SAML based SSO Implementation Guide

Addendum for ADFS

Identity Provider *using ADFS*

Document Details

Document #: 160_SG550_200423

Release Version: 05.50.00.00

Version Release Date: July 2017

Overview

Audience: The IT staff of CrunchTime's on-premise client managing IdP that uses ADFS.

This document explains how to implement SAML based SSO for an ADFS IdP.

System Requirements

- CES Release Version 05.50.00 or higher
- Be sure to grab the latest version of this document here: https://links.crunchtime.com/SG-SSOImplementationGuide-IdP-ADFS

Other Related Documentation

- SAML based SSO Implementation Guide-IdP: https://links.crunchtime.com/SG-SSOImplementationGuide-IdP
- SAML based SSO Implementation Guide-SP: https://links.crunchtime.com/SG-SSOImplementationGuide-SP

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Configure SAML SSO in ADFS to work with CrunchTime

Create ADFS relying party entries

1. On the ADFS Server, access the *ADFS Management Console*.
2. Navigate to *Trust Relationships > Relying Party Trusts > Add Relying Party Trust*.
3. Select *Start* on the Add Relying Party Trust Wizard page.
4. Select *Import Data about the relying party from a file*.
5. Select *Browse* and upload the Net-Chef metadata file received from CrunchTime!. Select *Next*. (You will repeat the same steps for EM Web metadata file from CrunchTime! later)
6. Enter a *Display* name such as "yousitename.net-chef.com" and select *Next*.
7. Select *I do not want to configure multi-factor authentication settings...*and select *Next*.
8. Select *Permit All Users to Access this Relying Party* and select *Next*.
9. Select *Next on the Ready to Add Trust* step and then select *Close* on the Finish step.
10. After the Relying Party Trust has been created, it should open the Edit Claims Rules if the last checkbox was left checked. Otherwise right-click the *Relying Party Trust* and select *Edit Claims*.

Configuration Note: It may be necessary to merge the Net-Chef and EM Web (two AcsURLs represented in two metadata files) into one relying party trust with two endpoint URLs.

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Configure SAML SSO in ADFS (Continued)

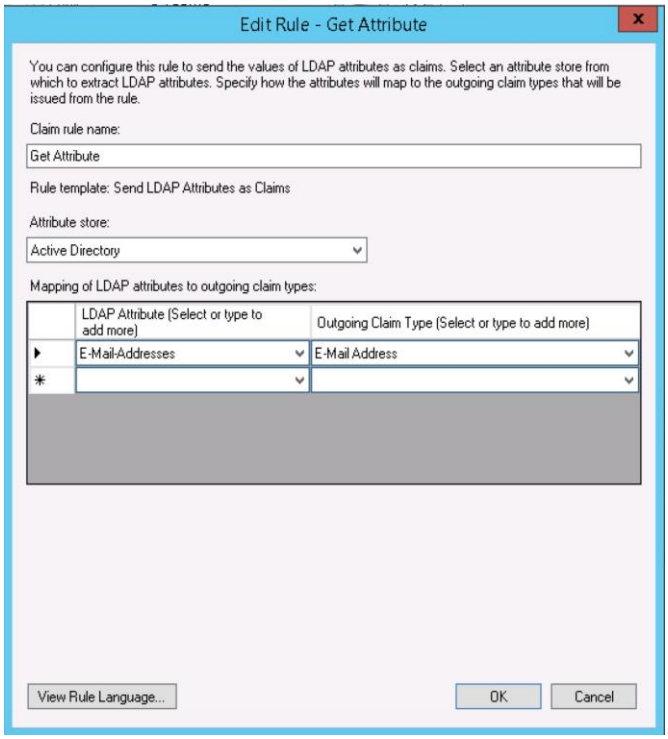
Configure ADFS relying party claim rules

Edit the Claim rules to enable proper communication with the instance.

Role required: admin

Procedure A: Create NameID for subject

1. Log into the ADFS server and open the management console.
2. Right-click the relying party trust and select *Edit Claim Rules*.
3. Click the *Issuance Transform Rules* tab.
4. Select *Add Rules*.
5. Select *Send LDAP Attribute as Claims as the claim rule template to use*.
6. Enter a Claim Rule Name such as **Get LDAP Attributes**.
7. Set the Attribute store to **Active Directory**, the LDAP Attribute to **E-Mail-Addresses**, and the Outgoing Claim Type to **E-mail Address**.




```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"]

=> issue(store = "Active Directory",

types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),

query = ";mail;{0}", param = c.Value);
```

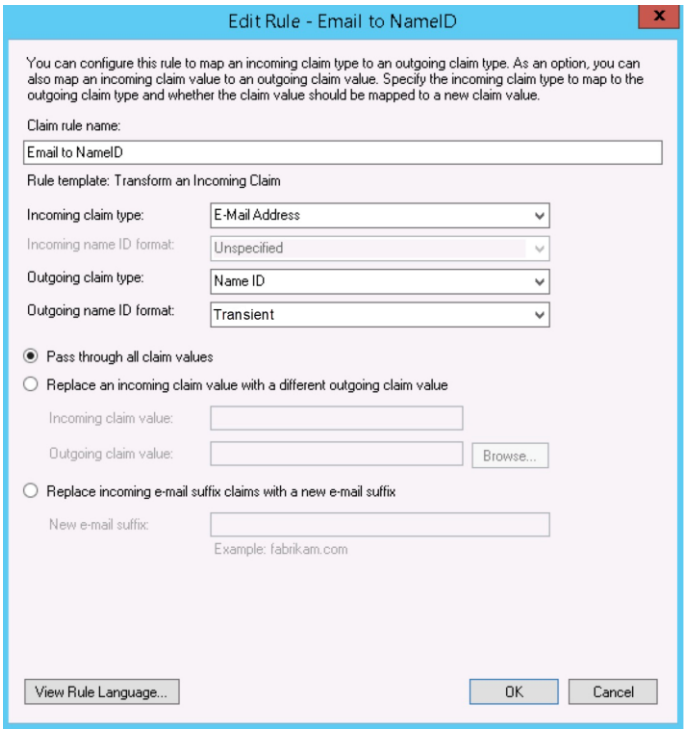
(Continued)

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Configure SAML SSO in ADFS (Continued)

8. Select *Finish*.
9. Select *Add Rules*.
10. Select *Transform an Incoming Claim as the claim rule template to use*.
11. Enter a Claim Rule Name such as **Email to Name ID**.
12. Set the Incoming Claim Type to the Outgoing Claim Type in the previous rule. For example, **E-Mail Address**.
13. Set the Outgoing Claim Type to **Name ID** and the Outgoing name ID format to **Transient**.

    Note: These values must match the Name ID policy you define during SAML 2.0 configuration.
14. Select *Pass through all claim values*.



This claim rule should look similar to the following rule language.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. Click *Finish*.

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com

Configure SAML SSO in ADFS (Continued)

Procedure B: Send username

1. On the Issuance Transform Rules tab, select *Add Rule*.
2. On the Select Rule Template page, select *Send LDAP Attributes as Claims as the Claim rule template* and select *Next*.
3. On the Configure Rule page, in the Claim Rule Name box, type **Create *username* Claim**.
4. In the Attribute Store drop-down, select *Active Directory*.
5. In the Mapping box on the left side select **SAM-Account-Name**.
6. In the Mapping box on the right side type **SamAccountName** and select *Finish*.
7. Select *Add Rule*.
8. On the Select Rule Template page, select *Transform an Incoming Claim for the Claim rule template* and select *Next*.
9. On the Configure Rule page, in the Claim Rule Name box, type **Send *username* Claim**.
10. Incoming Claim Type should be **SamAccountName**. It must match the Outgoing Claim Type created in the earlier rule.
11. Set the Outgoing Claim Type to ***username.***
12. Confirm *Pass through all claim values* is selected and select *Finish*.
13. Select *OK* to save the rule and *OK* again to complete the attribute mappings.

© 2021 CrunchTime! Information Systems, Inc. All Rights Reserved. | www.crunchtime.com