Cloud Basics for Administrators

Single sign-on

9/19/2021

Contents

Learn how single sign-on is supported in Genesys Engage cloud.

Most Genesys Engage cloud applications use single sign-on (SSO) to allow a logged-in user to navigate across supported applications without prompting for credentials again. Genesys Engage cloud can also be configured to use SAML 2.0 for integrations with third-party identity providers (IdP) such as Okta or Google. There are many advantages to enabling SSO in Genesys Engage cloud—for example:

- Users need to remember only one password.
- User credentials are managed by a third-party identity provider.
- Users must have multi-factor authentication by a third-party identity provider for additional security.
- Users only need to log in once to gain access to Genesys Engage cloud applications that have SSO enabled and non-Genesys applications that use the same identity provider.

For details about how a user logs in with SSO, see Log in to Genesys Engage cloud.

IdP-initiated login

Genesys Engage cloud supports IdP-initiated login using the SAML Single Sign-on integration. With this type of login, you can set up your own portal with links to Genesys Engage cloud applications. When a user is logged in to your IdP, they can click a link in the portal and directly log in to the Genesys application.

Set up this functionality in your IdP by providing the URL of the target application as part of the redirect URL. For example, the redirect URL for Agent Desktop would be in this format: `redirectUrl=https:///ui/wwe/index.html`

To get the URL for an application, go to your Genesys Portal page and click the application's widget. Immediately after, press "escape" on your keyboard to prevent the Authentication login page from loading so you can see the application URL in the browser.

SSO support by application

View which Genesys Engage cloud applications support SSO.

Applications	Single Sign On Support	Notes
Agent Desktop	Yes	
Agent Setup	Yes	
Callback	Yes	
Cloud Data Download Service	Yes	

Applications	Single Sign On Support	Notes
CX Contact	Yes	
Designer	Yes	
Genesys CX Insights	Yes	Supported in version 9.0.013.0+. Contact your Genesys representative to enable.
Genesys Softphone	Yes	
Screen Recording	Yes	Supported in Agent Desktop version 9, but not with custom desktops.
Real-Time Reporting (Pulse)	Yes	Supported in Real-Time Reporting version 9 on selective deployments. Contact your Genesys representative for details.
Gplus Adapter Salesforce	Yes	
Recording, Quality Management and Speech Analytics	No	
Workforce Management	Yes	Not supported for supervisor accounts for administrative activities.
Agent Scripting Administration	No	
Interactive Insights	No	
Outbound	No	
Platform Administration (GAX) *Includes plug-ins like eServices Manager and IVR Administration*	No	
WebRTC	Yes	

Configuring SSO in Genesys Engage

To enable single sign-on for your environments, see Single Sign-On in Agent Setup.

> **Important**
>
> SSO can be configured for different groups and you can have multiple identity providers, as long as there is only one per region.

If you're planning to enable SSO, consider the following conventions for creating users:

- The domain declared in the identity provider metadata should be part of the user name stored within Genesys, to create the most seamless experience. (Example: `john@mycompany.com`) Otherwise, users would need to enter a Tenant or enter the domain before their username. (Example: `mycompany\john`)

- The username provisioned within Genesys Engage cloud should match the username in the external identity provider.

Configuring SSO in the identity provider

Genesys Engage cloud must be defined as an application within the identity provider to support the SSO integration.

Genesys Engage cloud supports the SAML 2.0 protocol as a standard interface to identity providers, and has successfully validated with popular IdPs, including Okta and Ping. Other identity providers can be supported provided they comply with SAML 2.0 and you validate the integration before using in production.

SAML settings

Genesys Engage cloud supports some SAML configuration that must be set up by your Genesys representative:

- Configure a maximum age for SAML assertion. The default value is 2 hours.
- Configure "enforceAuthN" in SAML authentication requests. When enabled, Genesys Engage cloud's Authentication Service sends an attribute to the IdP that tells it to re-authenticate the user, regardless of their previous state.