Advarra SSO Specifications

May 2025

Table of Contents

Overview 2

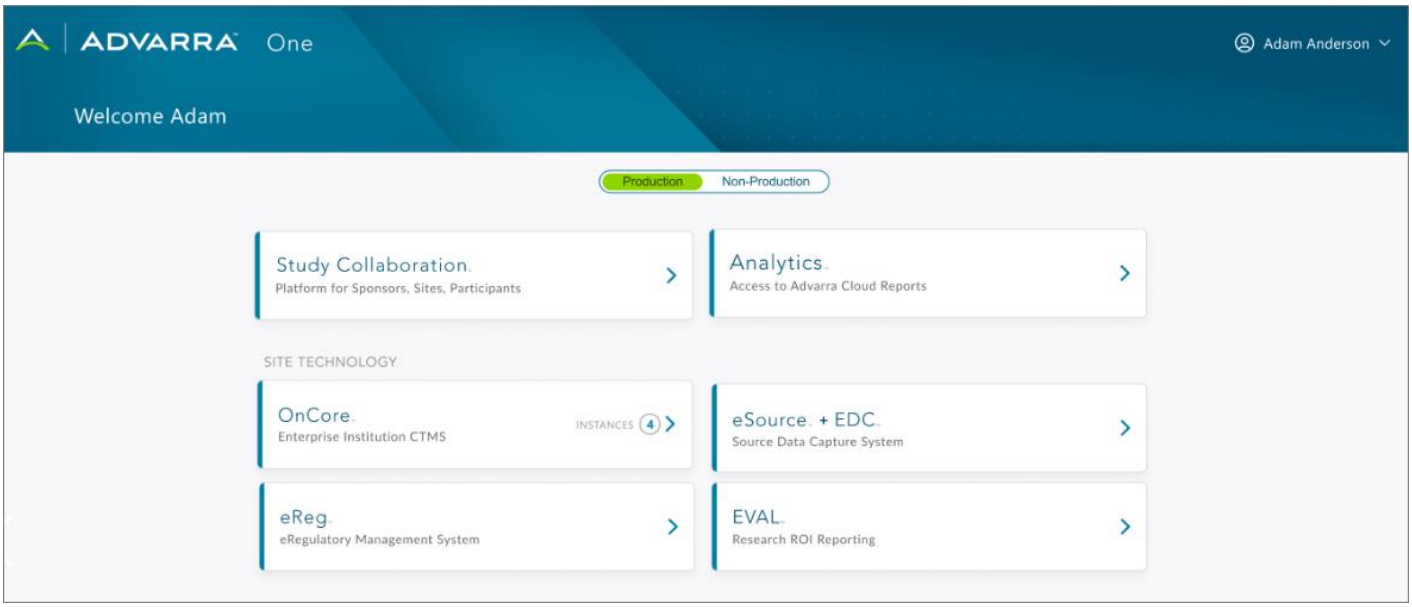
Requirements 2

- Identity Providers 2
- Email Addresses 3
- Access Across Organizations 3
- Passwords 5
- PIN 5
- Multi-Factor Authentication 6
- Timeout/Expiration Settings 6
- Domains to Allow 6
- Additional Resources 7

Overview

Advarra Single Sign-On (SSO) allows users to authenticate securely and efficiently. Users can log in once with a single set of credentials and then have access to all Advarra applications that are on Advarra Cloud and configured to use SSO without needing to log in again to the individual application environments with separate credentials. For organizations using SAML, Advarra SSO reduces the number of SAML connections to maintain to one instead of one for each application instance, as was previously required.

After a user logs in with SSO, they are directed to the Advarra One homepage, where tiles appear for any SSO-enabled Advarra application instances to which they have access. They can then click the tile for the application instance they would like to navigate to.



Requirements

In Advarra SSO, users are part of a global pool of SSO users that SSO-enabled Advarra applications connect to. A user's email address is used to identify and map the user.

Identity Providers

Advarra SSO supports SAML 2.0 and OIDC authentication via an organization's own identity provider (IdP). This allows users to log in to Advarra applications with their organization credentials. Organizations that choose not to set up SAML or OIDC and use their own IdP, or that have users who are not associated with their IdP, can have users use the Advarra IdP. In this case, when users create their Advarra SSO account, they are prompted to create a password.

Email Addresses

In Advarra SSO, a user's email address is used to identify them, and their email domain maps them to the correct IdP for authentication. An organization can use multiple email domains; each email domain must be mapped to a single IdP. If a user's email domain is not mapped to an IdP, the user is prompted to create a password and set up multi-factor authentication (MFA) when they create their Advarra SSO account and Advarra SSO acts as their IdP.

Because Advarra SSO relies on email addresses to identify and map users, users must use the same (unique) email address in all SSO-enabled application instances and cannot use aliases. This means the email address that is sent from the customer IdP must match the email address that identifies the user in each of the applications where the user has an account or the user will not be able to log in.

