One Identity Starling Two-Factor AD FS Adapter 7.0

Administration Guide

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.

AD FS Adapter Administration Guide
Updated - May 2019
Version - 7.0

Contents

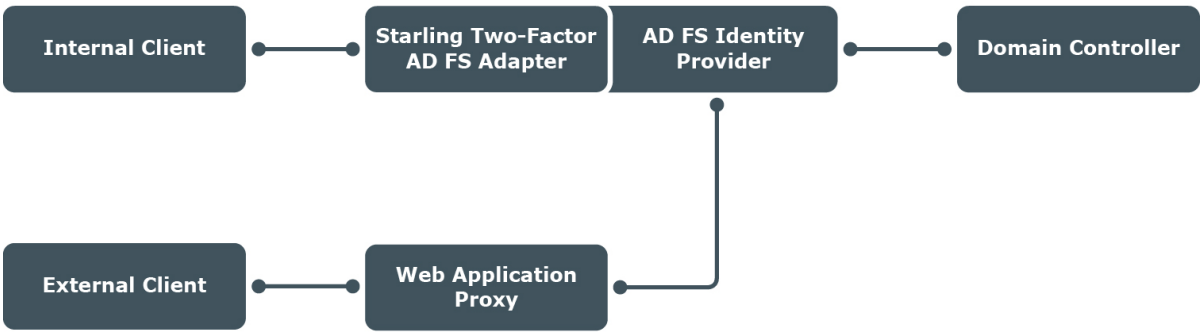
1

Overview

One Identity Starling Two-Factor AD FS Adapter integrates with Microsoft Active Directory Federation Services (AD FS) to add two-factor authentication to services using browser-based federated logins. Starling Two-Factor AD FS Adapter supports relying parties that use Microsoft WS-Federation protocol such as Office 365, as well as SAML 2.0 federated logins for cloud applications such as Google Apps and Salesforce.com. Starling Two-Factor AD FS Adapter supports Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

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, using standard methods such as Windows Integrated or Forms-Based, complete Starling Two-Factor authentication before getting redirected to the relying party. If the deployment is in an AD FS farm, install AD FS Adapter on all AD FS servers in the farm.

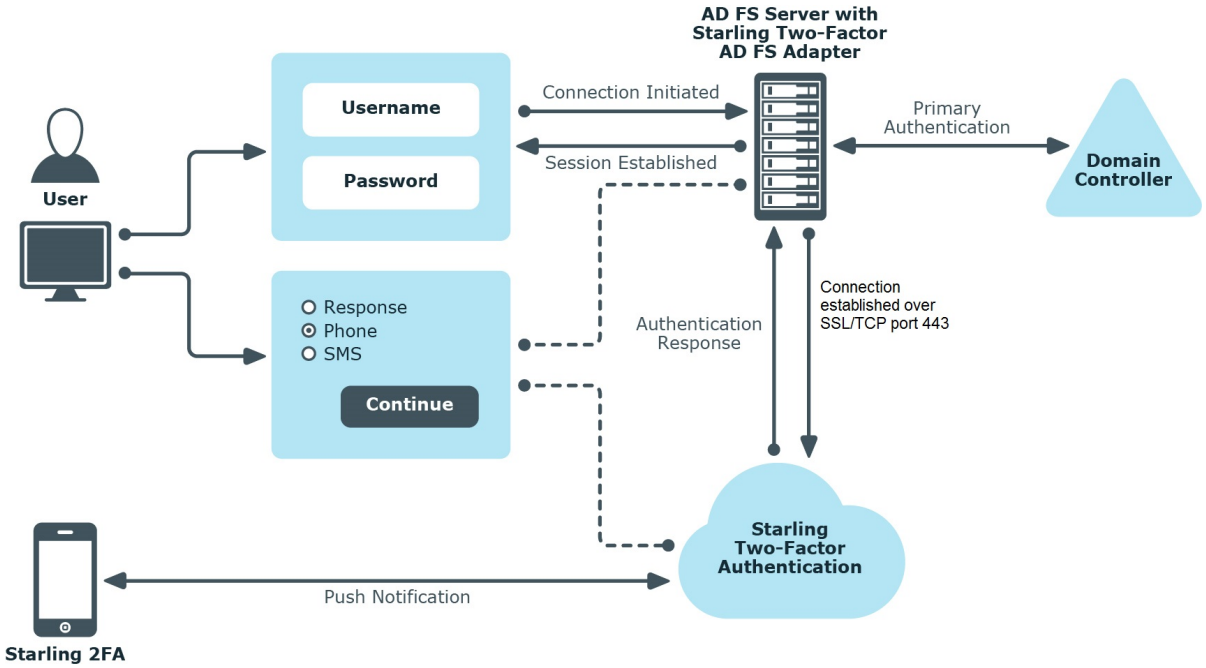
Figure 1: AD FS Adapter deployment overview



