

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?

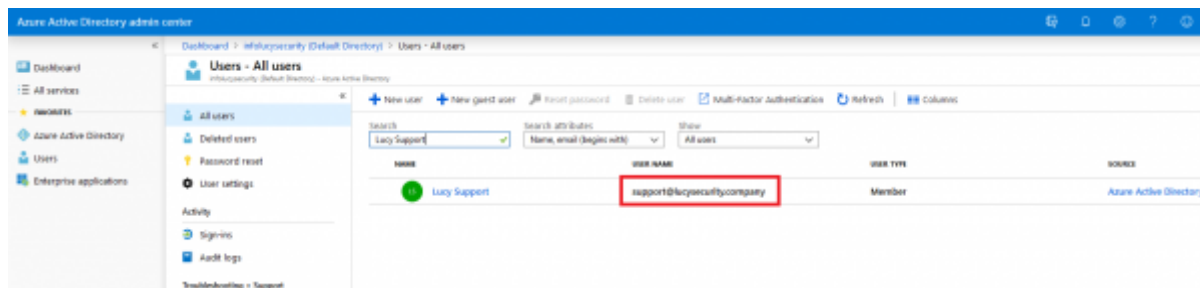
- Upload or create an SSL certificate for Lucy Admin console - see [this article](#).
- Make sure you have an Administrator account in Lucy (Settings > Users) with an email address that corresponds to your account in Azure Active Directory. Both accounts must have the same email address:

Home / Users / Lucy Support

Lucy Support

Email	<input type="text" value="support@lucysecurity.company"/>	
Country Code	<input type="text" value="Please select..."/>	
Phone	<input type="text"/>	
Two-Factor Authentication is not configured.		
Name	<input type="text" value="Lucy Support"/>	
Role	<input type="text" value="Administrator"/>	
<input type="checkbox"/> Enable incident reports notifier		
Change Password		

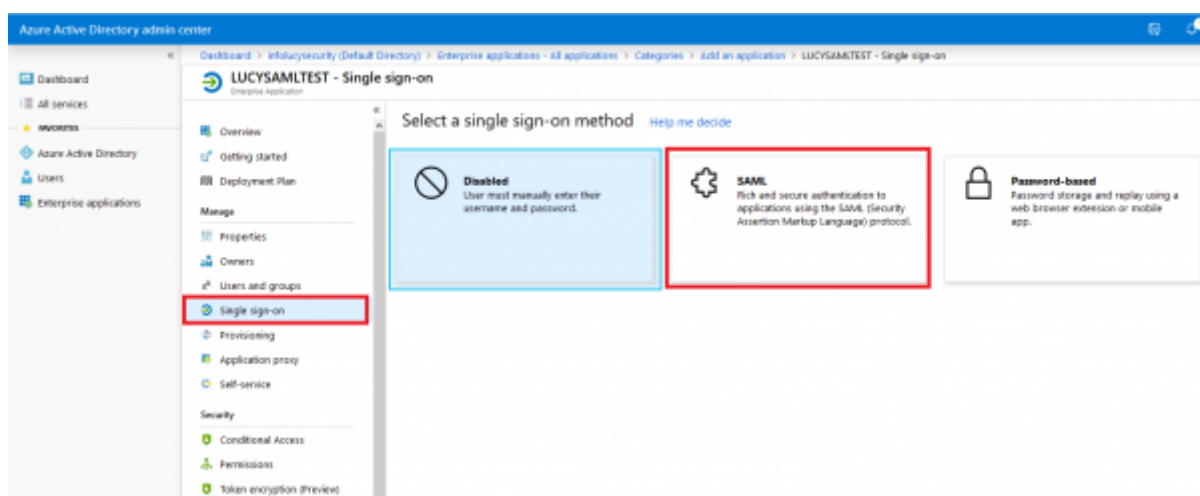
Current Certificate	N/A
<input type="checkbox"/> Certificate Required	



