LinkedIn

Recruiter and LTI Single Sign-On (SSO)

Introduction to SSO and implementation guide for:

Microsoft

Active Directory

Federation Services

Who this guide is for

Account Center Administrators

IT / House Security Professionals

Table of contents

Introduction to Single Sign-On (SSO)

What is SSO?

SSO is a way of sharing security credentials and login information between different systems. It trusts one system (e.g. Okta) to authenticate a user's identity for another system (e.g. Recruiter or LTI).

SSO does not transfer user data to or from LinkedIn.

SSO Identity Providers (IdPs) include:

Azure Active Directory

okta

onelogin

… and many more

Note: LinkedIn is SAML 2.0 certified and also supports Sign-In with Google. We currently don't support OAuth2.0 or OpenID.

Why use SSO?

Increased security

SSO offers the most secure way to log in to Recruiter by requiring employees to use your company's established authentication protocols.

Centralized access control

SSO simplifies the process of blocking access to an employee's corporate Recruiter or LTI license if they leave your company (learn more).

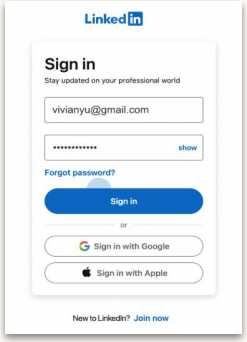
No need for 2FA

SSO eliminates LinkedIn's requirement for two factor authentication.

What does log-in look like?

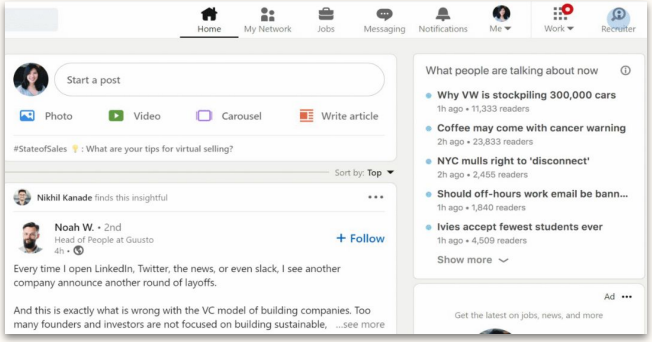
With SSO set up, this is the user journey when logging in to Recruiter or LTI.

1



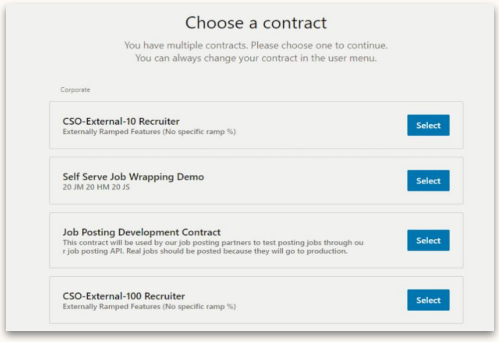
Sign in to LinkedIn

2



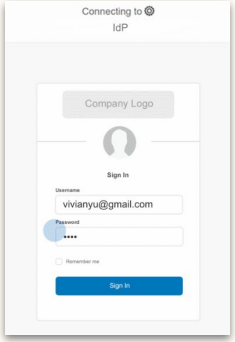
Click the Recruiter or LTI icon

3



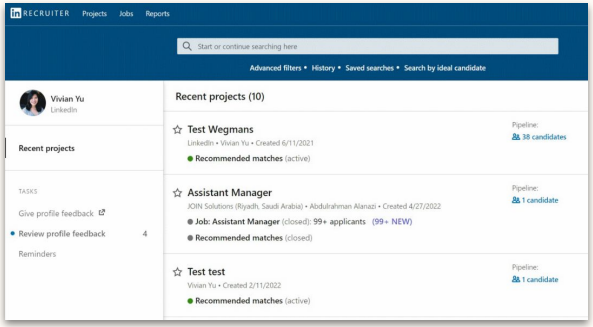
(If on more than one contract) select contract

4



Enter IdP credentials

5



Successful login

Why do users still need to enter LinkedIn login credentials?

Users must log in to their LinkedIn Member Identity once a day for security purposes.

Many LinkedIn Hiring product features depend upon a user's personal LinkedIn account, using shared connections, degree of connection, and candidate feedback.

To enable this, recruiters and hiring managers must 'bind' (connect) their personal LinkedIn account with Recruiter / LTI. Once a day, you must log in to both your Corporate Identity using SSO and your LinkedIn Member Identity using standard login.

Corporate Identity	Member Identity
Controlled centrally by your employer	Controlled by you
Information about you and your position	Information about your entire career

SSO does not solve for everything

It doesn't speed up log-in

Users still need to log in to their LinkedIn Profile once a day for security purposes.

SSO adds slightly more friction, as users also need to periodically re-enter their SSO/IdP credentials (depending on the IdP session length set by the company).

It doesn't automate user management

Admins will still need to log in to Account Center to make changes such as:

- Granting Project Creator or Hiring Collaborator licenses to users
- Updating a user's permissions, roles, or access to Account Center
- Reassigning licenses/projects from one user to another
- Revoking a user's license/permissions
- Updating a user's email, name, license/permissions settings

Learn more about managing licenses

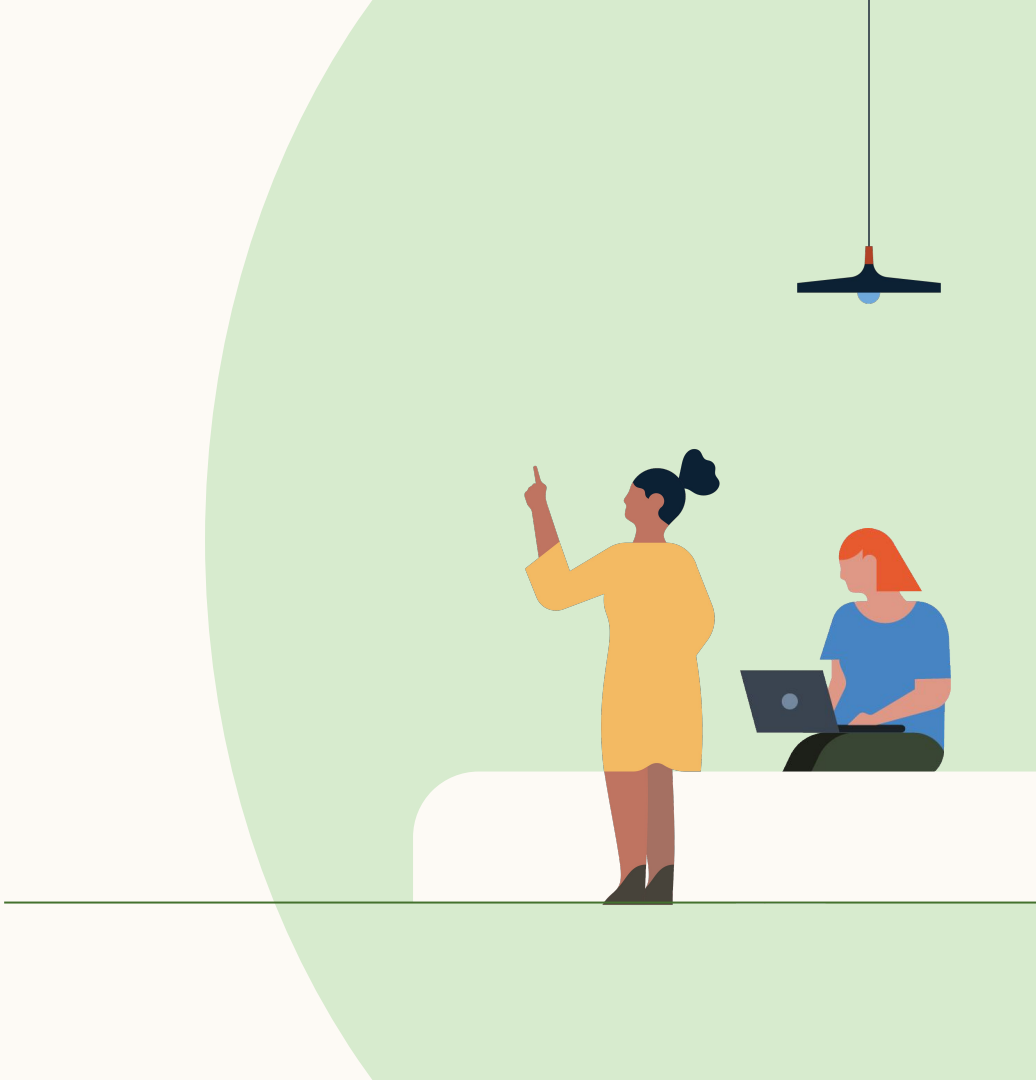
Changing the SSO session length

SSO session length (or timeout) refers to how long LinkedIn waits before re-pinging a user's IdP/SSO provider to re-authenticate the user. The default session length (or timeout) for LinkedIn Talent Solutions SSO is 8 hours.

