Requirements for ADFS with Hoonuit

- Microsoft Active Directory Federated Services 2.0 or newer
- Microsoft Windows Server 2008 R2 or newer
- Publicly accessible AD FS metadata via http

Setup for Microsoft Windows Server newer than 2008 (2008 see below)

Add Hoonuit’s Relying Party Using Metadata

1) In the AD FS Console:
   a. Expand the Trust Relationships -> Select then right-click the Relying Party Trusts -> Select Add Relying Party Trust...

2) In the wizard
   a. Select Start.
   b. On the Select Data Source screen, leave selected Import data about the relying party published online or on a local network. In the Federation metadata address field, type https://static.atomiclearning.com/sp-metadata.xml, and then select Next.
   c. Click OK to acknowledge the message “Some of the content in the federation metadata was skipped because it is not supported by AD FS…”
   d. In the Specify Display Name page, type Hoonuit, and then select Next.
   e. On the Configure Multi-factor Authenticate Now screen, leave “I do not want to configure multi-factor…” selected and then select Next.
   f. On the Choose Issuance Authorization Rules screen, leave the default Permit all users to access the relying party selected, and then select Next.
   g. Select Next
   h. Leave the “Open the Edit Claim Rules dialog……” option checked, then select Close

Edit Claim Rules for Relying Party Trust

Claim rules describe how AD FS determines what data should reside inside the federation security tokens that it generates. The claim rule in this section describes how data from Active Directory is inserted in the security token that is created for Shibboleth.

Shibboleth is preconfigured to assert multiple attributes of the eduPerson object class, which is specifically designed for higher education institutions. These are not configured by default in AD FS.

We will generate multiple claims to retrieve attributes from your Active Directory and issue attributes in to Atomic Learning. In order to have a complete user record, Hoonuit suggests the user attributes provided below be configured in your claim rules.

Configure user claims for sending attributes to Hoonuit

1) The Edit Claim Rules dialog box should already be open. If not, in the AD FS center pane, under Relying Party Trusts, right-click Hoonuit, and then click Edit Claim Rules.
2) Under the Issuance Transform Rules tab, click Add Rule.
3) On the Choose Rule Type screen, select the template Send LDAP Attributes as Claims
4) Click Next
5) On the Configure Claim Rule screen, Enter Hoonuit into the Claim rule name field
6) Select Active Directory from the dropdown on Attribute Store
7) We have setup mappings to make it easier to pass attributes to us. The following are our pre-mapped attributes:
8) Once you have entered all mappings, select OK

This completes this piece of the setup for Hoonuit. You may now complete the Hoonuit ADFS Customer Requirements document to provide the necessary information to Hoonuit for configuration of the ADFS connection on their side. The document can be found [here](#).

---

### Setup for Microsoft Windows Servers after 2008

**Add Hoonuit Relying Party Using Metadata**

1) In ADFS2.0, in the console tree, right-click the Relying Party Trusts folder, and then click Add Relying Party Trust to start the Add Relying Party Trust Wizard.

2) On the Select Data Source page, leave selected Import data about the relying party published online or on a local network.

3) In the Federation metadata address field, type `http://static.atomiclearning.com/sp-metadata.xml`, and then click Next.

4) Click OK to acknowledge the message “Some of the content in the federation metadata was skipped because it is not supported by ADFS2.0.”

5) In the Specify Display Name page, type Hoonuit, and then click Next.

6) On the Choose Issuance Authorization Rules page, leave the default Permit all users to access the relying party selected, and then click Next.

7) Click Next, and then click Close.

**Edit Claim Rules for Relying Party Trust**

Claim rules describe how ADFS2.0 determines what data should reside inside the federation security tokens that it generates. The claim rule in this section describes how data from Active Directory is inserted in the security token that is created for Shibboleth.

Shibboleth is preconfigured to assert multiple attributes of the eduPerson object class, which is specifically designed for higher education institutions. These are not configured by default in ADFS2.0. Also, Shibboleth expects inbound SAML attributes names to use a different name format (urn:oasis:names:tc:SAML:2.0:attrname-format:uri) than ADFS2.0 publishes by default (urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified). For these reasons, we will use the ADFS2.0 custom rule language to generate Shibboleth-compliant claims.

### LDAP Attribute | Outgoing Claim Type
---|---
SAM-Account-Name | sAMAccountName
Given-Name | giveName
Surname | sn
E-Mail-Addresses | mail
Title | title
Department | department
Description | description
Employee-Number | employeeNumber
We will generate multiple claims to retrieve attributes from your active directory and issue attributes into Atomic Learning. In order to have a complete user record, Hoonuit suggests the user attributes shown in the claim rule grid below be configured in your claim rules.