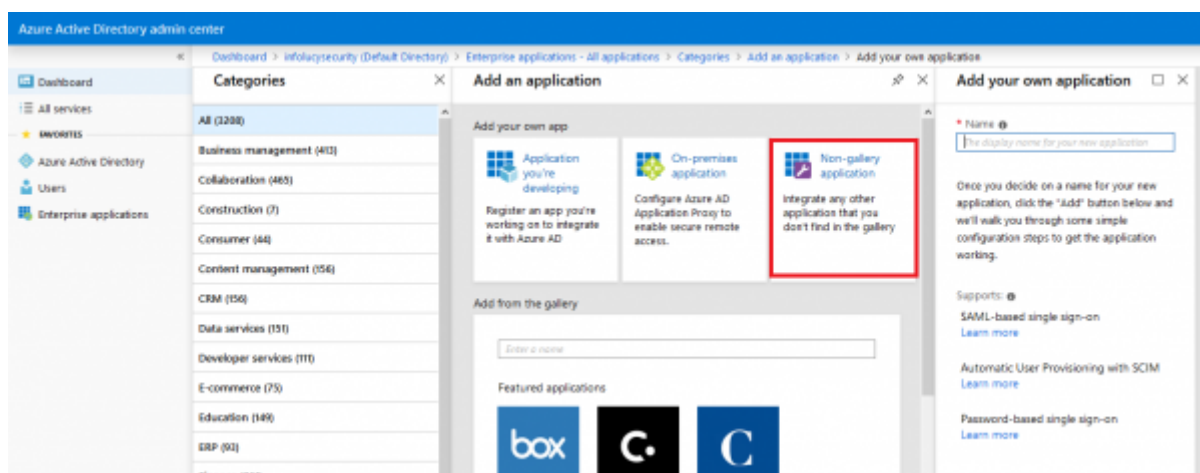
Enable Single sign-on in Lucy

- 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](#)




- Open Lucy Admin console
- Navigate to the **SSO Configuration** page (Settings > SSO Settings)
- Tick the option "**Enable Active Directory FS**"
- 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")

Home / SSO Configuration

SSO Configuration

☒ Enable Active Directory FS

Domain name 

Identity Provider Endpoint

Identity Provider Server XML metadata No file selected.

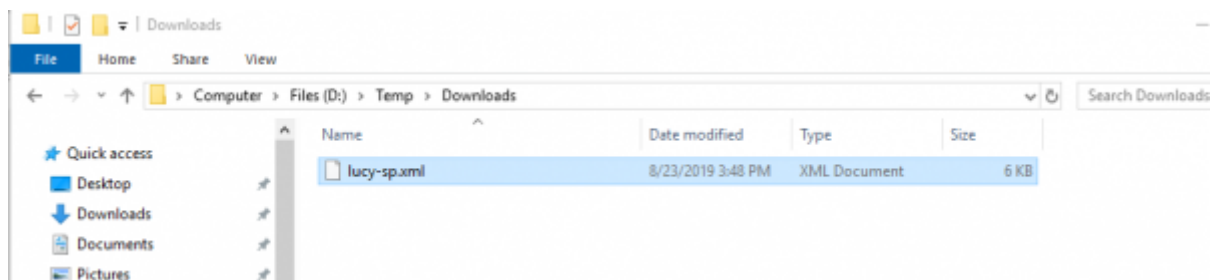
Identity Provider Certificate Thumbprint