To change the session length, please file a support ticket.

Things to note:

- Every time LinkedIn re-authenticates a user through SSO, the user does not necessarily need to re-enter their IdP/SSO credentials. This depends on what the company sets up for their IdP session length.
- LinkedIn SSO session timeout does not impact a user's IdP or Recruiter session timeouts.
- Neither you nor LinkedIn can check your current SSO session length. For certainty, you can request an adjustment to the session length, based on your preference.



Changing session lengths

Is a short or long SSO session length best?

Short session timeout

A short session timeout **optimizes for security.**

If an employee leaves the company, you can block access to their Recruiter / LTI license by removing or deactivating them in your IdP platform.

However, users will be asked to re-enter their SSO credentials more frequently.

Long session timeout

A long session timeout **optimizes for usability.**

Users won't have to re-enter their SSO credentials as often.

However, if you want to stop a terminated employee from using Recruiter or LTI by removing or deactivating them in your IdP platform, a long session timeout is less effective. For example, if the session timeout is 30 days, and the user is removed from the IdP on day 1, they will still have access to Recruiter or LTI for another 29 days.

Deactivating users

What happens when a user leaves my organization?

If an employee leaves, the first thing your IT team should do is remove or deactivate the employee in your IdP platform.

Then, if the employee tries to access Recruiter or LTI and their SSO session has expired, login will fail as the IdP will no longer authenticate them. Note: If SSO session length is one week, the employee retains access for the full week, even if they are deactivated at the start of the week.

The Recruiter or LTI license will remain assigned to the employee until your Account Center admin parks, reassigns, or revokes it. This part is not done automatically.

Activating SSO with AFDS

For help with other IdPs,
see this guide

Pre-work checklist for a successful SSO implementation

IMPORTANT: Admin(s) to confirm that all users have work emails in Account Center. If users don't have a work email, they will be locked out after SSO is activated. Work emails need to match the users' IdP-specific emails. Refer to the Admin guide on updating user emails in Account Center.

- ☐ Confirm that your organization uses a SAML 2.0 compliant IdP (e.g. Okta, Azure Active Directory) or Sign-In with Google.
- ☐ Confirm which Recruiter or Talent Insights dashboards will have SSO activated. Some organizations have more than one.
- ☐ Identify Account Center admin for each dashboard and any relevant internal IT point of contact. If you're not sure who your admins are, submit a ticket to LinkedIn customer support via the Recruiter Help Center. To configure SSO, admins will need both IdP and LinkedIn dashboard access:
  - ☐ IdP access: To arrange this, contact your IT or Security department (whoever has IdP admin/manager access), or your IdP service provider. Note that this may add extra time to your implementation.
  - ☐ Recruiter or Talent Insights dashboard admin access: The admin will need a "Product Settings and Account Center Admin" license for each dashboard you want to enable SSO on. This can be done by either:
    - ☐ Giving your IdP Admin or Manager the license on your dashboard(s), OR
    - ☐ Transferring the relevant information from your IdP admin to a Dashboard admin to enter in Account Center
- ☐ Admin to make teams aware of upcoming changes to their Recruiter / LTI log-in. Refer to sample email.

Please note: Your organization will need to activate SSO directly—enablement requires access to settings / permissions within your IdP that LinkedIn's support team cannot access.

Planning your SSO implementation

Phase 1

Assemble team

- Assemble your SSO team, including your Account Center admin and IT point of contact for IdP configuration
- Review the Recruiter SSO documentation

Phase 2

Review

- Schedule time with relevant internal partners to perform pre-work and testing

Phase 3

Pre-work and testing*

- **IMPORTANT:** Update email addresses in Account Center (refer to Help Doc)
- Activate SSO in TEST Mode (IdP Only) and verify
- Send communication to end users about the upcoming changes to their login steps (refer to sample email)

Phase 4

Activation

- Fully activate SSO
- For issues, consult the FAQ

**The time required to complete pre-work and testing will depend on the number of users and the number of dashboards. You need to set up SSO for each individual dashboard.*

5 steps to enabling SSO

Complete these steps for each Recruiter or LTI dashboard requiring SSO

Connecting your Identity Provider → **Setting up SSO** → **Activate SSO**

Step 1

- Create a new Relying Trust Party in ADFS

Step 2

- Install the Certificate

Step 3

- Configure ADFS

Step 4

- Upload your AD FS Metadata into LinkedIn Account Center
- Complete SSO Settings in Account Center

Step 5

- Activate SSO in LinkedIn Account Center (use Test Mode if you want to limit the usage of SSO to ensure it's working correctly)

For a step-by-step guide to setting up SSO, refer to the slides below.
For more information, see our SSO FAQ.

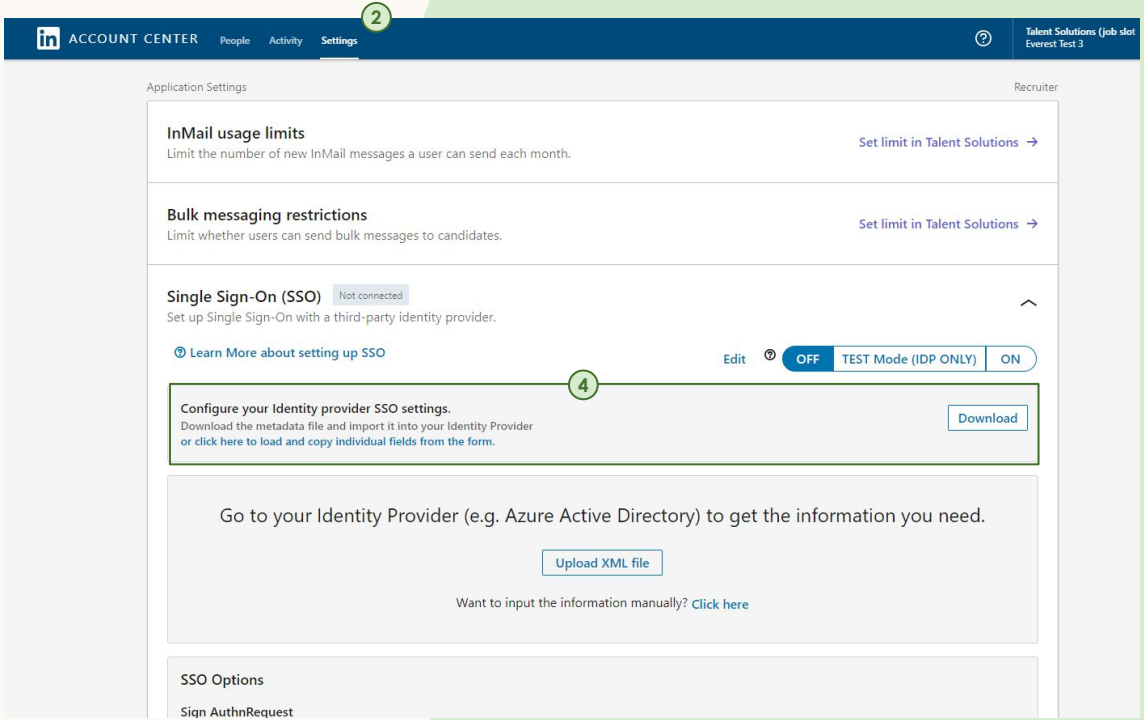
You may also want to refer to our Privacy and Security policies.

Step 1
Create a new Relying Trust Party in ADFS

Part 1 of 4 – Download Account Center metadata

Download settings in XML from Account Center and upload them into ADFS

1. Log in to LinkedIn Account Center and navigate to the Settings tab
2. Expand the Single Sign-On (SSO) panel
3. In the box labelled "Configure your Identity provider SSO settings", click the "Download" button to download the settings you'll need in ADFS in XML format
4. Save the resulting XML



Step 1
Create a new Relying Trust Party in ADFS

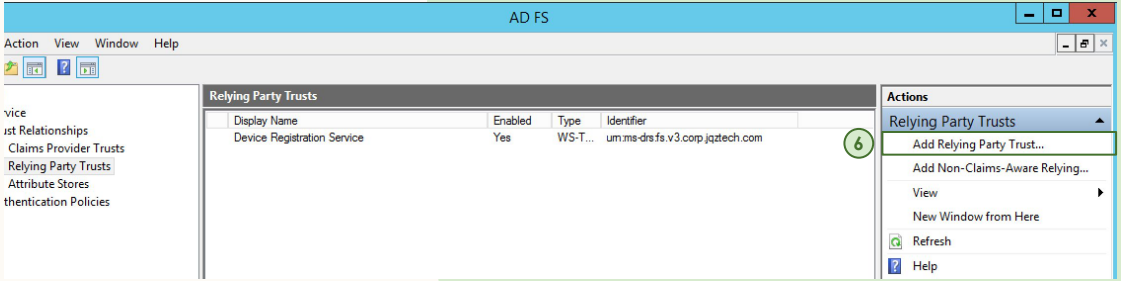
Part 2 of 9 – Create a new Relying Party Trust

In the Active Directory Federated Services admin console:

5. Go to Trusted Relationships and choose Relying Party Trusts
6. On the Right have panel, under actions select "Add Relying Party Trust"
7. A wizard will pop up to walk you through configuring a new service provider as a trusted relationship…

NOTE: Each different Talent Solutions dashboard has a different URL used during authentication for AD FS to respond to, the Assertion Consumer Service (ACS) URL.

