



### Requirements for ADFS with Infobase Learning Cloud

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

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

#### Add Infobase Learning Cloud Relying Party Using Metadata

- 1) In the ADFS 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.learningcloud.infobase.com/metadata/learningcloud.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 ADFS...."
  - d. In the **Specify Display Name page**, type **Infobase**, 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 ADFS 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 ADFS.

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

### Configure user claims for sending attributes to Infobase

- 1) The **Edit Claim Rules** dialog box should already be open. If not, in the ADFS center pane, under Relying Party Trusts, right-click Infobase, 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 **Infobase 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:

LDAP Attribute	Outgoing Claim Type
SAM-Account-Name	sAMAccountName
Given-Name	givenName
Surname	sn
E-Mail-Addresses	mail
Title	title
Department	department
Description	description
Employee-Number	employeeNumber

- 8) Once you have entered all mappings, select **OK**

*This completes this piece of the setup for Infobase Learning Cloud. You may now complete the ADFS Customer Requirements document to provide the necessary information to Infobase for configuration of the ADFS connection on their side.*

---

## Setup for Microsoft Windows Servers 2008 or earlier

### Add Infobase Learning Cloud Relying Party Using Metadata

- 1) In ADFS 2.0, 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 <https://static.learningcloud.infobase.com/metadata/learningcloud.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 ADFS 2.0."
- 5) In the **Specify Display Name** page, type **Infobase**, 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 ADFS 2.0 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 ADFS 2.0. Also, Shibboleth expects inbound SAML attributes names to use a different name format (urn:oasis:names:tc:SAML:2.0:attrname-format:uri) than ADFS 2.0 publishes by default (urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified). For these reasons, we will use the ADFS 2.0 custom rule language to generate Shibboleth-compliant claims.

We will generate multiple claims to retrieve attributes from your active directory and issue attributes in to Learning Cloud. In order to have a complete user record, Infobase suggests the user attributes shown in the claim rule grid below be configured in your claim rules.

### Configure user claims for sending attributes to Infobase

- 1) The **Edit Claim Rules** dialog box should already be open. If not, in the ADFS 2.0 center pane, under **Relying Party Trusts**, right-click **Infobase**, 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"]
```

```
⇒ issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer,  
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attribut  
ename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

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.**

Attribute Referenced	Get Rule Name	Get Claim Custom Rule Syntax	Transform Rule Name	Transform Claim Custom Rule Syntax
sAMAccountName (Username) <i>* (Already completed in steps 11 – 17)</i>	Get Username	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);	Transform Username	c:[Type == "urn:oid:2.5.4.3"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
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"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
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"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
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"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
title (Title) <i>** (Can be used for Staff or Student identifier in Learning Cloud)</i>	Get Title	c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("urn:oid:2.5.4.12"), query = ";title;{0}", param = c.Value);	Transform Title	c:[Type == "urn:oid:2.5.4.12"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
department (Department) <i>*** (Can be used for Location identifier in Learning Cloud)</i>	Get Department	c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => 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"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
description (Department) <i>**** (Can also be used for Staff or Student identifier in Learning Cloud)</i>	Get Description	c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("urn:oid:2.5.4.13"), query = ";description;{0}", param = c.Value);	Transform Description	c:[Type == "urn:oid:2.5.4.13"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
employeeNumber (Employee Number) <i>***** (Can be used for Unique Identifier in Learning Cloud)</i>	Get Employee Number	c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("urn:oid:2.16.840.1.113730.3.1.3"), query = ";employeeNumber;{0}", param = c.Value);	Transform Employee Number	c:[Type == "urn:oid:2.16.840.1.113730.3.1.3"] => issue(Type = c.Type, Value = c.Value, Issuer = c.Issuer, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

## Configure user claim for sending email address as Shibboleth Name Identifier to Infobase Learning Cloud

- 1) The **Edit Claim Rules** dialog box should already be open. If not, In the ADFS 2.0 center pane, under **Relying Party Trusts**, right-click **Infobase**, 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 LDAP Attributes as Claims**, and then click **Next**.
- 4) On the **Configure Rule** page, in the **Claim rule name** box, type **Send Email as Name ID**.
- 5) In the **Attribute Store** list, select **Active Directory**.
- 6) In the **Mapping of LDAP attributes** section, create the following mappings.

LDAP Attribute	Outgoing Claim Type
SAM-Account-Name	sAMAccountName
Given-Name	givenName
Surname	sn
E-Mail-Addresses	mail
Title	title
Department	department
Description	description
Employee-Number	employeeNumber

*This completes this piece of the setup for Infobase Learning Cloud. You may now complete the Infobase Learning Cloud ADFS Customer Requirements document to provide the necessary information to Infobase for configuration of the ADFS connection on their side.*