Advarra Single Sign-On (SSO) FAQ

August 2025

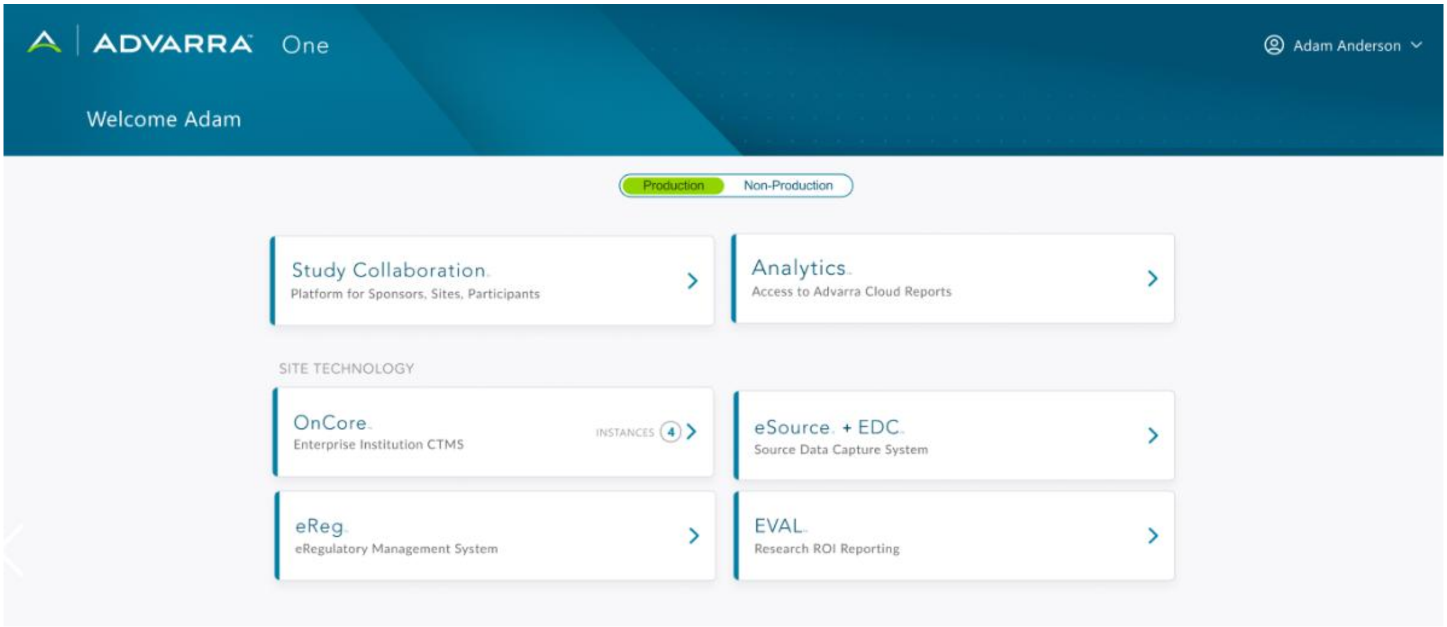
CONFIDENTIAL

Overview

Advarra's single sign-on (SSO) capabilities for user authentication allow users to access all 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 the application tile to access it.

Additionally, all site and sponsor users can now log in to SSO-enabled applications using their own organization-sanctioned credentials. This requires a direct authentication connection (SAML or OIDC). Please refer to the **SAML or OIDC 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. Please 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 products and instances
- One user account to access all Advarra technologies
- A single authentication method for all Advarra 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 (or OIDC) setup for a product, or want to set up your own SAML (or OIDC) with a product, Advarra will work with you to set this up. You can initiate this setup by submitting the SAML or OIDC for Advarra SSO form on the SSO Resources page. A representative from Advarra will reach out to schedule your setup from there.

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

During this 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.

Is SSO available for all Advarra products?

Advarra Study Collaboration, OnCore Cloud, Advarra eClinical products (eReg, EDC, and EVAL), Advarra Analytics, and Protocol Optimization are connected to Advarra One through Advarra SSO. Clinical Conductor 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.

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 appear on the Advarra One homepage.

Will the tiles include non-prod access?

There is a separate tile for each application instance. If you have access to a prod and a staging/test instance, you will see two tiles. Production and non-production tiles are separated by a filter at the top of the Advarra One homepage.

After we have SSO set up, can we turn it on in non-prod applications for an extended period before turning it on in prod?

