# Integrating authentication server with ForgeRock

On this page:

- Integrating the authentication server with ForgeRock
- Deploying the authentication server ٠
- Configuring SAMLv2 Remote Service Provider

This page contains the instructions to integrate the authentication server with the ForgeRock application (ForgeRock is the company that develops opensource identity and access management products for cloud, social, mobile, and enterprise environments). This documentation is based on ForgeRock version 13.0.0.

## Integrating the authentication server with ForgeRock

To integrate the authentication server with ForgeRock

- 1. Log in to ForgeRock as administrator.
- 2. Either select or create the realm, which will be used for integration. Make sure that the realm uses stateful sessions. The realm in this example is "twc".
- 3. In the realm overview select Authentication > Settings.
- 4. Click the General tab and clear the Use Stateless Sessions check box.
- 5. C

CK Save Cha	nges.	
🚯 Dashboard	Authentication Settings	
Authentication	9	
> Settings	Core User Profile Account Lockout General Security Post Authentication Processi	ing
> Chains		
> Modules	Default Authentication Locale en_US	
🖋 Services	Identity Types agent user	
Data Stores		
☑ Privileges	Pluggable User Status Event Classes	•
& Authorization	Use Stateless Sessions	•
Subjects		
Agents	Two Factor Authentication Mandatory	
🛷 STS	Default Authentication Level 0	
Scripts		
	Revert Save Changer	es

6. Go back to Dashboard and in the realm overview, select Create SAMLv2 Providers and then Create Hosted Identity Provider.

B Dashboard	Realm Overvie	ew		
<ul> <li>Authentication</li> <li>Sonicos</li> </ul>	Active 🛛 🚱 twc, twc.nomagic.com			Properties
<ul> <li>Data Stores</li> </ul>	Common Tasks			
☑ Privileges				
4 Authorization				
Subjects				
Agents			*	
IN STS	Create SAMLv2	Configure OAuth	Create Fedlet	Configure Google
>	Providers	Provider		Apps
	Ô	•	•	•
	Configure Salesforce CRM	Configure Social Authentication	Get Product Documentation	Create a Soap STS Deployment



#### 7. Fill in the Identity Provider data by selecting the realm, the signing key, and entering a new circle of trust's name.

This page allows you to configure this instance of OpenAll server as an identity Provider (DP). You can provide a Name for the provider, Circle of Trust (COT), its metadata of the provider and optionally Signing Certificate. A COT is a provide a Name for the provider. (SP) had trust each other and in effect represents the configured in a decimation to communications are performed. Metadata represents the configured in a decimation to communications are performed. Metadata represents the configured in provider and provider (SP) had trust each other and in effect represents the configured in a decimation to communications are performed. Metadata represents the configured in periods will be configured under the role read.	Create a SAMLv2 Identity Provider on this Server	Configure	Cancel
*Indicates required fea	This page allows you to configure this instance of OpenAM server as an identity Provider (IDP). You can provide a Name for the provider, Circle of Trust (COT), its metadata of the provider and optionally Signing C group of IDPs and Service Providers (SPs) that trust each other and in effect represents the configuration necessary protocols (ig GAMAU2) as well as the mechanism to communicat this is configuration to other entities (eg SPs) in a COT. We shall generate the metadata if you do not have one. You are required to pick a realm for more than one realm in the system. Otherwise, this provider will be configured under the root realm.	rtificate. A COT o execute feder this provider if	is a ration there are
b you have metadata for this provider? Yes in a interaction of the second secon		* Indicates re	aquired field
	Do you have metadata for this provider?: O Yes 🛞 No 🔮		
* Reading: Index of the set is a set of the set of the set of the set is a set of the set of the set is a set of the set is a set of the set of the set of the set is a set of the set of the set of the set is a set of the set is a set of the set of the set is a set of the set of the set of the set is a set of the set	metadata		
Circle of Trust  Choose from existing circles of trust listed or provide one to be created in which is IDP A COT is a group of IDPs and SPs that trust each other and provides the contines within which all SAML/2 communications are performed. * New Circle of Trust:  Attribute Mapping  Mapping attributes helps to ensure that both the Service Provider (SP) and the identity Provider (IDP) can recognize the same attributes that may have unique names. For example, the SP may have an attribute called UserName but the UP may call it UserIC Eliminating these inconsistencies by mapping the attributes will guarantee that the data will be passed correctly.  Attributes Mapping  Local Attribute Name  Server an attribute Name  Server an attribute Name	* Realm:: Mxc v * Name: http://openam.nomagic.com.8080/openam Signing Key: - v		
Choose from existing circles of trust listed or provide one to be created in which to indude this IDP A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAULy2 communications are performed. ** New Circle of trust:  Attribute Mapping Mapping attributes helps to ensure that both the Senice Provider (BP) and the identity Provider (DP) can recognize the same attributes that may have unique names. For example, the SP may have an attribute called UserName but the DP may call it UserID. Eliminating these inconsistencies by mapping the attributes will guarantee that the data will be passed corredy.  Attributes Mapping  Attributes Mapping  Centers  Name in Assertion  Local Attribute Name  Select an attribute	Circle of Trust		
Attribute Mapping Mapping ditributes helps to ensure that both the Service Provider (SP) and the identity Provider (DP) can recognize the same attributes that may have unique names. For example, the SP may have an attribute called UserName but the UP may call 4UserN Eliminating these inconsistencies by mapping the attributes will guarantee that the data will be passed corredy.  Attributes Mapping  Local Attributes Name  Served an attribute or Served an attribute or Served and the served attribute Name  Served an attribute or Served an attribute or Served and the served attribute or Served and the served attribute or Served and the served attribute or Served attribute or Served and the served attribute or Served attribute or Served attribute or Served and the served attribute or Served and the served or Served attribute or Served att	Choose from existing circles of trust listed or provide one to be created in which to include this IDP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 comperformed. * New Circle of Trust:	munications an	e
Mapping attributes helps to ensure that both the Service Provider (SP) and the identity Provider (IDP) can recognize the same attributes that may have unique names. For example, the SP may have an attribute called UserName but the UP may call (UserIC) Eliminating these inconsistencies by mapping the attributes will guarantee that the data will be passed correctly.  Attributes Mapping  Detecte Name in Assertion Local Attribute Name  Service an attribute.	Attribute Mapping		
Attributes Mapping  Detete Name in Assertion Local Attribute Name  Select an attribute.   S	Mapping attributes helps to ensure that both the Service Provider (SP) and the identity Provider (IDP) can recognize the same attributes that may have unique names. For example, the SP may have an attribute council of the may call it User(D. Eliminating these inconsistencies by mapping the attributes will guarantee that the data will be passed correctly.	illed UserName	e but the
Delete     Kacal Attribute Name       Name in Assertion     Local Attribute Name       Select an attribute.     Add	Attributes Mapping		
Name in Assertion Local Attribute Name	Delete		
Select an attribute 💟 🔍	Name in Assertion Local Attribute Name		
	Add		

