How to Configure SAML2 SSO and Session Timeout in Evolve (On-Premises)

Product: Casewise Evolve / erwin Evolve | Versions: 2022.0.0+ | On-Premises Deployments

Overview

This article explains how to enable Single Sign-On (SSO) using SAML 2.0 in Evolve on-premises deployments, and how to view and adjust the session timeout configuration.

Evolve Authentication Modes

- **Windows Authentication** — Direct Active Directory via IIS (NTLM/Kerberos)
- **Forms Authentication** — Username/password stored in Evolve database
- **SAML 2.0** — Federated SSO; recommended for cross-application SSO

> ***NOTE:*** *Windows Authentication cannot share sessions with external applications. To enable cross-application SSO (e.g. from a portal into Evolve without re-authentication), SAML 2.0 must be configured.*

Part 1 — Enabling SAML2 SSO in Evolve

Prerequisites

- An Identity Provider (IdP) already configured: ADFS or Azure AD
- Both source application and Evolve registered as Service Providers in the IdP
- Administrator access to the Evolve server

Step 1 — Register Evolve in your Identity Provider

If using ADFS:

1. Open ADFS Management Console → Add Relying Party Trust
2. Identifier (Entity ID): `https://[your-evolve-server]/`
3. ACS URL: `https://[your-evolve-server]/Saml2/Acs`
4. Complete wizard and configure claim rules to pass UPN/email

If using Azure AD:

1. Azure Portal → Enterprise Applications → New Application → Create your own
2. Set up Single Sign-On → SAML
3. Reply URL (ACS): `https://[your-evolve-server]/Saml2/Acs`
4. Identifier (Entity ID): `https://[your-evolve-server]/`
5. Download Federation Metadata XML — needed in Step 2

Step 2 — Configure SAML2 in Evolve Server Configurator

1. On the Evolve server, open **CwEvolveServerConfigurator.exe**
2. Navigate to: **Security Settings** → **Authentication Mode**
3. Select: **SAML2**
4. Enter your IdP Metadata URL (from ADFS or Azure AD)
5. Click **Save**

Step 3 — Restart IIS

Open Command Prompt as Administrator and run:

```
iisreset /restart
```

Step 4 — Verify

Navigate to your Evolve URL. You should be redirected to your IdP login page. After authenticating once, navigating from other registered applications should not prompt for credentials again.

Part 2 — Viewing and Adjusting Session Timeout

The session timeout controls how long a user remains logged in after inactivity. Three locations control this setting:

Method A — Evolve Server Configurator (Recommended)

1. Open **CwEvolveServerConfigurator.exe** on the Evolve server
2. Navigate to: **Security Settings** → **Session Timeout**
3. Change the value in minutes. Recommended: **60**
4. Click Save, then restart IIS: `iisreset /restart`

Method B — IIS Manager

1. Open IIS Manager
2. Application Pools → [Your Evolve App Pool] → Advanced Settings
3. Process Model → Idle Time-out (minutes) → set to **60**

Method C — web.config

File location: `C:\inetpub\wwwroot\[EvolveApp]\web.config`

```
<system.web>
  <sessionState timeout="60" slidingExpiration="true" />
</system.web>
```

After saving: `iisreset /restart`

Recommended Timeout Values

Environment	Recommended Timeout
Development / Testing	480 minutes (8 hours)
Production (standard)	60 minutes
High-security production	20 minutes

Related Articles

- Move MyErwin from ADFS to Azure for authentication

https://support.accelerite.com/hc/en-us/articles/39341314114701

Keywords: SSO, SAML2, single sign-on, session timeout, IIS, authentication, ADFS, Azure AD, Windows Authentication, Evolve, on-premises

Created by: Anand Kumar | support.accelerite.com