After the installation of 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 AD FS Adapter on the Web Application Proxy server.

AD FS Adapter Network diagram

The following diagram gives an overview of how AD FS Adapter functions with Starling Two-Factor Authentication to provide two-factor authentication to the relying parties.



Installing Starling Two-Factor AD FS Adapter

The following sections brief about the prerequisites and the steps to download and install the latest version of the **Starling Two-Factor AD FS Adapter**.

- Prerequisites to connect AD FS Adapter to Starling
- Connectivity requirements
- Downloading the Starling Two-Factor AD FS Adapter installer
- Installing Starling Two-Factor AD FS Adapter

Prerequisites for Starling Two-Factor AD FS Adapter installation

Before installing AD FS Adapter, verify the following on the system:

- Microsoft .NET Framework 4.6.2 or later is installed
- PowerShell 4.0 or later is installed
- AD FS role is installed
- AD FS service is running
- The federated logins to the relying parties are working
- A valid phone number and email address are configured in the Active Directory for the user

Connectivity requirements

After verifying and setting up the prerequisites, request the Starling Two-Factor Authentication subscription.

AD FS Adapter communicates with Starling Two-Factor Authentication on SSL/TCP port 443. Since the IP addresses may change over time, you must not lock down the firewall to individual IP addresses.

Downloading the Starling Two-Factor AD FS Adapter installer

The following section briefs about the steps to download the latest version of the **Starling Two-Factor AD FS Adapter**.

To download the installer

1. On the support.oneidentity.com site, sign in to the One Identity account by entering the appropriate credentials. If you do not have an account, click **Sign up for a new account**. You also have the option to sign in through the Microsoft account.

   The **One Identity Support page** is displayed.

2. In the **Identity as a Service** section, click **Starling Two-Factor Authentication**.

   The **Product Support - Starling Two-Factor Authentication** page is displayed.

3. Click **Install & Upgrade**.
4. Click **Starling Two-Factor AD FS Adapter 7.0**.

   The **Download Starling Two-Factor AD FS Adapter 7.0** page is displayed.

5. Click **Add to Downloads**.
6. Review the terms and conditions and click **Continue**.

   The **Add to My Downloads** page is displayed.

7. Click **Download Now** to download the `.msi` file.
8. Click **Add to My Downloads** to save the application in the **My Downloads** cart. It is recommended to use this option when you download multiple products.

   The **StarlingTwoFactorADFSAdapter.msi** file is downloaded.

Running the Starling Two-Factor AD FS Adapter installer

The following section briefs about the steps to install the latest version of the **Starling Two-Factor AD FS Adapter**.

To run the installer:

1. Launch AD FS Adapter installer MSI from an elevated command prompt or right-click **Command Prompt** and select **Run as Administrator**.
2. Complete the remaining steps for installing AD FS Adapter.

   NOTE: AD FS Service will restart during installation.