Metadata Endpoint

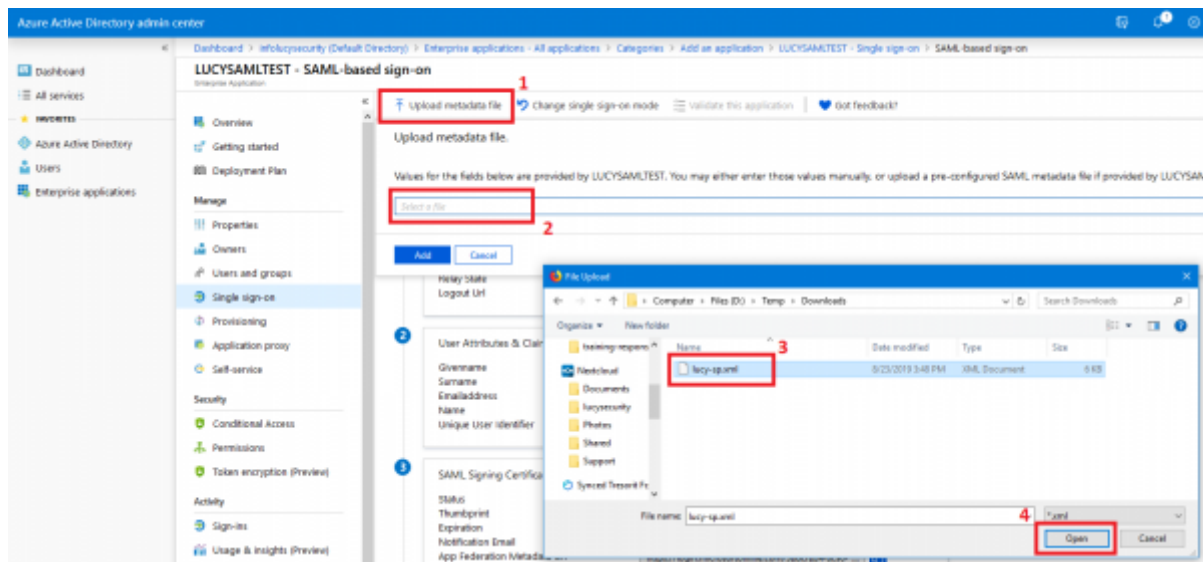
Provider Endpoint

Provider Certificate [Download Certificate](#)

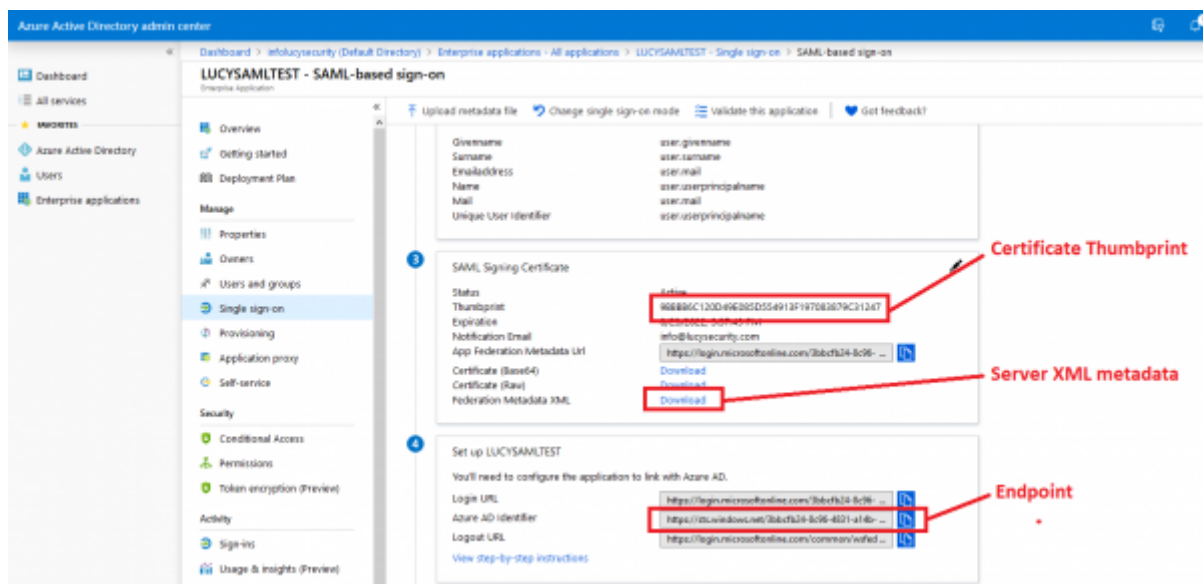
Auto Login ☐



- Upload the pre-configured SAML metadata file



- Download the FederationMetadata.xml file from Azure AD and fill the Identity Provider Endpoint and Certificate Thumbprint in Lucy



