AVAIL™

AVAIL & On-Premises Active Directory Integration

Reference & Instruction Guide

AVAIL™ & Active Directory Integration

Reference & Instruction Guide

Version: 20200520

Table of Contents

Overview

This document will guide you through the necessary steps for installing and configuring Active Directory Federation Services (ADFS) for your organization and integrating it with AVAIL. For further information or assistance in going through this guide, you can contact AVAIL Support at support@getavail.com.

Why Active Directory Federation Services (ADFS)?

Active Directory Federation Services (ADFS) is a claims-based, access-control service developed by Microsoft. It provides users managed by your organization's Active Directory with Single Sign-On (SSO) access to claims-aware systems and applications located across your organizational boundaries.

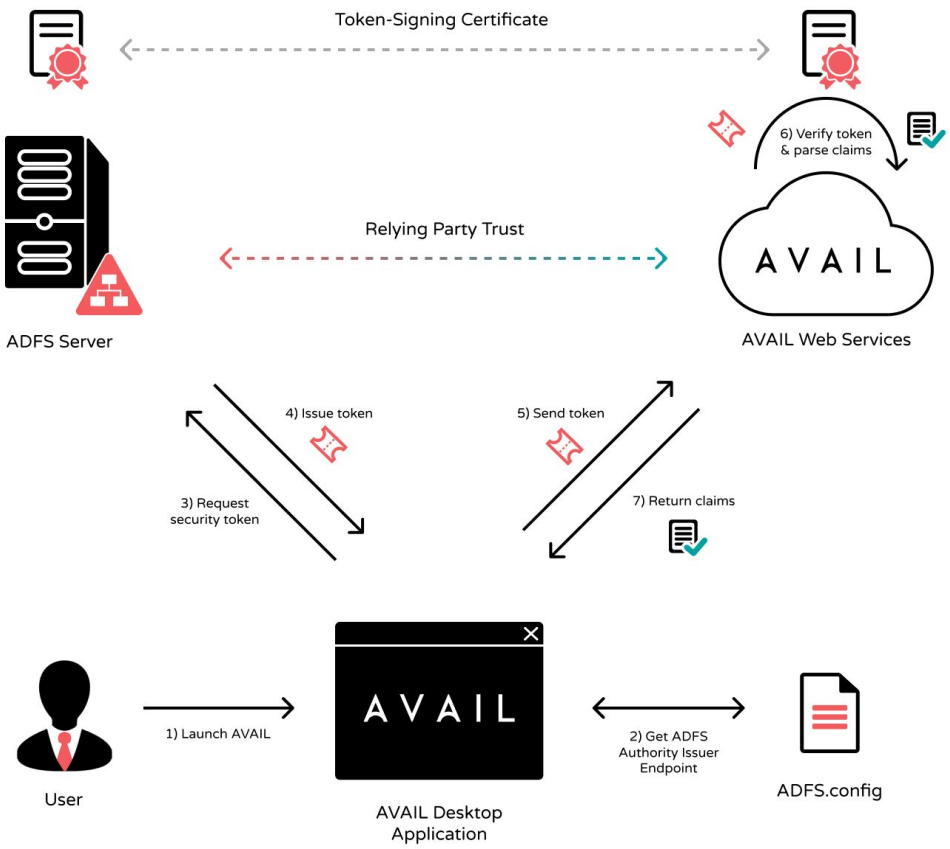
The primary benefit of ADFS is that it enables organizations to collaborate securely across Active Directory domains by using identity federation. Federation allows SSO without passwords. This eliminates the need for duplicate accounts and other credential management overhead by enabling federated SSO across organizations, platforms, and applications, such as AVAIL.

This means that users within your organization will not need to register or create accounts with AVAIL. An administrator will not need to perform any user and role management within your AVAIL plan. Instead the identity of the user and what particular operations that user can perform within the AVAIL platform is all provided by your existing Active Directory.

Your ADFS & AVAIL

Your federation server will contain a trust relationship with AVAIL. Because of this trust relationship, AVAIL is able to accept this token and authenticate the user. By default, your federation server will use a token-signing certificate to digitally sign all security tokens that it produces. Because each security token is digitally signed by your ADFS Server, AVAIL can verify that the security token was in fact issued by you and that it was not modified. This helps prevent attackers from forging or modifying security tokens to gain unauthorized access to resources.

(1) When a user launches the AVAIL application on their workstation, (2) AVAIL retrieves the necessary authority issuer endpoint for (3) requesting a security token from your ADFS. (4) ADFS provides a token that contains information about the user requesting access to AVAIL then (5) sends the token to the AVAIL web service. (6) Once the token is verified, AVAIL will parse the claims extracted from the token and determine what actions the user is authorized to perform, and then (7) return those as claims back down to the AVAIL application.



Installing ADFS

In this chapter, you will be installing ADFS on your Windows Server.

If you already have an ADFS installed, skip ahead to the Requesting & Installing an SSL Certificate chapter.

Prior to Installing ADFS

Before beginning the ADFS installation process, here are some resources to get yourself acquainted with SSO and Active Directory Federation Services:

- Have you done an SSO integration before?
    - Overview: https://technet.microsoft.com/en-us/library/cc755226(v=ws.11).aspx
- Do you have an SSL certificate for securing the ADFS Server?
    - **You will need an SSL certificate.** If your organization does not have one, we recommend purchasing a certificate from an authorized reseller. There are many SSL certificate resellers available, so choose one that works best for your organization.
    - Typically you will receive a signed certificate in 1 or 2 business days from the time your request is received and any necessary validation has been completed.
    - **Wildcard SSL certificates** are supported by all versions of ADFS and are generally recommended for ease of installation. Please verify that it complies with your corporate policy.
    - This certificate needs to be one that all workstations will trust. To generate an SSL certificate through IIS 7 management console, follow this URL: https://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx
- Is the ADFS role currently installed?
    - You can go to Administrative tools, and look for **ADFS Management**. You can also check by going to **Server Manager** and looking at roles. Do you see **ADFS (Active Directory Federation Services)**?

Windows Server

For ADFS to function properly, the computer that will operate as the federation server must be joined to your domain. The version of ADFS that you will be using is dependent on the version of Windows Server that is installed on this machine. For Windows Server 2008 R2, you will need to download the ADFS 2.0 installer. You can install ADFS 3.0 and 4.0 on Windows Server 2012 R2 and Windows Server 2016 respectively through the Server Manager.

If you are installing ADFS on a Domain Controller or want to use a different Fully Qualified Domain Name (FQDN) for ADFS than the server name, you will need to ensure the name you enter has a DNS Record created. We do recommend that the name of the target server and the federation service name that you will configure for ADFS be different values.

Windows Server 2008 R2 (ADFS 2.0)

- ADFS 2.0 requires **Windows Server 2008 R2 Service Pack 2.**
- If you're upgrading from ADFS 1.0 to ADFS 2.0, you will need to uninstall ADFS 1.0 first, which will require a reboot.
- You can download the ADFS 2.0 installer from the following link:
    - https://www.microsoft.com/en-us/download/details.aspx?id=10909
    - Run the setup program. The only thing you will need to be sure of, is to check **New Federation Server**, not **Proxy** during the installation process.
- For additional reference material, there are Step-by-Step and How To Guides available for ADFS 2.0 available at the following link:
    - https://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides(v=ws.10).aspx
- For an overview of ADFS 2.0 for Windows Server 2008 R2, please visit the following link:
    - https://technet.microsoft.com/en-us/library/cc755226(v=ws.11).aspx

Windows Server 2012 R2 (ADFS 3.0) & 2016 (ADFS 4.0)

- For a complete overview of Active Directory Federation Services, please visit:
    - https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services
- The following are basic instructions on how to install Active Directory Federation Services from Server Manager in Windows Server 2012 R2:
    - Open **Server Manager** and click **Add roles and features**.
    - Choose **Role-based or feature-based installation** and click **Next**.
    - Check **Active Directory Federation Services**, choose **Add Features**, and click **Next**.
    - On the **Features** menu, select **.NET Framework 3.5 Features**.

    - Click **Next** until you get to the **Role Services** menu. Leave everything but **Federation Service** unchecked and click **Next**.
    - Click **Next** until you get to the confirmation screen and click **Install**. Click **Close** when the installation is done.
- For additional reference material on ADFS 4.0 for Windows Server 2016, please visit the following link:
    - https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/install-the-ad-fs-role-service
- Overall Reference**:**
    - https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/deploying-a-federation-server-farm

Requesting & Installing an SSL Certificate

In this chapter, you will be using Microsoft Internet Information Services (IIS) Manager to generate a Certificate Signing Request (CSR), uploading the CSR to a Certificate Authority (CA) of your choice and installing your SSL certificate in the Personal Store on your Windows ADFS Server.

If you already have an SSL certificate, skip ahead to the Configuring ADFS chapter.

Federation Server Certificates

ADFS requires a standard Secure Sockets Layer (SSL) Certificate and is used for securing communications between federation servers and clients. The following are some requirements and information for the certificate (See here):

- Must be a **publicly trusted X509 v3 certificate** from a third-party certificate authority. All clients that access any ADFS endpoint must trust this certificate.
- **Wildcard certificates** are supported. If you choose to use a wildcard certificate, you will still need to provide the fully qualified domain name for the ADFS service (e.g. **adfs.mycompany.com**) when you configure your ADFS federation farm.
- The Subject name of this certificate is used to represent the Federation Service name for each instance of ADFS that you deploy. You may want to consider choosing a Subject name on any new CA-issued certificates that best represents the name of your company or organization to partners. The identity of the certificate must match the federation service name (for example, **adfs.mycompany.com**).
    - The identity is either a subject alternative name extension of type dNSName or, if there are no subject alternative name entries, the subject name specified as a common name. Multiple subject alternative name entries can be present in the certificate, provided one of them matches the federation service name.

Create Certificate Signing Request

ADFS doesn't include a straightforward way for creating a Certificate Signing Request (CSR). You can create your CSR using Microsoft IIS Manager.

