Single-Sign-On

authentik is an open-source Identity Provider, focused on flexibility and versatility.

Tutorials

Tutorials in performing certain configurations

Tutorials

Rancher-SAML-ADFS (Authentik)

What is Rancher

> An enterprise platform for managing Kubernetes Everywhere Rancher is a platform built to address the needs of the DevOps teams deploying applications with Kubernetes, and the IT staff responsible for delivering an enterprise-critical service.
>
> -- https://rancher.com/products/rancher

Preparation

The following placeholders will be used:

- `rancher.company` is the FQDN of the Rancher install.
- `authentik.company` is the FQDN of the authentik install.

Under *Customization -> Property Mappings*, *create a SAML Property Mapping*. Give it a name like "SAML Rancher User ID". Set the SAML name to `rancherUidUsername` and the expression to the following

```
return f"{user.pk}-{user.username}"
```

Create an application in authentik. Set the Launch URL to `https://rancher.company`, as Rancher does not currently support IdP-initiated logins.

Create a SAML provider with the following parameters:

- ACS URL: `https://rancher.company/v1-saml/adfs/saml/acs`
- Audience: `https://rancher.company/v1-saml/adfs/saml/metadata`
- Issuer: `authentik`
- Service Provider Binding: `Post`
- Property mappings: Select all default mappings and the mapping you've created above.
- Signing Certificate: Select the authentik self-signed certificate.

You can of course use a custom signing certificate, and adjust durations.

Rancher

In Rancher, navigate to *Global -> Security -> Authentication*, and select ADFS.

Fill in the fields

- Display Name Field: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`
- User Name Field: `http://schemas.goauthentik.io/2021/02/saml/username`
- UID Field: `rancherUidUsername`
- Groups Field: `http://schemas.xmlsoap.org/claims/Group`

For the private key and certificate, you can either generate a new pair (in authentik, navigate to *Identity & Cryptography -> Certificates* and select Generate), or use an existing pair.

Copy the metadata from authentik, and paste it in the metadata field.

Click on save to test the authentication.

Organizr LDAP Setup (Authentik)

Support level: Community

What is organizr

> Organizr allows you to setup "Tabs" that will be loaded all in one webpage.
>
> -- https://github.com/causefx/Organizr

This integration leverages authentik's LDAP for the identity provider to achieve an SSO experience. See ldap provider generic setup for setting up the LDAP provider.

Preparation

The following placeholders will be used:

- `organizr.company` is the FQDN of the Service install.
- `authentik.company` is the FQDN of the authentik install.

Create a new user account *(or reuse an existing)* for organizr to use for LDAP bind under *Directory -> Users -> Create*, in this example called `ldapservice`.

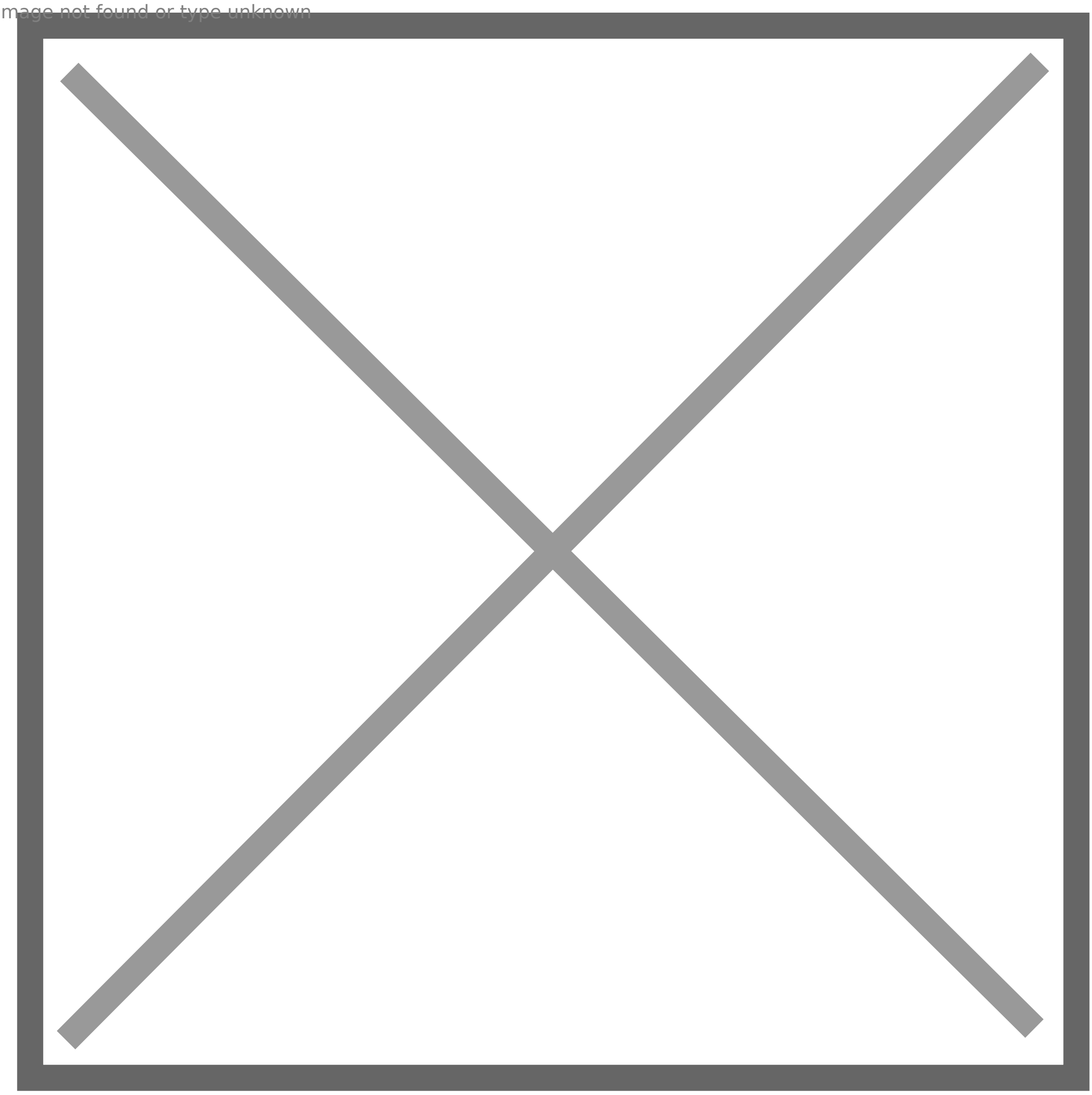
Note the DN of this user will be `cn=ldapservice,ou=users,dc=ldap,dc=goauthentik,dc=io`

> *Optionally*, create a new group like `organizr users` to scope access to the organizr application.

Authentik Configuration

1. Create a new Proxy Provider for `https://organizr.company`

   Image not found or type unknown

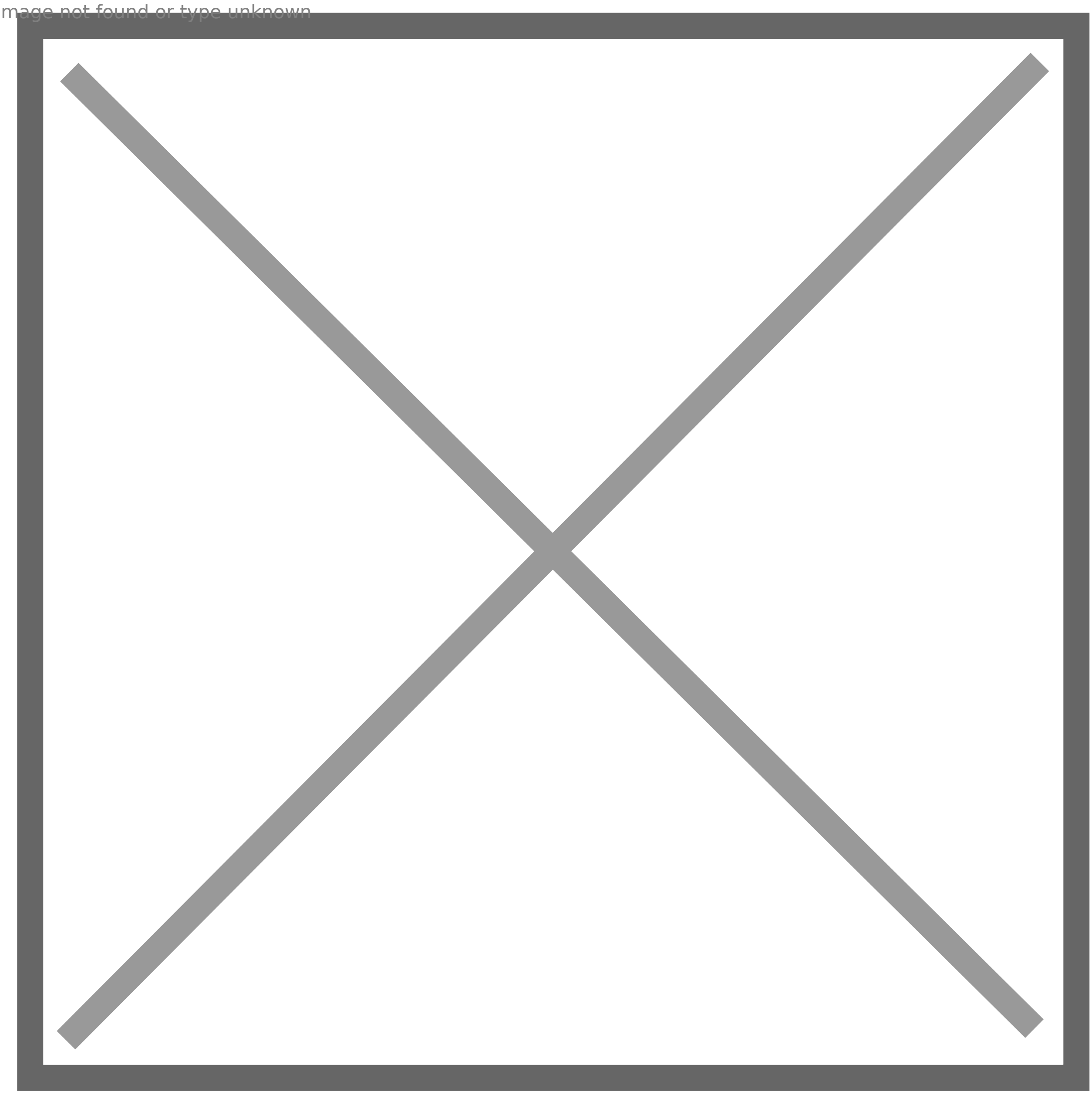
   

   Optionally, add the regular expression to allow api calls in the advanced protocol settings.

Image not found or type unknown

2. Create a new Application for the `https://organizr.company` Provider.

Image not found or type unknown



TIP

Optionally, bind the group to control access to the organizr to the application.

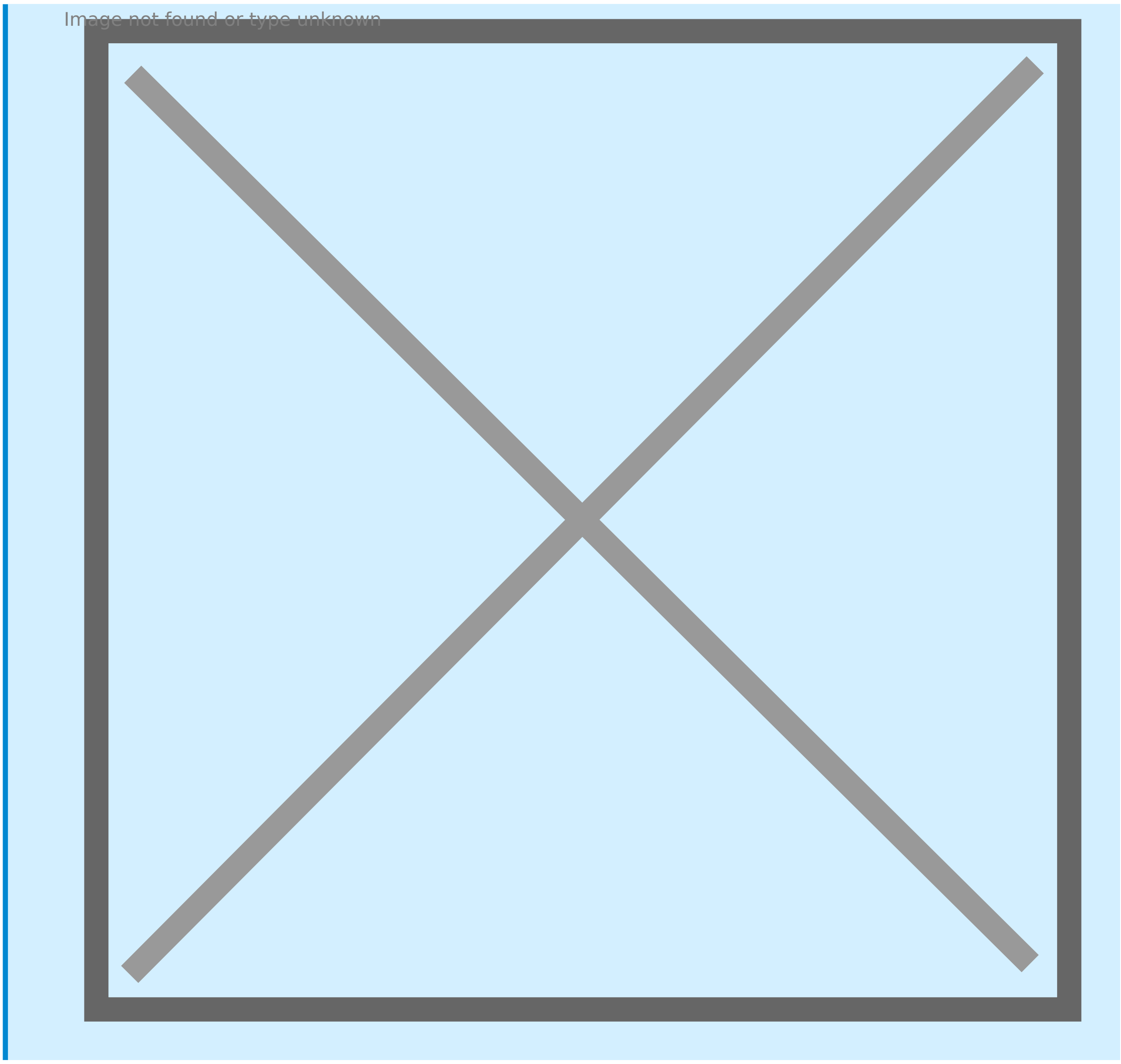
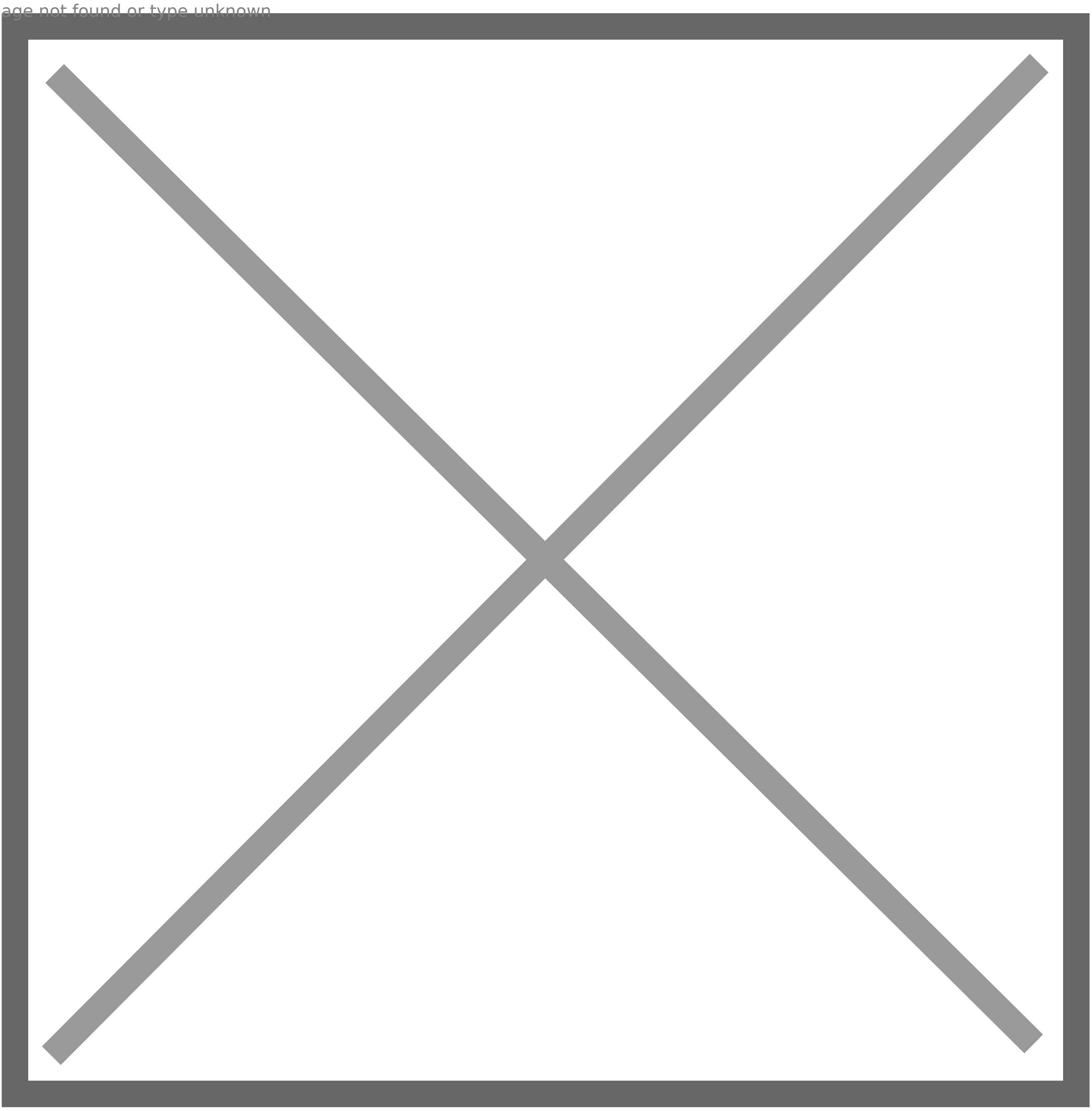


Image not found or type unknown

Image not found or type unknown



::: 3. Add the Application to the authentik Embedded Outpost.

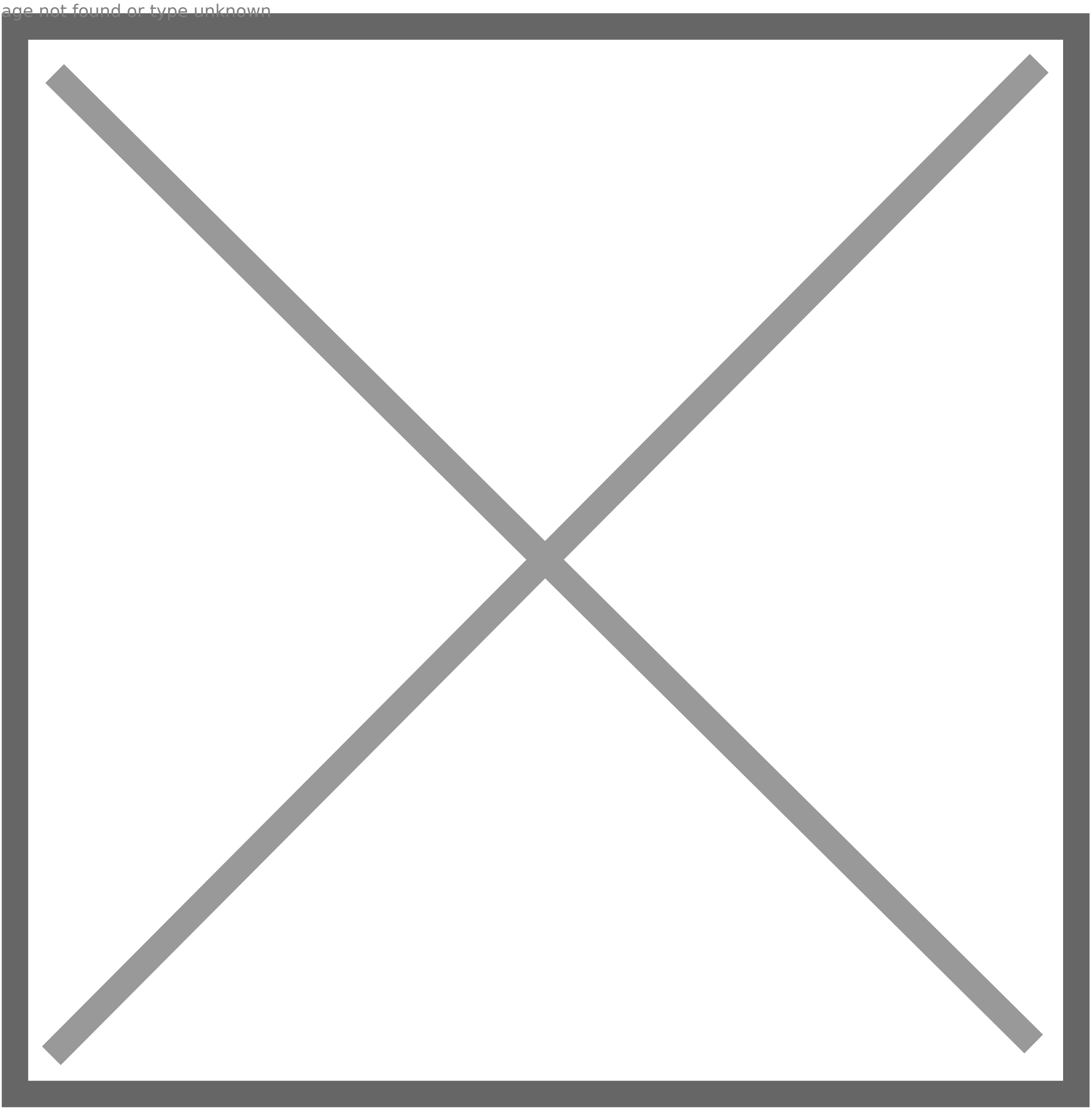
organizr Configuration

> CAUTION
> Ensure any local usernames/email addresses in organizr do not conflict with usernames/email addresses in authentik.