Each dashboard will require a separate Relying Trust Party to access the different ACS URLs of your different dashboards.

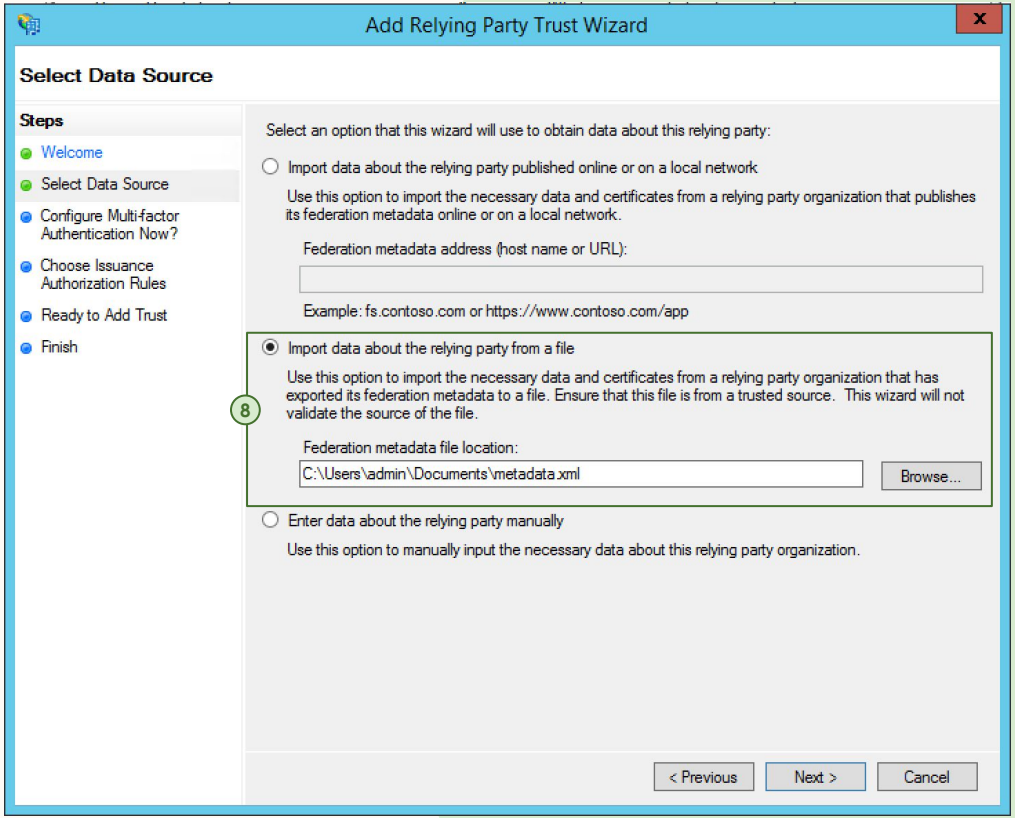


Step 1

Create a new Relying Trust Party in ADFS

Part 3 of 9 – Update Account Center Metadata

8. On the second page of the Add Relying Party Trust Wizard, under "Select Data Source", choose "Import data about the relying party from a file"
9. Browse to where you saved the Metadata XML file from Account Center and choose the file
10. Click "Next" to continue configuring the trusted relationship…

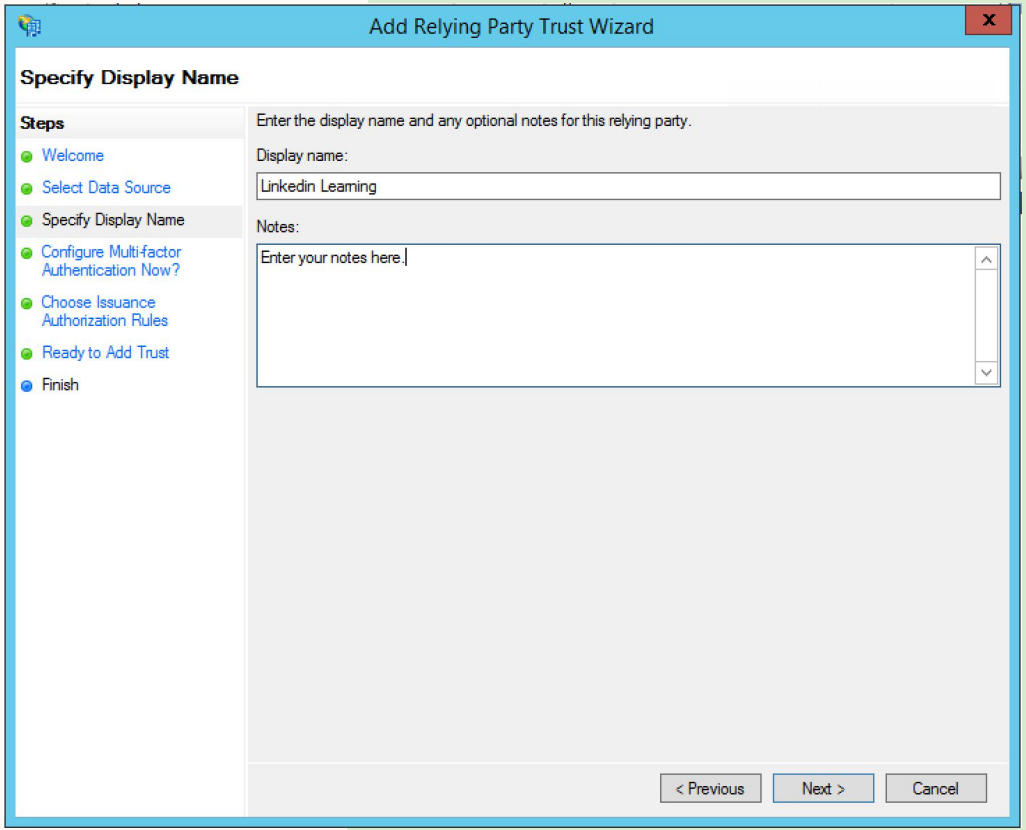


Step 1

Create a new Relying Trust Party in ADFS

Part 4 of 9 – Chose a name for the Trusted Relationship

11. On the third page of the Add Relying Party Trust Wizard you can name the Trusted Relationship. We suggest "LinkedIn Talent Solutions"
12. Notes are optional but can be useful if you have many different Trusted Relationships
13. Click on Next to continue the wizard…



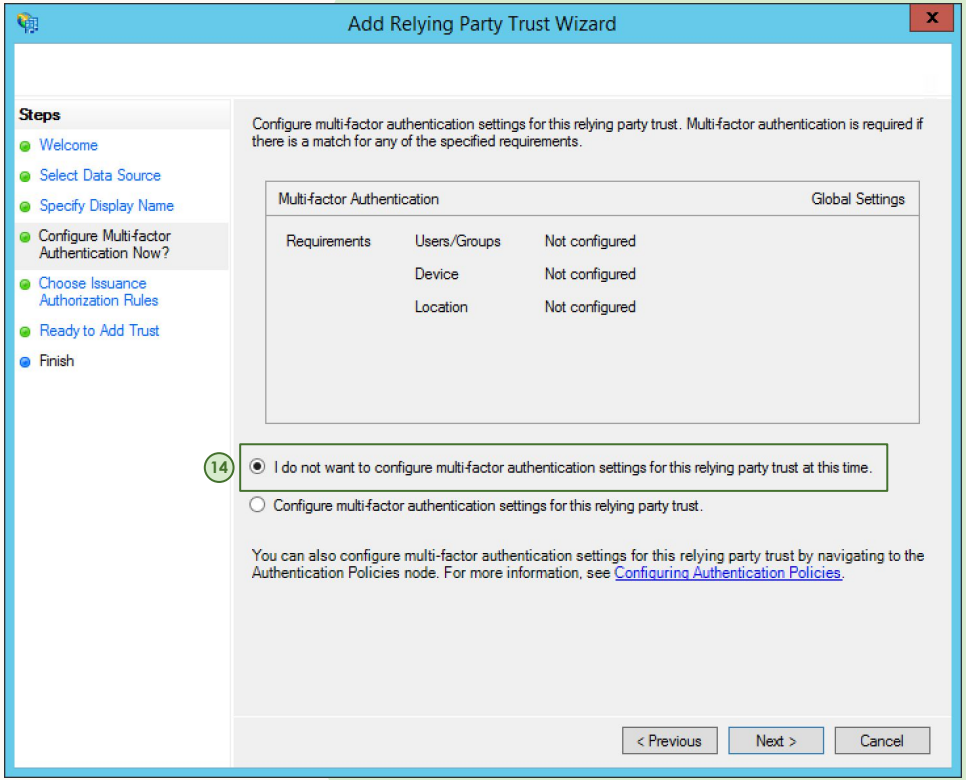
Step 1

Create a new Relying Trust Party in ADFS

Part 5 of 9 – Optionally Configure Multi-Factor authentication

[Optional] On the fourth page of the Add Relying Party Trust Wizard you can configure Multi-Factor Authentication.