IMPORTANT: In case of an upgrade to Starling Two-Factor AD FS Adapter 7.0, you must connect to Starling as the Subscription key related provision is removed. Connect to Starling using the credentials that were used to create the Starling account. You must configure the Push notification and AD attributes again, to overwrite the default values. For information on connecting to Starling, see Connecting Starling for authentication

3

Starling Two-Factor AD FS Adapter Configuration Settings

You can configure the Starling Two-Factor AD FS Adapter for two-factor authentication by setting the required parameters in the **Starling Two-Factor AD FS Adapter Configuration** window. You can set the parameters using the following options that are displayed on the **Starling Two-Factor AD FS Adapter Configuration** window:

- **Home**: Displays the various configuration options in a tree view and as tiles.
- **Connect Starling**: Allows you to connect to the Two-Factor Authentication subscription by logging in to your One Identity Starling account.
- **Push Notification**: Allows you to configure the push notifications messages and timeout settings.
- **Attribute names**: Allows you to specify the Active Directory attributes, which are used to retrieve the values for user who has logged in to the Starling Two-Factor AD FS Adapter.

Connecting Starling for authentication

To use the Starling two-factor authentication for AD FS Adapter, you must first connect to Starling using the Starling Join option available for One Identity on-premises products.

To obtain a Starling Two-Factor Authentication subscription and register with Starling, click https://www.cloud.oneidentity.com/.

NOTE: If you do not have a Starling account, for more information on creating a Starling account, see the *One Identity Starling User's Guide*

To connect Starling for authentication, see:

- Prerequisites to connect AD FS Adapter to Starling
- Connecting AD FS Adapter to Starling

Prerequisites to connect AD FS Adapter to Starling

The following are the prerequisites to connect AD FS Adapter to Starling:

- User must have a One Identity Starling account. For more information on creating a One Identity Starling account, see the *Starling Two-Factor Authentication Administration Guide*.
- The Starling Account must be activated with a valid Two-Factor Authentication subscription.

Connecting AD FS Adapter to Starling

After the pre-requisites to connect to Starling are met, connect AD FS Adapter to Starling using the Starling Join option available for One Identity on-premises products.

To connect and configure One Identity Starling for authentication

1. On the AD FS Adapter window, click **Connect Starling**.

   The **Connect Starling** window is dispalyed.

2. Click **Connect my account**.

   You are redirected to the **One Identity Starling** authentication window.

3. Provide your Starling credentials and click **SIGN IN**.
4. In the **Join to Starling** window, click **Accept**.

   NOTE: If you are a member of more than one Starling organization, use the drop-down to select the organization to which you want to connect.

5. Click **Join**.

   After successful authentication, you are redirected to the One Identity Starling Two-Factor Authentication **Connect Starling** window.

   NOTE: To connect to a different organization in your One Identity Starling account, click **Change Account**

   If the connection is unsuccessful, a message is displayed providing the details of the error and the previously connected account is continued to be used. In such a case, it is recommended to contact support for any help.

   NOTE: If there are network issues or if Starling is down, your account may get disconnected. In such cases, click **Reconnect**. To test the validity of your account connection, click **Test connection**.

Configuring Push notification settings

Push notification enables you to approve or deny login requests. These requests facilitate an end-to-end encrypted communication between the application and a secured authentication service. Accurate configuration of the push notification allows you to **Approve** or **Deny** a login attempt.

To configure the push notification settings

1. On the **Starling Two-Factor AD FS Adapter Configuration** page, click **Push notifications**.

   The **Push notifications** window is displayed.

2. In the **Message** field, enter the message that is to be displayed in the Starling Two-Factor application. The message size must range between 10 to 50 characters.
3. In the **Timeout (seconds)** field, from the drop-down menu, select the timeout duration or the validity of the notification .

   NOTE:

   - By default, 30 seconds is set as a timeout duration for notifications.
   - Select **Other** in the drop-down menu, to specify the customized timeout duration in seconds.

4. Click **Save Settings** after completing the configuration.

Configuring Active Directory attributes

If user data is stored in Active Directory, you must configure the user AD attributes that would be used to retrieve values of the log on user from the Active Directory. The user's email address and phone number specified in Starling Two-Factor AD FS Adapter are used to validate if the AD user can be authenticated to log in to the to services using browser-based federated logins.