1. Enable Auth Proxy in organizr *system settings* -> *main* -> *Auth Proxy*

Auth Proxy Header Name: `X-authentik-username` Auth Proxy Whitelist: *your network subnet in CIDR notation IE* `10.0.0.0/8` Auth Proxy Header Name for Email: `X-authentik-email` Logout URL: `/outpost.goauthentik.io/sign_out`

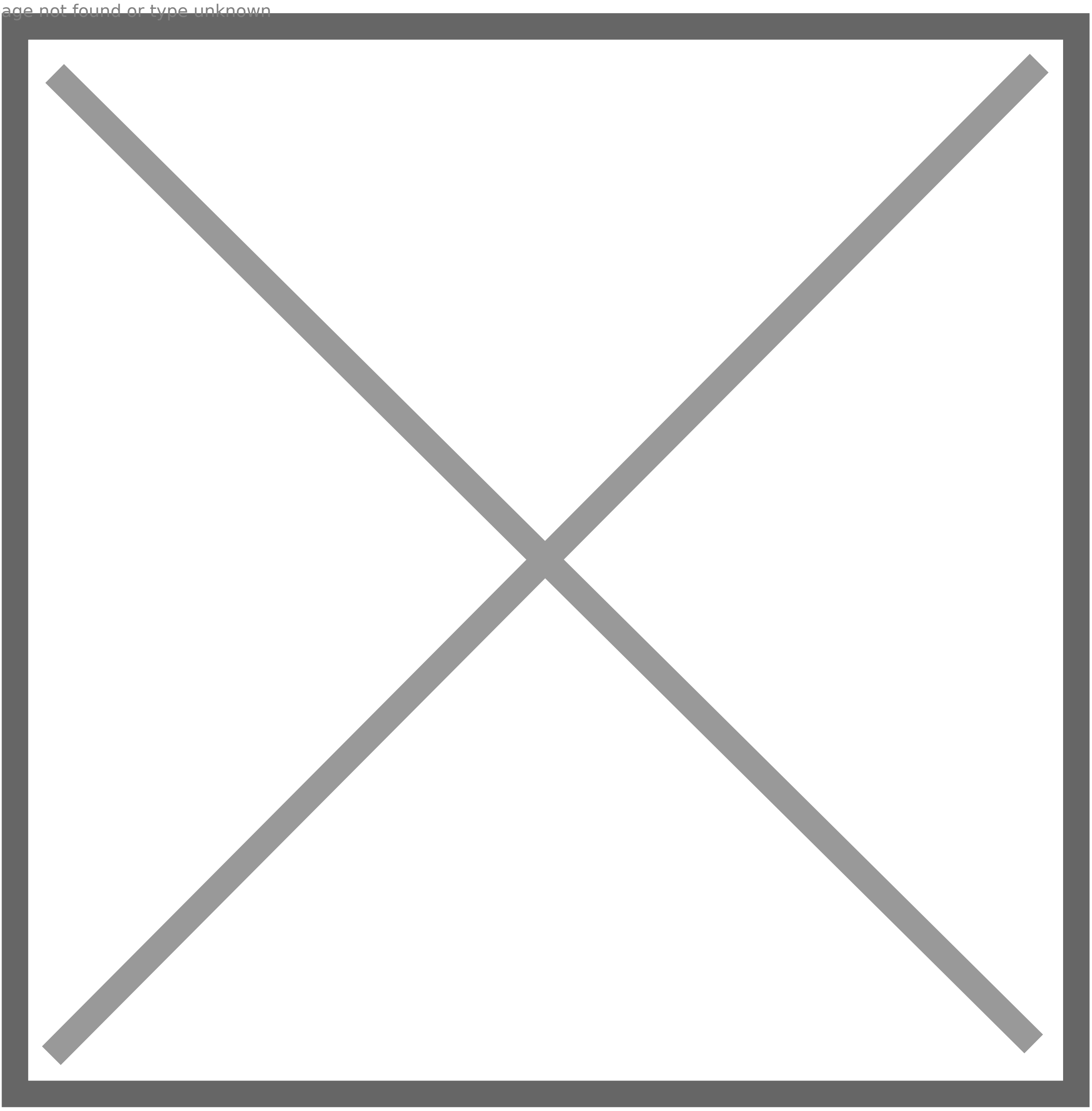
Image not found or type unknown



2. Setup Authentication in organizr *system settings -> main -> Authentication*

Authentication Type: `Organizr DB + Backend` Authentication Backend: `Ldap` Host Address: `<LDAP Outpost IP address:port>` Host Base DN: `dc=ldap,dc=goauthentik,dc=io` Account Prefix: `cn=` Account Suffix: `,ou=users,dc=ldap,dc=goauthentik,dc=io` Bind Username: `cn=ldapservice,ou=users,dc=ldap,dc=goauthentik,dc=io` Bind Password: `<LDAP bind account password>` LDAP Backend Type: `OpenLDAP`

Image not found or type unknown



INFO

Access for authentik users is managed locally within organizr under *User Management*. By default, new users are assigned the `User` group.

`TIP`

Consider front-ending your application with a forward auth provider for an SSO experience.

Tutorials

LDAP Provider Generic Setup (Authentik)

Create User/Group

1. Create a new user account to bind with under *Directory* -> *Users* -> *Create*, in this example called `ldapservice`.
   Note the DN of this user will be `cn=ldapservice,ou=users,dc=ldap,dc=goauthentik,dc=io`
2. Create a new group for LDAP searches. In this example `ldapsearch`. Add the `ldapservice` user to this new group.NFO

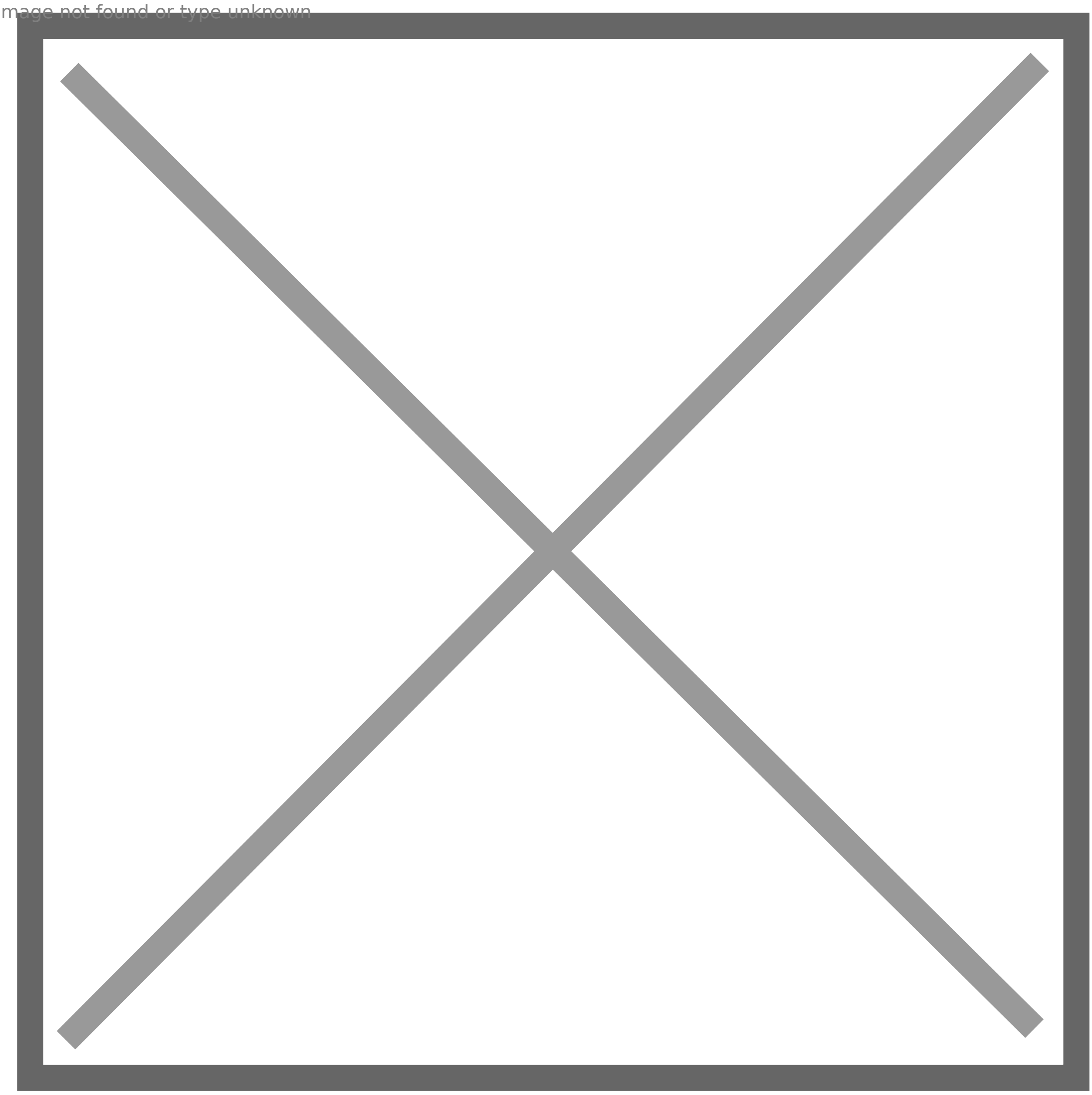
> Note: The `default-authentication-flow` validates MFA by default, and currently everything but SMS-based devices are supported by LDAP. If you plan to use only dedicated service accounts to bind to LDAP, or don't use SMS-based authenticators, then you can use the default flow and skip the extra steps below and continue at Create LDAP Provider

LDAP Flow

Create Custom Stages

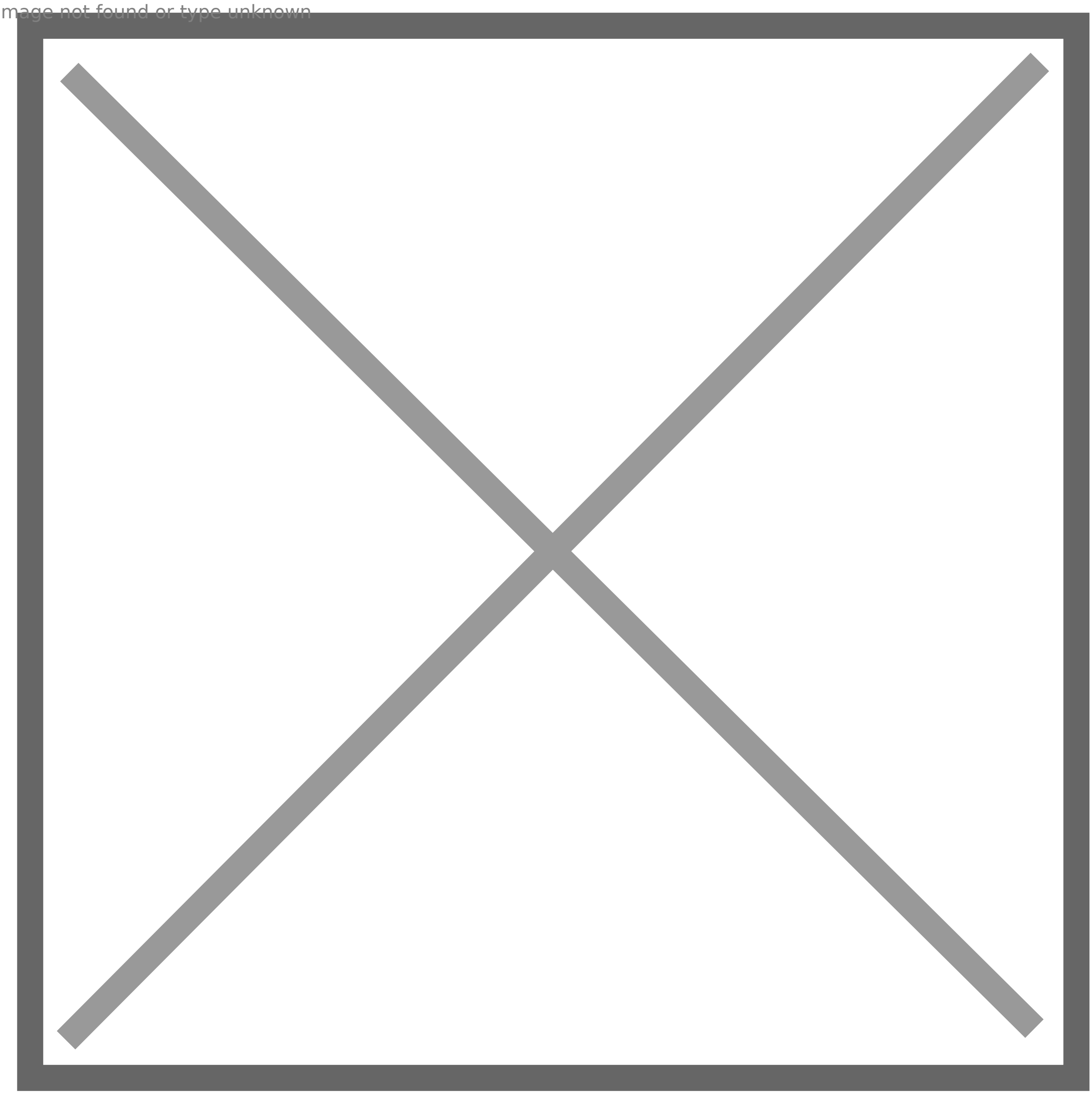
1. Create a new identification stage. *Flows & Stage* -> *Stages* -> *Create*

Image not found or type unknown



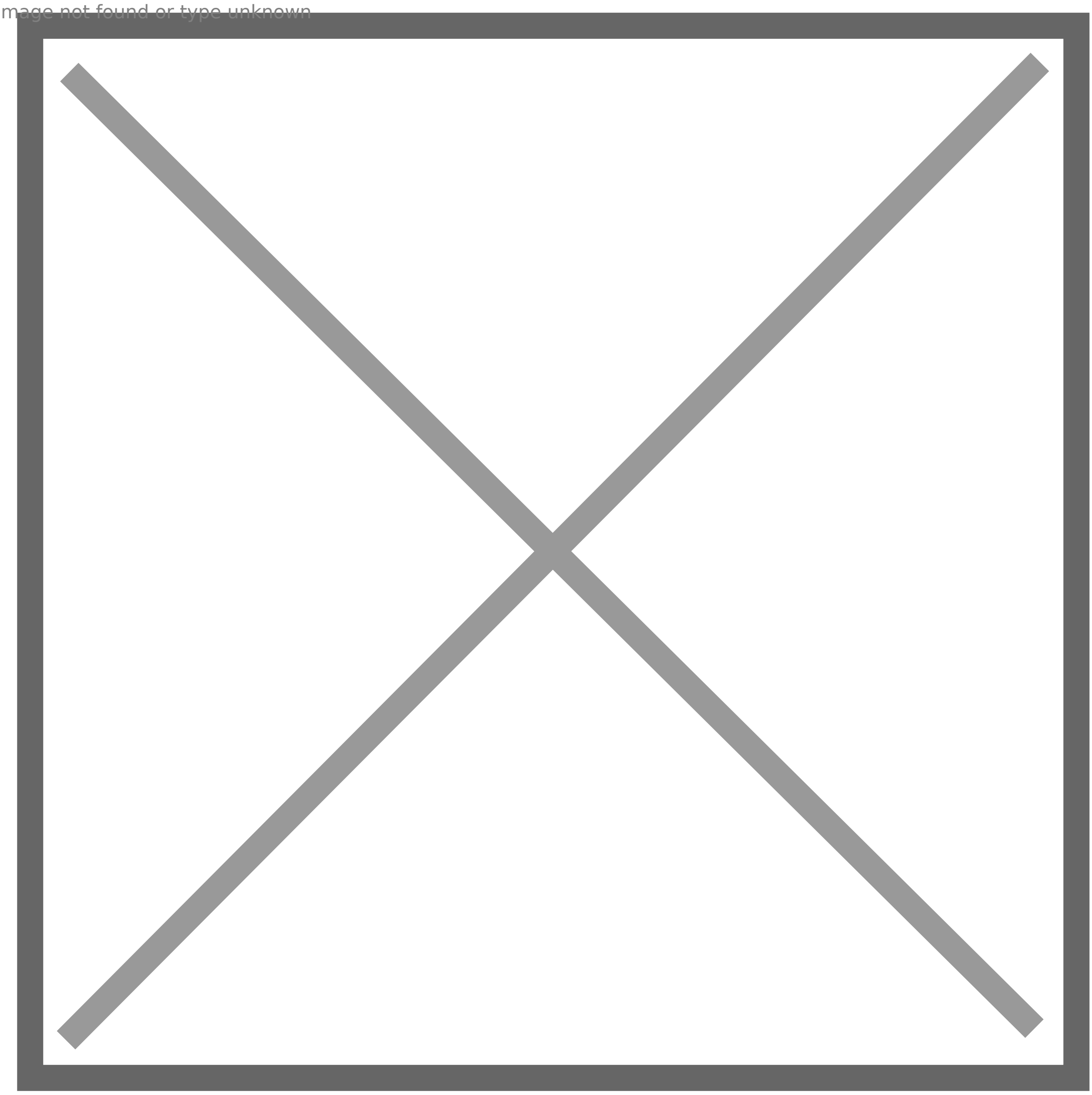
2. Name it something meaningful like `ldap-identification-stage`. Select User fields Username and Email (and UPN if it is relevant to your setup).

Image not found or type unknown



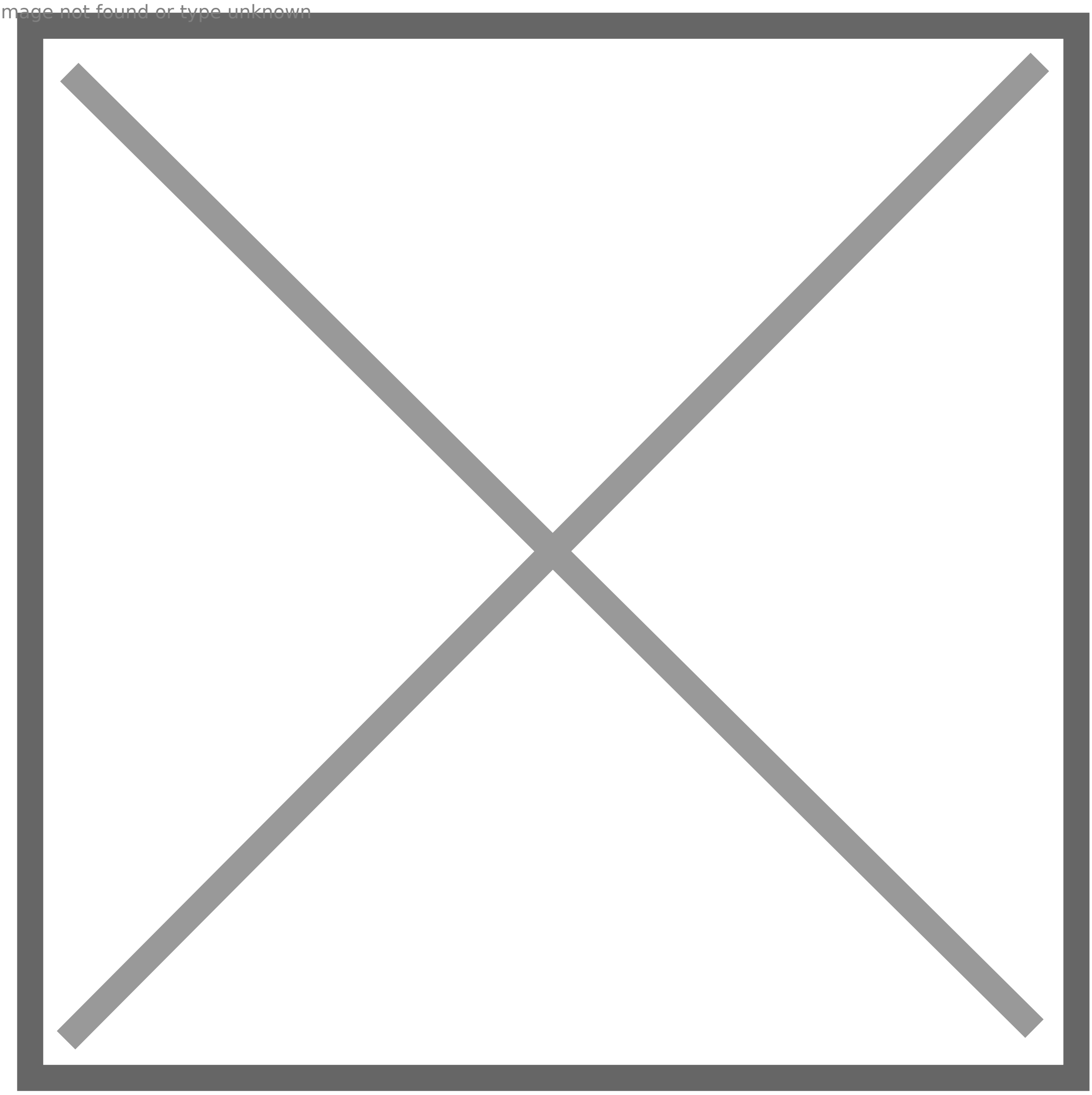
3. Create a new password stage. *Flows & Stage* -> *Stages* -> *Create*

