Configuring Active Directory Federation Services Authentication for Laserfiche Directory Server

White Paper

April 2018

Laserfiche®

Table of Contents

Introduction 3
Configuring a Relying Party Trust in the AD FS Management Console 4
Turning On AD FS Authentication in Directory Server 7

Introduction

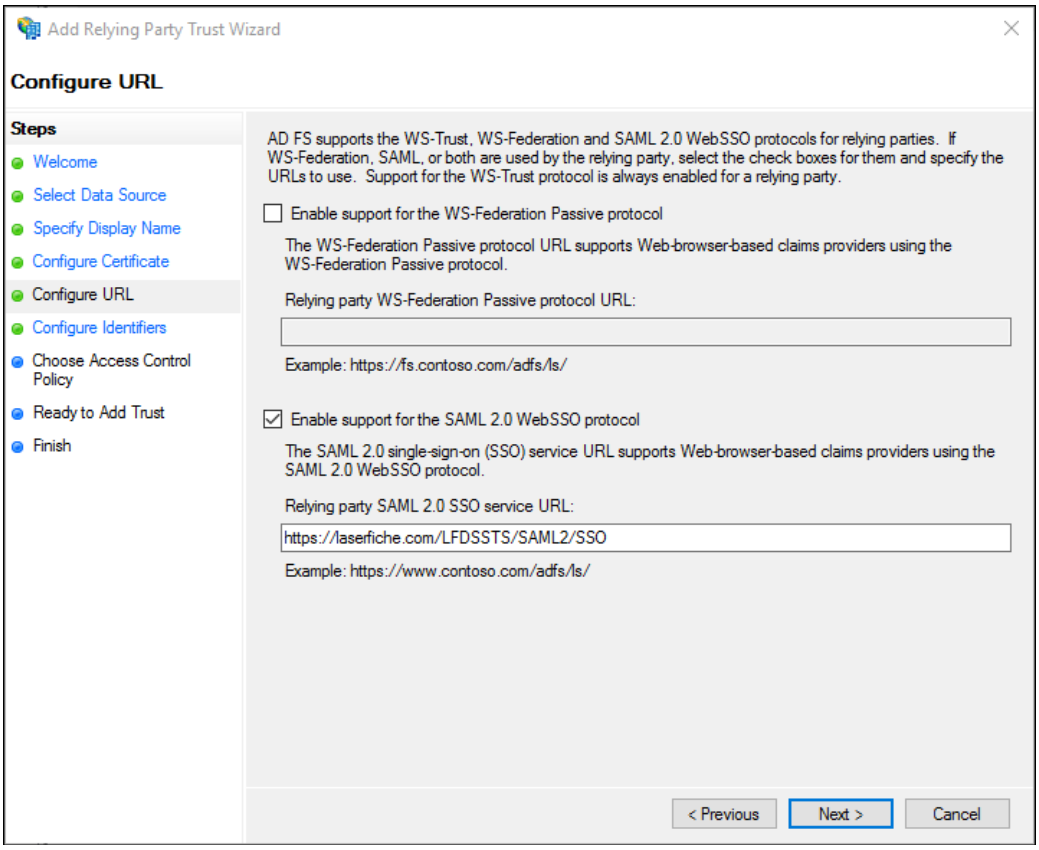
Active Directory Federation Services (AD FS) is a Windows feature that gives Active Directory users single sign-on access to services across organizational boundaries. Starting with Laserfiche Directory Server 10.2, administrators can configure Directory Server to allow users to authenticate using AD FS. Users can click **Sign in with AD FS** on the sign-in page to sign in to Laserfiche without specifying an additional user name and password. In this paper, we explain how to configure AD FS on Windows Server 2016 to enable AD FS to work with Directory Server. We also explain how to configure the Directory Server licensing site to allow users from certain identity providers to sign in using AD FS.

The AD FS sign-in option works well with having instances of the Security Token Service (STS) on computers other than the Directory Server computer, a feature available from Directory Server 10.2 onwards. Users can sign in using an STS instance that is on a computer they can access while Directory Server is hosted on a more secure network.

