# Single Sign-On (SSO) Options

Last Modified on 05/04/2021 3:04 pm EDT

The UNIFI platform can act as a Service Provider for SAML 2.0-compliant Identity Providers. Documentation is available for the Identity Providers listed below. If you're using an Identity Provider that isn't listed, please reach out to us (support@unifilabs.com) for assistance.

Supported SAML 2.0-based SSO functionality

- Single click user sign-on
- Automatic user creation on first sign-on.

# ΟΚΤΑ

Click here to view instructions

### **One Login (desktop client)**

Click here to view instructions

### One Login (web client)

Click here to view instructions

### **Microsoft Azure**

Click here to view instructions

# AD FS

Prerequisite: Install and configure an AD FS server

This may already be set up by your company administrator. If not, set up an AD FS (Active Directory Federation Services) Server according to Microsoft's Deployment Guide.

- ADFS 3.0 on (Server 2016 and 2012R2): https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/windows-server-2012-r2-ad-fs-deployment-guide
- ADFS 2.0 (Server 2008): http://go.microsoft.com/fwlink/p/?LinkId=191723

#### Configure AD FS to use a relying party for UNIFI

Use the procedure in this section to configure a relying party for UNIFI. The relying party defines how AD FS recognizes the relying party application (UNIFI) and issues claims to it. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer. For additional information about accounts and group memberships, see Understanding Local Users and Groups

To configure AD FS for a relying party (AD FS 3.0)

- 1. On the AD FS server, open the AD FS Management console.
- 2. In the navigation pane, expand **Trust Relationships**, and then click the **Relying Party Trusts** folder.
- 3. In the right pane, click Add Relying Party Trust. This opens the Add Relying Party Trust wizard.

- 4. On the Welcome to the Add Relying Party Trust Wizard page, click Start
- 5. Select Enter data about the relying party manually, and then click next.

<b>\$</b>	Add Relying Party Trust Wizard
Select Data Source	
Steps Steled Data Source Society Display Name Configure Cetificate Configure URL Configure URL Configure URL Configure URL Configure Metadar Automation Pulses Ready to Add Tuat Prinsh	Select an option that this wizard will use to obtain data about this relying party:         Import data about the relying party published online or on a local network.         Due this option to import the necessary data and coefficients from a relying party organization that publishes as federation metadata orders or on a local network.         Pederation metadata address (host name or URL):
	< Previous Next > Cancel

6. Type a relying party name, such as UNIFI, and then click **Next**.



7. Make sure AD FS Profile is selected, and then click Next.



8. Do not use a token encryption certificate. Click Next.

<b>%</b>	Add Relying Party Trust Wizard
Configure Certificate	•
Seps Wilcome Select Data Source Secoly Date/Prile Choose Profile Configure URL Configure URL Configure Mahfedor Authorization New? Proces Issuance Authorization News Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the dams that are sent to this retying party. The retying party will use the private key of this certificate to deput the claims that are sent to it. To specify the certificate, clock Browse
	< Previous Next > Cancel

9. Click to select the Enable support for the SAML 2.0 WebSSO protocol check box.

10. In the Relying party SAML 2.0 SSO service URL field, type the address https://licensing.inviewlabs.com/api/Login/OneLogin. Click Next.

<b>\$</b>	Add Relying Party Trust Wizard
Configure URL	
Steps  Websome Select Data Source Specify Daplay Name Consog Parls Configure Cestificate Configure URL Configure URL Configure URL Configure Multifactor Authorization Now? Concose Issuance Authorization Rules Ready to Add Truit Finish	AD FS supports the WS-Truit, WS-Federation and SAML 2.0 Web SSO protocols for relying parties. # WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URLs.  Relying party WS-Federation Passive protocol URL:  Example: https://s.cortoso.com/adfs/fa/  Enable support for the SAML 2.0 Web/SSO protocol The SAML 2.0 Web/SSO protocol The SAML 2.0 SSO service URL:  https://cerving.inviewlabs.com/adfs/fa/  Relying party SAML 2.0 SSO service URL:  https://cerving.inviewlabs.com/adfs/fa/
	< Previous Next > Cancel

11. Type the name of the relying party trust identifier, **INVIEWIabs** (case sensitive), and then click **Add**. Click **Next**.

<b>9</b>	Add Relying Party Trust Wizard	
Configure Identifiers		
Steps	Relving parties may be identified by one or more unique identifier strings. Specify the identifiers for this	nelvina
Welcome	party trust.	
Select Data Source	Relying party trust identifier:	
Specify Display Name		ldd .
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust	
Configure Certificate	Relying party trust identifiers:	
Configure URL	INVIEWIebs Re	move
Configure Identifiers		
<ul> <li>Configure Multi-factor Authentication Now?</li> </ul>		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
• Frish		
	<previous ned=""> Car</previous>	ncel

12. Choose your Multi-factor Authentication settings according to your company policy. This document will use the default option of not using multi-factor authentication.

13. Select **Permit all users to access this relying party** or other selection that applies to your SSO scenario. Click **Next**.

