Advarra Single Sign-On (SSO) FAQ

November 2024

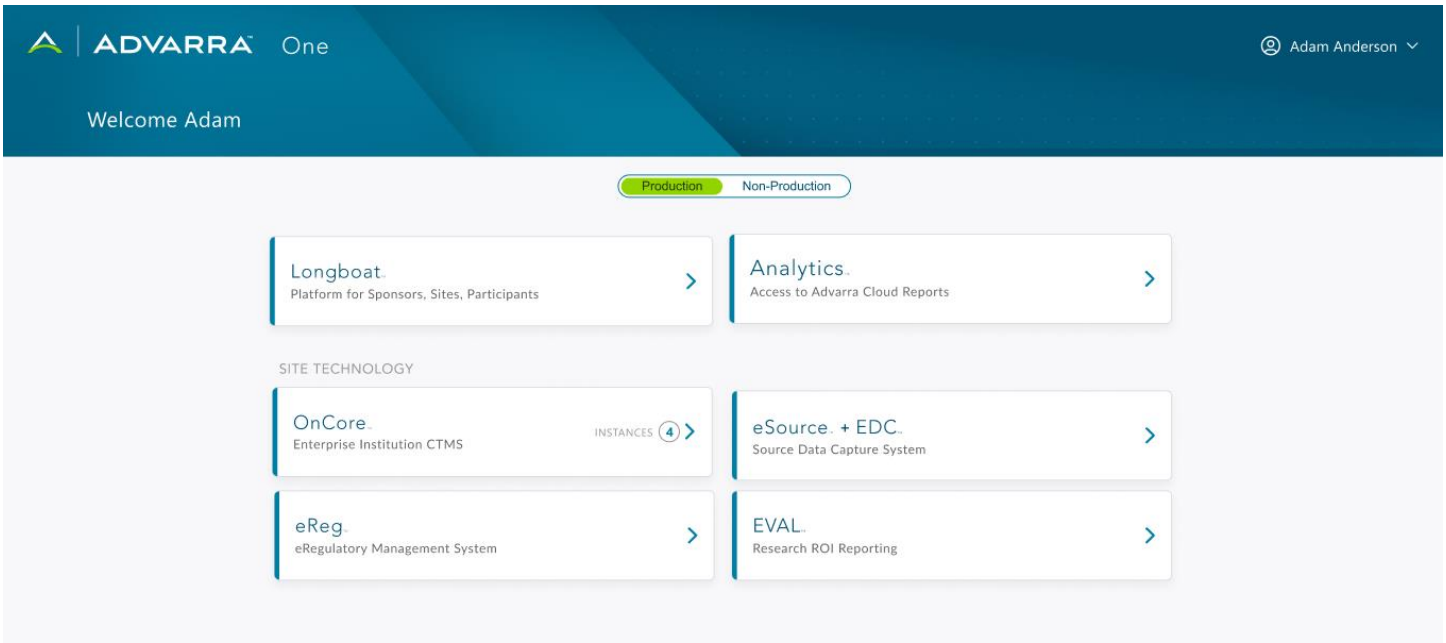
Overview 1
General 2
User Experience 4
SSO End User Support 4
MFA End User Support 6
SAML Setup for Organizations 7
Other 8

Overview

Advarra's single sign-on (SSO) capabilities for user authentication allow users to access SSO-enabled Advarra products in one place using just one set of credentials. After logging in with Advarra SSO, users will see the Advarra One homepage containing tiles for their SSO-enabled Advarra applications. They can then click an application's tile to access it.

Additionally, all site and sponsor users now have the option to log in to SSO-enabled applications using their own organization-sanctioned credentials. This requires a direct authentication connection (SAML). Refer to the **SAML Setup for Organizations** section of this FAQ for more details.

Advarra SSO users who do not have a direct authentication connection will need to authenticate using multi-factor authentication (MFA) through either an authenticator app of their choice or via email. See the **MFA End User Support** section of this FAQ for more information.



General

What are the benefits of Advarra SSO?

Advarra SSO delivers a sought-after process simplification crucial to sites, especially as the number of trial technologies continues to grow. Advarra SSO technology for clinical trial sites and sponsors reduces friction and increases security.

Benefits include:

- A single Advarra One homepage containing all Advarra SSO-enabled application instances
- One user account to access all Advarra SSO-enabled technologies
- A single authentication method for all Advarra SSO-enabled applications
- Improved interconnectivity and general accessibility

What is Advarra One?