Image not found or type unknown

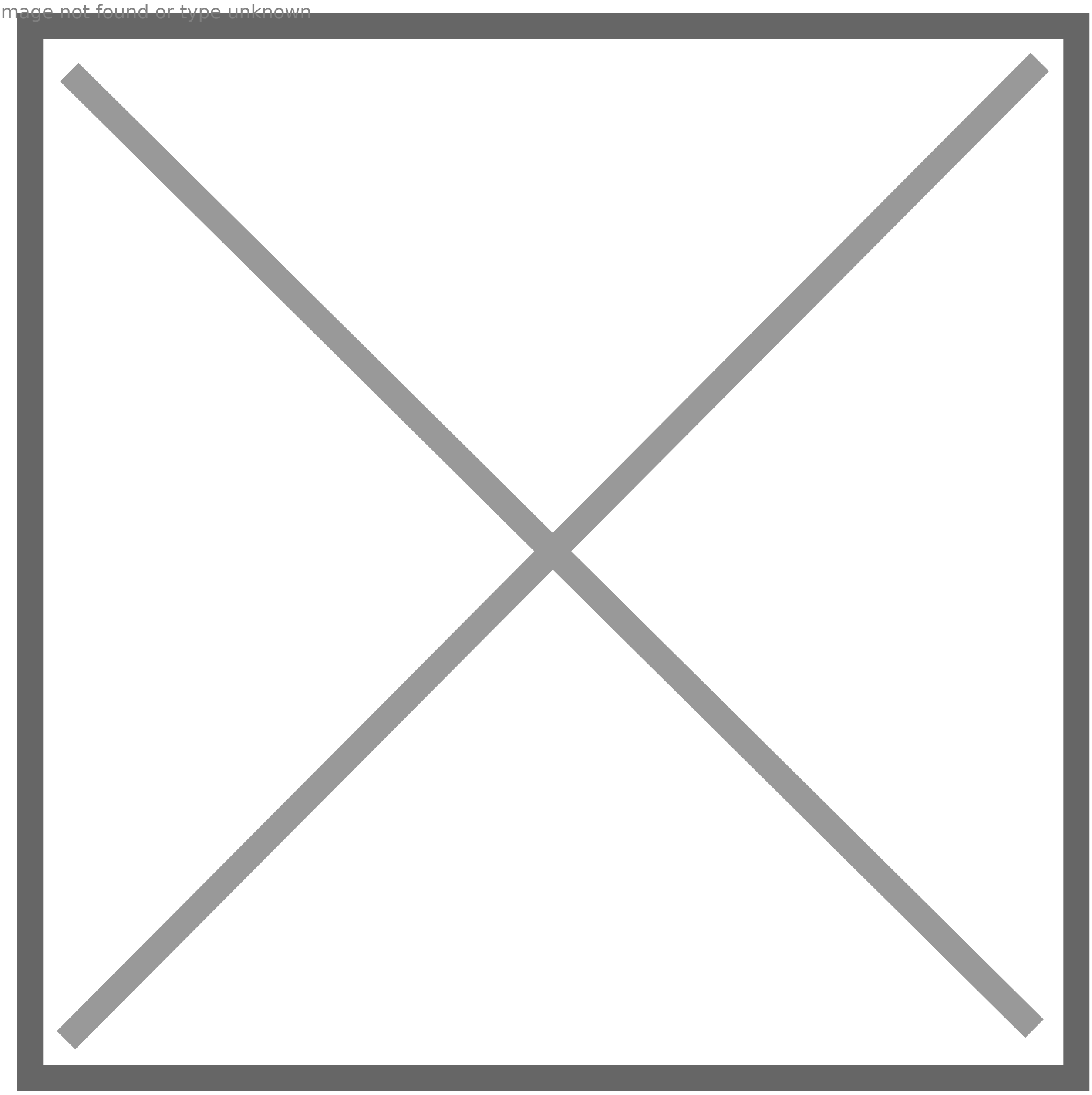


4. Name it something meaningful like `ldap-authentication-password`. Leave the defaults for Backends.

Image not found or type unknown

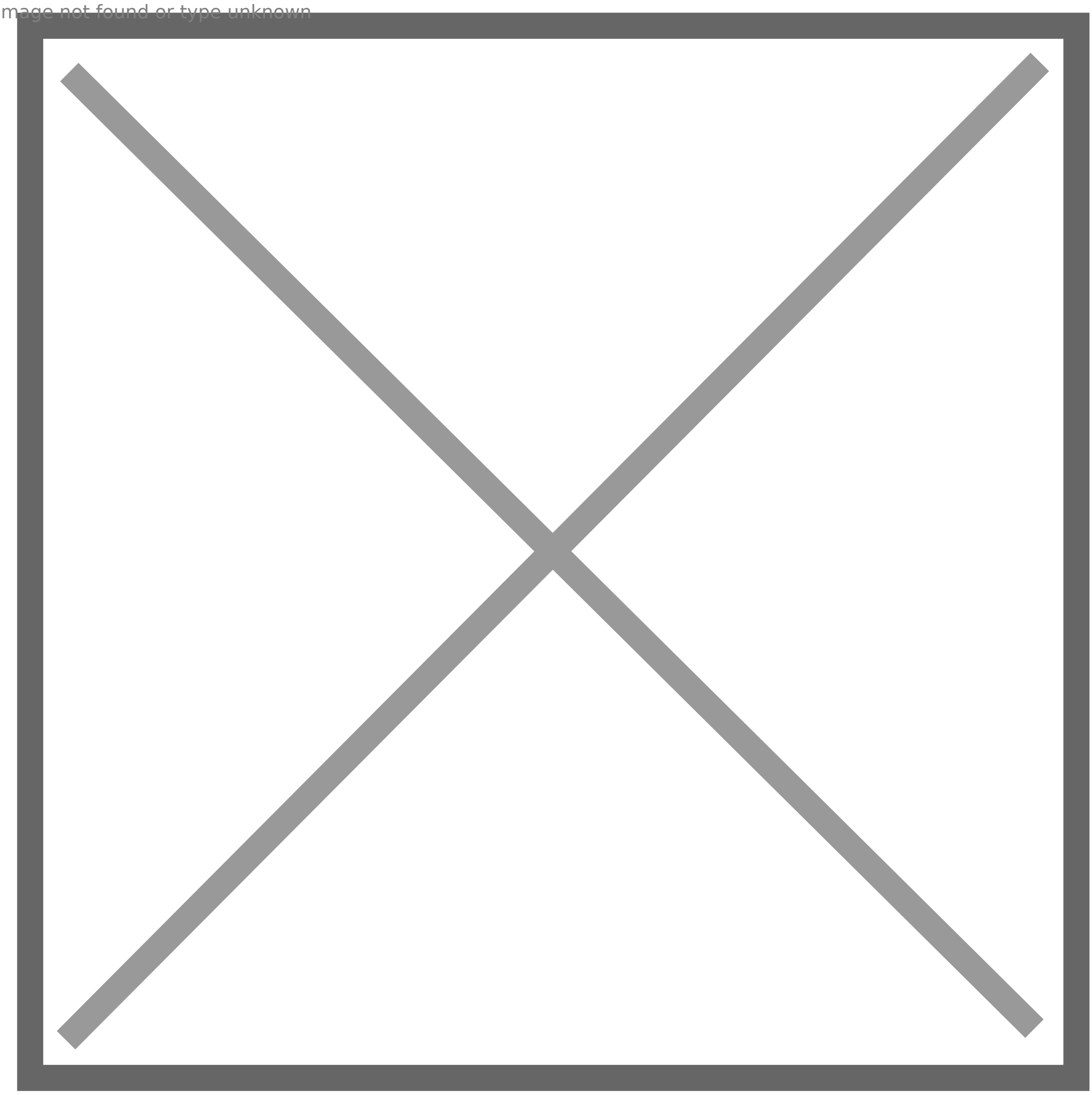


5. Create a new user login stage. *Flows & Stage* -> *Stages* -> *Create*



6. Name it something meaningful like `ldap-authentication-login`.

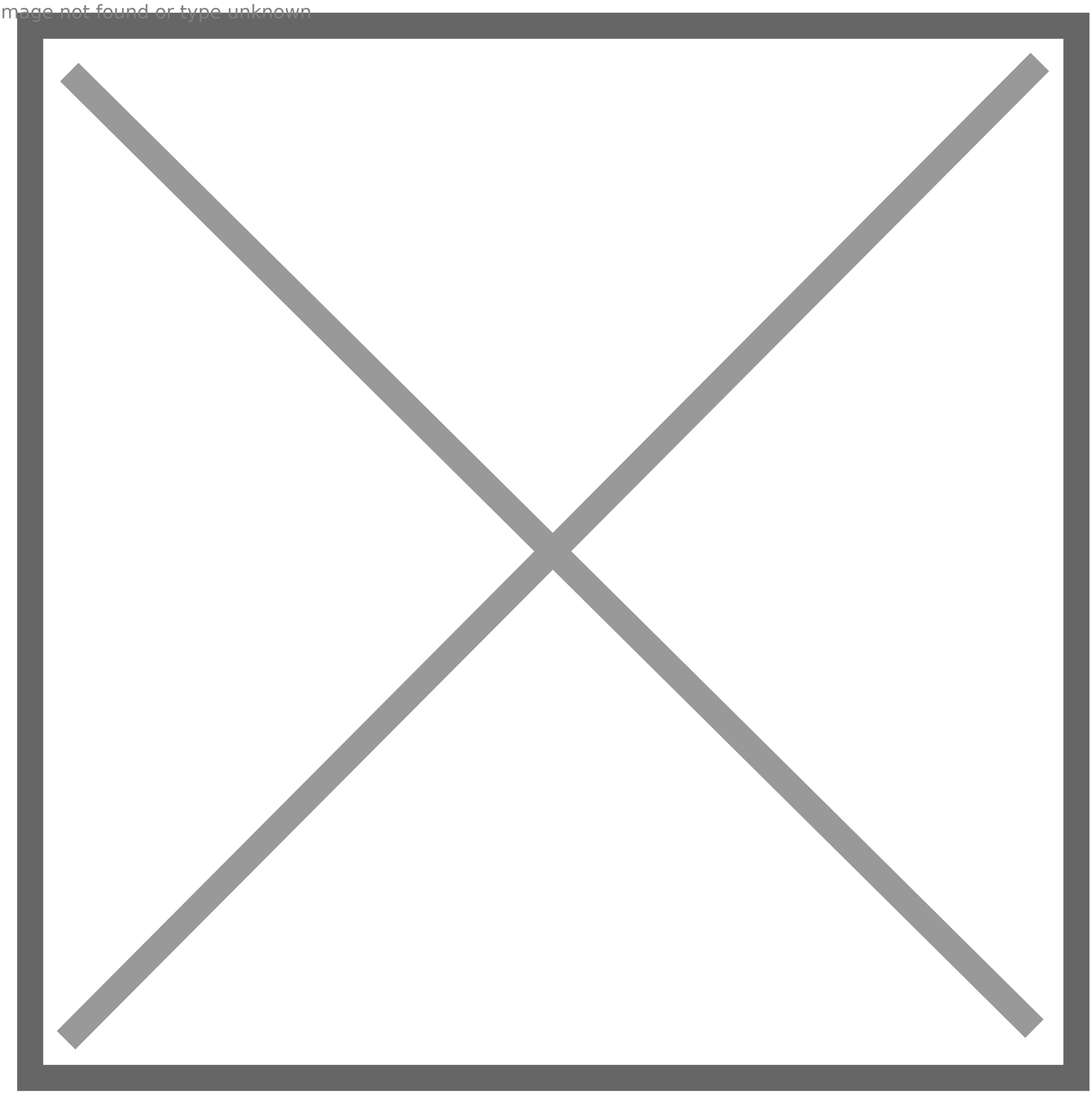
Image not found or type unknown



Create Custom Flow

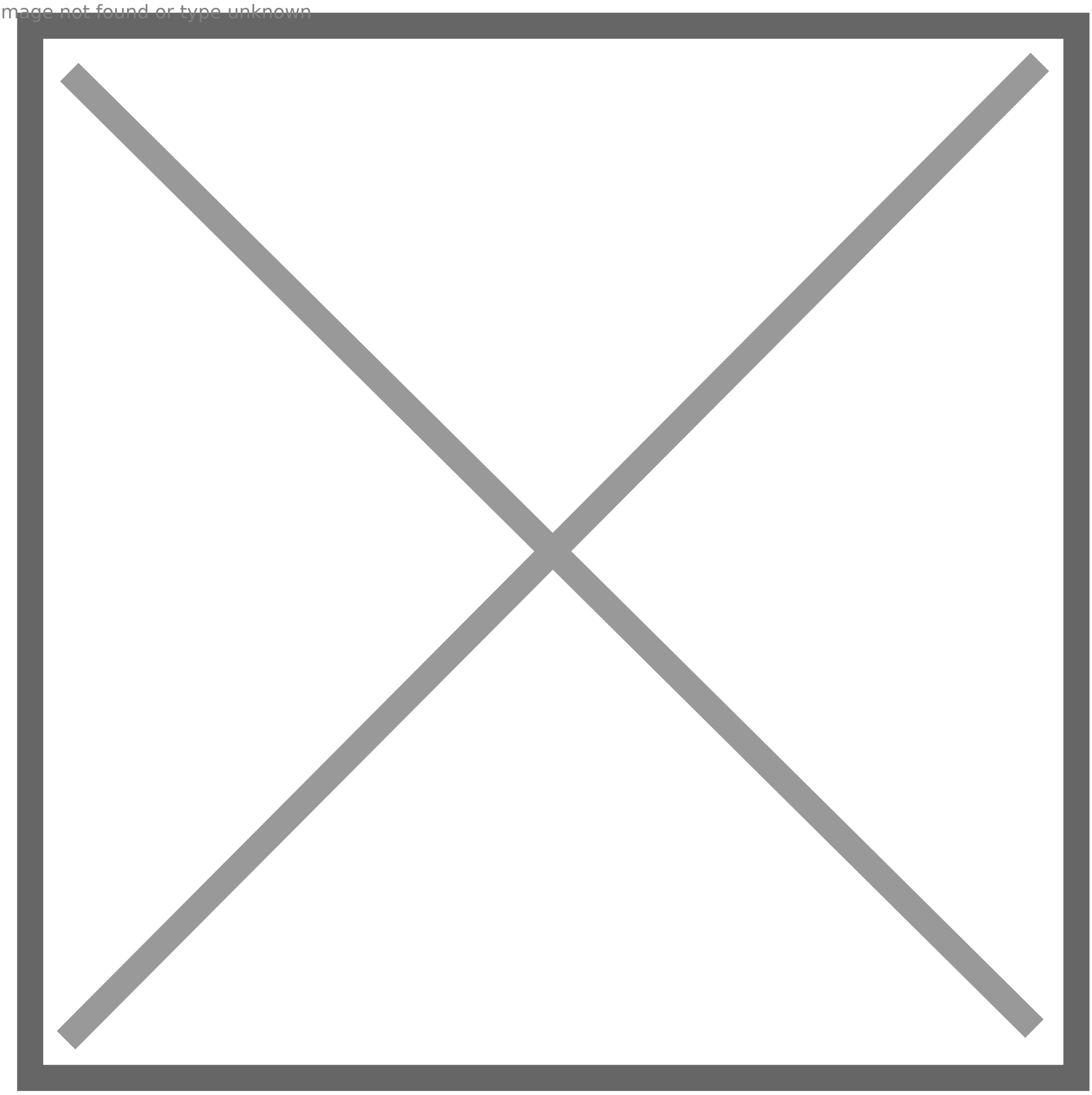
1. Create a new authentication flow under *Flows & Stage* -> *Flows* -> *Create*, and name it something meaningful like `ldap-authentication-flow`

Image not found or type unknown



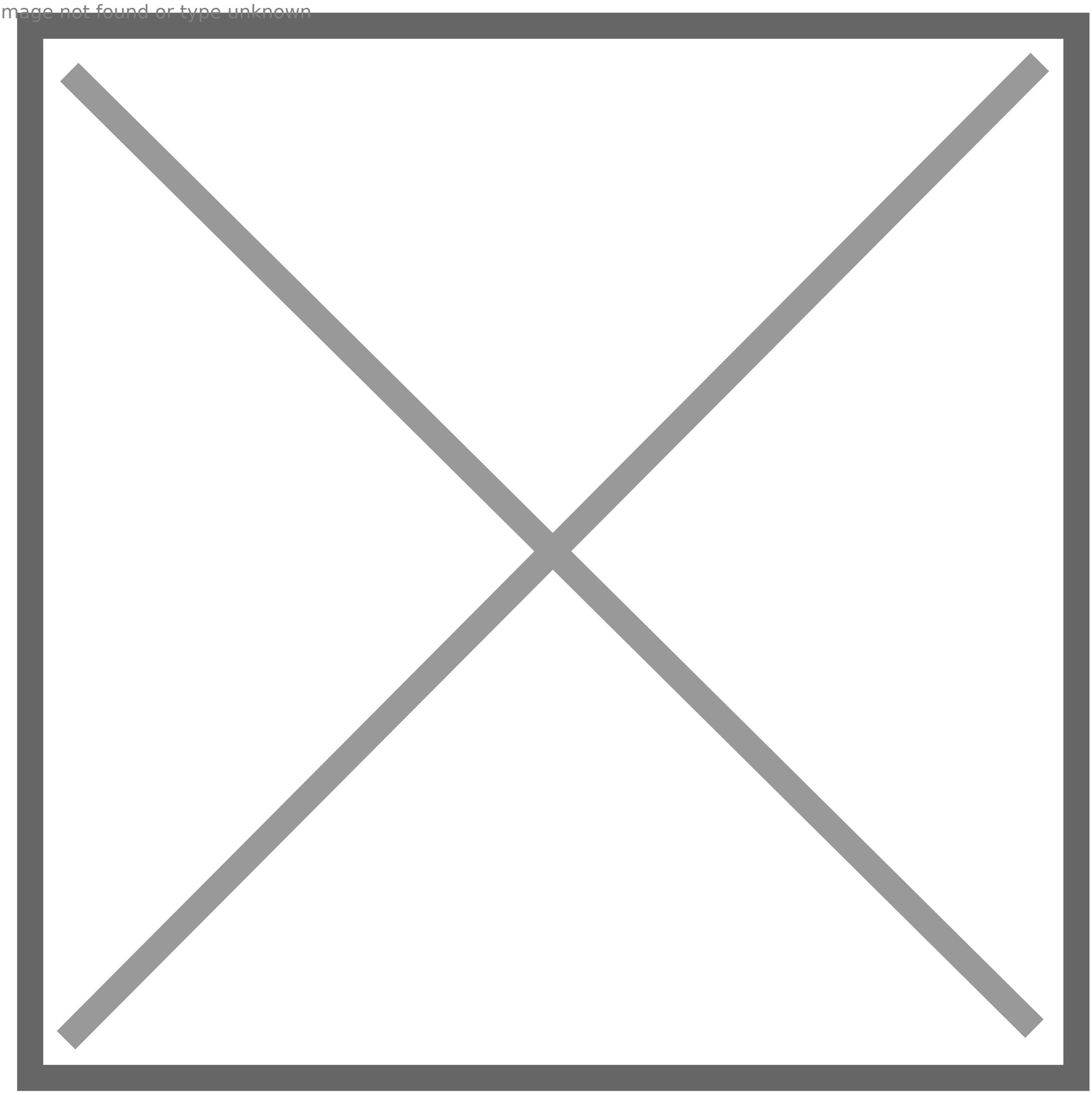
2. Click the newly created flow and choose *Stage Bindings*.

Image not found or type unknown



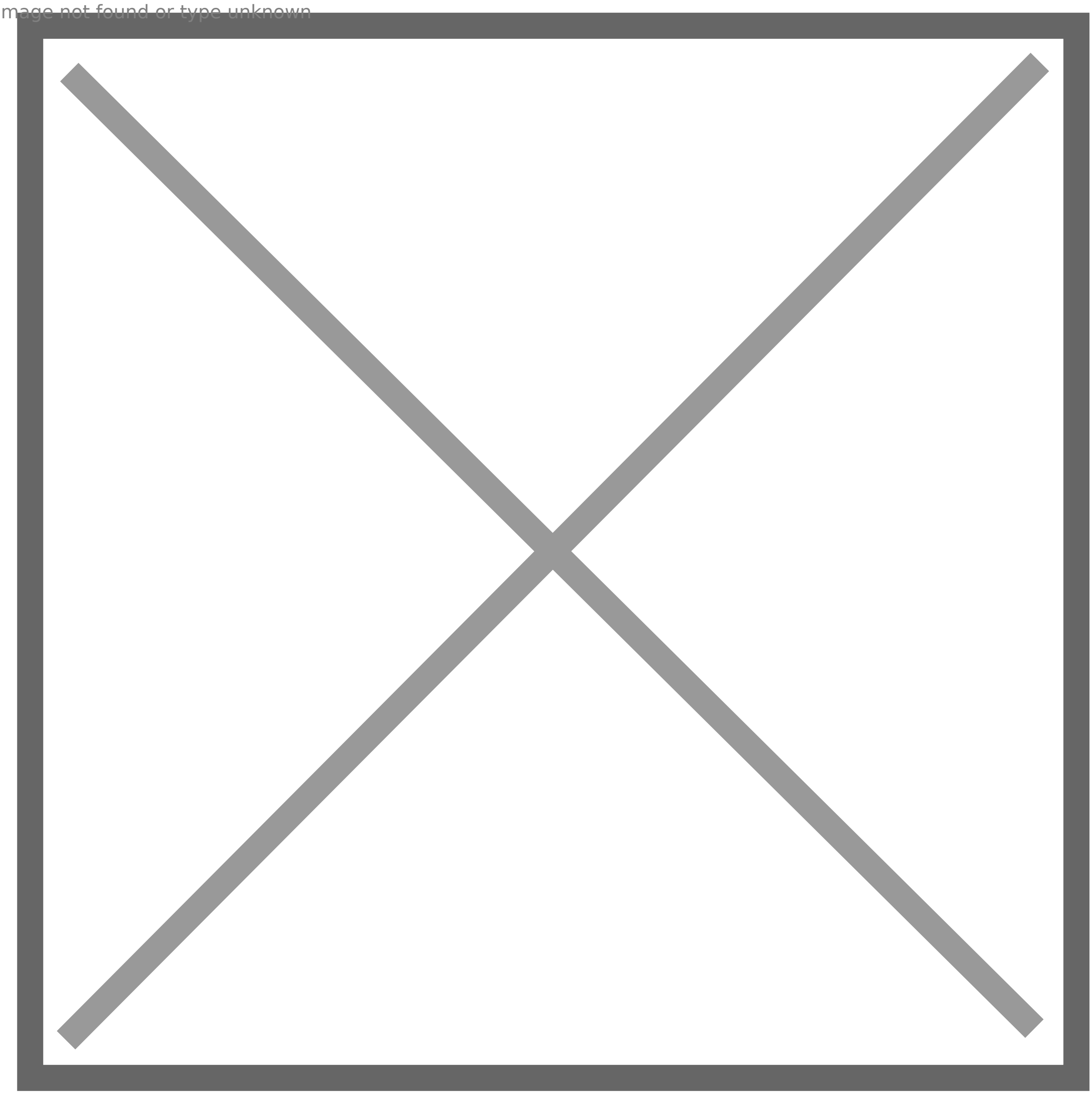
3. Click `Bind Stage` choose `ldap-identification-stage` and set the order to `10`.

Image not found or type unknown



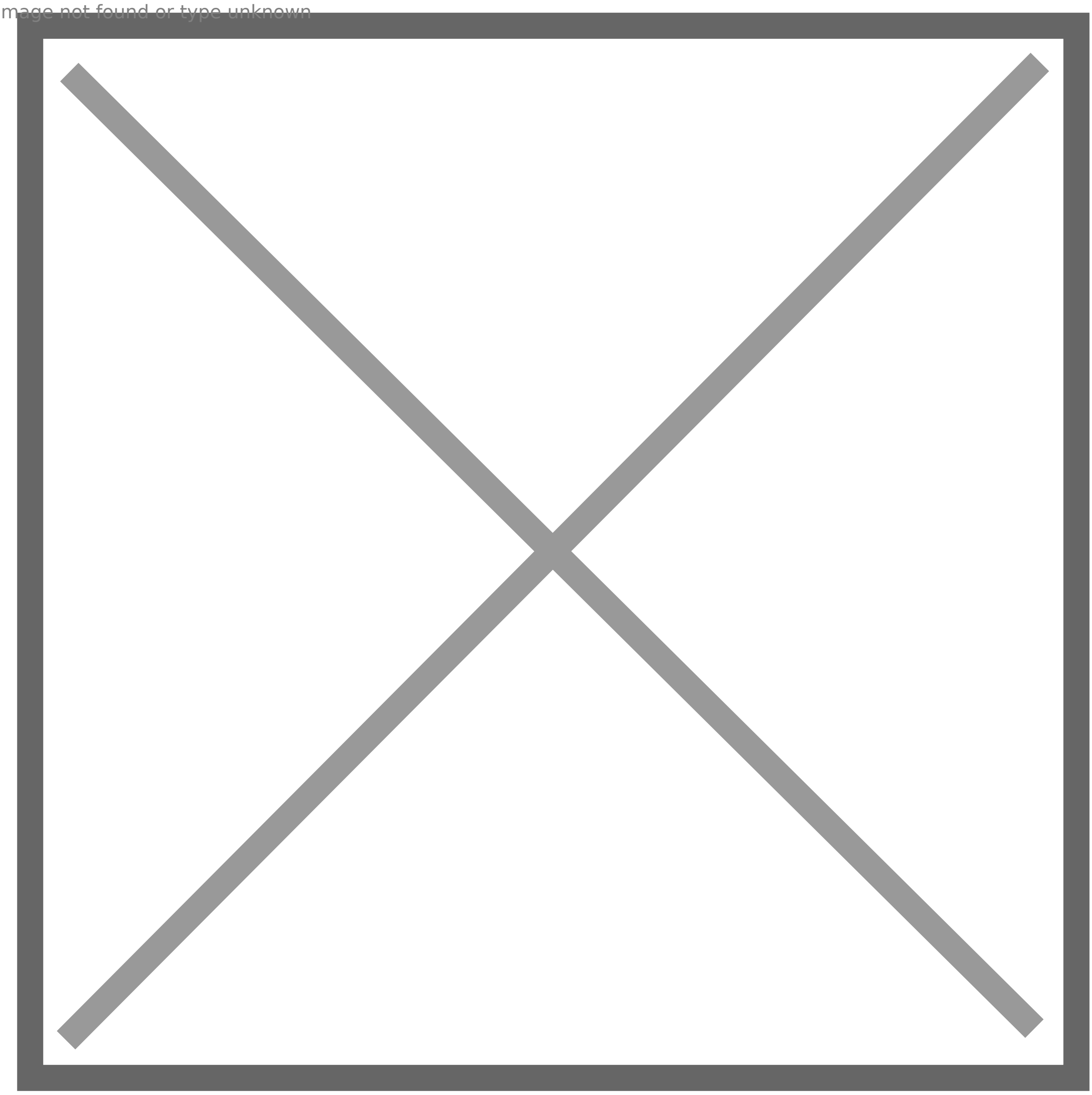
4. Click `Bind Stage` choose `ldap-authentication-login` and set the order to `30`.

