

Guide to Installing and Configuring ADFD for Ellucian CRM

NOTE - If you already have ADFS Setup, please proceed to Configure the ADFS Server

1) Go to Server Manager and choose to Add Roles and Features



2) Select the appropriate role

Select server roles

Select one or more roles to install on the selected server. Before You Begin Installation Type Roles Description Server Selection Active Directory Federation Services \sim Active Directory Certificate Services (AD FS) provides simplified, secured Server Roles Active Directory Domain Services identity federation and Web single Features Active Directory Federation Services sign-on (SSO) capabilities. AD FS includes a Federation Service that AD FS Active Directory Lightweight Directory Services enables browser-based Web SSO. Confirmation Active Directory Rights Management Services Application Server ≣ DHCP Server DNS Server Fax Server File and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services

DESTINATION SERVER ADFS.train.ellucian.com

Page 1 of 15 | Guide to Installing and Configuring ADFS | © 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

Next >

Install

Cancel

< Previous



3) When it finishes, click to "Configure the federation service on this server" and then proceed to the "Configure AD FS" section:





Install SSL Certificate on AD FS server

Import the SSL certificate into the Local Machine – Personal certificate store

		certlm -	[Certificates - Local C	omputer\Persona
File Action View Help Image: Constraint of the second seco) <mark>?</mark> F			
☐ Certificates - Local Compute △ △ Personal	er Issu द्वि*	ed To • .train.ellucian.com	lssued By *.train.ellucian.com	Expiration 5/12/2017
☐ Cert All Tasks	•	Request New Certificate	ucian.com	12/12/228
Cert View	•	Import	i.ellucian.com	5/20/2017
Contemponent C	t	Advanced Operations	ellucian.com	5/20/2017
▷ ☐ Untrust Help▷ ☐ Third-Party Root Certific▷ ☐ Trusted People	atior			

Navigate to the PFX with the certificate (be sure there's a private key associated with it) and complete the import. There are many resources online to explain these steps in more detail. (search "install SSL certificate windows")

Initial AD FS Configuration

This section will show the steps to configure AD FS for SSO with Microsoft CRM. These steps/screenshots should all be similar for AD FS 2.0, 2.1, and 3.0. The screenshots will primarily be form AD FS 3.0, but the previous versions will be similar enough. There are some additional steps required for AD FS 3.0, which will be called out at those particular steps.

To configure AD FS as a stand-alone federation server for Microsoft Dynamics CRM claims authentication, do the following steps:

- 1) On the AD FS server, click Start, and then click AD FS Management.
- 2) On the AD FS Management page, click AD FS Federation Server Configuration Wizard.
- 3) On the Welcome page, select Create a new Federation Service, and then click Next.
- On the Select Deployment Type page, select New federation server Farm, and then click Next. (adfs.school.edu)
- 5) Select your SSL certificate, add the Federation Service name (eg. adfs.school.edu), and then click Next.



6) AD FS 3.0 only – on the "Specify Service Account" screen, you may see warnings about gMSA (these are managed service accounts). These are only available if they have a Domain Controller running Windows 2012. If not, then you will see a warning such as:

	Specify Service Account	x
8	Error determining whether gMSA is available: Group Managed Service Accounts require a domain with at least one domain controller running Windows Server 2012, Windows Server 2012 R2 or later operating system. A domain controller that meets these requirements could not be found.	
	ОК	

You can safely ignore this warning. gMSA is not required to be the service account that ADFS runs on. It is an additional optimization that is available to customers if they have Win2012 domain controllers available. Simply choose the traditional service account option

- 7) AD FS 3.0 only If you see an error about "Group Managed Service Accounts are not available because the KDS Root Key has not been set", then open a Powershell window and run the following:
 - a. Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
- 8) AD FS 3.0 only At the "Specify Configuration Database" window, choose the Windows Internal Database



9) Review the settings on the Summary page, and then click Next.

10)Click Close to close the AD FS Configuration Wizard.

11) If you have not created a host record in DNS for the federation server name you specified in Step 5 previously, do so now.

