



One Identity Defender AD FS Adapter 5.9

Administration Guide

Copyright 2017 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

Overview	4
Prerequisites	5
Connectivity Requirements	5
Deployment Overview	5
Running the Installer	7
Configuring Defender AD FS Adapter	8
Enable LDAP over SSL	10
Configure AD FS Multi-factor Authentication	11
Windows Server 2012 R2	11
Windows Server 2016	11
Network Diagram	13
Test Your Setup	14
Using GrIDSure tokens for Authenticating AD FS relying parties.	14
How to configure and use your Personal Identification Pattern (PIP)	16
Diagnostic logging	18
About us	19
Contacting us	19
Technical support resources	19

Overview

One Identity Defender AD FS Adapter integrates with Microsoft Active Directory Federation Services (AD FS) to add Two-Factor authentication to services using browser-based federated logins. The Defender AD FS Adapter supports relying parties that use Microsoft WS-Federation protocol, like Office 365, as well as SAML 2.0 federated logons for cloud apps like Google Apps and salesforce.com. Defender AD FS Adapter supports Windows Server 2012 R2 and Windows Server 2016.

Prerequisites

Before installing Defender AD FS Adapter, verify the following:

- Microsoft .NET Framework 4.5.2 or later is installed
- Defender Client SDK 5.9 or later is installed
- AD FS role is installed and the AD FS service is running
- PowerShell 4.0 or later is installed
- The federated logins to the relying parties are configured and working

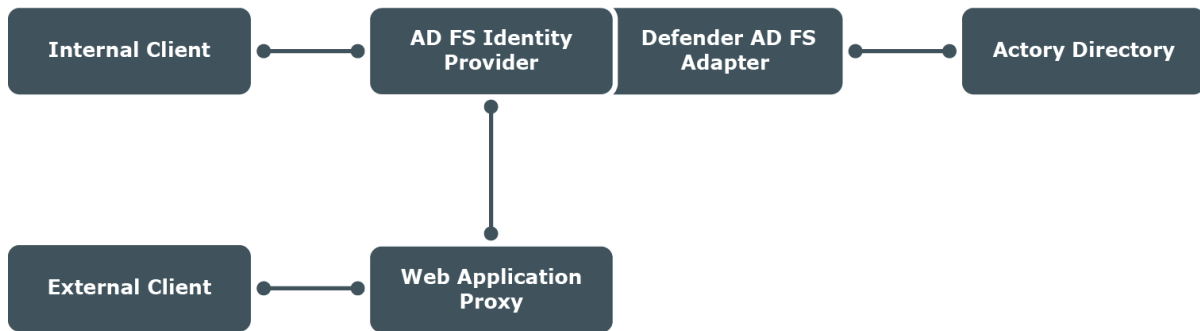
Connectivity Requirements

After verifying and setting up the prerequisites, connecting to Defender through Defender AD FS Adapter requires following parameters:

- IP address or DNS name of Defender Security Server (DSS)
- Port number (Default value is 1812)
- Timeout (Default value is 15 seconds)
- Shared Secret (The shared secret must be same as the shared secret configured in Defender Access Node.)
- User ID Attribute (The User ID Attribute must be same as the User ID Attribute configured in Defender Access Node. The default value is SAM Account Name.)

Deployment Overview

Defender AD FS Adapter adds Multi-Factor Authentication (MFA) that provides a Two-Factor authentication prompt to web-based logins through AD FS server or Web Application Proxy. After completing the primary AD FS server authentication (by any standard means such as Windows Integrated or Forms-Based), you have to complete Defender authentication challenge before getting redirected to the relying party. If the deployment is in an AD FS farm, install Defender AD FS Adapter on all AD FS servers in the farm.



After the installation of Defender AD FS Adapter on the AD FS servers in the farm, while configuring the Multi-Factor Authentication policies, select the MFA location (**Internal access** or **External access** or both as per the requirement). If you require Two-Factor authentication for External access locations, a Web Application Proxy is required and you do not have to install Defender AD FS Adapter on the Web Application Proxy server.

