Integrating authentication server with ForgeRock

On this page:

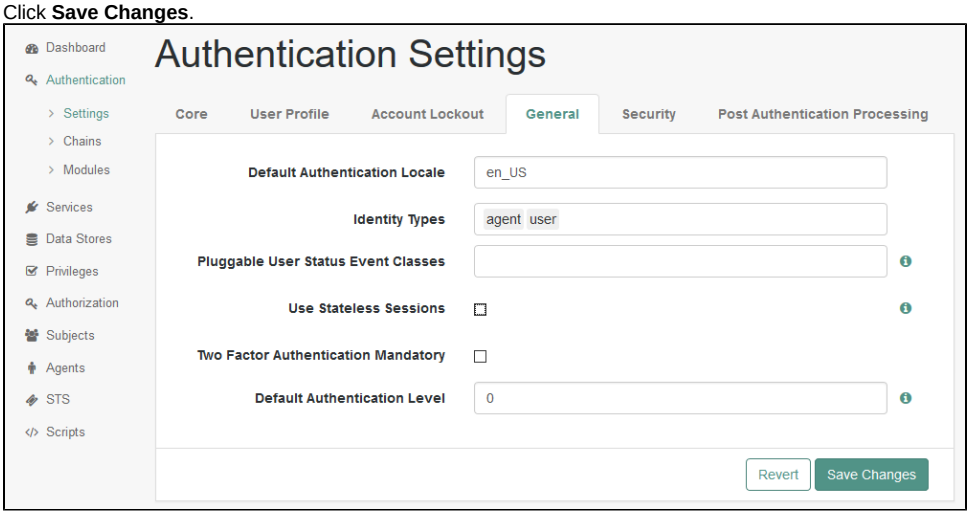
This page contains the instructions to integrate the authentication server with the ForgeRock application (ForgeRock is the company that develops open-source identity and access management products for cloud, social, mobile, and enterprise environments). This documentation is based on ForgeRock version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

Integrating the authentication server with ForgeRock

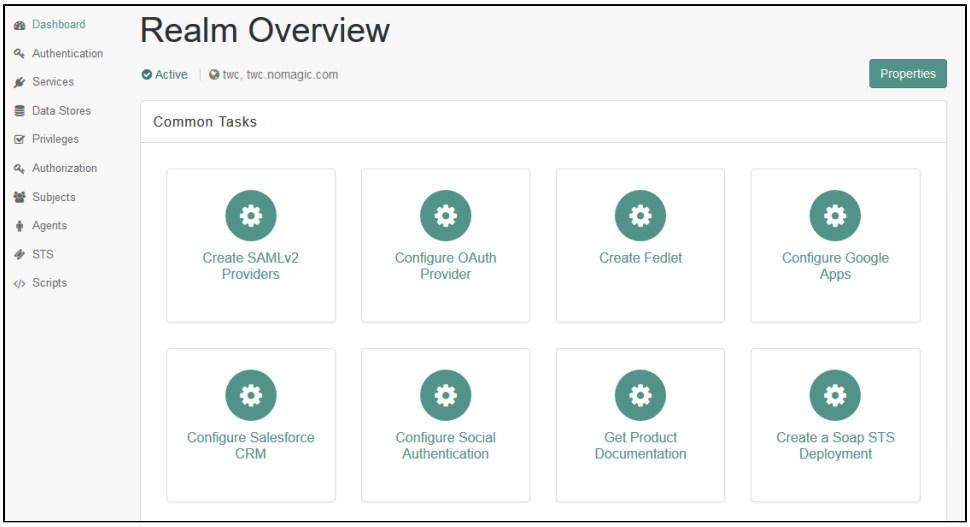
To integrate the authentication server with ForgeRock

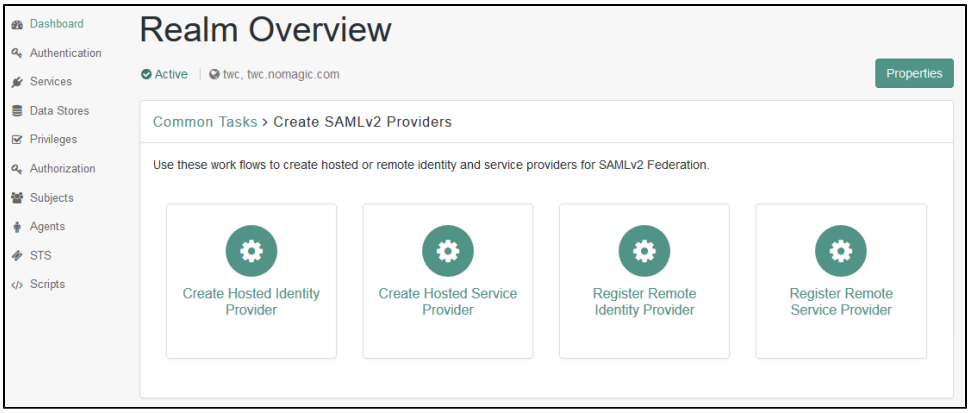
---

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. Click **Save Changes**.

