

Single sign-on authentication (SSO)

Background Info



This feature is available in Lucy 4.6 or newer version.

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:

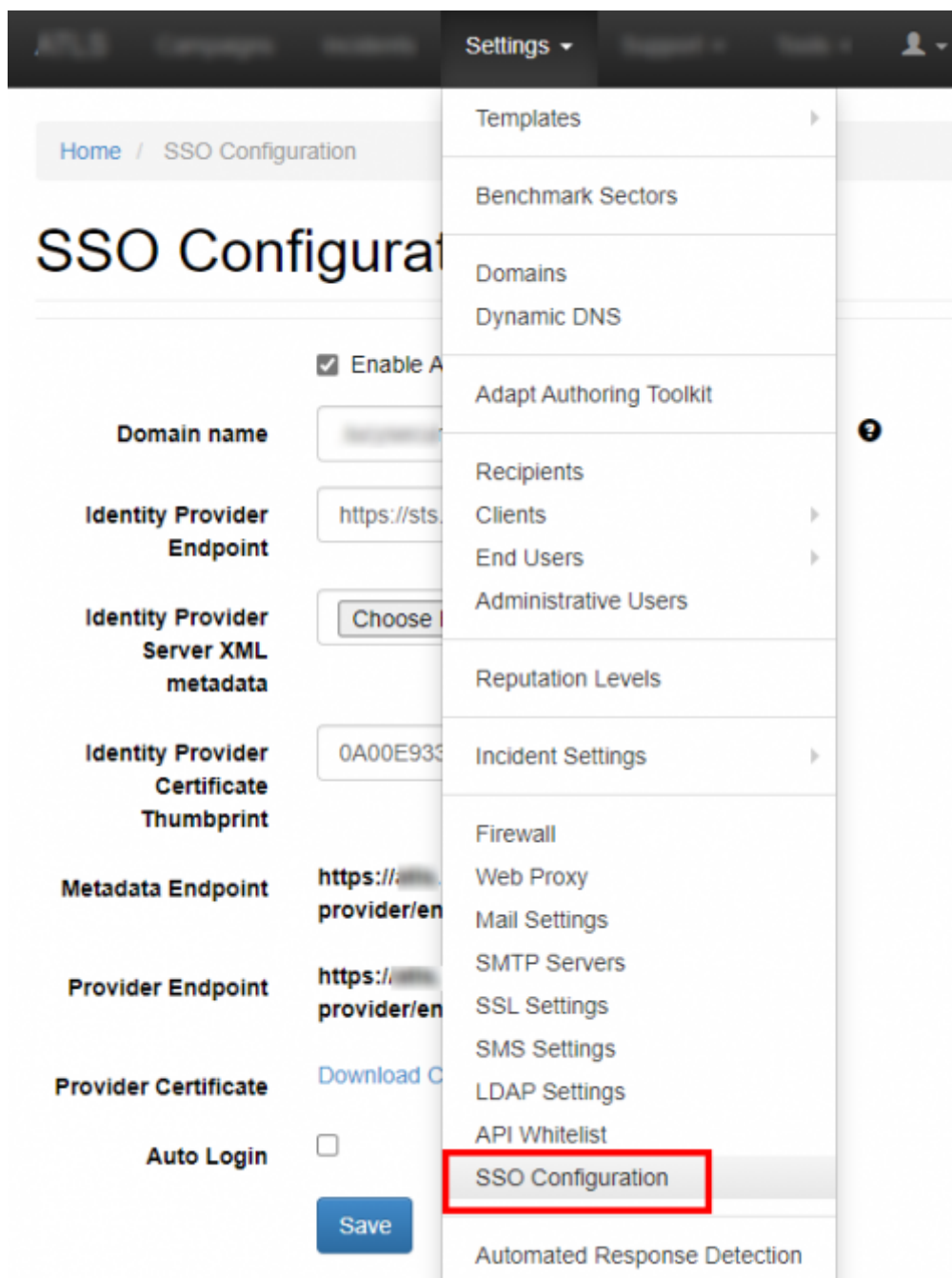
- authorization on Lucy's admin console and End-User portal:
- to identify users on awareness website.