Home / SSO Configuration

SSO Configuration

☒ Enable Active Directory FS

Domain name:

Identity Provider Endpoint:

Identity Provider Server XML metadata:

Identity Provider Certificate Thumbprint:

Auto Login: ☐

- Add a new Claim "mail" that contain an e-mail address of the user, see more [here](#)

Azure Active Directory admin center

Dashboard > Intefacysecurity (Default Directory) > Enterprise applications > All applications > Categories > Add an application > LUCYSAMLTEST - Single sign-on > SAML-based sign-on

LUCYSAMLTEST - SAML-based sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Validate this application | Get feedback?

Set up Single Sign-On with SAML

Read the [configuration guide](#) or for help integrating LUCYSAMLTEST.

- ##### Basic SAML Configuration

Identifier (Entity ID)	https://access.dreadserver783.com/simplesaml/module.php/saml/sp/metadata.php/Asp-tp
Reply URL (Assertion Consumer Service URL)	https://access.dreadserver783.com/simplesaml/module.php/saml/sp/ps/passid-acc.php/Asp-tp
Sign on URL	Optional
Relay State	Optional
Logout URL	Optional
- ##### User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- ##### SAML Signing Certificate

Status	Active
Thumbprint	968866C126D48C8D554913F197803876C31247
Expiration	8/27/2023, 8:37:48 PM
Notification Email	info@lucysecurity.com
App Federation Metadata URL	https://open.microsoftonline.com/3bbcfb24-8c96-4831-~i
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Azure Active Directory admin center

Dashboard > Intefacysecurity (Default Directory) > Enterprise applications > All applications > Categories > Add an application > LUCYSAMLTEST - Single sign-on > SAML-based sign-on > Manage user claims

Manage user claims

[+ Add new claim](#)

Name identifier value:

Groups returned in claims:

CLAIM NAME	VALUE
https://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
https://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
https://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
https://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
https://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Name:

Namespace:

Source: ☐ Attribute ☐ Transformation

Source attribute:



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

- Configure Azure AD SAML token encryption, see more [here](#)

