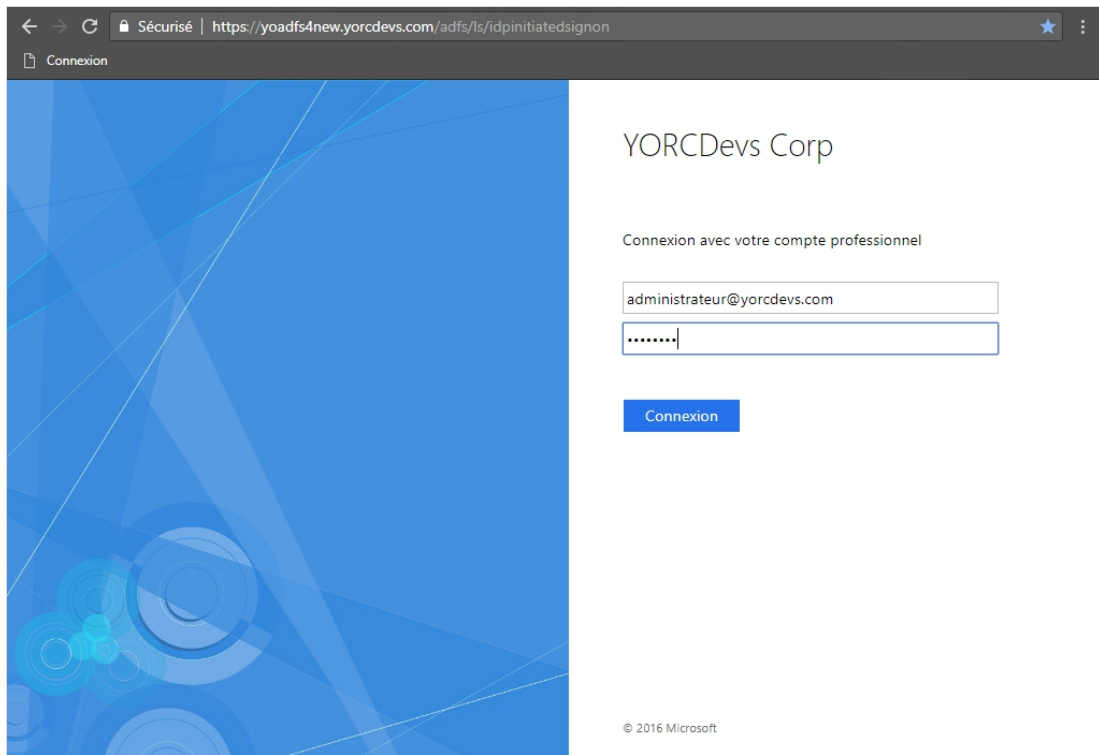
☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

< Previous Next > Cancel

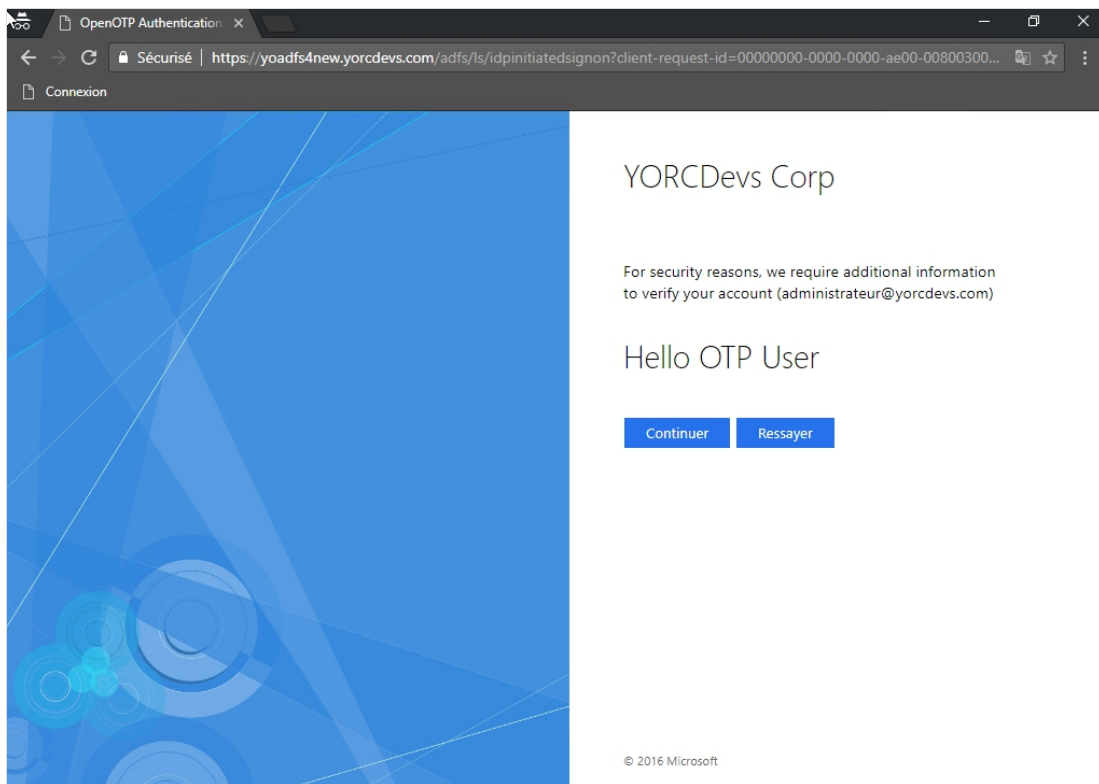
The configuration of the Relying Party Trust is now finished. Click on **Next** and **Close**.