14. On the Ready to Add Trust page, there is no action required, click Next.

15. On the Finish page, click **Close**.

#### Configure the claim rules

Use the procedure in this step to send values of a Lightweight Directory Access Protocol (LDAP) attribute as claims and specify how the attributes will map to the outgoing claim type.

To configure a claim rule:

1. Select the Relying Party Trust you just created in the previous steps. On the Issuance Transform Rules tab, click Add Rule.

2. On the Select Rule Template page, select Send LDAP Attributes as Claims. Click Next.

3. On the Configure Rule page, type a name for the claim rule in the **Claim rule name** field. For example, name it UNIFI LDAP.

4. From the Attribute Store drop-down list, select Active Directory.

5. In the Mapping of LDAP attributes to outgoing claim types section, under LDAP Attribute, select **E-Mail-Addresses**.

6. Under Outgoing Claim Type, select E-Mail Address.

7. Configure additional Incoming Claims (Optional):

- Map Given-Name to Given Name
- Map Surname to Surname

#### 8. Click Finish

You c	an configure this rule to send the values	of LD	AP attributes as claims. Select an attribute store from	
which	to extract LDAP attributes. Specify how i from the rule.	the at	tributes will map to the outgoing claim types that will t	æ
Claim	rule name:			
<b>N</b> 1	ILCAP			
Lie :	emplate: Send LDAP Attributes as Claim	6		
ent.	An store:			
ktive	e Directory	-	~	
lann	ing of LDAP attributes to outgoing claim (	hnes		
-45	LDAP Attribute (Select or type to add more)	0.000	Outgoing Claim Type (Select or type to add more)	
•	E-Mail-Addresses	¥ 8	Mail Address	¥
		¥		¥
_				
			_	

9. Under the Issuance Transform Rules tab, click Add Rule (to add another rule).

10. On the Select Rule Template page, select Transform an Incoming Claim.

11. On the Configure Rule page, type a name for the claim rule in the **Claim rule name** field. For example, UNIFI Transform.

- 12. From the Incoming claim type drop-down list, select E-Mail Address.
- 13. From the Outgoing claim type drop-down list, select Name ID.
- 14. From the Outgoing name ID format drop-down list, select Email.
- 15. Click Finish, then click OK.

laim rule name:			
INIFI Transform			
Lie template: Transform an	Incoming Claim		
coming claim type:	E-Mail Address	*	
coming name ID format:	Unspecified	×	
Autgoing claim type:	Name ID	~	
Autgoing name ID format:	Enal		
Incoming claim value: Outgoing claim value:		Browse	
Replace incoming e-mail	suffix claims with a new e-mail suffix		
New e-mail suffic:			
	Example: fabrikam.com		

#### Add Group Membership Claims (Optional)

Use this section to configure AD FS to send AD Group Membership as claims to Unifi. If a group that does not exist in UNIFI is sent on a claim, it will create the group and add the user to it. The user will be removed from any groups that do not appear in their claims. This means that any non-AD groups created inside of UNIFI will be removed from AD FS authenticated users if this feature is used.

There are two methods for sending group membership as claims. One is to send all group memberships, and the other will require you to set up which groups to send.

To send all group memberships as claims:

1. Right-click on the Relying Party Trust you have created.

#### 2. Select Edit Claim Rules

3. Either click Add Rule to add a new rule (select the Send LDAP Attributes as Claims), or highlight the rule that issues the email and other claims then click Edit Rule

4. Under LDAP Attribute, add a row with one of the Token-Groups values, depending on how you would like the group name formatted, most likely Token-Groups – Unqualified Names

#### 5. Under Outgoing Claim Type, select Group

6. Click Ok or Finish

7. If desired, you can at this point add transformation rules to rename the groups before sending them

- 8. Click Ok
- To send specific group memberships as claims:
- 1. Right-click on the Relying Party Trust you have created.
- 2. Select Edit Claim Rules
- 3. Click Add Rule
- 4. In the Select Rule Template page, select Send Group Membership as a Claim
- 5. On the Configure Rule page, type a name for the claim rule in the **Claim rule name** field.
- 6. Click **Browse...** and find the group whose members should receive a claim.
- 7. In Outgoing claim type, select Group
- 8. In Outgoing claim value, type the name of the group as you want it to appear in UNIFI
- 9. Click Finish
- 10. Repeat from step 3 for additional groups as desired
- 11. Click OK

Edit Rul	e - UNIFI SSO Test Group
You can configure this rule to send a claim group that the user is a member of, and spo	based on a user's Active Directory group membership. Specify the ecify the outgoing claim type and value to issue.
Claim rule name:	
UNIFI SSO Test Group	
Rule template: Send Group Membership as	a Claim
User's group:	
INVIEWLABS\SSO Test Group	Browse
O danina chim hana:	
Group	
and a	
Outgoing name ID format:	
Unspecified	Y
Outgoing claim value:	
SSO Test Group	

#### Export the signing certificate

Use the procedure in this section to export the token signing certificate of the AD FS server with which you want to establish a trust relationship, and then copy the certificate to a location that you can access.

