

Single sign-on authentication (SSO)

Background Info



This feature is available in Lucy 4.6 or newer version.



We do not recommend using Let's Encrypt certificates with an SSO provider due to the short live term of charge-free certificates.

Lucy allows you to set the SSO authentication by using the Lightweight Directory Access Protocol (LDAP) to access Admin console and EndUser portal. This also allows you to use a non-unique link for the awareness website within a campaign.

In general terms, SSO in Lucy can be used for:

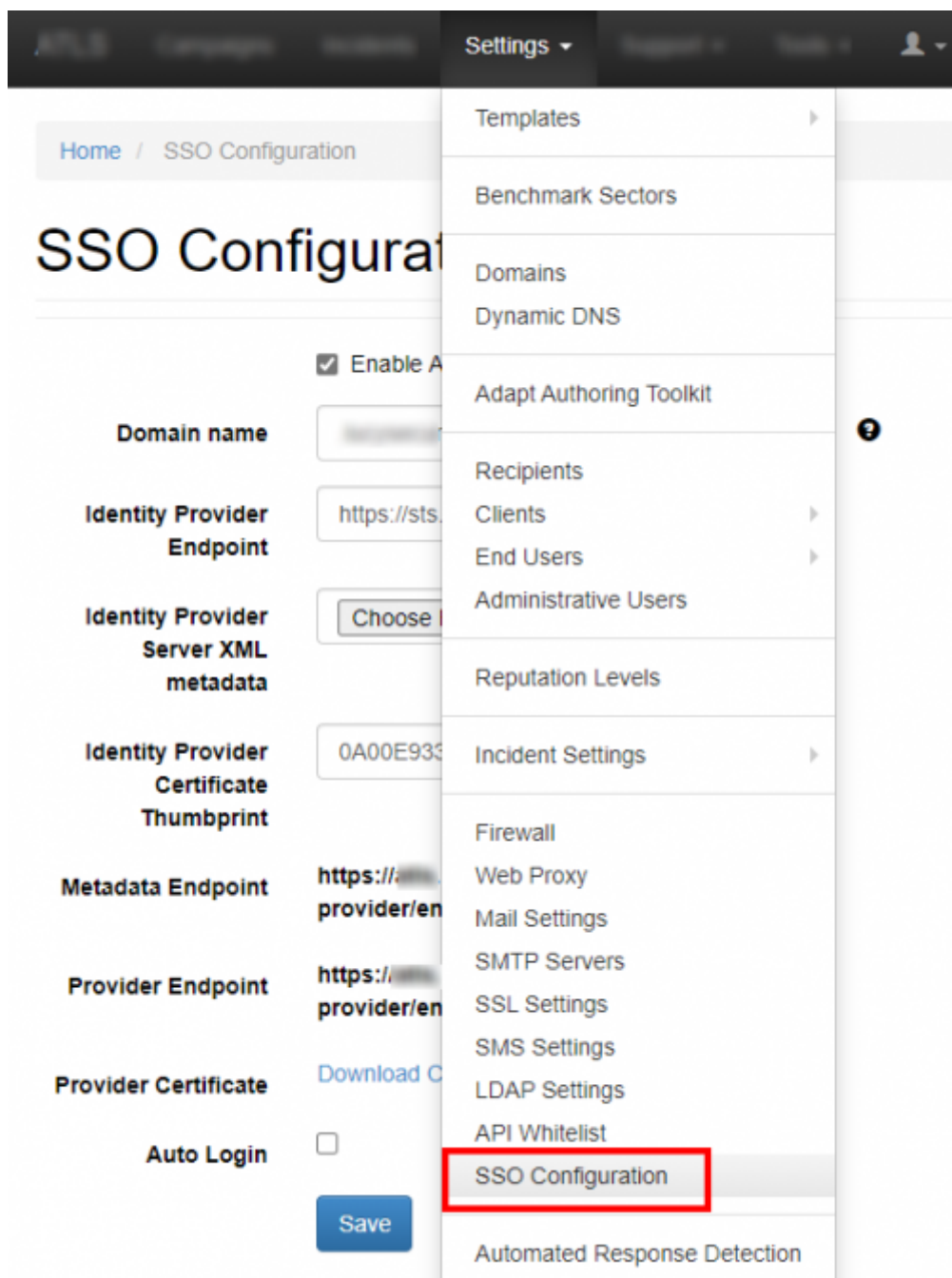
- authorization on Lucy's admin console and End-User portal:
- to identify users on awareness website.

Where can this be configured?

To use SSO in Lucy you should have installed [Active Directory Federation Services](#) (AD FS) on your Windows server. Lucy uses [Security Assertion Markup Language 2.0](#) (SAML 2.0) for exchanging authentication and authorization data, which supports the following versions of AD FS:

- ADFS 2.0 (Windows Server 2008 and Windows Server 2008 R2)
- ADFS 2.1 (Windows Server 2012)
- ADFS 3.0 (Windows Server 2012 R2)
- ADFS 4.0 (Windows Server 2016)
- ADFS 5.0 (Windows Server 2019)
- Azure AD (refer to [this guide](#) to have a detailed instructions)
- Okta (refer to [this guide](#) for more details)

The connection to the AD FS can be configured within the Settings / SSO Configuration:



What preparations need to be done before connecting to AD FS?

- Upload or create an SSL certificate for Lucy Admin console - see [this article](#).
- Make sure you have an Administrator account in Lucy (Settings> Users) with an email address that corresponds to your Windows account in Active Directory. Both accounts must have the same email address:

Home / Users / User #3

Lucy - Edit User

Email

Country Code

Phone

Two-Factor Authentication is not configured.

Name

Support Properties

Security	Environment	Sessions	Remote control
Remote Desktop Services Profile	COM+	Attribute Editor	
Published Certificates	Member Of	Password Replication	Dial-In
Object			
General	Address	Account	Profile
Telephones	Organization		

Support

First name: Initials:

Last name:

Display name:

Description:

Office:

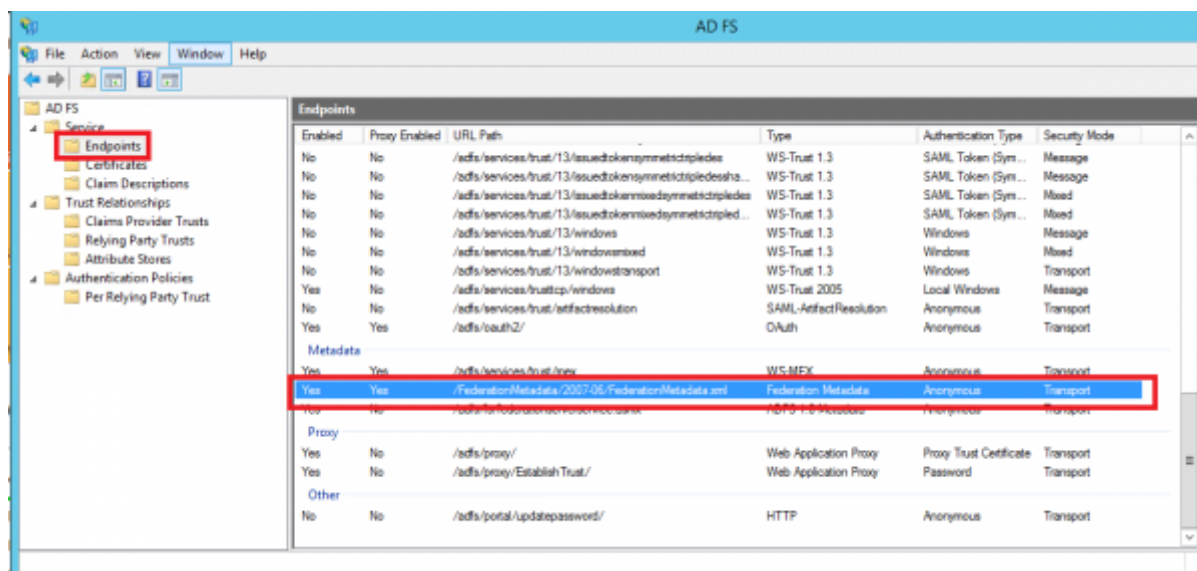
Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