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)

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:

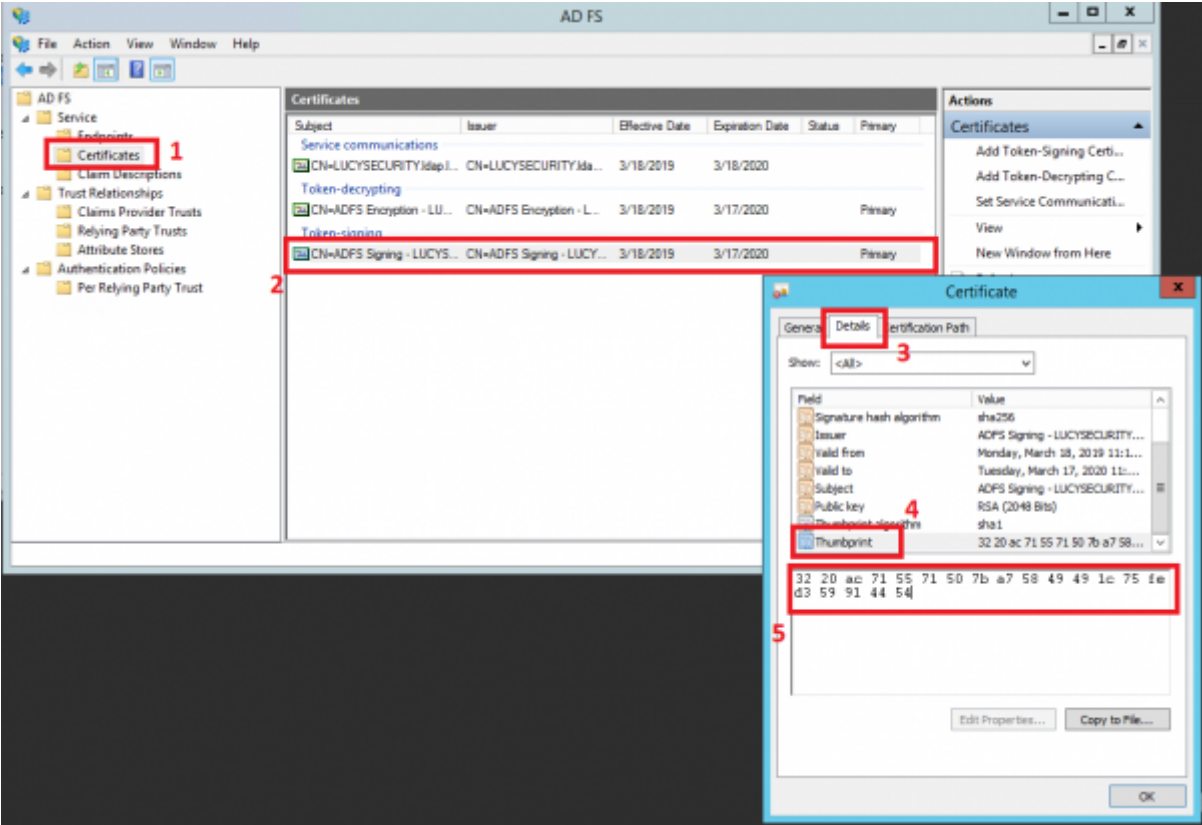
Telephone number: Other...

E-mail:

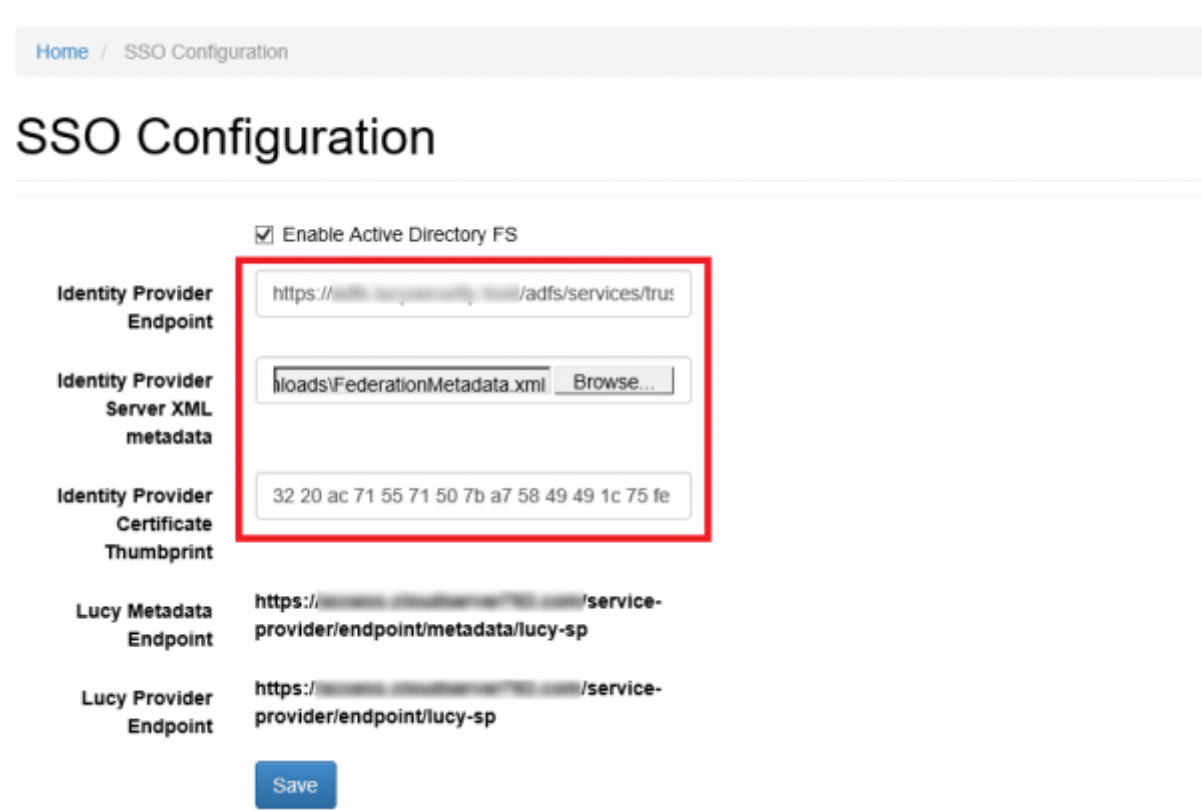
Web page: Other...