**Configure user claims for sending attributes to Hoonuit**

1) The **Edit Claim Rules** dialog box should already be open. If not, in the ADFS2.0 center pane, under **Relying Party Trusts**, right-click **Hoonuit**, and then click **Edit Claim Rules**.

2) On the **Issuance Transform Rules** tab, click **Add Rule**.

3) On the **Select Rule Template** page, select **Send Claims Using a Custom Rule** and click **Next**.

4) In the **Configure Rule** page, in the **Claim Rule Name** box, type **Get Username**

5) In the **Custom Rule** window, type or copy and paste the following:

   ```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("urn:oid:2.5.4.3"), query = ";sAMAccountName;{0}", param = c.Value);
```

6) Click **Finish**.

7) On the **Issuance Transform Rules** tab, click **Add Rule**.

8) On the **Select Rule Template** page, select **Send Claims Using a Custom Rule**, and then click **Next**.

9) On the **Configure Rule** page, in the **Claim Rule Name** box, type **Transform Username**

10) In the **Custom Rule** window, type or copy and paste the following:

   ```
c:[Type == "urn:oid:2.5.4.3"]
```

11) Click **Finish**, and then click **OK**.

Custom “Get” and “Transform rule” need to be created for each attribute. A table is provided below for all of the suggested attributes and rules.
<table>
<thead>
<tr>
<th>Attribute Referenced</th>
<th>Get Rule Name</th>
<th>Get Claim Custom Rule Syntax</th>
<th>Transform Rule Name</th>
<th>Transform Claim Custom Rule Syntax</th>
</tr>
</thead>
</table>
| sAMAccountName (Username)            | Get Username                  | c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
| * (Already completed in steps 11 – 17) | => add(store = "Active Directory", types = {"urn:oid:2.5.4.3"}, query = ";sAMAccountName;{0}", param = c.Value); | Transform Username           | c:[Type == "urn:oid:2.5.4.3"]
| givenName (First Name)               | Get First Name                | c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
|                                      | => add(store = "Active Directory", types = {"urn:oid:2.5.4.42"}, query = ";givenName;{0}", param = c.Value); | Transform First Name         | c:[Type == "urn:oid:2.5.4.42"]
| sn (Last Name)                       | Get Last Name                 | c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
|                                      | => add(store = "Active Directory", types = {"urn:oid:2.5.4.4"}, query = ";sn;{0}", param = c.Value); | Transform Last Name          | c:[Type == "urn:oid:2.5.4.4"]
| mail (eMail Address)                 | Get Email Address             | c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
|                                      | => add(store = "Active Directory", types = {"urn:oid:0.9.2342.19200300.100.1.3"}, query = ";mail;{0}", param = c.Value); | Transform Email Address      | c:[Type == "urn:oid:0.9.2342.19200300.100.1.3"]
| title (Title)                        | Get Title                     | c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
| **(Can be used for Staff or Student identifier in Atomic Learning) | => add(store = "Active Directory", types = {"urn:oid:2.5.4.12"}, query = ";title;{0}", param = c.Value); | Transform Title             | c:[Type == "urn:oid:2.5.4.12"]
| department (Department)              | Get Department                | c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
| ***(Can be used for Location identifier in Atomic Learning) | => add(store = "Active Directory", types = {"urn:oid:2.16.840.1.113730.3.1.211"}, query = ";department;{0}", param = c.Value); | Transform Department      | c:[Type == "urn:oid:2.16.840.1.113730.3.1.211"]
| description (Department)             | Get Description               | c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
| ***(Can also be used for Staff or Student identifier in Atomic Learning) | => add(store = "Active Directory", types = {"urn:oid:2.5.4.13"}, query = ";description;{0}", param = c.Value); | Transform Description | c:[Type == "urn:oid:2.5.4.13"]
Configure user claim for sending email address as shibboleth Name Identifier to Atomic Learning

12) The **Edit Claim Rules** dialog box should already be open. If not, in the AD FS 2.0 center pane, under **Relying Party Trusts**, right-click **Atomic Learning**, and then click **Edit Claim Rules**.

13) On the **Issuance Transform Rules** tab, click **Add Rule**.

14) On the **Select Rule Template** page, select **Send LDAP Attributes as Claims**, and then click **Next**.

15) On the **Configure Rule** page, in the **Claim rule name** box, type **Send Email as Name ID**.

16) In the **Attribute Store** list, select **Active Directory**.

17) In the **Mapping of LDAP attributes** section, create the following mappings.

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM-Account-Name</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Given-Name</td>
<td>giveName</td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
</tr>
<tr>
<td>E-Mail-Addresses</td>
<td>mail</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td>Employee-Number</td>
<td>employeeNumber</td>
</tr>
</tbody>
</table>

This completes this piece of the setup for Hoonuit. You may now complete the Hoonuit ADFS Customer Requirements document to provide the necessary information to Hoonuit for configuration of the ADFS connection on their side. The document can be found [here](#).