

Engage SAML Single Sign-On Set up Guide

Revision history

Rev	Date	Author	Description
1	04/03/2022	Wilson Lun	Initial Draft
2	24/06/2022	Wilson Lun	Add section to configure Azure Active Directory for SSO
3	23/03/2023	Brian Law	Remove authority claim rule Add authority_id claim rule

Disclaimer

This document contains information on a product under development. Amino Communications Ltd reserves the right to change or discontinue this product without notice.

Trademarks and copyright

Amino Communications and the Amino logo are trademarks of Amino Communications Limited.

Contents

Revision history
Disclaimer2
Trademarks and copyright2
Contents
Configure SAML authentication in Engage6
Configuring Your SAML 2.0 Identity Provider solution to work with Engage7
Configure ADFS as an Identity Provider for Single Sign-on8
Configure Engage as a trusted relying party8
Configure claim rules for the Engage relying party11
Configure signature verification for SAML requests13
Optional: configure authority_id claim rules15
Set up an Active Directory User and map to an Engage user role
Assign the user to the Active Directory User Group17
Configure authority_id claim rule with Token-Groups – Unqualified Names attribute
Configure Azure Active Directory as an Identity Provider for Single Sign-on
Configure Engage as a trusted relying party21
Configure claim rules for the Engage relying party23
Grant user to access Engage24
Signature verification for SAML requests24
Appendix: Authority Id List

Configure SAML authentication in Engage

To set up SAML 2.0 based federation, it is required to configure Engage and the identity provider to trust each other. This section describes the configuration to enable this trust environment for the Engage side.

- 1. Sign in to Engage with an Administrator user account
- 2. Navigate to the SAML Authentication tab: Manage Domain > Details > SAML Authentication
- 3. In the SAML Authentication tab, toggle the checkbox under Enable SAML Authentication

SAML Authentication	
Enable SAML Authentication	
When enabled, your SAML 2.0 identity provider (IdP) will be used for a Engage.	authentication. You can check the document for instructions on how to configure your IdP solution to work with
✓	
Entity ID	
SAML Request Binding	
HTTP-Redirect	~
Single Sign-On URL	
X.509 Signing Certificate	
Upload the X.509 Certificate from your IdP.	
Choose File No file chosen	
Sign Request	
When enabled, the SAML Authentication request will be signed. Downl	load the certificate and configure it in your IdP to validate the signature.
Save	

- 4. In the Entity ID textbox, input the entity ID of the identity provider
- 5. In SAML Request Binding dropdown box, select the binding protocol for Single Sign-On URL
- 6. In **Single Sign-On URL** textbox, input the endpoint URL of single sign-on service provided by the identity provider
- 7. Under **X.509 signing certificate**, click **Choose File** and upload the public certificate from identify provider
- 8. Under **Sign request**, toggle the checkbox if expect SAML request is signed by Engage. If enable this setting, download the certificate provided by Engage and configure it in the identify provider.

Configuring Your SAML 2.0 Identity Provider solution to work with Engage

After setting up SAML authentication in the previous section, the identity provider (IdP) used for authentication will be known to Engage. The next step is to configure Engage as a service provider in your IdP.

To allow Engage to know about a user after the identity is verified by IdP, claims are required to be configured in your IdP such that the identity information is included in the authentication response. A list of the available claims used by Engage is shown below.

Name ID (Required)

This is an identifier of the user who is being authenticated.

user_loginname (Required)

This is the Engage login username of the user who is being authenticated. It must be in email address format.

authority_id (Optional)

This is a list of Engage user roles to be granted to the user who is being authenticated.

Engage manages user access control to resources through the use of user roles. User roles can be configured for users under **Mange Users** in Engage web application. After enabling Engage SAML Single Sign-On, user roles can also be granted by the authority_id attribute.

The user role authority id can be found in the **Appendix: Authority Id List**.