Image not found or type unknown



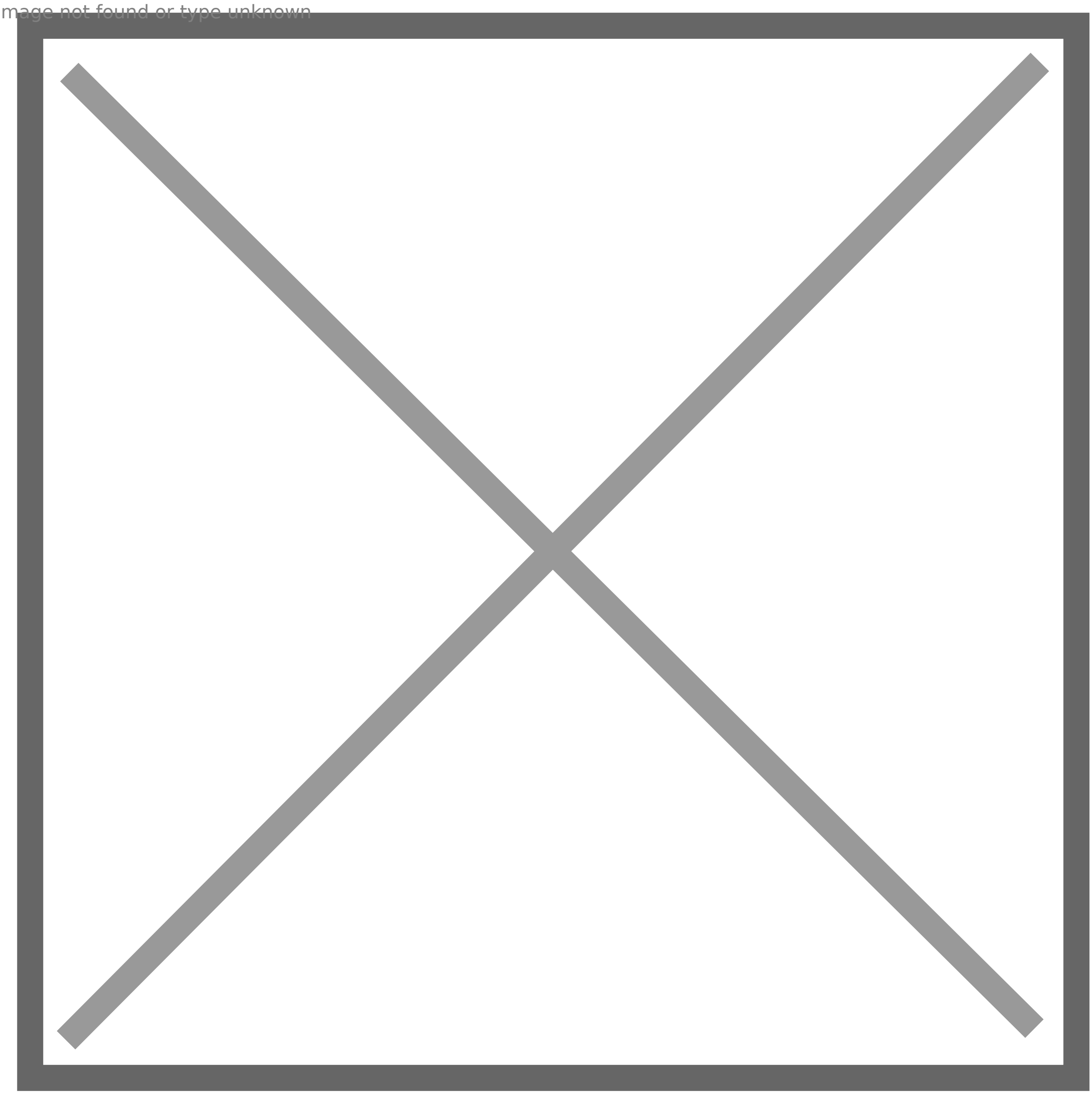
5. Edit the `ldap-identification-stage`.

Image not found or type unknown



6. Change the Password stage to `ldap-authentication-password`.

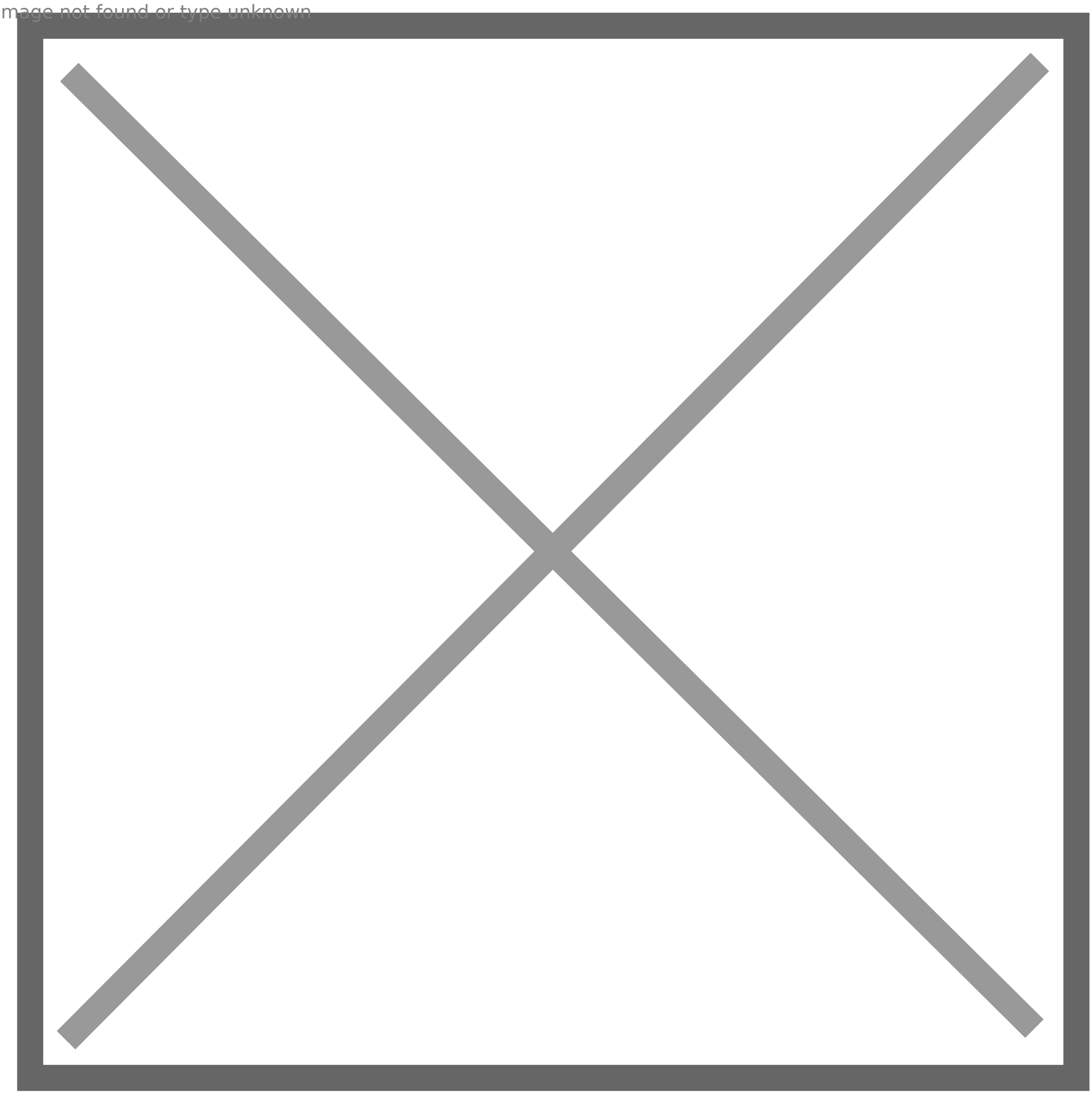
Image not found or type unknown



Create LDAP Provider

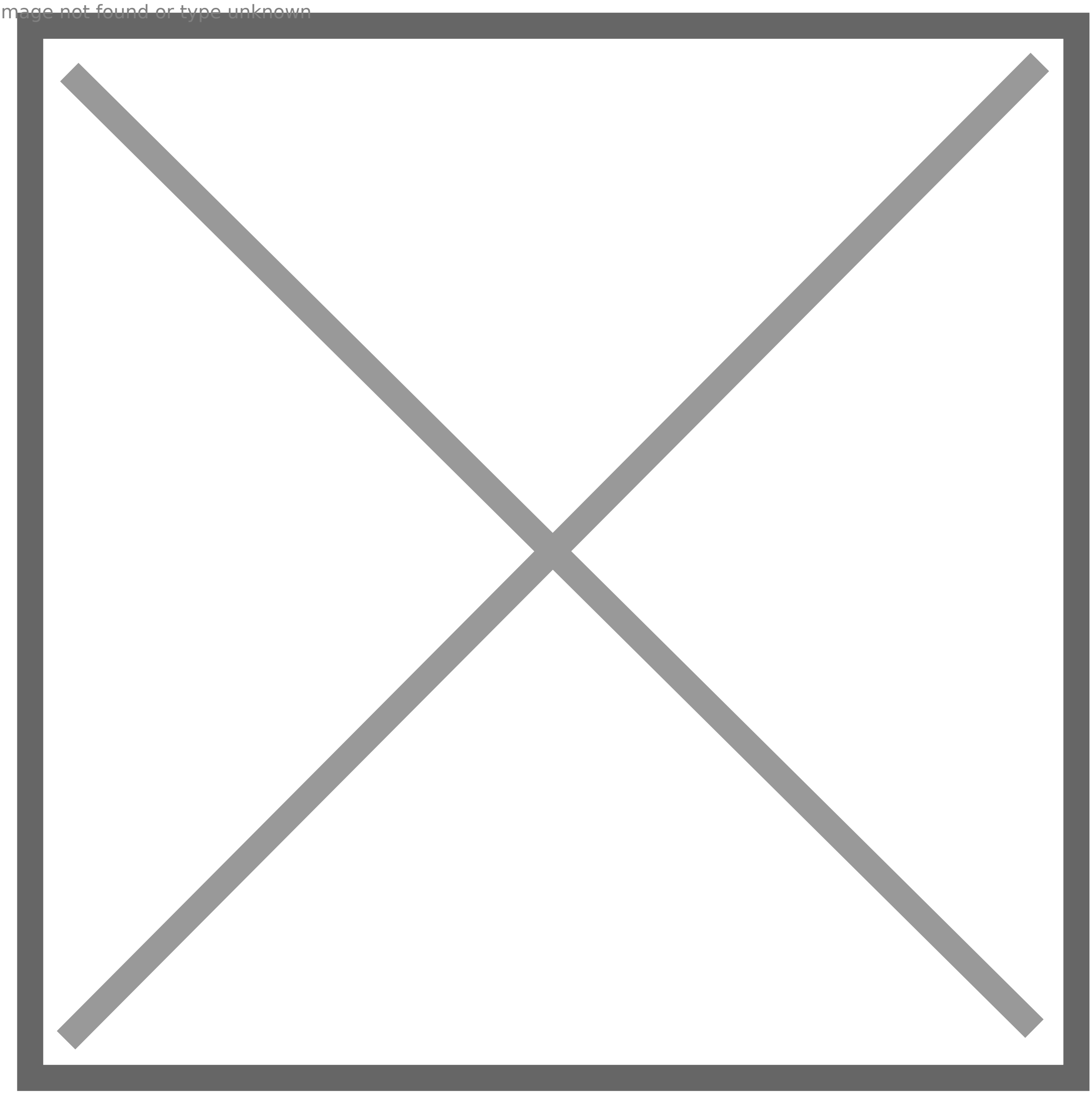
1. Create the LDAP Provider under *Applications* -> *Providers* -> *Create*.

Image not found or type unknown



2. Name is something meaningful like `LDAP`, bind the custom flow created previously (or the default flow, depending on setup) and specify the search group created earlier.

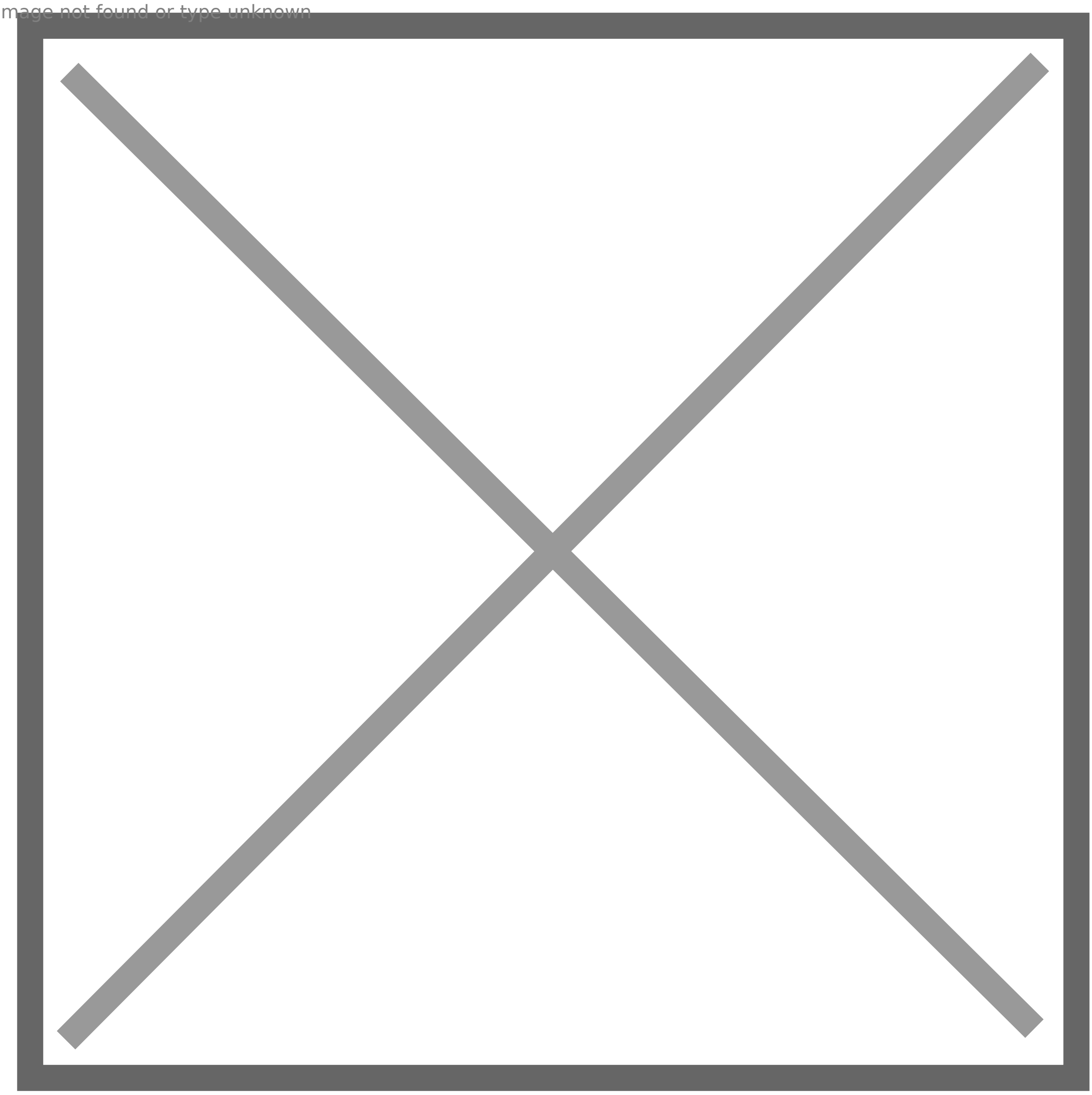
Image not found or type unknown



Create LDAP Application

1. Create the LDAP Application under *Applications* -> *Applications* -> *Create* and name it something meaningful like `LDAP`. Choose the provider created in the previous step.

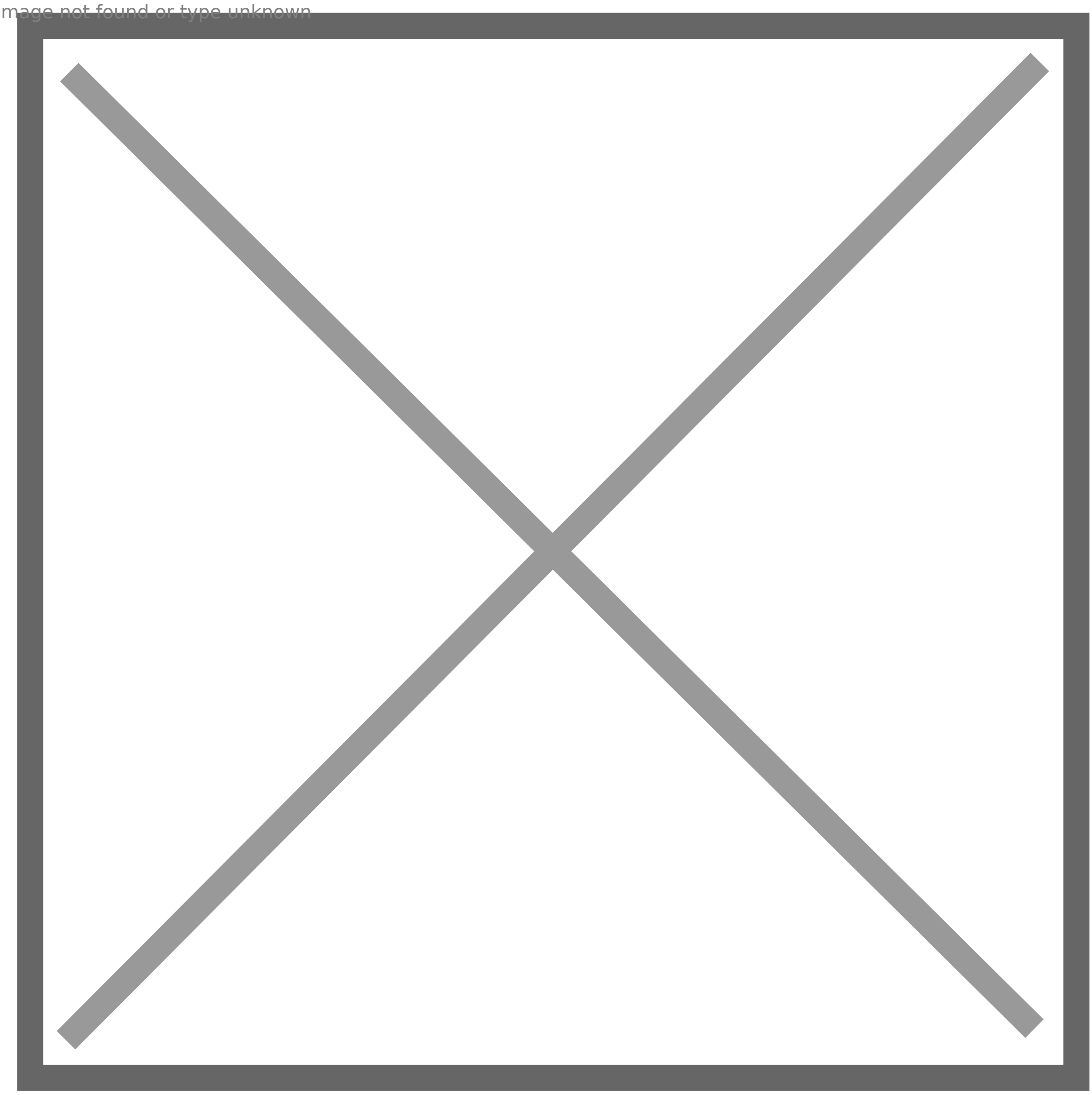
Image not found or type unknown



Create LDAP Outpost

1. Create (or update) the LDAP Outpost under *Applications* -> *Outposts* -> *Create*. Set the Type to `LDAP` and choose the `LDAP` application created in the previous step.

Image not found or type unknown



INFO
The LDAP Outpost selects different providers based on their Base DN. Adding multiple providers with the same Base DN will result in inconsistent access

ldapsearch Test

Test connectivity by using ldapsearch.

INFO
ldapsearch can be installed on Linux system with these commands

```
sudo apt-get install ldap-utils -y # Debian-based systems
sudo yum install openldap-clients -y # CentOS-based systems
```

```
ldapsearch \
  -x \
  -h <LDAP Outpost IP address> \
  -p 389 \ # Production should use SSL 636
  -D 'cn=ldapservice,ou=users,DC=ldap,DC=goauthentik,DC=io' \
  -w '<ldapuserpassword>' \
  -b 'DC=ldap,DC=goauthentik,DC=io' \
  '(objectClass=user)'
```

INFO This query will log the first successful attempt in an event in the *Events* -> *Logs* area, further successful logins from the same user are not logged as they are cached in the outpost.

Manual Outpost deployment in docker-compose

To deploy an outpost with docker-compose, use this snippet in your docker-compose file.

You can also run the outpost in a separate docker-compose project, you just have to ensure that the outpost container can reach your application container.

Proxy outpost

```
version: "3.5"

services:
    authentik_proxy:
        image: ghcr.io/goauthentik/proxy
        # Optionally specify which networks the container should be
        # might be needed to reach the core authentik server
        # networks:
```

```
    #   - foo
    ports:
      - 9000:9000
      - 9443:9443
    environment:
      AUTHENTIK_HOST: https://your-authentik.tld
      AUTHENTIK_INSECURE: "false"
      AUTHENTIK_TOKEN: token-generated-by-authentik
      # Starting with 2021.9, you can optionally set this too
      # when authentik_host for internal communication doesn't match the public URL
      # AUTHENTIK_HOST_BROWSER: https://external-domain.tld
```

LDAP outpost

```
version: "3.5"

services:
  authentik_ldap:
    image: ghcr.io/goauthentik/ldap
    # Optionally specify which networks the container should be
    # might be needed to reach the core authentik server
    # networks:
    #   - foo
    ports:
      - 389:3389
      - 636:6636
    environment:
      AUTHENTIK_HOST: https://your-authentik.tld
      AUTHENTIK_INSECURE: "false"
      AUTHENTIK_TOKEN: token-generated-by-authentik
```

Tutorials

Steps to configure SAML 2.0 SSO with Microsoft Active Directory Federation Services

PRODUCTS: Learn

Note: ADFS 2.0 on Windows Server 2008 r2 or ADFS 3.0 on Windows Server 2012 / 2012 r2)

SAML 2.0 single sign-on (SSO) supports integration with Microsoft Active Directory Federation Services (ADFS) 3.0.

Requirements

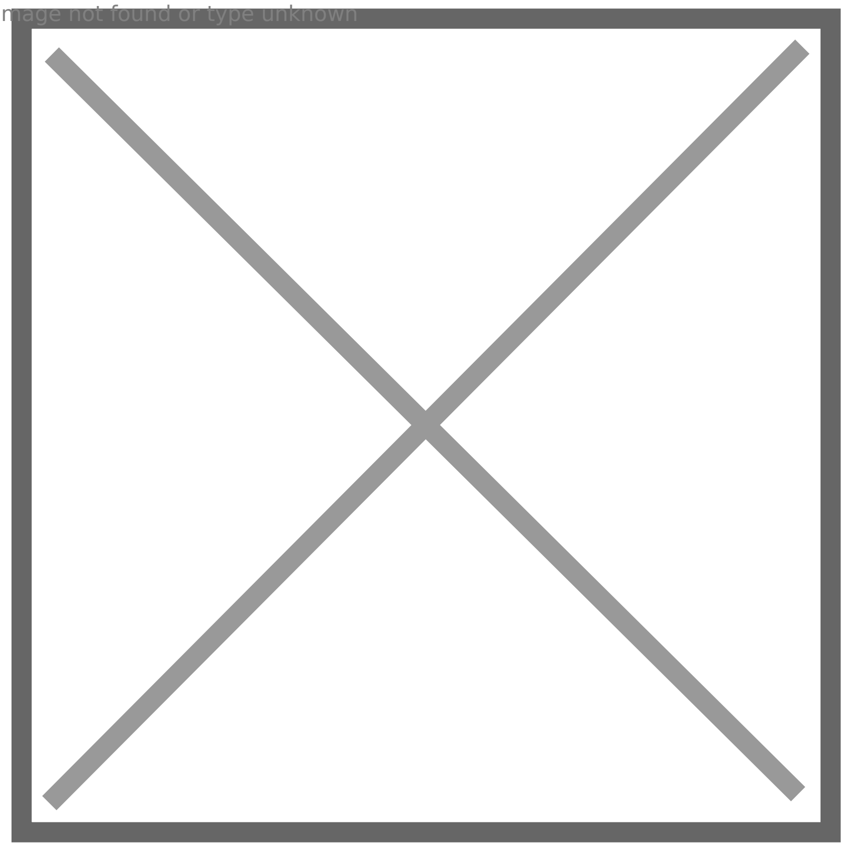
- A fully installed and configured ADFS service.
- A server running Microsoft Server 2008r2 or 2012/2012r2
- An SSL certificate to sign your ADFS login page and the thumbprint of that certificate

In this example we are using ADFS 2.0 on Windows Server 2008 R2. On Windows Server 2012 the steps will be the same except for the installation, because you install AD FS role via the server manager, not via the installation package as on Windows 2008 server r2.

Step 1. AD FS Management

Login in to your AD FS server and launch the ADFS Management Console via the shortcut in Control Panel\Administrative Tools.

