Steps to configure SAML 2.0 SSO with Microsoft Active Directory Federation Services

PRODUCTS: Learn

Note: ADFS 2.0 on Windows Server 2008 r2 or ADFS 3.0 on Windows Server 2012 / 2012 r2)

SAML 2.0 single sign-on (SSO) supports integration with Microsoft Active Directory Federation Services (ADFS) 3.0.

Requirements

- A fully installed and configured ADFS service.
- A server running Microsoft Server 2008r2 or 2012/2012r2
- An SSL certificate to sign your ADFS login page and the thumbprint of that certificate

In this example we are using ADFS 2.0 on Windows Server 2008 R2. On Windows Server 2012 the steps will be the same except for the installation, because you install AD FS role via the server manager, not via the installation package as on Windows 2008 server r2.

Step 1. AD FS Management

Login in to your AD FS server and launch the ADFS Management Console via the shortcut in Control Panel\Administrative Tools.

txyVmpwGv__tSTGJwXYyz0yC82ytijIjSb4t7TwX5aj2V7PBfMQHxioflnVrcd2zqsxe_DCaLQ3rsJMBsv1erQR9aFIR

Step 2. Check AD FS settings

Right-click on Service and sel ect Edit Federation Service Properties...

vpNhOmi5zA7XXr4zymN9Z2U4N5FQ5qsIaRdfJlknxBk8uXBO9wYo_mC3WsG9XQTJb6O4Z7eMNRwPlr_51L8tJ

Confirm that the General settings match your DNS entries and certificate names. Make a note with the Federation Service Identifier, since that is used in the iSpring Learn SAML 2.0 configuration settings.

1sY5XuJ0_hrWRWv07Qgv4f6mznJNfcQAYm-QLkN49QtLoExMMAmvhoD3SdVgo9KN9DjG92zjt3vjiWaKVjZxH3p

Step 3. Token-Signing certificate

1. Browse to the certificates.
2. Right-click on the certificate and sel ect View Certificate.
3. Go to the Details tab.
4. Find the Thumbprint field and copy the contents of this field to the Windows clipboard.

RWYwuaq5guXjKsQRWl50CwbHAbzlSJh2QVh-T9xA5xKBVihAiVxMs3YCTJ_xcGv7XzqWnqLGXOkponiAJjjcXb_

Step 4. Learn Settings

1. Log in into your iSpring Learn account and go to the SSO settings via this link: https://YourAcc?untURL.ispringlearn.com/settings/sso
2. Ins ert your Thumbprint into the Certificate Fingerprint field and remove all spaces between characters.
3. Enter your data to the Metadata URL, Sign ON URL and Logout URL fields.

SAML01.png

Step 5. ADFS Relying Party Configuration

Go to the ADFS Management console and select Relying Party Trusts, right-click on it and select Add Relying Party Trust…

DWe2TCjpUD-9mwb9YE-Yi_3VQvvLo6w5S4K9Tqo5iu3ytTrfMkakrv2THOkYo9HFrYZJMUyGxQCOOha-7EbJ_m

Select Next On the Welcome Screen of the wizard, and on the Select Data Source step, select the last option: Enter data about the relying party manually.

FedR8yJMFy79Wm7ZOapfx8-RgWO8Syz-VFPk5VezbDvw_urdX2UCWCFEakA7sMeQsRcVARsoJKANp8gKd0V

On the next screen, enter a Display name that you will recognize in the future.

gHTy1NaSaFcC9tAVCwq4nrI2YFD9YJQ8j_BVccexWw2E6wWMG9kkBI4su3Mf_kGmhhPf5lkCm-8p5W6i-L6119h

Next, select AD FS profile:

phGZye3RG4RuFv7kujBnkKtD75sg-YOU4hPlQHv--3weu7qnzB2QgwYSJ5a0vEWititNIzz_WbNDbojReboku0G12

Leave the default values:

E2twaBJWzoKspzzxkn-26XSsvalo8wAL3ayJYM3fVtszGyegf2o4-729bwV7jzammYv6Az1Ew2Mj--G3Kw4NZo0Ok

On the next screen, check the box labeled: Enable support for the SAML 2.0 WebSSO protocol. The service URL will be: https://YourAcc?untURL.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp

eJxJWt1KAQ5E7ldDZmtzrdiFB4icMGUHoVL5pDbAwO98o8CgHPIBOF73CHPQ6H1Cm7HuPbN4z-ZLf3Qt_ygNT

Click Next. Add Relying party trust identifier: https://YourAcc?untURL.ispringlearn.com/module.php/saml/sp/metadata.php/default-sp

X1S7UllJ3QhuitOZkPPDzm9GvR_oh0MZafS1VP4cMpGRNfmg8TVDzDePguMRDbQ61VwLaHMK6B2UuYIX_s4

Choose Permit all users to access this relying party.

_Dgqb5gnSjLRvtQKuIQ38K9wkVb97WYKFZXIiQb6OFAzlChmaFRNlH5H3J-YNS5h8j8it6BHfHADt88WfhCoUS3k

On the next step, just click Next.

AX0Y9Y9a0Al-EQAgUkmNTSC-tTxJXVe0K1G2fBf9_ZofD5PPBD9wltrEo1A6Av-SvpJwQ_bUibkawPZSjL-YMmJc

On the final screen, check the box Open the Edit Claim Rules dialog and use the Close button to exit.

ZS3_FXPmR5XFVIL4PE_wc5XczVkdUAtV17oG6Ed3qghwAdibKNFwmA8pISzu0ZUDoEvST2PA4NDgK_wLCb_

Step 6. Creating Claims Rules

1. Add the first rule
   ZUjVMXbGp0OoUkrJbpP90Tbgdx0vhmO6okP5lNz5kHXPxFqZ8zXCP22BK-mP0oYJKT3e0q4T1Al7pVMXfV
2. Select Send LDAP Attributes as Claims
   PfGJ2OSpACIm1nBtinVxH-hRr2IX7JsiG8V0wOASvZzD_5ohgTa5uQk3jFRwr9V8KcsIBSwBpNGBniGTAZpp
3. On the next screen, specify your Claim Rule, for Example E-mail to Learn, using Active Directory as your attribute store, and do the following:

1. Fr om the LDAP Attribute column, select E-Mail Addresses
2. Fr om the Outgoing Claim Type, enter “email” cbshGH1pmCu-u_um9H9JSU9MicGTn1jaoESRcZbqGhYy_wDAWT5TLi-7xjBvnhtoZx7NVxYAiKfRP75JD
3. Click on Finish or OK to save the new rule

4. After that, add the second rule and select Transform an Incoming Claim as the template Vldhqs282322jhhTUzugw7MZQzkKPrypE-UkoNmWx-D0X3cnlLQS2M6KVa82ORZ8ZFkPR9MjRRSmOUplU
   1. Give your Claim Rule a title, for example, Transform Account Name
   2. Select Windows account name as the Incoming Claim Type
   3. Under Outgoing Claim Type, select Name ID
   4. Under Outgoing Name ID Format, select Transient Identifier
   5. Leave the default rule Pass through all claim values J22FEWcG11f_f7Wta7PB0GepLEwafkUvUNuori6HE5SqEZqqiNS0HuTJ56PUaV-WiSsyUVHVAPops4QY
5. Finally, click on OK to create the claim rule, and then OK again to finish creating rules.

Step 7. Adjusting the Trust Settings

Some settings on your Relying Party Trust will need to be adjusted. To access these settings, select Properties from the Actions sidebar on the right while you have the Relying Party Trust selected.

- Under the Advanced tab, make sure that the selection is SHA-1 gNd4s8hFJrd4hzspladUgmtg60Q9bna6nn0O0q5TpNfkdwMr0dCftiWCFgT1mMPwQOg4BNuWQ8cMWYooU
- Under the Endpoints tab, click ADD to add a new endpoint
- For the Endpoint type, select SAML Assertion Consumer
- For the Binding, choose Artifact with Index 2
- The URL field should look like this: https://YourAcc?untURL.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp
- Leave the Response URL blank and click on OK gsGicTEDLYbI9F0K7iJIIWm_jmnD4rYS8dQeJDEM3ncvix3uMW4v1mWmEb5FKKkC3JKwNAFs9HfLpYDHU
- Click ADD one more time
- For the Endpoint type, sele ct SAML Logout
- For the Binding, choose POST

- The URL field should look like this: https://Y?UR_ADFS_SERVERNAME.domail.local/adfs/ls/?wa=wsignout1.0
- Leave the Response URL blank and click on OK
gf1gpP3TETi2aIqvn79UxX2UY5Y8lxXS6bneJEpQMkBBKEAOq998XfDnZXm6Kd4FNgCBWknm-wEm1BAe6

Step 8. Logging

Go to your SSO login page: https://YourAcc?untURL.ispringlearn.com/sso/login and enter your credentials.

Related Articles

- Integrating iSpring Learn with your system: User Management and Single Sign On
- SAML Technology for SSO
- iSpring Learn SSO with Azure AD + SAML

Revision #1
Created 2024-01-21 18:50:42 UTC by joliveira
Updated 2024-01-21 19:23:47 UTC by joliveira