Recast

Single Sign-On Overview

Last Modified on 2026-09-24

By default, Single Sign-On (SSO) is not performed when multiple identity sources are visible to the user, even when explicitly activating SSO.
Either hide other identity sources that are not used for SSO or specify which identity source to use for SSO.

SSO is performed automatically on OAuth 2.0 configurations with a single visible identity source, all other SSO protocols require to explicitly activate SSO.

Activate Single Sign-On

There are a number of ways to activate SSO:

Agent

The Agent supports SSO by setting it to 'true' in the **Login** section of the supplied Agent.xml/Agent.json file, which can be modified on the Recast servers.
When multiple identity sources are visible, you can specify the default identity source by providing the name within the `Login` > `IdentitySource` parameter.

Agent.xml

```
<Login>
  <Enabled>True</Enabled>
  <SSO>True</SSO>
  <IdentitySource>RecastSoftware</IdentitySource>
</Login>
```

Agent.xml file location: `C:\Program Files (x86)\Liquit Workspace\Agent\Agent.xml`

Agent.json

```
{
  "login": {
    "enabled": true,
    "sso": true,
    "identitySource": "RecastSoftware",
    "timeout": 4
  }
}
```

Agent.json file location:
Windows – `%ProgramData%\Liquit\Agent\Agent.json`
macOS – `/Library/Application Support/com.liquit.Agent/Agent.json`

URL Parameters

For more information about available parameters, see URL Parameters.
Activate SSO by adding the `?sso=1` option to the URL.
When multiple identity sources are visible, specify the `identitySource` option to the URL.

Example:

Recast

```
https://workspace.recastsoftware.com/?sso=1&identitySource=AD
```

where `workspace.recastsoftware.com` is replaced by your Recast FQDN.

HTTP Headers

Activate SSO by adding the following HTTP headers (to the request to: /api/identity/domains):

X-Liquit-SSO – Value needs to be set to 1 to activate SSO
X-Liquit-IdentitySource – Value needs to be the name of the identity source to use for SSO.

macOS behavior without platform SSO configuration

When Platform SSO is not configured on macOS devices and Conditional Access policies are enforced, users will experience significant limitations. They will be unable to sign into Application Workspace, which prevents the deployment of applications and restricts access to the Application Workspace Launcher.