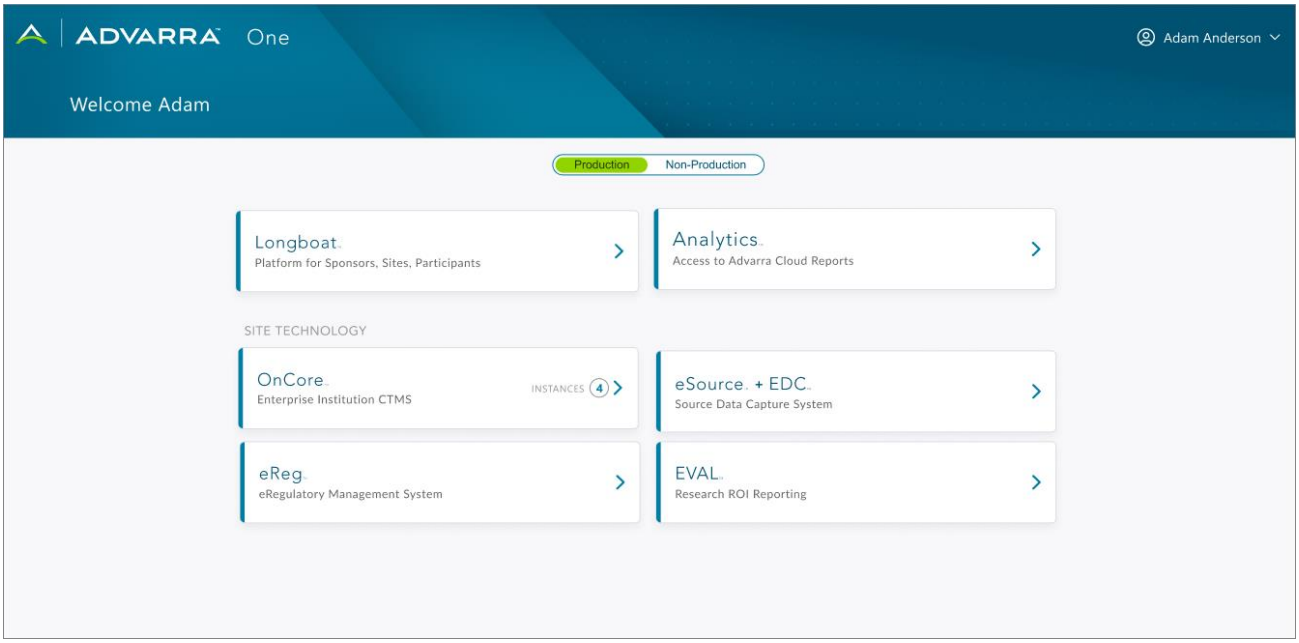
Advarra SSO Specifications

April 2025

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 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.

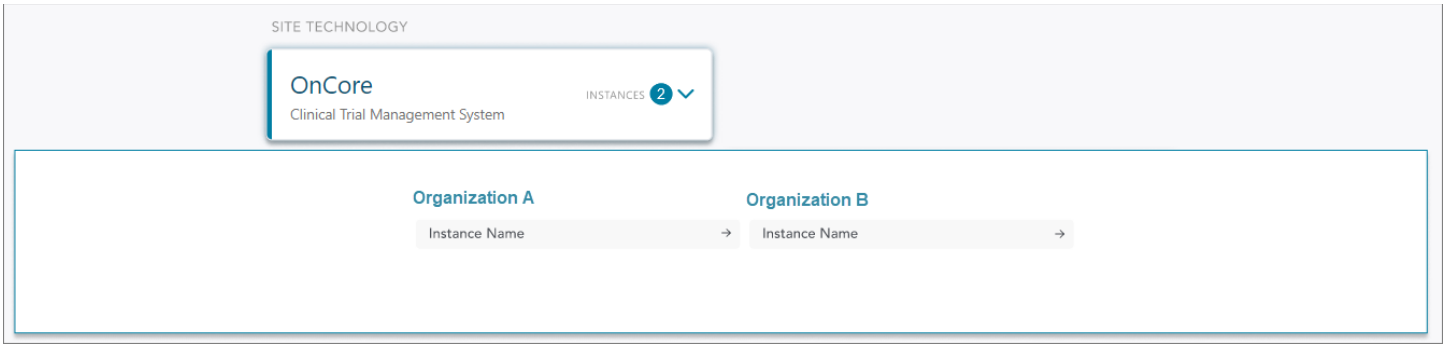
> Note: In accordance with industry standards and security best practices, Advarra SSO does not currently support email aliases.

Access Across Organizations

With SSO, a user can log in once and access all SSO-enabled Advarra application instances in which they are an active user. This can include instances for multiple organizations.

While the user's authorization to access an application instance is controlled by the organization that owns that instance, their ability to authenticate with Advarra SSO is controlled by their home organization.

For example, if Organization B has an affiliate (Organization A) that also uses Advarra SSO and needs to have an affiliate user log in to their OnCore instance to enter data, Organization B can activate them as a user (using their affiliate email address). The tile for Organization B's OnCore instance then appears on the affiliate user's Advarra One homepage.



This means that:

- The affiliate user does not need a separate set of credentials to access Organization B's OnCore instance, as they would have previously.
- Organization B controls the user's authorization to access their OnCore instance, and the affiliate (as the user's home organization) controls the user's ability to authenticate.
    - When the affiliate user no longer needs access, Organization B can inactivate their account in their OnCore instance, and the user can no longer see that tile or access that instance.
    - If the user's employment ends, the affiliate can deactivate the user's Advarra SSO account, and the user can no longer log in via Advarra SSO or access any SSO-enabled application instances. No extra steps are needed to make sure the user is deactivated for both the affiliate and the organization.

Passwords

For users associated with their 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 Longboat is currently using this functionality. Additional development is needed before other applications can adopt it.

Multi-Factor Authentication

For users associated with their organization's IdP, multi-factor authentication (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.
- SAML/OIDC Configuration for Advarra SSO document. Provides instructions for setting up SAML or OIDC with your organization's IdP.

Longboat 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.