To export a token signing certificate:

- 1. On the AD FS server, open the AD FS Management console.
- 2. In the navigation pane, expand **Service**, and then click the **Certificates** folder.
- 3. Under Token signing, click the primary token certificate as indicated in the Primary column.
- 4. In the right pane, click View Certificate link. This displays the properties of the certificate.
- 5. Click the **Details** tab.
- 6. Click Copy to File. This starts the Certificate Export Wizard.
- 7. On the Welcome to the Certificate Export Wizard page, click Next.
- 8. On the Export Private Key page, click **No, do not export the private key**, and then click **Next**.
- 9. On the Export File Format page, select DER encoded binary X.509 (.CER), and then click Next.



10. On the File to Export page, type the name and location of the file that you want to export, and then click **Next**. For example, enter **C:\ADFS.cer**.

- 11. On the Completing the Certificate Export Wizard page, click Finish.
- 12. Once exported, use a utility below to convert it to .pem format.

Convert the certificate:

1. OpenSSL on Linux or Mac (Not included with Windows):

Convert the DER encoded file to PEM using OpenSSL with the following command: **openssl x509 - in C:\ADFS.cer - inform DER -out C:\ADFS.pem** 

2. SSLShopper.com Website:

Go to https://www.sslshopper.com/ssl-converter.html and use the tool provided.

### **Configure a New Identity Provider in UNIFI**

Use this example configuration to create an Identity Provider registration in the https://licensing.inviewlabs.com website or in the Unifi Application.

1. In a different web browser window, sign on to your **UNIFI** company site as an administrator.

#### 2. Click on the Users.

😨 UNIFI	UNIFI Web Portal				🛔 Demo Admin 🗸 🛓
Deshboard	NAVIGATION	SSO Ic	dentity Pro	viders	Ø
D Project Analytics	<ul> <li>Wanage Users</li> <li>User Groups</li> </ul>	Provide	ers		add provider
Shared Parameters	Office Locations	Default	Name	URL	
Subscriptions	Configure SSO	~	UNIFI Labs	This is the default UNIFI provider. Users will log in with with their UNIFI email and password.	
🕫 Notifications	TOOLS				
Libraries	<ul> <li>Import Users</li> <li>Export User Report</li> </ul>				
Satch Editor					
👗 Users					
<ul> <li>Settings</li> </ul>					

#### 3. Click on **Configure SSO**.

#### 4. Click on the **Add Provider**.

#### 5. In the Add SSO Provider window, perform the following steps:

Add SSO Provider	$\times$
Name	
SAML SSO	
URL	_
https://login.microsoftonline.com/	
Token	
Token	
Certificate	
BEGIN CERTIFICATE	<u>^</u>
	•
SAVE CAN	CEL

a. In the Name textbox, type the name of the Identity Provider Name.

b. In the **URL** textbox paste the Provider Login URL value, which you have copied from Azure portal.

c. Open the **Certificate** that you have downloaded from the Azure portal in notepad, remove the —BEGIN CERTIFICATE— and —END CERTIFICATE— tag and then paste the remaining content in the Certificate textbox.

d. Select the "Make this the default identity provider" checkbox.

Provider URL – The SAML endpoint from the AD FS Management tool. Look under AD FS -> Service -> Endpoints for SAML 2.0/WS-Federation.

- Bearer Token Used for SCIM provisioning, optional field.
- Certificate The contents of the ADFS.pem file created in the previous step.
- Is Default Provider If checked, this will be used for new users as they are created.

### Import Users in UNIFI (Optional)

If you choose not to import users, they can be created through an Identity Provider initiated session. To be able to begin a Service Provider Initiated session (logging into the Portal or the Unifi Client), we need to know to associate the user with the identity provider. Otherwise, they can use a known address, such as the administrator's email in order to get to the SSO provider the first time they log in on a machine.

Use the procedure in this section to batch create users in Unifi and set their identity provider to the newly created identity provider.

- 1. Open Unifi application
- 6. Login as company admin user
- 7. Go to the user management screen
- 8. Click Batch Create

9. You may either paste from excel using the Paste from Excel tab or you can manually import your users by copy and pasting their email addresses into the boxes provided in the Manual Import tab.

10. You will want to uncheck Automatically send out activation email. This email would normally notify your users that an account has been created for them with their credentials.

11. Set **Identity Provider** to the identity provider you created in the Create New Identity Provider in the UNIFI section.

12. Click Import Users.

	or Croation	음이가 모두 1
Paste from Excel	Manual Import	
Paste your data from either a normal exc the column orders other columns will	m an excel spreadsheet belo el spreadsheet OR a comma are the same: 1) Email Addre be ignored.	w. You must copy and paste from separated (CSV) file. Make sure that ess. 2) First Name, 3) Last Name. All
Import Users As: <ul> <li>Regular User</li> <li>Company Admin</li> </ul>	Automatically send Set Temporary Password	f out activation email 🕜
	Inview Labs	*
Email Address	First Name	Last Name
Clear Fields Imp	ort Users	