- On your Windows ADFS Server, open **Internet Information Services (IIS) Manager**.
- In **IIS Manager**, under **Connections** located on the left side, select your server's hostname.
- In the center menu under the **IIS** section, double-click the **Server Certificates** icon.
- In the **Actions** menu located on the right, click **Create Certificate Request** to open the **Request Certificate** wizard.
- Once the wizard launches, you will see a **Distinguished Name Properties** page. Enter the following information:

Attribute	Description
Common Name	The **fully-qualified domain name** (or URL) for which you plan to use your certificate. ● An SSL certificate issued for **www**.mycompany.com is not valid for **adfs**.mycompany.com. If you want your SSL to cover **adfs**.mycompany.com, make sure the common name submitted in the CSR is **adfs**.mycompany.com ● If you are requesting a **wildcard certificate**, add an asterisk (*****) on the left side of the common name (e.g. *****.mycompany.com)
Organization	The legally registered **name of your organization or company**
Organizational Unit	The **name of your department** within your organization (e.g. "*IT*" or "*Engineering*")
City/locality	The full **name of the city or locality** in which your organization is located (Do not abbreviate)

State/province	The full **name of the state or province** where your organization is located (Do not abbreviate)
Country/region	Your two-digit ISO-format country code

- Click **Next.**
- On the **Cryptographic Service Provider Properties** section of the wizard:
    - For **Cryptographic Service Provider**, select **Microsoft RSA SChannel Cryptographic Provider**
    - For **Bit Length**, select **2048** or higher.
- Click **Next.**
- On the **File Name** page, click **...** to select a location to save the CSR file. Enter the filename, then click **Open**.
    - If you only enter the filename without selecting a location, the CSR file is saved to *C:\Windows\System32*
- Click **Finish.**

It is strongly recommended to use certificates that are issued by a public (third-party) certification authority (CA). Please review and follow the instructions provided by the preferred CA of your choice on completing an SSL certificate request and how to download the certificate once it is approved.

Most CA providers will require you to open the file you had just generated with a text editor and copy/paste the entire contents of that file into an order form. For most CA providers, you will typically receive a signed certificate within 1 or 2 business days from the time your request is received and any necessary validation has been completed.

Import the Signed Certificate

Now that you have received your SSL Certificate, you will now need to import it onto the server where ADFS was installed.

- From the server, open **Microsoft Management Console (MMC).**
- Click **File,** then **Add/Remove Snap In...**
- Under **Available snap-ins** (left side), click **Certificates.**
- With **Certificates** selected, click the **Add >** button in the center to launch the **Certificates snap-in** wizard.
    - Select **Computer Account,** then click **Next.**
    - Select **Local computer** and click **Finish**.
    - When the **Certificates snap-in** is added to the right pane, click **OK.**
- Once the console is open, expand the **Certificates** item and right click on **Personal.**
- Select **All Tasks > Import...**
- The **Certificate Import Wizard** will launch. Click **Next** to continue.
    - Click the **Browse...** button to select the signed certificate file (.cer)
    - Click **Next.**
    - Place the certificate in the **Personal Certificate store.**
    - Click **Next.**
    - Click **Finish** to import the certificate.

Configuring ADFS

Getting Started

The steps outlined in this section are targeted towards the installation of an **on-premises ADFS 2.0** for **Windows Server 2008 R2**, but many of the steps for configuring **ADFS 3.0 and ADFS 4.0** on higher versions of Windows Server are applicable. Please read through the steps in this guide for important notes that apply to higher versions of ADFS.

- For **Windows Server 2008 R2 (ADFS 2.0)**, please continue to the Running the ADFS Configuration Wizard section.
- For **Windows Server 2012 R2 (ADFS 3.0)** or **Windows Server 2016 (ADFS 4.0)**, please review the information at the following link:
    - https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-a-federation-server

Running the ADFS Configuration Wizard

In this section, we will run the ADFS Configuration Wizard for creating a new Federation Service and Federation Server Farm, importing your SSL certificate and setting up and configuring a service account. If ADFS was already installed, skip this section and go to Configure Service Endpoints.

1) Launch **ADFS 2.0** from the Administrative Tools.
2) Select **ADFS 2.0 Federation Server Configuration Wizard** on the overview screen.
3) On the Welcome screen, select **Create New Federation Service**.
4) Always say **Yes** to **New Federation Server Farm**.
5) Select an SSL certificate.
    a) If there is no certificate, you will need to create an SSL certificate. This certificate needs to be one that all workstations will trust.
    b) If you do not have an SSL certificate, the recommendation would be to purchase a certificate from an authorized reseller.
    c) ADFS can accept a Self-Signed Server Certificate and will work fine in a testing environment, but **you will need to generate an SSL certificate for production**. To generate a Self-Signed Certificate through IIS 7 Manager, follow the instructions at this link: https://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx
    d) To generate your SSL certificate through IIS 7 management console, visit the Installing SSL Certificate chapter of this document.
6) Note: If you are installing ADFS on a Domain Controller or want to use a different Fully Qualified Domain Name (FQDN) for ADFS than the server name, you will need to ensure the name you enter has a DNS Record created. We do recommend that the name of the target server and the federation service name that you will configure for ADFS be different values.
7) Next, setup a dedicated service account located in the organization.
    a) You will be creating a new account that represents this ADFS service. This account is necessary for the Kerberos authentication protocol to work in a farm scenario and to allow pass-through authentication on each of the federation servers.
    b) We recommend "**adfsservice**" as the name of the account.
    c) Set the first and last name, and make sure to check **Password never expires**.
    d) This account does not require any special permissions to be set by you. The ADFS Configuration Wizard will grant this service account the SeServiceLogonRight and the SeAuditPrivilege permissions automatically.
8) Additionally, the SPN (Service Principal Name) must be set manually. Run the following in Command Prompt:
    a) **setspn -a host/[your_federation_service_name] [service_account]**

b) **Example**: If the name of the account was **adfsservice,** then it might look like:
setspn -a host/**adfs.mycompany.com adfsservice**

9) Finish the wizard and relaunch the ADFS 2.0 Management Console.

Configure Service Endpoints

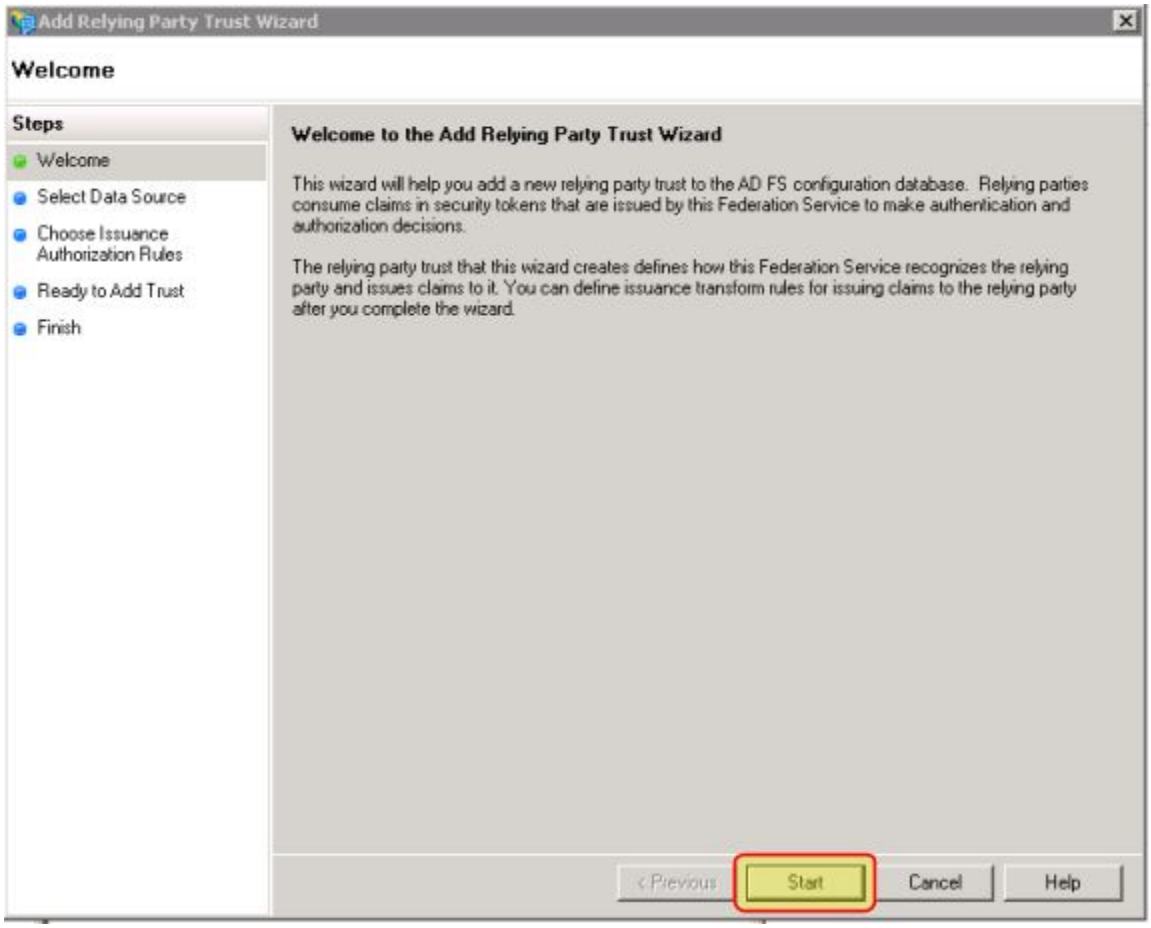
In this section, we will enable the Windows authentication endpoint that will allow AVAIL to retrieve SAML tokens from your ADFS using the user's Windows credentials. This is done over the WS-Trust 1.3 Protocol using Transport Security with a Message Credential.

1) On the left hand navigation, select **Service** and expand, then select **Endpoints**.
2) Look for **adfs/services/trust/13/windowsmixed**, then right-click and enable that endpoint.
3) Restart ADFS.
    a) Close the ADFS 2.0 management Console.
    b) Open **Services** and find **ADFS 2.0 Windows Service**.
    c) Right-click this service and select **Restart**.
4) Relaunch the ADFS 2.0 Management Console.

