One Identity Starling Two-Factor AD FS Adapter 6.0

Administrator Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.

Patents

Quest Software 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 www.quest.com/legal.

Trademarks

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.

Starling Two-Factor AD FS Adapter Administrator Guide
Updated - April 2017
Version - 6.0

Contents

1

Overview

One Identity Starling Two-Factor AD FS Adapter integrates with Microsoft Active Directory Federation Services (AD FS) 3.0 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, like Office 365, as well as SAML 2.0 federated logons for cloud applications like Google Apps and salesforce.com. Starling Two-Factor AD FS Adapter with AD FS 3.0 supports Windows Server 2012 R2.

Prerequisites

Before installing Starling Two-Factor AD FS Adapter, verify the following:

- Microsoft .NET Framework 4.6.1 or later is installed
- PowerShell 4.0 or later is installed
- AD FS role is installed and the AD FS service is running
- The federated logins to the relying parties are working
- A valid phone number and email id is configured in Active Directory for the user

Connectivity requirements

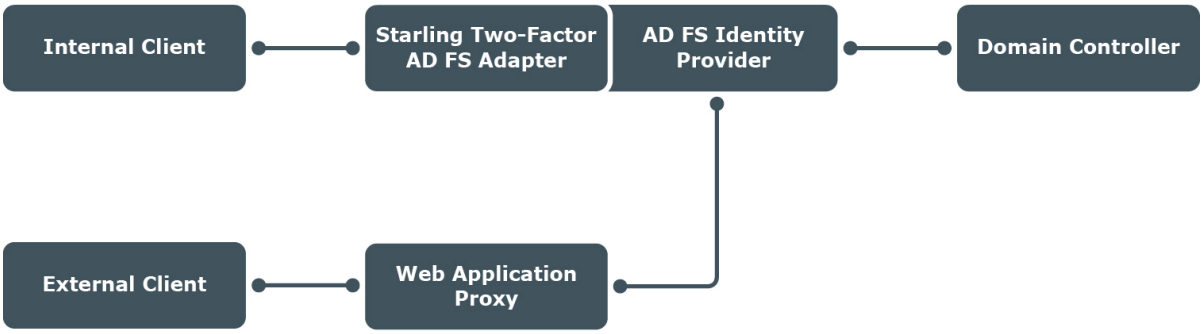
After verifying and setting up the prerequisites, do the following:

1. Request Starling Two-Factor Authentication subscription.
2. Log in to Starling Two-Factor Authentication Dashboard and get the subscription key (required for Starling Two-Factor AD FS Adapter installation).

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

Deployment Overview

Starling Two-Factor 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 Starling Two-Factor authentication challenge before getting redirected to the relying party. If the deployment is in an AD FS farm, install Starling Two-Factor AD FS Adapter on all AD FS servers in the farm.



After the installation of Starling Two-Factor 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 Starling Two-Factor AD FS Adapter on the Web Application Proxy server.

Running the installer

To run the installer:

1. Launch Starling Two-Factor AD FS Adapter installer MSI from an elevated command prompt or right-click **Command Prompt** and select **Run as Administrator**.
2. Accept the license agreement and continue with the installation.
3. Enter Starling Two-Factor Authentication subscription key obtained from **Starling Two-Factor Authentication Dashboard** page.

   NOTE: You can modify the parameters after installation as per the requirement. For more information, see Starling Two-Factor AD FS Adapter Configuration Settings.

4. Complete the remaining steps for installing Starling Two-Factor AD FS Adapter.

   NOTE: AD FS service will restart during installation.

Starling Two-Factor AD FS Adapter Configuration Settings

You can modify Starling Two-Factor AD FS Adapter configuration settings using Starling Two-Factor AD FS Adapter configuration tool.

Modifying the settings using configuration tool

To modify the settings using the configuration tool:

1. From the **Start** menu, open **Starling Two-Factor AD FS Adapter Configuration**.
2. Modify the required parameters. The available parameters are:
    - **Subscription key**: The subscription key obtained from Starling Two-Factor Authentication Dashboard. For details, see Connectivity requirements.
    - **Notification message**: The push notification message that has to be displayed on **Starling 2FA** application, when an approval request is received.
    - **Timeout in seconds**: The duration for which the push notification approval request, received on **Starling 2FA** application, is valid.
3. Click **Apply** to save the settings.