14. For the simplest implementation of SSO please select "I do not want to configure multi-factor authentication for this relying party trust at this time"
15. Click Next to continue the wizard…



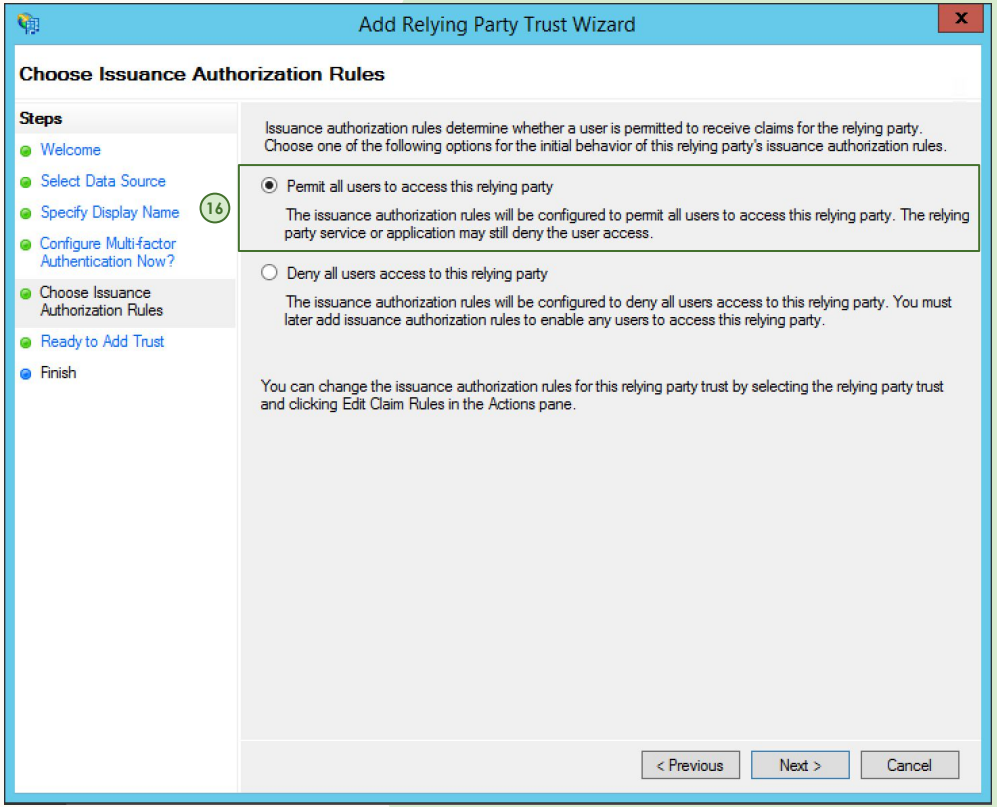
Step 1

Create a new Relying Trust Party in ADFS

Part 6 of 9 – Permit all Users to access the service

16 On the fifth page of the Add Relying Party Trust Wizard you will need to choose the option "Permit all users to access this relying party"

17 Click Next to continue the wizard…



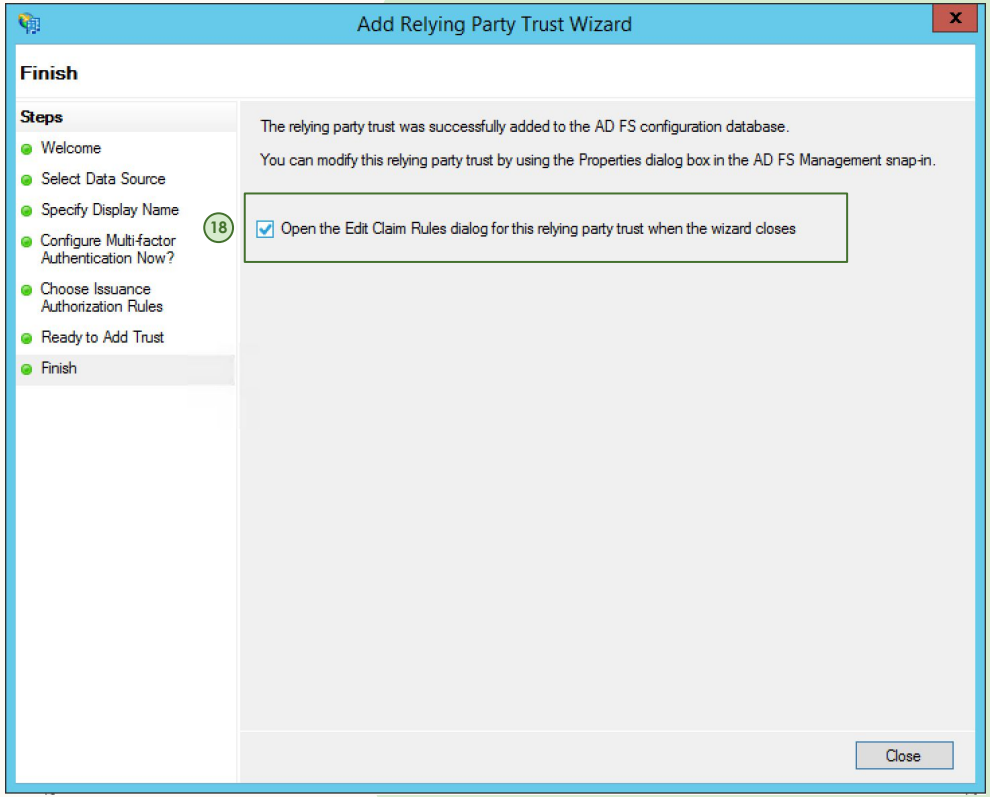
Step 1

Create a new Relying Trust Party in ADFS

Part 7 of 9 – Permit all Users to access the service

18 On the last page of the Add Relying Party Trust Wizard there is an option to "Open the Edit Claim Rules dialog for this relying party trust when the wizard closes". Ensure this is checked.