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:



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:

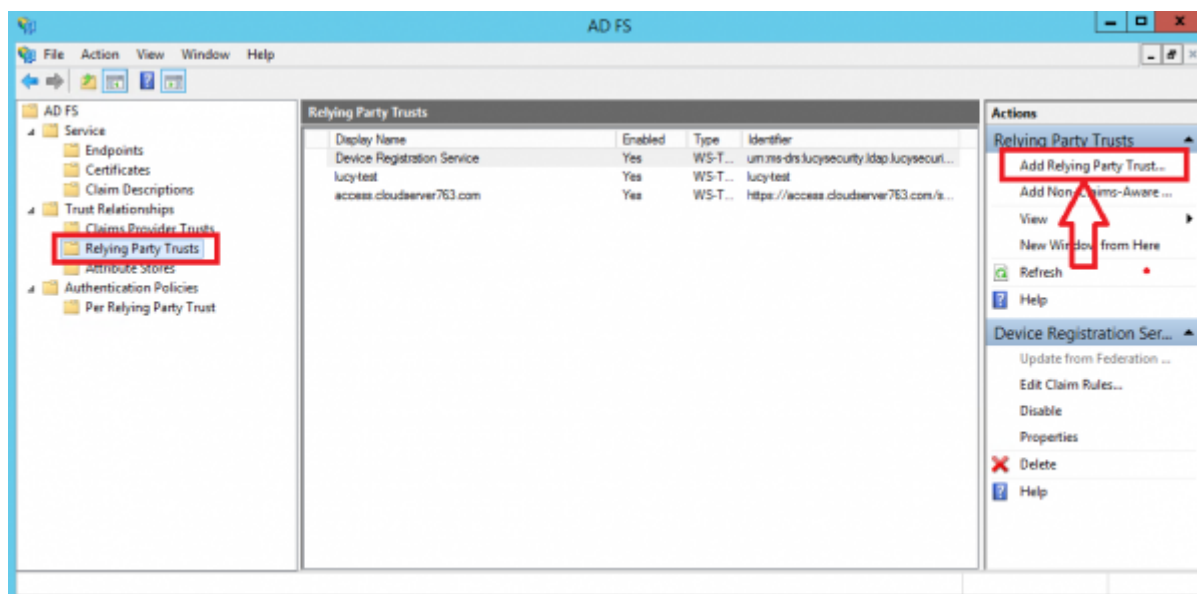
Identity Provider Certificate Thumbprint:

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**:



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

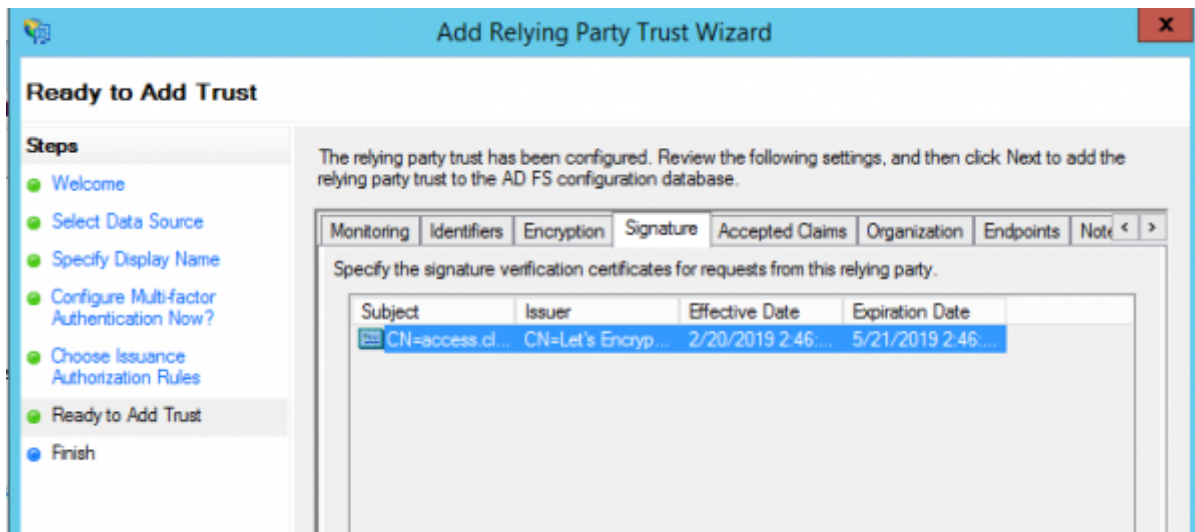
Next.

The screenshot shows the 'Add Relying Party Trust Wizard' window. On the left, a 'Steps' pane lists: Welcome, Select Data Source (current), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Select Data Source' and contains the instruction: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' (selected). Description: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' Input field: 'Federation metadata address (host name or URL):' with the value 'https://access.cloudserver763.com/service-provider/endpoint/metadata/lucy-sp'. Example text below: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Description: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' Input field: 'Federation metadata file location:' with a 'Browse...' button. 3. 'Enter data about the relying party manually'. Description: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right are buttons: '< Previous', 'Next >', and 'Cancel'.

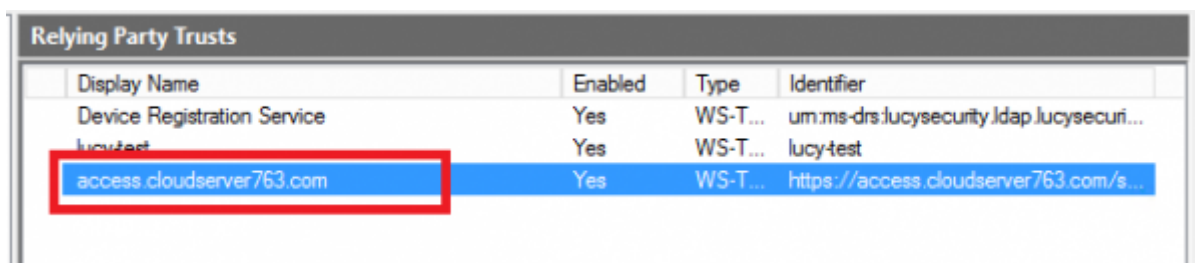
- Accept the warning:

The screenshot shows a warning dialog box titled 'AD FS Management'. It contains a yellow warning icon and the text: 'Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.' There is an 'OK' button at the bottom right. In the background, the 'Add Relying Party Trust Wizard' is visible, showing the 'Ready to Add Trust' step.

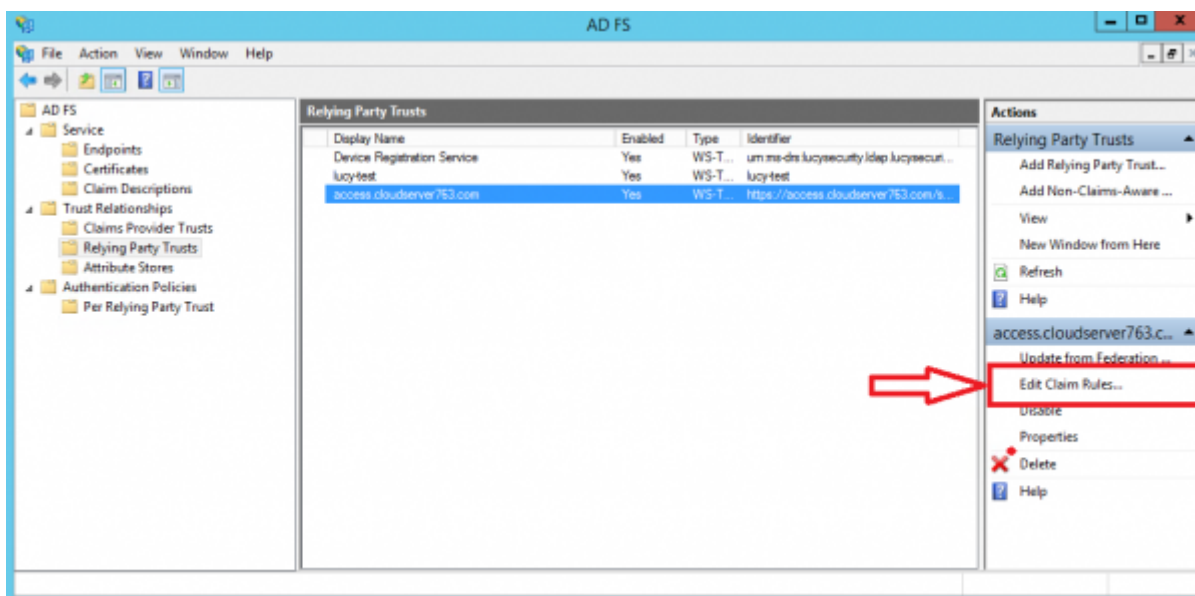
- Click the **Next** button in the wizard until you reach the Ready To Add Trust page. Check the Encryption and Signature tabs have certificates associated with them:



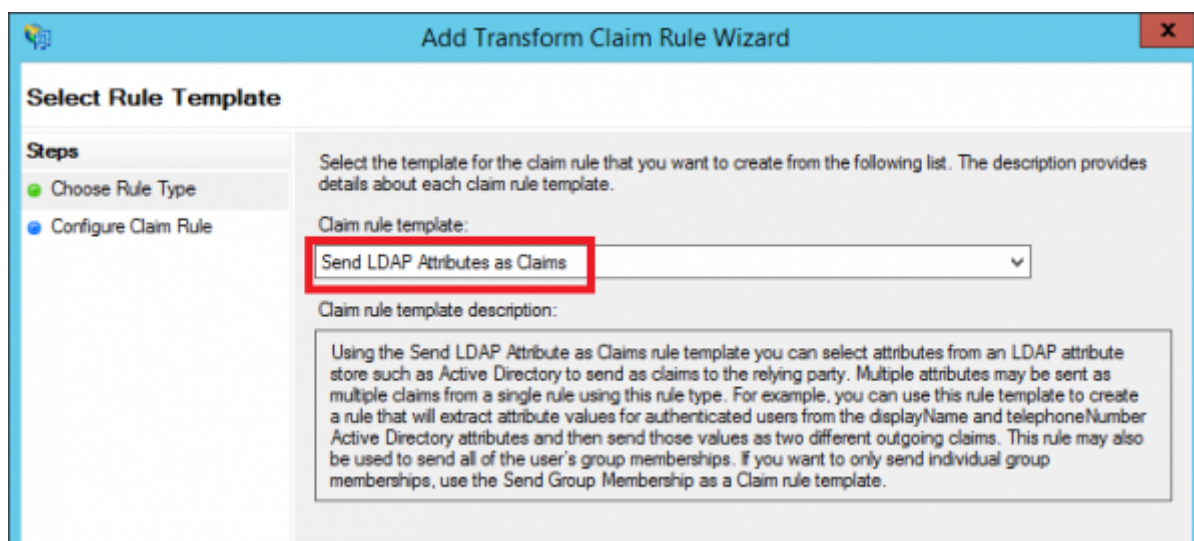
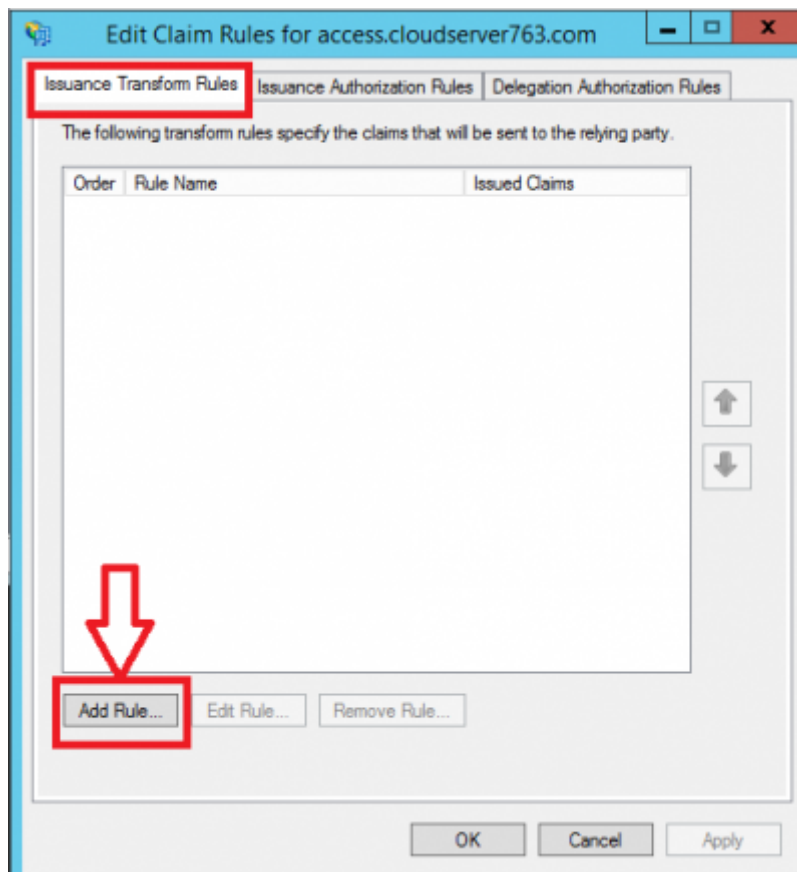
- Click **Next** and the Relying Party Trust is added:



- 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 Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: UPN

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	UPN
SAM-Account-Name	uid
E-Mail-Addresses	mail
*	

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

Add Transform Claim Rule Wizard

Select Rule Template

Steps

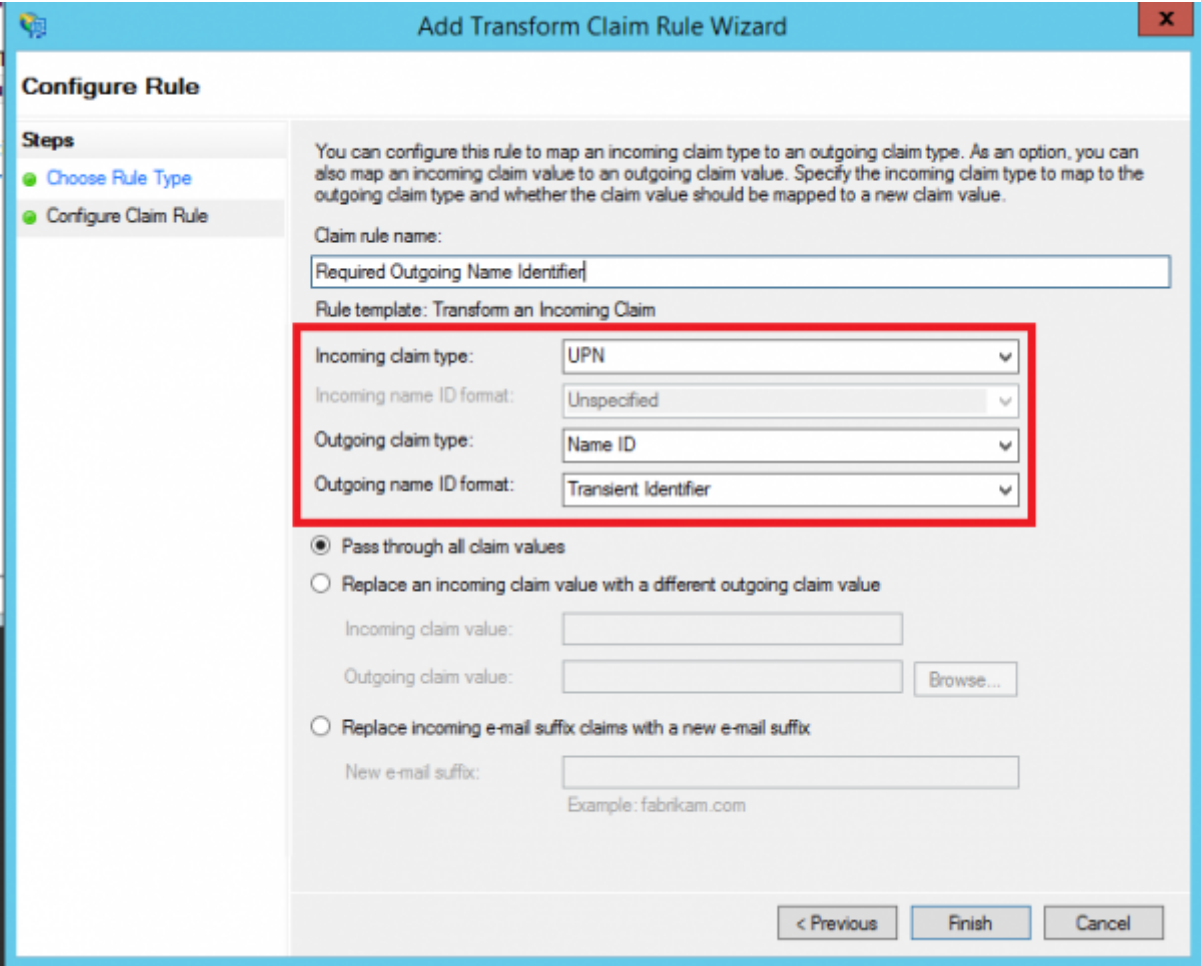
- Choose Rule Type
- Configure Claim Rule

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.

