

Eurécia Single Sign-On (SSO)

Setting up SSO with ADFS

# Glossary:

|  |  |
| --- | --- |
| **Name** |  |
| IDP | Identity Provider: your company’s ADFS (or similar product) which provides your authenticated user access |
| SP | Service Provider: the Eurécia application |
| AD | Active Directory |

Hardware requirements:

|  |  |
| --- | --- |
| **Minimum configuration** |  |
| Windows Server version | Windows Server 2008 Enterprise or later |
| Memory | 2 GB RAM |
| Disk space | At least 10 GB |

1. Install and configure the software required

|  |  |  |  |
| --- | --- | --- | --- |
| **Software/Service** | **Action** | **Description** | **Link** |
| IIS (Internet Information Service) server | Use the **Server manager** to add the “Web Server (IIS)” server role | This server is needed to provide the web pages |  |

1



|  |  |  |  |
| --- | --- | --- | --- |
| ADFS 2016 | Use the **Server manager** to add the ADFS role | This is the Identity Provider that will provide the user identities from the AD data | [https://docs.microsoft.com](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-deployment)[/en-us/windows-](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-deployment) [server/identity/ad-fs/ad-fs-](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-deployment) [deployment](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-deployment)[https://docs.microsoft.com](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2)[/en-us/windows-](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2) [server/identity/ad-](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2) [fs/deployment/set-up-the-](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2) [lab-environment-for-ad-fs-](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2) [in-windows-server-2012-](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2)[r2](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/set-up-the-lab-environment-for-ad-fs-in-windows-server-2012-r2) |

# Creating a self-signed certificate using the IIS server (optional)

The purpose of this step is to ensure that SSL is activated. If it already is, you can ignore this step.

* 1. Open the IIS manager from the console (Start menu > IIS manager
	2. Double-click the “Server certificates” icon. See the red box in the following screen capture:



2

* 1. In the “Actions” pane, click “Create self-signed certificate”. See following screen capture:



* 1. In the “Specify a friendly name for the certificate” field, enter your server’s FQDN (Full Qualified Domain Name)
	2. In the same view’s “Connections” pane, click “Default Web Site” and then, in the “Actions” pane, click “Bindings”



* 1. Next, click the “Add” button and then, in the “Type” value list, select “https”.
	2. In the “Certificate” field, select the name of the certificate that you created earlier. Finish by clicking “OK”

3





4



# Configuring the ADFS 2016 server

* 1. In the home page, type “AD” and then select “AD FS management”
	2. In the home page’s “Actions” (right-hand) pane, click “Add Relying Party Trust”



In the window that opens, click the “Welcome” button and then select “Import data about the replying party published online or on a local network”



5

The URLs are in the following form:

*https://EuréciaServerAddress/Shibboleth.sso/Metadata*

The EuréciaServerAddress part of the URL depends on which Eurécia server you want to connect to via SSO.

For example, to connect to the Eurécia production platform via SSO, the URL is:

*https://plateforme.eurecia.com/Shibboleth.sso/Metadata*

For the demo platform, the URL is:

*https://demo.eurecia.com/Shibboleth.sso/Metadata*

If you see the following error message:



your ADFS is probably unable to negotiate the proper HTTPS protocol with our site – we accept **TLS 1.1** or later.

If you see the following message, you can ignore it and simply click “OK”



* 1. In the next window, leave the prefilled full name unchanged (it must be in the form of XXX.eurecia.com) and then click “Next”
	2. Select “Permit all users to access this replying party” and then click

“Next”.

6

* 1. A summary of the information entered is displayed. Click “Next ”.
	2. Leave the “Open the Edit Claim Rules dialog for this replying party trust when the wizard closes” checkbox selected in the next window and then click “Close”.
	3. A new window is displayed. Click the “Add rule” button.
	4. In the value list, select “Send LDAP Attributes as Claims” and then click “Next” (see screen copy).



7

* + 1. Type **GetEmail** in the “Claim rule name” field. In the “Attribute store” field, select “Active Directory”. In the “Mapping of LDAP attributes to outgoing claim types” section”, select the values shown in the following table:



1. Click the “Finish” button
2. Open an internet browser and then enter the following URL (the URL may differ depending on your version of ADFS):

[**https://localhost/FederationMetadata/2007-06/FederationMetadata.xml**](https://localhost/FederationMetadata/2007-06/FederationMetadata.xml)

**Note**: the URL used to access your ADFS may be displayed instead of localhost

1. Save the generated XML file on your Desktop, naming it IDPFederationMetadata.xml

You have now finished setting up identity federation from your Active Directory. You now only have to send the **IdpFederationMetadata.xml** file to the Eurécia customer support team at **support@eurecia.com**

8



# Setting up acceptance testing

* Testing requirements:
	+ Eurécia’s employee database of identified users must be installed.
	+ The metadata file must have been sent to Eurécia (Step k. of the “Configuring the ADFS 2016 server” section)
* Create a shortcut for making a test sign-on from the client workstation: *https://demo.eurecia.com/Shibboleth.sso/Login?target=https://demo.eurecia.com/eurecia/s ecureshib&entityID=*[*http://****url.access.adfs****/adfs/services/trust*](http://url.access.adfs/adfs/services/trust)

**url.access.adfs =** URL used to access your ADFS

**demo.eurecia.com =** the Eurécia platform address used to set up the SSO connection

**Note:** The method using a shortcut to test the sign-on may cause a redirection error, depending on which browser is used and how your ADFS is configured.

This is because the first time you sign in, you will be asked to enter your Windows username and password. When you do so, the browser may “forget” the dialogue that it had previously with the Eurécia platform and therefore not send all the necessary information to your ADFS.

In this case, simply run the shortcut again – as the username and password have already been saved, you will be able to sign in without any problem.

# Setting up employee database provisioning via FTP (optional)

This section explains how to set up LDAP directory synchronisation with the Eurécia employee database. This synchronisation will be carried out using a file in a special format defined by Eurécia (see following shell script). This file will be placed in an FTP repository (Eurécia must be told the login/sign-on details to enable us to configure the job).

**From Windows**, create a shell script that runs a scheduled task at the intervals you specify. The output file will be placed in an FTP repository (overwriting the previous copy there)

Get-ADUser -Filter { memberOf -RecursiveMatch "CN=EURECIA,CN=Users,DC=XXXX,DC=com" } -Properties emailaddress | Select @{Name="LASTNAME";Expression={$\_.Surname}},@{Name="FIRSTNAME";Expression={$\_.GivenName}},@{Name="EMAIL\_USER";Expression={$\_.emailAddress}} | Convertto-CSV -Delimiter ";" -NoTypeInformation > "c:\temp\fichierOut.csv"

Eurécia must configure the data transfer module that will regularly retrieve the data (in the special format defined by Eurécia) from an FTP/sFTP repository and update the employee database:

9

Whenever a new employee is created

o

* Whenever an employee’s information is updated
* Whenever an employee is archived upon leaving the company

# Frequent problems

Some Windows Server versions may cause redirection problems during the authentication phase.

This problem results in a “web page unavailable” error message.

**Update:** Install update [2896713](http://support2.microsoft.com/kb/2896713)

10