Kivuto™

*Digital Distribution. **Simplified.***

Active Directory Federation Services (ADFS)

Customer Implementation Guide

2018-11-01
Version 2.3

TABLE OF CONTENTS

INTRODUCTION

This document describes how to implement the Active Directory Federation Service (ADFS) Single Sign-On (SSO) verification method on your WebStore. It is intended for school IT administrators who will perform the implementation of this verification system.

EXCHANGING METADATA

Before you can implement ADFS SSO on your WebStore, you must send a copy of your ADFS metadata (FederationMetadata.xml) to Kivuto, at tac@kivuto.com.

Kivuto will respond by sending you a copy of their ADFS metadata file, which you will need to perform the implementation.

CREATING A RELYING PARTY TRUST IN ADFS

After receiving the necessary metadata from Kivuto (OnTheHub_Shibboleth_MetaData.xml), the next step is for you to set up a relying party trust in ADFS.

To create a relying party trust in ADFS:

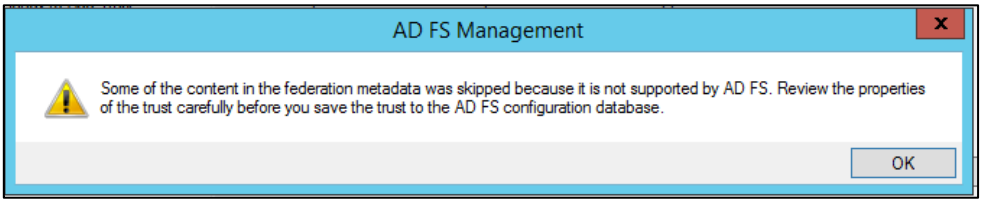
1. Select the “Relying Party Trusts” folder in ADFS, and then click **Add Relying Party Trust**. The Relying Party Trust Wizard will open.

2. Click **Start** to proceed.

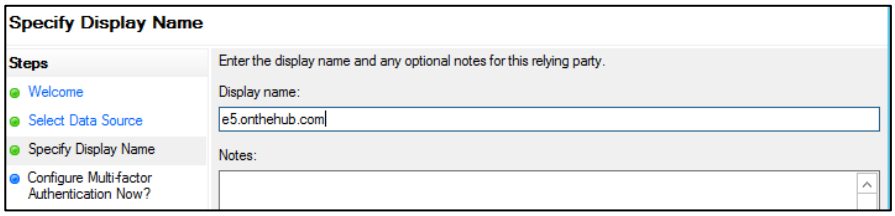
3. Select the option: **Import data about the relying party from a file**. Browse for the metadata file provided by Kivuto, and then click **Next** to continue.

Note: If Kivuto has not provided you with the metadata file you need, contact them to request it.

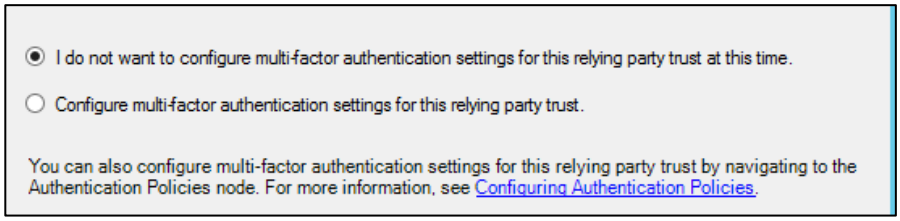
You may be shown a message indicating that some content was skipped. This is normal. Click **OK** to close the window and proceed.



