

Aras Innovator External Authentication using Aras CIAM

Important

This feature applies to: Aras Innovator deployed from SDE referencing Aras.SaaS.DevOpsFramework.AICD package (Aras DevOps 1.15+)

Aras Innovator in Aras Cloud supports external authentication through the Centralized Identity Access Management (CIAM). CIAM provides a unified identity layer across Aras environments, enabling customers to log into Aras Innovator using a centrally managed identity provider rather than local Aras Innovator credentials.

When CIAM integration is enabled, the Aras DevOps deploy pipeline automatically creates and manages a dedicated CIAM application for each Aras Innovator instance, eliminating manual identity configuration per environment.

For general CIAM documentation, visit <https://docs.aras.com/iam-user-guide>.

High-level process of CIAM authentication configuration

The following high-level steps are required to enable CIAM integration:

1. Confirm prerequisites with Aras Global Cloud Services Team.
2. Configure CIAM application and user mapping according to documentation on <https://docs.aras.com/iam-user-guide>
3. Commit the required transformation file changes to the SDE.
`${CIAM_INTEGRATION_OAUTHSERVER_CLIENTREGISTRY_USERPROVISIONER}` placeholder is added to `OAuth.config`.
`OAuthServer.Plugins.json` uses the four
`"${CIAM_INTEGRATION_OAUTHSERVER_PLUGINS_*}"` placeholders
4. Run the CI pipeline on the target branch.
5. Enable CIAM for the target environment type.
Update the `CIAMIntegrationConfigValues` variable group by setting
`CIAM_integration_environment_<ENV>_enabled = true`



6. Deploy Aras Innovator with CIAM integration.

Run the deploy pipeline for each instance as soon as CI pipeline completed successfully after merge and make sure pipeline log confirms **CIAM application ... is enabled successfully**

7. Verify the instance is integrated with CIAM