[Home](#) / SSO Configuration

SSO Configuration

☒ Enable Active Directory FS

Domain name

example.domain.com ⓘ ⓘ

Identity Provider Endpoint

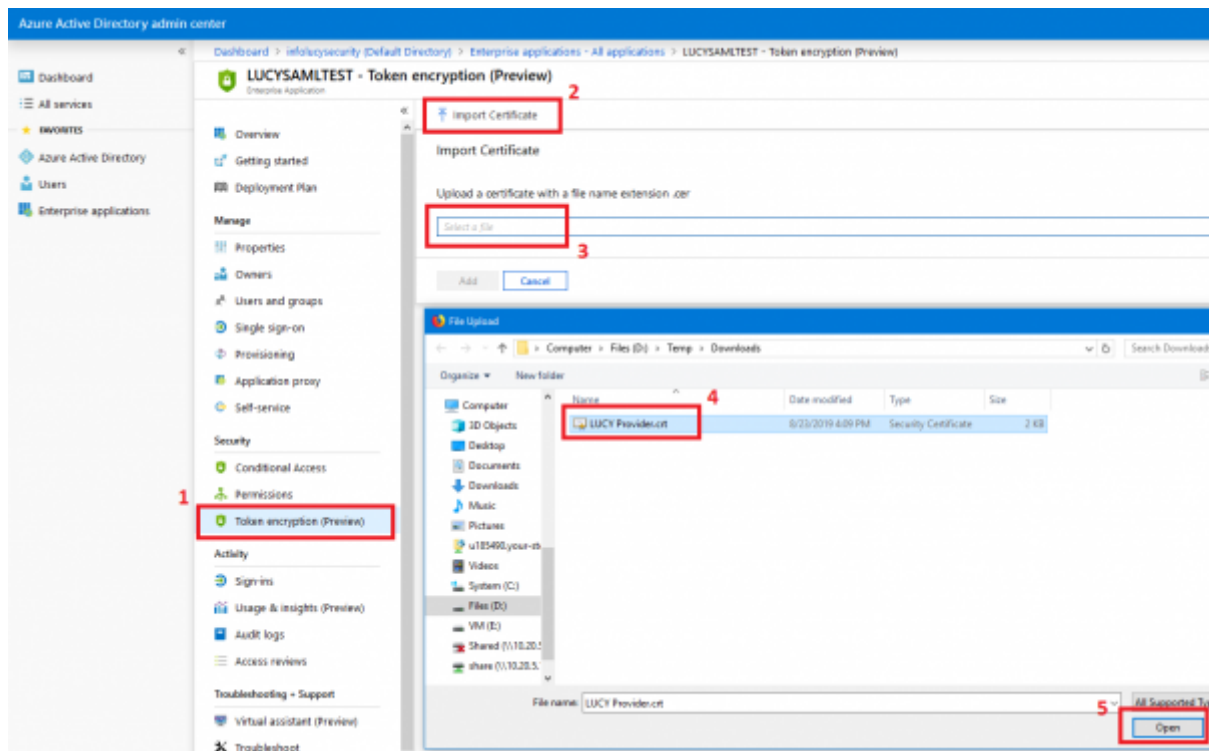
https://ad.example.com/identity-provider-endpoint/

Identity Provider Server XML metadata

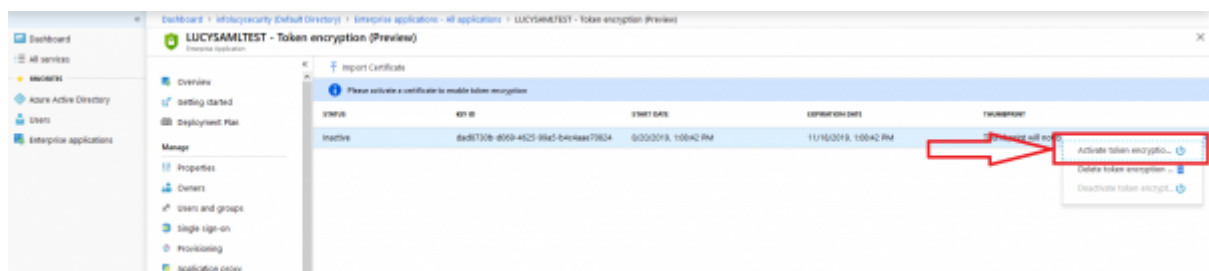
Browse... No file selected.

Identity Provider Certificate Thumbprint

SHA-1 thumbprint: 1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P7Q8R9S0T1U2V3W4X5Y6Z7A8B9C0D1E2F3G4H5I6J7K8L9M0N1O2P3Q4R5S6T7U8V9W0X1Y2Z3A4B5C6D7E8F9G0H1I2J3K4L5M6N7O8P9Q0R1S2T3U4V5W6X7Y8Z9A0B1C2D3E4F5G6H7I8J9K0L1M2N3O4P5Q6R7S8T9U0V1W2X3Y4Z5A6B7C8D9E0F1G2H3I4J5K6L7M8N9O0P1Q2R3S4T5U6V7W8X9Y0Z1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P



Do not forget to activate the encryption for the uploaded certificate



- **(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"