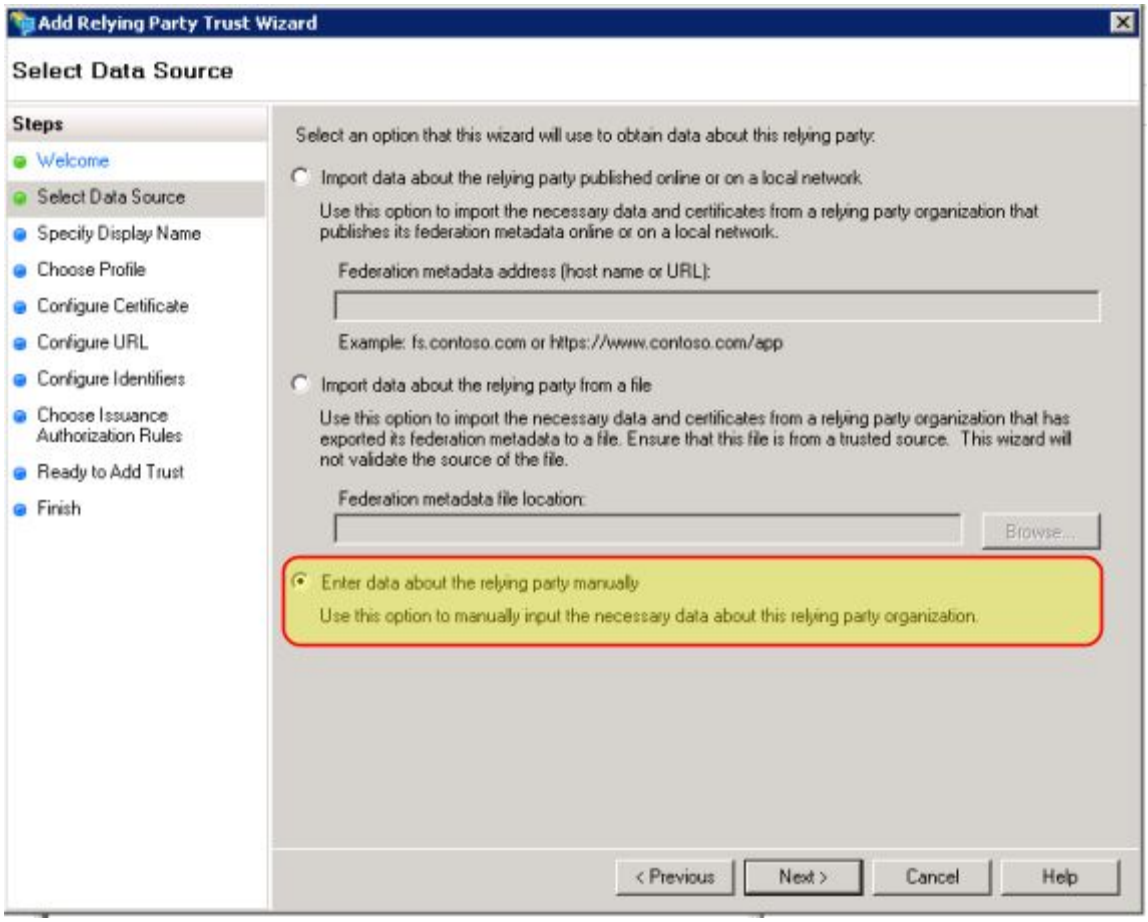
Configure Relying Party

In this section, we will configure AVAIL as a trusted relying party to your ADFS. This allows AVAIL to consume claims in security tokens issued by your ADFS for authentication and authorization.

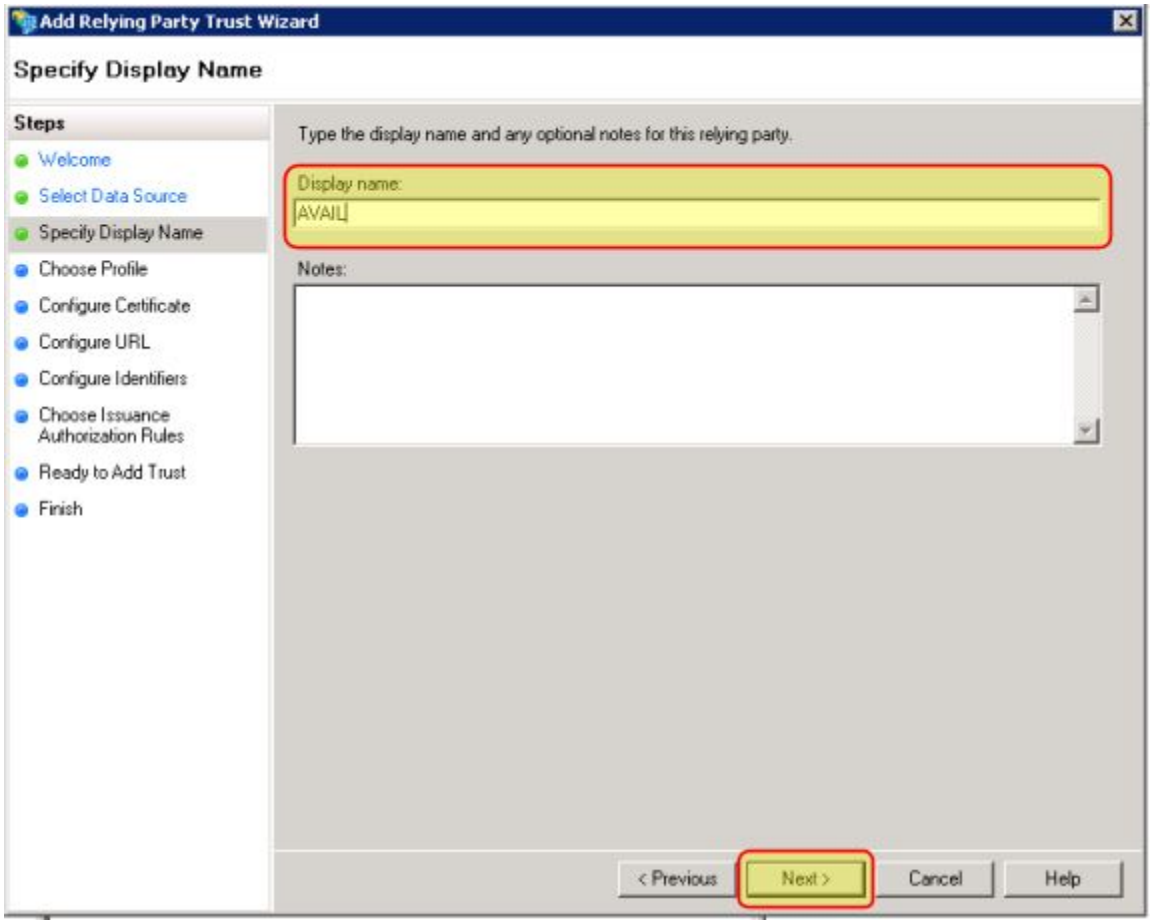
1) From the left side navigation in the ADFS Management Console, select **Trust Relationships**.
2) Expand and select **Relying Party Trusts**.
3) Right-click and select **Add Relying Party Trust**.
    a) For ADFS 4.0 select **Claims Aware**.
4) From the first screen of the wizard (the **Welcome** step), select **Start**.



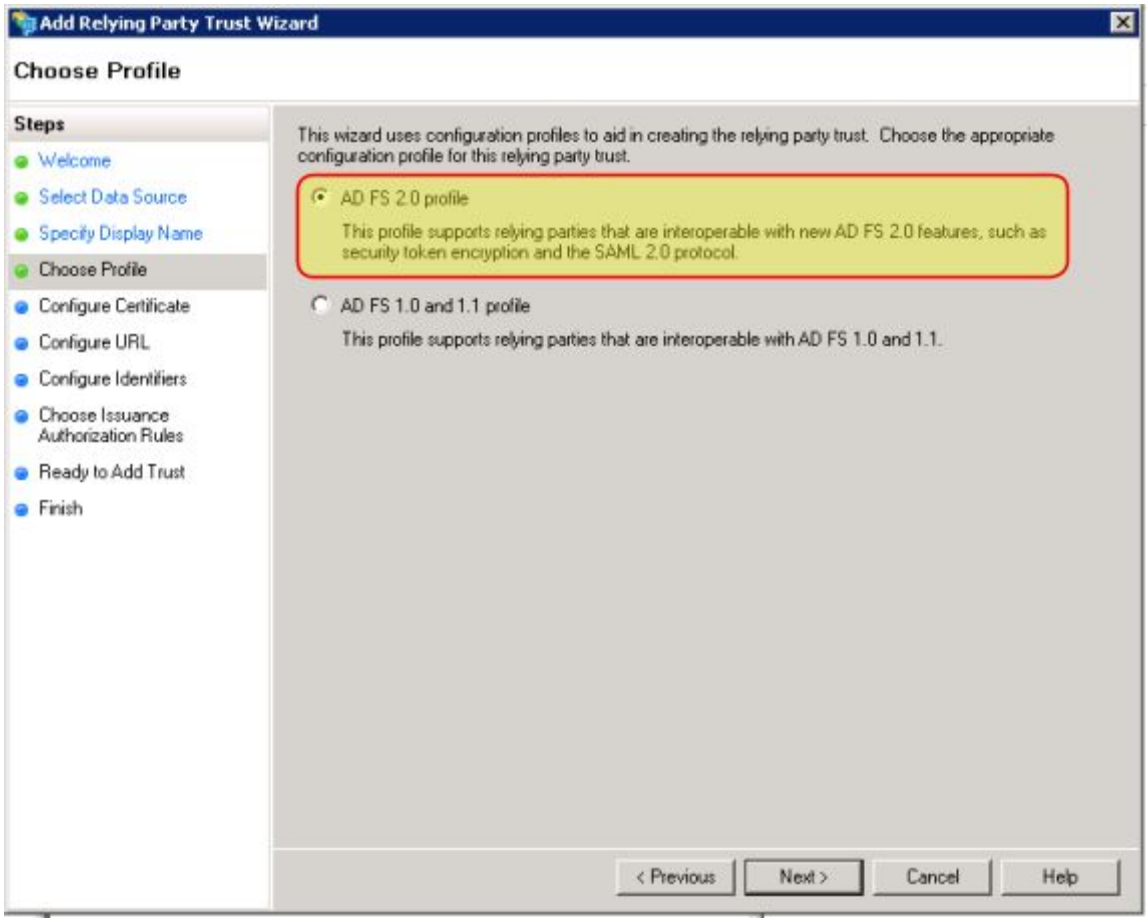
5) Select the **Enter Data about the relying party manually** option.