Advarra One is a homepage that displays user-specific application tiles. It is powered by Advarra SSO authentication. After a user logs in with SSO, they are directed to the Advarra One homepage where tiles display for any SSO-enabled Advarra application instances to which they have access.

How does my organization set up Advarra One?

If you are replacing your current SAML setup for a product or want to set up your own SAML with a product, Advarra will work with you to set this up. You can initiate SAML setup by submitting the SAML for Advarra SSO form on the SSO Resource Page. A representative from Advarra will reach out to schedule your SAML setup from there.

Requirements, resources, and tasks to complete configuration are listed in the SAML Configuration for Advarra SSO document available on application Learning Portals and the SSO Resource Page.

During setup, your organization's certificate is stored in the Advarra SSO IdP. If the certificate expires, you will need to provide us with a new certificate. The certificate is then updated in the Advarra IdP and restores user access.

How does a user get access to the Advarra One homepage to view their application tiles?

First, a user's record in an Advarra application instance is set to the Advarra SSO authentication realm. If the user's email address does not have an associated Advarra SSO account, the user receives an email to initiate Advarra SSO account setup.

After the SSO account setup is complete, users are brought to the Advarra One homepage. Tiles display on the Advarra One homepage for any SSO-enabled applications where the user's SSO account email address matches the email address in their product user account.

Please note that SSO does not control in-application access or configuration. SSO is only used for authentication into an application.

Will users see tiles for non-SSO-enabled products that they have access to on the Advarra One homepage?

No. Only SSO-enabled products display on the Advarra One homepage.

If my organization already has a single application portal for our applications, including Advarra applications, do we need to make any changes?

Advarra One can be added as an icon to your organization's application portal. An Advarra application icon should be removed from your organization's portal when that specific application adopts Advarra SSO and becomes available through the Advarra One homepage.

After Advarra SSO is enabled for an instance, can it be turned off?

No.

After Advarra SSO is enabled for an instance, can authentication realms other than Advarra SSO be assigned to user records?

No. Only the Advarra SSO authentication realm is available after SSO is enabled for an application instance.

Will the URLs for the current application instances still work after Advarra One is implemented?

Yes. However, Advarra recommends removing former bookmarked URLs and bookmarking the Advarra One URL when an application is using Advarra One.

Is there a customer-facing UI for Advarra SSO account management?

Not at this time. Advarra SSO accounts are created via application user records. Advarra Product Support and/or the Advarra Cloud team will work with you if any issues arise.

What does my organization need to do to implement Advarra SSO?

If your organization has already set up a direct authentication connection (SAML) for Advarra SSO, your end users will log in to Advarra SSO using their organization-managed credentials.

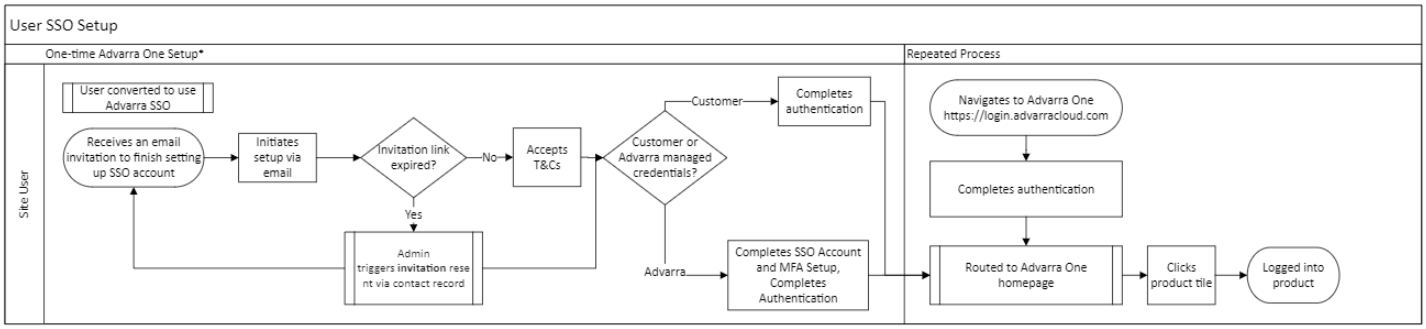
If your organization has not already set up SAML for Advarra SSO, please submit the SAML for Advarra SSO form available on the SSO Resource Page. Advarra will work with you to set this up and ensure you and your end users are prepared for the change.