Verifying AD FS installation

Use the following steps to verify the AD FS 2.0 installation:

- a. On the AD FS server, open a browser
- b. Browse to the URL of the federation metadata. For example, <u>https://adfs.school.edu/federationmetadata/2007-</u>06/federationmetadata.xml
- c. Verify that no certificate-related warnings appear. If necessary, check your certificate and DNS settings



Configure the AD FS server

- 1) Configure AD FS to send the UPN LDAP attribute as a claim to a relying party
 - a) On the computer that is running Windows Server where the AD FS federation server is installed, start AD FS Management.



- c) Under Claims Provider Trusts, right-click Active Directory, and then click Edit Claims Rules.
- d) In the Rules Editor, click Add Rule.
- e) In the Claim rule template list, select the Send LDAP Attributes as Claims template, and then click Next.
- f) Create the following rule:

🕑 ellucian.

- i. Claim rule name: UPN Claim Rule (or something descriptive)
- ii. Add the following mapping:
 - 1. Attribute store: Active Directory
 - 2. LDAP Attribute: E-Mail-Addresses
 - 3. Outgoing Claim Type: UPN

\$ 1	Add Transform Claim Rule Wizard		
Configure Rule			
Configure Rule Steps • Choose Rule Type • Configure Claim Rule	You can configure this rule to send the values which to extract LDAP attributes. Specify how issued from the rule. Claim rule name: UPN Claim Rule Rule template: Send LDAP Attributes as Claim Attribute store: Active Directory Mapping of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) User-Principal-Name *	a of LDAP attributes as claims. Select an attribute store from the attributes will map to the outgoing claim types that will be is types: Outgoing Claim Type (Select or type to add more) VUPN V V V V V V V V V V V V V V V V V V V	
		< Previous Finish Cancel Help	

- g) Click Finish, and then click OK to close the Rules Editor.
- h) NOTE: With AD FS 3.0, there's a rule that sounds similar, called "Pass through all UPN claims". You still need to create the above rule.

Configure a Dev relying party trust

- a. On the computer that is running Windows Server where the AD FS federation server is installed, start AD FS Management.
- b. In the Navigation Pane, expand Trust Relationships, and then click Relying Party Trusts.
- c. On the Actions menu located in the right column, click Add Relying Party Trust.
- d. In the Add Relying Party Trust Wizard, click Start.



e. On the Select Data Source page, click Import data about the relying party published online or on a local network, and then type the URL

https://adfsdevus01.elluciancloud.com/FederationMetadata/2007-06/FederationMetadata.xml

f. Click Next.

ii.

- i. If you receive an error, try accessing the above URL from a browser. If you receive a certificate warning, then import the root certificate into the Local Computer's "Trusted Root Certification Authorities"
- **g.** On the Specify Display Name page, type a display name, such as RecruiterSaaS Relying Party, and then click Next.
- h. On the Choose Issuance Authorization Rules page, click Permit all users to access this relying party, and then click Next.
- i. On the Ready to Add Trust page, on the Identifiers tab, verify that Relying party identifiers has one or more identifiers.
- j. Click Next, and then click Close.
- **k.** If the Rules Editor appears, click Add Rule. Otherwise, in the Relying Party Trusts list, right-click the relying party object that you created, click Edit Claims Rules, and then click Add Rule.
- I. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.
- m. Create the following rule:
 - i. Claim rule name: Pass Through UPN (or something descriptive)
 - Add the following mapping:
 - 1. Incoming claim type: UPN
 - 2. Pass through all claim values

Q	Add Transform Claim Rule Wizard
Configure Rule	
Steps Choose Rule Type Configure Claim Rule	You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claim type and whether only some claim values or all claim values should pass through. Claim rule name: Pass Through UPN Rule template: Pass Through or Filter an Incoming Claim Incoming claim type: UPN Incoming claim type: UPN Incoming claim type: UPN Incoming name ID format: Unspecified Incoming claim values Incoming claim value Incoming claim value
	< Previous Finish Cancel

- n. Click Finish.
- o. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.
- **p.** Create the following rule:



- Claim rule name: Pass Through Primary SID (or something descriptive) i. ii.
 - Add the following mapping: 1. Incoming claim type: Primary SID 2. Pass through all claim values