19 Click on Close to finish the wizard and open the Edit Claim Rules dialog.

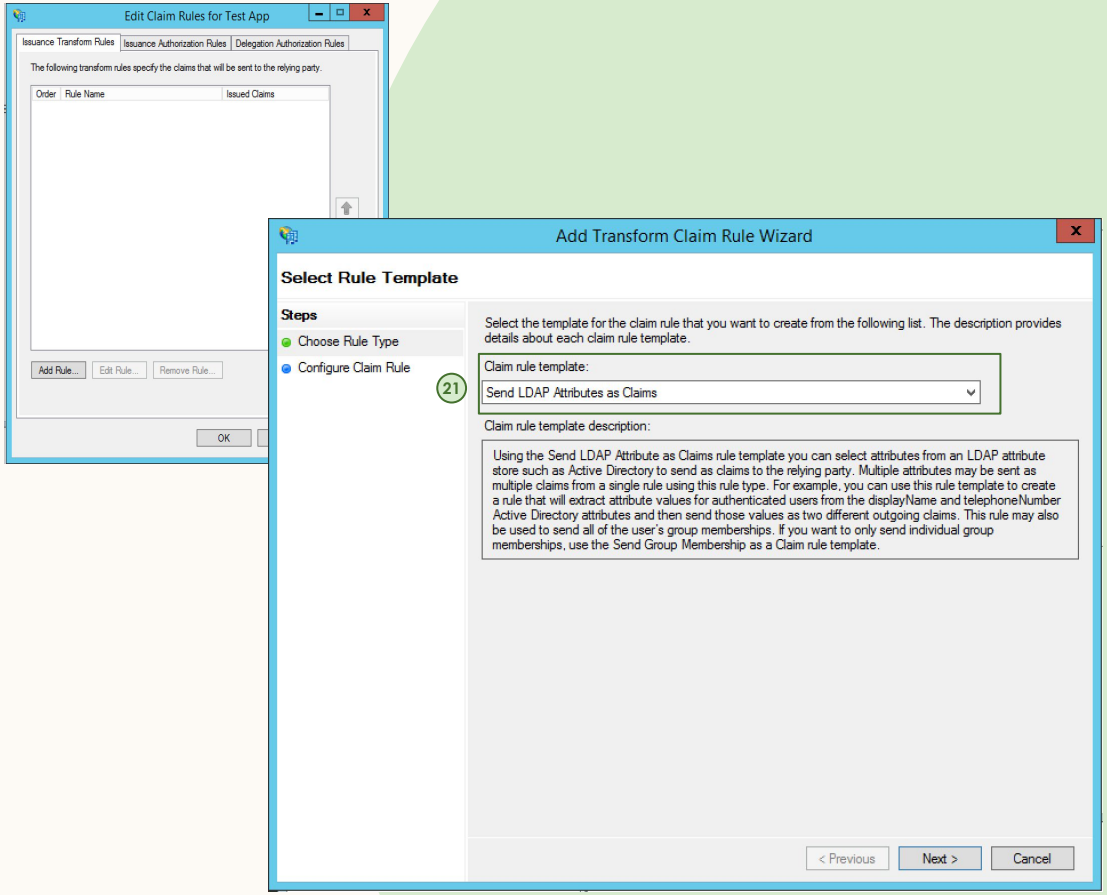


Step 1

Create a new Relying Trust Party in ADFS

Part 8 of 9 – Add a Claim Rule

20. When the Add Relying Party Trust Wizard closes a dialog should open to allow you to edit the claim rules for your Trusted Relationship. Click Add Rule to create a new rule.
21. Choose the "Send LDAP Attributes as Claims" rule template
22. Click Next to move the Add Transform Claim Rule Wizard on to configure the rule

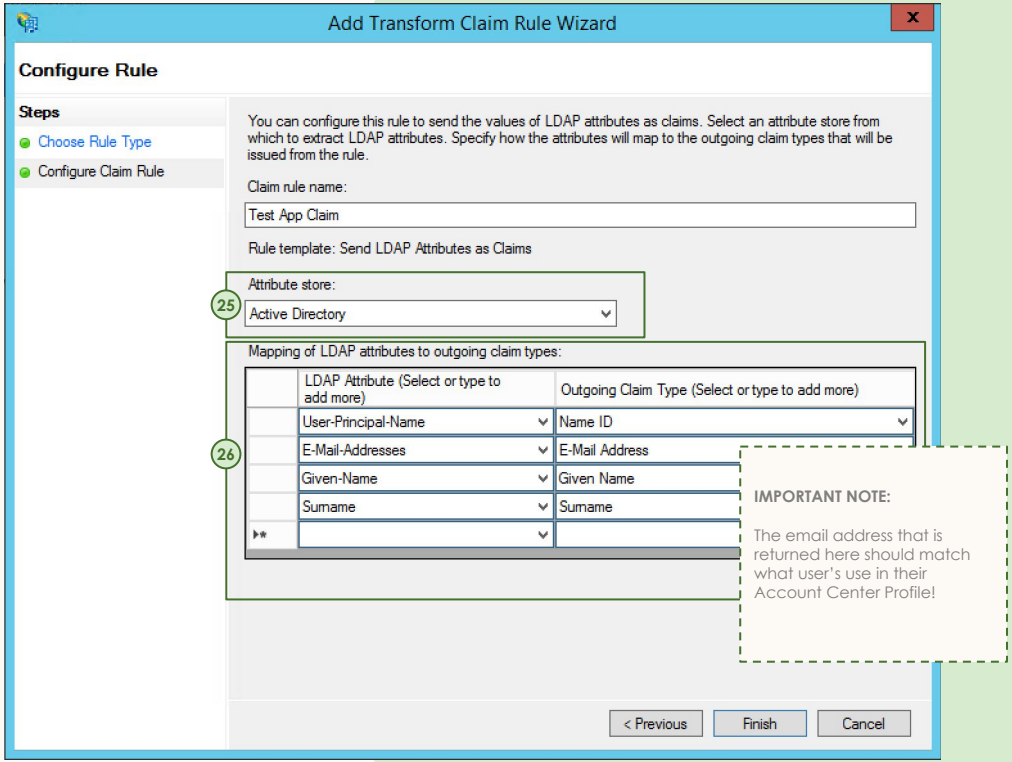


Step 1

Create a new Relying Trust Party in ADFS

Part 9 of 9 – Configure the Claim Rule

23. In the second page of Add Relying Party Trust Wizard, you will be able to configure your Claim Rule to send the data Account Center will need to connect an authenticated user to their Talent Solutions products
24. Name your rule - we suggest "Talent Solutions Claim Rule"
25. Ensure the Attribute Store is set to "Active Directory"
26. Map data about your users you will need in Account Center from the LDAP attributes. It is mandatory that you configure User-Principal-Name and E-Mail-Addresses. It is suggested you configure Given-Name and Surname for troubleshooting. Other attributes, such as Department are optional.



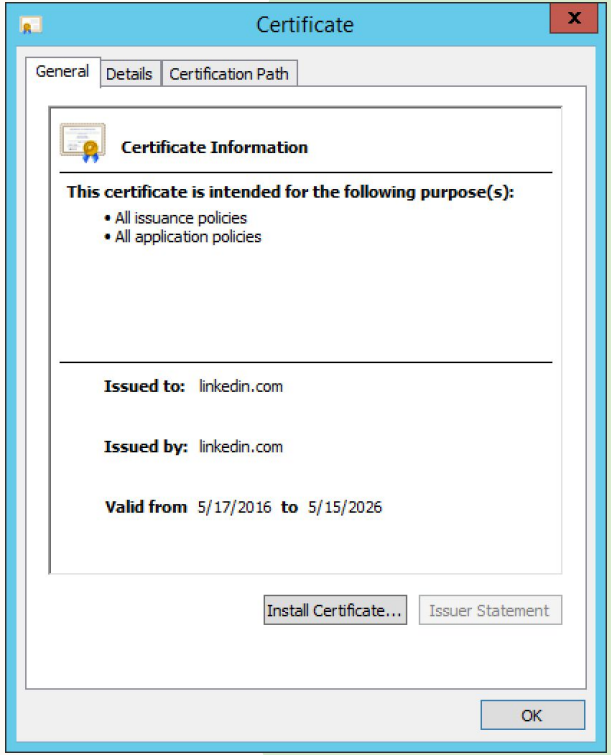
Step 2

Install the Certificate

Part 1 of 3 – Check current certificate state

You will need to check to make sure that your Certificate installed correctly. To do this:

1. Right click on your newly created Relying Party Trust and select Properties
2. Select the Signature tab and double click on the certificate found there
3. It should appear the same as the one shown here. If so, move on to the next step, Step 3 - Upload your ADFS Metadata into LinkedIn Account Center
4. If it does not appear the same as the one shown continue this step….

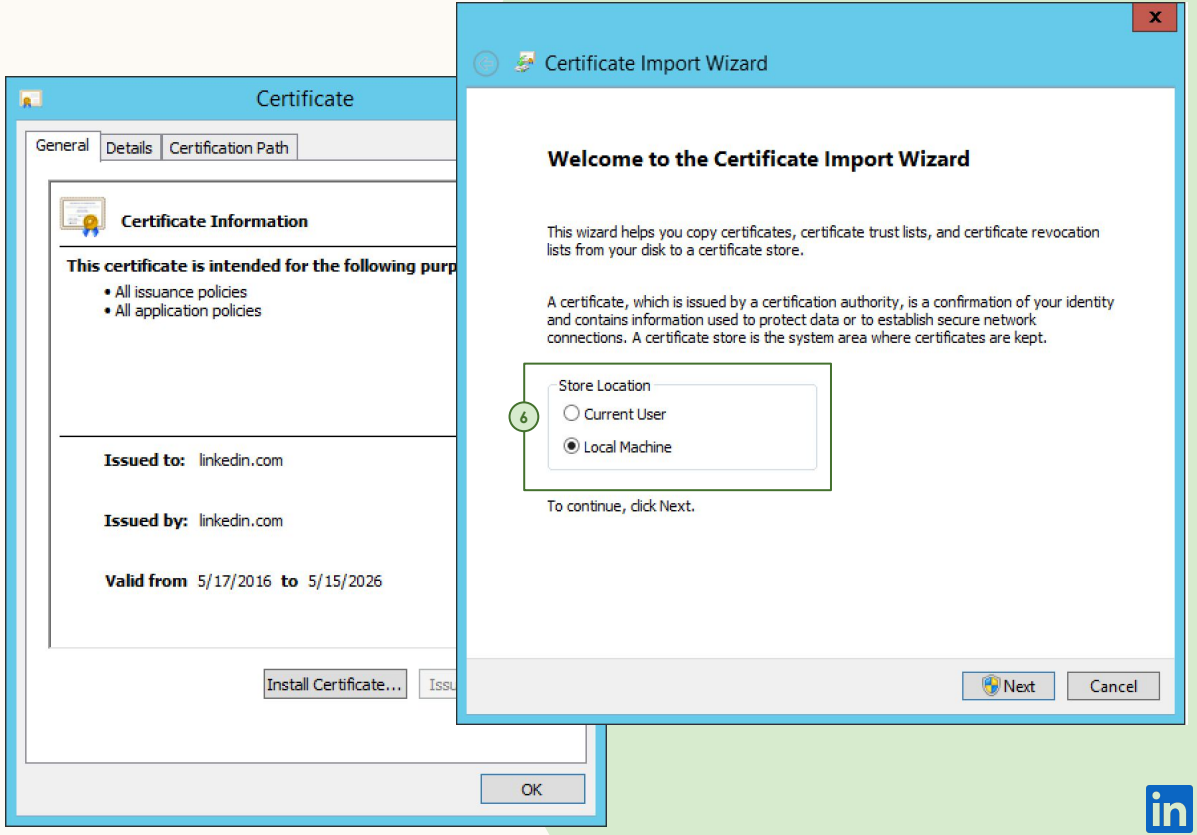


Step 2

Install the Certificate

Part 2 of 3 – Check current certificate state

5. On the Certificate details window click Install Certificate… to open the Certificate Import Wizard
6. Choose Local Machine as the Store Location
7. Click Next to continue configuring your Certificate…



