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:

ATLS Company		Settings -
Home / SSO Configu	iration	Templates
		Benchmark Sectors
SSO Cont	figurat	Domains Dynamic DNS
	Enable A	Adapt Authoring Toolkit
Domain name		Recipients
Identity Provider Endpoint	https://sts.	Clients
Identity Provider	Choose I	Administrative Users
Server XML metadata		Reputation Levels
Identity Provider Certificate	0A00E933	Incident Settings
Thumbprint		Firewall
Metadata Endpoint	https://	Web Proxy
	provider/en	Mail Settings
Provider Endpoint	https://	SMTP Servers
	provider/en	SSL Settings
Brouider Cartificate	Download C	SMS Settings
Provider Certificate		LDAP Settings
Auto Login		API Whitelist SSO Configuration
	Save	Automated Response Detection

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 - Ed	it User	
Email	support@lucysecurity.com	
Country Code	Please select •	
Phone		
	Two-Factor Authentication is not configured.	
Name		

		Support	Proper	ties		?	×
Security	En	vironment	Sessi	ions	R	emote co	ontrol
Remote Des	ktop Se	rvices Profile	0	DM+	A	ttribute E	Editor
Published Certifi	cates	Member Of	Password	d Replicat	tion	Dial-in	Object
General Ad	dress	Account	Profile	Teleph	ones	Orga	nization
👗 Su	pport						
First name:		Support		Initial	s:		
Last name:							
Display name:		Support					
Description:							
Offi <u>c</u> e:							
Telephone nur	nber:] [<u>O</u> ther	
E- <u>m</u> ail:		support@lucys	security.co	m			
Web page:						Other	

Download the <u>FederationMetadata.xml</u> 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:

			AD FS				
File Action View Window Help							
🔿 🖄 📰 📓 📰							
AD FS	Endpoints						
Service Endpoints	Enabled	Proxy Enabled	URL Path	Туре	Authentication Type	Security Mode	
Certificates	No	No	/adfs/services/trust/13/asuedtokensymmetricitipledes	WS-Trust 1.3	SAML Token (Sym	Message	
Claim Descriptions	No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha	WS-Trust 1.3	SAML Token (Sym	Message	
Trust Relationships	No	No	/adfs/services/trust/13/asuedtokennixedaymmetrictripledes	WS-Trust 1.3	SAML Token (Sym	Mored	
Claims Provider Trusts	No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripled	WS-Trust 1.3	SAML Token (Sym	Mored	
Relying Party Trusts	No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows	Message	
Attribute Stores	No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mored	
Authentication Policies	No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport	
Per Relying Party Trust	Yes	No	/adfs/services/trustcp/windows	WS-Trust 2005	Local Windows	Message	
Per neying rany must	No	No	/adfs/services/trust/attfactresolution	SAML-AttfactResolution	Anonymous	Transport	
	Yes	Yes	/adfs/cauth2/	OAuth	Anonymous	Transport	
	Metadata						
	Yes	Yes	/adla/services/tost/mex	WS-MEX	Accorners	Transport	_
	Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Агопутоца	Transport	1
	100	140		NOTO 1.0 PRODUCE	The proof	Transport.	
	Proxy						
	Yes	No	/adfs/prox/	Web Application Proxy	Proxy Trust Certificate	Transport	
	Yes	No	/adfs/proxy/EstablishTrust/	Web Application Proxy	Password	Transport	
	Other						
		No	the state of the s	HTTP			
	No	red	/adfs/portal/updatepassword/	nur.	Anonymous	Transport	

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

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

• Open a browser and navigate to the <u>FederationMetadata.xml</u> 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 <u>FederationMetadata.xml</u> file we downloaded earlier:



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

The <u>Certificate Thumbprint</u> 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 "<u>Token-signing</u>" section:

9	AD FS	_ D X
Si File Action View Window Help		_ <i>a</i> ×
AD FS	Certificates Subject Issuer Effective Date Expiration	Actions Date Status Primary Certificates
Clam Descriptions Clam Descriptions Clam Descriptions Claim Strovider Trusts Relying Party Trusts	Subject Issuer Effective Date Expiration Service communications CN-LUCYSECURITYIda 3/18/2019 3/18/2020 Token-decrypting CN-ADFS Encryption - LL CN-ADFS Encryption - L 3/18/2019 3/17/2020 Token-signing	Add Token-Signing Certi Add Token-Decrypting C Set Service Computing L.
Attribute Stores	CN+ADFS Signing - LUCYS CN+ADFS Signing - LUCY 3/18/2019 3/17/2020	D Primary New Window from Here
		Genera Detxils ertification Path Sheric call> v Pield Value n Signature hash algorithm drb256 n Pield Value n Pield Value n Pield Value n Pield Value n Pield Monday, March 18, 2029 11:1 E Viald b Tuesday, March 18, 2029 11:1 E Public key 4 R54 (2048 Btb) E Public key 4 R54 (2048 Btb) r Public key 4 R54 (2048 Btb) r Public key 4 S54 190 7b a7 58 49 49 1c 75 fe 20 ac 71 55 71 50 7b a7 58 49 49 1c 75 fe d d 21 20 ac 71 55 71 50 7b a7 58 49 49 1c 75 fe d d 22 0 ac 71 55 71 50 7b a7 58 49 49 1c 75 fe d d 21 20 ac 71 55 71 50 7b a7 58 49 49 1c 75 fe d d 22 20 ac 71 55 71 50 7b a7 58 49 49 1c 75 fe d d 23 59 91 44 50 Capy to Place d d 24 50 Fropertes <td< td=""></td<>
		OK

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

Home / SSO Config	uration	
SSO Con	figuration	
	Enable Active Directory FS	
Identity Provider Endpoint	https:// /adfs/services/trus	
Identity Provider Server XML metadata	Noads\FederationMetadata.xml Browse	
Identity Provider Certificate Thumbprint	32 20 ac 71 55 71 50 7b a7 58 49 49 1c 75 fe	
Lucy Metadata Endpoint	https:// /service- provider/endpoint/metadata/lucy-sp	
Lucy Provider Endpoint	https:///service- provider/endpoint/lucy-sp	
	Save	

• Click Save.

Create the Relying Party Trust in AD FS

• Copy the Lucy Metadata Endpoint link arom the SSO Configuration page:

Home / SSO Configu	ration	
SSO Cont	figuration	
	Directory FS	
Identity Provider Endpoint	https:///adfs/services/trus	
Identity Provider Server XML metadata	Browse	
Identity Provider Certificate Thumbprint	32 20 ac 71 55 71 50 7b a7 58 49 49 1c 75 fe	
Lucy Metadata Endpoint	https:// service- provider/endpoint/metadata/lucy-sp	
Lucy Provider Endpoint	https:////service- provider/endpoint/lucy-sp	
Lucy Provider Certificate	Download Certificate	
	Save	

 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:

AD FS	Relying Party Trusts				Actions
Service Endpoints Certificates Claim Descriptions Claims Provider Trusts Claims Provider Trusts Actinotic Stores Authentication Policies Per Relying Party Trust	Display Name Device Registration Service Jucy-test access:cloudserver763.com	Enabled Yes Yes Yes	WS-T	Identifier um me dis Augiseounty Idap Augiseount Augistest https://woccess.cloudserver763.com/s	Relving Party Trusts Add Relying Party Trust Add Non Chimo-Aware View New Window from Here Refresh Help Device Registration Ser Update from Federation Edit Claim Rules Disable Properties Delete Help

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

7/15

Next.

