# Enabling single sign-on authentication (SSO) for Azure Active Directory (Azure AD)

#### **Background Info**

This feature is available in Lucy 4.6 or newer version.

This article describes step by step instruction of the SSO integration with Azure AD. An additional information about what SSO in Lucy is designed for can be found here.

# What preparations need to be done before connecting to Azure AD?

- 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 account in Azure Active Directory. Both accounts must have the same email address:

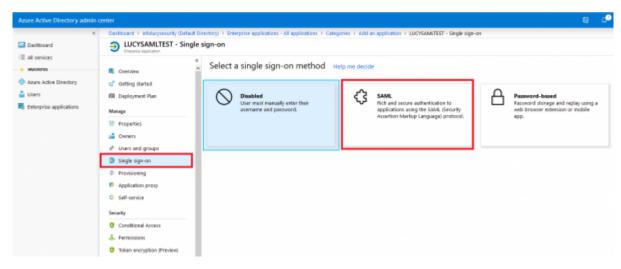
Home / Users / Lucy S	upport		
Lucy Suppo	ort		
Email	support@lucysecurity.company		
Country Code	Please select	•	
Phone			
	Two-Factor Authentication is not configured.		
Name	Lucy Support		
Role	Administrator	~	
	Enable incident reports notifier		
	Change Password		
Current Certificate	N/A C		
	Certificate Required		
	Save		

	Dephoard > infolucysecarity (Defealt Di	rentoryt > Users - All users			
Deskboard	Users - All users	ia Bieroy			
E All services		+ New user + New guest user 🌾 teampar	coveral 📋 Delete user 🕑 Multi-Ractor Authent	ication 👌 Refrech 🛛 👬 Columns	
ALL AND A	🛔 All users				
Azure Active Directory	Deleted users	Search Search attribut		4	
🏜 Users	Password reset	hanne	1000 0000	USER TYPE	100403
Enterprise applications	O Liter settings	usy Support	support@lucysecurity.company	Mamber	Azure Active Directo
	Activity				
	B Sign-ins				
	Audit loga				
	Troubleshooting + Support				

## **Enable Single sign-on in Lucy**

• Configure SAML-based single sign-on to your non-gallery application

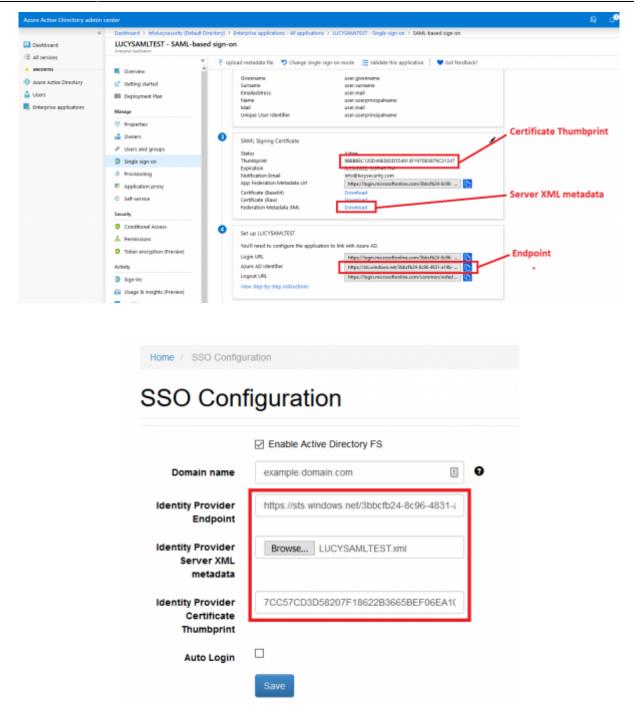
Find more about Azure AD Single Sign-on configuration here



• Add a new non-gallery web app to your Azure AD, see more here

Dashboard	Cashboard > infolucysecurity (Defail Categories		an application		\$		Add your own application
All services	conceptites		an appreasion		~		nea jour onn appreadon S
All services	All (1208)	Add 1	our own app			^	• Name o
Azure Active Directory	Business management (413)		Application you're	On-premises	Non-galary application		The display name for your new application
Users	Collaboration (465)		you're developing	application			Once you decide on a name for your new
Enterprise applications	Construction (7)		gister an app you're	Configure Azure AD Application Proxy to	integrate any other application that you		application, dick the "Add" button below and we'll walk you through some simple
	Consumer (44)		rking on to integrate ith Azure AD	enable secure remote access.	don't find in the gallery		configuration steps to get the application
	Content management (154)						working.
	CRM (156)	Add t	from the gallery				Supports: 0
	Data services (151)						SAML-based single sign-on Learn more
	Developer services (111)		Enter a name				Automatic User Provisioning with SCIM
	E-commerce (75)		Featured applications				Learn more
	Education (149)						Password-based single sign-on
	ERP (93)		box	C C			Learn more
	Finance (200						

