Setup adfs

Getting adfs

Download from http://www.microsoft.com/en-US/download/details.aspx?id=10909

Choose the right version (x84/x64)

Can also be done with Servermanager (see ADFS Proxy)

Install

Install the adfs on the Active Directory Server

http://support.druva.com/entries/21437659-How-to-install-and-Configure-Active-Directory-Federat

ion-Services-for-Druva-inSync-Cloud-SAML-integr

To install the ADFS 2.0 software using the setup wizard

1. Download the ADFS 2.0 software by saving the AdfsSetup.exe setup file onto the computer. To download this file, go to Active Directory Federation Services 2.0 RTW (http://go.microsoft.com/f wlink/?LinkId=151338).

2. Locate the AdfsSetup.exe setup file that you downloaded to the computer, and then double-click it.

3. On the Welcome to the ADFS 2.0 Setup Wizard page, click Next.

4. On the End-User License Agreement page, read the license terms.

5. If you agree to the terms, select the I accept the terms in the License Agreement check box, and then click Next.

6. On the Server Role page, select one of the following options, depending on the role for which you will configure this computer.

- To install ADFS 2.0 and to begin the process of configuring it for the federation server role, select **Federation server**, and then click **Next.**
- To install ADFS 2.0 and begin the process of configuring it for the federation server proxy role, select **Federation server proxy**, and then click **Next**.

7. On the Install Prerequisite Software page, click Next.

After you click Next, you see the Installing ADFS 2.0 page.

Note: The installation process can take up to 20 minutes to complete, depending on how many of the prerequisites are already installed on the computer.

8. On the Completed the ADFS 2.0 Setup Wizard page, verify that the Restart now checkbox is selected, and then click Finish to restart the computer.

After setup, open "AD FS 2.0 Management"

When installing adfs on the AD server it adds automaticly the AD to the atribute store, meaning that the AD is coupled to the adfs.



Configuring an Service provider from simple saml

Open AD FS 2.0 Manager

Right click on "Relying Party Trusts" and click "Add Relying Party Trust..."



Then the wizard start to add the service provider.

📬 Add Relying Party Trust	Wizard	×
Welcome		
Welcome Steps Velcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.]	
	< <u>P</u> revious <u>S</u> tart Cancel <u>H</u> elp	

Click start

💱 Add Relying Party Trust	Wizard X
Select Data Source	
Select Data Source Velcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: Rectangular Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): [tps://pc-192.168-2.217.office.aventiv.com/simplesaml/module.php/saml/sp/metadata.php/default.sr, Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has experied its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Federation metadata file location: Federation metadata file location: Federation to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel Help

Select the first option and enter the url from the service provider

url example	
https://[HOSTNAME]/simplesaml/module.php/saml/sp/metadata.php/[SER	VICE]

Make sure that the certificate is accepted by the ADFS server, this can be tested by surfing to the url in a webbrowser.

Then click next and Ok in the pop up.

🙀 Add Relying Party Trust Wizard 🛛 🔀				
Specify Display Name				
Specify Display Name Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	Type the display name and any optional notes for this relying party. Display name: bc-192-168-2-217.office.aventiv.com Notes:			
	< Previous Next > Cancel Help			

Insert a Display name, or leave it at the default.

Click next.

Add Relying Party Trust Wizard				
Choose Issuance Authorization Rules				
Steps Welcome Select Data Source	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.			
 Specify Display Name Choose Issuance Authorization Rules 	Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.			
 Ready to Add Trust Finish 	 Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane. 			
	< Previous Next > Cancel Help]		

Select the first option and click next.

🙀 Add Relying Party Trust Wizard 🛛 🗙 🗙				
Ready to Add Trust				
Steps Velcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N ◆ Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL: [https://pc-192-168-2-217.office.aventiv.com/simplesaml/module.php/saml/sp/metadata.php/defau Image: Monitor relying party Monitor relying party Image: Automatically update relying party This relying party's federation metadata data was last checked on: 1/21/2014 This relying party was last updated from federation metadata on: 1/21/2014 Chevious Next> Cancel Help			

This is the overview of all the settings coming from the server.