\$	Add Relying Party Trust Wizard
Select Data Source	
Steps	Select an option that this wizard will use to obtain data about this relying party:
Welcome	Import data about the relying party published online or on a local network
Select Data Source	Use this option to import the necessary data and certificates from a relying party organization that publishes
 Configure Multi-factor Authentication Now? 	its federation metadata online or on a local network.
 Choose Issuance Authorization Rules 	Federation metadata address (host name or URL): https://access.cloudserver763.com/service-provider/endpoint/metadata/lucy-sp
Ready to Add Trust	Example: ts.contoso.com or https://www.contoso.com/app
Finish	Import data about the relying party from a file 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. Federation metadata file location: Browse Enter data about the relying party manually Browse Use this option to manually input the necessary data about this relying party organization. Cancel

• Accept the warning:

Authonization Hules	парали молоалогичаниты и чалопти англосуюттани и пропагатониции посу ар	
Beady to Add Trust	Example: fs.contoso.com or https://www.contoso.com/app	
	AD FS Management	×
	in the federation metadata was skipped because it is not supported by AD FS. Review the propertie before you save the trust to the AD FS configuration database.	s
	ок	
(Enter data about the relying party manually	

• 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:

Ready to Add Trust									
Steps	The relying r	party trust has	s been config	ured Revie	w the following sett	ings, and then d	lick Next to	add the	
Welcome			D FS configu						
Select Data Source	Monitoring	Identifiers	Encryption	Signature	Accepted Claims	Organization	Endpoints	Note <	>
Specify Display Name	Specify the	e signature v		tificates for r	requests from this re	lying party.			
Configure Multi-factor Authentication Now?	Subject	t	Issuer	Đ	fective Date	Expiration Date			1
 Choose Issuance Authorization Rules 	E CN	=access.cl	CN=Let's E	ncryp 2/	/20/2019 2:46:	5/21/2019 2:46			
Ready to Add Trust									

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

Device Registration Service	Yes	WS-T	um:ms-drs:lucysecurity.ldap.lucysecuri
unviet	Yes	WS-T	lucy-test
access.cloudserver763.com	Yes	WS-T	https://access.cloudserver763.com/s

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

• 1	A	AD FS	_ D X
State Action View Window Help			_ # ×
🕈 🏟 🖄 📰 📓 🗊			
AD FS	Relying Party Trusts		Actions
⊿ ≝ Service ≣ Endpoints	Display Name	Enabled Type Identifier	Relying Party Trusts
Certificates	Device Registration Service lucy-test	Yes WS-T um ms-dm lucysecunty idep lucysecunt. Yes WS-T lucytest	Add Relying Party Trust
Claim Descriptions	access cloudserver753.com	Yes WS-T https://access.cloudserver753.com/s.	Add Non-Claims-Aware
Trust Relationships Claims Provider Trusts			View 🕨
Relying Party Trusts			New Window from Here
Attribute Stores			Refresh
A Authentication Policies Per Relying Party Trust			🛛 Help
			access.cloudserver763.c +
			Update from Federation
			Edit Claim Rules
		-	Uisable
			Properties
			🗶 Delete
			Help
	1		

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

💱 👘 Edit Claim Rules for access.clou	dserver763.com 🗕 🗆 🗙
Issuance Transform Rules Issuance Authorization I	Rules Delegation Authorization Rules
The following transform rules specify the claims that	t will be sent to the relying party.
Order Rule Name	Issued Claims
	1
	+
JL	
V	
Add Rule Edit Rule Remove Rule	
	OK Cancel Apply

\$ 1	Add Transform Claim Rule Wizard	
Select Rule Template		
Steps Ghoose Rule Type	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.	
Configure Claim Rule	Claim rule template: Send LDAP Attributes as Claims	
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	

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

Q		Add Transform Cla	im Rule	Wizard		X
Configure Rule						
Steps	You c	an configure this rule to send the	values of L	DAP attributes as	s claims. Select an attribute store from	
Choose Rule Type		to extract LDAP attributes. Speci from the rule.	fy how the	attributes will may	p to the outgoing claim types that will be	*
Configure Claim Rule	Claim	rule name:				
	UPN					
	Rule t	emplate: Send LDAP Attributes a	s Claims			
		Attribute store:				
		e Directory		*		
	-					
	Марр	ing of LDAP attributes to outgoing		s:		_
		LDAP Attribute (Select or type	to	Outgoing Claim	Type (Select or type to add more)	
		User-Principal-Name	Ý	UPN		¥
		SAM-Account-Name	Ý	uid		¥
	•	E-Mail-Addresses	Ý	mail		×
	•		-			~

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

\$	Add Transform Claim Rule Wizard	x
Select Rule Template		
Steps	Select the template for the claim rule that you want to create from the following list. The description provides	
Choose Rule Type	details about each claim rule template.	
 Configure Claim Rule 	Claim rule template: Transform an Incoming Claim Claim rule template description: 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.	