- Download the [FederationMetadata.xml](#) file from your AD FS server. Log in to Windows Server > open **Server Manager** > click **Tools** > click **AD FS Management** > expand **Service** and select the **Endpoints** node:



Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode
No	No	/ads/services/trust/13/issuedtokensymmetricdesha...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/ads/services/trust/13/issuedtokensymmetricdesha...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/ads/services/trust/13/issuedtokensymmetricdesha...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/ads/services/trust/13/issuedtokensymmetricdesha...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/ads/services/trust/13/windows	WS-Trust 1.3	Windows	Message
No	No	/ads/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mixed
No	No	/ads/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport
No	No	/ads/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Mixed
Yes	No	/ads/services/trust/13/windowstransport	WS-Trust 2005	Local Windows	Message
No	No	/ads/services/trust/artifactresolution	SAML Artifact Resolution	Anonymous	Transport
Yes	Yes	/ads/oauth2/	OAuth	Anonymous	Transport
Metadata					
Yes	Yes	/ads/services/trust/13/	WS-MEX	Anonymous	Transport
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Anonymous	Transport
No	No	/ads/artifactresolution/	SAML Artifact Resolution	Anonymous	Transport
Proxy					
Yes	No	/ads/proxy/	Web Application Proxy	Proxy Trust Certificate	Transport
Yes	No	/ads/proxy/EstablishTrust/	Web Application Proxy	Password	Transport
Other					
No	No	/ads/portal/updatepassword/	HTTP	Anonymous	Transport

For example, your Federation Service is located at <https://fs.domain.tld/>, then the link to download the FederationMetadata.xml file looks like:

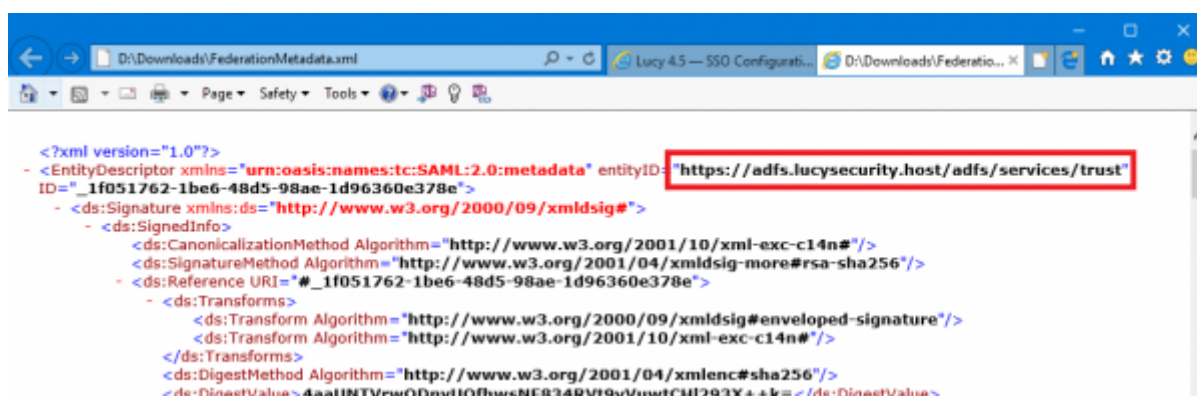
<https://fs.domain.tld/FederationMetadata/2007-06/FederationMetadata.xml>

- Open a browser and navigate to the FederationMetadata.xml location where you'll be prompted to save the file to disk.

Enable Single sign-on in Lucy

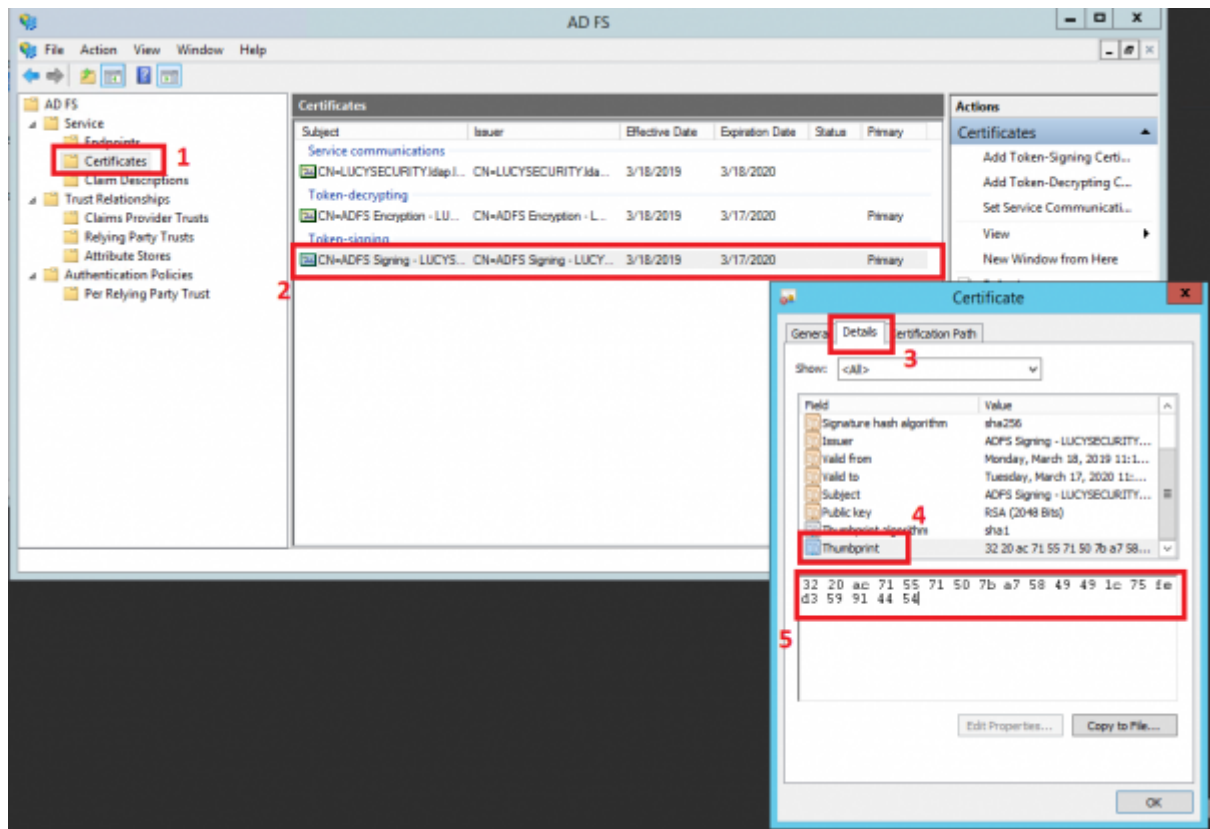
- Navigate to the **SSO Configuration** page
- Active the option "**Enable Active Directory FS**"
- Insert the URL in to the field **Identity Provider Endpoint**:

The URL of **Identity Provider Endpoint** can be taken from the FederationMetadata.xml file we downloaded earlier:

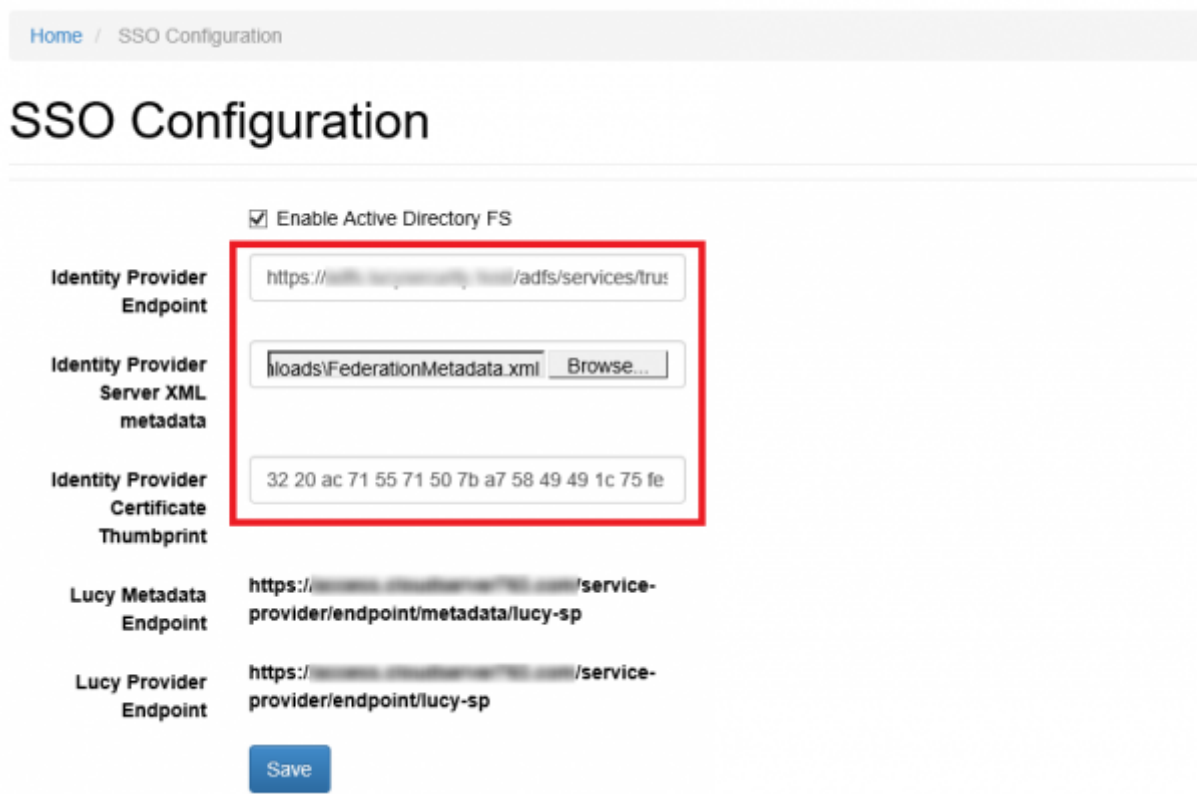


- Select the FederationMetadata.xml file in to the field **Identity Provider Server XML metadata**.
- Insert the Thumbprint information in to the field **Identity Provider Certificate Thumbprint**:

The Certificate Thumbprint can be taken from the AD FS server. Open **Server Manager** > click **Tools** > click **AD FS Management** > expand **Service** and select the **Certificates** node > open the certificate from the "Token-signing" section:



In the end, the SSO Configuration page will look like this:



- Click Save.

Create the Relying Party Trust in AD FS

- Copy the **Lucy Metadata Endpoint** link from the **SSO Configuration** page:

Home / SSO Configuration

SSO Configuration

☒ Enable Active Directory FS

Identity Provider Endpoint

Identity Provider Server XML metadata


Identity Provider Certificate Thumbprint

Lucy Metadata Endpoint

Lucy Provider Endpoint

Lucy Provider Certificate [Download Certificate](#)

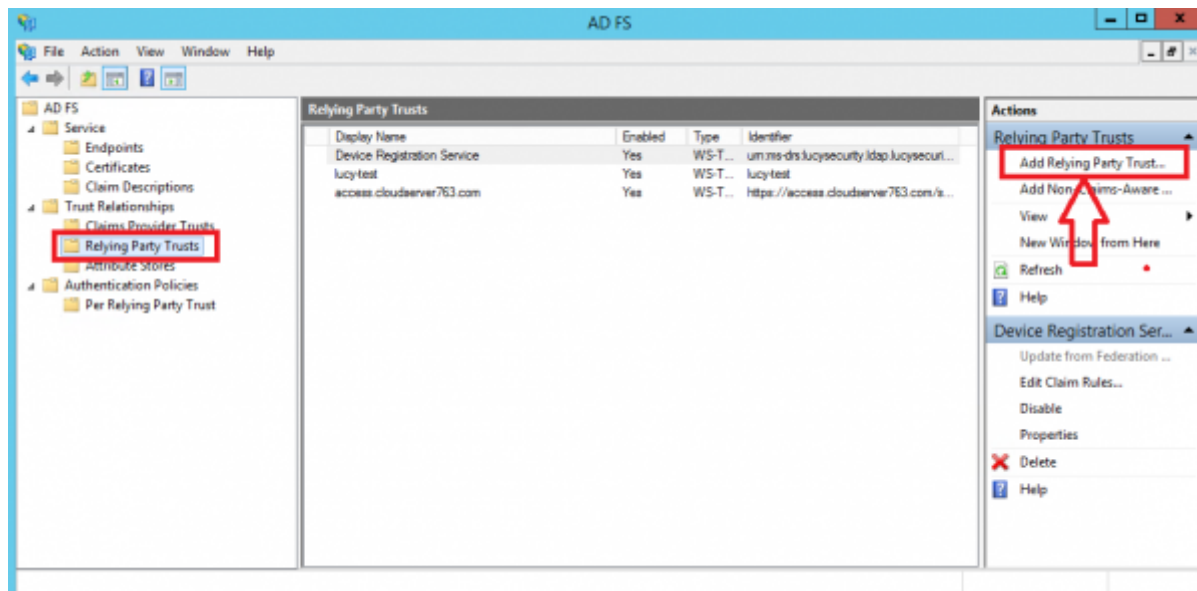
- On your AD FS server, open the **AD FS Management** console, expand **Trust Relationships** and select the **Relying Party Trusts** node. In the Actions pane, click **Add Relying Party Trust**:

Attention  If the Lucy Admin Console is configured on a non-standard port (for example, port 8443, see more [here](#)), then you will need to add **two separate entry of Relying Party Trust** with the identical parameters, but different Federation metadata address (URL):

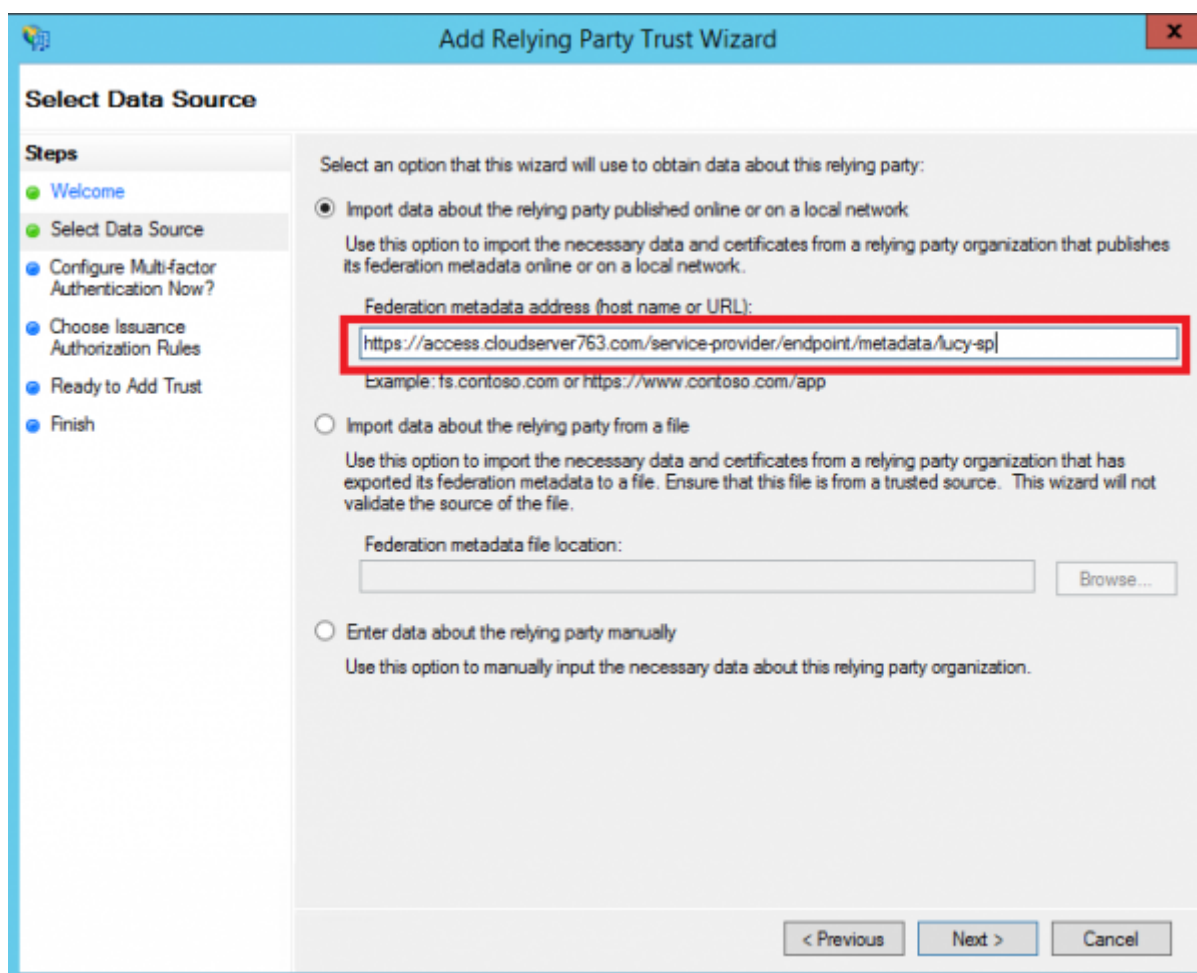
The first will be: <https://lucydomain.com/service-provider/endpoint/metadata/lucy-sp>