The following excerpt shows an example of attribute in SAML response:

<Attribute Name="authority_id">
 <AttributeValue>101</AttributeValue>
 <AttributeValue>103</AttributeValue>
 <AttributeValue>202</AttributeValue>
</Attribute>

Configure ADFS as an Identity Provider for Single Sign-on

This section provided instructions on how to integrate Active Directory Federation Services (ADFS) instances with Engage using SAML-based single-sign-on (SSO).

Configure Engage as a trusted relying party

To begin, we first configure the ADFS server to trust Engage as a relying party.

- 1. Sign in to the ADFS server
- 2. Open the Server Manager and select **AD FS Management** from Tools
- 3. In the left console tree, right-click **Relying Party Trusts** and then click **Add Relying Party Trust...**
- 4. In the Add Relying Party Trust Wizard, select the option Claims aware and click Start

🐃 Add Relying Party Trust W	fizard	×
Welcome		
Steps	Welcome to the Add Relying Party Trust Wizard	
Welcome		
Select Data Source	Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows	
 Choose Access Control Policy 	Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. <u>Learn more</u>	
Ready to Add Trust	Claims aware	
Finish	O Non claims aware	
	< Previous Start Cancel	

5. In the **Select Data Source** tab, select the option **Enter data about the relying party manually**

翰 Add Relying Party Trust	Wizərd ×
Select Data Source	
Steps Velcome Select Data Source Secify Display Name Configure Certificate Configure URL Configure Identifiers Choose Access Control Policy Ready to Add Trust Finish	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. 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): 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 exported 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. Pederation metadata file location: Browse Perior metadata about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.

- 6. In the **Specify Display Name** tab, specify the display name for the application.
- 7. In the **Configure Certificate** tab, leave the certificate settings at their defaults.
- 8. In the **Configure URL** tab, select the box **Enable support for the SAML 2.0 WebSSO protocol** and enter the SAML service endpoint.
 - a. For Engage: https://engage.aminoengage.com/engage/saml/SSO
 - b. For Orchestrate: <u>https://system.amino-orchestrate.com/system/saml/SSO</u>

훾 Add Relying Party Trust '	Wizard X
Configure URL	
Steps Velcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Identifiers Choose Access Control Policy Ready to Add Trust Finish	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSD protocols for relying parties. If 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-Trust protocol is always enabled for a relying party. Enable 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 URL: Example: https://fs.contoso.com/adfs/ls/ Enable support for the SAML 2.0 WebSSD protocol The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSD protocol Relying party SAML 2.0 SSO service URL: <hr/> https://engage.aminoengage.com/engage/saml/SSO Example: https://www.contoso.com/adfs/ls/
	< Previous Next > Cancel

- 9. In the **Configure Identifiers** tab, enter
 - a. For Engage: <u>https://engage.aminoengage.com/engage/saml/sp</u>
 - b. For Orchestrate: https://system.amino-orchestrate.com/system/saml/sp

and click Add

- 10. In the **Choose Access Control Policy** tab, select **Permit all users to access this relying party**, then click **Next** and review your setting.
- 11. In **Ready to Add Trust** tab, click **Next** if information is correct.
- 12. In **Finish** tab, toggle **Configure claims issuance policy for this application**, and click **Close** to complete.

输 Add Relying Party Trust	Wizard	X
Finish		
Steps Welcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Identifiers Choose Access Control Policy Ready to Add Trust Finish	The relying party trust was successfully added.	
	Close]

Configure claim rules for the Engage relying party

Next, add the claim rules for the relying party trust so that the attributes that Engage requires are added to the SAML authentication response. Engage requires two claims, **Name ID**, and **user_loginname**.