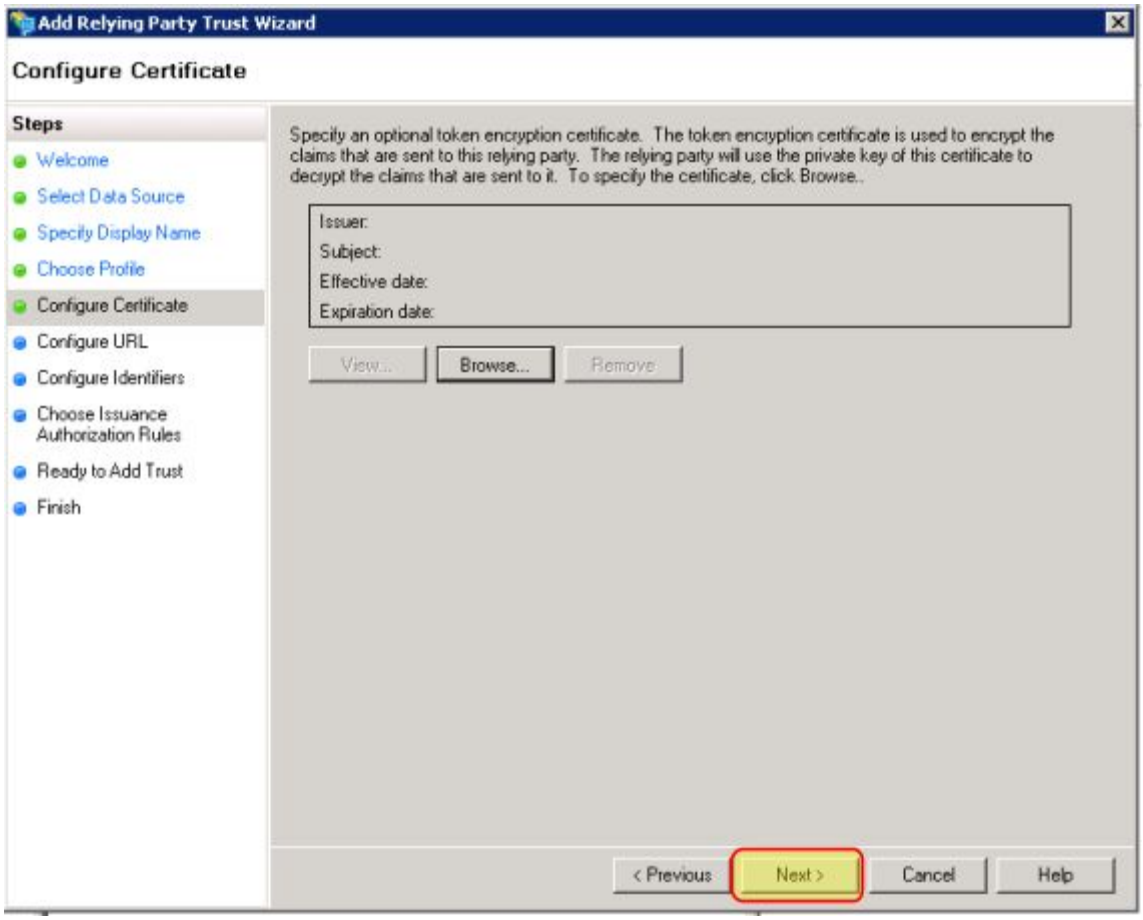
6) For display name, enter “AVAIL”.



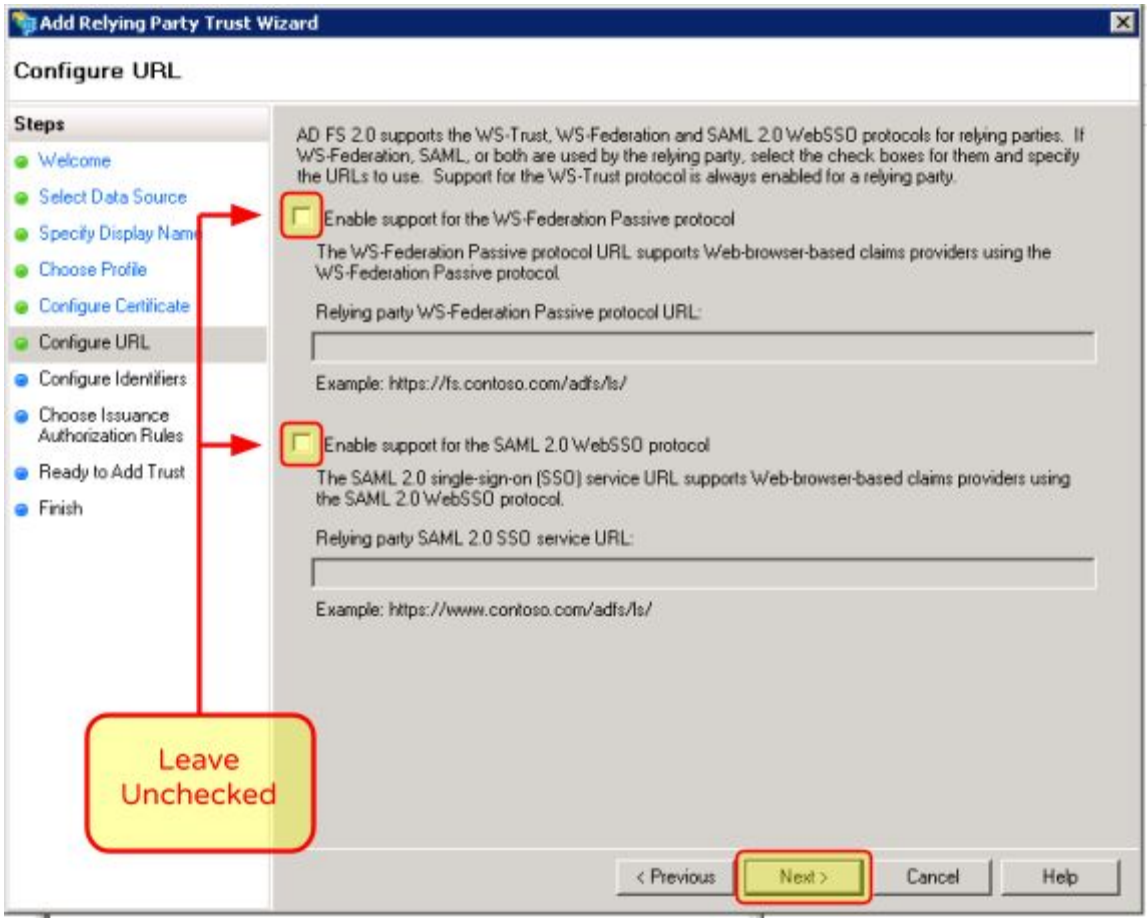
7) Select **ADFS 2.0 Profile**. Click **Next**. (For newer versions of ADFS, this step is skipped)



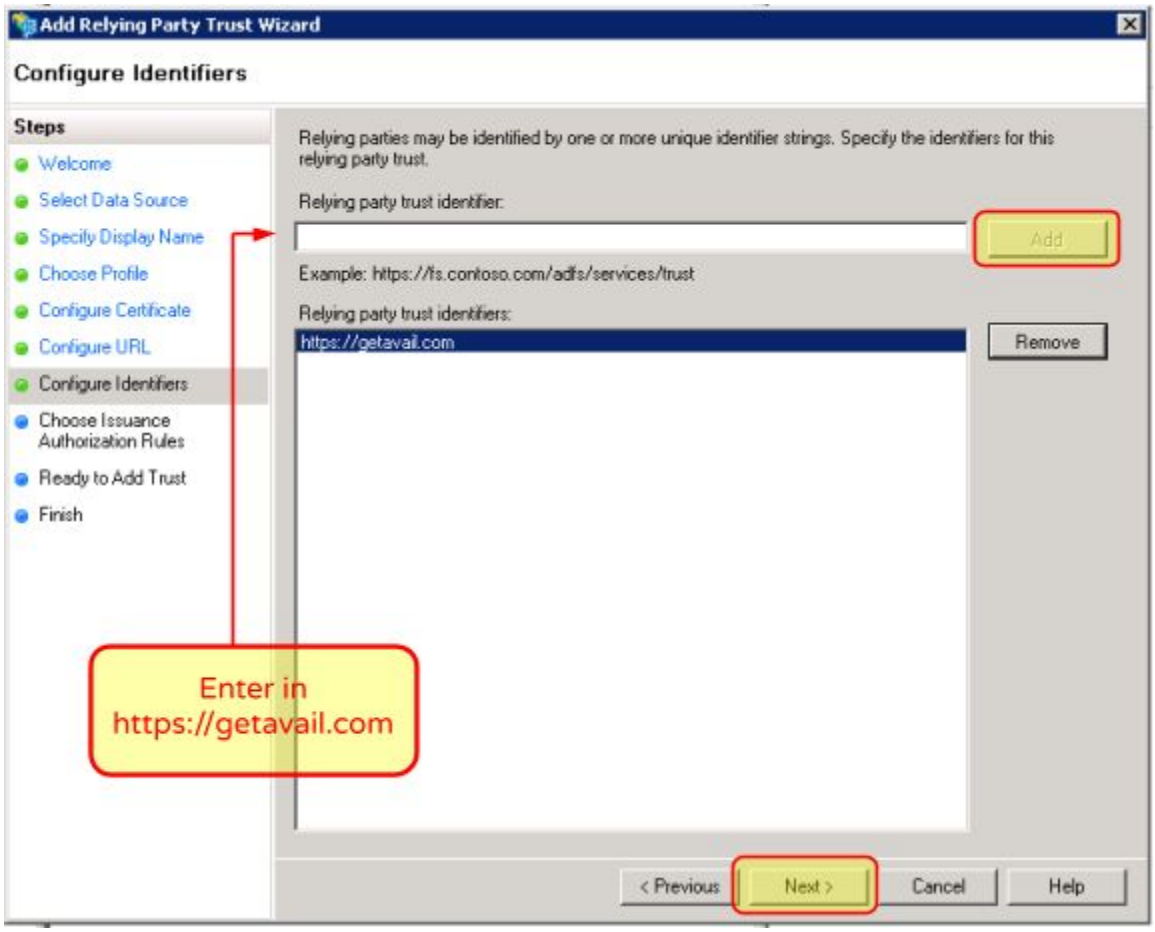
8) Do not select anything for a token encryption certificate. Leave this section blank, and select **Next**.