Configuring a Relying Party Trust in the AD FS Management Console

These instructions are based on a Windows Server 2016 AD FS server. We assume that the STS instance referred to is installed on a computer with the fully-qualified domain name *YourSTSmachine.com*. You have to configure a relying party trust for every STS instance for which you want to enable AD FS authentication.

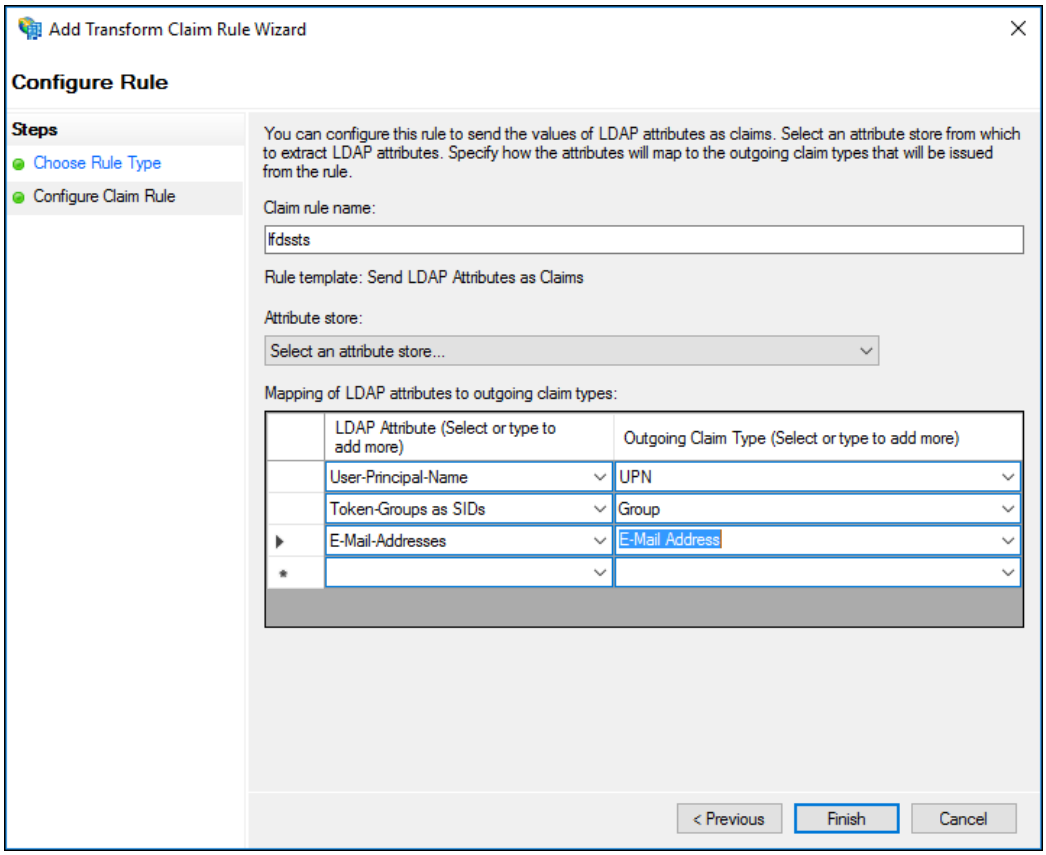
1. On the AD FS server, navigate to the AD FS Management Console from the Windows start menu by selecting **Windows Administrative Tools**, then **AD FS Management**.
2. Right-click on the **Relying Party Trusts** node in the left pane, and select **Add Relying Party Trust…**.
3. On the Welcome screen, choose to add a **Claims aware** relying party trust, and click **Start**.
4. In the **Select Data Source** step, select the **Enter data about the relying party manually** option. Click **Next.**
5. Specify a display name for Directory Server, and notes if desired. Click **Next**.
6. You can skip the option to specify a token encryption certificate, and simply click **Next**.
7. In the **Configure URL** step, select **Enable support for the SAML 2.0 WebSSO protocol**. Specify the following SSO service URL, making sure to begin with "https": https://*YourSTSmachine.com*/LFDSSTS/SAML2/SSO



Click **Next** to continue.