Click next

📬 Add Relying Party Trust ¥	/izard 🔀
Finish	
Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snaprin. ✓ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
	Close

Let the checkbox checked and click close

Then a window appears to setup de SAML message.

hit Claim Rules for pc-192-16	8-2-217.office.aventiv.com			
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules				
The following transform rules specif	y the claims that will be sent to the relying party.			
Order Rule Name	Issued Claims			
		•		
Add Rule Edit Rule	Remove Rule			
	OK Correct Ac-tu	Help		
	UN Lancel Apply	нер		

Click on Add Rule to configure the message

翰 Add Transform Claim Rule	Wizard	×
Select Rule Template		
Steps Choose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.	
 Configure Claim Rule 	Claim rule template: Send LDAP Attributes as Claims Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values at two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template. Tell me more about this rule template	
	< Previous Next > Cancel Help	

We want to send info from AD (LDAP)

Click Next

add Transform Claim Rule Wizard 🛛				
Configure Rule				
Steps Choose Rule Type Configure Claim Rule	You ca which t issued Claim m Idap-cl. Rule te Attribut Select	n configure this rule to send the values of LDAP attributes as claims. Select an attribute store from o extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be from the rule. ale name: aims mplate: Send LDAP Attributes as Claims e store: an attribute store or of LDAP attributes to outgoing claim types: LDAP Attribute Outgoing Claim Type		
		< Previous Finish Cancel Help		

Give the rule a name, then select the attribute store (Default is Active Directory)

Then add at least one rule:

	LDAP Attribute		
	SAM-Account-Name	l	Outgoing Claim Type
	Company Department	LÍ	Name ID
	Display-Name	í	E-Mail Address
	E-Mail-Addresses	14	Given Name
	Employee-ID		Name
	Employee-Number		UPN
	Employee-Type		Common Name
	Given-Name		AD FS 1.x E-Mail Address
1	Is-Member-Of-DL	٢I	Group
	Organizational-Unit		AD FS 1.x UPN
	Organization-Name	1	Kole
	Proxy-Addresses		Surname
	SAM-Account-Name		PPID Nexe ID
	State-Ur-Province-Name		Name ID Authoritiestics time stores
	Street-Address		Authentication withod
	Surname Talaahaya Numbar		Deputorlu group SID
1	। elephone-inumber		Deny only group sto
	Taken Groups as SIDs	Ν.	Deny only primary group SID
	Token-Groups as SID's Token-Groups - Qualified by Domain Nam		Group SID
1	Token-Groups - Qualified by Domain Nam	۲P	Primary group SID
	Token-Groups - Ungualified Names		Primary SID
	User-Principal-Name	"	Windows account name
		1	

Add other attributes if neccesery then click Finish.

Edit Rule - Idap claims 🛛 🔀				
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.				
<u>C</u> laim	rule name:			
ldap c	claims			
Rule t	emplate: Send LDAP Attributes a	as Claims		
Attribu	ute store:			
Active	e Directory		•	
		I-i- I		
Mappi	Ing of LUAP attributes to outgoin	ig claim type:		
	LDAP Attribute	Ţ	Name ID	
	E-Mail-Addresses		F-Mail Address	
	Given-Name		Given Name	
	Surname		Surname 🗾	
	Telephone-Number		PhoneNumber	
*		•		
View	View Rule Language OK Cancel Help			

*Note: For Outgoing claim "Name ID", you have to manualy type "objectSid" into the LDAP Attribute list.

Add other rules if neccesery of click Apply - Ok to close.