Running the Installer

1. Launch Defender AD FS Adapter installer MSI from an elevated command prompt (right-click **Command Prompt** and select the **Run as Administrator**).
2. Accept the license agreement and continue with the installation.
3. Complete the remaining steps for installing Defender AD FS Adapter.
 - i** | **NOTE:** AD FS service will restart during installation.
4. By default **Start Defender AD FS Configuration Tool** check box is selected. User can unselect this option, if they do not wish to configure Defender AD FS. Click Finish to complete the setup and start Defender AD FS Adapter configuration tool.
 - i** | **NOTE:** After configuration, select the Multi-factor Authentication method on the AD FS Management console.

Configuring Defender AD FS Adapter

To configure Defender AD FS Adapter

1. On the computer where the Defender AD FS Adapter is installed, run the Defender AD FS Adapter Configuration tool.

NOTE: Configuration is required for all installations of AD FS servers in the farm.

2. In the dialog box that opens, specify the Defender AD FS Adapter settings, and then click **OK**.

The dialog box looks similar to the following:

The screenshot shows the 'Defender AD FS Adapter Configuration' dialog box. It features a title bar with the text 'Defender AD FS Adapter Configuration' and a close button (X). The dialog is split into two main panels. The left panel, titled 'Defender Security Servers', contains a large empty rectangular area for a list of servers, with 'Add' and 'Remove' buttons positioned below it. The right panel, titled 'Edit DSS Entry', contains several input fields: 'Name' (with a placeholder '<new entry>'), 'IP Address or DNS Name', 'Port Number' (with '1812' entered), 'Shared Secret', 'Timeout in seconds' (with '15' entered), and 'User ID Attribute' (a dropdown menu currently showing 'SAM Account Name'). At the bottom right of the dialog are 'Apply' and 'Close' buttons.

Defender Security Servers Parameters

On this tab, specify the Defender Security Servers to which you want the Defender AD FS Adapter to connect. You can use the following elements:

- **Defender Security Servers** Use this area to set up a list of the Defender Security Servers to which you want the Defender AD FS Adapter to connect.
 - **Add** Adds a new entry to the list. After adding a new entry, edit its properties in the **Edit DSS Entry** area.

- **Remove** Removes the selected entry from the list.
- **Edit DSS Entry** Use this area to specify or edit the name, address, port number, and shared secret of the Defender Security Server to which you want the Defender AD FS Adapter to connect.
 - **Name** Type the name of the Defender Security Server you want to use for user authentication.
 - **Address** Type the IP address of the Defender Security Server.
 - **Port** Type the communication port number configured on the access node you want the Defender AD FS Adapter to use. The default value is set to **1812**.
 - **Shared Secret** Type the shared secret configured on the access node you want the Defender AD FS Adapter to use.
 - **Timeout in seconds** Specify the default timeout value in seconds. The default timeout is set to **15** seconds.
 - **User ID Attribute** Select the name of the attribute containing the user ID used to authenticate. User ID value must match with DSS Access Node. The default value is set to **SAM Account Name**.

Enable LDAP over SSL

To enable LDAP over SSL for communicating with Active Directory server.

NOTE: Configuration is required for all installations of AD FS servers in the farm.

On a computer where Defender AD FS Adapter is installed, create the following value in the "**HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Defender\AD FS Adapter**" registry key using the Registry Editor:

Value type: **REG_DWORD**

Value name: **LdapOverSsl**

Value data: **1**

Configure AD FS Multi-factor Authentication

- [Windows Server 2012 R2](#)
- [Windows Server 2016](#)

Windows Server 2012 R2

1. Launch the **AD FS Management console** on the primary AD FS internal server.
2. Navigate to **AD FS > Authentication Policies** and click **Edit Global Multi-factor Authentication** or **under Multi-factor Authentication > Global Settings** section, click **Edit**.
3. In the **Edit Global Authentication Policy** window, click **Multi-factor** tab.
4. In **Users/Groups** section, click **Add** and select a domain for MFA (for example, Domain Users).

i | **NOTE:** The Users or the Groups must be a member of Defender Access Node.

5. In the **Location** section, select **Extranet** and/or **Intranet** checkboxes depending on the required type of connection.

For example, if you always require two-factor authentication, select both Extranet and Intranet when configuring the multi-factor authentication policy. If you want to enforce two-factor authentication for external users, and if you have configured your network such that external users communicate with an AD FS Web Application Proxy while internal users communicate with the Identity Provider, select only **Extranet**.

6. Select **One Identity Defender AD FS Adapter** authentication method to enable multi-factor authentication using Defender.

