AvePoint®

Configuring ADFS 2.0 for Use with DocAve 6

User Guide

September 2015

REVISION HISTORY

Table 1

Version	Effective Date	Summary of Changes
1.0	09/2015	Initial version.

TABLE OF CONTENTS

OVERVIEW

Active Directory Federation Services (ADFS) 2.0 is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries.

***Note:** This guide presumes that your environment already has a fully functional Active Directory (AD), SQL Server, SharePoint 2013 farm using the default claim authentication method, and DocAve Manager with the default Windows Authentication installed and configured. This guide is applicable to all versions of DocAve 6.

To install and configure ADFS for use with DocAve 6, see the following sections:

1. Installing ADFS
2. Configuring Trust Relationships
3. Manage Trust with the Token Signing Certificate
4. Configure DocAve to Use the Trusted Relying Partner

INSTALLING ADFS ON WINDOWS SERVER

To install ADFS on your Windows Server, follow the instructions below:

***Note**: If you are using Windows Server 2012 or later, the ADFS feature has been integrated into the operating system, which means you need not to download and install it. Continue to the Configuring ADFS 2.0 section.

1. Download the ADFS installer from http://www.microsoft.com/en-gb/download/details.aspx?id=10909
2. Run **AdfsSetup.exe** to begin the wizard.
3. At the **Server Role** screen, choose **Federation Server**.
4. Complete the installation by clicking **Next** for each screen.
5. Click **Finish** to start the ADFS 2.0 Management snap-in.

Configuring ADFS 2.0

To configure ADFS 2.0, follow the steps below on your Windows Server:

1. Open the **ADFS 2.0 Management Console** on the Federation Server (ADFS01Srv.ADFS01.NET).
2. Click **AD FS 2.0 Federation Server Configuration Wizard** in the management console. The wizard appears.
3. Select **Create a new Federation Service,** and click **Next.**
4. Select **New federation server farm** or **Stand-alone federation server** according to your environment requirements.
    - **New federation server farm** will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm.
    - **Stand-alone federation server** will create a new Federation Service on this computer. This option is recommended for evaluation purposes or small production environments, because you cannot add more servers to create a farm after selecting this option.
5. Select the SSL certificate and port, and click **Next**.
6. Enter a service account and password into the appropriate text boxes and click **Next**.

   ***Note**: The same service account must be used on all federation servers in the farm.
7. Review the certificate information on the summary page.
8. Click **Finish** to complete the wizard.

Configuring Trust Relationships

By configuring the Relying Party Trusts, you can specify the claims sent to DocAve. Additional claims can be sent, but a unique identifier is required.

SharePoint can use the following types of claims:

- User Principle Name (UPN), for example user@avepoint
- E-Mail Address, for example user@avepoint.com
- Common Name, which is an arbitrary string

To configure the Relying Party Trusts, follow the steps below on your Windows Server:

1. Open the **ADFS 2.0 Management Console** on the ADFS Server.
2. Select **Trust Relationships**.
3. Right-click **Relying Party Trusts**, and select **Add Relying Party Trust**.
4. Complete the wizard with the following information:

***Note**: WS-Federation and SAML 1.0, 1.1, and 2.0 protocols are all supported by DocAve.

a. Click **Start** on the configuration wizard.

b. Select **Enter data about the relying party manually** and click **Next**.

c. Enter the display name into the **Specify Display Name** field, and click **Next**.

d. Select **AD FS profile (2.0)**, and click **Next.**

e. On the **Configure Certificate** page, click **Browse** to browse to and locate a certificate file and add it to the list of certificates, and then click **Next**.

f. Select **Enable support for the WS-Federation Passive protocol**, enter the Relying party WS-Federation Passive protocol URL, and click **Next**.

g. In the **Relying party trust identifier**s field, remove the default Relying Party Trust identifiers and enter the URL you want to use. Click **Add**, and click **Next**.

h. Select **Permit all users to access this relying party** and click **Next**.

i. Review settings you have configured in the above steps to ensure each has been correctly configured. Click **Next.**