Open in the AD FS 2.0 Manager the "Relying Party Trusts" folder

🃬 AD F5 2.0				
翰 File Action View Window Help				
🗢 🔿 🖄 🖬 🔽 🗊				
AD F5 2.0	Display Name	Enabled	Identifier	
🖃 🚞 Service	pc-192-168-2-217.office.aventiv.com	Yes	https://pc-192-168-2-217.office.avent	
Endpoints				
Certificates				
Claim Descriptions				
🖃 🧮 Trust Relationships				
Claims Provider Trusts				
Relying Party Trusts				
Attribute Stores				

Double click on the newly added Service provider

pc-192-168-2-217	.office.aventiv.c	om Properti	es		×		
Monitoring Accepted Claims	Identifiers Organization	Encrypti Endpoints	ion Notes	Signature Advanced	1		
Specify the secure hash algorithm to use for this relying party trust. Secure hash algorithm: SHA-1							
	OK Car	ncel	Apply	Help			

Open the "Advanced" Tab and set Secure hash algorithm to SHA-1

Basic Authentication and Chrome

In the event viewer you will see an 'Audit Failure' event with "Status: 0xc000035b".

You can circumvent this problem by switching off 'Extended Protection' for the adfs/ls web application.

Some extra info about the extended protection:

Disabling Extended Protection does make the credential more vulnerable to man-in-the-middle attacks. But since Chrome does not support Extended Protection, you have to disable it.

For more information about the Extended Protection in ADFS, you may refer the following links,

Configuring Advanced Options for AD FS 2.0 and Office 365 http://technet.microsoft.com/en-us/library/hh237448%28v=ws.10%29.aspx

AD FS 2.0: Continuously Prompted for Credentials While Using Fiddler Web Debugger http://social.technet.microsoft.com/wiki/contents/articles/ad-fs-2-0-continuously-prompted-for-credentials-whileusing-fiddler-web-debugger.aspx

Extended Protection for Authentication

http://support.microsoft.com/kb/968389

Note that this is also for old firefox versions, it was fixed in Mozilla 11.

To turn Extended Protection off, on the AD FS server:

- 1. launch IIS Manager,
- 2. In the left side tree view, access Sites -> Default Web Site -> adfs -> ls.
- 3. Selected the "/adfs/ls" folder,
- 4. double-click the Authentication icon,
- 5. Right-click Windows Authentication and select "Advanced Settings..."
- 6. On the Advanced Settings dialog, choose Off for Extended Protection.
- 7. Restart IIS

Step 1 => 4



Step 5:



<u>Step 6:</u>

¥ Internet Information Services (IIS) Manager							
③ ● DC01 > Sites > Default Web Site > adfs > Is >							
File View Help							
Connections	Authentication Group by: No Grouping Name Advanced Settings Anonymous Asp.HET Im Extended Protection: Off Forms Auther Off Windows Au Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Krebres authentication in your environment and the application pool is configured to use a custom identity. Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information online Image: Cick here for more information <td>Alerts Alerts Click here to learn how to configure Extended Protection. Actions Disable Advanced Settings Providers Image: Provider Protection Online Help</td>	Alerts Alerts Click here to learn how to configure Extended Protection. Actions Disable Advanced Settings Providers Image: Provider Protection Online Help					
Configuration: 'localhost' applicationHost.co	nfig , <location path="Default Web Site/adfs/ls"></location>	€ 1.:					

Error log

Open the Windows event viewer and go to "Applicatios and Services Logs" - "AD FS 2.0" - "Admin"