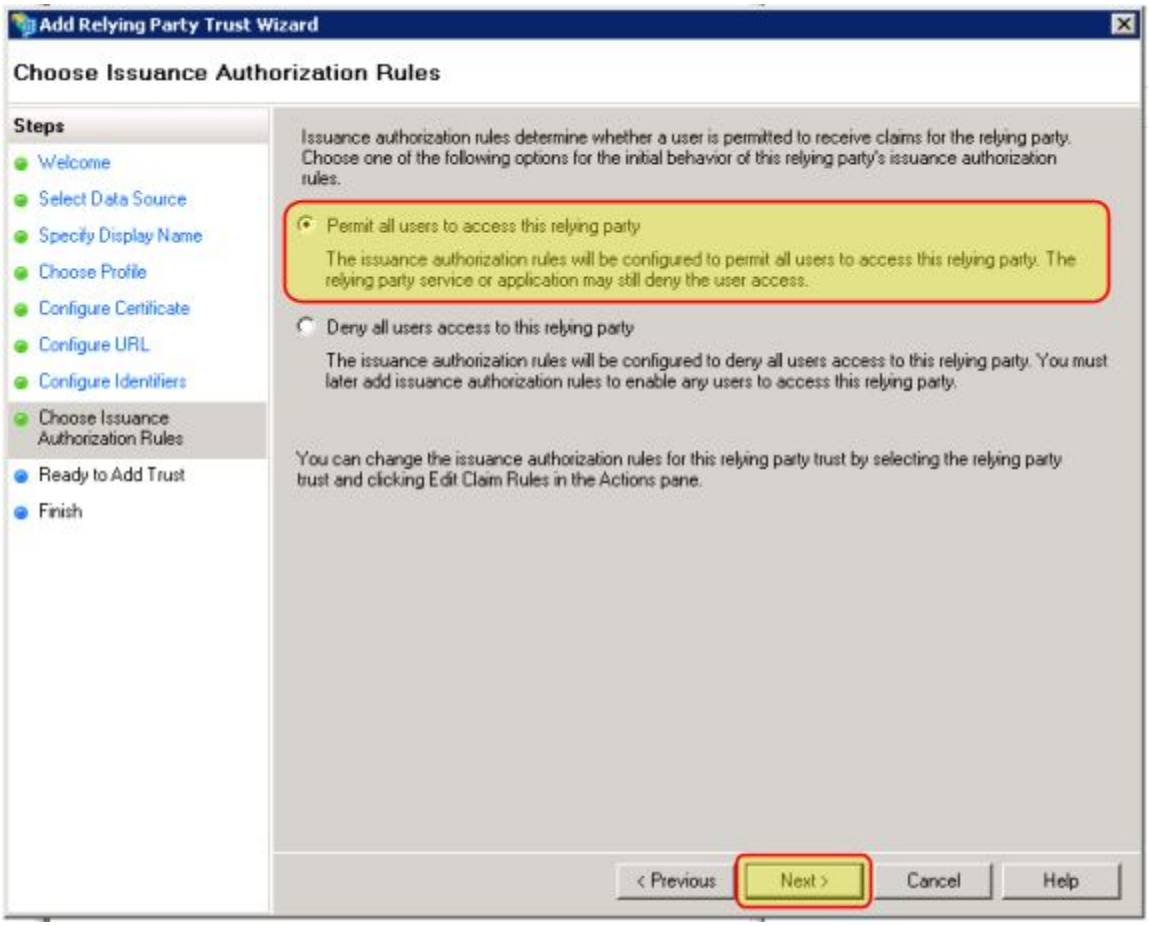
9) Leave both options unchecked for WS-Federation and support for SAML 2.0.



10) Enter **“https://getavail.com”** as the relying party trust identifier, and select **Add**.



11) Select **Permit all users to access this relying party**. Click **Next**. (For ADFS 4.0, this dialog is a bit different. Select **Permit Everyone.**)

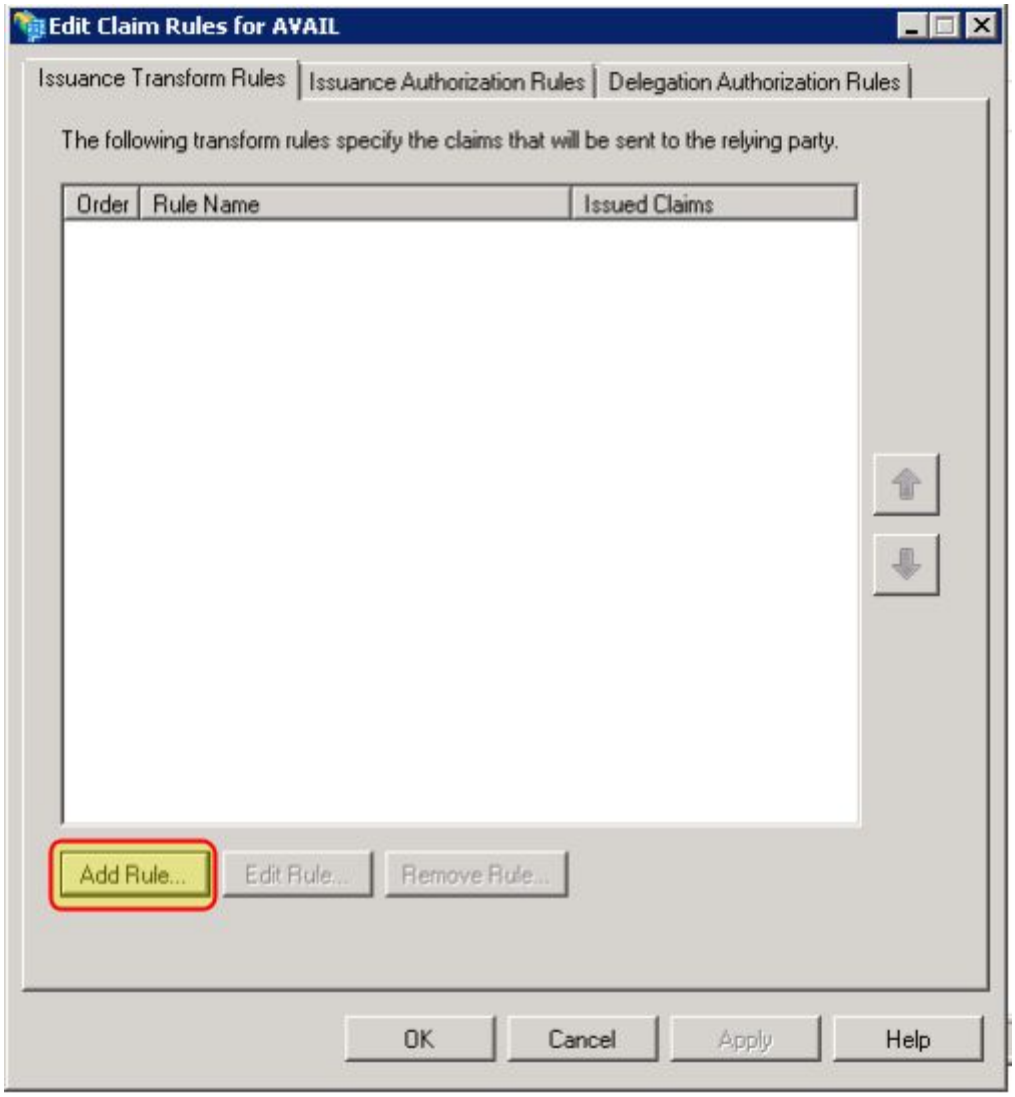


12) Select **Finish** to add the relying party.

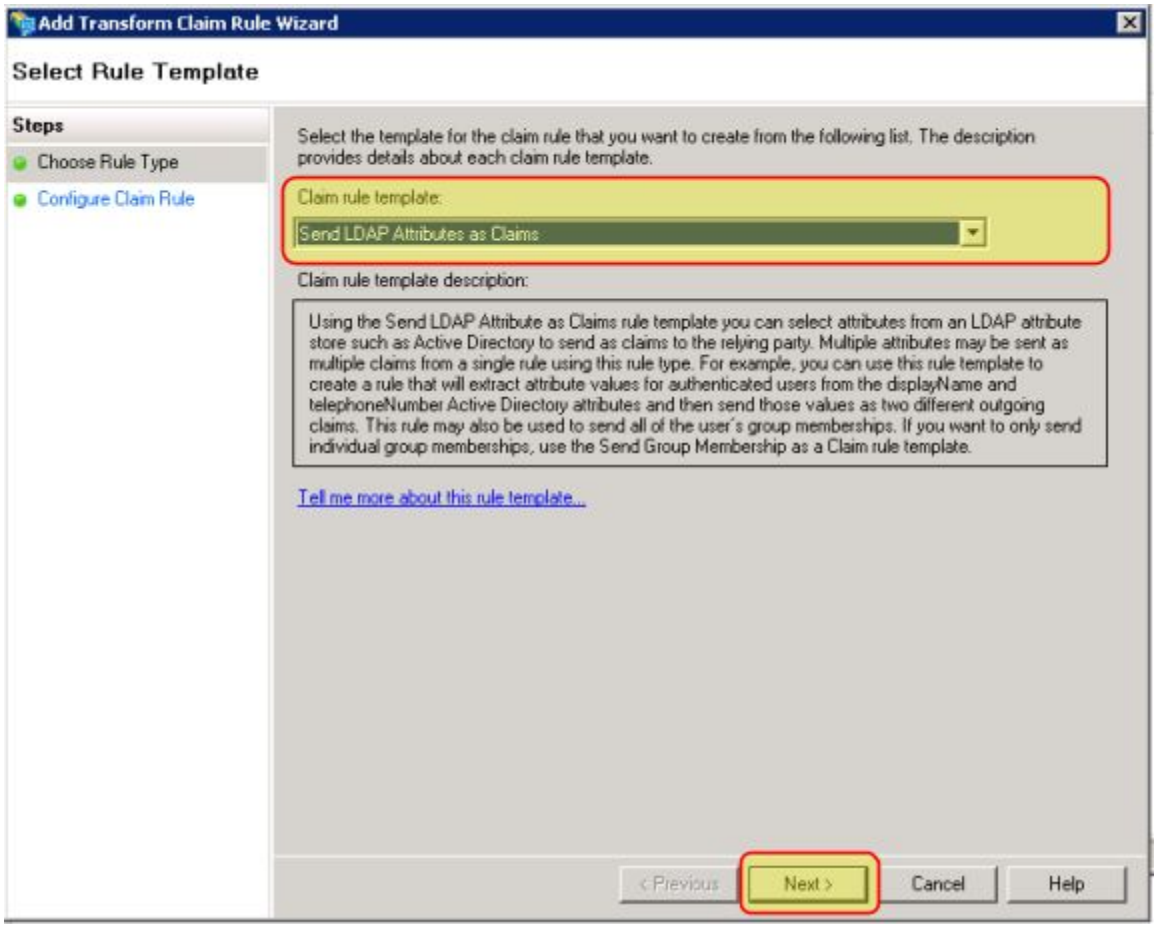
Setup Claim Rules

In this section, we will configure ADFS to send information about the user to the AVAIL service.

1) From the created Relying Party, right-click and select **Edit Claim Rules**.
    a) For ADFS 4.0, Right-click and select **Edit Claim Issuance Policy**.
2) Under **Issuance Transform Rules**, select **Add Rule**.

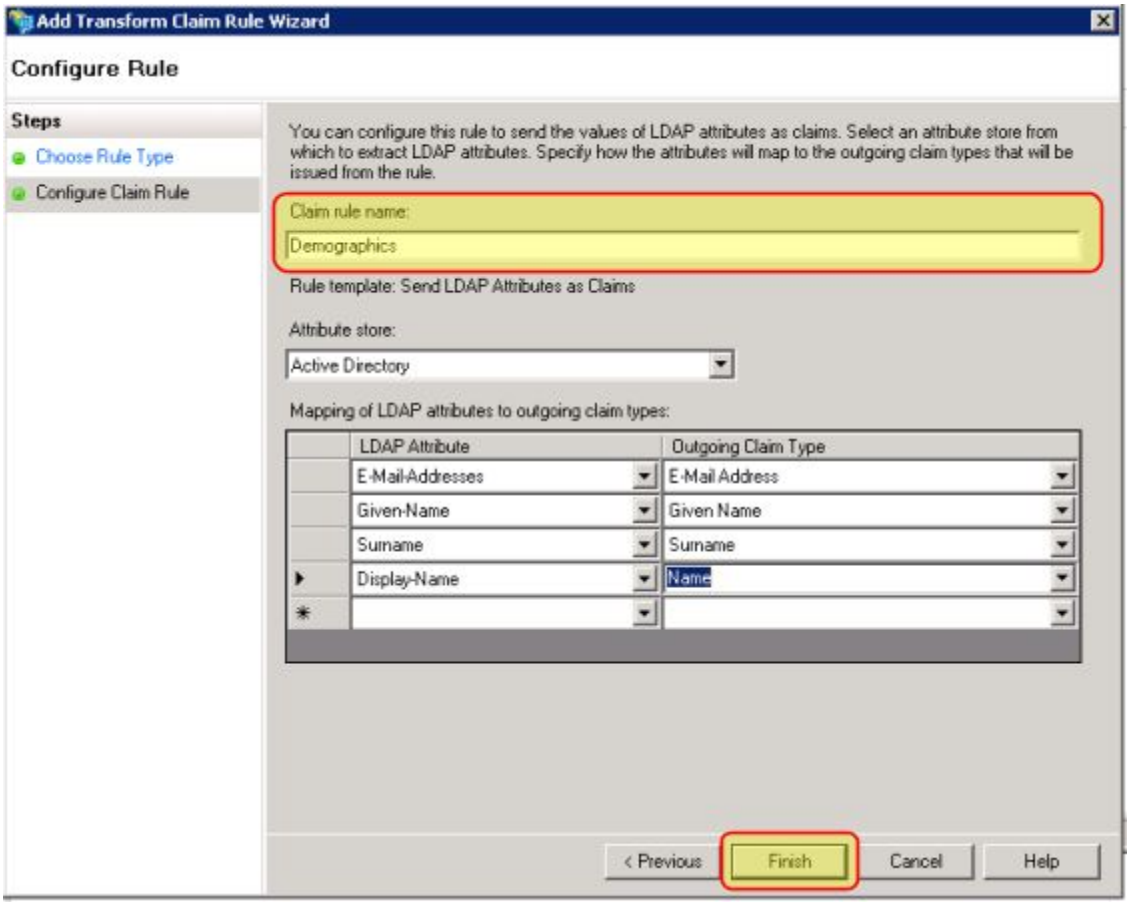


3) Select **Send LDAP Attributes as Claims.**



4) Under **Claim Rule Name,** enter the value **"Demographics"**. Under **Mapping of LDAP Attributes to outgoing claim types,** enter in the following values (per the given screenshot):

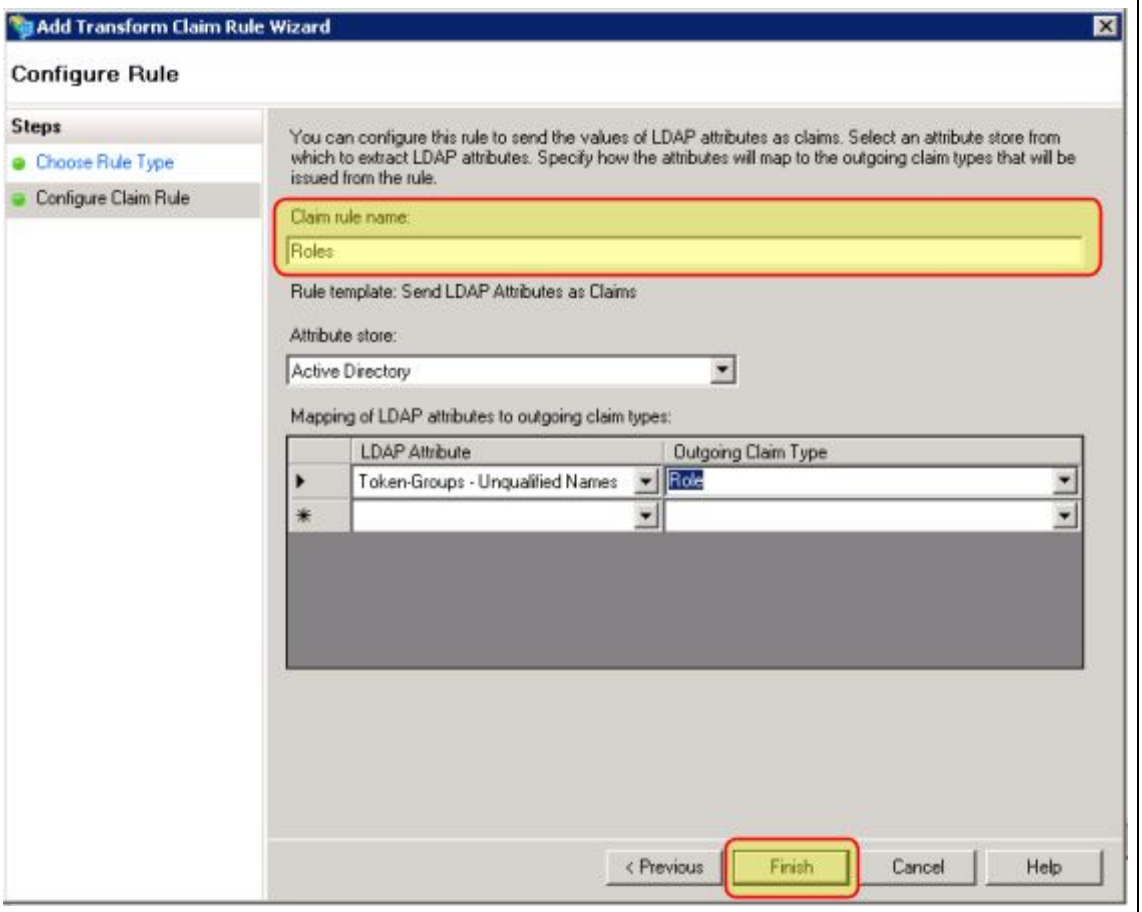
LDAP Attribute	Outgoing Claim Type
E-Mail-Addresses	E-Mail Address
Given-Name	Given Name
Surname	Surname
Display-Name	Name



5) Select **Finish**.
6) From the relying party, right-click and select **Edit Claim Rules**. (Repeat Step 1)
    a) For ADFS 4.0, Right-click and select **Edit Claim Issuance Policy**.
7) Under **Issuance Transform Rules**, select **Add Rule**. (Repeat Step 2)
8) Select **Send LDAP Attributes as Claims.** (Repeat Step 3)

9) Under **Claim Rule Name,** enter the value **"Roles"**. Under **Mapping of LDAP Attributes to outgoing claim types,** enter in the following value (per the given screenshot):

LDAP Attribute	Outgoing Claim Type
Token-Groups - Unqualified Names	Role

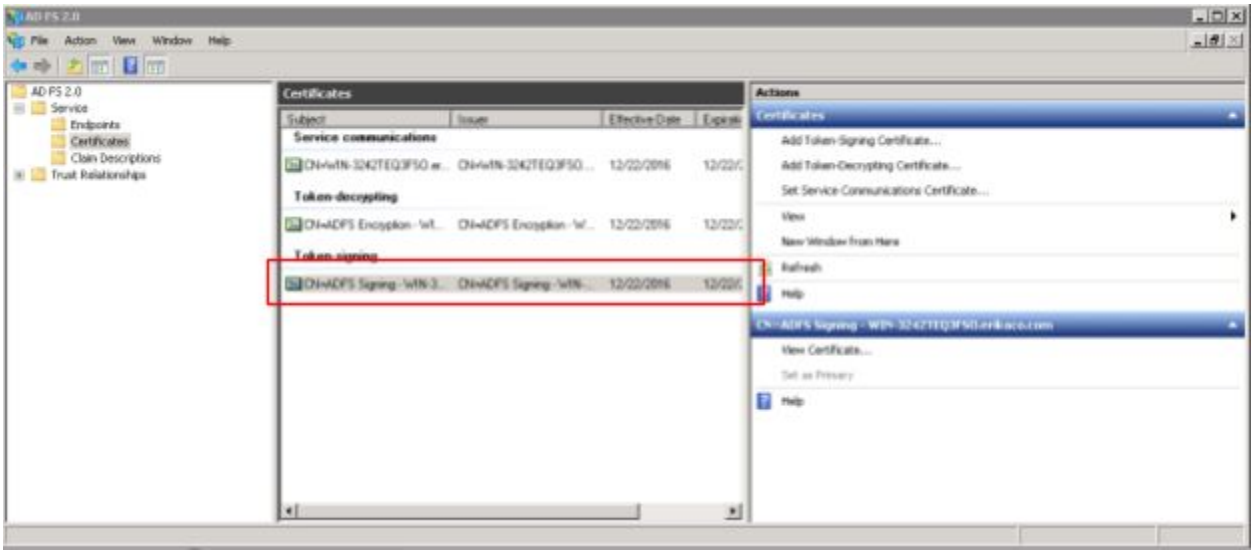


10) Select **Finish.**

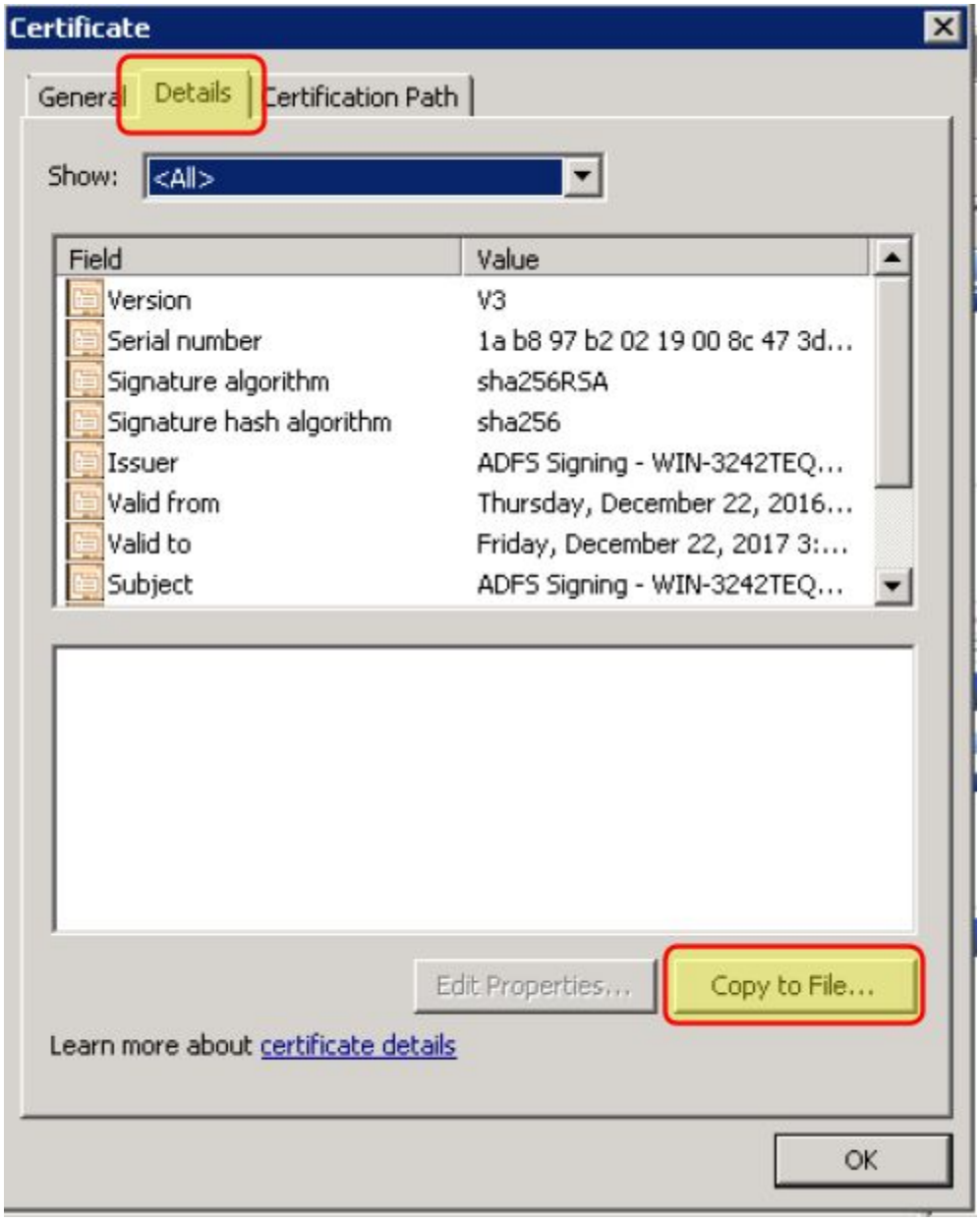
Exporting the Token Signing Certificate

In this section, we will export the certificate that is being used to sign tokens. Once it has been exported, this certificate will be used on AVAIL servers to authenticate the token, thereby granting access.

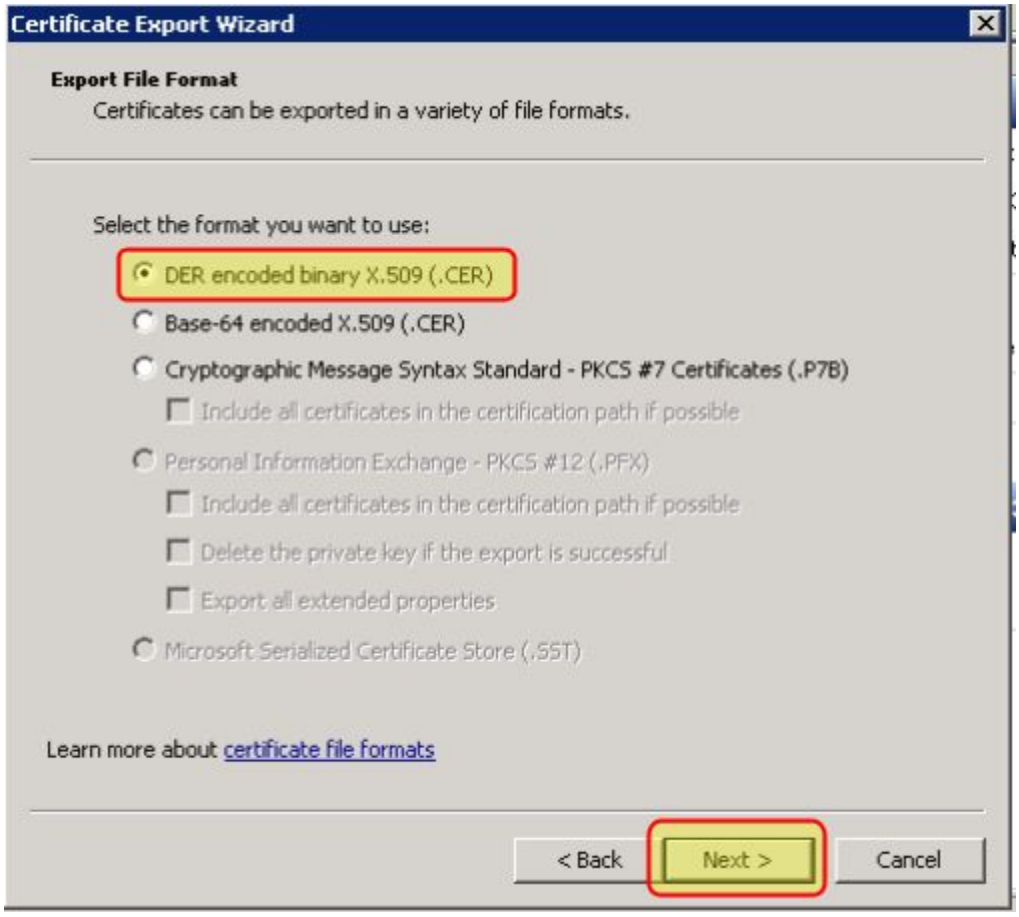
1) From ADFS 2.0 Management console, select **Service** from the left navigation menu, and then click **Certificates**.
2) Select the certificate labeled as the **Primary** certificate listed under **Token-signing**, and from the right-hand menu select **View Certificate**.



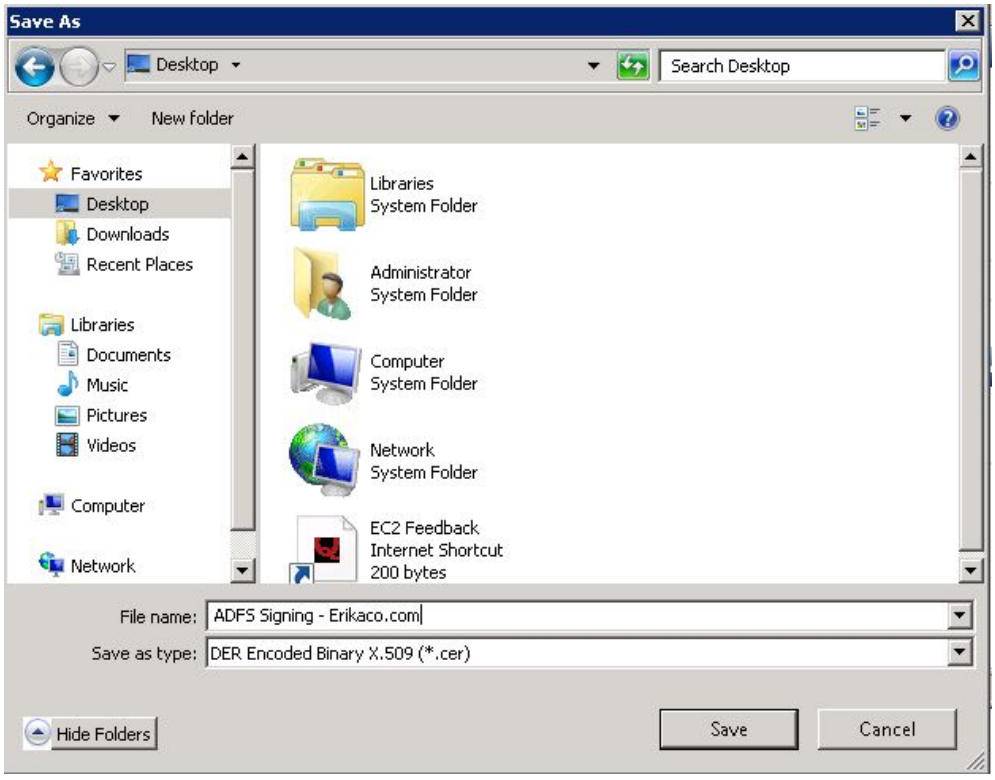
3) Select the **Details** tab of the properties window, then click **Copy to File…**



4) In the Certificate Export Wizard, select **DER encoded binary X.509 (.CER)**.