- 1. Right-click the relying party for Engage and then click Edit Claim Issuance Policy...
- In the Edit Claim Issuance Policy dialog box, click Add Rule... to create a claim rule for Name ID
- 3. Select Transform an Incoming Claim and then click Next.
- 4. Configure the rule with the following settings:
 - a. Claim rule name: NameID
 - b. Incoming claim type: UPN
 - c. Outgoing claim type: Name ID
 - d. Outgoing name ID format: Persistent Identifier

翰 Add Transform Claim I	Rule Wizard			>
Configure Rule				
Steps	You can configure this rule	e to map an incoming claim typ	be to an outgoing claim type. <i>i</i>	As an option, you can
Choose Rule Type	also map an incoming clair outgoing claim type and w	m value to an outgoing claim v hether the claim value should	value. Specify the incoming cl be mapped to a new claim va	laim type to map to the alue.
Configure Claim Rule	Claim rule name:			
	NamelD			
	Rule template: Transform a	an Incoming Claim		
	Incoming claim type:	UPN		~
	Incoming name ID format:	Unspecified		~
	Outgoing claim type:	Name ID		~
	Outgoing name ID format:	Persistent Identifier		~
	Pass through all claim v	values		
	 Replace an incoming of 	laim value with a different out	going claim value	
	Incoming claim value:			
	Outgoing claim value:			Browse
	 Replace incoming e-ma 	ail suffix claims with a new e-m	nail suffix	
	New e-mail suffix:			
		Example: fabrikam.com		
			< Previous Fin	ish Cancel

- 5. Click Finish
- 6. Next, click Add Rule... to create a claim rule for user_loginname
- 7. Select **send LDAP Attributes as Claims** and then click **Next**. Create a rule with the following settings:
 - a. Claim rule name: user_loginname
 - **b.** Attribute store: Active Directory
 - c. LDAP Attribute: E-Mail-Addresses
 - d. Outgoing Claim Type: user_loginname

Add Transform Claim I Configure Rule	Rule Wizard		×
Steps Choose Rule Type Configure Claim Rule	You co to extr from th Claim i	an configure this rule to send the values of L act LDAP attributes. Specify how the attribut e rule. ule name:	DAP attributes as claims. Select an attribute store from which es will map to the outgoing claim types that will be issued
	user_ Rule to Attribu Activo	loginname emplate: Send LDAP Attributes as Claims te store: s Directory no of LDAP attributes to outgoing claim tune	×]
		LDAP Attribute (Select or type to add more) E-Mail-Addresses	Outgoing Claim Type (Select or type to add more) user_loginname
	•	~	~
			< Previous Finish Cancel

- 8. Click Finish
- 9. In the Edit Claim Issuance Policy dialog box, click Apply and OK to complete

Configure signature verification for SAML requests

Next, configure the **signature verification certificate** which will allow verification of signatures in SAML requests. The certificate can be downloaded from **Manage Domain > SAML Authentication** in Engage.

- 1. Right-click the relying party for Engage and then click Properties
- 2. In Signature tab, click Add

Organization	Endpoints	Proxy Eng	lpoints	Notes	Advanced			
Monitoring	Identifiers	Encryption Signature			ccepted Claims			
Specify the signature verification certificates for requests from this relying party.								
Subject	Issu	Effect	ive Date	Expirati				
Add.	. Vie	w R	emove					
		OK	C	ancel	Apply			

3. Upload the signature verification certificate provided by Engage

Organization	Endpoints	Proxy Eng	lpoints	Notes	Advanced			
Monitoring	Identifiers	Encryption	Signat	ure A	Accepted Claims			
Specify the sig party.	nature verifica	tion certificate	s for requ	iests from	this relying			
Subject	Subject Issuer Effective Date							
1								
<					>			
				_				
Add.	Vie	w F	emove					

5. Click Apply and OK to complete

4.

Optional: configure authority_id claim rules

After completing the above sections, SSO should now work with Engage. This section is an optional step that will allow granting Engage User roles to users through set up claims in IdP.

There are several ways to retrieve a user's group membership and transform the membership into a claim. The following is an example of how to set up Active Directory user groups and map them to an Engage user role using the standard ADFS attribute, **Token-Groups – Unqualified Names**, to provide all group names as Engage user roles in the **authority_id** claim.