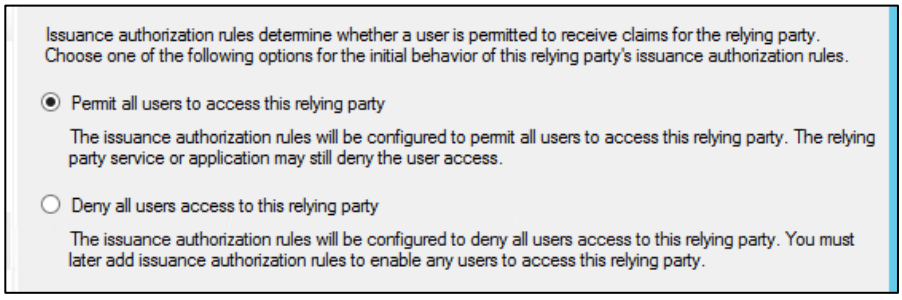
4. In the **Display name** field, type: “e5.onthehub.com,” and then click **Next**.



5. When prompted to choose whether you wish to configure multi-factor authentication (which is optional), choose the option that will work best for your organization, and then click **Next**.

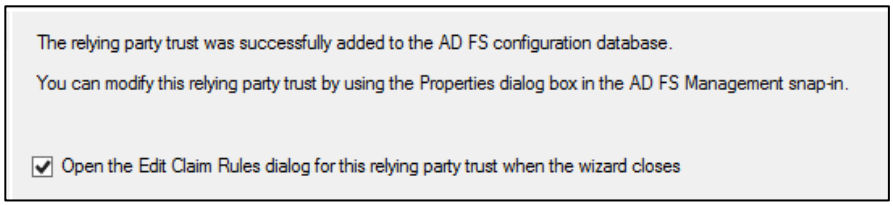


6. Select the option: **Permit all users to access this relying party**, and then click **Next**.



7. Review the summary screen and all tabs for options you configured. If all of the information looks ok, click **Next**.

8. Ensure that the option: **Open the Edit Claim Rules dialog** is selected, and then click **Close**.

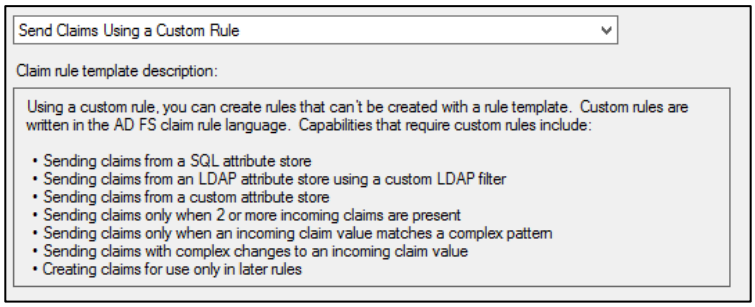


ADDING CLAIM RULES FOR E5.ONTHEHUB.COM

Custom rules need to be added to the e5.ontheub.com relying party trust in order for ADFS to be able to communicate properly.

To add custom claim rules for e5.onthehub.com:

1. Right click on the **e5.onthehub.com** entry created earlier, and select **Edit Claim Rules**.
2. Under the **Issuance Transform Rules** Tab, click **Add rule**.
3. Choose the template **Send Claims Using a Custom Rule**.



4. Enter a **Claim rule name** and the appropriate **Custom rule** text. See Table 1 for a list of rules you need to add and the appropriate rule text to enter for each.
5. Repeat steps 2-4 for each rule listed in Table 1 and described in the Mapping User Groups section below.

Table 1: Custom Rules

Rule Name	Rule Text
OntheHubData	c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", "http://schemas.xmlsoap.org/claims/Group"), query = ";userPrincipalName,tokenGroups;{0}", param = c.Value);
OTH Transform UPN to epPN	c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"] => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.6", Value = c.Value, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
OTH Transform Group to epSA	c:[Type == "http://schemas.xmlsoap.org/claims/Group", Value == "Domain Users"] => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.9", Value = "member@contoso.com", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

Note: After passing the rules listed above, you will need to pass additional claim rules to map users to groups. See Mapping User Groups for details.

Mapping User Groups

Additional claim rules must be passed to map specific groups in your active directory to the equivalent user groups on your WebStore (Students, Faculty, Staff). This is necessary to establish your users' eligibility to order products.

> **Note:** If you do not have specific user groups set up in your active directory, you will need to create some and then map them to their equivalent WebStore user groups.