Yes. This will be part of your transition plan. SSO will first be enabled in your non-prod instance(s) for a product prior to enabling for prod.

How quickly will the tile(s) appear/disappear when activating/deactivating via an application?

The tile(s) will appear immediately. There is no delay.

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.

How is permission handled for applications on the landing page once the user is authenticated via SSO? For example, some users can access all apps while other users can only access certain apps.

Users see tiles for applications for which they have an active user account. If a user is added to an application, that application tile will appear for the user. If a user is inactivated in an application, the tile will be removed. The application itself verifies that the user is active within the application before completing an SSO login.

Are there domains specific to Advarra SSO that my organization needs to allow users to access?

Yes. To ensure users are able to successfully log in to Advarra products with Advarra SSO, your organization's firewall and security policies must allow users to browse to the following domains:

- advarracloud.com
- advarracloud.au
- advarracloud.eu
- clinicalconductor.com
- cctrialsuite.com
- longboat.com
- forteresearchapps.com
- advarra.app

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 (https://login.advarracloud.com) 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.

We have a general support user account for our Advarra support team. What will this look like after converting to Advarra SSO?

After SSO is enabled, the support user will be inactivated. Instead, invite individual product support users via SSO. Their access to SSO is tied to their corporate Advarra login. They will no longer be able to access Advarra SSO or your application once deactivated at the corporate level.

Who provisions users to the Advarra One homepage?

Application administrators provision users to Advarra One. The only way for a user to gain access to the Advarra One homepage is for the user to have access to an application within the Advarra SSO authentication realm.

For customer-managed user accounts, is the name information for SSO coming from our contacts records?

Currently, you are able to store name information in both the application (in the contact record) and in SSO. It is on our roadmap to sync these fields automatically in the future.

How does Advarra determine if the email address provided for a user is their primary email address?

The IdP typically has an internal attribute that is mapped to a SAML or OIDC response attribute. Once the user is active in SSO, there is an internal ID that links the user in the application to their Advarra SSO account. Email address is the primary identifier used during the registration and login process. Admins adding new users would need to use the value of that attribute as the email when creating the user.

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

If your organization has already set up a direct authentication connection (SAML or OIDC) 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 or OIDC for Advarra SSO, please submit the SAML or OIDC for Advarra SSO form available on the SSO Resources page. Advarra will work with you to set this up and ensure you and your end users are prepared for the change.

Can my organization's admins be involved in setting up or assisting users with their Advarra SSO account?

You will retain some tools to troubleshoot site tech product login issues independently (such as the "resend activation email" action). For more advanced troubleshooting of user login issues, you will need to reach out to Advarra Product Support.

Please note that Advarra SSO user login issues will be triaged based on priority. If the login need is high priority, the ticket and turnaround will be treated as high priority.

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.

When will Advarra SSO be mandatory for applications that already have the option to use it? My organization uses multiple Advarra applications – can we convert all systems and users at the same time?

There is not currently a mandatory date to convert all Advarra systems, but we will be sure to communicate that when it's been defined. We plan to have all Clinical Conductor + eClinicals customers converted to Advarra SSO by the end of 2025.

Advarra will work with you on a timeline and a plan that makes the most sense for your organization's needs.

For OnCore, is Advarra SSO only available for the Cloud (AWS) hosted OnCore (as opposed to AMI/on-prem)?

Correct. Advarra SSO is only available with OnCore hosted on Cloud (AWS).

Is there a cost to using Advarra SSO for all products?

There is no additional cost to customers to use Advarra SSO. Any fees associated with Advarra SSO are covered as part of your organization's annual license fee for the product(s).

Do we have the option to not implement Advarra SSO?

Customers are required to implement Advarra SSO to ensure that security and compliance needs are met. Advarra will work with you on timelines to ensure you're prepared for the change.

Will users still be able to sign documents from their phones with the eReg authentication realm?

Yes. The Advarra SSO conversion will not impact the ability to use a phone to sign documents.

Will we need to change the OnCore email for eReg users to match what Advarra SSO will use for authentication?

Yes. If you use the Hub to sync your users' OnCore and eReg emails, the email needs to be the same. The Advarra SSO email (the email in both OnCore and any eClinical applications) needs to be the one used as primary email by the IdP. Once the eReg user record (Hub linked application) has been updated to the Advarra SSO auth realm, the email cannot be updated directly in eReg or in OnCore via the Hub.

Is SSO setup related to Advarra products moving to AWS (Amazon Cloud) hosting?