Set up an Active Directory User and map to an Engage user role.

- 1. In your Windows Server, open Active Directory User and Computers
- 2. Right-click Users and select New > Group

Active Directory Users and Computers			-	×
File Action View Help	7 🗔 🖓			
	· 🖉 🖉			
Active Directory Users and Com Name	Туре	Description		^
adfs	User	Built-in account for ad		
Builtin	. Security Group	Members in this group c		
> 🧰 Cext Bublishers	User Security Group	Members of this group		
> 💼 Domain Controllers	Security Group	Members of this group		
Foreign SecurityPrincipal: DefaultAccount	User	A user account manage		
Users Managed Service Accourt	. Security Group	Members in this group c		
Delegate Control mins	Security Group	DNS Administrators Gro		
Find dateProxy	Security Group	DNS clients who are per Designated administrato All workstations and ser		
n Admins	Security Group			
New > Computer				
All lasks > Contact		All domain quests		
View > Group		All domain users		
Refresh				
Export List	msDS-KeyCredential			
msDS-ResourcePrope	tyList IContainer			
Properties msDS-ShadowPrincip				
Help msImaging-PSPs				
MSMQ Queue Alias				
A ENSIC Printer				
Rensic User				
ENSIC Shared Folder				4
	Security Group			•

- 3. Create a group mapped to Engage user role with following settings:
 - a. Group name: < Engage user role authority id>

< Engage user role authority id > can be found in the **Appendix: Authority Id List**. The following is using **102(SYSTEM Operator)** as an example.

New Obje	ct - Group		×
8	Create in:	adfs-local.aminoengage.com/Users	
Group na	ame:		
102			
Group na	ame (pre-Wind	ows 2000):	
102			
Group	scope	Group type	
	main local	Security	
● Glo	bal	O Distribution	
OUni	iversal		
		OK Cancel	

4. Click **OK** to complete

Assign the user to the Active Directory User Group

- 1. Open Active Directory User and Computers
- 2. Right-click a user and select **Properties**



3. In Member Of tab, then click Add...

Test Properties				?	×
Remote control General Address Member Of	Remote D Account Dial-in	esktop Se Profile Env	rrvices Profile Telephones ironment	CO Organi Sessio	M+ zation
Member of:					
Name	Active Direct	ory Domain	Services Folde	:r	
Add	Remove				
Primary group: D	omain Users There is n you have application	o need to Macintosh ns.	change Primary clients or POSI>	group unk X-compliar	ess nt
0	K C	Cancel	Apply	Н	elp

4. In **Enter the object name to select** textbox, input the name of the Group mapped to Engage user role. Click **Check Names** to verify, and the group name will be underlined. Click **OK** to confirm.

Select Groups		×
Select this object type:		
Groups or Built-in security principals		Object Types
From this location:		
adfs-local.aminoengage.com		Locations
Enter the object names to select (examples):		
102		Check Names
Advanced	ОК	Cancel

5. In **Member Of** tab, a new group name will be added.

	opercies				f	
Remote	control	Remote [Desktop Sei	vices Profile	CON	1+
General	Address	Account	Profile	Telephones	Organiza	atio
Membe	er Of	Dial-in	Envi	ronment	Session	s
Member o	of:					
Name		Active Direct	ory Domain	Services Folder	r	
102		adfs-local.am	inoengage.	com/Users		
Domain	Users	adfs-local.am	inoengage.	com/Users		
Add.	_	D				
		Remove				
Primary gr	roup: D	lomain Users				
Primary gr Set Pri	roup: D	Iomain Users There is n you have application	io need to c Macintosh ns.	hange Primary g clients or POSIX	group unles <-compliant	35

6. Click **Apply** and **OK** to complete.

Configure authority_id claim rule with Token-Groups – Unqualified Names attribute

1. Right-click the relying party for Engage and then click Edit Claim Issuance Policy...

- 2. In the Edit Claim Issuance Policy dialog box, click Add Rule... to create a claim rule for authority
- 3. Select Send LDAP Attributes as Claims and then click Next.