The Starling Two-Factor AD FS Adapter Configuration window allows you to specify the user attributes that would be used to retrieve the user's email address and phone number from Active Directory.

To configure AD FS Adapter to retrieve user attributes stored in Active Directory

1. On the **Starling Two-Factor AD FS Adapter Configuration** page, click **Attribute names**.

   The **Active Directory attributes** window is displayed.

2. In the **E-Mail attribute** field, select the required email attribute from the drop-down

menu, or enter the value of the email attribute. The entered value must be an AD attribute. By default, the following values are available as part of the drop-down menu:

- mail
- userPrincipalName

The default email attribute is **mail**.

3. In the **Phone number attribute** field, select the required phone attribute from the drop-down menu, or enter the value of the email attribute. The entered value must be an AD attribute. By default, the following values are available as part of the drop-down menu:
   - mobile
   - homephone

   The default email attribute is **mobile**.
4. Select the **Enable LDAP over SSL** option, to enable AD FS Adapter to communicate over secured LDAP connection with Active Directory server.
5. Click **Save Settings** after completing the configuration.

NOTE: If the attribute entered is invalid, an error message is displayed when you click **Save Settings**.

4

Upgrading Starling Two-Factor AD FS Adapter

This section describes the procedures that must be followed before upgrading One Identity Starling Two-Factor AD FS Adapter on Windows Server 2012 R2.

1. Launch the **AD FS Management** console on the primary server in the AD FS farm.
2. Navigate to **AD FS** | **Authentication Policies**, and click **Edit Global Multi-factor Authentication**. Alternatively, navigate to **Multi-factor Authentication** | **Global Settings**, and click **Edit**.
3. In the **Edit Global Authentication Policy** dialog box, click **Multi-factor**.
4. Clear the **Starling Two-Factor Authentication** method.

To upgrade the One Identity Starling Two-Factor AD FS Adapter, use the **StarlingTwoFactorADFSAdapter.exe file**, and follow the on-screen instructions. For information on the procedure to be followed after installing Starling Two-Factor AD FS Adapter, see Configuring AD FS Multi-factor Authentication.

IMPORTANT: In case of an upgrade to Starling Two-Factor AD FS Adapter 7.0, you must connect to Starling as the Subscription key related provision is removed. Connect to Starling using the credentials that were used to create the Starling account. You must configure the Push notification and AD attributes again, to overwrite the default values. For information on connecting to Starling, see Connecting Starling for authentication

5

Configuring AD FS Multi-factor Authentication

AD FS server must be configured to enable multi-factor authentication to communicate with the Starling Two-Factor Authentication AD FS adapter for two-factor authentication. If it is not configured, you cannot authenticate the users or groups trying to login to AD FS through Starling Two-Factor Authentication.

This section provides information on the configuration of AD FS Multi-factor Authentication on Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

To configure AD FS Multi-factor authentication on 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**.

   Alternatively, under **Multi-factor Authentication | Global Settings** section, click **Edit**.
3. In the **Edit Global Authentication Policy** dialog box, click **Multi-factor**.
4. In **Users/Groups** section, click **Add** and select an object for multi-factor authentication, for example, **Domain Users**.
5. In the **Locations** section, select the **Extranet** or **Intranet** option, based on the required type of connection.

   For example, if you always require two-factor authentication, select both Extranet and Intranet locations when configuring the multi-factor authentication policy.

   If you want to enforce two-factor authentication for external users and 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 **Extranet** only.

   > NOTE: In an advanced multi-factor scenario, you can choose either Intranet, Extranet, or both the options 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*.
6. In **Select additional authentication methods**, select **Starling Two-Factor**

Authentication.