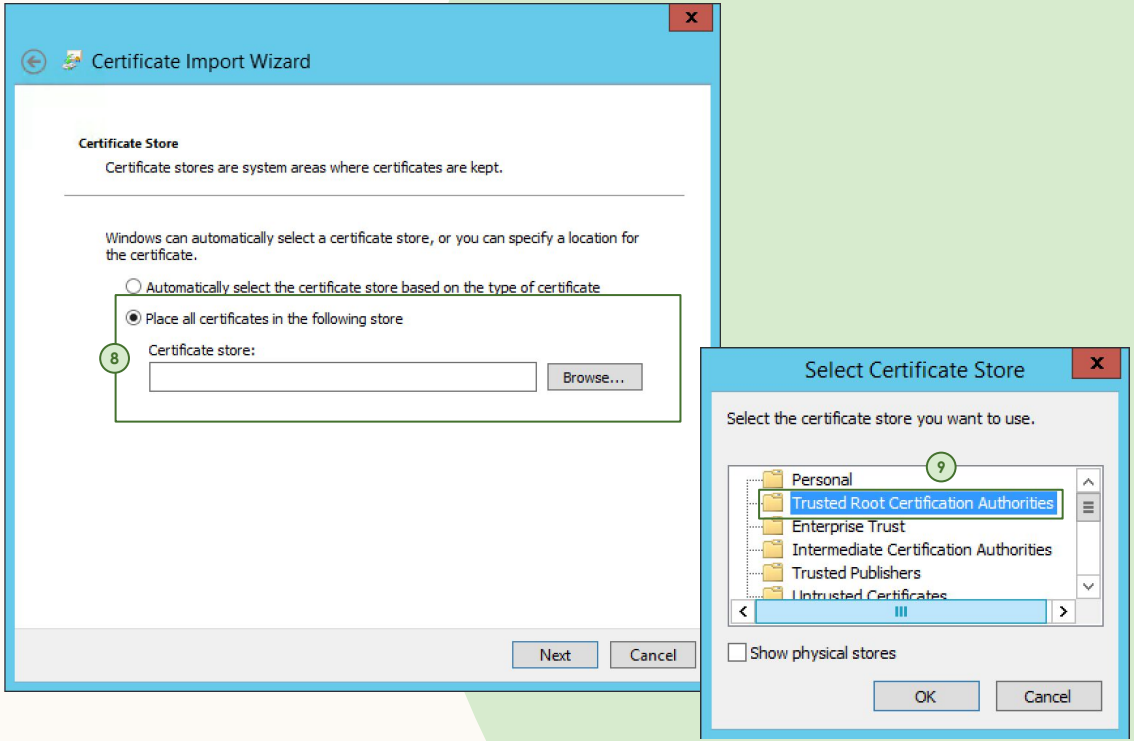
Step 2

Install the Certificate

Part 3 of 3 – Install the certificate

On the next page of the Certificate Import Wizard, configure the store for your Certificate.

8. Select "Place all certificates in the following store", then select Browse
9. In the Select Certificate Store dialog, choose the "Trusted Root Certification Authorities" store
10. Click OK, then click Next and your certificate should now look like the one in [Step 2, Part 1 - Check current certificate state]



Step 2

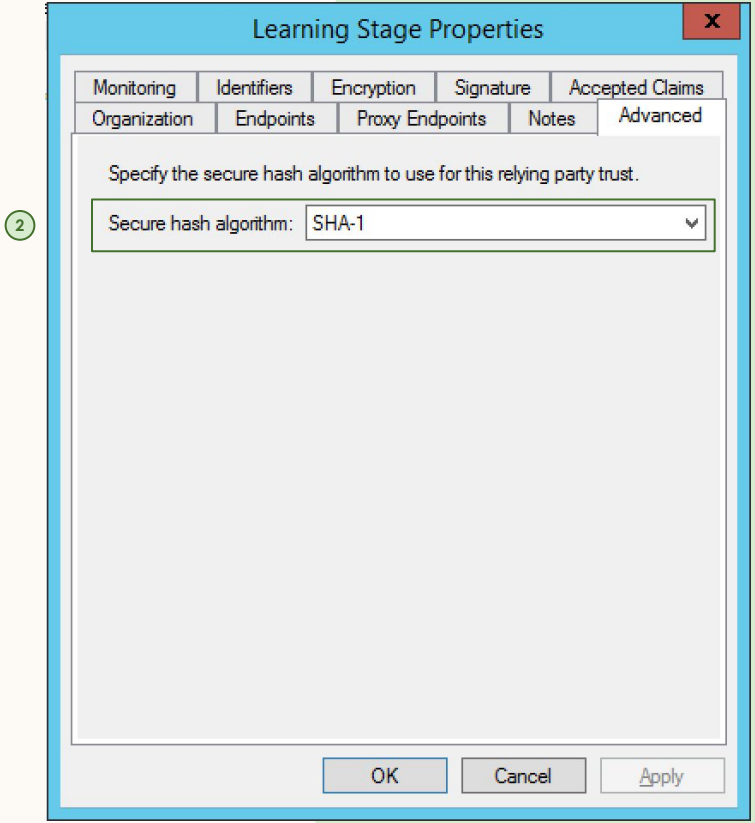
Configure AD FS

Part 1 of 2 – Configure your hashing algorithm

Before uploading your ADFS metadata into Account Center it's best to ensure that ADFS is set up correctly. There are two points we need to ensure are configured correctly:

1. Clicking on your Relying Party Trust within AD FS, and going to Properties, first we need the Advanced tab
2. Change the Secure hash algorithm to either "SHA-1" (recommended) or "SHA256" (if required).

   Note the choice made as this will be used in Account Center later



Step 3

Configure AD FS

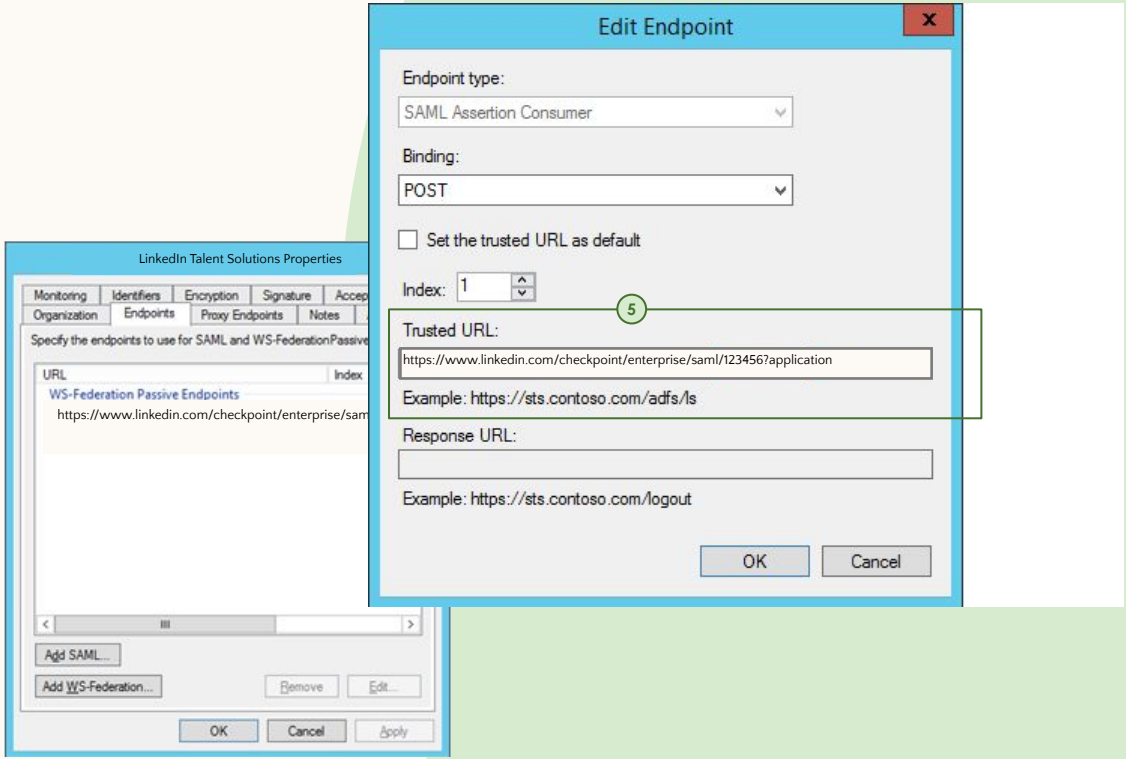
Part 2 of 2 – Configure your hashing algorithm