    NOTE: AD FS service will restart while saving the settings.

Configuring AD FS Multi-factor Authentication

To configure AD FS Multi-factor authentication:

1. Launch the **AD FS Management console** on the primary AD FS 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** dialog box, click **Multi-factor** tab.
4. In **Users/Groups** section, click **Add** and select a domain for MFA (for example, **Domain Users**).
5. In the **Locations** 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 locations 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. In **Select additional authentication methods**, select **Starling Two-Factor Authentication**.

   NOTE: In an advanced multi-factor scenario, you can choose 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*.

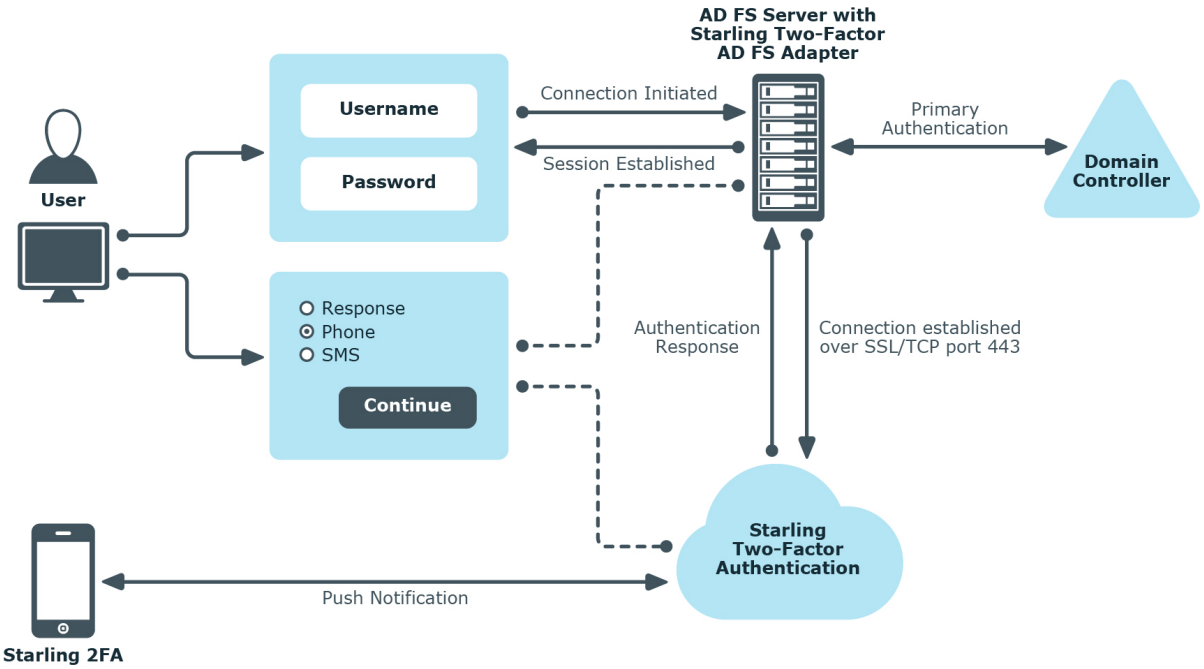
5

Testing the setup

To test your setup, do the following:

1. Use a web browser to 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. Starling Two-Factor Authentication enrollment or login prompt is displayed.
    - If push notification is enabled, 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 token response obtained from SMS, Phone call, or Starling 2FA application.
    - If push notification is not enabled, user can sign in with token response obtained from SMS, Phone call, or Starling 2FA application.

Network diagram



Diagnostic logging

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

- On a computer where Starling Two-Factor AD FS Adapter is installed, in the **HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Starling Two-Factor AD FS Adapter** registry key, create the following values using Registry Editor:
  - Value type: **REG_SZ**
  - Value name: **Diagnostics**
  - Value data: **1**

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

Disabling diagnostic logging

To disable diagnostic logging for Starling Two-Factor AD FS Adapter:

- Delete the Diagnostics value from **Starling Two-Factor AD FS Adapter** registry key or set the value data to **0**.

About us

Contacting us

For sales or other inquiries, visit www.quest.com/company/contact-us.aspx or call +1 949 754-8000.

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 Quest Support Portal at https://support.quest.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