8. In the "Configure Identifiers" step, do one of the following:
    - **Directory Server 10.2:** add **https://*YourSTSmachine.domain.com*** as the relying party trust identifier.
    - **Directory Server 10.3:** add ***https://YourSTSmachine.domain.com/lfds*** as the relying party trust identifier.
9. In the "Choose Access Control Policy" dialog, choose an access control policy and click **Next**.
10. In the "Ready to Add Trust" dialog, you can check your settings and go back to change them if required. Click **Next** to finish creating the relying party trust.
11. Once your relying party trust is created, it should be listed in the Relying Party Trusts pane in the AD FS Management Console. Add a claim rule to your trust as follows:
    - Right-click on your relying party trust and select **Edit Claim Issuance Policy**.
    - Select **Add Rule**… to add a claim rule.
    - In the "Select Rule Template" dialog, select **Send LDAP Attributes as Claims** as the claim rule template. Click **Next.**
    - Assign a name to your claim rule. Select **Active Directory** as your attribute store.

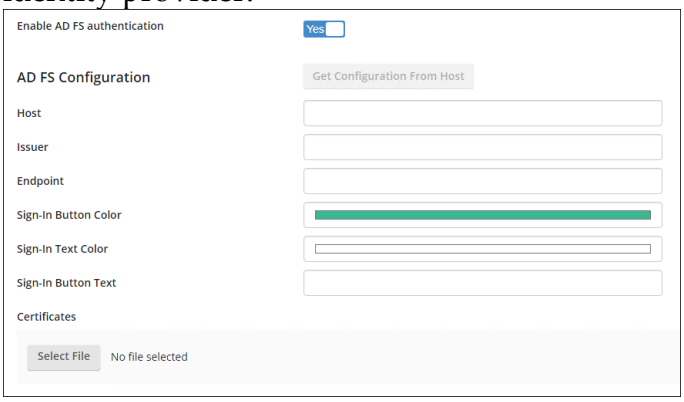
- Now you can decide which LDAP attributes to add. First, you must add the LDAP attribute **User-principal-name,** with the outgoing claim type **UPN**.



- **Directory Server 10.3:** Add the LDAP attribute **SAM-Account-Name**, with the outgoing claim type **Name ID**.
- **Directory Server 10.3:** Add the LDAP attribute **objectSid**, with the outgoing claim type **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sid**.
- Add the LDAP attribute **Token-Groups as SIDs**, with the outgoing claim type **Group**. This is required if AD groups are used for controlling access to a repository, granting entry access rights, and so on.
- Add the LDAP attribute **E-Mail-Addresses**, with the outgoing claim type **E-Mail Address**. This is required if you want users' email addresses to be synchronized in Directory Server so that Laserfiche applications like Forms can send emails to users.
- Click **Finish** to save the rule, then **OK** to implement the rule.

Turning On AD FS Authentication in Directory Server

1. On the Directory Server licensing site, navigate to the **Settings** tab and select **Identity Providers**.
2. In the left pane, select the identity provider that you want to enable AD FS authentication for. Scroll down to the "AD FS Configuration" section for that identity provider.



3. Turn the **Enable AD FS authentication** switch to **Yes**.
4. For **Host**, enter your **Federation Service name**. If you do not know what this, open the AD FS Management Console on your AD FS server, following the previous instructions. Right-click on the **Service** node and select **Edit Federation Service Properties…**.