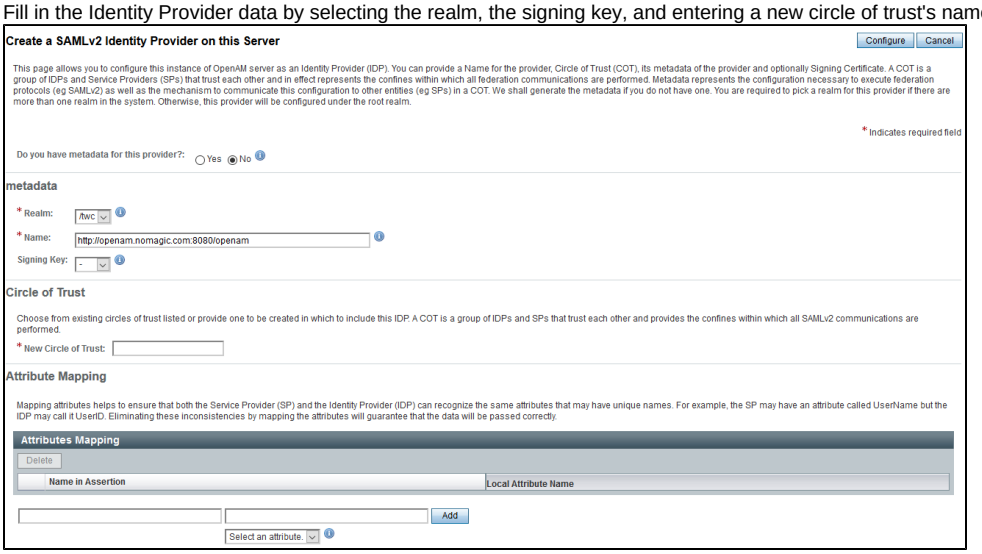


6. Go back to **Dashboard** and in the realm overview, select **Create SAMLv2 Providers** and then **Create Hosted Identity Provider**.

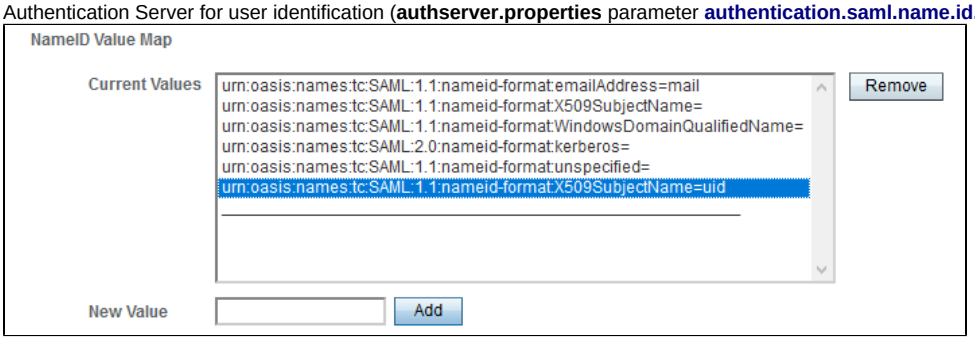




7. Fill in the Identity Provider data by selecting the realm, the signing key, and entering a new circle of trust's name.



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**).



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.

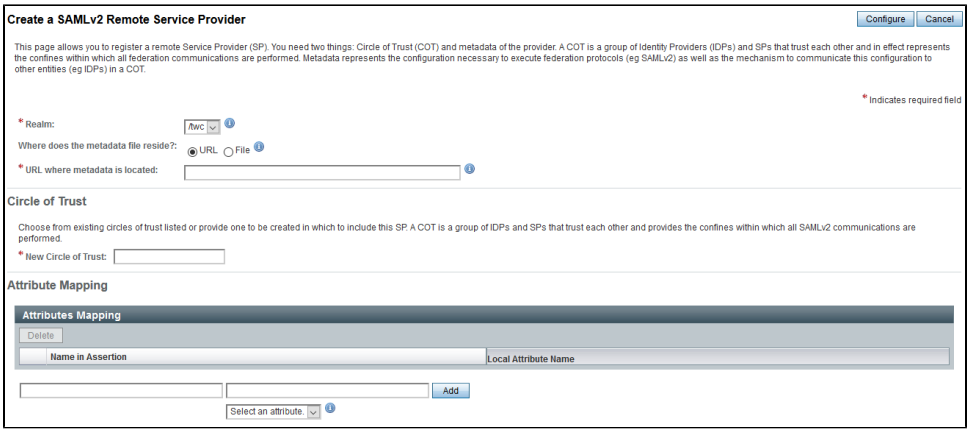
2. Save the **authserver.properties** file and (re)start the WebAppPlatform service.

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**.



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).