- Open Lucy Admin console
- Navigate to the SSO Configuration page (Settings > SSO Settings)
- Tick the option "Enable Active Directory FS"
- Download the <u>FederationMetadata.xml</u> file from Azure AD and fill the <u>Identity Provider</u> Endpoint and <u>Certificate Thumbprint</u> in Lucy

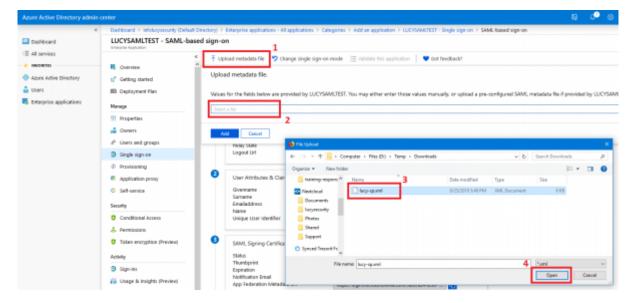


• Download a pre-configured SAML metadata file (copy the URL and paste into your web browser address bar, change the extension of the file to .XML, for example "lucy-sp.xml")

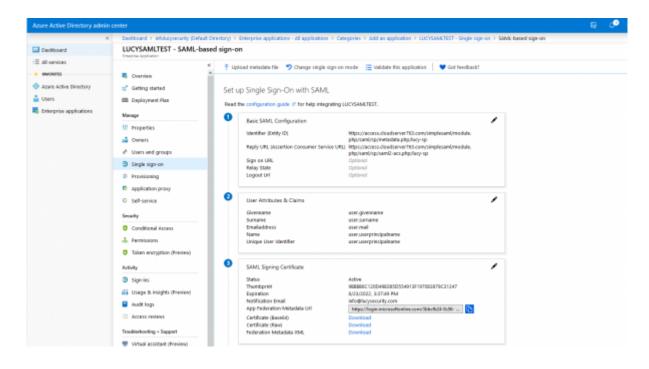
		Enable Active Directory FS		
	Domain name	example.domain.com	Θ	
Ide	entity Provider Endpoint	16ps 745 amilian 147703-0214-0214		
Ide	entity Provider Server XML metadata	Browse No file selected.		
Ide	entity Provider Certificate Thumbprint			
Meta	adata Endpoint	https://domain.com/service-provider /endpoint/metadata/lucy-sp		
Pro	vider Endpoint	https://domain.com/service-provider /endpoint/lucy-sp		
Provi	ider Certificate	Download Certificate		
	Auto Login			
		Save		

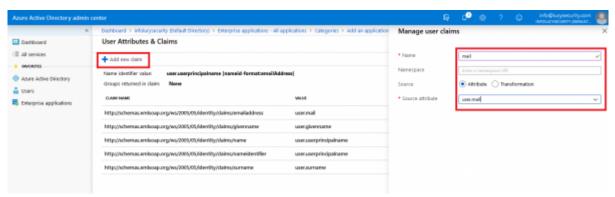


• Upload the pre-configured SAML metadata file



• Add a new Claim "mail" that contain an e-mail address of the user, see more here





**Note** The attribute <u>user.mail</u> is always empty if the user does not exist in your Office 365 Exchange server. Instead you will have to use the attribute <u>user.userprincipalname</u> or other one that contains user's email address.

• Configure Azure AD SAML token encryption, see more here

Home / SSO Config	uration	
SSO Con	figuration	
	Enable Active Directory FS	
Domain name	example.domain.com	0
Identity Provider Endpoint	16ga, 76b, amilion, 167700-7623-8236-8271 -	
Identity Provider Server XML metadata	Browse No file selected.	
Identity Provider Certificate Thumbprint	10070000007-000800796040	
Metadata Endpoint	https://domain.com/service-provider /endpoint/metadata/lucy-sp	
Provider Endpoint	https://domain.com/service-provider /endpoint/lucy-sp	
Provider Certificate	Download Certificate	
Auto Login		
	Save	

Azure Active Directory admi	center
	Deal-board > infolucysecurity (Default Directory) > Enterprise applications - All applications > LUCYSAMLTEST - Toban encryption (Preview)
Daskboard	1 LUCYSAMLTEST - Token encryption (Preview)
i≡ All services	Consister Application 2
Asure Active Directory     Asure Active Directory     Users     Bitterprise applications	
	Add Cancel Add Cancel Add Cancel Single Spr-on
	Provisioning
	Applications proxy     Digasize = New failer
	Image: Balinsights (Preview)     Image: Balinsights (Preview)     Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (Preview)     Image: Balinsights (Preview)       Image: Balinsights (P
	Toublehooling + Support           Toublehooling + Support         File name         UCT Providencet         5         All Supported           W trutal assistant (troview)         X         Toublehool         0ppm

Do not forget to activate the encryption for the uploaded certificate

1.

