Portal SSO: Transform UserPrincipalName to NameID

Last Modified on 03.05.2024

To successfully configure Single Sign-On (SSO) to the Userlane Portal using Microsoft ADFS as your Identity Provider (IdP), you must add a Rule to the Claim Issuance Policy of the Relying Party Trust you created for Userlane.

To do so, follow the steps outlined and shown below:

 Go to the Control Panel > All Control Panel Items > Administrative Tools and open the AD FS Management

	Name	Date modified	Type	Size
	Tomin 10 million	0/15/2010 7.10 414	51. 6.1.1	
*	Ierminal Services	9/15/2018 7:19 AM	Filefolder	
	Active Directory Administrative Center	9/15/2018 7:13 AM	Shortcut	2 KB
π	Active Directory Domains and Trusts	9/15/2018 7:14 AM	Shortcut	2 KB
*	🗦 Active Directory Module for Windows PowerShell	9/15/2018 7:13 AM	Shortcut	2 KB
*	provide Active Directory Sites and Services	9/15/2018 7:13 AM	Shortcut	2 KB
	notive Directory Users and Computers	9/15/2018 7:14 AM	Shortcut	2 KB
c	狩 AD FS Management	9/15/2018 7:13 AM	Shortcut	2 KB
	📝 ADSI Edit	9/15/2018 7:13 AM	Shortcut	2 KB
	Certification Authority	9/15/2018 7:13 AM	Shortcut	2 KB
	🌮 Component Services	9/15/2018 7:12 AM	Shortcut	2 KB
	🎥 Computer Management	9/15/2018 7:12 AM	Shortcut	2 KB
	📸 Defragment and Optimize Drives	9/15/2018 7:12 AM	Shortcut	2 KB
	📜 Disk Cleanup	9/15/2018 7:12 AM	Shortcut	2 KB
	🚔 DNS	9/15/2018 7:13 AM	Shortcut	2 KB
	🛃 Event Viewer	9/15/2018 7:12 AM	Shortcut	2 KB
	Group Policy Management	9/15/2018 7:13 AM	Shortcut	2 KB

2. On the left column, select Relying Party Trust, select your Userlane configuration and click on Edit Claim Issuance Policy on the right column.



3. In the new window, click on Add Rule

Order	Rule Name	Issued Claims			
			\$ \$		
Add F	Lule Edit Bule Remove Bule				

4. Then select Transform as Incoming Claim from the dropdown and click on Next

Select Pule Tomplet					
Select Rule Templa					
Steps	Select the template for the claim rule that you want to create from the following list. The description provide	s			
Choose Rule Type	details about each claim rule template.				
Configure Claim Rule	Claim rule template:				
	Send LDAP Attributes as Claims				
	Send LDAP Attributes as Claims				
	Send Group Membership as a Claim Transform an Incoming Claim				
	Pass Through or Filter an Incoming Claim Send Claims Using a Custom Rule 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 as 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.				

- 5. In the next screen complete the following form and press OK:
 - 1. Claim rule name: Transform UserPrincipalName to NameID
 - 2. Incoming claim type: UPN
 - 3. Outgoing claim type: Name ID
 - 4. Outgoing name ID format: Email
 - 5. O Select "Pass through all claims"

You can configure this rule to		
also map an incoming claim v outgoing claim type and whe	o map an incoming claim type to an outgoing claim type. As an op value to an outgoing claim value. Specify the incoming claim type ther the claim value should be mapped to a new claim value.	tion, you can to map to the
laim rule name:		
Transform UserPrincipalName	e to NameID	
Rule template: Transform an	Incoming Claim	
ncoming claim type:	UPN	~
ncoming name ID format:	Unspecified	~
Outgoing claim type:	Name ID	~
Outgoing name ID format:	Email	~
Incoming claim value:		
Outgoing claim value:		Browse
	suffix claims with a new e-mail suffix	
Preplace incoming emails		
New e-mail suffix:		