For example, Bob Smith at Site X has an email address of bob.smith@example.com, but prefers to use an email alias of bsmith@example.com. Bob has a user account created in Site X's OnCore instance using bsmith@example.com as the email address in his contact record. When Bob is sent an invitation to Advarra SSO at bsmith@example.com and completes the Advarra SSO invitation workflow, he is unable to authenticate into Advarra SSO via Site X's IdP. This is because the Site X IdP is sending an email assertion claim that contains bob.smith@example.com, which does not match the provided email address of bsmith@example.com. Bob's email address must be updated in either the Site X IdP or in OnCore so that the same email address is being used by both.

To minimize disruptions to user access, we recommend that organizations verify the email addresses being used to identify users in their IdP and in Advarra applications and reconcile any differences before they go live with Advarra SSO.

> Note: In accordance with industry standards and security best practices, Advarra SSO does not currently support email aliases.

Access Across Organizations

If your organization needs to provide access to Advarra application instances to users outside of your organization, there are three different ways you can have those external users authenticate with Advarra SSO:

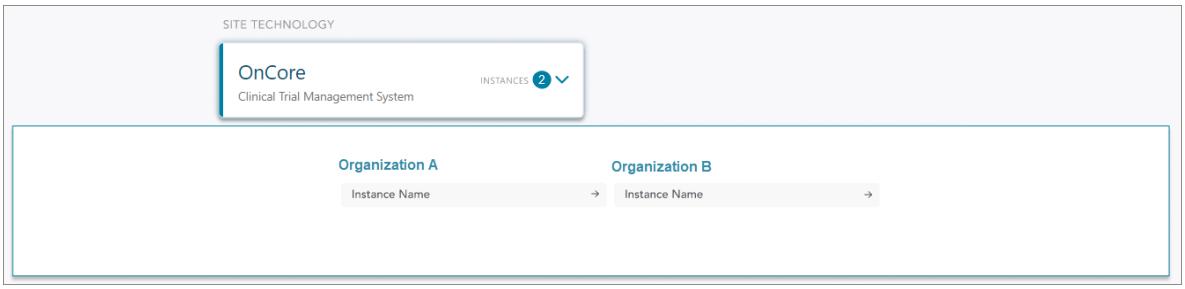
- Using their organization's IdP
- Using your organization's IdP
- Using the Advarra IdP

Your organization always controls users' authorization to access your application instances; at any time, you can inactivate a user's account in an application instance, and the user can no longer see that tile in Advarra One or access that instance. However, you can decide which IdP external users will use to authenticate based on your organization's policies and how you want to manage users. Consider the following factors in deciding which option to use:

Their Organization's IdP

Users authenticate via their own organization's IdP if their organization's IdP is configured to work with Advarra SSO.

- Less user burden. External users can log in with their own organization credentials, using their organization email address and see all the SSO-enabled application instances in which they are an active user, across organizations. They don't need to manage a separate set of credentials.



- Users' ability to authenticate with Advarra SSO is controlled by their organization. Their organization controls the security policy for their IdP.
- Less administrative burden for your organization. You don't need to create email accounts for external users. If a user's employment/access ends, their organization inactivates them, and they can't log in via Advarra SSO or access any SSO-enabled application instances. No extra steps are needed to make sure the user is inactivated for both organizations.

Your Organization's IdP

Users authenticate via your organization's IdP, using an email address with a domain that maps to your IdP.

- Greater user burden. External users must manage a separate email address and credentials. You must maintain email addresses and inboxes for them, as they need to be able to use and access this email for application workflows (notifications, account activation, etc.).
- Users' ability to authenticate with Advarra SSO is controlled by your organization. Your organization controls the security policy.
- More administrative burden for your organization. You must manage email accounts for external users. If a user's employment/access ends, you must inactivate them so that they can no longer authenticate with Advarra SSO.

Advarra IdP

When the user sets up their Advarra SSO account and their email domain isn't mapped to an IdP, they're prompted to create a password and set up MFA, and Advarra SSO acts as their IdP.

- Some user burden. External users can specify the email address to use to authenticate (as long as it matches what's used in their Advarra application accounts), but must manage additional credentials (password, MFA setup).
- Users' ability to authenticate with Advarra SSO is controlled by Advarra. Advarra controls the security policy. Advarra requires strong passwords and MFA to be set up and adheres to NIST and OWASP guidelines.
- Some administrative burden for your organization. You don't need to create email accounts for external users. You need to contact Advarra Product Support to inactivate a user's Advarra SSO account.

Keep in mind that:

- Your organization always controls external users' authorization to access your Advarra application instances. You can inactivate a user's account in an application instance, and the user can no longer access that instance.
- When organizations configure their IdP to work with Advarra SSO, they must agree to adhere to industry standards for user management and security, including strong password and MFA requirements.
- Authenticating with any of the three IdP options offers greater security than previously used local authentication.