- 4. Configure the rule with the following settings:
 - a. Claim rule name: authority_id
 - **b.** Attribute store: Active Directory
 - c. LDAP Attribute: Token-Groups Unqualified Names

d. Outgoing Claim Type: authority_id

Edit Rule	e - authority_id		
You can to extrac from the	configure this rule to send the values o t LDAP attributes. Specify how the attril rule.	f LE bute	OAP attributes as claims. Select an attribute store from whic is will map to the outgoing claim types that will be issued
Claim rule	e name:		
authority	/ id		
Rule tem	plate: Send LDAP Attributes as Claims		
Attribute	store:		
Active [Directory		\sim
Mapping	of LDAP attributes to outgoing claim ty	pes	:
	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)
•	Token-Groups - Unqualified Names	\sim	authority_id ~
		\sim	~
		_	
View F	Rule Language		OK Cancel

5. Click Finish

6. In the Edit Claim Issuance Policy dialog box, click Apply and OK to complete

Configure Azure Active Directory as an Identity Provider for Single Sign-on

This section provided instructions on how to integrate Azure Active Directory (Azure AD) with Engage using SAML-based single-sign-on (SSO).

Configure Engage as a trusted relying party

To begin, we first configure the ADFS server to trust Engage as a relying party.

- 1. Sign in to the Azure portal by using a Microsoft account
- 2. Select Azure Active Directory service

All services All								
All	Filter services							
Favorites								
Recents		.	[]	۲		SQL	3	{·· }
Categories	Azure Active	Virtual	Resource	App Services	Storage	SQL	Cost	Virtual
General	Directory	machines	groups		accounts	databases	Management	networks

- 3. On the left panel, select Enterprise Applications
- 4. To add an application, select **New Application**
- 5. In the Browse Azure AD Gallery page, select Create your own application

Browse Azure AD Gallery

+ Create your own application 8 Got feedback?

6. The **Create your own application** pane opens. Input a name and select **Integrate any other application you don't find in the gallery (Non-gallery)**

Create your own application	\times
Sot feedback?	
If you are developing your own application, using Application Proxy, or want to integrate application that is not in the gallery, you can create your own application here.	an
What's the name of your app?	
Amino Engage 🗸	
What are you looking to do with your application?	
O Configure Application Proxy for secure remote access to an on-premises application	
 Register an application to integrate with Azure AD (App you're developing) 	
 Integrate any other application you don't find in the gallery (Non-gallery) 	

7. Click Create.

8. Once the app is created, the Enterprise Application page shows. On the left panel, select **Single** sign-On

Home > Enterprise applications >	
Amino Engage O	verview
Overview	Properties
Deployment Plan	AE Name 🗊
Manage	Amino Engage 🗈
Properties	Application ID ①
🦀 Owners	Object ID ①
🎝 Roles and administrators	. 1
🚨 Users and groups	Cotting Started
Single sign-on	Getting started

9. On the Select a single sign-on method pane, select SAML

Select a single sign-on method Help me decide

SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

10. In the **Set up Single Sign-On with SAML** page, select the **Edit** button for **Basic SAML Configuration**

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide 🖒 for help integrating Amino Engage.