7. Click **OK** to save the multi-factor authentication settings.

To configure AD FS Multi-factor authentication on Windows Server 2016 or Windows Server 2019

1. Launch the AD FS Management console on the primary AD FS internal server.
2. Navigate to **AD FS | Service | Authentication Methods**.
3. On the **Authentication Methods** pane, under **Multi-factor Authentication Methods**, click the **Edit** .

   Alternatively, in the **Actions** pane, click **Edit Multi-factor Authentication Methods**.
4. On the **Edit Authentication Methods** wizard, under the **Multi-factor** tab, select the **Starling Two-factor Authentication** option and click **OK**.
5. Navigate to **AD FS | Access Control Policies**.
6. On the **Access Control Policies** pane, edit one of the existing policies.

   Alternatively, create a new multi-factor authentication policy if a pre-defined policy is not sufficient for your organization's multi-factor authentication requirements.
7. Navigate to **AD FS | Relying Party Trusts**.
8. On the **Relying Party Trusts** pane, right-click the relying party trust, and select **Edit Access Control Policy**.
9. On the **Edit Access Control Policy for <*relying party trust*>** wizard, under **Access control policy**, select a policy for the relying party that includes multi-factor authentication, and then click **OK**.

   The multi-factor authentication policy is applied to the selected relying party.

6

Testing the setup

After completing required configurations on the AD FS Management Console and Starling Two-factor Authentication AD FS Adapter, you can test the setup for successful authentication.

To test the two-factor authentication for the relying party using AD FS Adapter

1. Use a web browser to log in to a relying party. For example, log in to Office 365 by using https://portal.microsoftonline.com.
2. Enter the required credentials to perform the primary authentication .

   After successful primary authentication, user receives an approval request on the Starling 2FA application. User can approve or deny the request. If the request is denied or timed out, user can request for another approval request or sign in with the token response obtained from SMS, Phone call, or the Starling 2FA application.

Diagnostic logging

To troubleshoot issues that may occur during authentication with Starling Two-Factor Authentication, you need to enable diagnostic logging for AD FS Adapter. By default, diagnostic logging is disabled.

NOTE: After enabling or disabling diagnostic logging, you must restart AD FS service.

Enabling diagnostic logging

To enable diagnostic logging for AD FS Adapter:

1. On a computer where Starling Two-Factor AD FS Adapter is installed, use the Registry Editor to create the following values in the **HKLM\SOFTWARE\One Identity\Starling Two-Factor AD FS Adapter** registry key:
    - Value type: **REG_DWORD**
    - Value name: **Diagnostics**
    - Value data: **1**
2. Restart the AD FS Adapter service.

The path to the log file: **%ProgramData%\One Identity\Starling Two-Factor AD FS Adapter\Diagnostics**

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

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

Disabling diagnostic logging

To disable diagnostic logging for AD FS Adapter:

1. On a computer where Starling Two-Factor AD FS Adapter is installed, in the **HKLM\SOFTWARE\One Identity\Starling Two-Factor AD FS Adapter** registry

key, delete the Diagnostics value or set the value data to **0** using the Registry Editor.

2. Restart the AD FS Adapter service.

8

Uninstalling Starling Two-Factor AD FS Adapter

The following section briefs about the steps to perform before you uninstall and to uninstall the **Starling Two-Factor AD FS Adapter**.

Before you uninstall the Starling Two-Factor AD FS Adapter

1. On the computer where Starling ADFS Adapter is installed, open the **Control Panel** and click **Administrative Tools**.
2. Click **AD FS Management**.
3. In the **AD FS** tree view, click **Authentication Policies**.
4. In the **Multi-factor Authentication** section, click **Edit**.
5. In the authentication methods, clear the **Starling Two-Factor Authentication** check box and click **Apply**.

To uninstall the **Starling Two-Factor AD FS Adapter**, from the control panel, uninstall the **One Identity Starling Two-Factor AD FS Adapter**.

After uninstalling the One Identity Starling Two-Factor AD FS Adapter, details regarding the Starling Two-Factor AD FS Adapter get deleted from the Starling account.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

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 at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product