Second: <https://lucydomain.com:8443/service-provider/endpoint/metadata/lucy-sp>

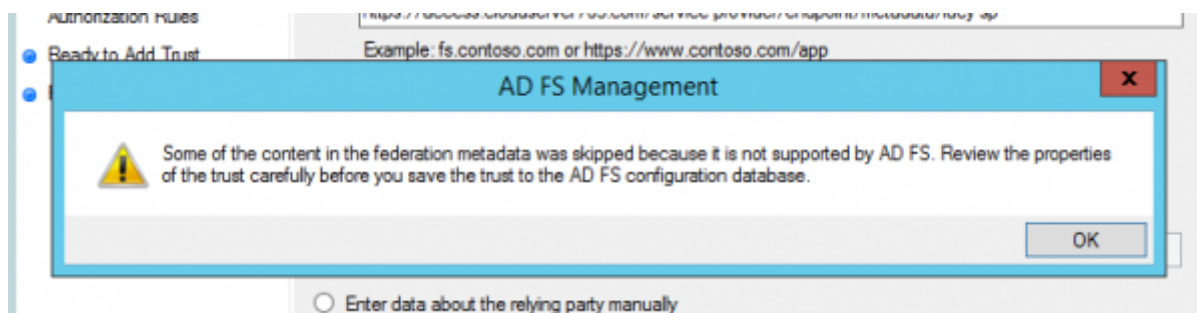
In case access to the Lucy Admin Console is limited to a range of IP addresses, you must include an ADFS server in this range.



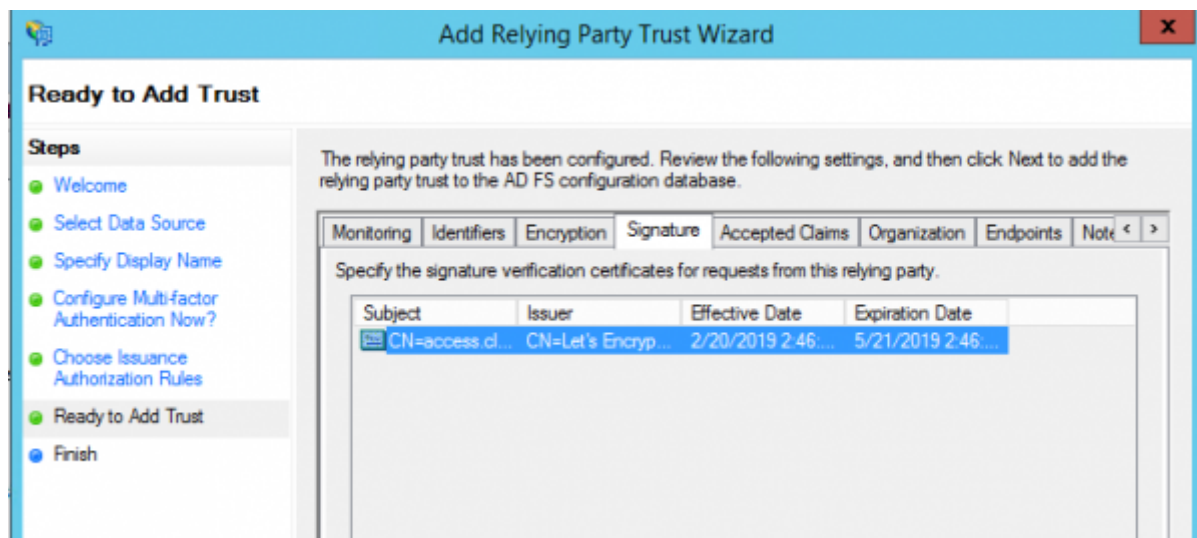
- Click **Start** then paste the **Entity ID** url in to the Federation Metadata address field and click **Next**.



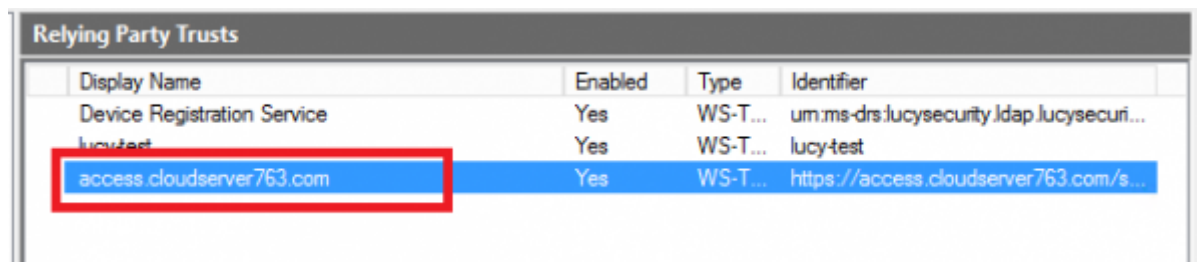
- Accept the warning:



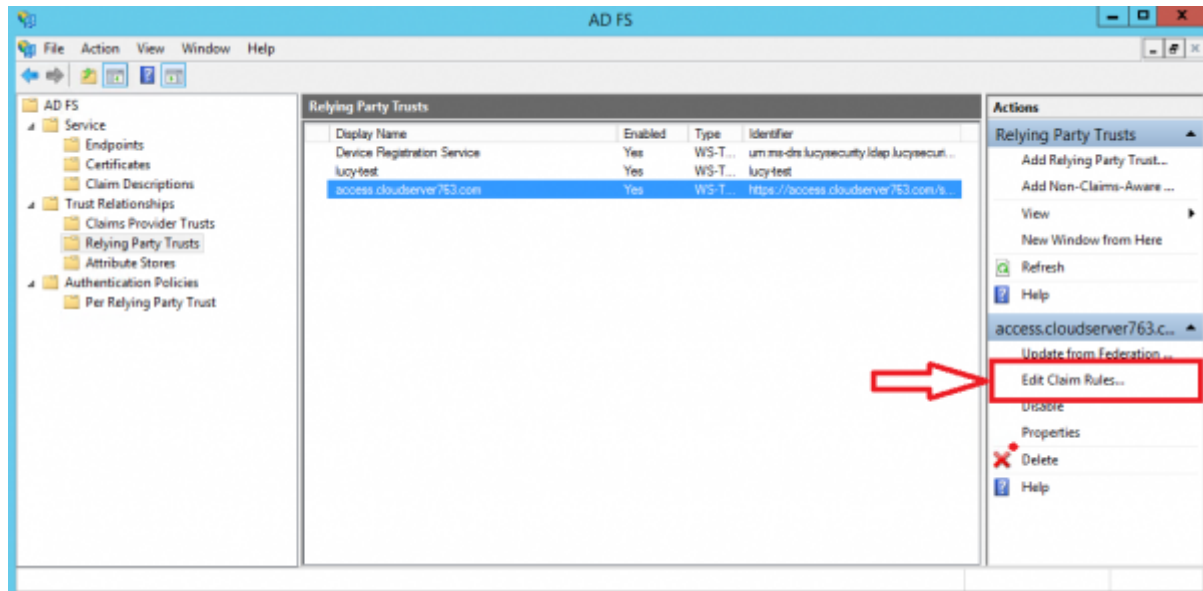
- Click the **Next** button in the wizard until you reach the Ready To Add Trust page. Check the Encryption and Signature tabs have certificates associated with them:



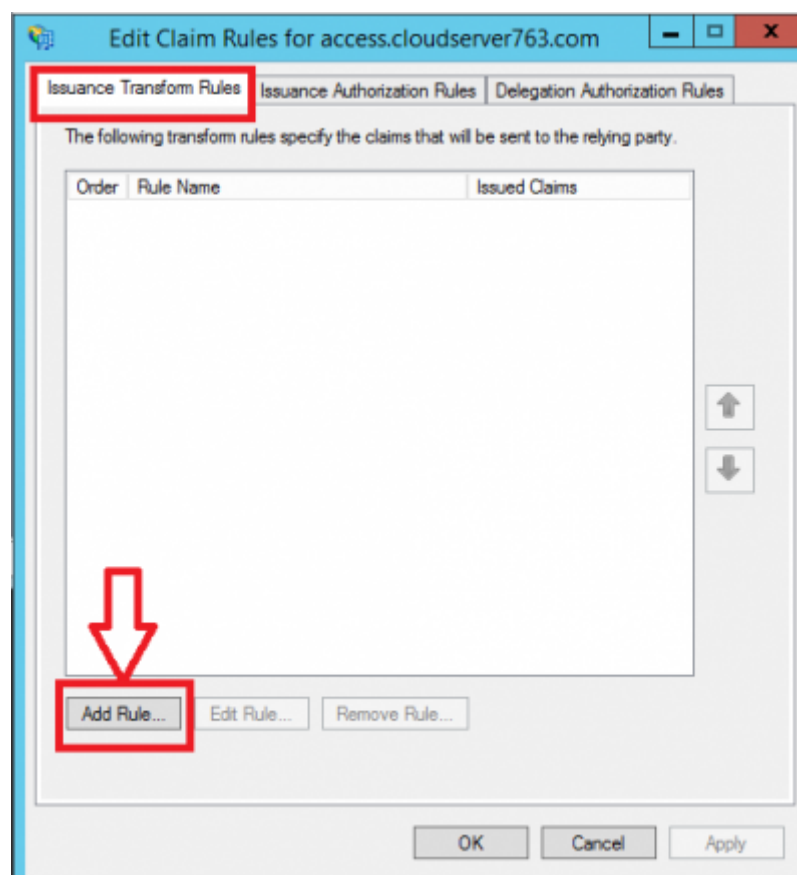
- Click **Next** and the Relying Party Trust is added:

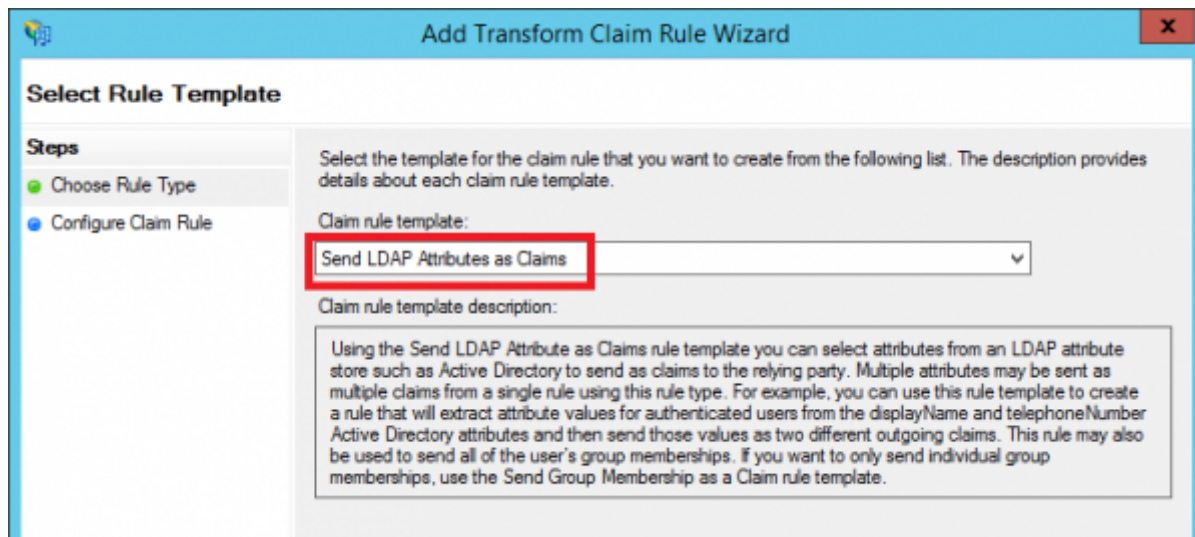


- Select the Relying Party Trust you have just added and then click **Edit Claim Rules**:

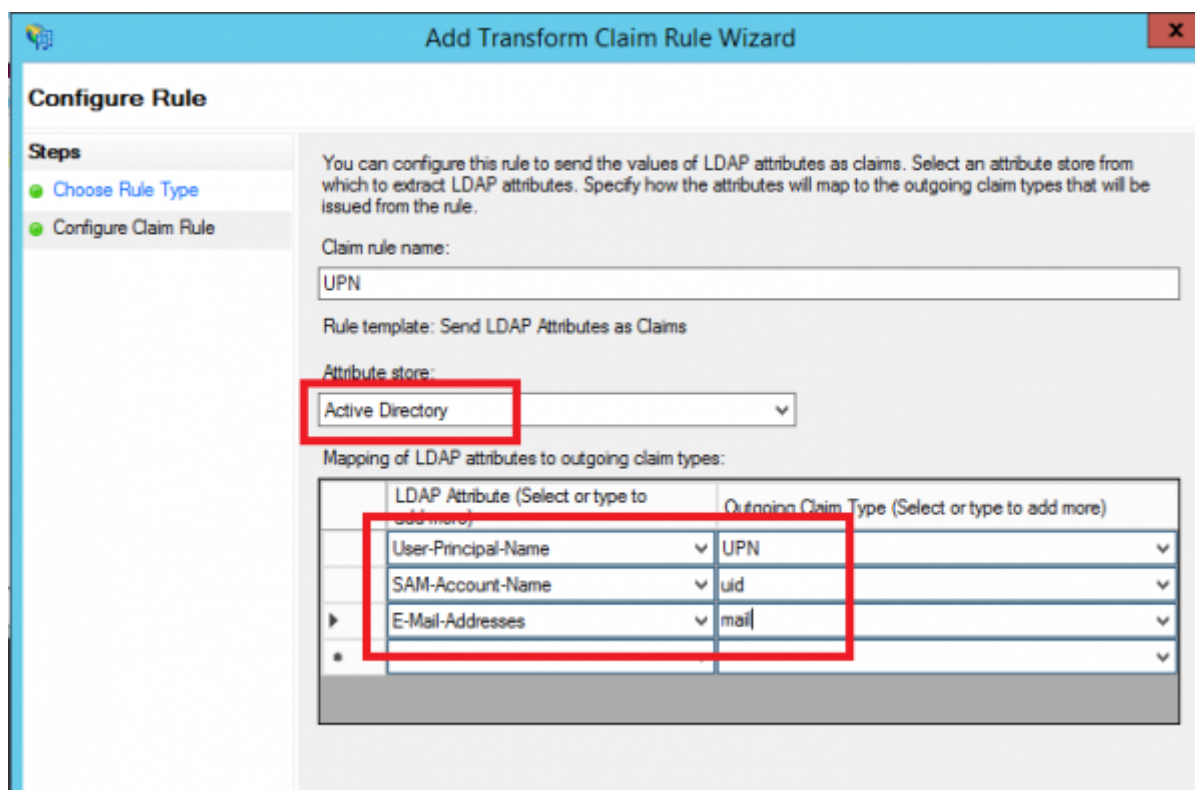


- Add an **Issuance Transform Rule** based on the **Send LDAP Attributes as Claims** template:

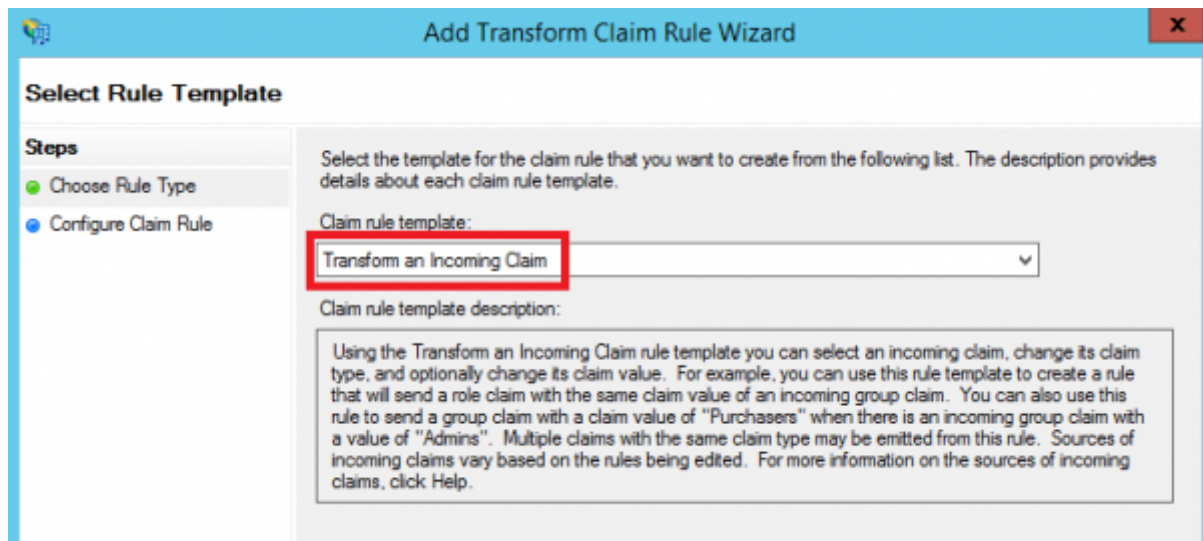




- Select UPN, uid and mail as shown on the screenshot below:



- Add another **Issuance Transform Rule** based on the **Transform an Incoming Claim** template:



The screenshot shows the 'Add Transform Claim Rule Wizard' window, specifically the 'Select Rule Template' step. The 'Steps' pane on the left shows 'Choose Rule Type' as the current step. The main area contains a description of the wizard and a dropdown menu for 'Claim rule template:'. The dropdown is set to 'Transform an Incoming Claim', which is highlighted with a red rectangle. Below the dropdown is a text box for 'Claim rule template description:'.

Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

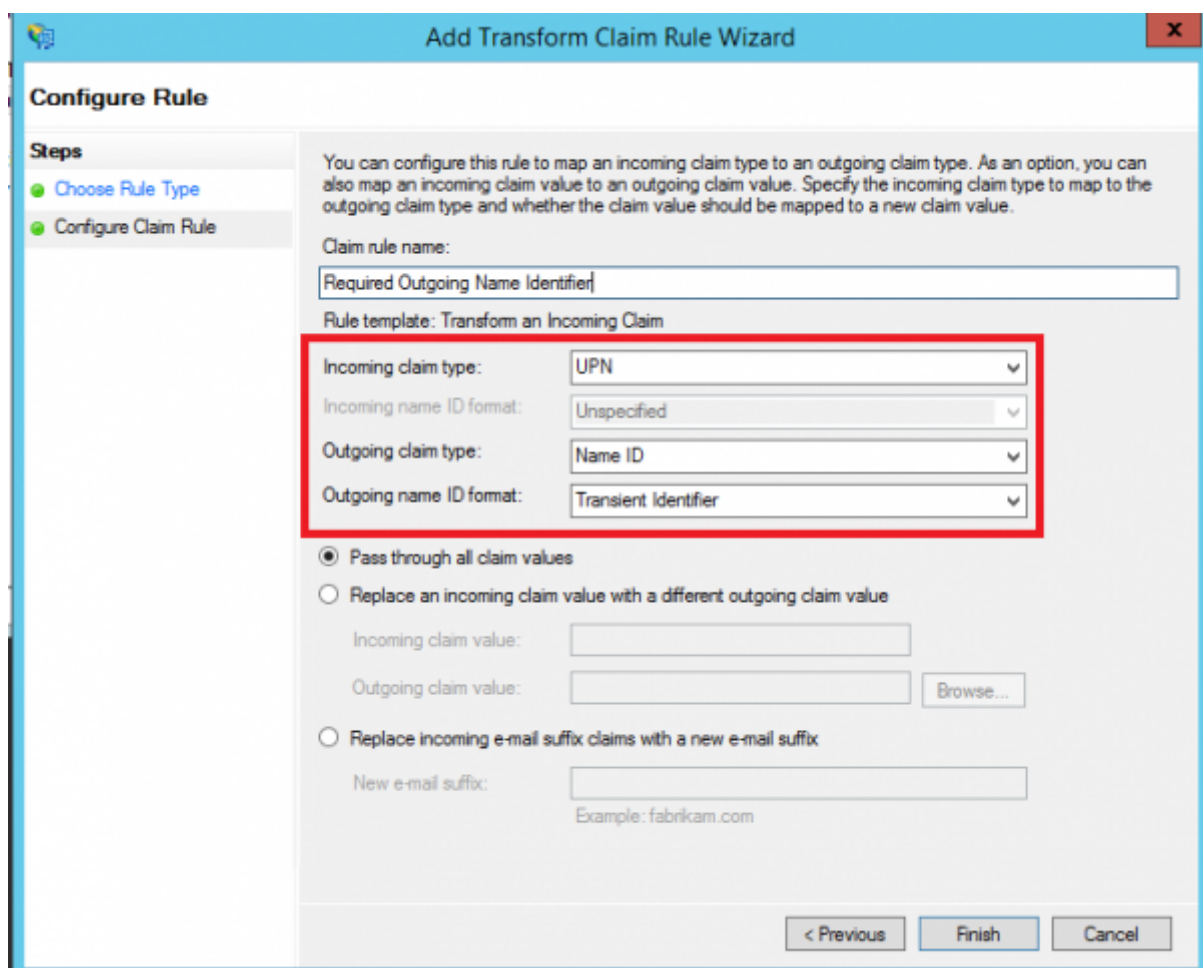
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.