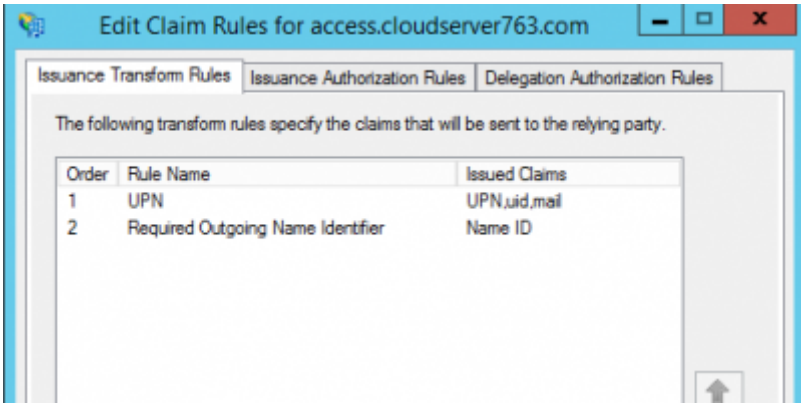
Claim rule template: Transform an Incoming Claim

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.



- 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**:

Home / SSO Configuration

SSO Configuration

☒ Enable Active Directory FS

Identity Provider Endpoint:

Identity Provider Server XML metadata:

Identity Provider Certificate:

- 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":


Sign In

Not secure | https://adfs.lucysecurity.host/adfs/ls/?SAMLRequest=pVJda%2BMwEPwrRu%2B2HDuXuCU5B...

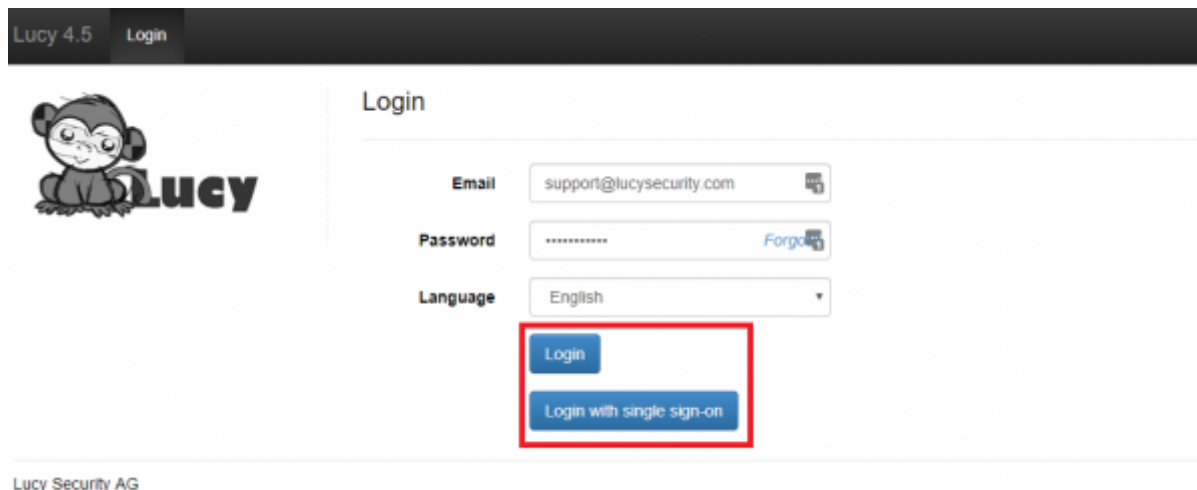
Lucy Security

Sign in with your organizational account

© 2013 Microsoft

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 recommend 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:



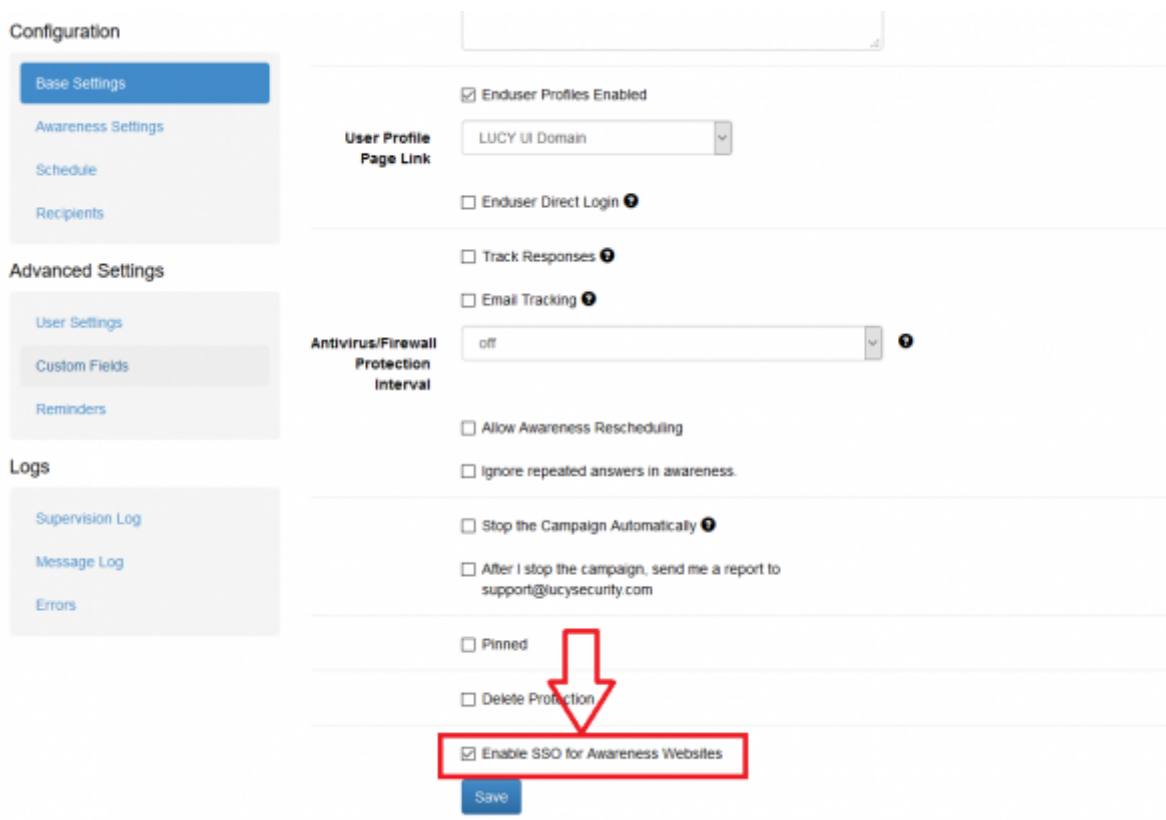
Enable SSO for Awareness Websites

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 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...


Base Settings

Website

SSL Settings

Message


Mail Settings

Campaign Status Running 


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 / PHSH-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

Source

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 ✓

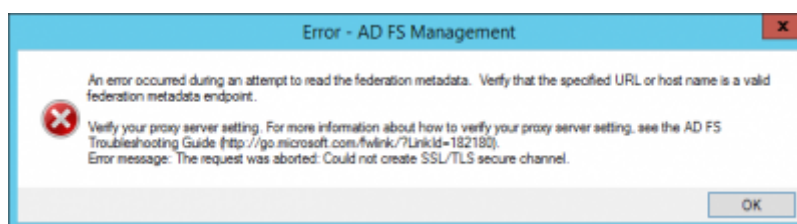
Email:

Save

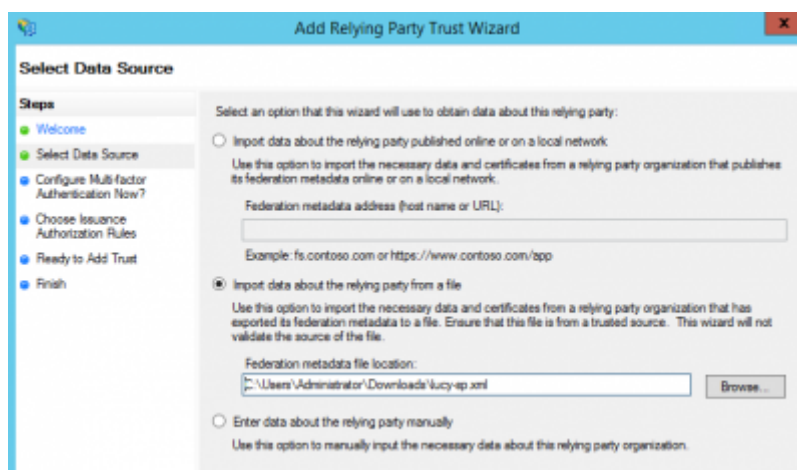
Let's Encrypt needs a publicly available domain name to generate a certificate. Please make sure your domain is accessible and points to Lucy.

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.

From:

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

Permanent link:

https://wiki.lucysecurity.com/doku.php?id=sso_authentication&rev=1559199436

Last update: **2019/07/25 12:51**