Q	Add Transform Claim Rule Wizard
Configure Rule	
Steps Configure Claim Rule Configure Claim Rule	You can configure this rule to pass through or fitter an incoming claim. You can also configure this rule to fitter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through. Claim rule name: Pass Through Primary SID Rule template: Pass Through or fitter an Incoming Claim v Incoming claim type: immery SID Incoming claim type: immery SID Incoming rame ID format: Unspecified Incoming rame ID format: Unspecified Incoming claim values v Pass through only a specific claim value v Incoming claim value: v Incoming claim value: v Pass through only claim values that match a specific enail suffix value: Erample: fabrikam.com Pass through only claim values that start with a specific value: Starts with: Example: FABRIKAMY Example: FABRIKAMY
	< Previous Finish Cancel

q. Click Finish.

i.

- r. In the Rules Editor, click Add Rule.
- s. In the Claim rule template list, select the Transform an Incoming Claim template, and then click Next.
- Create the following rule: t.
 - Claim rule name: Transform Windows Account Name to Name (or something descriptive)
 - ii.
- Add the following mapping:
 1. Incoming claiming type: Windows account name
 2. Outgoing claim type: Name or * Name
 3. Pass through all claim values



Ŷ	Add Transf	orm Claim Rule Wizard
Configure Rule		
Steps Choose Rule Type Configure Claim Rule	You can configure this rule to also map an incoming claim v outgoing claim type and whe Claim rule name: Transform Windows Account Rule template: Transform an	o map an incoming claim type to an outgoing claim type. As an option, you can value to an outgoing claim value. Specify the incoming claim type to map to the ther the claim value should be mapped to a new claim value.
	Incoming claim type: Incoming name ID format:	Windows account name
	Outgoing claim type:	Name V
	Outgoing name ID format: Pass through all claim val Replace an incoming clai	Unspecified v ues m value with a different outgoing claim value
	Incoming claim value: Outgoing claim value:	Browse
	O Replace incoming e-mail : New e-mail suffic:	suffix claims with a new e-mail suffix Example: fabrikam.com
		< Previous Finish Cancel

u. Click Finish, and when you have created all three rules, click OK to close the Rules Editor.

Order 1	Rule Name Pass Through UPN	UPN	1
2	Pass Through Primary SID Transform Windows Account Name to N	Primary SID Name	
			\$
			•
Add R	he Edt Rule Remove Rule	í.	

Configure a Prod relying party trust

- v. On the computer that is running Windows Server where the AD FS federation server is installed, start AD FS Management.
- w. In the Navigation Pane, expand Trust Relationships, and then click Relying Party Trusts.
- x. On the Actions menu located in the right column, click Add Relying Party Trust.
- y. In the Add Relying Party Trust Wizard, click Start.
- z. On the Select Data Source page, click Import data about the relying party published online or on a local network, and then type the URL

https://adfsprodus01.elluciancloud.com/FederationMetadata/2007-06/FederationMetadata.xml

aa. Click Next.

) ellucian.

- If you receive an error, try accessing the above URL from a browser. If you receive a i. certificate warning, then import the root certificate into the Local Computer's "Trusted Root Certification Authorities"
- bb. On the Specify Display Name page, type a display name, such as RecruiterSaaS Relying Party, and then click Next.
- cc. On the Choose Issuance Authorization Rules page, click Permit all users to access this relying party, and then click Next.
- dd. On the Ready to Add Trust page, on the Identifiers tab, verify that Relying party identifiers has one or more identifiers.
- ee. Click Next, and then click Close.
- ff. If the Rules Editor appears, click Add Rule. Otherwise, in the Relying Party Trusts list, right-click the relying party object that you created, click Edit Claims Rules, and then click Add Rule.
- gg. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.
- **hh**.Create the following rule:
 - Claim rule name: Pass Through UPN (or something descriptive) İ. ii.
 - Add the following mapping:
 - 1. Incoming claim type: UPN
 - 2. Pass through all claim values



