2024/05/05 08:40

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)
- 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:

| ATLS Company | - | Settings - | 1. |
|----------------------------------|--------------|------------------------------|----|
| Home / SSO Configu | Iration | Templates | |
| | | Benchmark Sectors | |
| SSO Cont | figurat | Domains Dynamic DNS | |
| | Enable A | Adapt Authoring Toolkit | |
| Domain name | | Recipients | |
| Identity Provider | https://sts. | Clients | |
| Endpoint | | End Users | |
| Identity Provider | Choose | 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 | |
| Provider Certificate | Download C | SMS Settings | |
| | | API Whitelist | |
| Auto Login | | 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

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

| | Supp | ort Proper | ties | | ? | × | |
|--------------------|--------------------|----------------|-------------------|-----|----------------|-------|--|
| Security | Environment | Sessi | ions | Re | Remote control | | |
| Remote Desk | top Services Profi | le C(| -MC | At | tribute Ed | tor | |
| Published Certific | ates Member C | f Password | Password Replicat | | tion Dial-in (| | |
| General Add | dress Account | Profile | Profile Telephor | | Organiz | ation | |
| 🧏 Sup | oport | | | | | | |
| First name: | Support | | Initials | : | | | |
| Last name: | | | | | | | |
| Digplay name: | Support | | | | | | |
| Description: | | | | | | | |
| Office: | | | | | | | |
| Telephone num | ber: | | |] [| Other | | |
| E- <u>m</u> ail: | support@l | ucysecurity.co | om | | | | |
| 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:

| 1 | | | AD FS | | | | |
|------------------------------|-----------|---------------|---|------------------------|-------------------------|---------------|----|
| File Action View Window Help | p | | | | | | |
| • 🔿 🛋 🖬 🖬 | | | | | | | |
| AD FS | Endpoints | | | | | | |
| Service | Enabled | Proxy Enabled | URL Path | Туре | Authentication Type | Security Mode | |
| Endpoints Certificates | No | No | /adfs/services/trust/13/asuedtokensymmetrictripledes | 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 | Mooed | |
| Claims Provider Trusts | No | No | /adfs/services/trust/13/issuedtokenmixedsymmetrictripled | WS-Trust 1.3 | SAML Token (Sym | Moved | |
| 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 | Moved | |
| Authentication Policies | No | No | /adfs/services/trust/13/windowstransport | WS-Trust 1.3 | Windows | Transport | |
| Per Relying Party Trust | Yes | No | /adfs/services/trusticp/windows | WS-Truat 2005 | Local Windows | Message | |
| - removing rancy max | No | No | /adfs/services/trust/attfactresolution | SAML-AttfactResolution | Anonymous | Transport | |
| | Yes | Yes | /adfs/cauth2/ | OAuth | Anonymous | Transport | |
| | Metadata | | | | | | |
| | Yes | Yes | /adla/services.lto.st/sex | WS-MEX | Accorners | Transport | _ |
| | Yes | Yes | /FederationMetadata/2007-05/FederationMetadata.xml | Federation Metadata | Агопутоца | Transport | 1 |
| | 100 | 140 | | NOTO 1.0 PRODUCT | The proof | Transport | ۰. |
| | Proxy | | | | | | |
| | Yes | No | /adfs/prox/ | Web Application Proxy | Proxy Trust Certificate | Transport | |
| | Yes | No | /adfs/proxy/EstablishTrust/ | Web Application Proxy | Password | Transport | |
| | Other | | | | | | |
| | No | No | /adfs/contal/updatepassword/ | HTTP | Anonimous | Transport | |
| | | THE | raurarponiar upsacepasawora/ | niir | renorgenous | That reports | |
| | | | | | | | |

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:

5/17

| 9 | AD FS | _ D X |
|---|---|--|
| Se Action View Window Help | | _ Ø × |
| 🜩 < 📩 📰 📓 📰 | Certificates | Actions |
| Service Service Certificates Clam Discoptions | Service communications | ration Date Status Primary Certificates Add Token-Signing Certi Add Token-Decrypting C |
| I a I Trust Relationships Claims Provider Trusts Relying Party Trusts | | 7/2020 Primary Set Service Communicati View |
| Attribute Stores | CN+ADFS Signing - LUCYS CN+ADFS Signing - LUCY 3/18/2019 3/17 | 7/2020 Plimary New Window from Here |
| Per Relying Party Trust | | Certificate Certif |
| | | 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:////int/lucy-sp | |
| | Save | |

• Click Save.