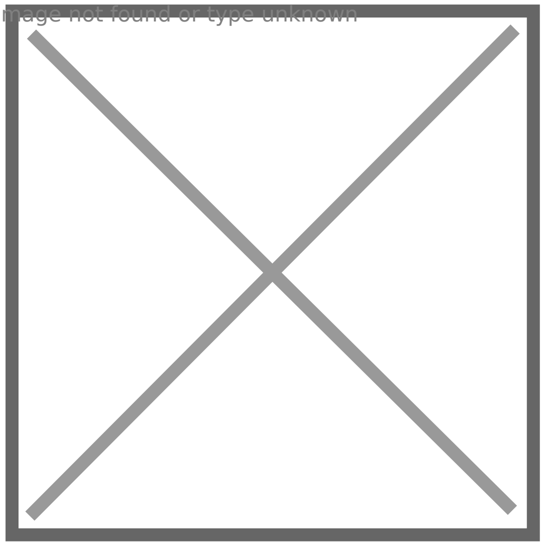
Image not found or type unknown



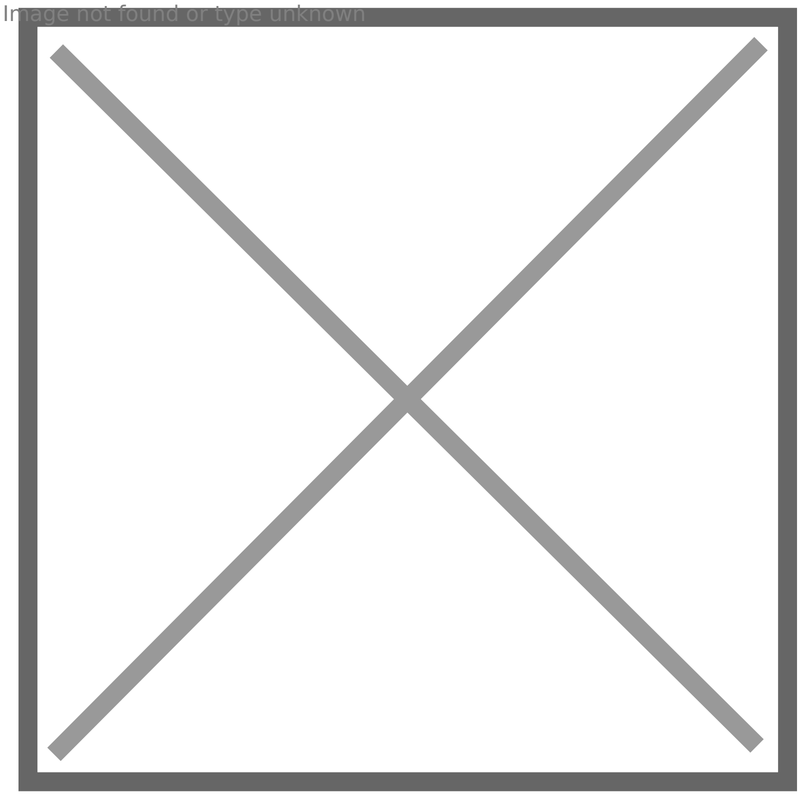
Step 2. Check AD FS settings

Right-click on Service and sel ect Edit Federation Service Properties...

Image not found or type unknown



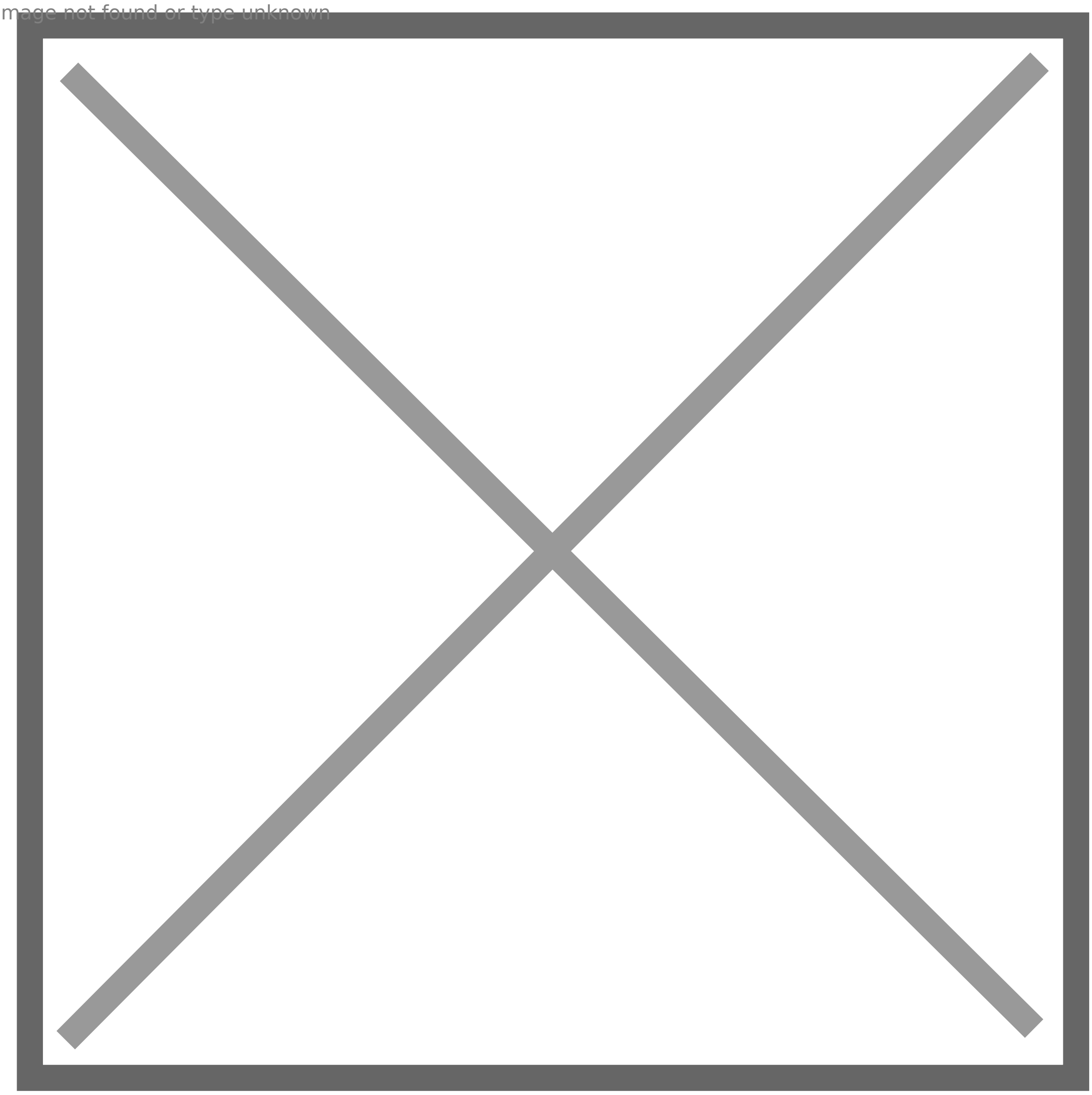
Confirm that the General settings match your DNS entries and certificate names. Make a note with the Federation Service Identifier, since that is used in the iSpring Learn SAML 2.0 configuration settings.



Step 3. Token-Signing certificate

1. Browse to the certificates.
2. Right-click on the certificate and sel ect View Certificate.
3. Go to the Details tab.
4. Find the Thumbprint field and copy the contents of this field to the Windows clipboard.

Image not found or type unknown



Step 4. Learn Settings

1. Log in into your iSpring Learn account and go to the SSO settings via this link: https://YourAccountURL.ispringlearn.com/settings/sso
2. Ins ert your Thumbprint into the Certificate Fingerprint field and remove all spaces between characters.
3. Enter your data to the Metadata URL, Sign ON URL and Logout URL fields.

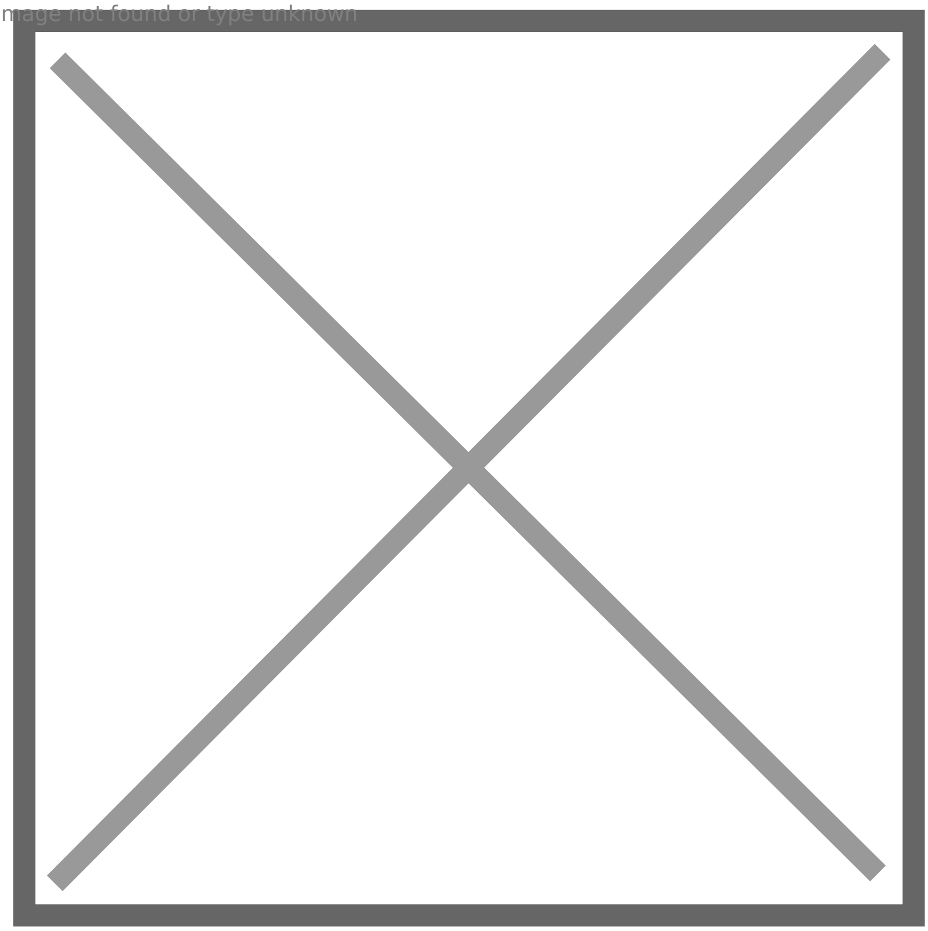
SAML01.png

Image not found or type unknown

Step 5. ADFS Relying Party Configuration

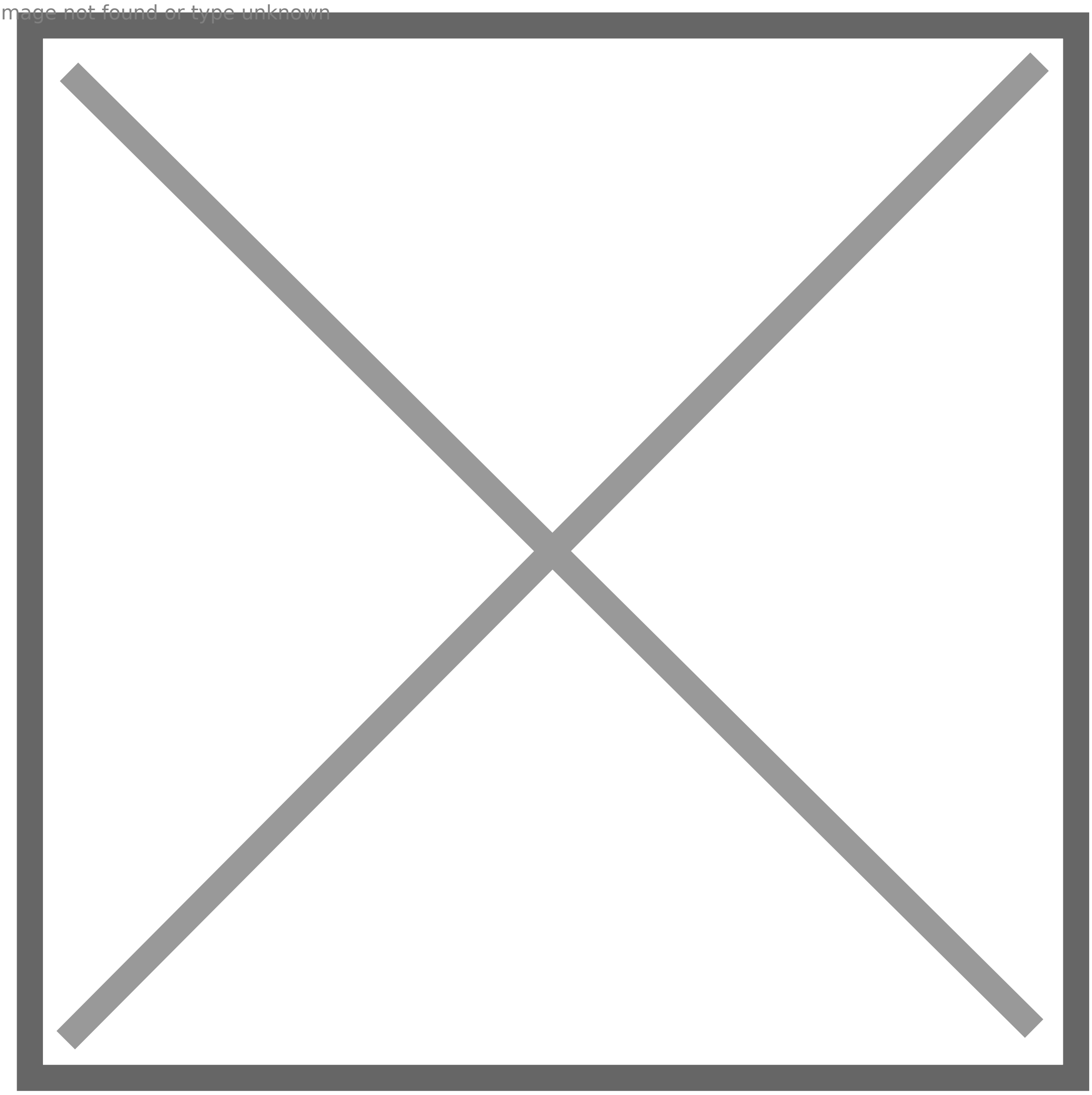
Go to the ADFS Management console and select Relying Party Trusts, right-click on it and select Add Relying Party Trust…

Image not found or type unknown



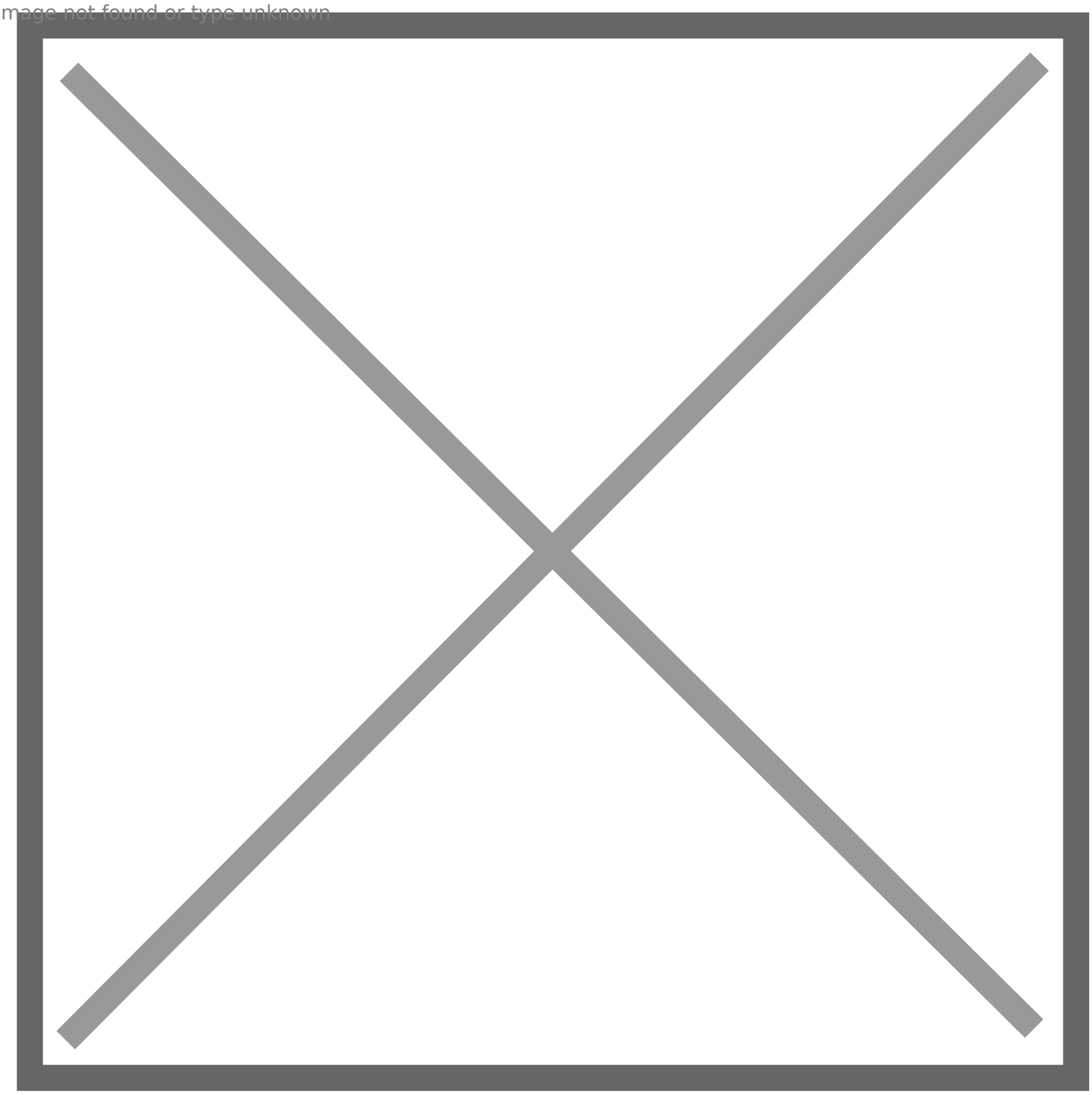
Select Next On the Welcome Screen of the wizard, and on the Select Data Source step, select the last option: Enter data about the relying party manually.

Image not found or type unknown



On the next screen, enter a Display name that you will recognize in the future.

Image not found or type unknown

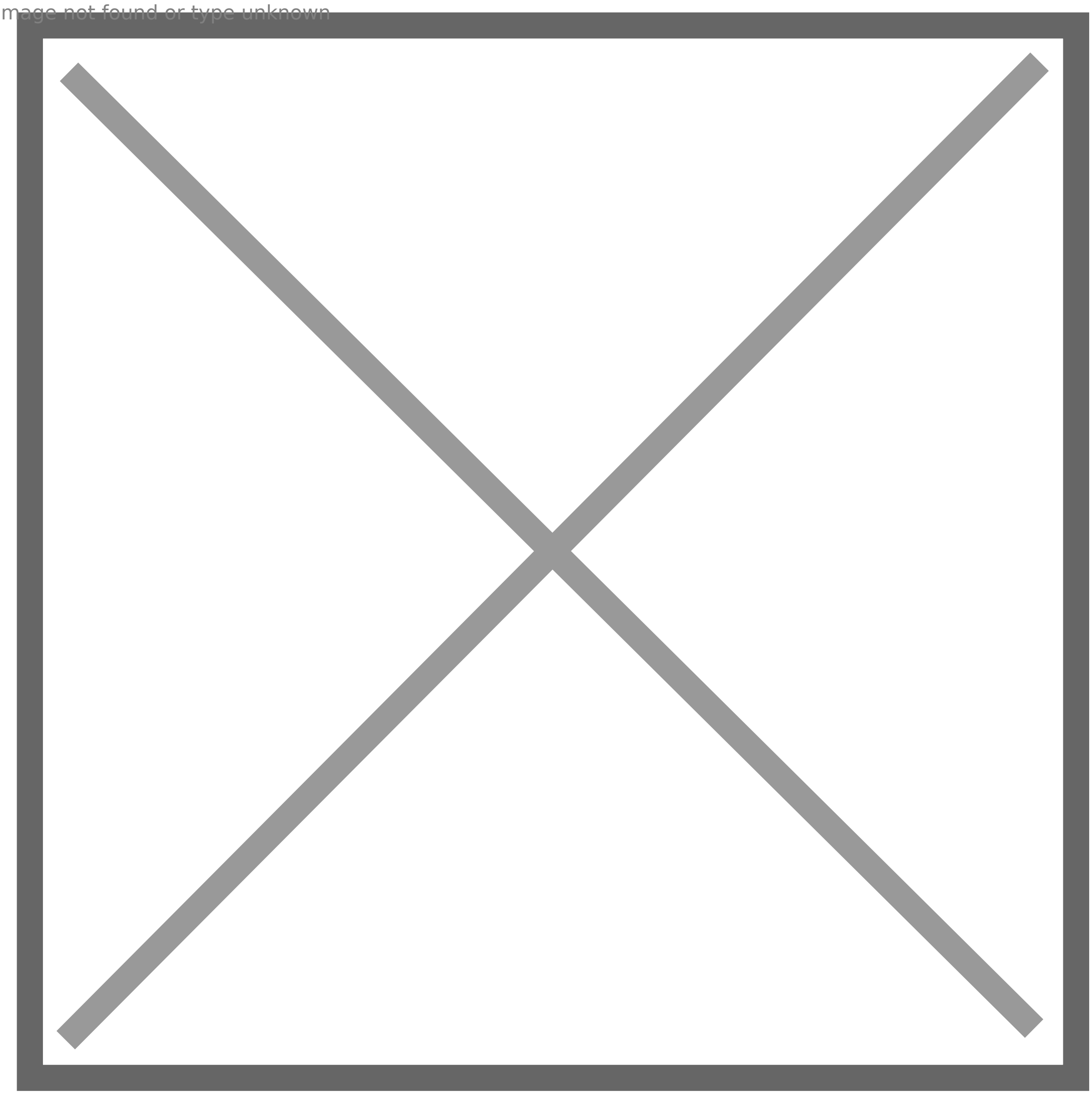


Next, select AD FS profile:

Image not found or type unknown

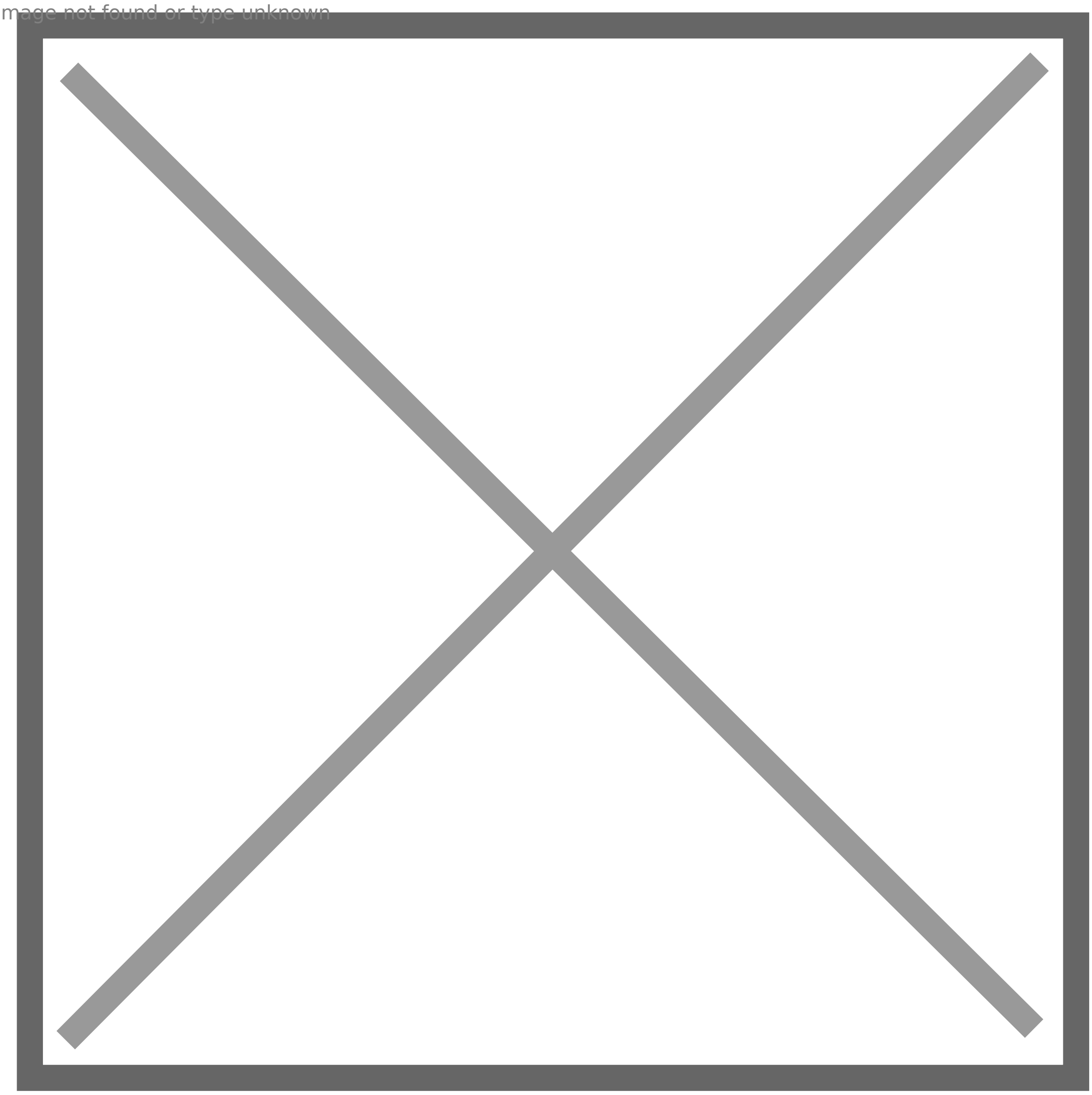
Leave the default values:

Image not found or type unknown



On the next screen, check the box labeled: Enable support for the SAML 2.0 WebSSO protocol. The service URL will be: https://YourAccountURL.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp

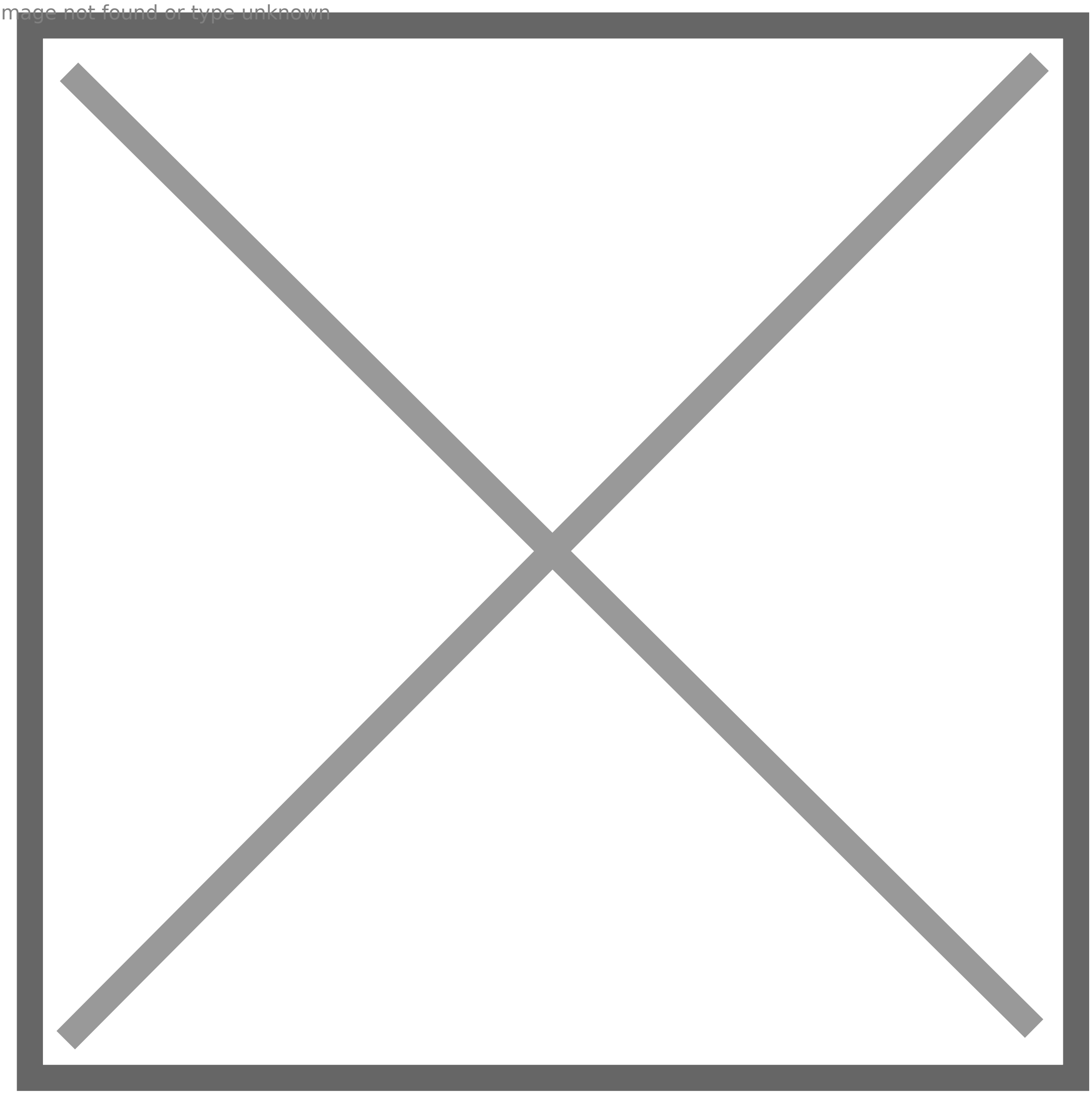
Image not found or type unknown



Click Next. Add Relying party trust identifier:

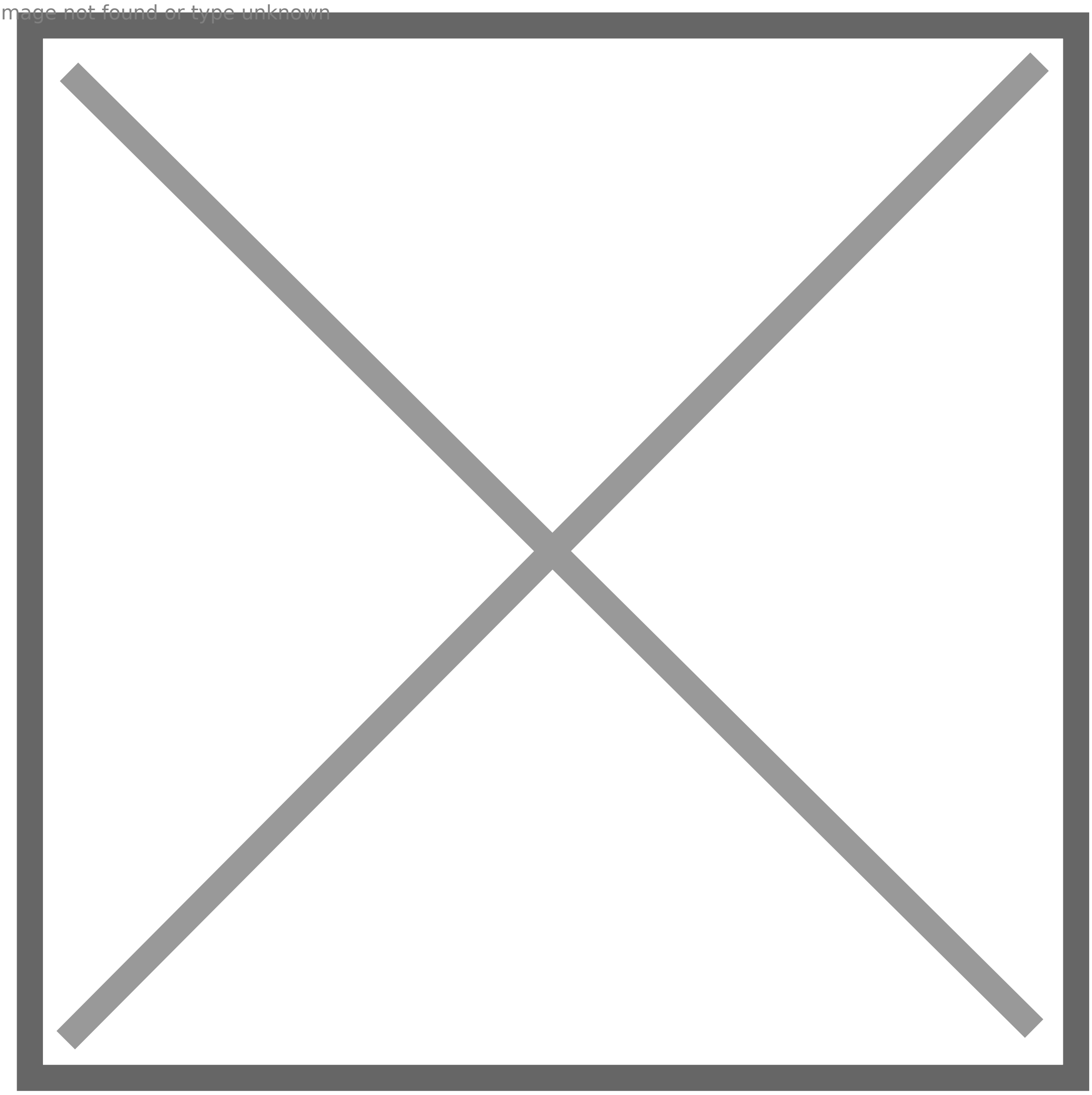
https://YourAccountURL.ispringlearn.com/module.php/saml/sp/metadata.php/default-sp

Image not found or type unknown



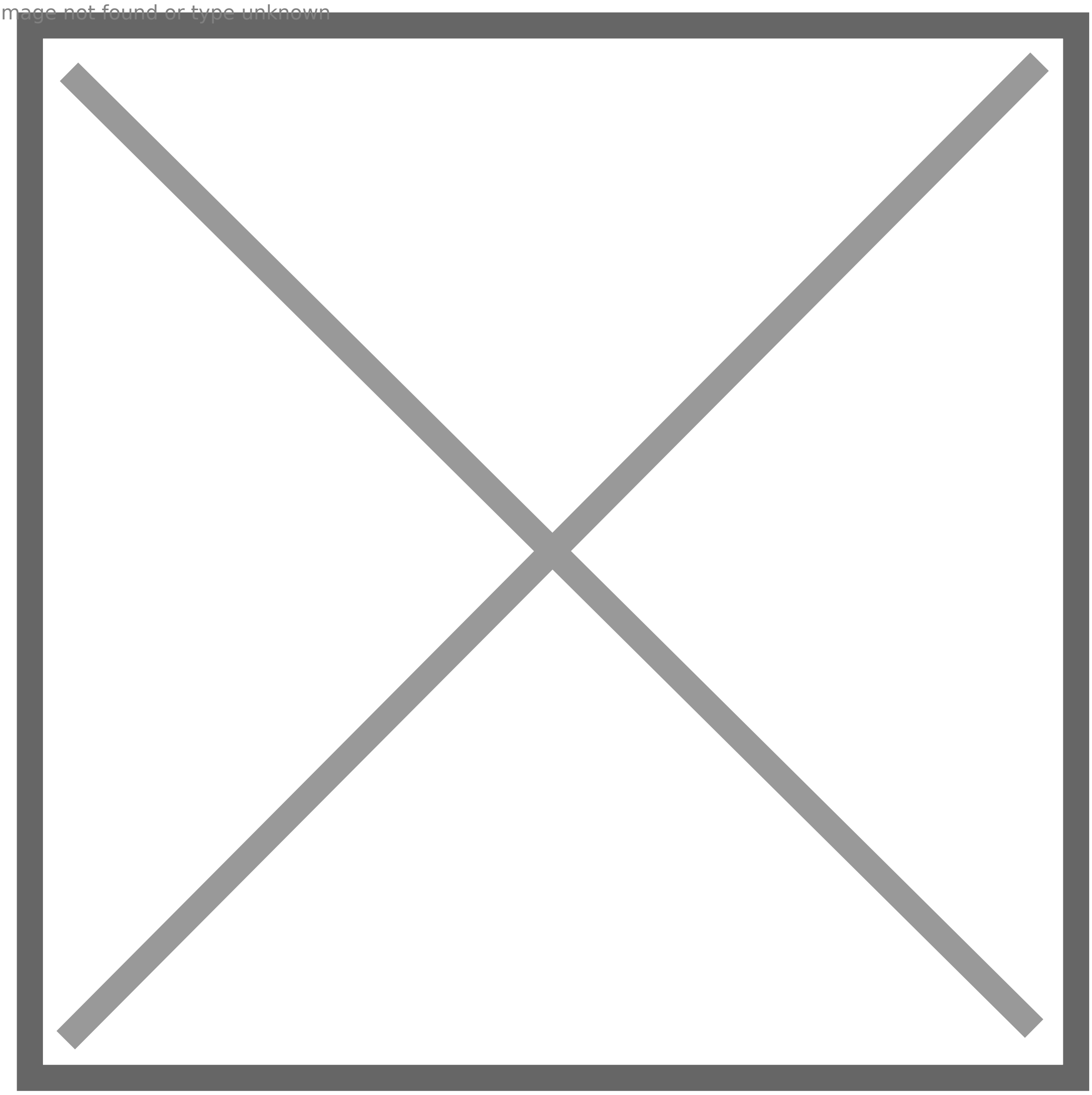
Choose Permit all users to access this relying party.

Image not found or type unknown



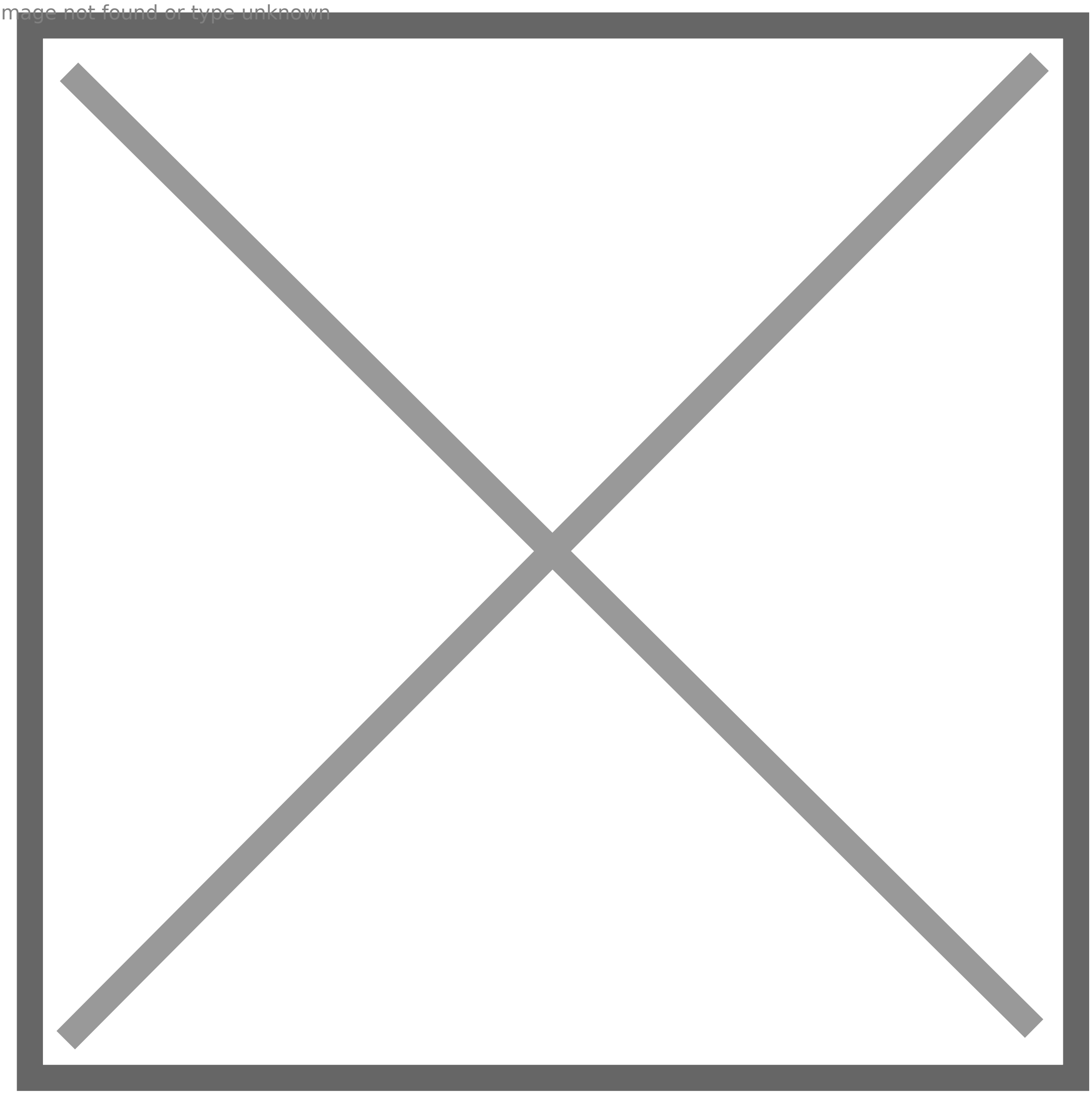
On the next step, just click Next.

Image not found or type unknown



On the final screen, check the box Open the Edit Claim Rules dialog and use the Close button to exit.

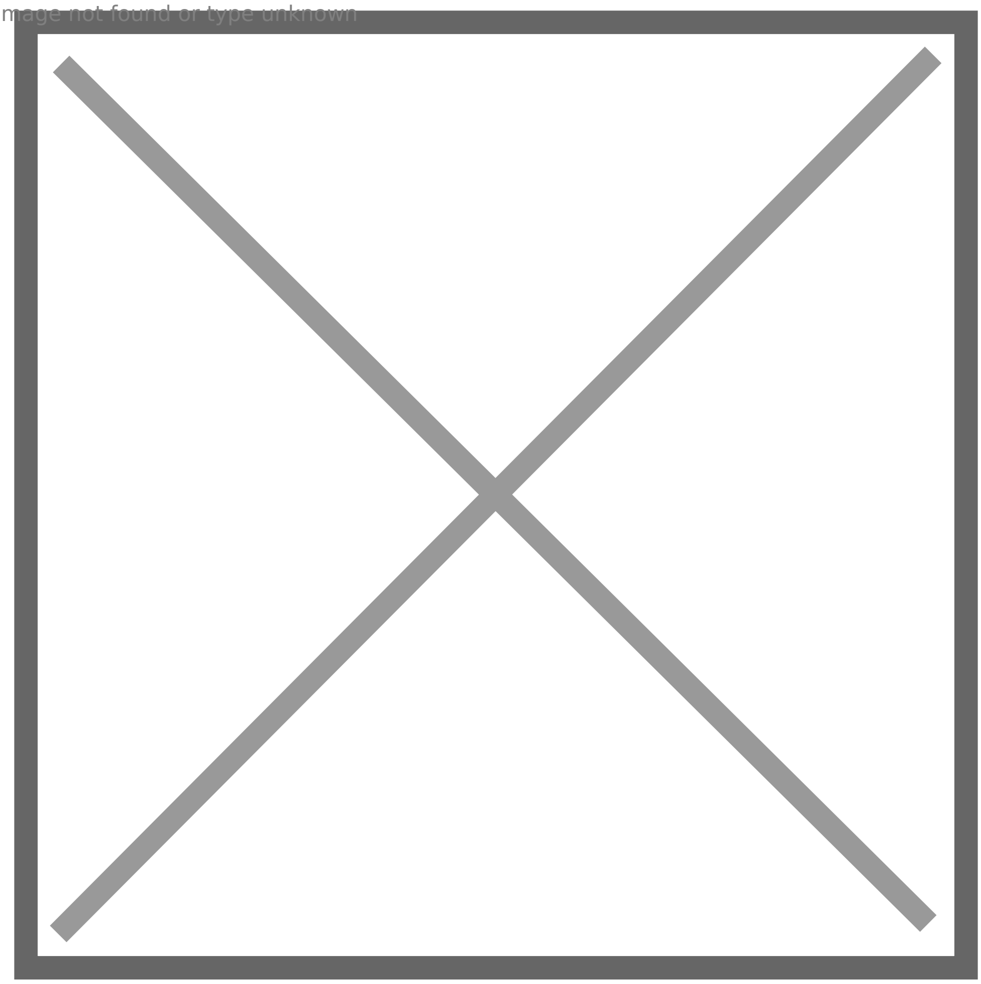
Image not found or type unknown



Step 6. Creating Claims Rules

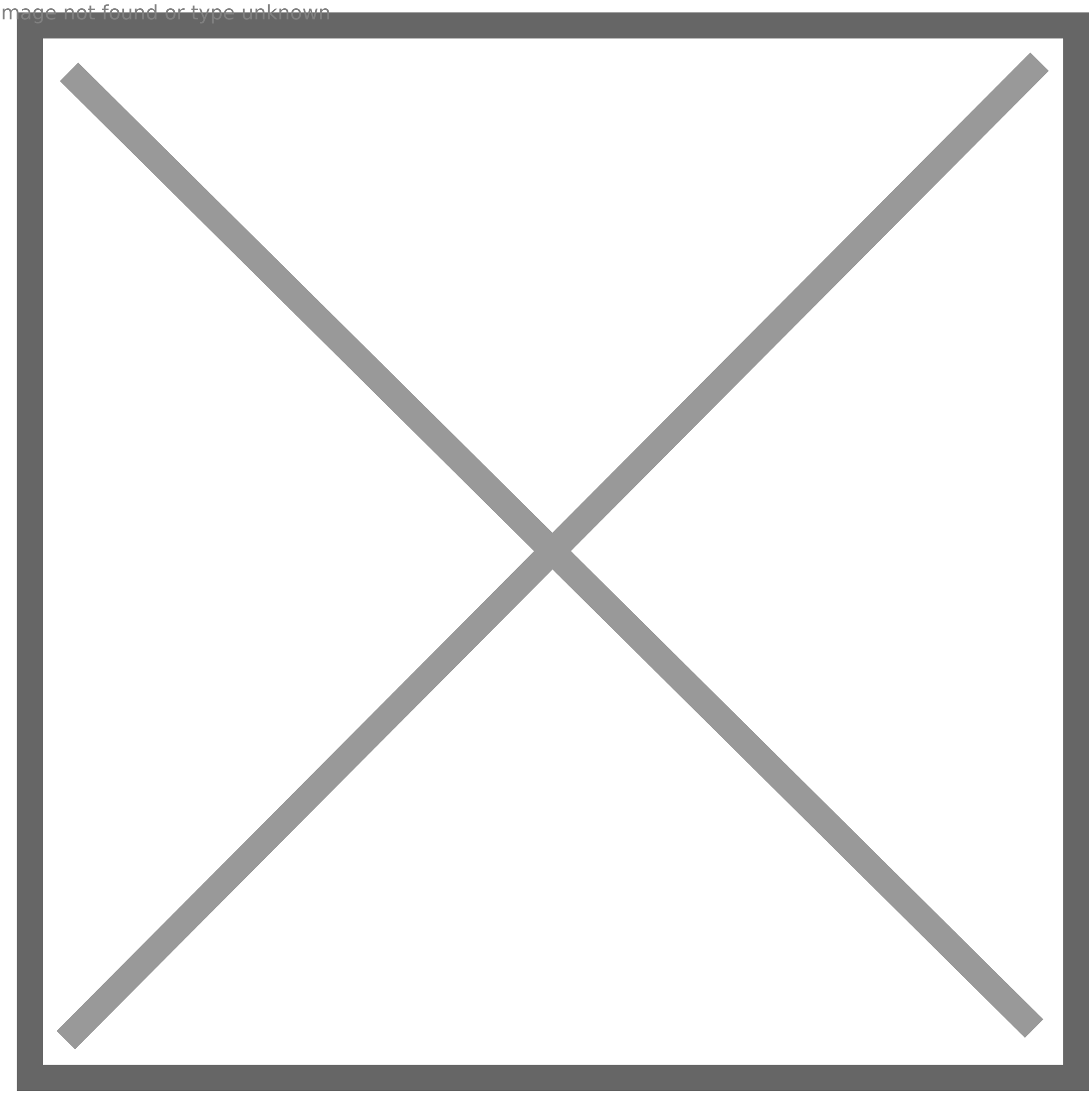
1. Add the first rule

Image not found or type unknown



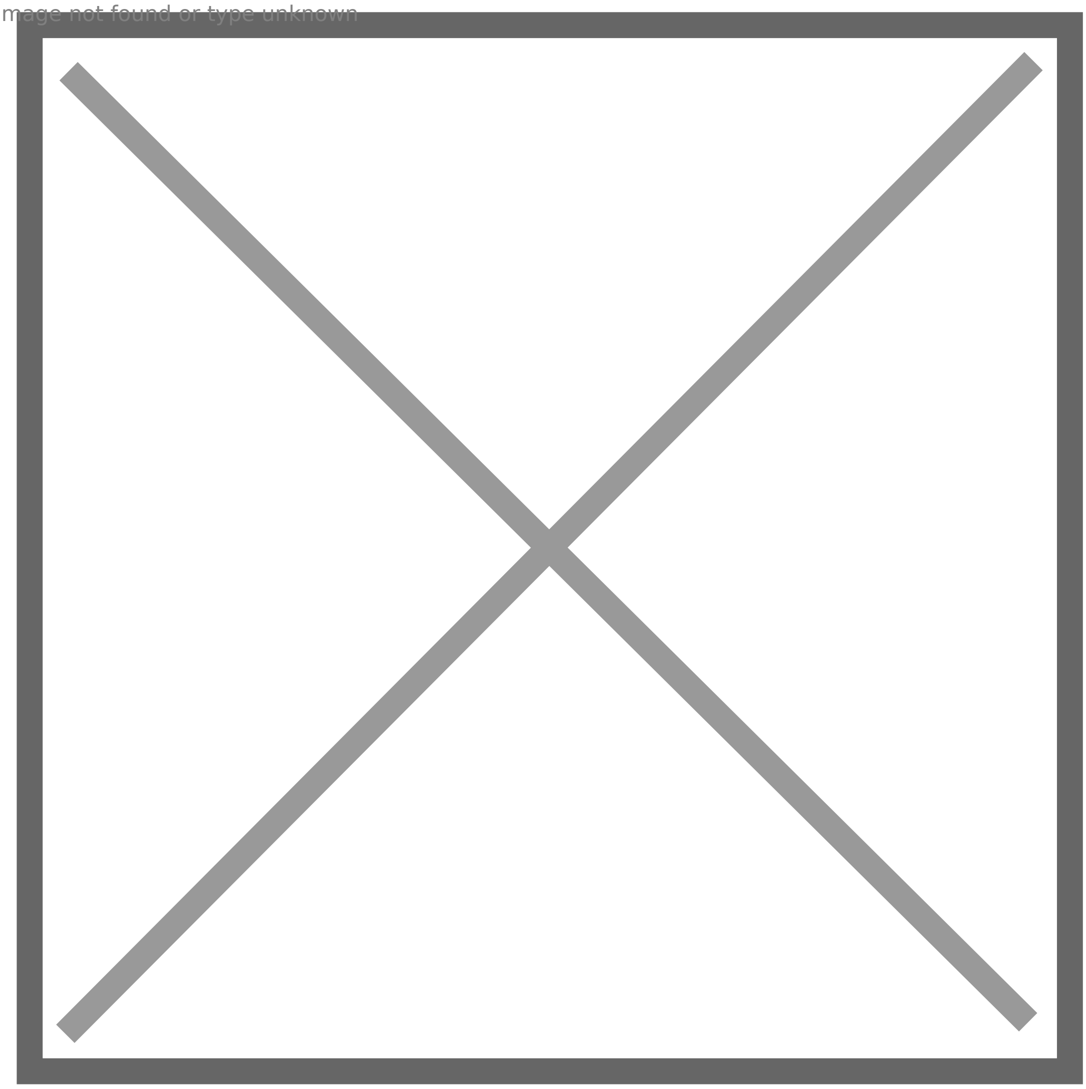
2. Select Send LDAP Attributes as Claims