Yes. Advarra SSO functionality relies on the AWS infrastructure.

Can one email address be authenticated via different means at different institutions?

No. One email address equates to one Advarra SSO account that can only be authenticated in one way. This allows a user to have a single SSO account to access multiple application instances, even for different organizations.

If a user logs into Advarra SSO and then navigates to more than one application, what happens when they log out of one application while still using the other? Are they automatically logged out of all applications?

Logging out of a single application will log you out of your entire Advarra SSO session, including any other apps you are logged into.

Will we have the ability to make configurations (such as inactive session timeout) more strict than the default Advarra SSO values? Can these configurations be set at the application level?

Yes. Advarra One will enforce the max values that can be set in an application instance, but these values also can be updated to be less than those maxes.

What contact information needs to be reviewed and updated to get ready for Advarra SSO for Advarra eClinical applications (eReg, eSource + EDC, and EVAL)?

The user’s record email address field must be the same in all products. The email address in the contact records for Advarra SSO-enabled applications must also match the email address that your IdP returns in the email claim. The work usually involves reviewing the email addresses that are in the IdP against those in OnCore, eReg, eSource + EDC, and EVAL.

If our OnCore is not on Cloud, and the eReg system is linked, can eReg adopt Advarra SSO?

eReg can adopt Advarra SSO before OnCore moves to the Cloud (AWS). Note that once a eReg user record has been updated to the Advarra SSO auth realm, the email cannot be updated directly in eReg or in OnCore via the Hub.

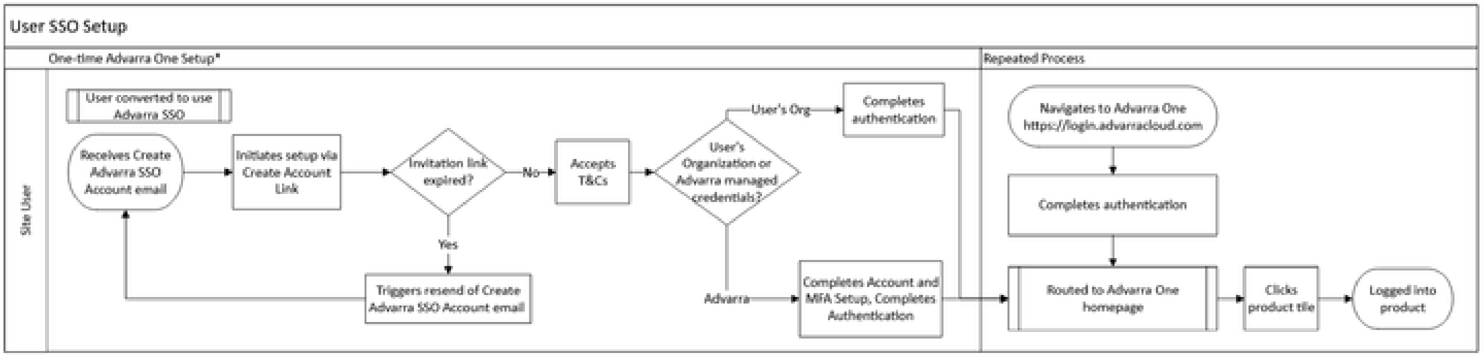
Is Advarra SSO available for sites that host On Prem or on AMI?

Currently, applications hosted on prem do not have access to Advarra SSO functionality, as it is hosted on AWS.

Can our site still control user application access within the application?

Yes, the active field on the user account determines if the user can log into the application. Setting the user to inactive also removes the tile from the user's home page.

User Experience


User SSO Setup
One-time Advarra One Setup*
Repeated Process
Site User
User converted to use Advarra SSO
Receives Create Advarra SSO Account email
Initiates setup via Create Account Link
Invitation link expired?
No
Yes
Triggers resend of Create Advarra SSO Account email
Accepts T&Cs
User's Organization or Advarra managed credentials?
User's Org
Completes authentication
Advarra
Completes Account and MFA Setup, Completes Authentication
Navigates to Advarra One https://login.advarracloud.com
Completes authentication
Routed to Advarra One homepage
Clicks product tile
Logged into product

* 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 Advarra 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).

What if the email invitation expires?

If the link in your email invitation is expired, you are prompted to send a new, valid link to your email. Use that link to complete your SSO registration.