\$	Add Transform Claim Rule Wizard
Configure Rule	
Steps	You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter
Choose Rule Type	claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.
 Configure Claim Rule 	Claim rule name:
	Pass Through UPN
	Rule template: Pass Through or Filter an Incoming Claim
	Incoming claim type: UPN V
	Incoming name ID format: Unspecified
	Pass through all claim values
	Pass through only a specific claim value
	Incoming claim value:
	Pass through only claim values that match a specific email suffix value:
	Email suffix value:
	Example: fabrikam.com
	O Pass through only claim values that start with a specific value:
	Starts with:
	Example: FABRIKAM\
	< Previous Finish Cancel

- ii. Click Finish.
- jj. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.
- kk. Create the following rule:

 i. Claim rule name: Pass Through Primary SID (or something descriptive)
 ii. Add the following mapping:

 1. Incoming claim type: Primary SID
 2. Pass through all claim values



\$	Add Transform Claim Rule Wizard
Configure Rule	
Steps Choose Rule Type Configure Claim Rule	You can configure this rule to pass through or fitter an incoming claim. You can also configure this rule to fitter claim type and whether only some claim values or all claim values should pass through. Claim rule name: Pass Through Primary SID Rule template: Pass Through or Filter an Incoming Claim Incoming claim type: Primary SID Incoming name ID format: Unspecified Incoming claim values Incoming claim value: Incoming claim value: Incoming claim value: Enail suffix value: Example: Fass through only claim values that match a specific email suffix value: Example: Starts with: Example: Example: FABRIKAMV
	< Previous Finish Cancel

II. Click Finish.

mm. In the Rules Editor, click Add Rule.

- nn. In the Claim rule template list, select the Transform an Incoming Claim template, and then click Next.
- oo. Create the following rule:
 - Claim rule name: Transform Windows Account Name to Name (or something i. descriptive)
 - ii.
- Add the following mapping:
 1. Incoming claiming type: Windows account name
 2. Outgoing claim type: Name or * Name
 3. Pass through all claim values



\$	Add Transform Claim Rule Wizard
Configure Rule	
Configure Rule Steps Choose Rule Type Configure Claim Rule	You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value. Claim rule name: Transform Windows Account Name to Name Rule template: Transform an Incoming Claim Image: Windows account name Incoming claim type: Windows account name Incoming name ID format: Unspecified Outgoing name ID format: Unspecified Inspecified Image: Claim value Outgoing name ID format: Unspecified Incoming claim value Image: Claim value Outgoing name ID format: Unspecified Incoming claim value Image: Claim value Outgoing claim value Image: Claim value Incoming claim value Image: Claim value Incoming claim value Enouge: Claim value Incoming claim value: Enouge: Claim value Incoming claim value Enouge: Claim value Incoming claim value Enouge: Claim value
	New e-mail suffix: Example: fabrikam.com

pp. Click Finish, and when you have created all three rules, click OK to close the Rules Editor.

Order 1	Rule Name Pass Through UPN	Issued Claims UPN	
2	Pass Through Primary SID	Primary SID	
			\$
Add R	ule Edit Rule Remove Rule	[



2) (AD FS 3.0 only) Enable Forms Authentication

By default, forms authentication is not enabled for the Intranet. The default is to use Windows authentication, which will use Integrated Windows Authentication (Negotiate – Kerberos and NTLM). If so desired, enable forms authentication:

- a. Log on to the AD FS server as an administrator.
- b. Open the AD FS management console and click Authentication Policies.
- c. Under Primary Authentication, Global Settings, Authentication Methods, click Edit.
- d. Under Intranet, enable (check) Forms Authentication.

Edit Global Authentication Policy
Primary Multi-factor
Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.
If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.
Extranet
Forms Authentication Certificate Authentication
Intranet Forms Authentication Windows Authentication Certificate Authentication
Enable device authentication
OK Cancel Apply



Information to send

UPN/sAMAccountName Information

- a. Open Active Directory Users and Computers on a Domain controller
- b. Locate a user account
- c. Right client and go to properties
- d. Click on the "Account" tab
- e. The value under "Userlogonname:" is the sAMAccountName
- f. The value in the drop down box next to that is the UPN for that account.

General	Address	Account	Profile	Telephones	Organization
User logon name:					
belegg			@ad.admin 💌		•

Federation Metadata XML URL

g. i.e. https://adfs.school.edu/federationmetadata/2007-06/federationmetadata.xml