Image not found or type unknown



3. On the next screen, specify your Claim Rule, for Example E-mail to Learn, using Active Directory as your attribute store, and do the following:
   - Fr om the LDAP Attribute column, select E-Mail Addresses
   - Fr om the Outgoing Claim Type, enter “email”

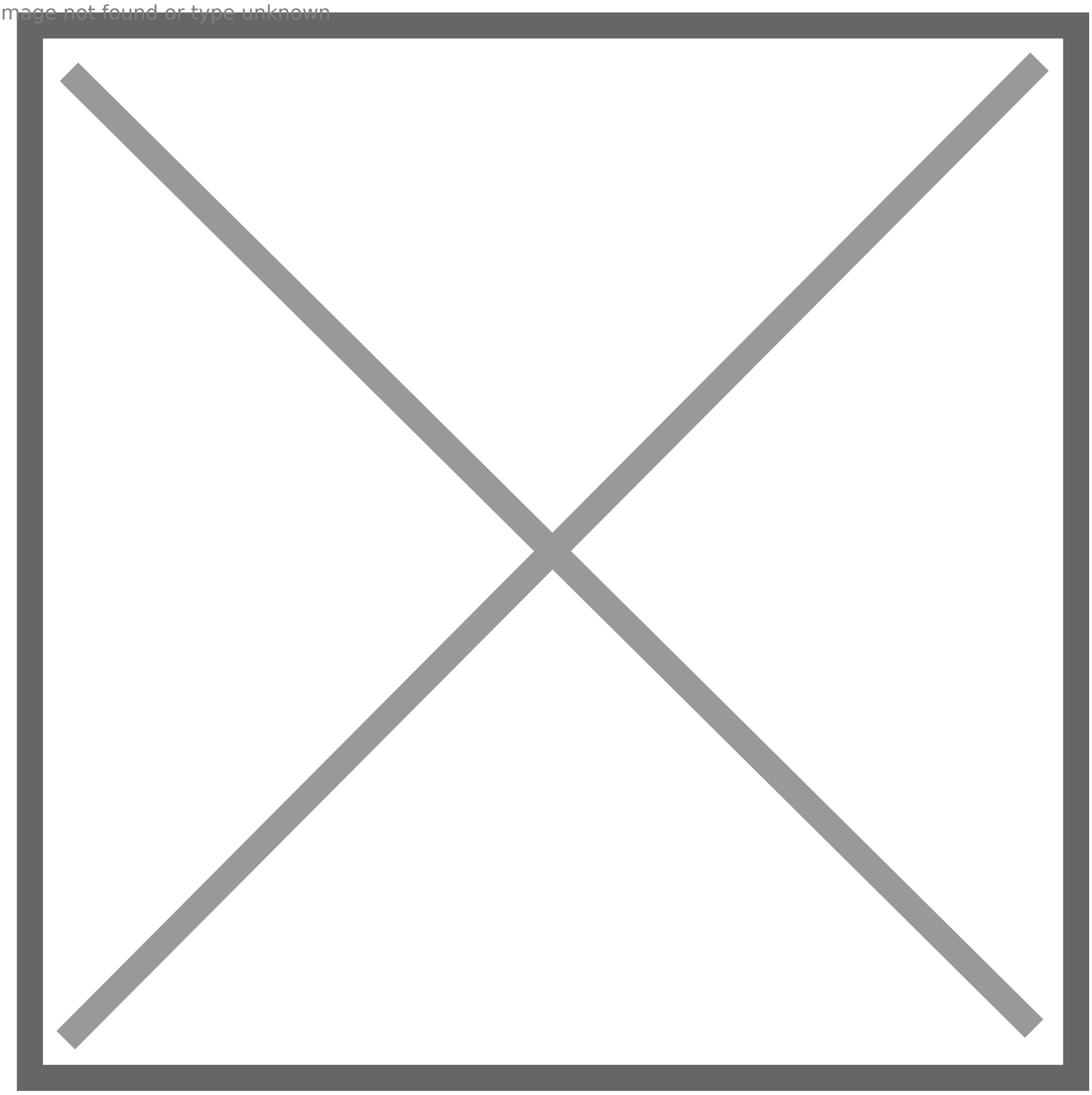
Image not found or type unknown



- Click on Finish or OK to save the new rule

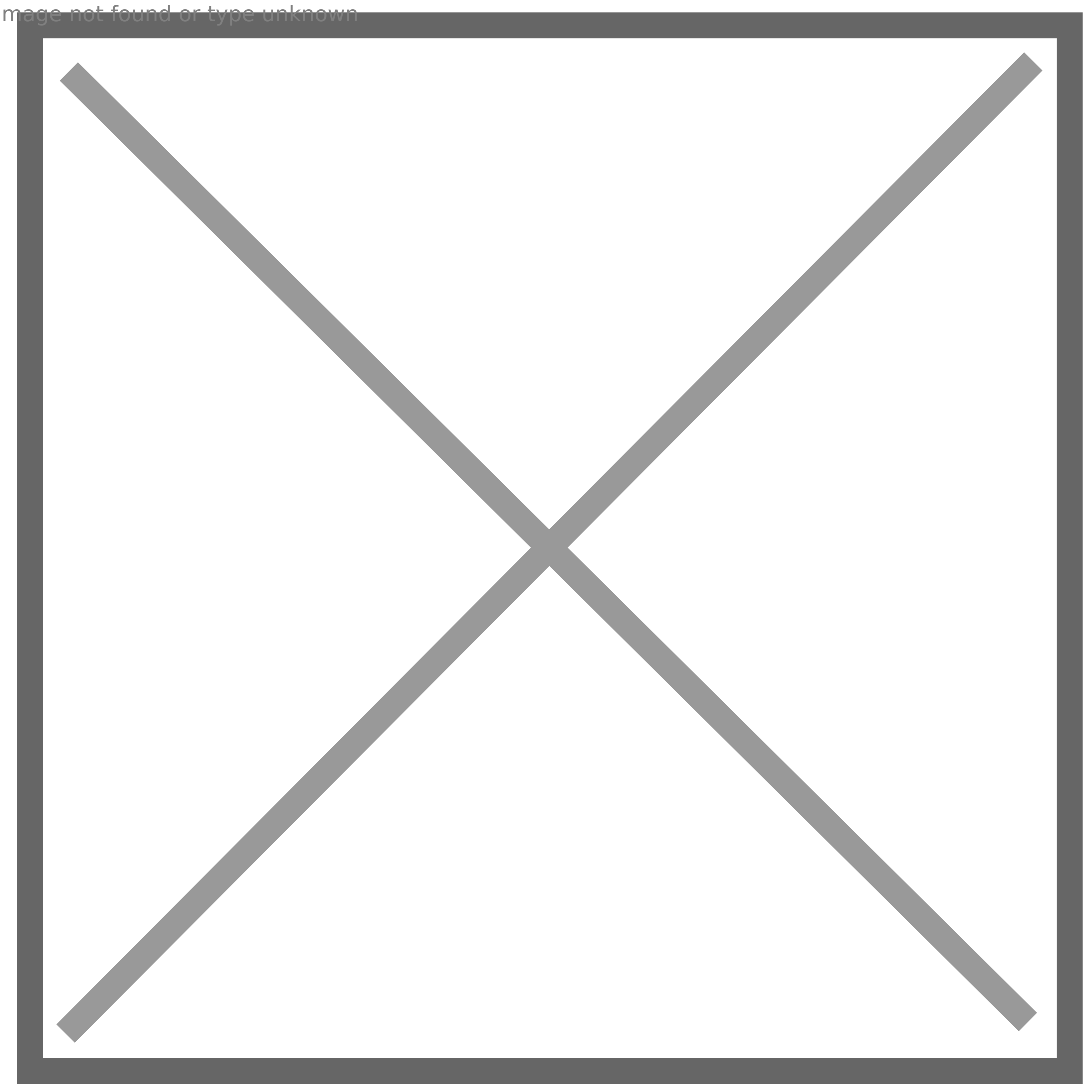
4. After that, add the second rule and select Transform an Incoming Claim as the template

Image not found or type unknown



- Give your Claim Rule a title, for example, Transform Account Name
- Select Windows account name as the Incoming Claim Type
- Under Outgoing Claim Type, select Name ID
- Under Outgoing Name ID Format, select Transient Identifier
- Leave the default rule Pass through all claim values

Image not found or type unknown



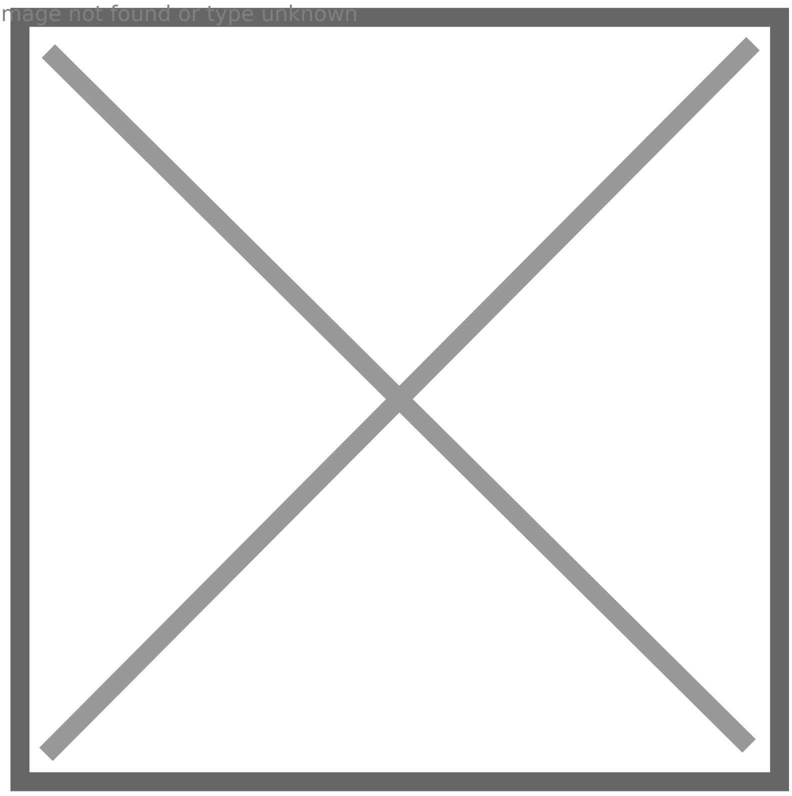
5. Finally, click on OK to create the claim rule, and then OK again to finish creating rules.

Step 7. Adjusting the Trust Settings

Some settings on your Relying Party Trust will need to be adjusted. To access these settings, select Properties from the Actions sidebar on the right while you have the Relying Party Trust selected.

- Under the Advanced tab, make sure that the selection is SHA-1

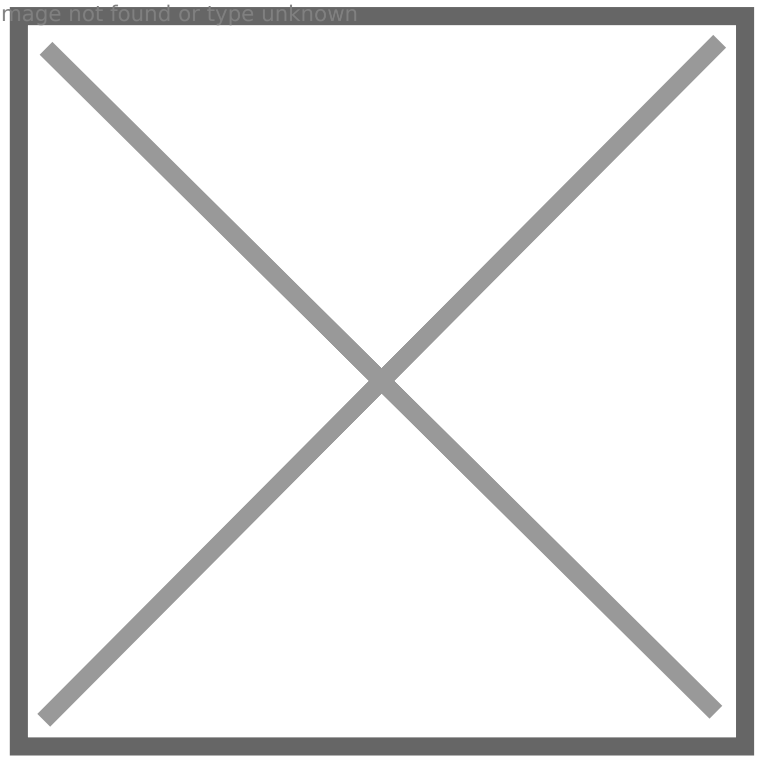
Image not found or type unknown



- Under the Endpoints tab, click ADD to add a new endpoint
- For the Endpoint type, select SAML Assertion Consumer
- For the Binding, choose Artifact with Index 2
- The URL field should look like this:

  https://YourAccountURL.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp
- Leave the Response URL blank and click on OK

Image not found or type unknown

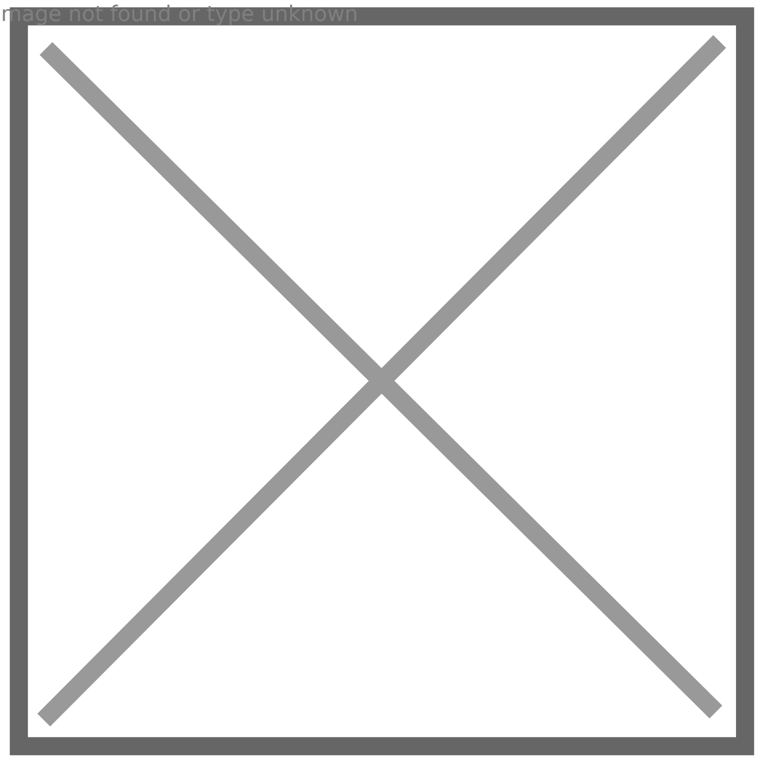


- Click ADD one more time
- For the Endpoint type, sele ct SAML Logout
- For the Binding, choose POST

- The URL field should look like this:

  https://YOUR_ADFS_SERVERNAME.domail.local/adfs/ls/?wa=wsignout1.0
- Leave the Response URL blank and click on OK

Image not found or type unknown



Step 8. Logging

Go to your SSO login page: https://YourAccountURL.ispringlearn.com/sso/login and enter your credentials.

Related Articles

- Integrating iSpring Learn with your system: User Management and Single Sign On
- SAML Technology for SSO
- iSpring Learn SSO with Azure AD + SAML

Tutorials

iSpring Learn SSO with Azure AD + SAML

PRODUCTS: Learn

Azure Active Directory (Azure AD) is a part of the Microsoft Azure cloud service that makes it possible to enjoy SSO (Single sign-on) without employing on-prem AD FS (Active Directory Federated Services). It is basically a cloud alternative to Microsoft Active Directory. In this scenario, there is no need to maintain an on-premise infrastructure, the process of setting it up is rather easy, and it works with most cloud-based services.

Requirements

A Microsoft Azure account with Azure AD Premium activated.

How to set up Azure AD

1. Go to the Microsoft Azure Home Page. From the Azure services menu, select Enterprise applications.
   01.png
   Image not found or type unknown
2. Select New application.
   02.png
   Image not found or type unknown
3. Select **Create your own application**.
   03.png
   Image not found or type unknown
   In the right-side menu that appears, enter the name for the application, such as iSpring Learn SSO.
   04.png
   Image not found or type unknown
4. Click Create and wait until the application is added to your library. You will then be redirected to the Overview page.

   In the sidebar menu, select Users and groups. There, you can add all the users who should

be able to log into their iSpring Learn account using SSO.
05.png Image not found or type unknown

5. In the sidebar menu, select **Single sign-on**. Then, select **SAML for SAML-based SSO**.
   06.png Image not found or type unknown
   Set up Single Sign-On with SAML. Here’s how:
   First, select Edit, to open the right-side menu.
   07.png Image not found or type unknown

In the right-side menu, fill out Identifier (Entity ID), Reply URL, and Relay state as shown in the table below, where ‘_____’ is the first part of the URL of your iSpring Learn account. Pay attention to the domain for your iSpring Learn account: it is either .com or .eu.

Identifier (Entity ID)	https://_____.ispringlearn.com/module.php/saml/sp/metadata.php/default-sp
Reply URL	https://_____.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp
Relay state	https://_____.ispringlearn.com/sso/login

08.png Image not found or type unknown

Save the changes.

1. Second, select

Edit

1. to edit User Attributes and Claims.

09.png Image not found or type unknown

The first claim in the list is the Required claim. Its claim name is Unique User Identifier (Name ID) and its Value is user.mail. It is there by default. Leave it as it is.
The additional claims are those used by iSpring Learn to sync the data about your users and fill out their user profiles in iSpring Learn. The information will be updated in iSpring Learn each time you log in.

1. Since iSpring Learn requires each user to have a login, this is the required claim. We also strongly recommend using email so your users get notifications from the system about new courses assigned, coming deadlines, and scheduled meetings and webinars. The rest of the claims are optional.

1. Delete the preset claim names and values and add your own. You can use your own names for the claims while you select values from the available list. To simplify the process, we recommend using the same claim name as the value. The only exception is user.login, where we use user.mail, thus making the login correspond with the email. Use the table below for the correct claim names and their values.

Claim Name	**Value**
user.login	user.mail
user.mail	user.mail
user.surname	user.surname
user.givenname	user.givenname
user.jobtitle	user.jobtitle

1. Only the Name and the Source Attribute fields need to be changed. Leave the rest empty.

11.png Image not found or type unknown

1. When you are done, you should see the list of all the claims you want your iSpring Learn account to be in sync with.

10.png Image not found or type unknown

Note that you won't be able to sync the user's country and department.

1. Return to the previous page to configure the third step: the certificate. Select **Add a certificate** to open the menu on the right side of the screen and select **New Certificate**. 12.png Image not found or type unknown For **Signing Option**, select **Sign SAML assertion**. For **Signing Algorithm**, select **SHA-1**. Select **Save** for the certificate to be generated and the thumbprint to be displayed. You will need the thumbprint when you configure the connection settings in iSpring Learn.

   Close the menu on the right side of the screen to return to configuring the fourth step: iSpring Learn SSO.

   The data from this step should be used in the Connection Settings of your iSpring Learn account.

How to set up iSpring Learn

1. Log into your iSpring Learn account and go to https://_____.ispringlearn.com/settings/sso
2. In Connection Settings, fill in the fields with the information from Azure.

iSpring Learn name	**Azure name**
Issue URL (IdP Entity ID)	Azure AD Identifier
Sign-on URL	Login URL
Logout URL	Logout URL
Certificate Fingerprint	Thumbprint

13.png Image not found or type unknown

If you have selected the **Redirect users to the SSO login page**, the user will be automatically redirected to the Azure login page when they open iSpring Learn. If they are already logged in there, they will see their main page with the courses that have been assigned.

If this option is not selected, upon opening iSpring Learn, the user will see the default login screen with an additional option to use a corporate account to log into the account.

We recommend keeping this option deselected initially for the sake of testing the connection and to avoid being locked out of your iSpring Learn account. If this happens for some reason, you can use https://____.ispringlearn.com/login?no_sso to bypass SSO.

Proceed to Matching fields of iSpring Learn with the external SSO attributes and use the claims you created in the second step of the Azure Set up Single Sign-On with SAML page.

14.png Image not found or type unknown

When done, scroll up and click **Save**.

You can now test the connection.

15.png Image not found or type unknown

If something is not clear or additional questions arise, don’t hesitate to contact us at support@ispring.com and we’ll do our best to assist you.

Related Articles

- SAML Technology for SSO
- Integrating iSpring Learn with your system: User Management and Single Sign On
- How to upload SCORM courses to ...