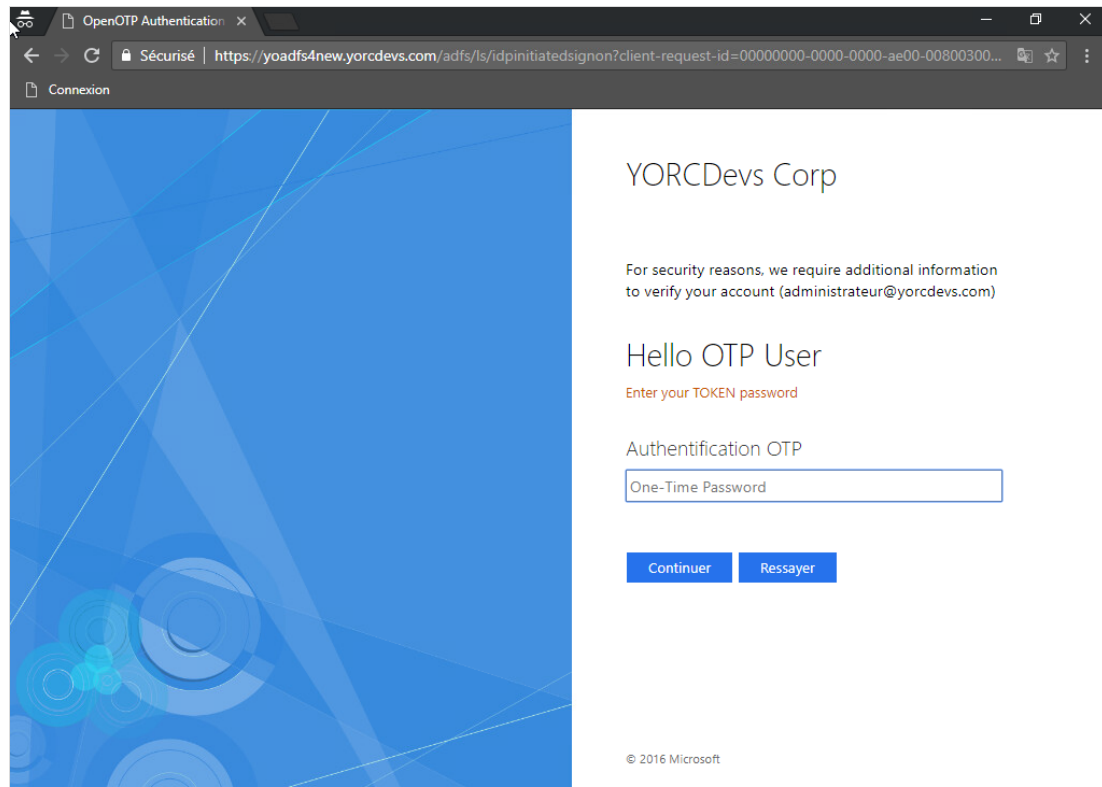
Multi-Factor Authentication is now configured for the default ADFS login page. We will now perform an authentication.