Does Advarra SSO impact OnCore OAuth and BarTender users?

OAuth users are not impacted by Advarra SSO.

BarTender users will receive an email to set up an Advarra SSO account. However, since these are not actual user accounts, Advarra SSO will not be set up. BarTender accounts will continue to work as they do today without a locally stored password. Advarra will address this situation in a future release.

User Experience



* User completes a one-time SSO setup for the first SSO-enabled product. A user will see additional Advarra One homepage tiles for products when they are SSO-enabled and the user has an active user account in that product.

SSO End User Support

How does an end user activate their SSO account?

Users will be invited to initiate Advarra SSO account setup via an email invitation from no-reply@advarracloud.com. They can click the “Create Account” link in the email to activate their account. After account setup is complete and the user logs in with their Advarra SSO account, tiles for all SSO-enabled applications that they have access to will be available on the Advarra One homepage.

If users haven’t received the email invitation, be sure they check spam/junk folders or organization-level email filters (for example, Mimecast).

Does the email invitation expire?

The link in the Advarra SSO setup invitation email is configured to expire after 72-120 hours.

What if the email invitation expires?

If a user tries to log in to Advarra SSO using old credentials, the system will prompt them to check their email for the invitation to set up SSO. If the invitation has expired, a new email will be automatically sent to the user.

Be sure to use the most recent invite link. When new links are generated, previous links become invalid.

What information is needed for an end user to activate their account?

Advarra SSO requires only first name, last name, and email address to set up. No other identifying information is necessary.

An end user did not receive an email invitation. What now?

Generally, the user can generate a new email invitation by navigating to the application they are trying to access via SSO and entering their email address. If they are not already registered in the system, a new invitation will be sent.

If this does not generate a new email to the user, please contact Advarra Product Support.

My organization uses an email scanning tool (such as Mimecast) that prevents access to the link in the email invitation.

Please contact your internal IT team and ask them to allow emails from no-reply@advarracloud.com. This is the email address the invitation email comes from.

Users are having issues with the link in the email invitation.

Users should navigate to the application they are trying to access via SSO and enter their email. This will prompt the system to send a new email invitation. After they receive this new email and link, they can manually copy and paste the link into the browser instead of clicking the link to access the Advarra One Account Registration page without interference from email scanning systems. They can then fill out and submit the registration form to create their account.

If there are still issues after manually copying and pasting the link, please contact Advarra Product Support

What resources are available for users?

The SSO Help Center is available from the Advarra One login page to help users with registration and login.

When do users see and accept the Advarra Terms and Conditions?

Users see the Advarra Terms and Conditions when they set up their Advarra SSO account and when updates are made to the Terms and Conditions. They can also review them at any time by clicking the Terms and Conditions link at the bottom of the Advarra One homepage.

If customers want to view the Advarra Terms and Conditions prior to the above user workflow, they can do so by submitting a ticket to the Advarra Product Support team.

Will the same Terms and Conditions apply to all users?

Yes.

After an Advarra SSO account is set up, can users return to existing accounts?

No.

Do users need to create a password for Advarra Single Sign-On?

If your organization has set up a direct authentication connection (SAML) for Advarra SSO, users will be able to log in with their organization-managed credentials. They will not need to create a password.

If your organization does not yet have SAML set up, users will be prompted to create a password during account setup.

How can end users change their passwords?

If your organization set up a direct login connection to Advarra SSO, then user passwords are not managed by Advarra, and users must work with your organization to update their passwords.

If your organization didn't set up a direct login connection to Advarra SSO, then users can follow these steps to change their password from Advarra One:

1. On the Advarra One homepage, go to the user menu > Change Password. To access the user menu, click your name in the upper right corner of the Advarra One homepage.
2. The Change Password page opens.
3. Enter and confirm your new password. Make sure your password meets the criteria listed below the Confirm Password field.
4. Click Update.

Can users unlock their account if they get locked out?

If your organization set up a direct login connection to Advarra SSO, then user passwords are not managed by Advarra, and users must work with your organization to regain access to their account.

If your organization didn't set up a direct login connection to Advarra SSO, then users can contact Advarra Product Support to have their account unlocked.

How can users change their first or last name with Advarra SSO?

Please contact Advarra Product Support.