The screenshot shows the 'Add Transform Claim Rule Wizard' window, specifically the 'Configure Rule' step. The 'Steps' pane on the left shows 'Configure Claim Rule' as the current step. The main area contains a description of the step and several configuration fields. The 'Rule template' is 'Transform an Incoming Claim'. The 'Incoming claim type' is 'UPN', 'Incoming name ID format' is 'Unspecified', 'Outgoing claim type' is 'Name ID', and 'Outgoing name ID format' is 'Transient Identifier'. These four fields are grouped together and highlighted with a red rectangle. Below these fields are three radio button options: 'Pass through all claim values' (selected), 'Replace an incoming claim value with a different outgoing claim value', and 'Replace incoming e-mail suffix claims with a new e-mail suffix'. The 'Finish' button is highlighted.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Required Outgoing Name Identifier

Rule template: Transform an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Transient Identifier

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

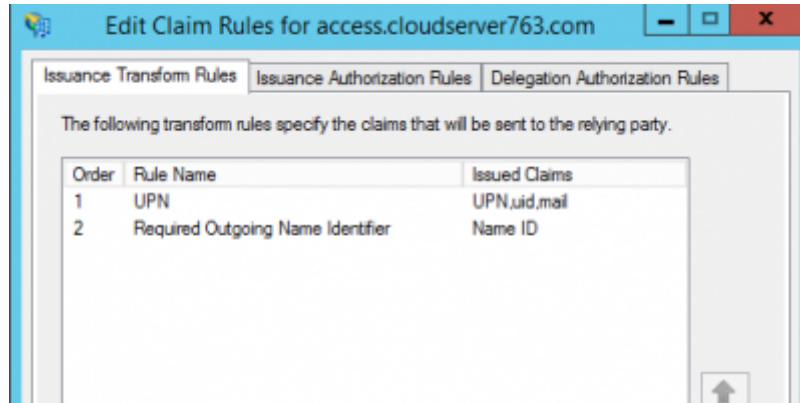
☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

< Previous Finish Cancel

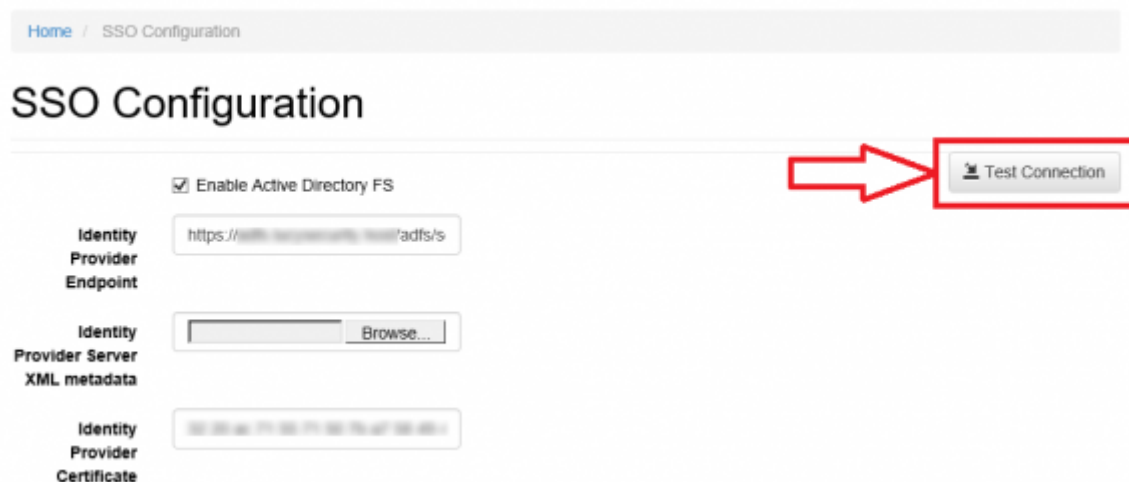
- Once configured, you should have two **Issuance Transform Rules** that look as follows:



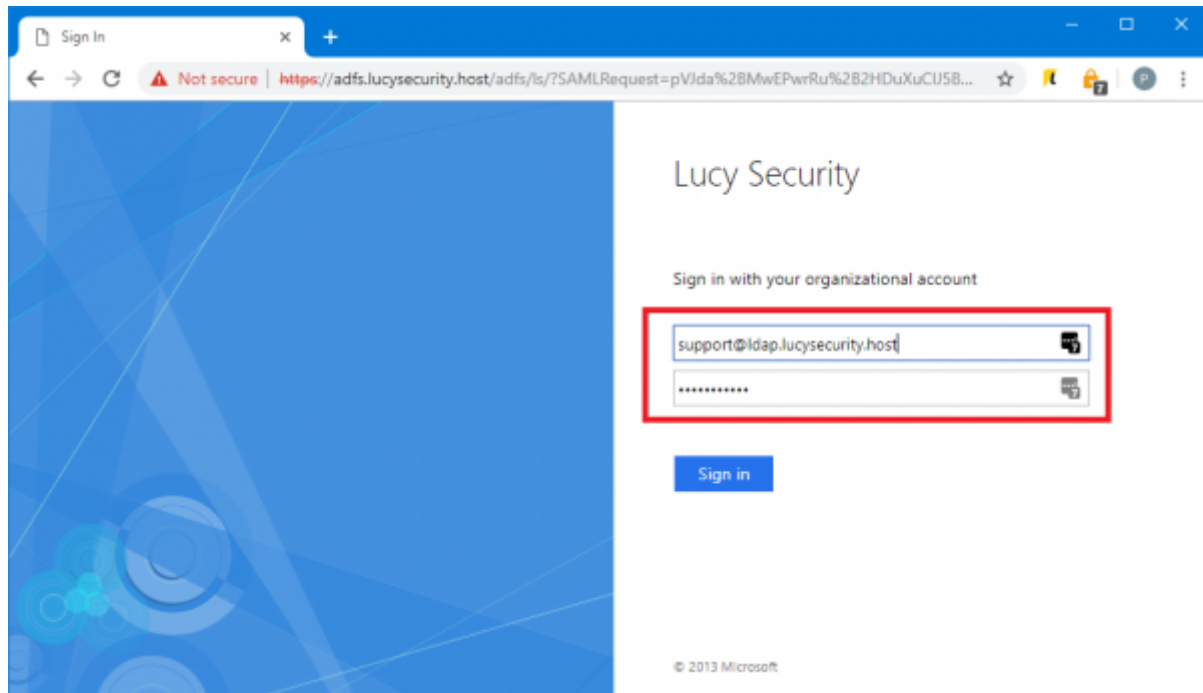
Testing Authentication


Now that we have configured Lucy as the service provider, ADFS as the identity provider (IdP), exchanged metadata between the two and configured some basic claims rules. We are now able to test authentication.

- Navigate to the **SSO Configuration** page in Lucy Admin console and click the button **Test Connection**:

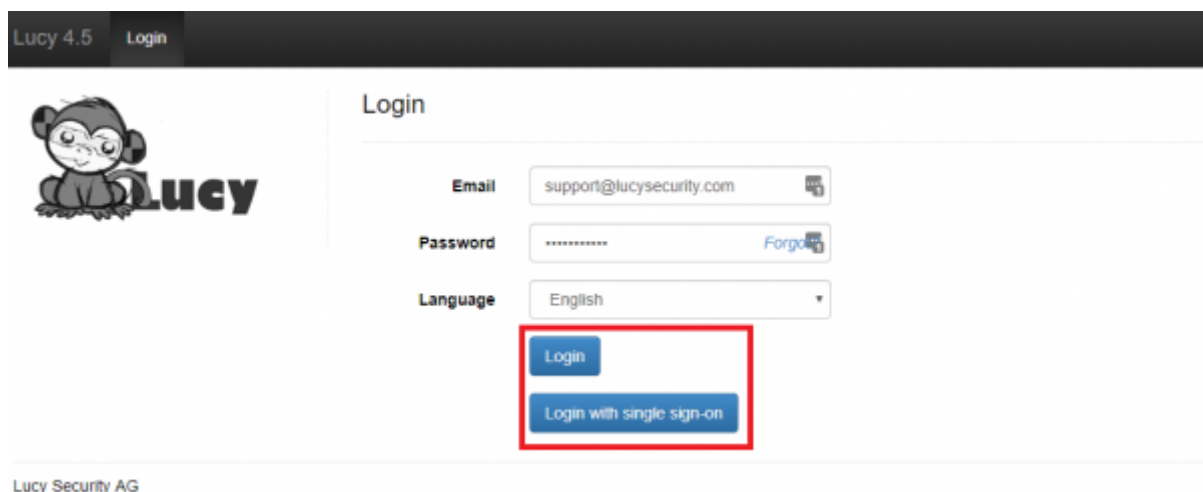


- You will be immediately forwarded to the AD FS server (or Web Application Proxy depending on how your AD FS farm is configured). Enter your user ID in the format "domain\user" or "user@domain":



Note  User ID may differ from the E-mail address specified in the Active Directory attributes. If this is the case, you can enable [Alternate Login ID](#). Microsoft strongly recommends using the mail attribute for sign in.