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

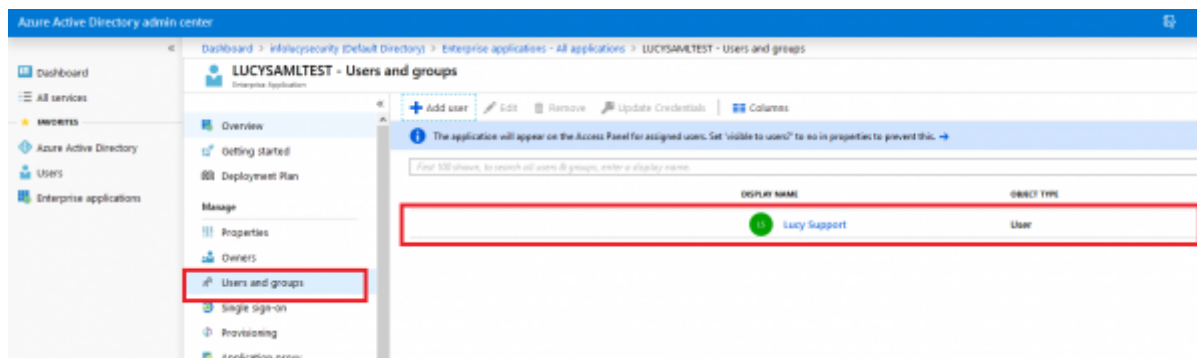


Please note, Azure AD does not support multiple second-level domains in a single application.

- **(optional)** If the option "**Auto Login**" enabled, Lucy tries to automatically log in using Single Sign-on instead of showing the Login page.

Testing Authentication

- Make sure you have added users to your app



- 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

Domain name

Identity Provider Endpoint

Identity Provider Server XML metadata No file selected.

Identity Provider Certificate Thumbprint

Metadata Endpoint

Provider Endpoint

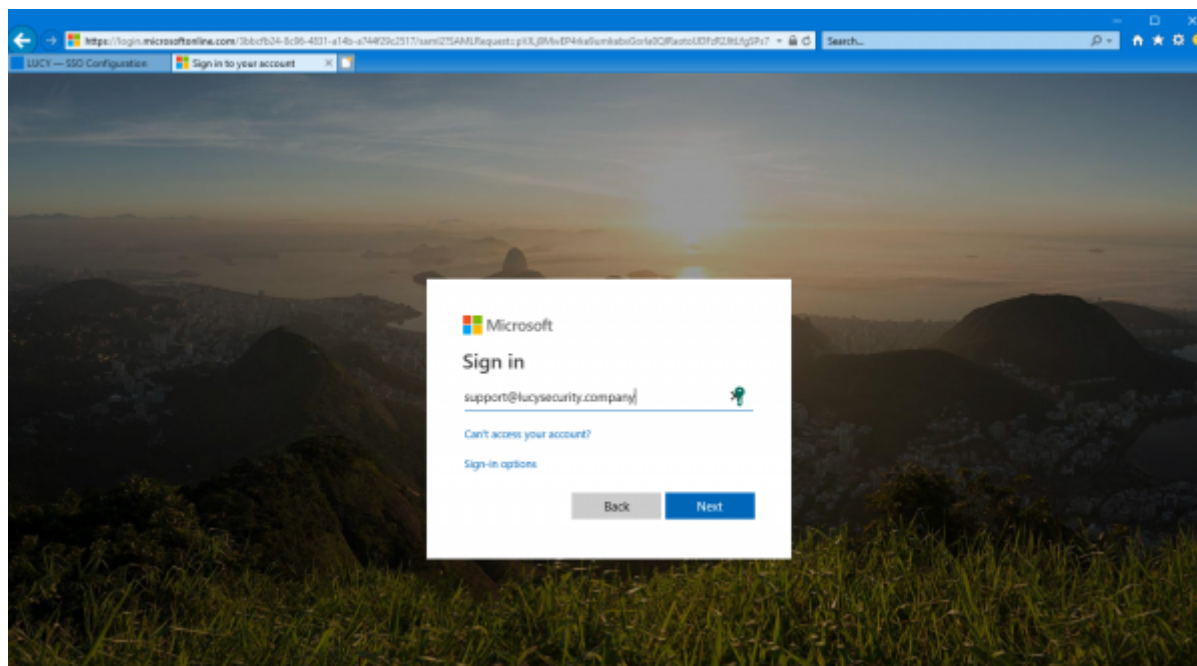
Provider Certificate [Download Certificate](#)