If you continue to have issues or don’t receive a new link, please follow these instructions:

- For OnCore, eClinicals (eReg, eSource + EDC, and EVAL), Analytics, and Clinical Conductor: Your organization’s product administrator can click the “Resend Invitation” button in your user record to generate and send you a new, active email invitation.
- For Advarra Study Collaboration: If you try to log in to Advarra SSO using old credentials, the system will prompt you to check your email for the invitation to set up Advarra SSO. If the invitation has expired, a new email will automatically be sent to you.

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 you want to view the Advarra Terms and Conditions prior to the above workflow, you 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 or OIDC) 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 or OIDC 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.

For OnCore, Hub, and eReg, please note that the email address cannot be updated directly in eReg or OnCore via the Hub once the eReg user record (Hub linked application) has been updated to the Advarra SSO authorization realm.

How do I submit a support request for additional help?

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

Who decides what IdP a given email is associated with (e.g., outside monitors)?

The owner of the email domain decides this. For example, "Ext Org" owns ext-org.com and would work with Advarra to establish an IdP connection.

MFA End User Support

Are users required to set up MFA with Advarra SSO?

If your organization set up a direct authentication connection to Advarra SSO, users will use your usual organization authentication. You will not be prompted to set up Advarra SSO MFA 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.

For users external to our institution, how will MFA be managed by Advarra?

MFA is required for Advarra-managed users. Advarra-managed users new to Advarra SSO will be prompted to add an authentication method when setting up their Advarra SSO account. Users may use email or an authenticator app. 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.

Administrators or users can contact Advarra Product Support for MFA support on an ongoing basis.

SAML or OIDC Setup for Organizations

What is SAML?

SAML uses XML to exchange identity data with the service requesting identity information (in this case, Advarra SSO). SAML requires your technical team to exchange and maintain certificates with Advarra. For more information on SAML, please see the SAML/OIDC Configuration for Advarra SSO document located on the Learning Portal and the SSO Resources page.

What is OIDC?

OIDC is a newer protocol built on the OAuth 2.0 framework. It exchanges data using lightweight JSON web tokens. For more information on OIDC, please see the SAML/OIDC Configuration for Advarra SSO document located on the Learning Portal and the SSO Resources page.

Should my organization set up SAML or OIDC?

Your technical team should carefully consider the benefits and drawbacks of each protocol before making a decision and proceeding.

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.

Is SAML Advarra SSO the same thing as Advarra SSO?

SAML for Advarra SSO is one method for users to authenticate into Advarra SSO. Advarra SSO can authenticate a user via a SAML IdP or by checking user credentials managed by Advarra SSO.

Is this one SAML (or OIDC) setup per institution?

SAML (or OIDC) is set up once per institution; however, each application instance must have SSO enabled and users converted.

Will my organization still have access to SSO-enabled Advarra products if we choose to not set up SAML or OIDC 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 or OIDC prior to the conversion to Advarra SSO?

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

We have users who have already set up Advarra SSO for other applications, but we have not yet configured our SAML (or OIDC) for Advarra SSO. What do we need to do?

This user-level conversion from Advarra-managed credentials to your own IdP-managed credentials (if your IdP is set up later) is automated. No admin actions are required. Once the IdP is configured, the user begins to use your IdP immediately instead of their previous Advarra-managed setup.

Are we able to set up multiple SAML with Advarra SSO? Or do we only need to set up one for our institution?

Routing to SAML IdPs is done by email domain. If the users' email addresses are all on the same domain, we would need one SAML IdP to broker. If they have different domains (e.g., cardio.research.org vs. oncology.research.org), then those can be mapped to different IdPs.

Our organization has multiple email conventions (e.g., user@cardio.research.org vs. user@oncology.research.org) but our SAML is set to return a standard email response of user@email.edu. How will this impact Advarra SSO account setup for our users?

The SAML email attribute must match the email address of the application user account. This is used during the first linking with the IdP.

How will we manage updating SAML certificates with SAML for Advarra SSO?

This will happen similar to how it does today. You can reach out to Advarra Product Support, and we will swap your certs. The advantage is that you only need to do this once, and you will not need to update this for each individual application.

If we already have SSO set up Advarra SSO, do we also need to set it up for an individual product?

If your organization already has Advarra SSO set up, no further setup is necessary as Advarra SSO setup will apply to all product instances that are enabled for Advarra SSO.

For OnCore (AMI or on-prem) customers, will implementing SSO for an eClinical product (eReg, eSource + EDC, EVAL) impact SAML authentication for OnCore users?

No, there is no impact on the OnCore configuration on AMI/on-prem when adding Advarra SSO for eClinical applications.