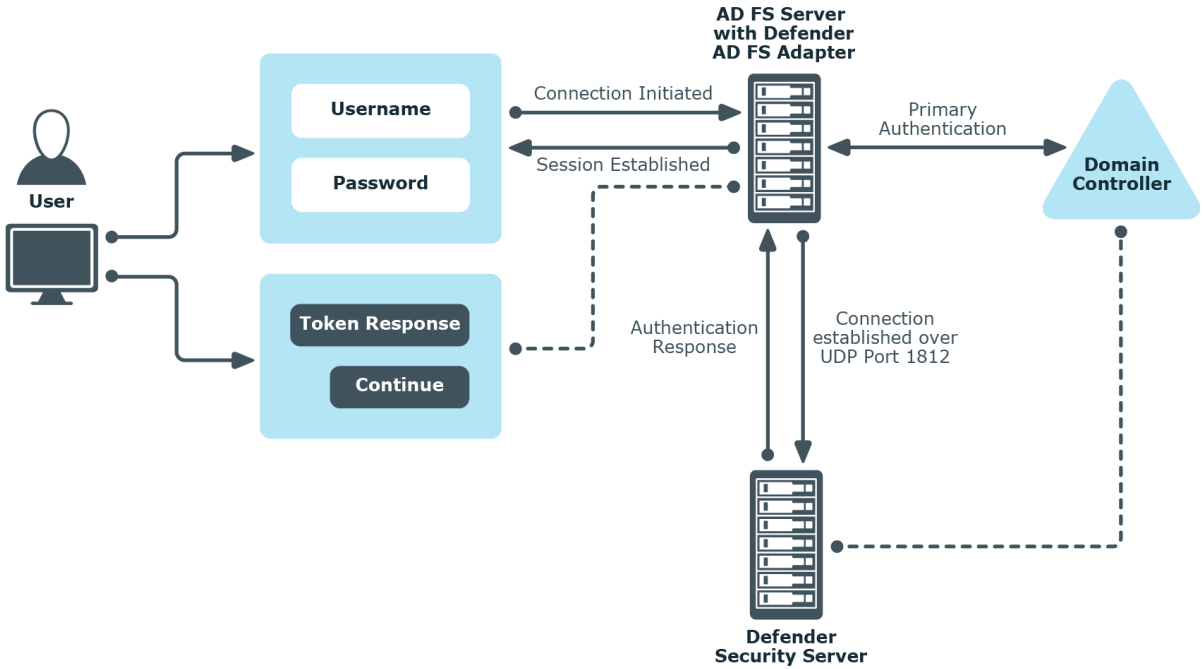
i | **NOTE:** In an advanced multi-factor scenario, you can select **Intranet** and/or **Extranet** for each user or for each relying party. For more information, see the Microsoft's TechNet article *Overview: Manage Risk with Additional Multi-Factor Authentication for Sensitive Applications*.

Windows Server 2016

1. Launch the AD FS Management console on your primary AD FS internal server and navigate to **AD FS → Service → Authentication Methods**.

2. Click the **Edit** link under **Multi-factor Authentication Methods** or click **Edit Multi-factor Authentication Methods**.
3. Check the box next to the **One Identity Defender AD FS Adapter** authentication method to enable MFA authentication. Click **OK**.
4. Go to **AD FS** → **Access Control Policies** and either edit one of the existing MFA policies to apply it to users or groups, or create a new MFA policy if no pre-defined one is sufficient for your organization's MFA requirements.
5. Go to **AD FS** → **Relying Party Trusts**, right-click the relying party trust where you want to add Defender AD FS, then select **Edit Access Control Policy**.
6. Pick a policy for the relying party that includes MFA and then click **OK**. The MFA policy immediately applies to the selected relying party.

Network Diagram



Test Your Setup

To test your setup, do the following:

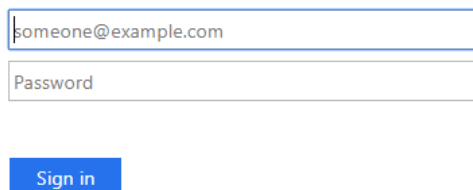
1. Using a web browser log in to a relying party for your AD FS deployment. For example, you can log into <https://portal.microsoftonline.com> to access Office 365.
2. Complete primary authentication of your AD FS server. The two-factor authentication page is displayed.
3. In the **Token Response** field, enter the response displayed on your token. The authentication type depends on the Defender policy that has been configured. For example, if Defender is configured to use a token policy, the Enter Synchronous Response prompt is displayed.