Create the Relying Party Trust in AD FS

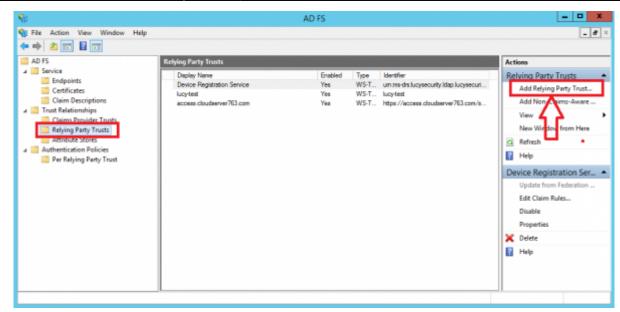
• Copy the Lucy Metadata Endpoint link from the SSO Configuration page:

| Home / SSO Config | uration | |
|--|---|--|
| SSO Con | figuration | |
| | ✓ Enable Active 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:// i/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:

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

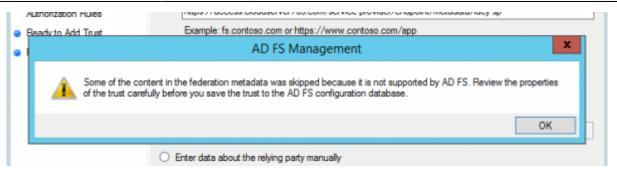
In case access to the Lucy Admin Console is limited to a range of IP addresses, you must include an ADFS server in this range.



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

| \$ 1 | Add Relying Party Trust Wizard | x |
|---|---|---|
| Select Data Source | | |
| Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules | Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network 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. Federation metadata address (host name or URL): [https://access.cloudserver763.com/service-provider/endpoint/metadata/ucy-sp] | |
| Ready to Add Trust Finish | Example: fs.contoso.com or https://www.contoso.com/app 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 Use this option to manually input the necessary data about this relying party organization. Previous Next > | |

• Accept the warning:



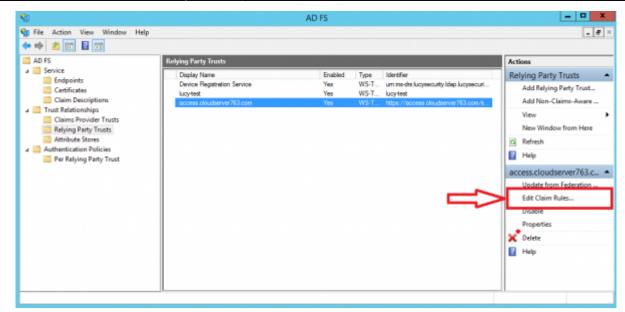
• Click the **Next** button in the wizard until you reach the Ready To Add Trust page. Check the Encryption and Signature tabs have certificates associated with them:

| \$ | | Add Relying Party Trust Wizard | | | | | | | |
|---|---------------|--------------------------------|---------------|--------------|----------------------|------------------|--------------|---------|---|
| Ready to Add Trus | st | | | | | | | | |
| Steps | The relving p | arty trust has | s been config | ured. Review | w the following sett | ings, and then o | 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 | | | equests from this re | lying party. | | | |
| Configure Multi-factor Authentication Now? | Subject | t | Issuer | Ef | fective Date | Expiration Date | | | |
| 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 | | | | | | | | | |
| Finish | | | | | | | | | |

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

| Display Name | Enabled | Туре | Identifier |
|-----------------------------|---------|------|--|
| Device Registration Service | Yes | WS-T | um:ms-drs:lucysecurity.ldap.lucysecuri |
| lucuted | Yes | WS-T | lucy-test |
| access.cloudserver763.com | Yes | WS-T | https://access.cloudserver763.com/s. |
| access.cloudserver763.com | Yes | WS-T | https://access.cloudserver763 |

• 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:

| 翰 👘 Edit Claim Rules | for access.cloudserver763.com 📃 🗖 🗙 |
|---------------------------------|---|
| Issuance Transform Rules Issu | ance Authorization Rules Delegation Authorization Rules |
| The following transform rules a | pecify the claims that will be sent to the relying party. |
| Order Rule Name | Issued Claims |
| | |
| | |
| | |
| | |
| | 1 |
| | 4 |
| | |
| | |
| JL | |
| | |
| Add Rule Edit Rule | Remove Rule |
| | |
| | |
| | OK Cancel Apply |

| \$ 0 | Add Transform Claim Rule Wizard | | | | | |
|--|--|--|--|--|--|--|
| Select Rule Template | e | | | | | |
| 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 ✓ Claim rule template description: | | | | | |
| | 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:

| \$ | 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 V UPN SAM-Account-Name vid 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 | 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: 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. | | | |