3. Click on the Endpoints tab. There should be a single URL there configured from the XML you downloaded from Account Center
4. Click on the URL and then click Edit
5. In the pop-up Edit Endpoint dialog:

   Copy the URL from your metadata XML you initially uploaded into ADFS, from the AssertionConsumerService URL

   OR

   Copy it from Account Center directly from the Assertion Consumer Service (ACS) URL field. Click on the link underneath the Configure your Identity provider SSO settings heading to access additional fields in Account Center

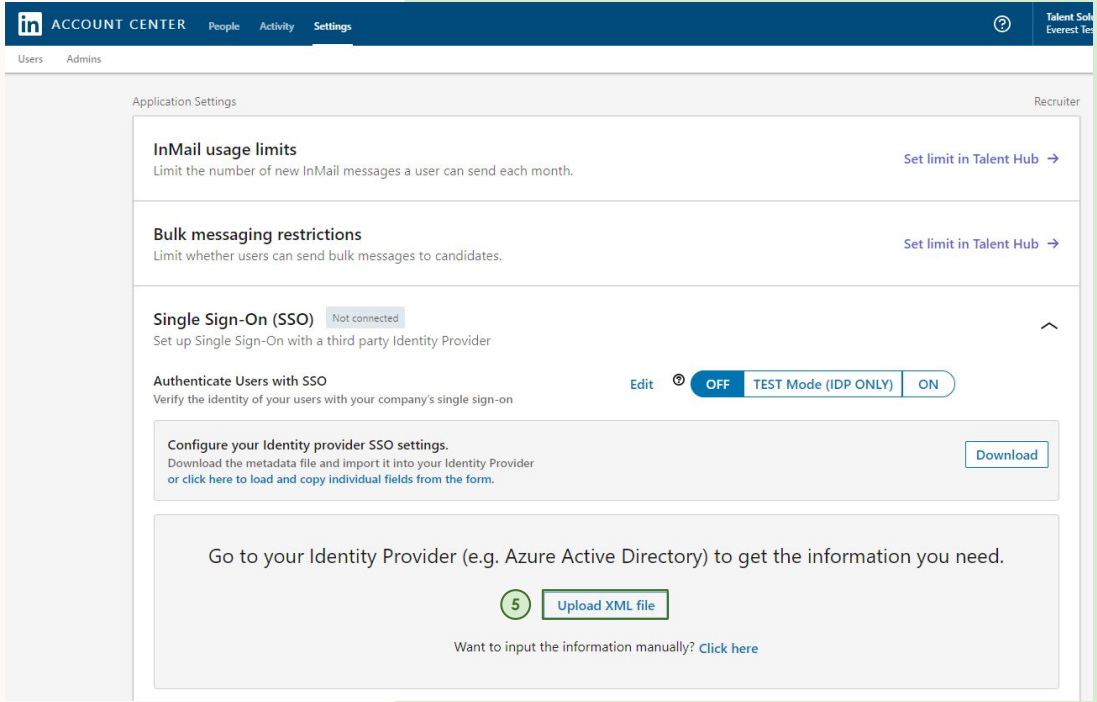


Step 4

Upload your AD FS Metadata into LinkedIn Account Center

We recommend the use of dynamic SSO configuration, letting the systems export XML and talk to each other via pre-configured means using the SAML2 standard. To do this:

1. Use the [ADFS Help Service here] to download your AD FS Metadata. Save this XML.
2. Log into LinkedIn Account Center and navigate to [Settings].
3. Expand the Single Sign-On (SSO) panel
4. Click on the "Upload XML File" button
5. Find your saved XML and upload

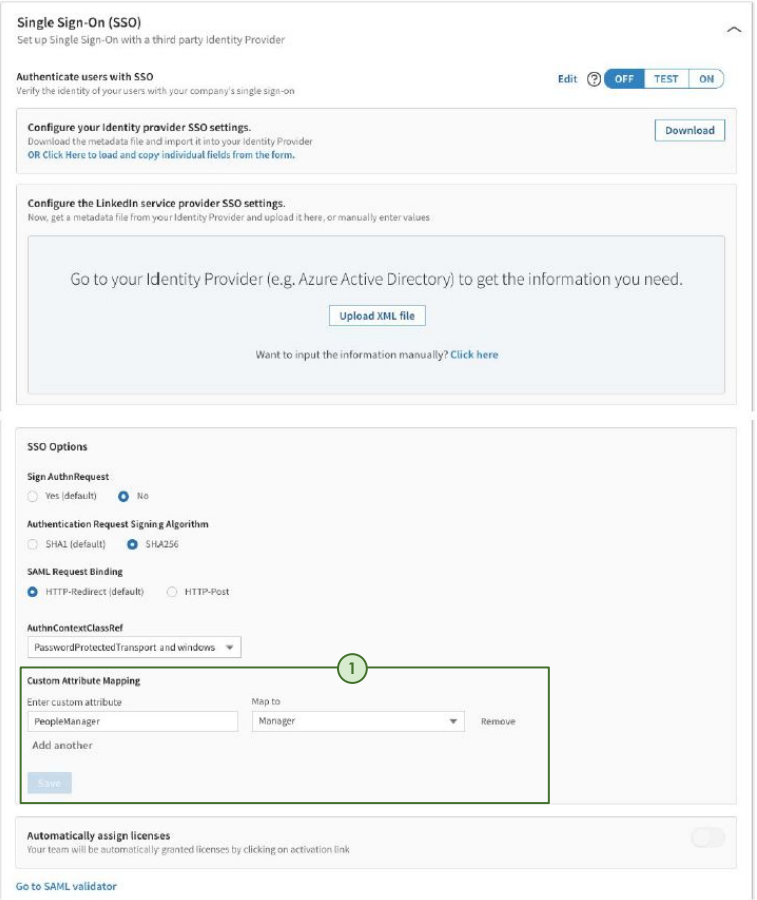


Step 4
Complete SSO settings in Account Center

Once configuration of your Azure AD Application and Account Center is complete, you can adjust settings within Account Center.

Defaults are set for the most common scenarios. Consult with your in-house IT Security team about making any changes.

1. If you added User Attributes & Claims to your Enterprise Application (Step 1 Part 9) you can configure them in Account Center here



NOTE:

Fields to map Attribute Statements to in Account Center include:

- Building Code
- Department
- Desk Location
- Job Function
- Job Level
- Manager
- Mobile Phone Number
- Primary Email Address
- First Name
- Last Name
- Worker Status
- Worker Type
- Work Title
- Work Phone Number

Step 5
Activate SSO in LinkedIn Account Center

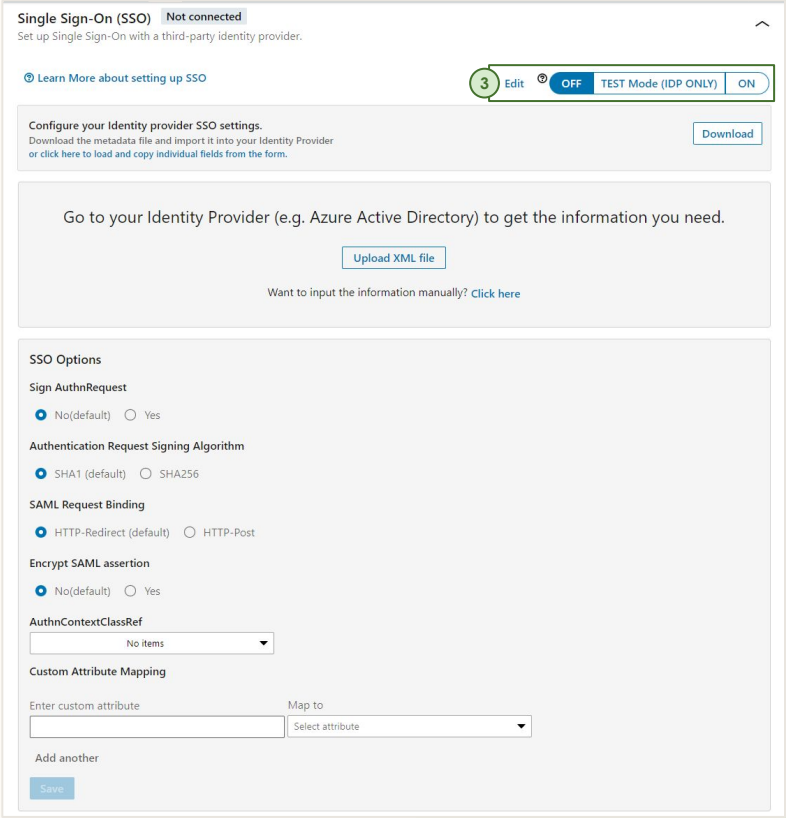
The final step is to switch on SSO within LinkedIn Account Center:

1. Go to the Settings tab at the top of the screen
2. Expand the Single Sign-On (SSO) panel
3. Select either:

   TEST Mode (IDP ONLY) to enable SSO for IdP-initiated login flows only, and still allow normal login to Recruiter / LTI via LinkedIn.com (learn more)

   OR:

   ON to enable and require SSO for all users and login flows accessing Recruiter or LTI on this dashboard.