- Once signed in, you will be bounced back to Lucy Admin console. If an error occurs, double-check everything and then check the Event Viewer for hints as to what could have gone wrong.
- Click Logout to test this works as expected. On the Login page you can now choose a way of login to the Admin console:



Enable SSO for Awareness Websites

This option allows you to obtain a static link of the awareness website. This can be useful in the case when you do not need to send e-mail messages to each user, and to distribute only one link through other sources. The link is unique in the context of a specific awareness scenario and campaign.



The list of possible domains for the awareness web site is limited to those domains that you added to the [Relying Party Trust](#) in AD FS. You can add as many domains as you need by simply replacing the domain name in the Lucy Metadata Endpoint link.

The option **SSO for Awareness Websites** is available in the **Base Settings** section of campaign:

The screenshot shows the 'Configuration' page with a sidebar on the left containing 'Configuration', 'Advanced Settings', and 'Logs'. Under 'Configuration', 'Base Settings' is selected. The main area shows various settings: 'Enduser Profiles Enabled' (checked), 'User Profile Page Link' (set to 'LUCY UI Domain'), 'Enduser Direct Login' (unchecked), 'Track Responses' (unchecked), 'Email Tracking' (unchecked), 'Antivirus/Firewall Protection Interval' (set to 'off'), 'Allow Awareness Rescheduling' (unchecked), 'Ignore repeated answers in awareness' (unchecked), 'Stop the Campaign Automatically' (unchecked), 'After I stop the campaign, send me a report to support@lucysecurity.com' (unchecked), 'Pinned' (unchecked), 'Delete Protection' (unchecked), and 'Enable SSO for Awareness Websites' (checked and highlighted with a red box). A red arrow points down to this checkbox. A 'Save' button is at the bottom.

The option can be used in conjunction with the option "**Do not send emails**" ([Awareness Settings](#)) that blocking the sending of e-mail messages to users:

Home / Campaigns / PHISH-4247 (awareness only) / Awareness Settings / Avoid & Recognize Phishing Attacks

Avoid & Rec...

Campaign Status Running

Base Settings

Website

SSL Settings

Message

Mail Settings

Name

Avoid & Recognize Phishing Attacks

Risk Level

0

☒ Website Enabled

☐ Create Awareness Training Diploma

☒ Do not send emails

Languages

Dutch

English

+ Add

Page Views

1

Save

The global link that can be used by users to access awareness website is placed under the **Website** section of the Awareness Settings:

Home / Campaigns / PHISH-4247 #3 / Awareness Settings / Internet Security Exam 1.2 / Website

Internet Sec...

Campaign Status Not Started

Export to SCORM

Upload Webpage

Base Settings

Website

SSL Settings

Message

Mail Settings

Domain

access.cloudserver763.com

☒ Quiz

Preview link

https://access.cloudserver763.com/awareness/37f6c979613315eb957b6be2530cdc9bab5731ee546c686f150b7b28f3ee6530/11/index.html

Global link

https://access.cloudserver763.com/awareness/37f6c979613315eb957b6be2530cdc9bab5731ee546c686f150b7b28f3ee6530

Language

English

File


index.html

Content


Note In order this feature to work you should also enable SSL for the domain used in the awareness scenario:


Home / Campaigns / PHISH-4247 #2 / Awareness List / Comprehensive security course / SSL Settings

SSL Settings


Campaign Status Running 

[Base Settings](#)
[Website](#)
[SSL Settings](#)
[Message](#)
[Mail Settings](#)

☒ Use Custom SSL Certificate 

SSL Provider Let's Encrypt 

☒ Enable Domain Checking

Domain access.cloudserver763.com 
Let's Encrypt needs a publicly available domain name to generate a certificate. Please make sure your domain is accessible and points to Lucy.

Email

Useful tips

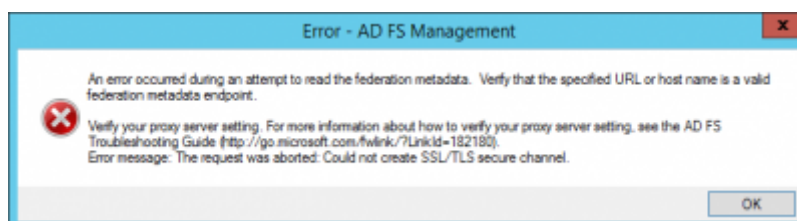
How to update or replace SSL certificate used for SSO authentication?

You should first update your SSL certificate within the SSL Settings. Refer to this [page](#) for detailed instructions.

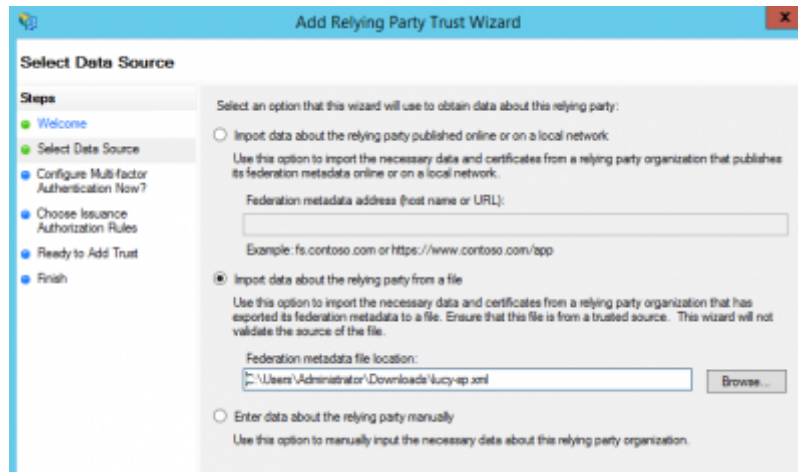
Once the SSL certificate is updated, go to the SSO Settings page, upload XML metadata file and click Save button. To verify whether the certificate is applied, click "Download Certificate" link, open the file and check certificate details.

Troubleshooting

Issue: An error occurs when importing a data about the relying party (Lucy Metadata Endpoint URL):



Solution: Copy the URL of Lucy Metadata Endpoint from the SSO Configuration page and paste into the address bar in your browser. Rename the downloaded file to "lucy-sp.xml". Use the file to import the data about relying party:



Issue: A blank page is opened after successful login with a single sign-on.

Solution: The time difference between AD FS and Lucy servers can cause an authentication problem. Make sure that the time zone setting is correct on the Advanced Settings page in Lucy.

Issue: (AD FS) Login with a single sign-on sometimes does not work (it redirects to the Lucy's login page after successful login at AD FS website) .

Solution: Disable the revocation check on your AD FS server by the PowerShell command (see details [here](#)):

```
Set-AdfsRelyingPartyTrust -TargetName "Your RelyingParty Name" -  
SigningCertificateRevocationCheck None
```

Issue: (AD FS) Login with a single sign-on stopped working after update to Lucy 4.7 (it redirects to the Lucy's login page after successful login at AD FS website) .

Solution: Update the Relying Party Trust on your Windows Server by clicking "Update from Federation Metadata..." link in AD FS Management console or through the [PowerShell](#).

Issue: A blank window appears after successful authentication at SSO provider website and there an error in the web server logs (Apache): "Uncaught exception 'SimpleSAML\\Error\\Error' with message 'ACSPARAMS'".

Solution: Verify your SSO provider settings, make sure that all required attributes are passed to Lucy during Single sign-on authentication.

From:
<https://wiki.lucysecurity.com/> - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=sso_authentication

Last update: **2021/03/16 14:36**