## **Testing Authentication**

• Make sure you have added users to your app

Azure Active Directory admi	in center							
	< Dashboard > infoliocysecurity ()	Delauit Di	rectory) > Enterpri	ise applications - All a	pplications > LUCYSAMETES	f - Users and groups		
E Dashboard	LUCYSAMLTEST - U	Users a	nd groups					
E All services		×	+ Add user	/ Edit - III Remot	ve 🎜 Update Credestials	EE Columns		
A INVOLUTIS	B Overview	^	· · · · · · · · · · · · · · · · · · ·			Set 'visible to users'' to no in properties to prevent		
Azure Active Directory	of Oetting started		<ul> <li>The application</li> </ul>	ation will appear on the	Access Panel for accigned users	set wable to users, to so in properties to prevent	8w. +	
🛓 Users	BB Deployment Plan		First 100 shown	n, to search off users (0, gr	roups, enter a display name.			
Enterprise applications	Manage					OISPLAY NAME	060627 7995	
	11 Properties					15 Lucy Support	User	
	🝰 Owners							
	x <sup>P</sup> Users and groups							
	Single sign-on	- 1						
	Provisioning							
	Application proxy							

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

Home / SSO Configu	ration		
SSO Cont	figuration		
	Enable Active Directory FS		Test Connection
Domain name	example.domain.com	0	
Identity Provider Endpoint	Mps. 108 and on, not 785-7824 (198-4021)		
Identity Provider Server XML metadata	Browse No file selected.		
Identity Provider Certificate Thumbprint	Record concerns the second resident		
Metadata Endpoint	https://domain.com/service-provider /endpoint/metadata/lucy-sp		
Provider Endpoint	https://domain.com/service-provider /endpoint/lucy-sp		
Provider Certificate	Download Certificate		
Auto Login			
	Save		

• You will be immediately forwarded to the Microsoft login page. Enter your username and password:

00-					- D X
LUCY - SSO Configuration		4831-a146-a744829c2517/ ×	umi25AMLRequests pill, pMwBP4kaSumkubsGorleOQRactoUDFd	12.86/gSPi7 - 🗑 🗘 Seatch	<i>₽</i> - <b>n</b> ★ Q €
A STATISTICS					
			-		
			Microsoft	Contraction of the	
			Sign in	- Section -	
			support@lucysecurity.company	*	
			Can't access your account?	Sall a hold	
			Sign-in options		
				and the second se	
			Back New	·	
				and the start	
CA MA					
SALA A		<b>这个人的</b>		NAL CREATE AND	ARUS FERRIA S
ALC: NOT STATE	1211年1月7月21月36日	O. L. SAR SAL	SHE DIK SHE A SHRUM		

 Once signed in, you will be bounced back to Lucy Admin console. If an error occurs, doublecheck everything and then check the Sign-ins page within the Activity section for hints as to what could have gone wrong.

4	Dashboard > infolucysecurity (Default Directory) > Enterprise applications - All applications > LUCYSAMCTEST - Sign-ins
Dashboard	LUCYSAMLTEST - Sign-ins
All services  Swoounts  Aure Active Directory  Users  Enterprise applications	Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started     Image: Control of the started     Image: Control of the started       Image: Control of the started     Image: Control of the started<
	Manage       8/23/2019. 4:33:55 PM       Lucy Support       LUCYSAMLTEST       Success         III Properties       8/23/2019. 4:28:38 PM       Lucy Support       LUCYSAMLTEST       Success       Image: Conditional Access         III Provisioning       Application proxy       Set-service       Image: Conditional Access       Image: Conditional Access       Image: Conditional Access       Image: Conditional Access       Image: Conditional Provision (Preview)         Activity       Sign-ins       Image: Conditional Provision (Preview)       Image: Condite Provision (Preview

 (optional) You may also configure a domain name that Azure AD will use to receive authentication requests. Azure supports both single domain and range of subdomains, however, for this you need to use a wildcard SSL certificate. By default, Lucy is configured to use system domain.

To enable support for the subdomains, set the value in the Domain field in the following way ".domain.com"

Home / SSO Configur	ration		
SO Conf	iguration		
	Enable Active Directory FS		
Domain name	.domain.com	ŧ	0
Identity Provider Endpoint	185ps. 1951. attrations. 1487 (2010) 75(1): 51-56. 40		
Identity Provider Server XML metadata	Browse No file selected.		

Using wildcard domain name will allow you to use different subdomains in your campaigns.

Please note, Azure AD does not support multiple second-level domains in a single application.

#### **Troubleshoot problems**

• I am redirected back to Lucy's login page after successful authorization through the Single singon.

If you are getting back to the login page, try checking the Claim rules (see the section Enable Single sign-on in Lucy, "Add a new Claim 'mail'..."). There must be a claim named "mail", with empty "Namespace" and Source attribute that contains user email address. For example:

🕂 Save 🗙 Discard	changes	
* Name	mail	
Namespace	Enter a namespace URI	
* Source	Attribute	
* Source attribute	user.userprincipalname	

