conductor

Conductor Single Sign-On (SSO) Integration Guide

Conductor provides two methods for our users to access the Conductor platform:

- Username and password on our sign-in page
- Single Sign-On (SSO) through a SAML-enabled identity manager

Using SSO lets your Conductor users access the platform using the credentials they use for your organization's internal tech ecosystem. Many large organizations require or prefer SSO credentials to accommodate specific security needs.

For organizations interested in enabling Conductor's SSO sign-in option for their account, this guide provides an overview of the steps involved and the technical specifications for your organization’s IT team to set up the integration.

Who Should Use the Conductor SSO Integration?

For some organizations—especially those managing sensitive user data (such a PII, financial info, etc.)—managing user identity themselves may be preferable to using Conductor’s default user management system (username and password entry on Conductor’s sign-in page).

Using SSO, organizations can maintain control over the users that have access to data in its Conductor account by applying the organizations’ user password security policies.

How It Works

Your organization’s IT team can create this integration through the industry-standard SAML 2.0 authentication protocol. Through this protocol, Conductor acts as the “Service Provider” (SP) and your organization hosts the “Identity Provider” (IdP) that the integration uses to authenticate users.

Conductor uses an SP-initiated SSO flow, which lets users be automatically redirected to the IdP. From a technical perspective, this is how the flow proceeds:

1. A Conductor user with an SSO-enabled profile requests access to Conductor.
2. Conductor’s SP Federation Server responds to the user’s browser with an HTML form (“AuthRequest”), and submits the form automatically to your organization’s IdP.
3. How the next steps occur depends on whether the user already has an active session with the IdP:

- If the user does not have an active session:
    - i. Your organization’s system prompts the user for their credentials.
    - ii. Your IdP submits an HTML form (“AuthResponse”) to the Conductor SP Federation Server.
    - iii. The user is authenticated, and the system redirects the user’s browser to Conductor.
- If the user has an active session with the IdP:
    - i. Your IdP automatically submits an HTML form (“AuthResponse”) to the Conductor SP Federation Server.
    - ii. The user is authenticated, and the system redirects the user’s browser to Conductor.

Can I use an IDP-initiated SSO flow?

No, Conductor supports only SP-initiated SSO flows. Accordingly, your organization should not add Conductor to your IDP as a method for your organization's users to access the Conductor platform. Any IDP-initiated flows will not allow access to Conductor.

Integration Process

There are a few steps that are common for all integrations. Depending on your organization’s unique requirements, these steps may differ slightly.

Planning

You will want to have a quick kick-off meeting with your Conductor team and your organization’s IT team (and any other stakeholders). Consider discussing:

- The SSO flow between Conductor and your organization’s user identity management system described above.
- The integration and onboarding process described below.
- The technical details of the SAML SSO integration.
- Your organization’s security policies (if any).

Resolving any questions around these items will help avoid confusion or unset expectations during the integration process.

Configuration

The SAML SSO integration configuration requires the following actions regarding:

- Conductor’s SP
- Your organization’s IdP
- User access

Send Required Details from the Conductor SP to Your IT Team

Your IT team will need the following information about the Conductor SP:

- Entity ID
  https://auth.searchlight.conductor.com/saml/metadata
- Subject NameId Format
  urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- Metadata XML
  Can be downloaded from *https://auth.searchlight.conductor.com/saml/metadata*
- Single Sign On URL / Assertion Consumer Service (ACS) URL
  https://auth.searchlight.conductor.com/saml/SSO
- Direct link to initiate SSO
  https://auth.searchlight.conductor.com/login/<alias>
- Certificate
  Is derived from the metadata.