A separate rule must be passed for each user group in each department supported by your WebStore. Choose a suitable name for each rule. Base the rule text on the User Group Rule Template below, but make the following changes.

- Replace [AD group name] with the term used to identify the group in your active directory.
- Replace [user group] with the name of the corresponding WebStore user group (i.e. Students, Faculty, or Staff).

> **Note:** If one of your AD groups corresponds to more than one WebStore user group (e.g. Faculty/Staff), separate the user groups with a comma in your rule text (e.g. "faculty,staff").

- Replace [department] with the name of the department users in the group belong to, as identified in your active directory.

  Exception: If your WebStore supports only a campus-wide subscription, omit ",[department]" from each rule and create only one Students user group, one Faculty user group, and one Staff user group for your whole campus. A department only needs to be identified if your WebStore supports department-specific programs.

User Group Rule Template

```
c:[Type == "http://schemas.xmlsoap.org/claims/Group", Value == "[AD group name]"]
 => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.7", Value = "[user group],[department]",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

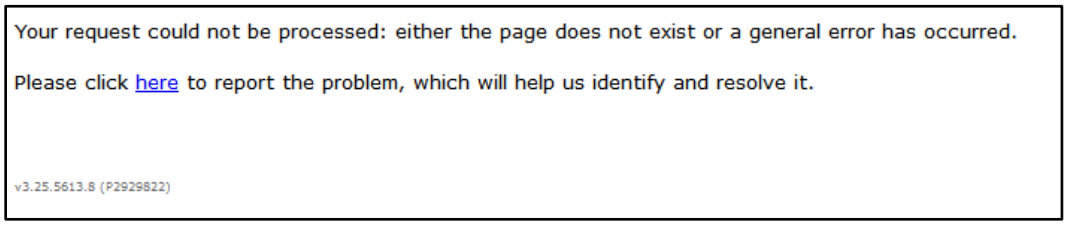
Example: A rule to map students from the Department of Mathematics to the correct user group might look like this.

```
c:[Type == "http://schemas.xmlsoap.org/claims/Group", Value == "mathstudents"]
 => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.7", Value = "students,departmentofmathematics",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

TROUBLESHOOTING

Known issues you may encounter and their solutions are identified below.

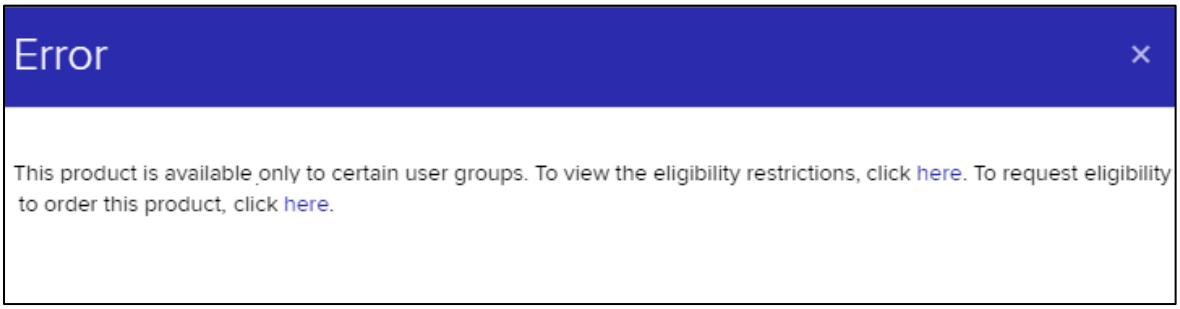
Error message:



Cause: The "OTH Transform UPN to epPN" rule is missing.

Resolution: Add the "OTH Transform UPN to epPN rule" (see Adding Claim Rules for e5.OnTheHub.com and Table 1).

Error message:



Cause: If users can access the WebStore but encounter the above message when they try to order software, it means that user groups are not being correctly passed.

Resolution: Ensure that user groups are being correctly mapped and passed (see Mapping User Groups).