Can my organization determine which IdP each user utilizes?

This is determined based on the domain at the end of the user's email address.

When will the existing application SAML authentication method stop working?

This is likely to be removed as part of a future release. Advarra will only remove the functionality once we have confirmed that all groups have successfully transitioned to Advarra SSO. Once you set up Advarra SSO, you can remove your legacy SAML settings to ensure that is no longer possible to be used.

After SAML is set up and the app/instance is enabled for Advarra SSO, are users able to log in the old way?

Users are able to log in the pre-SSO way up until the day of conversion. This is intentional so that users are not locked out of access during the transition. If you are interested in an approach where users cannot log in via the old way, you can swap the authentication realms directly in the application for all users. This would force all users to move to SSO.

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

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

External Users

How do we establish external users as Advarra SSO users?

If a user's authentication realm is set to Advarra SSO, they will use Advarra SSO. When we enable Advarra SSO in production, an email will be sent to every active user that does not already have an Advarra SSO account to confirm and create their Advarra SSO account. External users whose email address is not mapped to an IdP will create a password and set up MFA at that time. Once they've completed registration, their realm is automatically switched in the application. The only difference in this process for external users (vs. internal) is if the user's email address maps to an IdP.

I have external users who authenticate through our site IdP but use their organizational email for everything else. Do I need to take any action for these users?

With Advarra SSO, the user's email must be accessible and used for key workflows, such as account activation. That user can use Advarra's IdP or their home IdP if you decide to set up your external users with their organizational email (instead of your site IdP).

Is there an option for Advarra to "sponsor" external users rather than having sites sponsor them?

External users can either be authenticated directly by Advarra SSO (meaning they have a username, password, and MFA set up with Advarra SSO) or by an IdP relationship with Advarra SSO (meaning users are authenticated by that IdP).

If you have additional requirements for sponsorship, please let us know during Advarra SSO implementation.

Is it possible for my site users to be set up on site IdP and my external users set up on Advarra SSO?

Yes, this is possible. However, it is important to note that the external user's home organization will need their IdP set up with Advarra SSO for their authentication.

What is the "home organization" referring to in regard to Advarra SSO?

With Advarra SSO, the "home organization" is the org that owns the domain for that user. This is different than "organization" functionality related to permissions in the application. Advarra SSO does not change or affect the contact record's Home Organization; that will still be controlled by your application admins.

Can only Advarra customers set up an external organization's IdP? Or can other companies, like a CRO, set this up?

We can set up IdPs with CROs and sponsors as long as they agree to have an industry standard user management policy in place, including password and MFA requirements.

If we set up a site IdP for an external user, can we send notifications to their external email? Or will notifications go to the email address that we created for our site IdP?

Currently, application notifications only use the email associated with that user's contact record. It is important that the user's email address is fully accessible for key application workflows (like notifications) and user setup workflows (such as user activation). This email needs to be the one in use by the IdP set up in Advarra SSO.

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.

Will the Advarra SSO tiles include the FileShare site, Zendesk, and Onsemble?

We are exploring future roadmap items for Zendesk and Onsemble.

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.

Will we still be able to use our local authentication accounts without disruption?

With Advarra SSO, current local authentication accounts should be transitioned to Advarra-managed SSO accounts.

If our site and another site have Advarra SSO for the same application (e.g., eReg), what cross-site functionality is available with Advarra SSO?

If you'd like a user from another site to access your eReg application and be authenticated by their "home IdP,” you can add them as a user with the email address they already use when logging in to Advarra SSO. An Advarra SSO user could have access to multiple organizations' eReg instances, if invited.

How does SSO handle users who authenticate with one email address, have their account inactivated, and come back with a new email address (e.g., external monitors who switch companies, staff who leave and work for other organizations with a new email)?

Their email address can be changed if the user is the same person. Please contact Advarra Product Support to request an email address change.

How does Advarra SSO know which applications a user has access to if they use different email addresses for SSO login and application login?

Email address is a unique identifier for an SSO user. If a user utilizes multiple email addresses, then the user would need multiple SSO accounts. In most cases, we would like each user to have just one Advarra SSO account.

What identifier is the application using to determine if the user is active within the application?

The application continues to use the active setting on the user record to determine if the user is allowed to use the application. Users can have an active SSO account in an application even if they've been inactivated in another application.

Does this impact user PINs for signatures in eReg?

Advarra SSO rollout will not impact eReg user PINs.