Thank you

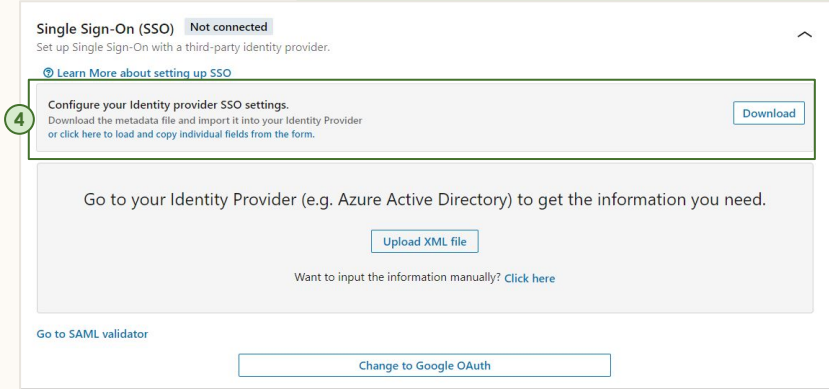
LinkedIn

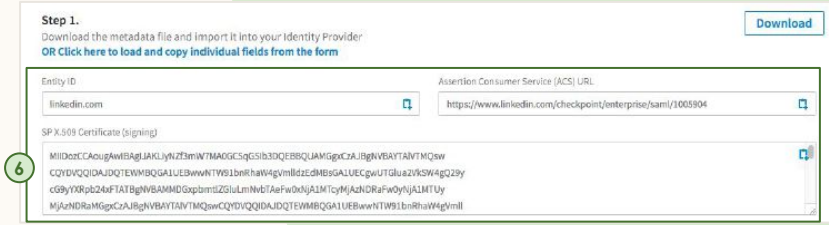
Appendix

Step 1 (alt):
Configuring LinkedIn metadata in your IdP (manually)

If you can't upload XML into your IdP, you can configure LinkedIn Account Center manually.

1. Log in to LinkedIn Account Center
2. Go to Settings
3. Expand the Single Sign-On (SSO) panel
4. In the **Configure your Identity Provider SSO settings**, select **Click here to load and copy individual fields from the form**
5. Log in to your IdP
6. Configure a new Application
7. On the Application Configuration, copy the values loaded in Account Center to the appropriate field in your IdP

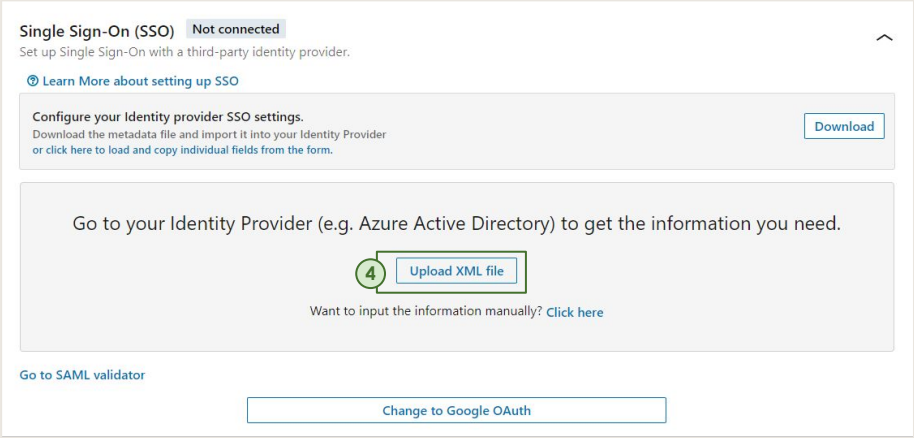


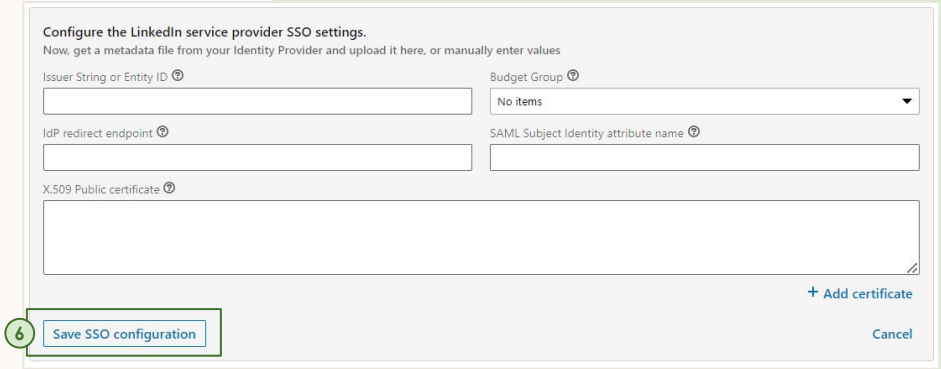


Step 2 (alt):
Configuring IdP metadata in Account Center (manually)

If you can't download a metadata XML file from your IdP, you can configure the required fields in Account Center manually.

1. Log in to LinkedIn Account Center
2. Go to Settings
3. Expand the Single Sign-On (SSO) panel
4. Underneath the **Upload XML file** button, click on "Click here"
5. Copy the values for each field from your IdP
6. Click **Save SSO Configuration**





How often do users need to log in?

Product	Current session length	Definition	Can customers configure?	Notes
LinkedIn.com	365 days (fixed)	How often users must re-enter their email and password to access LinkedIn.com (flagship)	No	
Talent Solutions Recruiter and LTI	30 days (fixed)	How often LinkedIn Hiring products require a user to re-enter their flagship credentials	No	If you've logged in to LinkedIn.com **in the last 15 minutes**, we won't ask you to re-enter your credentials to access Recruiter. If it's been **more than 15 minutes,** you will need to re-enter your LinkedIn credentials to access Recruiter.
Single Sign-On	8 hours (changeable)	How often Recruiter will re-ping a user's identity provider to re-authenticate *(Note: how often you have to re-enter your IdP email/password depends on the IdP session length, see below)*	Yes	The default SSO session length is 8 hours. To adjust the SSO session timeout, please raise a support ticket with LinkedIn. For accounts with multiple LOBs using SSO (e.g. different departments use Recruiter, Learning, or SalesNav), a user's SSO session length will depend on the last application the user accessed.
Identity Provider (e.g., OneLogin, Okta, etc…)	Differs per provider	How often the IdP requires a user to re-enter their credentials	Yes	You should be able to configure this through your IdP. LinkedIn cannot adjust this session length.

Note: If your users experience different session lengths, ask them to check their browser cookie settings—if cookies are disabled, they will be prompted to log in every time. Also check if they are seat sharing and/or using a different browser, as these can also affect session lengths. If the issue is still not resolved, please raise a support ticket.

Sample email to send to your employees

Comms before launching SSO - set expectations for user experience when logging in.

Hi [NAME],

I hope this email finds you well. [COMPANY NAME] will be ramping a new security feature for LinkedIn Recruiter / Talent Insights called Single Sign-On (SSO). SSO will help us boost security by acting as an extra layer of protection against unauthorized Recruiter / Talent Insights users.

What does this mean for you?

As a user, you'll be asked to enter in your [IdP name] credentials before logging in to Recruiter or LTI. This extra step helps us ensure the security of our data. After you log in, you can use Recruiter and LTI as normal.

If you experience any issues logging in, please contact your Recruiter or Talent Insights admin or log a ticket with LinkedIn support.

Thanks for your support,

<<YOUR NAME>>

Additional Resources

Set up Single Sign-on for Recruiter (Help Center article)

SSO FAQ (English)

LinkedIn privacy policy

LinkedIn security email
security@linkedin.com

User email updates

To update the email address of a small number of users
Updating a user to work email in Account Center (admin guide)

To update the email address of multiple users in bulk

1. Assign unique user IDs to bulk manage users in Account Center
2. Edit user attributes in bulk via CSV in Recruiter