Send Required Details from your Organization's IdP to Your Conductor Team

Your IT team will need to send the following details about your organization's IdP to your Conductor team. Conductor's Engineering team must add this information to the Conductor platform for the integration to work:

- Entity ID
- Metadata XML
  (Either the file itself or a URL where it is hosted. Note that the metadata must be signed)
- Certificate
  (Optional. This can be derived from the XML metadata)
- User session inactivity timeout, in minutes
- Sample of SAML AuthResponse (Assertion) message
  - Attribute name of First name
  - Attribute name of Last name

Configure Access to Users

For users to have access to the Conductor platform through your organization's SSO, they must be provisioned on both your organization's SSO platform and on the Conductor Platform. After both your IT team and the Conductor team finish configuring the integration with the information described above, be sure to perform both of the following actions:

- Your IT team must provision Conductor to users in your organization's SSO management platform.
- Indicate to your Conductor representative how you want your users to be provisioned in Conductor:
  - When auto-provisioned, any user who signs into Conductor using your SSO will have a Conductor user profile created for them automatically.

    - When not auto-provisioned, you will need to add users individually before they are able to sign in to the Conductor platform through the SSO integration.

Testing

Your IT team can begin testing once the initial configuration is complete on both sides of the integration. They can verify that the IdP appropriately handles the AuthRequest message and Conductor engineers will verify that the SP correctly handles the AuthResponse message.

You can complete testing by adding a test user or editing a live user in the Conductor platform and configuring them to use SSO. To do this, you can follow the directions found in the relevant Conductor Knowledge Base article below:

- Adding a user: *https://support.conductor.com/hc/en-us/articles/214209957-User-Setup#01GDEAR93VF2K1E60P7NFKV6T0*
- Editing a user: *https://support.conductor.com/hc/en-us/articles/214209957-User-Setup#01GDEAR93VCVE4Z6CVD8PWQ1D4*

Once you have confirmed that this process works for the test user or a live user, you can proceed.

Onboarding

My Users Are Auto-Provisioned in Conductor

If your users are provisioned in your SSO platform and auto-provisioned in Conductor, new users may access Conductor as soon as the SSO integration is complete. Note the following:

- Auto-provisioned users will have Read-only permissions by default. An Admin user in Conductor will be needed to change those users' permission level. For details about Conductor's different user permissions refer to the What Are the Differences Between User Types in Conductor? Article found here: *https://support.conductor.com/hc/en-us/articles/360000996547-User-Management-FAQs#h_01GCWAGYAMZNFD9M9757FCPH7R*
- Auto-provisioned users will have access to all of the Conductor platform accounts associated with your organization. You can update the access your auto-provisioned users have after they have their user provisioned.

My Users Are Not Auto-Provisioned in Conductor

If your users are provisioned in your SSO platform and not auto-provisioned in Conductor, You can activate SSO access for your organization's users as follows:

1. Your Conductor representative will decide who at your organization (this may be you) should be responsible for granting access to the rest of the users on your account. Note that the user or users granted this task must have Admin permissions to add new and manage existing users. For details about Conductor's different user permissions refer to the What Are the Differences Between User Types in Conductor? Article found here: *https://support.conductor.com/hc/en-us/articles/360000996547-User-Management-FAQs#h_01GCWAGYAMZNFD9M9757FCPH7R*
2. Your Conductor representative will enable SSO for the Admin user or users they identify in step 1 above.
3. The users identified in step 1 and enabled for SSO in step 2 then enable the SSO toggle for all the relevant users in Conductor. To do this, refer to the Edit User Settings article on the Conductor Knowledge Base: *https://support.conductor.com/hc/en-us/articles/214209957-User-Setup#01GDEAR93VCVE4Z6CVD8PWQ1D4*

Once non-auto-provisioned users in the account becomes SSO-enabled, they receive an email indicating that they are no longer able to sign in with standard credentials and that they must sign in using the SSO authentication instead. All SSO-enabled admin users in the account should continue using the SSO toggle when they add new users to the account. To do so, refer to the Add Users to Conductor article on the Conductor Knowledge Base: *https://support.conductor.com/hc/en-us/articles/214209957-User-Setup#01GDEAR93VF2K1E60P7NFKV6T0*