Can users change their email address associated with Advarra SSO?

Please contact Advarra Product Support.

How do I submit a support request for additional help?

If you have any further questions, contact Advarra Product Support.

MFA End User Support

Are users required to set up MFA with Advarra SSO?

If your organization set up a direct login connection to Advarra SSO, users will use your usual organization authentication. You will not be prompted to set up Advarra SSO multi-factor authentication if this is in place.

If your organization did not set up a direct login connection to Advarra SSO, you will need to set up MFA.

How does the end user set up MFA for their Advarra SSO account?

If the end user is new to Advarra SSO, they will be prompted to add an authentication method when they are setting up their SSO account.

If the end user has used Advarra SSO before but has not yet set up MFA, the user will be prompted to add an authentication method when logging in with their SSO account.

For a step-by-step guide on how to set up MFA, please refer to the Advarra SSO page on the Learning Portal or the SSO Help Center.

What authentication methods can be used for MFA with Advarra SSO?

Valid authentication methods include authenticator apps and email verification. Advarra recommends using an authenticator application as the most secure MFA method.

Is there a certain authenticator app end users should use for MFA?

Advarra does not require a specific authenticator app. Users should contact their organization's system administrator with any questions regarding authenticator apps.

How do users get support if they are experiencing issues within their authenticator app?

If there are issues within the user's authenticator app of choice, they should reach out to their system administrator. Advarra does not provide support for third-party authenticator applications.

When do users need to modify their multi-factor authentication setup?

If they're using an authenticator application, users might need to modify their setup when they want to use a new device. If they're using email, they might need to modify their setup if they change their email.

Important: If they're using an authenticator application, it is important to transfer their existing authenticator setup to any new devices. They should confirm authentication is working correctly with their new device before removing the former device.

For a step-by-step guide on how to modify MFA setup, please refer to the Advarra SSO page on the Learning Portal or the SSO Help Center.

Can end users bypass MFA after initial setup?

Users can select the "Trust this device" checkbox to prevent repeated authentication verifications for a limited time.

SAML Setup for Organizations

How does Advarra One change the current SAML setup for site technology products?

Prior to Advarra One, password authentication for many Advarra site technology products was set up per product, per instance. For example, Advarra and the customer would set up SAML for OnCore Production, OnCore Staging, and OnCore Train. The customer would set up SAML the same way for any additional Advarra technologies.

Optimally, the SAML IdP for all products and environments would be the same. However, this could differ depending on each customer's unique environment. For instance, if Production was copied to Staging, then SAML would need to reset before Staging users could log in.

With Advarra One, Advarra SSO services and the customer IdP are set up one time for all products and instances. This reduces the amount of IT maintenance, as they only need to integrate their IdP one time for Advarra site technology products.

Will my organization still have access to SSO-enabled Advarra products if we choose to not set up SAML for Advarra SSO at this time?

Yes. Users will access these applications with their new Advarra-managed SSO credentials.

What if we don't have time to set up SAML prior to the conversion to Advarra SSO?

If your organization does not set up SAML before the user conversion to SSO, end users will need to set up a new password and MFA when registering for Advarra SSO.

My organization is interested in setting up a direct authentication connection (SAML) to use our own credentials.

You can learn more about SAML Setup for Advarra SSO and submit a form to initiate this set up on the Advarra SSO Resource Page. If you still have questions after reviewing this page, please contact Advarra Product Support.

Other

Does adopting Advarra SSO impact how users complete electronic signatures?

Users will continue to use their existing PIN function within eSource + EDC, eReg, and OnCore. In a future upgrade, these products will adopt a universal PIN service that will apply across applications.

How does Advarra SSO manage IdP certificate expirations?

It is important that you take note of the expiration date of your IdP certificate and reach out to Advarra Product Support a few months prior to that date. Advarra will replace expiring IdP certificates. Please ensure that you are timely in this outreach, as a lapse in certification validity will prevent all users on that IdP from accessing Advarra applications.

Is SSO available for all Advarra products?

Longboat, OnCore Cloud, and Advarra Analytics are connected to Advarra One through Advarra SSO, and eReg, eSource + EDC, and EVAL will be connected in the coming months. As we continue to add new Advarra applications to Advarra SSO, you will be using Advarra One to access these systems.

Are there any validation impacts due to this change?

There should be no validation impacts due to this change. Be sure to follow your organization’s change management SOPs.