Auto Login ☐

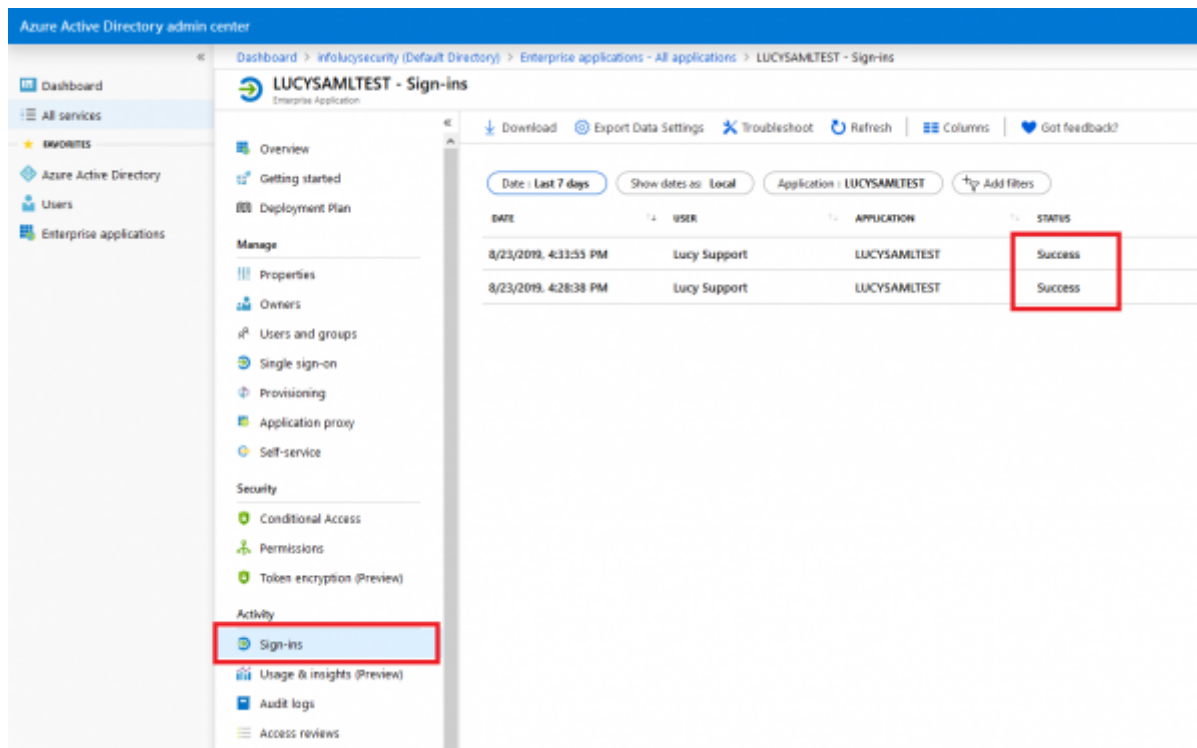
[Save](#)

[Test Connection](#)

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



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



OAuth 2.0

The method of authentication is described [here](#).

Troubleshoot problems

- I am redirected back to Lucy's login page after successful authorization through the Single sign-on.

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:

Manage claim

Save Discard changes

* Name mail ✓

Namespace Enter a namespace URI

* Source ☒ Attribute ☐ Transformation

* Source attribute user.userprincipalname

Claim conditions

From:

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

Permanent link:

https://wiki.lucysecurity.com/doku.php?id=sso_azure

Last update: **2022/10/04 15:18**