2024/04/26	09:11
------------	-------

11/15

%	Add Transfo	orm 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: Incoming name ID format: Outgoing claim type: Outgoing name ID format:	UPN V Unspecified V Name ID V Transient Identifier V		
	Incoming claim value: Outgoing claim value:	es a value with a different outgoing claim value		

• 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 Co	onfiguration	
SSO Co	onfiguration	
	Enable Active Directory FS	Test Connection
Identity Provider Endpoint	https:// 'adfs/s	
identity Provider Server XML metadata	Browse	
Identity Provider Certificate	10.00 at 71.00.71.00.76.at 90.401	

 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 🗙 🕂	– 🗆 X
← → C ▲ Not secure https://adfs.lucysecurity.host/adfs/is/?SAMLR	equest=pVJda%28MwEPwrRu%282HDuXuCU58 🖈 🥂 🔓 ! 🕐 🚦
	Lucy Security
	Sign in with your organizational account
	support@ldap.lucysecurity.host
	Sign in
	© 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 enabled 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, doublecheck 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:

	Login			
Lucy	Email	support@lucysecurity.com	5	
-	Password		Forgo	
	Language	English	•	
		Login		
		Login with single sign-on		

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:

Configuration			4
Base Settings		Enduser Profiles Enabled	
Awareness Settings	User Profile	LUCY UI Domain ~	
Schedule	Page Link		
Recipients		Enduser Direct Login	
Advanced Settings		Track Responses	
User Settings		Email Tracking	
Custom Fields	Antivirus/Firewall Protection	off	~ O
Reminders	Interval		
		Allow Awareness Rescheduling	
Logs		Ignore repeated answers in awareness.	
Supervision Log		Stop the Campaign Automatically	
Message Log		After I stop the campaign, send me a report to support@(ucysecurity.com)	
Errors			
		Pinned	
		Delete Protection	
	[Enable SSO for Awareness Websites	
		Save	

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

Home / Campaigns / PHISH-4	247 (awareness only) / Aware	ness Settings / Avoid & Recognize Phisi	hing Attacks
void & Rec	Campaign Status R	unning	
Base Settings	Name	Avoid & Recognize Phishing Attacks	
Website	Risk Level	0	۲
SSL Settings		Website Enabled	
Message		Create Awareness Training Diploma	0
Mail Settings		☑ Do not send emails	
	Languages	Dutch	×
		si 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 <u>Awareness Settings</u>:

Home / Campaigns / PHSH-4247 #3	/ Awareness Settings	/ Internet Security Exam 1.2 / Website		
Internet Sec	Campaign Status Not :	Started	A Export to SCORM	O Upload Webpage
Base Settings	Domain	access.cloudserver763.com	θ	
Website		🖂 Quiz 😡		
SSL Settings	Preview link	https://access.cloudserver763.com/awareness /3716c979613315eb957b6be2530cdc9bab5731ee54 /11/index.html	l6c686f150b7b28f3ee6530	
Mail Settings	Global link	https://access.cloudserver763.com/awareness /s/37/6c979613315eb957b6be2530cdc9bab5731ee	546c686f150b7b28f3ee6530	
Quick Tips	Language	English	v	
Awareness Website Variables Quiz Integration	File	index.html v	× O	
Create Custom Video	Content		B B ← → Q t3 ₩	₩-

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

		Comprehensive security course / SSL Settings	
SL Settings			
Base Settings Website	SSL Provider	Use Custom SSL Certificate	~ 9
SSL Settings		🗹 Enable Domain Checking	
Message	Domain	access.cloudserver763.com	~
Mail Settings		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	1	
		Save	

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

Permanent link: https://wiki.lucysecurity.com/doku.php?id=sso_authentication&rev=1555580597



Last update: 2019/07/25 12:50