




Mi-Token

How to Setup ADFS for Office 365 for Single Sign-On



© 2019 Mi-Token Inc.

All rights reserved. No parts of this work may be reproduced in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Mi-Token version 1.0.0. Document version 1, January 2019.

Published: June 2019 in Austin, Texas, United States of America.

Set up ADFS for Office 365 for Single Sign-On

This document shows how to set up Active Directory Federation Service (ADFS) to work together with Office 365. It does not cover the ADFS proxy server scenario. This document discusses ADFS for Windows Server 2012 R2. However, the procedure also applies to ADFS 2.0 — except for steps 1, 3, and 7. In each of those steps, see the "Notes for ADFS 2.0" section for more information about how to use this procedure in Windows Server 2008.

Step 1: Install Active Directory Federation Services

Add ADFS by using Add Roles and Features Wizard.

Notes for ADFS 2.0

If you are using Windows Server 2008, you must download and install ADFS 2.0 to be able to work with Office 365. You can obtain ADFS 2.0 from the following Microsoft Download Center website:

[Active Directory Federation Services 2.0 RTW](#)

After the installation, use Windows Update to download and install all applicable updates.

Step 2: Request a certificate from a third-party CA for the Federation server name

Office 365 requires a trusted certificate on your ADFS server. Therefore, you must obtain a certificate from a third-party certification authority (CA).

When you customize the certificate request, make sure that you add the Federation server name in the **Common name** field.

We explain only how to generate a certificate signing request (CSR). You must send the CSR file to a third-party CA. The CA will return a signed certificate to you. Then, follow these steps to import the certificate to your computer certificate store:

1. Run Certlm.msc to open the local computer's certificate store.
2. In the navigation pane, Expand **Personal**, expand **Certificate**, right click the Certificate folder, and then click **Import**.

About the Federation server name

The Federation Service name is the Internet-facing domain name of your ADFS server. The Office 365 user will be redirected to this domain for authentication. Therefore, make sure that you add a public A record for the domain name.

Step 3: Configure ADFS

You cannot manually type a name as the Federation server name. The name is determined by the subject name (Common name) of a certificate in the local computer's certificate store.

Notes for ADFS 2.0

In ADFS 2.0, the Federation server name is determined by the certificate that binds to "Default Web Site" in Internet Information Services (IIS). You must bind the new certificate to the Default website before you configure ADFS.

You can use any account as the service account. If the service account's password is expired, ADFS will stop working. Therefore, make sure that the password of the account is set to never expire.

Step 4: Download Office 365 tools

Windows Azure Active Directory Module for Windows PowerShell and Azure Active Directory sync appliance are available in Office 365 portal. To obtain the tools, click Active Users, and then click Single sign-on: Set up.

Step 5: Add your domain to Office 365

This document does not explain how to add and verify your domain to Office 365. For more information about that procedure, see [Verify your domain in Office 365](#).

Step 6: Connect ADFS to Office 365

To connect ADFS to Office 365, run the following commands in Windows Azure Directory Module for Windows PowerShell.

Note In the Set-MSolADFSContext command, specify the FQDN of the ADFS server in your internal domain instead of the Federation server name.

PowerShell

```
Enable-PSRemoting
Connect-MSolService
Set-MSolADFSContext -computer <the FQDN of the ADFS server>
Convert-MSolDomainToFederated -domain <the custom domain name you added into Office 365>
```

If the commands run successfully, you should see the following:

- A "Microsoft Office 365 Identify Platform" Relying Party Trust is added to your ADFS server.
- Users who use the custom domain name as an email address suffix to log in to the Office 365 portal are redirected to your ADFS server.

Step 7: Sync local Active Directory user accounts to Office 365

If your internal domain name differs from the external domain name that is used as an email address suffix, you have to add the external domain name as an alternative UPN suffix in the local Active Directory domain. For example, the internal domain name is "company.local" but the external domain name is "company.com." In this situation, you have to add "company.com" as an alternative UPN suffix.

Sync the user accounts to Office 365 by using Directory Sync Tool.

Notes for ADFS 2.0

If you are using ADFS 2.0, you must change the UPN of the user account from "company.local" to "company.com" before you sync the account to Office 365. Otherwise, the user will not be validated on the ADFS server.

Step 8: Configure the client computer for Single Sign-On

After you add the Federation server name to the local Intranet zone in Internet Explorer, the NTLM authentication is used when users try to authenticate on the ADFS server. Therefore, they are not prompted to enter their credentials.

Administrators can implement Group Policy settings to configure a Single Sign-On solution on client computers that are joined to the domain.

Video:

How to Configure Federated Identity Sign In Model For Office 365

<https://www.microsoft.com/en-us/videoplayer/embed/9ffdb7ee-07bf-45ba-adec-f1acf576bd65>

Credits:

<https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/set-up-adfs-for-single-sign-on#useful-notes-for-the-steps-in-the-video>