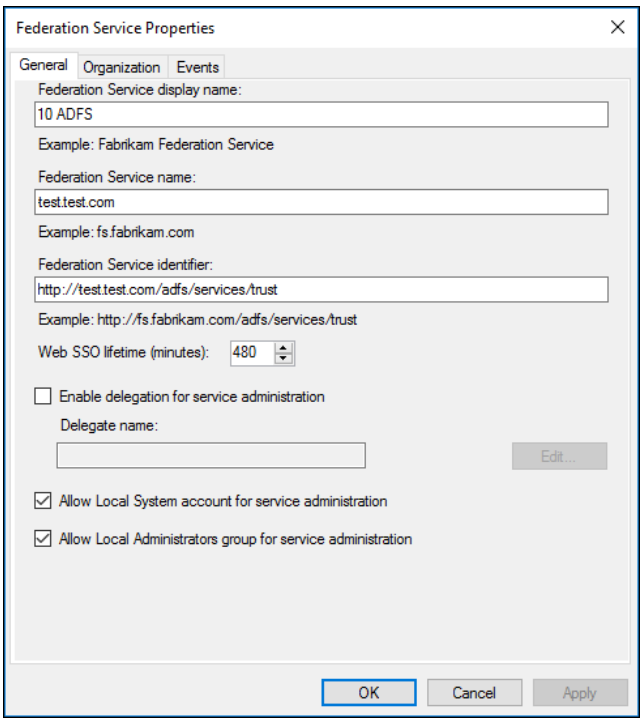
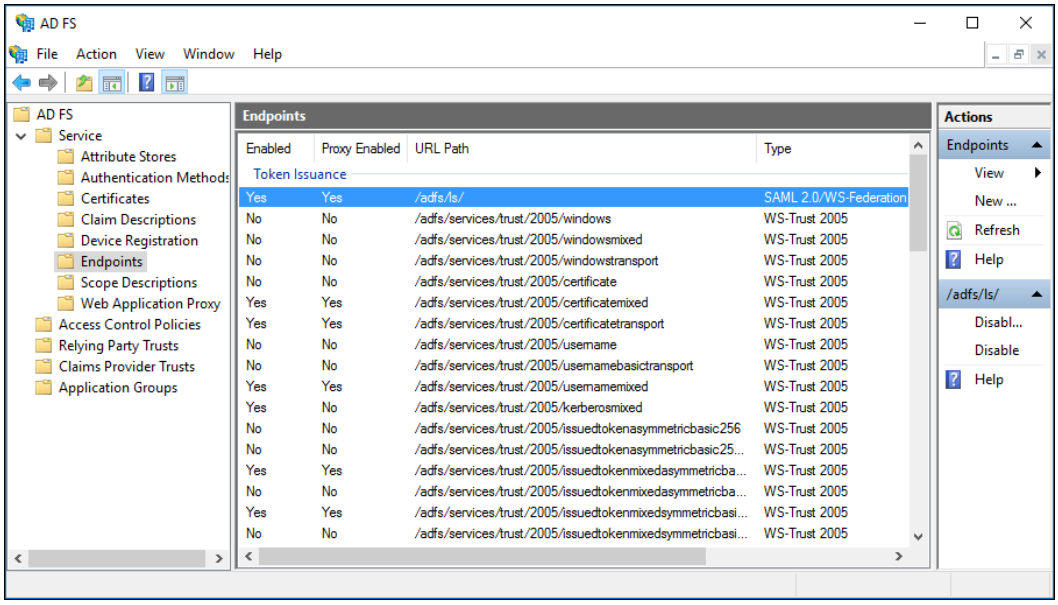
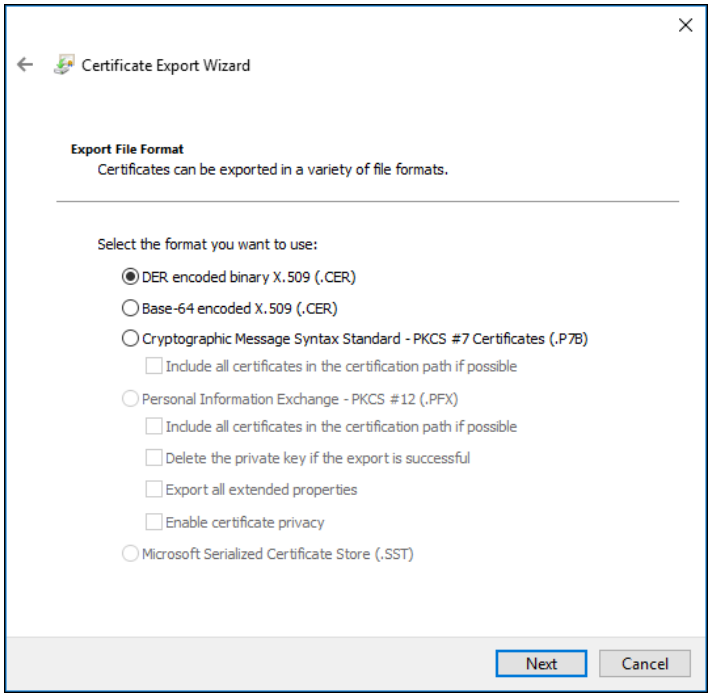