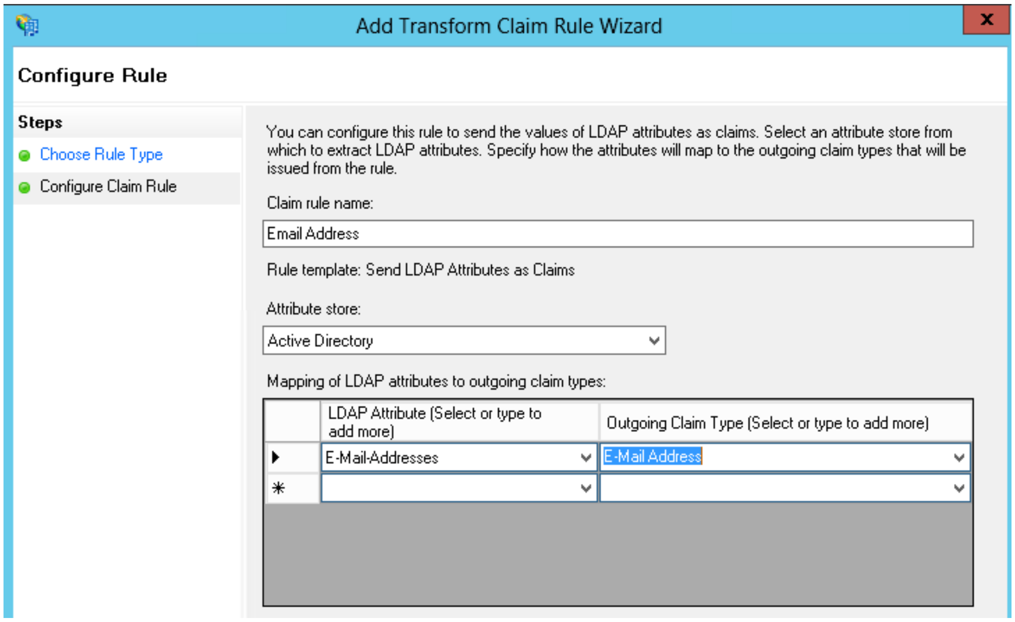
j. Select **Open the edit Claims Rules Dialog for this relying party trust when the wizard closes**, and click **Close.** The **Edit Rules for SharePoint ADFS** page appears.

k. Navigate to the **Issuance Transform Rules** tab, and select **Add Rule**.

l. Select **Send LDAP Attributes as Claims**, and click **Next.**

m. Configure the following information in the **Configure Rule** page:

- **Claim Rule Name:** Email Address
- **Attribute Store:** Active Directory
- **LDAP Attribute:** E-Mail-Addresses
- **Outgoing Claim Type**: E-Mail Address



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Email Address

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

Figure 1: Configuring the Claim Rule

Exporting the Token Signing Certificate

After configuring Trusted Relationships, the token signing certificate must be exported to the DocAve Server that will be configured as the trust relationship between the DocAve Server and ADFS Server. To export the token signing certificate, follow the steps below:

1. Open the ADFS 2.0 management console on the ADFS Server.
2. Select **Service**.
3. Select **Certificates**, and double-click **Token-signing certificate**.
4. Select the **Details** tab.
5. Select **Copy to File**, and select the following options:
   - **No do not export the private key**
   - **DER encoded binary X.509 (.CER)**
6. Save the file as **ADFS01Srv_Token.cer**.

Managing Trust with the Token Signing Certificate

The token signing certificate must be added to the Trusted Root Certification Authorities in DocAve. To add the token signing certificate to DocAve, follow the steps below:

1. Navigate to the DocAve Control server.

2. Click **Start…** > **Run** > **Microsoft Management Console**.

3. Click **File** > **Add/Remove Snap-in…**

4. In the **Available Snap-ins** area, select **Certificates** and add it to the **Selected Snap-in area**.

5. In the Certificates snap-in dialog, select **Computer account** > **Next** > **Local computer** > **Finish**.

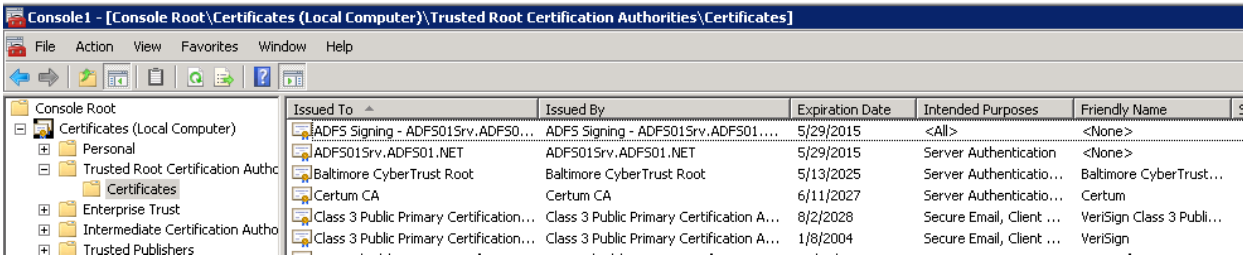
6. Double-click **Certificates(Local Computer)**.

7. Expand the **Trusted Root Certification Authorities** tree.

8. Right-click on **Certificates** below the **Trusted Root Certification Authorities**, and select **All Tasks** > **Import…**

9. Click **Next** > **Browse and select Token-signing Cert** > **Next** > **Next** > **Finish.**

After completing the steps above, the console will look similar to the screenshot below.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authc
Certificates
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
ADFS Signing - ADFS01Srv.ADFS0…	ADFS Signing - ADFS01Srv.ADFS01.…	5/29/2015	<All>	<None>
ADFS01Srv.ADFS01.NET	ADFS01Srv.ADFS01.NET	5/29/2015	Server Authentication	<None>
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Server Authenticatio…	Baltimore CyberTrust…
Certum CA	Certum CA	6/11/2027	Server Authenticatio…	Certum
Class 3 Public Primary Certification…	Class 3 Public Primary Certification A…	8/2/2028	Secure Email, Client …	VeriSign Class 3 Publi…
Class 3 Public Primary Certification…	Class 3 Public Primary Certification A…	1/8/2004	Secure Email, Client …	VeriSign

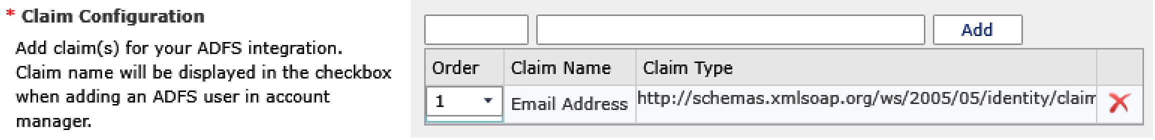
Figure 2: Adding the token signing certificate to DocAve

CONFIGURE DOCAVE TO USE THE RELYING PARTNER TRUSTS

To configure DocAve to use the Relying Party Trusts that were set up in the previous sections, follow the steps below:

1. Log into DocAve Manager.
2. Navigate to **DocAve Control Panel** > **Authentication Manager** > **ADFS Integration** > **ADFS Integration**.
3. In **ADFS Integration Method**, select **Manually**.
4. In the **ADFS Issuer** area, enter the ADFS Issuer URL.
5. In the **Relying Party Identifier** area, enter the value configured in step **g.** of Configuring Trust Relationships.
6. In the **Token-signing** area, click **Select** and find the token signing certificate that you placed in trust store.
7. In the **Claim Configuration** area, enter the correct **Claim Name** and **Claim Type** of the e-mail claim information.

   - Name: Email Address
   - Type: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress



* **Claim Configuration**

Add claim(s) for your ADFS integration. Claim name will be displayed in the checkbox when adding an ADFS user in account manager.

Order	Claim Name	Claim Type
1	Email Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claim

8. Remove the other default claims from the **Claim Configuration** area.
9. ADFS is now configured for use with DocAve.

NOTICES AND COPYRIGHT INFORMATION

Notice
The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright

Trademarks
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA