# OpenSSO WS-Federation How-to

This document describes the sequence of actions required to deploy WS-Federation in OpenSSO.

READ THE ENTIRE DOCUMENT BEFORE YOU START, especially the 'Gotchas' section. The listed steps must be followed in strict order as there are many dependencies in the sequence,some not at all obvious.

In case of any problem, set debug logging to 'message', zip the contents of the OpenSSO debug and log directories and the webcontainer's log directory and email them to `dev@opensso.dev.java.net` with as detailed a description as possible

## Contents

## References

| | |
|---|---|
| 1 | Step-by-Step Guide for Active Directory Federation Services<br>http://www.microsoft.com/downloads/details.aspx?familyid=062F7382-A82F-4428-9BBD-A103B9F27654&displaylang=en |

## Prerequisites

A suitable container (any OpenSSO-supported container will do), **with SSL configured**. ADFS will not POST a WS-Federation RSTR to a non-HTTPS URL.

## AM Install/Configuration

- Deploy OpenSSO WAR file – build from CVS or use any nightly after 6/21/07. Ensure that the services are available via SSL - you should now be able to log in securely to AM via `https://`*`amhost`*`(:`*`amsecureport`*`)/amserver/console`
  You'll have to accept the new cert in the browser. In IE, ensure you add the root cert, rather than the server cert itself.
- While you're logged in to AM, create a new user – Directory Management/Users/New.

## ADFS Install/Configuration

- Setup ADFS as per 'Step-by-Step Guide for Active Directory Federation Services' [1]. Where I don't mention an option, just leave it with the default.
- Add a new 'Resource Partner' to each box:

    - Display name: `OpenFM`
    - Federation Service URI: `urn:federation:openfm`
    - Federation Service endpoint URL: `http(s)://`*`amhost`*`(:`*`port`*`)/openfm/WSFederationServlet/metaAlias/wsfedsp`
- Create a new user in AD, with login name the same as the UID you created in AM: Start/Administrative Tools/Active Directory Users and Computers, right click Users, New/User. If you want to be able to login on the domain controler as this new user then, after creating the new user, right click, Add to a group, and type 'Domain Admins' (without the quotes) into the dialog.

## AM WS-Federation Configuration

- Convert the AD machine's token signing certificate file (e.g. adfsaccount_ts.cer) to PEM format. You can use OpenSSL for this: `openssl x509 -in adfsaccount_ts.cer -inform DER -out adfsaccount_ts.pem -outform PEM`
- Create the following files:

  **`adfsaccount.xml`** – you will need to paste the PEM-encoded certificate from `adfsaccount_ts.pem` into the `<ns2:X509Certificate>` element.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Federation FederationID="urn:federation:adatum"
xmlns="http://schemas.xmlsoap.org/ws/2006/12/federation">
    <TokenSigningKeyInfo>
        <ns1:SecurityTokenReference ns1:Usage=""
xmlns:ns1="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
            <ns2:X509Data
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
                <ns2:X509Certificate>
MIIC0DCCAbygAwIBAgIQ/SQKpB08uqtJ/4BwGzpTODAJBgUrDgMCHQUAMCgxJjAk
BgNVBAMTHUZlZGVyYXRpb24gU2VydmVyIGFkZnNhY2NvdW50MB4XDTA3MDMxNjAw
MTIyMVoXDTA4MDMxNTA2MTIyMVowKDEmMCQGA1UEAxMdRmVkZXJhdGlvbiBTZXJ2
ZXIgYWRmc2FjY291bnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCk
TBDiJ3KUU1/1Z2k1DFlsz1ztP+IzuB4TSvUKn75FYQlJfzawuUhGdugozuUpkWlP
mEWi4HsKtL/cyVN+KmVihbUCPvBWq9k/7J37xXi93r85hEq3KCI+lIIfr354qqWO
tGChPUG258rElcTNIeP2IKIJxhcp7LGeTcryAgSGbj5lT6NrFX4dCM8jyzQjY1xP
UPpgoxb44cIpq8wW/jnbJMYMHOJFbEK57sXtU3+4sw75757QZA/QSOlkYfBgJa7c
y5kemHEnvN/tQiCDcrW9HoVhJnzy0RLLx6QO0MdDSx1R/AXADYkPfh1EsqWnpUoe
Q89Rh2mQKEXh7Zc8rZZJAgMBAAEwCQYFKw4DAh0FAAOCAQEAoiVAAoYpG+ka7qTo
28xaJnzrStMGb04faHoVpy9j6CaUSk/tweUzDVVxSvhOYXCNPykP9yWDUv5md46Q
xvhhfrQvXHkbbW1x+PAMjBkH9roTT8xyv0i9+anOZd7V46iSlObcSeSQvaUH2iB2
w+dGEFwKJSNs/8Cl8Ib157Uq6kwKoJvhn6zGb9j9tr4ryoa6UvDB73AYcIg3imX0
tkKZ9/rNkKaV9R9TfykzX5Tgih348FFtSElSp12QaTOTs/Ct2WK5enBz0Dlc83sb
wQ3sBrv1ZPP/gwpqW6fQuLnH2tZSF910SNNDlWnpDMnM9KqVRLyKI6fXDwnaL7ZB
22xkiw==
                </ns2:X509Certificate>
            </ns2:X509Data>
        </ns1:SecurityTokenReference>
    </TokenSigningKeyInfo>
    <TokenIssuerName>urn:federation:adatum</TokenIssuerName>
    <TokenIssuerEndpoint>
```

```
        <ns3:Address
xmlns:ns3="http://www.w3.org/2005/08/addressing">https://adfsaccount.adat
um.com/adfs/ls/</ns3:Address>
    </TokenIssuerEndpoint>
    <TokenTypesOffered>
        <TokenType Uri="urn:oasis:names:tc:SAML:1.1"/>
    </TokenTypesOffered>
    <UriNamedClaimTypesOffered>
        <ClaimType Uri="http://schemas.xmlsoap.org/claims/UPN">
            <DisplayName>UPN</DisplayName>
        </ClaimType>
    </UriNamedClaimTypesOffered>
</Federation>
```

**adfsaccountx.xml**

```
<FederationConfig xmlns="urn:sun:fm:wsfederation:1.0:federationconfig"
    xmlns:fm="urn:sun:fm:wsfederation:1.0:federationconfig"
    hosted="0"
    FederationID="urn:federation:adatum">
    <IDPSSOConfig metaAlias="/adatumidp">
        <Attribute name="DisplayName">
            <Value>Adatum Corp</Value>
        </Attribute>
    </IDPSSOConfig>
</FederationConfig>
```

**wsfedsp.xml** – you will need to change the hostname and port in the `<ns3:Address>` element to match your configuration.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Federation FederationID="wsfedsp"
xmlns="http://schemas.xmlsoap.org/ws/2006/12/federation">
    <TokenIssuerName>urn:federation:openfm</TokenIssuerName>
    <TokenIssuerEndpoint>
        <ns3:Address
xmlns:ns3="http://www.w3.org/2005/08/addressing">https://patlinux.red.ip
lanet.com:8443/openfm/WSFederationServlet/metaAlias/mywsfedsp</ns3:Addres
s>
    </TokenIssuerEndpoint>
</Federation>
```

**wsfedspx.xml** – you will need to change the hostname and port in the `HomeRealmDiscoveryService` attribute to match your configuration.

```
<FederationConfig xmlns="urn:sun:fm:wsfederation:1.0:federationconfig"
    xmlns:fm="urn:sun:fm:wsfederation:1.0:federationconfig"
    hosted="1" FederationID="wsfedsp">
    <SPSSOConfig metaAlias="/wsfedsp">
        <Attribute name="AccountRealmSelection">
            <Value>cookie</Value>
        </Attribute>
        <Attribute name="AccountRealmCookieName">
            <Value>amWSFederationAccountRealm</Value>
        </Attribute>
        <Attribute name="HomeRealmDiscoveryService">
            <Value>http://patlinux.red.iplanet.com:8180/amserver/RealmSel
ection</Value>
        </Attribute>
    </SPSSOConfig>
</FederationConfig>
```

- Create a circle of trust and import the newly created metadata using fmadm:

```
fmadm create-circle-of-trust -u amadmin -w password -t cot1

fmadm import-entity -u amadmin -w password -m adfsaccount.xml -x
adfsaccountx.xml -t cot1 -c wsfed

fmadm import-entity -u amadmin -w password -m wsfedsp.xml -x wsfedspx.xml -t
cot1 -c wsfed
```

- If all is well, you should be able to go to `https://patlinux.red.iplanet.com:8443/openfm/WSFederationServlet?wreply=https://patlinux.red.iplanet.com:8443/openfm&wtrealm=/mywsfedsp` and be forwarded to the realm selection page. Click 'Proceed' and you'll see a few redirections in the browser's address bar before landing at the user's AM page. If you do this from outside the Window domain, you'll get an HTTP basic auth-style username/password dialog. Enter the test user's credentials and you should be in. The realm selection process sets a persistent cookie; if you go to the above URL a second time, you should not be prompted for a realm – you should be redirected straight to the AM user page.

## Gotchas

- The ADFS box's clock needs to be at the same time as the AM box. Configuring NTP everywhere is a good solution.
- If you do a desktop SSO from a browser window, then try to do another one in quick succession from the same window, ADFS will fail with an error stating that you have tried to request two tokens from the same browser session within a 20 second window. Just close the browser window(s) and try again – this deletes the non-persistent cookies.
- The logo jpg on the realm selection and login pages looks a bit crap in IE. It seems to have transparent areas top and bottom.