et land i Ri land							
2 🖸 🖬 🖬							
k Viewer (Local)	Admin Number of events: 107					Actions	
Justom views Modows Loos	Level	Date and Time 🐨	Source	Event ID Task Category	-	Admin	-
Applications and Services Logs	Error	1/21/2014 3:03:49 PM	40 FS 2.0	364 None		👩 Open Saved Log	
Active Directory Web Services	0 Error	1/21/2014 3:03:49 PM	AD FS 2.0	184 None		👻 Crashe Custom View	
AD PS 2.0	. Error	1/21/2014 3:03:49 PM	AD FS 2.0	364 None		T Create Coston New	
Admin	U Error	1/21/2014 3:03:49 PM	AD P5 2.0	303 None		Import Custom View	
DHS Repecation	Error	1/21/2014 2:43:00 PM	AD P5 2.0	364 None		Clear Log	
DNS Server	Error	1/21/2014 2143300 PM	AD PS 2.0	184 None		The Current Lon	
Hardware Events	Ener	1/21/2014 2:43:00 PM	AD F5 2.0	209 Notes			
Internet Explorer	Fror	1/21/2014 2:42:00 PM	AU FS 2.0	303 None 362 None		Properties	
Key Management Service	a France	1/21/2014 2:42:05 PM	AD #5 2.0	302 Note		Disable Log	
Mcrosoft	A Warning	1/21/2014 1:21:44 PM	40 F5 2.0	174 None		00 End	
👔 Windows PowerShell	Information	1/21/2014 1:21:44 PM	40 F5 2.0	157 None			
Subscriptions	Information	1/21/2014 1:21:44 PM	AD F5 2.0	337 None		Save All Events As	
	() Information	1/21/2014 1:21:44 PM	A0 F5 2.0	336 None		Attach a Task To this Log	
	1 Information	1/21/2014 1:21:43 PM	AD #5 2.0	156 None		View	
	D Error	1/21/2014 1:17:43 PM	AD FS 2.0	362 None		1977	,
	Error	1/21/2014 1:17:43 PM	AD FS 2.0	378 None		Refresh	
	0 Error	1/21/2014 12:18:52 PM	AD FS 2.0	362 None		12 Help	
	😣 Error	1/21/2014 12:18:52 PM	AD F5 2.0	378 None		E	
	O Error	1/21/2014 12:07:45 PM	AD #5 2.0	364 None		Event 364, AD FS 2.0	A
	9 Error	1/21/2014 12:07:45 PM	AD FS 2.0	184 None		Fvent Properties	
	9 Error	1/21/2014 12:07:45 PM	AD FS 2.0	364 None			
	U Error	1/21/2014 12:07:45 PM	AD FS 2.0	303 None		Attach Task To This Event	
	Information	1/21/2014 12:04:39 PM	AD F5 2.0	251 None		Save Selected Events	
	Error	1/21/2014 11:56:49 AM	AD P5 2.0	364 None		Ro. Com	
	Error	1/21/2014 11:56:49 AM	AD PS 2.0	184 None			
	Error	1/21/2014 11:56:49 404	AD FS 2.0	364 None		Refresh	
	Enor	121/2014 11:56:49 464	A0 F3 2.0	303 Norie		1 Help	•
	Error Error	1/21/2014 11:50:12 AM	AUFS2.0	364 None		-	
	Ener	1/21/2014 11:56:12:00	AD F5 2.0	264 None	-		
	- Dia	TELEVICE FOR THE PARTY	Reform	COT HATE			
	Event 364, AD FS 2.8				×		
	General Details						
					1		
	C Friendly-View	w					
	- «Event ymins="http:/	/schemas microsoft.com/win/2004/08/er	ents /event				
	- <system></system>	50101105111010501100111/1111/2001/00/0					
	<pre>Provider Name="#"""""""""""""""""""""""""""""""""""</pre>	D FS 2.0" Guid="{20F25DDB-09F5-404B-84	56-EDAE2E12EE813* />				
	<eventid>364<td>rentID></td><td></td><td></td><td></td><td></td><td></td></eventid>	rentID>					
	<pre>cVersion>0</pre>	an>			_		
	<level>2</level>						
	<task>0</task>						
	<opcode>0<td>de></td><td></td><td></td><td></td><td></td><td></td></opcode>	de>					
	<keywords>0x800</keywords>	000000000001					
	<timecreated sys<="" td=""><td>emTime="2014-01-21T14:03:49.068007000</td><td>Z' /></td><td></td><td></td><td></td><td></td></timecreated>	emTime="2014-01-21T14:03:49.068007000	Z' />				
	<eventrecordid>1</eventrecordid>	07					
	<correlation activi<="" td=""><td>tyID="{25EF66E7-D657-4F41-82D3-DAE8C</td><td>3D70A63}" /></td><td></td><td></td><td></td><td></td></correlation>	tyID="{25EF66E7-D657-4F41-82D3-DAE8C	3D70A63}" />				
	<execution proces<="" td=""><td>sID="1380" ThreadID="4116" /></td><td></td><td></td><td>-</td><td></td><td></td></execution>	sID="1380" ThreadID="4116" />			-		
	A 10000						
•	1						