- 8. Click Configure to save the Identity Provider.
- 9. Return to the main page.
- 10. Select FEDERATION menu item and select to modify the newly created Identity Provider in the Entity Providers table in the Circle of Trust Configuration section.
- 11. Remove the value "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName=" in NameID Value Map in the Assertion Content tab, if any.
- 12. Add the value "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName=uid" to the map. By default, this nameID is used in the Authentication Server for user identification (authserver.properties parameter authentication.saml.name.id.format).

Current Values	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress=mail urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName= urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName= urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos= urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified= <u>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName=uid</u>	< · · ·	Remove
New Value	Add		

13. Save the configuration changes.

## Deploying the authentication server

To deploy the authentication server

- 1. During the deployment process add the SAML integration configuration parameters to the file authserver.properties.
  - Set authentication.saml.enabled to true.
  - If the authentication server is deployed on a cluster, set value for the parameter **authentication.saml.entity.id** (default is **com.nomagic. authentication.server**). This value should be unique for each authentication server instance.

- Set authentication.saml.idp.metadata.url to the appropriate ForgeRock server address (should be http://<server>:<port>/openam /saml2/jsp/exportmetadata.jsp?entityid=http://<server>:<port>/openam&realm=/<realm name>).
- Set the name of the button to the parameter authentication.saml.link. Users will click this button to log in using ForgeRock as the Identity Provider.
- 2. Save the authserver.properties file and (re)start the WebAppPlatform service.

## Configuring SAMLv2 Remote Service Provider

To configure SAMLv2 Remote Service Provider

- 1. Go back to ForgeRock and, in the realm overview, select Create SAMLv2 Providers and then Register Remote Service Provider.
- 2. Select the realm.
- 3. Specify the URL of Authentication Server metadata: http[s]://<auth-server-host>:<auth-server-port>/authentication/saml/metadata (if such URL is accessible from ForgeRock) or select a file of stored Authentication Server metadata (usually used in https case).
- 4. Enter or select the same circle of trust as that of the Identity Provider and click Configure.

Create a SAMLv2 Remote Servi	ce Provider	Configure	Cancel			
This page allows you to register a remote the confines within which all federation co- other entities (eg IDPs) in a COT.	Service Provider (SP). You need two things: Circle of Trust (COT) and metadata of the mmunications are performed. Metadata represents the configuration necessary to a	e provider. A COT is a group of identity Providers (IDPs) and SPs that trust each other and in effect repr xecute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration	esents i to			
		* Indicates req	uired field			
* Realm:	/twc 🗸 🐠					
Where does the metadata file reside?:	● URL _ File <sup>(1)</sup>					
* URL where metadata is located:	0					
Circle of Trust						
Choose from existing circles of trust liste performed.	Choose from existing circles of trust listed or provide one to be created in which to include this SP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAML/2 communications are performed.					
* New Circle of Trust:						
Attribute Mapping						
Attributes Mapping						
Delete						
Name in Assertion	Local	Attribute Name				
	Add					
	Select an attribute. 🔽 💷					

5. A Service Provider with the default name **com.nomagic.authentication.server** will be created. The name of the service provider is configured in the Authentication Server's **authserver.properties** file (parameter **authentication.saml.entity.id**).

Once you have completed the steps on this page, you should be able to log in through ForgeRock by clicking the SAML integration button on the **Authentication Server** login page. If later the Authentication Server configuration, related to SAML or server keystore file is changed, delete the remote service provider and add a new one (see Create SAMLv2 Providers > Register Remote Service Provider).