Basic SAML Configuration		
dentifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State (Optional)	Optional	
ogout Url (Optional)	Optional	

- 11. The Basic SAML Configuration pane opens.
 - a. Under Identifier (Entity ID) section, select Add identifier and input
 - i. For Engage: https://engage.aminoengage.com/engage/saml/sp

- ii. For Orchestrate: <u>https://system.amino-orchestrate.com/system/saml/sp</u>
- b. Under **Reply URL (Assertion Consumer Service URL)** section, select **Add identifier** and input
 - i. For Engage: https://engage.aminoengage.com/engage/saml/SSO
 - ii. For Orchestrate: https://system.amino-orchestrate.com/system/samI/SSO
- c. Under Sign on URL (Optional) section, input
 - i. For Engage: https://engage.aminoengage.com/engage/saml/SSO
 - ii. For Orchestrate: https://system.amino-orchestrate.com/system/samI/SSO

Basic SAML Configuration

☐ Save 🔗 Got feedback?		
floor Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. $ o$		
Identifier (Entity ID) * 🕕		
The unique ID that identifies your application to Azure Active Directory. This value must be unique acro	oss all applicatio	ns in
your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for	r IDP-initiated S.	<i>SO.</i>
	Default	
https://engage.aminoengage.com/engage/saml/sp	V 0	Î
Add identifier		
Renky LIRL (Assertion Consumer Service LIRL) *		
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML.	l to as the "Assei	rtion
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML. Index	I to as the "Asser Default	rtion
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML. Index https://engage.aminoengage.com/engage/saml/SSO	I to as the "Asset Default	rtion
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML. Index https://engage.aminoengage.com/engage/saml/SSO Add reply URL	I to as the "Assen Default	rtion
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML. Index https://engage.aminoengage.com/engage/saml/SSO Add reply URL	Default	rtion
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML. Index https://engage.aminoengage.com/engage/saml/SSO Add reply URL Sign on URL (Optional)	Default	rtion
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML. Index https://engage.aminoengage.com/engage/saml/SSO Add reply URL Sign on URL (Optional) Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is is	I to as the "Asset Default the sign-in page	e URL
Reply URL (Assertion Consumer Service URL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred Consumer Service" (ACS) in SAML. Index https://engage.aminoengage.com/engage/saml/SSO Add reply URL Sign on URL (Optional) Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is so for your application. This field is unnecessary if you want to perform identity provider-initiated single sign single sign or single sign.	to as the "Asset Default the sign-in page ign-on.	et URL

12. Click **Save** button at the top of the pane

Configure claim rules for the Engage relying party

Next, add the claim rules for the relying party trust so that the attributes that Engage requires are added to the SAML authentication response. Engage requires two claims, **Name ID**, and **user_loginname**.

1. On the Set up Single Sign-On with SAML page, select the Edit button for Attributes & Claims

Attributes & Claims		Ø
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

- 2. Skip configure the claim **Name ID**, because it is added as **Unique User Identifier** by Azure AD automatically
- 3. On Attributes & Claims page, select Add new claim button
- 4. On Manage Claim pane, create a cliam for user_loginname with the following settings:
 - **a.** Name: user_loginname
 - b. Source: Attribute
 - c. Source attribute: user.mail

🔚 Save 🗙 Discard changes 🕴 ,	중 Got feedback?
Name *	user_loginname
Namespace	Enter a namespace URI
Source *	• Attribute
Source attribute *	user.mail

5. Click Save button

Grant user to access Engage

Next, enable users to use Azure Single Sign On by granting access to Engage

- 1. In the Azure portal, select Enterprise Applications, and then select All applications.
- 2. In the applications list, select Amino Engage
- 3. On the left panel, select Users and groups
- 4. Select Add user/group button
- 5. In Add Assignment page, select user in Users list. Click Select button at the bottom of the pane.
- 6. Click Assign button

Signature verification for SAML requests

Azure AD does not validate signed authentication requests if a signature is present. There is no effect to enable **Sign Request** in Engage **SAML Authentication** page.

Appendix: Authority Id List

Module	Authority Role Name	Authority Id
System	Administrator	101
System	Operator	102
System	INI Signer	104
System	Server Monitor	105
Manage	Administrator	201
Manage	Operator	202
Manage	RMA User	204
Resolve	Domain Administrator	302
Resolve	Operator	303
Resolve	Technician	304
Resolve	Viewer	305
Optimize	Administrator	501
Optimize	Viewer	502