Click on Login and the next page will prompt you the following:



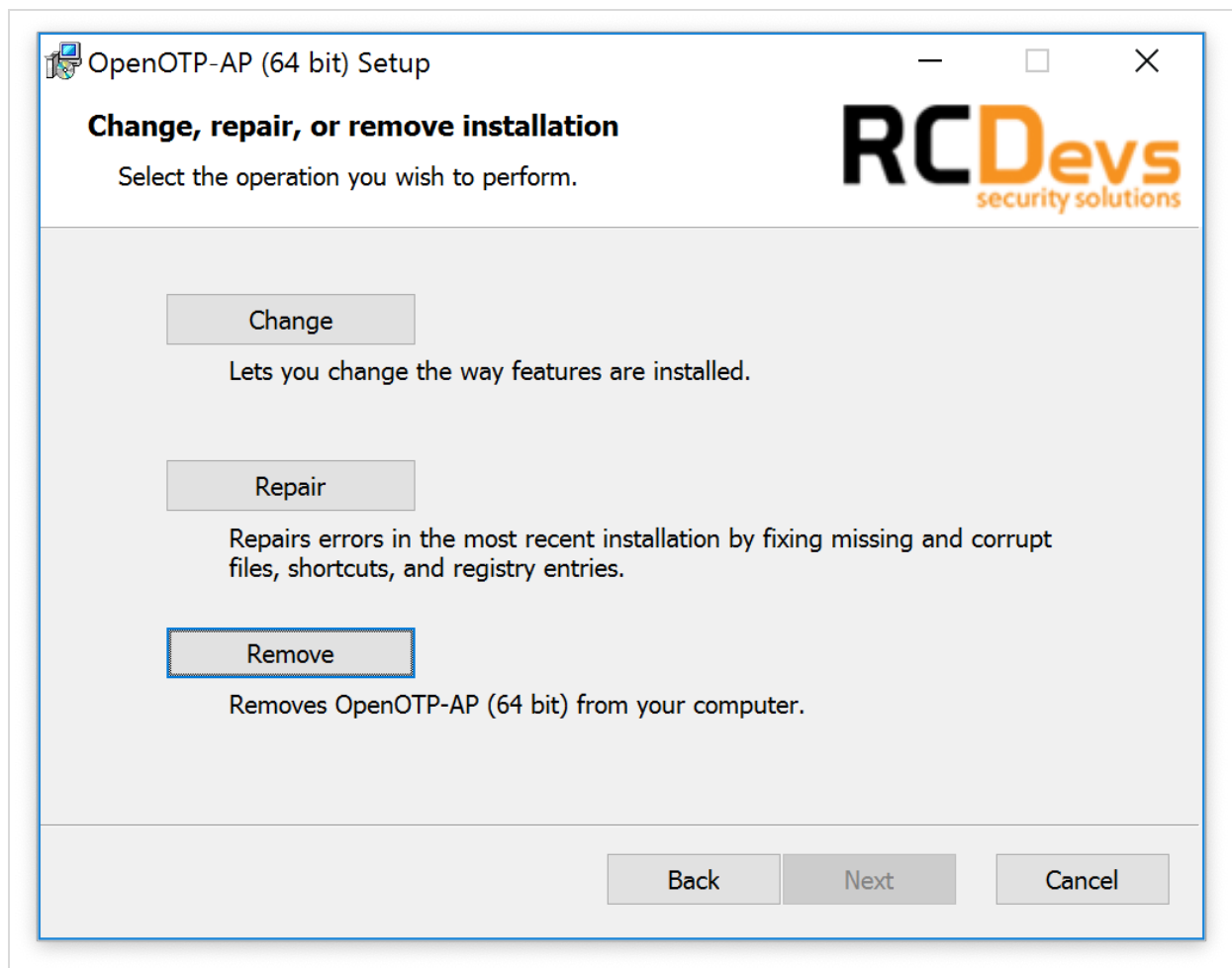
Click on Continue button and the next page will ask you to enter your OTP:



Provide your OTP and you are logged on.

7. Uninstalling the OpenOTP Authentication Provider

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



8. Troubleshooting

To pinpoint a problem in your AD FS/OpenOTP setup, you can start with the Windows Event. Viewer: “Applications and Services Logs”, then “AD FS”, then the “Admin” log. Also look at `/opt/webadm/logs/webadm.log`, or the equivalent in the WebADM interface (under the “Database” section).

9. Video Demonstration



Play Video on Youtube

This manual was prepared with great care. However, RCDevs 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 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 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 S.A. The latter especially applies for data processing systems. RCDevs 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 S.A. © 2019 RCDevs SA, All Rights Reserved