| \$ | Add Transfo | orm Claim Rule Wizard |
|---|--|--|
| Configure Rule | | |
| Steps Choose Rule Type Configure Claim Rule | also map an incoming claim v | |
| | Incoming claim type: Incoming name ID format: Outgoing claim type: Outgoing name ID format: Pass through all claim value | UPN v Unspecified v Name ID v Transient Identifier v |
| | Replace an incoming claim Incoming claim value: Outgoing claim value: | vos m value with a different outgoing claim value m value with a different outgoing claim value Browse Browse Browse 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**:

| Home / SSO Co | onfiguration | |
|---|----------------------------|-----------------|
| SSO Co | onfiguration | |
| | Enable Active Directory FS | Test Connection |
| ldentity Provider Endpoint | https:// 'adfs/s |] |
| ldentity Provider Server XML metadata | Browse | |
| 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": 13/17

| 🗅 Sign In 🗙 🕂 | × |
|---|---|
| ← → C ▲ Not secure https://adfs.lucysecurity.host/adfs/ls/?SAMLRe | nquest=pVJda%28MwEPwrRu%282HDuXuCIJ58 🛧 🎵 😰 🗄 |
| | Lucy Security |
| | Sign in with your organizational account support@Idap.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:

| Lucy 4.5 Login | | | | |
|------------------|----------|---------------------------|-------|--|
| 6 | Login | | | |
| Lucy | Email | support@lucysecurity.com | 5 | |
| | Password | | Forgo | |
| | Language | English | • | |
| | | Login | | |
| | | Login with single sign-on | | |
| Lucy Security AG | | | | |

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 | | |
|---|--|---|
| Base Settings Awareness Settings Schedule Recipients | User Profile Page Link | C Enduser Profiles Enabled |
| Advanced Settings | | Track Responses |
| User Settings Custom Fields | Antivirus/Firewall Protection Interval | O v |
| Reminders | | Allow Awareness Rescheduling Ignore repeated answers in awareness. |
| Supervision Log Message Log Errors | | Stop the Campaign Automatically After I stop the campaign, send me a report to supportigitucysecurity.com |
| | [| 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:

| se Settings | Name | Avoid & Recognize Phishing Attacks | |
|-------------|------------|-------------------------------------|---|
| bsite | Risk Level | 0 | ۲ |
| L Settings | | Website Enabled | |
| isage | | Create Awareness Training Diploma 9 | |
| il Settings | - E | ☑ Do not send emails | |
| | Languages | Dutch | × |
| | | si English | × |
| | | + Add - | |

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>:

| nternet Sec | Campaign Status Not | Started | Export to SCORM | Upload Webpage |
|---|---------------------|--|-------------------------|----------------|
| Base Settings | Domain | access.cloudserver763.com | θ | |
| Website | | 🗹 Quiz 9 | | |
| SSL Settings | Preview link | https://access.cloudserver763.com/awareness /37f6c979613315eb967b6be2530cdc9bab6731ee546 | c686f150b7b28f3ee6530 | |
| Message | | /11/index.html | | |
| Mail Settings | Global link | https://access.cloudserver763.com/awareness /s/37f6c979613315eb967b6be2530cdc9bab5731ee54 | 46c686f150b7b28f3ee6530 | |
| | Language | English | ~ | |
| Quick Tips | | | | |
| | File | index.html ~ | × O | |
| Quick Tips Awareness Website Variables Quiz Integration | File | index.html v | × O | |

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

| SL Settings | Campaign Status | Running | |
|--------------------------|-----------------|--|-----|
| 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 | |

Useful tips

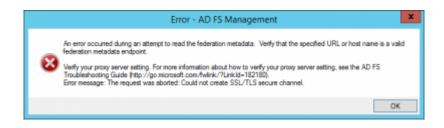
How to update or replace SSL certificate used for SSO authentication?

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:

| \$ 1 | 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 put | history | | | |
| Configure Multi-factor Authentication Now? | Its federation metadata online or on a local network. Federation metadata address flost name or URL): | | | | |
| Choose Issuance Authorization Rules | recension messoas accress (nos name or Unit): | | | | |
| Ready to Add Trust | Example: fs.contoso.com or https://www.contoso.com/app | | | | |
| Fnish | 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 wi validate the source of the file. | | | | |
| | Federation metadata file location: | | | | |
| | C-/Users/Administrator/Downloads/kucy-ep.xml Brow | | | | |
| | O Enter data about the relying party manually | | | | |
| | Use this option to manually input the necessary data about this relying party organization. | | | | |

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&rev=1593500008



Last update: 2020/06/30 08:53