Tutorials

Setting-up Azure Entra with Classlink

Notes

This is an all or none type of configuration. Once enabled all users of the domain will be redirected to Launchpad for authentication in all Microsoft applications. Users previously Authenticated to Office 365/Entra ID (Azure AD) may need to reauthenticate their desktop applications. Office365 Administrator accounts will not be affected by this workflow.

Prerequisites

- Authenticate to LaunchPad with AD (technically could be Google as well but unlikely)
  - District’s Azure user profile **must** contain an ImmutableI
  - If the district uses Azure AD Connect, it’s handled
  - If the district enters users manually, it’s handled
  - If the district uses OneSync for Azure, it can be handled in the configuration
- Add Verified Domain to Entra ID (Azure AD)
  - Do not make it primary.
- Install MSOnline PowerShell module

```
Install-Module MSOnline
```

- Install Azure Active Directory Connect and configure it – Do not federate via this method.
- Active Directory should be connected in launchpad under settings > domain gear icon
- Active Directory Groups should be imported into launchpad

Step 1

1. In the Classlink tenant SAML Console, Create a new SAML configuration by copying existing and selecting “A New SAML App (template)”
2. Configure the following options.

- Metadata URL
  - https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
- Loginurl with custom login, e.g. https://launchpad.classlink.com/<customurl>

- Attribute Mapping
- ? Select “Custom Attribute”
    - Change name of the custom attribute to “IDPEmail”
    - Add {email} in the data field
- MetaOverrides
    - Logout Service URL (POST)
        - https://login.microsoftonline.com/common/oauth2/logout
    - NamedID Format
        - Persistent
    - NameID Custom Value
        - {ldapguid:hexbase64}
- Save or Update

Step 2

- Copy the metadata URL and modify the PowerShell Script below
- Use this PowerShell Script, change the file extension to “.ps1” after downloading - You may need to unblock the file and change your execution policy on the server
    - [Google Drive]()

Azure AD PowerShell Code

```
<#
.SYNOPSIS
    Federate Microsoft Entra ID (Azure AD/Microsoft Online Services) to ClassLink for IdP Services.

    Change the <GUID> in the $idpMetadataUrl to be the GUID from your SAML console App.
    Change $DomainName to match your domain name that is going to be Federated
    Change the script extension to ".ps1"

    *NOTE: you may need to set the PowerShell Execution Policy to remote signed or bypass temporarily.

#>

Install-Module -Name MSOnline
Import-Module MSOnline

$idpMetadataUrl = "https://idp.classlink.com/sso/metadata/<GUID>"

$DomainName = "<your domain name>"
```

```
$metadataxml = [Xml](Invoke-WebRequest -Uri $idpMetadataUrl -ContentType "application/xml").content

$cert = -join
$metadataxml.EntityDescriptor.IDPSSODescriptor.KeyDescriptor.KeyInfo.X509Data.X509Certificate.Split()
$issuerUri = $metadataxml.EntityDescriptor.entityID
$logOnUri = $metadataxml.EntityDescriptor.IDPSSODescriptor.SingleSignOnService | ? {
$_.Binding.Contains('Redirect') } | % { $_.Location }
$LogOffUri = $metadataxml.EntityDescriptor.IDPSSODescriptor.SingleLogoutService | ? {
$_.Binding.Contains('Redirect') } | % { $_.Location }
$brand = "ClassLink Identity"
Connect-MsolService
$DomainAuthParams = @{
    DomainName = $DomainName
    Authentication = "Federated"
    IssuerUri = $issuerUri
    FederationBrandName = $brand
    ActiveLogOnUri = $logOnUri
    PassiveLogOnUri = $logOnUri
    LogOffUri = $LogOffUri
    SigningCertificate = $cert
    PreferredAuthenticationProtocol = "SAMLP"
}

Set-MsolDomainAuthentication @DomainAuthParams
```

> If you receive an error regarding scripts being disabled Open an elevated PowerShell prompt
> Type the following:
> `set-executionpolicy remotesigned -force`
> This will allow local PowerShell scripts to run

? If you use an account that is being federated (using the custom domain instead of an onmicrosoft.com domain) https://portal.azure.com should redirect you to https://launchpad.classlink.com/<customurl> for login from now on, along with any other Microsoft Service

Step 3:

? Make sure you have break-glass accounts within Microsoft in case something happens.

? https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-acc ess

Revert to Entra ID (Azure AD) Managed Authentication

Open PowerShell

1. Run the command
2. Connect-MsolService

After authenticating to your Entra ID (Azure AD) Tenant

Run the command:

```
  Set-MsolDomainAuthentication -authentication managed -domainName
<domainname>
```

> Replace `<domainname>` with your domain you wish to remove federation

Classlink LTI v1.3 (OIDC) Details

Dear Vendor,

Our school is going to add your app as an LTI v1.3 SSO app through ClassLink. Please provide me with the following information:

ClientID (generated in the Partner Portal)

OIDC Login Initiation URL

Target Link URL

LTI Message Type (default is LtiResourceLinkRequest)

Person SourcedID

Role

With PII

Any Input Fields that I would need

Here is information about our school system and ClassLink:

The OpenID Connect (OIDC) discovery endpoint is https://launchpad.classlink.com/.well-known/openid-configuration

The OIDC discovery endpoint contains the following:

- Issuer ID: https://launchpad.classlink.com
- OIDC URL: https://launchpad.classlink/com/oauth2/v2/auth
- JWKS URL: https://launchpad.classlink/com/oauth2/v2/jwks

Our SchoolDeployment ID (Tenant ID) is xxxx. (Not all vendors require a Deployment ID, but it's best to include it in case it is needed.)

Thank you so much for your help with this,

Insert Your Name and Contact Information

Disable MFA in EntraID (Azure AD)

1. You are using 3rd party MFA which is ClassLink, is this correct?

2. You want to disable the Microsoft MFA, or you do not wish your users to be asked for a Microsoft MFA, is this correct?

-If yes is your answer the above information, disable the following: "Registration Campaign", "System-Preferred Multi-factor Authentication" and your tenants "Security Defaults".

3. To disable the "Registration Campaign":

- Go to > https://portal.azure.com >Microsoft Entra ID >Manage >Security >Authentication Methods >Registration Campaign >switch the State from Enabled or Microsoft Managed to Disable.

4. To disable the "System-Preferred Multi-factor Authentication"

- Go to > https://portal.azure.com >Microsoft Entra ID >Manage >Security >Authentication Methods >Settings >System-Preferred Multi-factor Authentication >switch the State from Enabled or Microsoft Managed to Disable.

5. To disable the "Security Defaults"

- Go to > https://portal.azure.com >Microsoft Entra ID >Manage >Properties >Manage Security Defaults >switch from Enable to Disable.

Authentik Docs

Docs copied from authentik

Welcome to authentik

What is authentik?

authentik is an open-source Identity Provider, focused on flexibility and versatility. With authentik, site administrators, application developers, and security engineers a dependable and secure solution for authentication in almost any type of environment. There are robust recovery actions available for the users and applications, including user profile and password management. You can quickly edit, deactivate, or even impersonate a user profile, and set a new password for new users or reset an existing password.

You can use authentik in an existing environment to add support for new protocols, so introducing authentik to your current tech stack doesn't present re-architecting challenges. We already support all of the major providers, such as OAuth2, SAML, LDAP, and SCIM, so you can pick the protocol that you need for each application.

The authentik product provides the following consoles:

- **Admin interface**: a visual tool for the creation and management of users and groups, tokens and credentials, application integrations, events, and the Flows that define standard and customizable login and authentication processes. Easy-to-read visual dashboards display system status, recent logins and authentication events, and application usage.
- **User interface**: this console view in authentik displays all of the applications and integrations in which you have implemented authentik. Click on the app that you want to access to open it, or drill down to edit its configuration in the admin interface
- **Flows**: *Flows* are the steps by which the various *Stages* of a login and authentication process occurs. A stage represents a single verification or logic step in the sign-on process. authentik allows for the customization and exact definition of these flows.

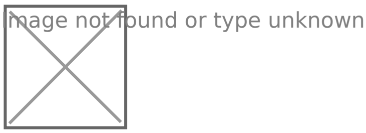
Installation

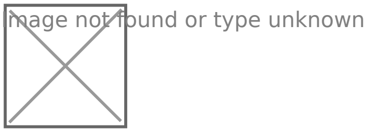
Refer to the installation steps in either Docker-compose or Kubernetes.

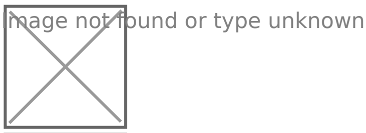
For more information about configuration, Beta versions, and additional installation options, see our main Installation section.

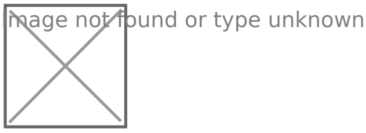
Screenshots

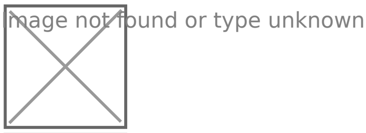
authentik can use Light or Dark mode for the Admin interface, User interface and the flow interface.

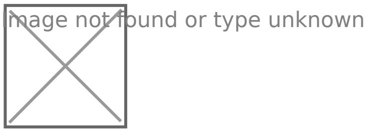












Docker Compose installation

This installation method is for test-setups and small-scale production setups.

Requirements

- A host with at least 2 CPU cores and 2 GB of RAM
- Docker
- Docker Compose

Preparation

To download the latest `docker-compose.yml` open your terminal and navigate to the directory of your choice. Run the following command:

```
wget https://goauthentik.io/docker-compose.yml
```

If this is a fresh authentik installation, you need to generate a password and a secret key. If you don't already have a password generator installed, you can run this command to install **pwgen**, a popular generator:

```
# You can also use openssl instead: `openssl rand -base64 36`
sudo apt-get install -y pwgen
```

Next, run the following commands to generate a password and secret key and write them to your `.env` file:

```
echo "PG_PASS=$(pwgen -s 40 1)" >> .env
echo "AUTHENTIK_SECRET_KEY=$(pwgen -s 50 1)" >> .env
# Because of a PostgreSQL limitation, only passwords up to 99 chars are supported
# See https://www.postgresql.org/message-id/09512C4F-8CB9-4021-B455-EF4C4F0D55A0@amazon.com
```

To enable error reporting, run the following command:

```
echo "AUTHENTIK_ERROR_REPORTING__ENABLED=true" >> .env
```

Email configuration (optional but recommended)

It is also recommended to configure global email credentials. These are used by authentik to notify you about alerts and configuration issues. They can also be used by Email stages to send verification/recovery emails.

To configure email credentials, append this block to your `.env` file

```
# SMTP Host Emails are sent to
AUTHENTIK_EMAIL__HOST=localhost
AUTHENTIK_EMAIL__PORT=25
# Optionally authenticate (don't add quotation marks to your password)
AUTHENTIK_EMAIL__USERNAME=
AUTHENTIK_EMAIL__PASSWORD=
# Use StartTLS
AUTHENTIK_EMAIL__USE_TLS=false
# Use SSL
AUTHENTIK_EMAIL__USE_SSL=false
AUTHENTIK_EMAIL__TIMEOUT=10
# Email address authentik will send from, should have a correct @domain
AUTHENTIK_EMAIL__FROM=authentik@localhost
```

Configure for port 80/443

By default, authentik listens internally on port 9000 for HTTP and 9443 for HTTPS. To change the exposed ports to 80 and 443, you can set the following variables in `.env`:

```
COMPOSE_PORT_HTTP=80
COMPOSE_PORT_HTTPS=443
```

See Configuration to change the internal ports. Be sure to run `docker-compose up -d` to rebuild with the new port numbers.

Startup

> DANGER
> The server assumes to have local timezone as UTC. All internals are handled in UTC; whenever a time is displayed to the user in UI, the time shown is localized. Do not update or mount `/etc/timezone` or `/etc/localtime` in the authentik containers. This will not give any advantages. It will cause problems with OAuth and SAML authentication, e.g. see this GitHub issue.

Afterwards, run these commands to finish:

```
docker-compose pull
docker-compose up -d
```

The `docker-compose.yml` file statically references the latest version available at the time of downloading the compose file. Each time you upgrade to a newer version of authentik, you download a new `docker-compose.yml` file, which points to the latest available version. For more information, refer to the **Upgrading** section in the Release Notes.

To start the initial setup, navigate to `http://<your server's IP or hostname>:9000/if/flow/initial-setup/`.

There you are prompted to set a password for the akadmin user (the default user).

An explanation about what each service in the docker compose file does, see Architecture.

Configuration

These are all the configuration options you can set via environment variables.

Append any of the following keys to your `.env` file, and run `docker-compose up -d` to apply them.

> **Info**
> The double-underscores are intentional, as all these settings are translated to yaml internally, a double-underscore indicates the next level.

All of these variables can be set to values, but you can also use a URI-like format to load values from other places:

- `env://<name>` Loads the value from the environment variable `<name>`. Fallback can be optionally set like `env://<name>?<default>`
- `file://<name>` Loads the value from the file `<name>`. Fallback can be optionally set like `file://<name>?<default>`

Checking settings

To check if your config has been applied correctly, you can run the following command to output the full config:

```
docker-compose run --rm worker dump_config
# Or for kubernetes
kubectl exec -it deployment/authentik-worker -c authentik -- ak dump_config
```

PostgreSQL Settings

- `AUTHENTIK_POSTGRESQL__HOST`: Hostname of your PostgreSQL Server
- `AUTHENTIK_POSTGRESQL__NAME`: Database name

- `AUTHENTIK_POSTGRESQL__USER`: Database user
- `AUTHENTIK_POSTGRESQL__PORT`: Database port, defaults to 5432
- `AUTHENTIK_POSTGRESQL__PASSWORD`: Database password, defaults to the environment variable `POSTGRES_PASSWORD`
- `AUTHENTIK_POSTGRESQL__USE_PGBOUNCER`: Adjust configuration to support connection to PgBouncer
- `AUTHENTIK_POSTGRESQL__SSLMODE`: Strictness of ssl verification. Defaults to `verify-ca`
- `AUTHENTIK_POSTGRESQL__SSLROOTCERT`: CA root for server ssl verification
- `AUTHENTIK_POSTGRESQL__SSLCERT`: Path to x509 client certificate to authenticate to server
- `AUTHENTIK_POSTGRESQL__SSLKEY`: Path to private key of `SSLCERT` certificate

Redis Settings

- `AUTHENTIK_REDIS__HOST`: Hostname of your Redis Server
- `AUTHENTIK_REDIS__PORT`: Redis port, defaults to 6379
- `AUTHENTIK_REDIS__PASSWORD`: Password for your Redis Server
- `AUTHENTIK_REDIS__TLS`: Use TLS to connect to Redis, defaults to false
- `AUTHENTIK_REDIS__TLS_REQS`: Redis TLS requirements, defaults to "none"
- `AUTHENTIK_REDIS__DB`: Database, defaults to 0
- `AUTHENTIK_REDIS__CACHE_TIMEOUT`: Timeout for cached data until it expires in seconds, defaults to 300
- `AUTHENTIK_REDIS__CACHE_TIMEOUT_FLOWS`: Timeout for cached flow plans until they expire in seconds, defaults to 300
- `AUTHENTIK_REDIS__CACHE_TIMEOUT_POLICIES`: Timeout for cached policies until they expire in seconds, defaults to 300
- `AUTHENTIK_REDIS__CACHE_TIMEOUT_REPUTATION`: Timeout for cached reputation until they expire in seconds, defaults to 300

Listen Setting

- `AUTHENTIK_LISTEN__HTTP`: Listening address:port (e.g. `0.0.0.0:9000`) for HTTP (Server and Proxy outpost)
- `AUTHENTIK_LISTEN__HTTPS`: Listening address:port (e.g. `0.0.0.0:9443`) for HTTPS (Server and Proxy outpost)
- `AUTHENTIK_LISTEN__LDAP`: Listening address:port (e.g. `0.0.0.0:3389`) for LDAP (LDAP outpost)
- `AUTHENTIK_LISTEN__LDAPS`: Listening address:port (e.g. `0.0.0.0:6636`) for LDAPS (LDAP outpost)
- `AUTHENTIK_LISTEN__METRICS`: Listening address:port (e.g. `0.0.0.0:9300`) for Prometheus metrics (All)

- `AUTHENTIK_LISTEN__DEBUG`: Listening address:port (e.g. `0.0.0.0:9900`) for Go Debugging metrics (All)
- `AUTHENTIK_LISTEN__TRUSTED_PROXY_CIDRS`: List of CIDRs that proxy headers should be accepted from (Server)
  Defaults to `127.0.0.0/8`, `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`, `fe80::/10`, `::1/128`.
  Requests directly coming from one an address within a CIDR specified here are able to set proxy headers, such as `X-Forwarded-For`. Requests coming from other addresses will not be able to set these headers.

authentik Settings

`AUTHENTIK_SECRET_KEY`

Secret key used for cookie signing and unique user IDs, don't change this after the first install.

`AUTHENTIK_LOG_LEVEL`

Log level for the server and worker containers. Possible values: debug, info, warning, error

Starting with 2021.12.3, you can also set the log level to *trace*. This has no affect on the core authentik server, but shows additional messages for the embedded outpost.

> DANGER
> Setting the log level to `trace` will include sensitive details in logs, so it shouldn't be used in most cases.
>
> Logs generated with `trace` should be treated with care as they can give others access to your instance, and can potentially include things like session cookies to authentik **and other pages**.

Defaults to `info`.

`AUTHENTIK_COOKIE_DOMAIN`

Which domain the session cookie should be set to. By default, the cookie is set to the domain authentik is accessed under.

`AUTHENTIK_GEOIP`

Path to the GeoIP database. Defaults to `/geoip/GeoLite2-City.mmdb`. If the file is not found, authentik will skip GeoIP support.

`AUTHENTIK_DISABLE_UPDATE_CHECK`

Disable the inbuilt update-checker. Defaults to `false`.

`AUTHENTIK_ERROR_REPORTING`

- `AUTHENTIK_ERROR_REPORTING__ENABLED`
  Enable error reporting. Defaults to `false`.

  Error reports are sent to https://sentry.io, and are used for debugging and general feedback. Anonymous performance data is also sent.
- `AUTHENTIK_ERROR_REPORTING__SENTRY_DSN`
  Sets the DSN for the Sentry API endpoint.
  When error reporting is enabled, the default Sentry DSN will allow the authentik developers to receive error reports and anonymous performance data, which is used for general feedback about authentik, and in some cases, may be used for debugging purposes.
  Users can create their own hosted Sentry account (or self-host Sentry) and opt to collect this data themselves.
- `AUTHENTIK_ERROR_REPORTING__ENVIRONMENT`
  The environment tag associated with all data sent to Sentry. Defaults to `customer`.
  When error reporting has been enabled to aid in debugging issues, this should be set to a unique value, such as an e-mail address.
- `AUTHENTIK_ERROR_REPORTING__SEND_PII`
  Whether or not to send personal data, like usernames. Defaults to `false`.

`AUTHENTIK_EMAIL`

- `AUTHENTIK_EMAIL__HOST`
  Default: `localhost`
- `AUTHENTIK_EMAIL__PORT`
  Default: `25`
- `AUTHENTIK_EMAIL__USERNAME`
  Default: `` (Don't add quotation marks)

- `AUTHENTIK_EMAIL__PASSWORD`
  Default: `` (Don't add quotation marks)
- `AUTHENTIK_EMAIL__USE_TLS`
  Default: `false`
- `AUTHENTIK_EMAIL__USE_SSL`
  Default: `false`
- `AUTHENTIK_EMAIL__TIMEOUT`
  Default: `10`
- `AUTHENTIK_EMAIL__FROM`
  Default: `authentik@localhost`
  Email address authentik will send from, should have a correct @domain
  To change the sender's display name, use a format like `Name <account@domain>`.

`AUTHENTIK_OUTPOSTS`

- `AUTHENTIK_OUTPOSTS__CONTAINER_IMAGE_BASE`
  Placeholders:
  - `%(type)s`: Outpost type; proxy, ldap, etc
  - `%(version)s`: Current version; 2021.4.1
  - `%(build_hash)s`: Build hash if you're running a beta version

  Placeholder for outpost docker images. Default: `ghcr.io/goauthentik/%(type)s:%(version)s`.
- `AUTHENTIK_OUTPOSTS__DISCOVER`
  Configure the automatic discovery of integrations. Defaults to `true`.
  By default, the following is discovered:
  - Kubernetes in-cluster config
  - Kubeconfig
  - Existence of a docker socket

`AUTHENTIK_AVATARS`

Configure how authentik should show avatars for users. Following values can be set:

Default: `gravatar,initials`

- `none`: Disables per-user avatars and just shows a 1x1 pixel transparent picture
- `gravatar`: Uses gravatar with the user's email address
- `initials`: Generated avatars based on the user's name
- Any URL: If you want to use images hosted on another server, you can set any URL.
  Additionally, these placeholders can be used:
  - `%(username)s`: The user's username
  - `%(mail_hash)s`: The email address, md5 hashed
  - `%(upn)s`: The user's UPN, if set (otherwise an empty string)

Starting with authentik 2022.8, you can also use an attribute path like `attributes.something.avatar`, which can be used in combination with the file field to allow users to upload custom avatars for themselves.

Starting with authentik 2023.2, multiple modes can be set, and authentik will fallback to the next mode when no avatar could be found. For example, setting this to `gravatar,initials` will attempt to get an avatar from Gravatar, and if the user has not configured on there, it will fallback to a generated avatar.

`AUTHENTIK_DEFAULT_USER_CHANGE_NAME`

> INFO
> Requires authentik 2021.12.5

Enable the ability for users to change their name, defaults to `true`.

`AUTHENTIK_DEFAULT_USER_CHANGE_EMAIL`

> INFO
> Requires authentik 2021.12.1

Enable the ability for users to change their Email address, defaults to `false`.

`AUTHENTIK_DEFAULT_USER_CHANGE_USERNAME`

> Info
> Requires authentik 2021.12.1

Enable the ability for users to change their Usernames, defaults to `false`.

`AUTHENTIK_GDPR_COMPLIANCE`

> Info
> Requires authentik 2021.12.1

When enabled, all the events caused by a user will be deleted upon the user's deletion. Defaults to `true`.

`AUTHENTIK_DEFAULT_TOKEN_LENGTH`

> Info
> Requires authentik 2022.4.1

Configure the length of generated tokens. Defaults to 60.

`AUTHENTIK_IMPERSONATION`

> Info
> Requires authentik 2022.4.2

Globally enable/disable impersonation. Defaults to `true`.

`AUTHENTIK_FOOTER_LINKS`

> Info
> Requires authentik 2021.12.1

This option configures the footer links on the flow executor pages.

The setting can be used as follows:

```
AUTHENTIK_FOOTER_LINKS='[{"name": "Link Name","href":"https://goauthentik.io"}]'
```

`AUTHENTIK_LDAP__TASK_TIMEOUT_HOURS`

> INFO
> Requires authentik 2023.1

Timeout in hours for LDAP synchronization tasks.

Defaults to `2`.

`AUTHENTIK_LDAP__PAGE_SIZE`

> INFO
> Requires authentik 2023.6.1

Page size for LDAP synchronization. Controls the number of objects created in a single task.

Defaults to `50`.

`AUTHENTIK_LDAP__TLS__CIPHERS`

> INFO
> Requires authentik 2022.7

Allows configuration of TLS Cliphers for LDAP connections used by LDAP sources. Setting applies to all sources.

Defaults to `null`.

`AUTHENTIK_WEB__WORKERS`

> INFO
> Requires authentik 2022.9

Configure how many gunicorn worker processes should be started (see https://docs.gunicorn.org/en/stable/design.html).

If running in Kubernetes, the default value is set to 2 and should in most cases not be changed, as scaling can be done with multiple pods running the web server. Otherwise, authentik will use 1 worker for each 4 CPU cores + 1 as a value below 2 workers is not recommended.

`AUTHENTIK_WEB__THREADS`

INFO
Requires authentik 2022.9

Configure how many gunicorn threads a worker processes should have (see https://docs.gunicorn.org/en/stable/design.html).

Defaults to 4.

Custom python settings

To modify additional settings further than the options above allow, you can create a custom python file and mount it to `/data/user_settings.py`. This file will be loaded on startup by both the server and the worker. All default settings are here

CAUTION
Using these custom settings is not supported and can prevent your authentik instance from starting. Use with caution.