- In Advarra SSO, users are identified by their email address, and they must use the same email address for logging in to Advarra SSO and in their Advarra application accounts. In accordance with industry standards and security best practices, Advarra SSO does not currently support email aliases or forward messages to alternate email addresses. If you want external users to authenticate with your organization's IdP but don't want to maintain email inboxes for them, you can consider using an email routing table.
- If a user's email is linked to an organization IdP that is configured to work with Advarra SSO, that organization IdP is used to authenticate the user. They can't opt to use the Advarra IdP with that email. Similarly, if a user is authenticating with the Advarra IdP and the organization IdP to which their email is linked is subsequently configured to work with Advarra SSO, the user will then authenticate via the organization IdP and no longer authenticate via the Advarra IdP.

Passwords

For users associated with an organization's IdP, password requirements are determined by that IdP, not Advarra.

Users who are not associated with an organization IdP and are using the Advarra IdP are prompted to create a password when they create their Advarra SSO account. The following password requirements apply:

- Must be at least 12 characters and contain at least one uppercase letter, one lowercase letter, one special character, and one number.
- Cannot match any of the user's previous 24 passwords.
- Cannot match a password that was detected in a previous data breach. (We use a number of open data sources of previously breached passwords to detect this.)
- Expires and must be reset every 365 days. (Users can reset their password at any time.)
- After 10 failed login attempts within 15 minutes, the user's account is locked for 15 minutes.

We use a salted PBKDF2 HMAC algorithm with a 512-bit derived key and a load factor of 100,000, hashed with SHA-256 to protect user credentials.

PIN

In SSO-enabled applications that use PIN functionality (for electronic signatures or completing certain workflows), users can set and manage their PIN from the Advarra One homepage. The following PIN requirements apply:

- Must be between 6 and 12 digits.
- Must include only digits, and at least two digits must be unique.
- Must be entirely non-sequential in both directions. (112233 is a valid PIN, but 123456 and 654321 are not.)
- Cannot match the current or three previous PINs.
- Expires and must be reset every 365 days. (Users can reset their PIN at any time.)
- After five consecutive incorrect entries, the user's PIN is locked, and the system prevents attempts to enter it again for five minutes.

Note that only Study Collaboration is currently using this functionality. Additional development is needed before other applications can adopt it.

Multi-Factor Authentication

For users associated with an organization's IdP, MFA options are determined by that IdP, not Advarra. Users who aren't associated with an organization IdP and are using the Advarra IdP must set up and use MFA. They are prompted to do this after they enter their Advarra password. Users can select a checkbox to trust their device, which allows them to bypass the MFA challenge for seven days, as long as they are logging in with the same device and browser and haven't updated their password.

Timeout/Expiration Settings

For SSO-enabled application instances, the following are controlled by global settings in Advarra Cloud:

Inactive Session Timeout

For application instances on Advarra SSO, inactive session timeout is set to 30 minutes.

For OnCore (as of OnCore 2024R2), eSource + EDC, eReg, and EVAL users authenticating with Advarra SSO, the Inactive Session Timeout setting in the application (Application Settings > Application Configurations) is respected and used in conjunction with the global setting:

- When users are inactive, they are logged out after the time specified in the Inactive Session Timeout setting or the global setting in Advarra Cloud (30 minutes), whichever is shorter.
- If a user is logged in but doesn't have the application open (for example, they opened the application, but then closed the browser tab without logging out), then the global setting is used.

Absolute Session Timeout

Advarra SSO sessions time out after 12 hours, regardless of user activity. When the SSO session times out, any application instances the user is logged in to with SSO are also terminated.

Invitation Link Expiration

After the necessary setup is complete and Advarra SSO is enabled for an environment, active users are sent an email invitation with a link to create their SSO account. That link is valid for 120 hours.

MFA Verification Code Expiration

MFA verification codes sent to Advarra IdP users via an authenticator application or email are valid for 30 minutes.

Domains to Allow

For users to log in successfully 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

Additional Resources

OnCore and eSource + EDC Learning Portals:

- Advarra SSO page. Provides more information about getting started with Advarra SSO.
- Application Settings > Application Configurations page. Provides information about Application Settings and when they are applied differently or not used with Advarra SSO.
- SAML/OIDC Configuration for Advarra SSO document. Provides instructions for setting up SAML or OIDC with your organization's IdP.

eReg and EVAL Learning Portals:

- Advarra SSO page. Provides more information about getting started with Advarra SSO.
- Configure System Settings page. Provides information about Application Settings and when they are applied differently or not used with Advarra SSO.
- SAML/OIDC Configuration for Advarra SSO document. Provides instructions for setting up SAML or OIDC with your organization's IdP.

Study Collaboration Help Section:

- PIN Service. Provides information about creating and resetting a PIN from the Advarra One homepage.

Advarra One login page > SSO Help Center

- Provides help and resources for users who encounter issues while logging in.