Using GrIDSure tokens for Authenticating AD FS relying parties.

To authenticate on a AD FS relying party by using the GrIDSure token

1. In your Web browser, enter the address of the AD FS relying party you want to access.
If the AD FS relying party is protected with the GrIDSure personal identification system, the following page opens:

Sign in with your organizational account



The screenshot shows a sign-in form with the following elements:

- A text input field containing the email address "someone@example.com".
- A text input field labeled "Password".
- A blue button labeled "Sign in".

2. Type your user name, password, and then click **Sign In**.

When configuring GrIDSure token for the first time, the login page prompts to enter your Windows password:

Two-Factor Authentication is required

Enter Windows password.

Continue

Note that the page that opens may look differently if you have two or more different types of Defender Token assigned:

Two-Factor Authentication is required

Enter token response.

Continue

Use GrIDSure

In this case, click the **Use GrIDSure** button.

3. Type your Windows password, and then click **Continue**.

If this is the first time you authenticate using the GrIDSure token, you may be prompted to configure your GrIDSure Personal Identification Pattern (PIP). For more information, see [How to configure and use your Personal Identification Pattern \(PIP\)](#).

4. You are now prompted to authenticate using your GrIDSure PIP. Type the numbers located in the cells you chose when configuring your GrIDSure PIP:

Two-Factor Authentication is required

Use your GrIDSure PIP.

2	8	3	5	4	3
8	1	8	1	5	9
0	6	6	2	7	0
2	3	0	9	7	1
2	1	4	4	6	0
3	5	7	5	4	9

Reset GrIDSure PIP

Continue

In the **Enter passcode** text box, type your PIP, and then click **Sign In** to access the protected Web site.

You can select the **Reset PIP** check box to reset your current PIP after you sign in.

How to configure and use your Personal Identification Pattern (PIP)

To authenticate with the GrIDSure token, you need to use a special code which is called the GrIDSure Personal Identification Pattern (PIP).

When you access a resource protected with the GrIDSure personal identification system for the first time, you are prompted to configure your PIP. In this case, a matrix of cells similar to the following displays:

CC	AP	BC	AH	AI	BD
AM	AJ	BI	AD	AA	AE
AO	BF	CA	AN	AG	BN
AC	BE	AK	BG	BP	BB
BL	BJ	AB	CB	BM	BA
AF	BK	CD	AL	BO	BH

In this matrix, choose the cells you want to use for authentication, and then, in the **Configure your GrIDSure PIP** text box, type the codes contained in the cells you have chosen. Do not leave blank spaces between the codes.

For example, if you choose the first four cells in the first row of the matrix above, in the **Configure your GrIDSure PIP** text box, type **CCAPBCAH** (without spaces), and then press ENTER or click **Continue**.

From now on, each time you authenticate with your GrIDSure token, you must use the codes displayed in the matrix cells you have chosen when configuring your PIP. These codes will be different each time the matrix of cells displays.

For example, next time the matrix may look as follows:

2	8	3	5	4	3
8	1	8	1	5	9
0	6	6	2	7	0
2	3	0	9	7	1
2	1	4	4	6	0
3	5	7	5	4	9

In this case, use the **Use your GrIDSure PIP** text box to type **2835**, and then press ENTER or click **Continue**.

Diagnostic logging

To troubleshoot issues that may occur during authentication with Defender, you need to enable diagnostic logging for the Defender AD FS Adapter.

To enable diagnostic logging for Defender AD FS Adapter

- On a computer where Defender AD FS Adapter is installed, create the following value in the

HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Defender\AD FS Adapter registry key using the Registry Editor:

Value type: **REG_DWORD**

Value name: **Diagnostics**

Value data: **1**

The path to the log file: **%ProgramData%\One Identity\Defender\Diagnostics\AD FS Adapter**

File name for Adapter: **DefenderAdapter.log**

File name for Configuration tool: **Configuration.log**

To disable diagnostic logging for Defender AD FS Adapter, delete the Diagnostics value from the Defender AD FS Adapter registry key or set the value data to **0**.

Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product