5) Select a file name and location, then Save the X.509 certificate.



6) Supply this certificate file (.cer) to AVAIL. This file will be imported into our server's certificate store for token validation and translating the user's Active Directory claims into claims used in the AVAIL Application.

AD Token Groups & the AVAIL Publisher Role

AVAIL supports two primary roles: Publisher and Consumer. Publishers are generally those who manage content on your network, such as your BIM Managers.

In the Setup Claim Rules section, you configured the AVAIL Relying Party to be able to receive specific LDAP attributes as claims. One of the claim rules that was issued was “Roles”, which allows AVAIL to view a user’s group memberships in Active Directory. This claim is what determines what actions a user is authorized to perform within the AVAIL application.

When AVAIL receives, verifies and parses the claims from the token, it will check to see if that user is a member of a group that you will specify as representing the AVAIL Publisher Role. Upon detecting the user is a member of that group, AVAIL will determine that user is a Publisher in your plan and provide specific claims back to the AVAIL desktop application.

Prior to deploying AVAIL on your user’s workstations, you will need to inform us of the name of that group. We recommend creating a dedicated “AVAIL Publishers” group, but it is absolutely acceptable if you already have an existing AD group in mind (such as a “BIM Managers” group). Every organization is just a little bit different, and we're happy to talk through an appropriate configuration for your company.

Submit Information to AVAIL

You have completed all the necessary steps for integrating AVAIL with your Active Directory. In this section, you will need to share some information with AVAIL about your Active Directory.

There are just two values associated with your Active Directory that you will need to submit: the Federation Service Authorization Endpoint and the Publisher Group Name.

Please fill in the information located in the form linked below. Once you have submitted the form, await confirmation from a member of the AVAIL Support team before continuing to the Installing AVAIL chapter of this instruction document. You will also need to prepare to share the Token-Signing Certificate.

On-Premises Active Directory Information Form

Installing AVAIL

NOTE: Before continuing this section, you must provide AVAIL with the necessary values prior to deploying the AVAIL application across your organization. Please fill in the values in the form located in the Submit Information to AVAIL section.

Once you have completed the form, please wait for confirmation from the AVAIL Support team before continuing this instruction document.

Overview

Once you have supplied the necessary values to AVAIL and have received confirmation, you will need to inform you assigned AVAIL Support team member your preferred method of installation: .msi or .exe. Prior to installing AVAIL on your user's workstations, you will need to configure your software deployment process to include specific installer switches.

During installation, the switches defined in the sections of this chapter will create a special configuration file titled **ADFS.config** on each workstation. This file is critical for providing the AVAIL desktop application with special values for authenticating users through your Active Directory. You will need the value for the **Federation Service Authorization Endpoint** that you found earlier in the Submit Information to AVAIL chapter.

It is highly recommended that you first perform a test installation with the defined installer switches prior to deploying AVAIL. In the sections below, there are examples provided which will show you how to install via command line so that you may test the installation.

EXE Installation

AVAILInstaller.exe

This file packages both the AVAIL Desktop application and the SQL LocalDB msi files into a single installer. The switches below are the values written in the ADFS.config file upon installing AVAIL.

Switches

- DisableUpdates=1
- ActiveDirectory=1
- ActiveDirectoryVersion="ADFS2"
- ActiveDirectoryAuthority="https://**adfs.mycompany.com**/adfs/services/trust/13/windowsmixed/"
- ActiveDirectoryRealm="https://getavail.com"

Example

```
C:\>"C:\AvailInstaller.exe" /i /quiet /norestart DisableUpdates=1
ActiveDirectory=1 ActiveDirectoryVersion="ADFS2"
ActiveDirectoryAuthority="https://adfs.mycompany.com/adfs/services/trust/13
/windowsmixed/" ActiveDirectoryRealm="https://getavail.com"
```

MSI Installation

In order to properly install the AVAIL application via MSI installation, you will need to deploy one .exe installer and two .msi installers in the following order:

1. *vc_redist.x64.exe (optional, see below)*
2. *AvailSyncService.msi*
3. *Avail.msi*

1. vc_redist.x64.exe

The *vc_redist.x64.exe* file is the Microsoft Visual C++ 2015 Redistributable (x64) and installs run-time components of Visual C++ libraries. These components are required to run C++ applications that are developed using Visual Studio 2015 Update 3 RC and link dynamically to Visual C++ libraries.

Note that many modern applications, such as Autodesk Revit® 2018 (or greater), also require the Microsoft Visual C++ Redistributable package and a supported newer version may already be installed.

Switches

- `/i /quiet /norestart`

Example

```
C:\>"C:\vc_redist.x64.exe" /i /quiet /norestart
```

2. AvailSyncService.msi

The *AvailSyncService.msi* file installs a background service that manages syncing the content that is indexed into AVAIL.

Example

```
C:\>msiexec.exe /i "C:\AvailSyncService.msi" /qn
```

3. AVAIL.msi

This .msi is the installer for the AVAIL Desktop application. The switches below are the values written in the ADFS.config file upon installing AVAIL.

Switches

- DISABLEUPDATES=1
- ACTIVEDIRECTORY=1
- AD_VERSION="ADFS2"
- AD_AUTHORITY="https://**adfs.mycompany.com**/adfs/services/trust/13/windowsmixed/"
- AD_REALM="https://getavail.com"

Example

```
C:\>msiexec.exe /i "C:\Avail.msi" /quiet /norestart DISABLEUPDATES=1
ACTIVEDIRECTORY=1 AD_VERSION="ADFS2"
AD_AUTHORITY="https://adfs.mycompany.com/adfs/services/trust/13/windowsmixed/" AD_REALM="https://getavail.com"
```

The ADFS.config file

After installing with the switches defined (either msi or exe), a special configuration file titled **ADFS.config** will be created on each workstation. This file is located in the same installation directory as the AVAIL.exe application (`C:\Program Files\AVAIL`). This file is a crucial component for providing the AVAIL desktop application with special values for authenticating users via your Active Directory.

Example

A proper, Azure-based ADFS.config file should look something like this:

```
<adfsSettings>
    <add key="ActiveDirectoryVersion" value="ADFS2" />
    <add key="ActiveDirectoryAuthority"
value="https://adfs.mycompany.com/adfs/services/trust/13/windowsmixed/" />
    <add key="ActiveDirectoryRealm" value="https://getavail.com" />
</adfsSettings>
```

Troubleshooting

Every ADFS installation and integration is a little different. Here are some “gotchas” that we have encountered:

- **AD FS Rapid Restore Tool (Windows 2012 R2, Windows Server 2016):**
  - The **AD FS Rapid Restore tool** provides a way to restore AD FS data without requiring a full backup and restore of the operating system or system state. You can use the new tool to export AD FS configuration either to Azure or to an on-premises location. Then you can apply the exported data to a fresh AD FS installation, re-creating or duplicating the AD FS environment.
  - Reference**:**
    - https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-rapid-restore-tool
  - Download and install the **MSI** to your **AD FS Server**:
    - Download: https://go.microsoft.com/fwlink/?LinkId=825646
    1. Launch a new **PowerShell** prompt window.
    2. Run the following command:

```
import-module 'C:\Program Files (x86)\ADFS Rapid Recreation
Tool\ADFSRapidRecreationTool.dll'
```

3. Create the backup using the **Backup-ADFS** cmdlet (assuming running as domain admin):

```
Backup-ADFS -StorageType "FileSystem" -StoragePath
"C:\Users\administrator\testExport\" -EncryptionPassword "password"
-BackupComment "Clean Install of ADFS (FS)" -BackupDKM
```

4. Use the **Restore-ADFS** cmdlet to restore the ADFS configuration:

```
Restore-ADFS -StorageType "FileSystem" -StoragePath
"C:\Users\administrator\testExport\" -DecryptionPassword "password"
-RestoreDKM
```

5. While running the **Restore-ADFS** cmdlet, you will be prompted to enter in the service account credentials that runs the AD FS service (initially configured in the Running the ADFS Configuration Wizard section).

- **If you get "SOAP Security Negotiation failed"**:
    - The inner exception is the most helpful part of this. This exception is a generic failed message. However, here are some things to check:
        - Is the SSL certificate securing the site trusted on the client?
        - Does the ADFS service user account have the SPN set properly?
            - **setspn -l [user name]**
            - **setspn -q "host/[url]"**
        - Is there a time discrepancy between the ADFS server and the domain controller?
        - Is there a time discrepancy between the desktop and the domain controller?
        - One customer had an error "Specified handle is invalid". We ended up trying the setup on a different workstation and it worked. So we have not yet resolved why we get the error "Specified handle is invalid".
- **If importing an SSL certificate after ADFS has already been configured**:
    - Does the ADFS Service user account have the SPN set properly?
        - **setspn -l [user name]**
        - **setspn -q "host/[url]"**
    - Does the ADFS Service user account have **Full control** permissions for the SSL certificate?
        - Open MMC, click on **File**, then **Add/Remove Snap-in…**
            - Under **Available snap-ins** (left side), Select **Certificates**.
            - Select **Add >.**
            - In the Certificates snap-in dialog, select **Computer Account**, then click **Next.**
            - Leave the **Local computer** option selected, then click **Finish.**
            - Once the dialog closes, click **OK.**
        - On the left, Expand **Certificates (Local Computer)**, then **Personal**, then **Certificates.**
        - Select the SSL certificate, then right-click and select **All Tasks,** then **Manage Private Keys…**
            - Select the service user account under **Group or user names**
                - If the account is not listed, select **Add…**, then enter the name of the service account, then click **OK.**
            - Verify that this account has **Allow** checked for **Full control.**
            - Click **OK.**

Support

Have a question?
Email us at support@getavail.com or call us at +1 859-963-1616

AVAIL Solutions, Inc.
163 East Main Street
3rd Floor
Lexington, KY 40507
USA

Website: www.getavail.com
Phone: +1 859-963-1616
Email: support@getavail.com