Figure 1: Federation Service Properties

5. After entering the **Host** details, Laserfiche highly recommends that you obtain the other configuration details by clicking **Get Configuration From Host**. This will automatically fill in the **Issuer**, **Endpoint**, and **Certificates** details for you. Once you do this, all you need to do is click **Save** at the bottom of the Directory Server Identity Providers page to save your configuration details.
6. If you choose to enter the configuration details manually, further steps are required:
    a. For **Issuer**, enter your **Federation Service identifier**, which is in the Federation Service Properties dialog box depicted in Figure 1.
    b. For **Endpoint**, enter the URL with type SAML 2.0/WS-Federation that is listed in the AD FS Management Console under **Service → Endpoints**. The URL path listed here is relative to the local server, so make sure to add the fully-qualified domain name of your ADFS server before the path when you enter the URL in Directory Server. In the screenshot, the URL Path listed is /adfs/ls, so we will enter http://*ADFSServer.com*/adfs/ls as the **Endpoint** in Directory Server.



c. For the certificate, you will need to export and upload the token-signing certificate from your AD FS server.
   i. In the AD FS Management Console, navigate to **Services → Certificates.**
   ii. Right-click on the token-signing certificate and select **View Certificate...**.
   iii. Click on the **Details** tab and select **Copy to File…**.
   iv. In the Certificate Export Wizard, select either of the .CER formats and click **Next**.



v. Specify the path to which you want to save the exported certificate. Click **Next**.
vi. Click **Finish** to exit the Certificate Export Wizard.
vii. Back in the Directory Server configuration page, click **Select File** under "Certificates" to upload your certificate from where you saved it.

Note: The certificate must be able to pass chain trust validation on the STS instance (i.e., if the certificate is a self-signed certificate, you must add the certificate in the trusted root store in the STS machine).

---

d. Click **Save** at the bottom of the Directory Server Identity Providers page to save your configuration.

7. **Directory Server 10.3:** navigate to the **Settings** tab and select **STS Sites**. Add the STS instance used for AD FS (e.g., *https://YourSTSmachine.com/LFDSSTS/SAML2/SSO*). Note that this value is case-sensitive.
8. Repeat Steps 2-7 for each identity provider for which you want to enable AD FS authentication.
9. **Directory Server 10.3:** Directory Server supports AD FS single sign-on to 1 licensing site. If you have multiple licensing sites attached to your Directory Server instance, you must specify a default licensing site for AD FS single sign-on to function properly. Manually edit the LFDS.exe.config file in the Directory Server installation folder to add a default licensing site. In the **<appSettings>** block, insert the following line:

```
<add key="DefaultRealm" value="SampleLicensingSiteName" />
```

After saving your change, restart the Directory Server service.

Laserfiche®

Configuring Active Directory Federation Services Authentication for Laserfiche Directory Server
April 2018

Author: Leif Hancox-Li
Editor: Roger Wu
Technical Editor: Rufei Huang

Description:
Active Directory Federation Services (AD FS) allows users to sign in to Laserfiche with single sign-on when services cross organizational boundaries. This paper explains how you can configure AD FS authentication for Directory Server.

Laserfiche
3545 Long Beach Blvd.
Long Beach, CA 90807
U.S.A

Phone: +1.562.988.1688
www.laserfiche.com

Laserfiche, Compulink, and Run Smarter are registered trademarks of Compulink Management Center, Inc. dba Laserfiche. All other trademarks are properties of their respective companies.

Compulink Management Center, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties, merchantability, or fitness for any particular purpose. Furthermore, Compulink Management Center, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Copyright 2018 Laserfiche