Developer's Guide

Visitor Identification

4/22/2025

Visitor Identification

Contents

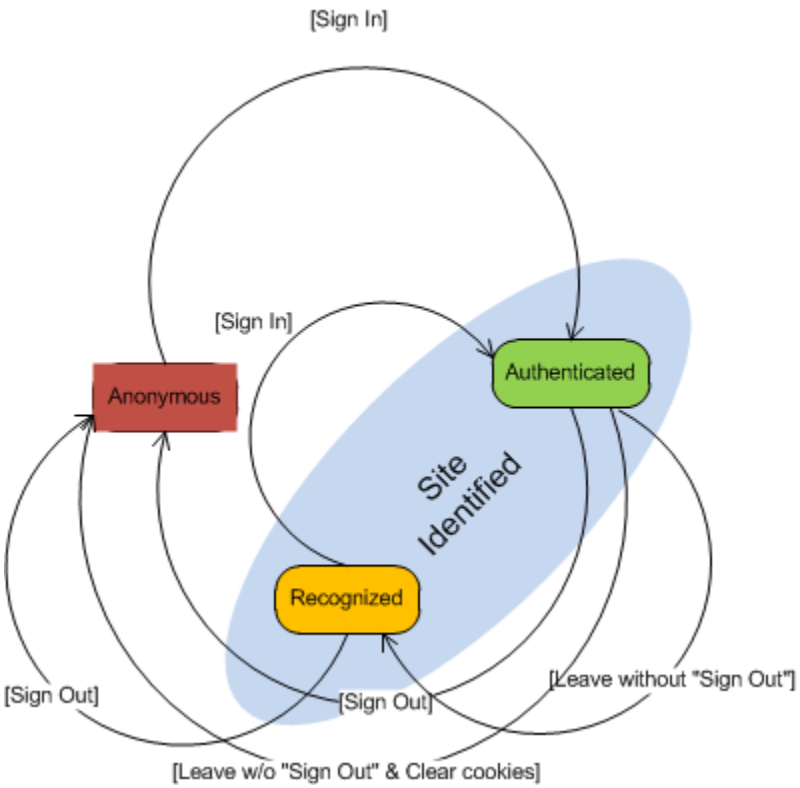
Overview

Genesys Web Engagement allows you to capture visitor activities on your website and to build a complete history of the visitor's interactions with your contact center.

When a visitor browses your website, the tracking code submits SYSTEM events to the Web Engagement servers that constitute a visit, such as `VisitStarted`, `PageEntered`, `SignIn`, `UserInfo`, and so on. The association or relationship between the visit and the visitor is based on the flow derived from SYSTEM events, in addition to the information retrieved from the Contact Server. In the end, you can access visit history through the Event Resource in the History REST API.

To associate the visitor with the visit, Genesys Web Engagement must "identify" the visitor as one of three possible states:

- `Authenticated`—The visitor logged in to the website with a username and password. The username can be an e-mail address, an account name or other similar identifier, depending on your website. When a user is authenticated, Genesys Web Engagement can maintain an association between the visitor and the visit.
- `Recognized`—The visitor closed the browser window and did not log out, but the website can submit user information with the sendUserInfo event, which contains the `userId`.
- `Anonymous`—The visitor is anonymous.



Visitor states

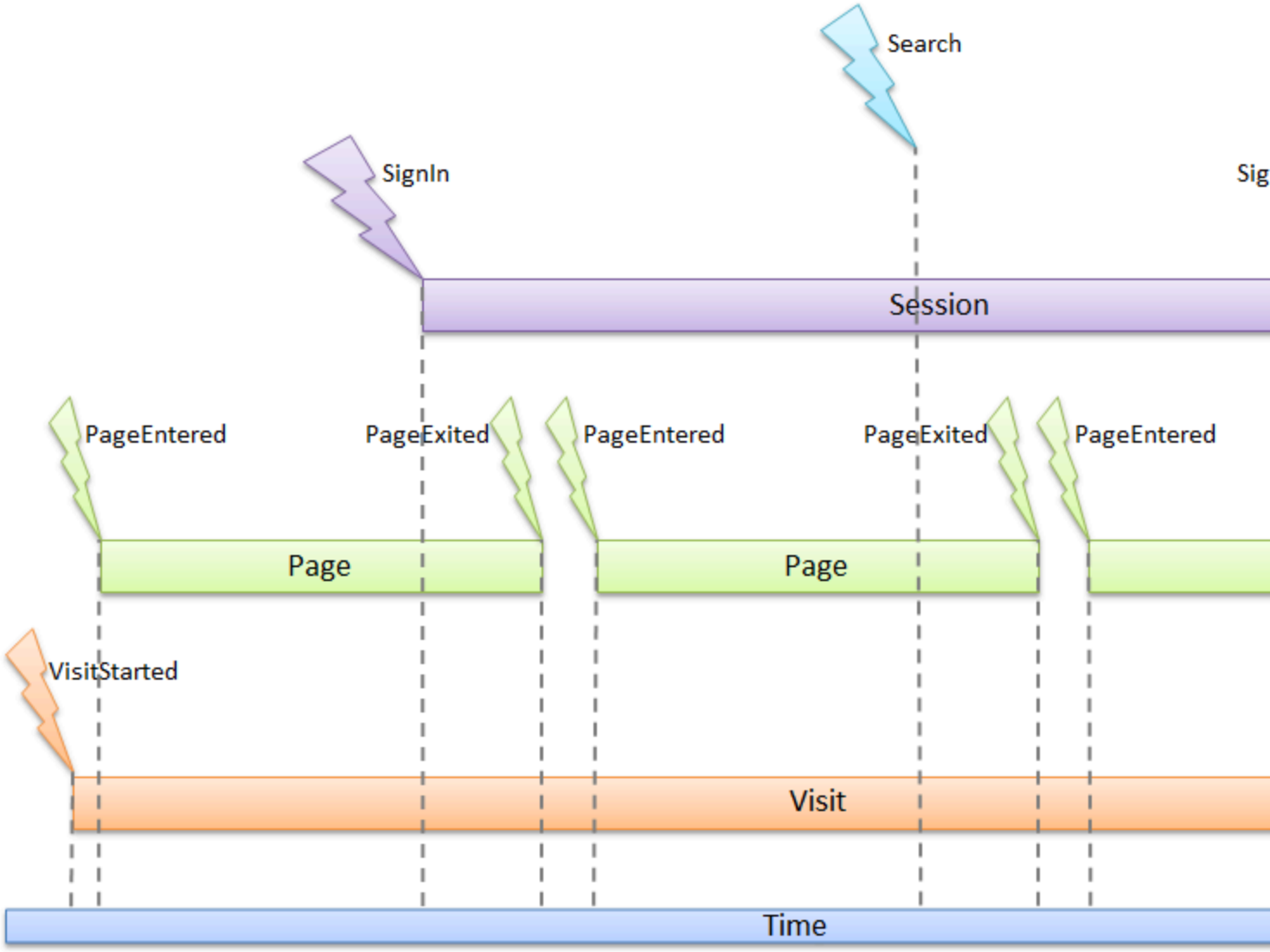
Genesys Web Engagement relies on your website to trigger the transitions between visitor states. You can do this by updating the tracking code with the following events in the Monitoring JavaScript API:

- sendSignIn—Send this event when the user is authenticated by the website. This allows the system to identify the user and creates a new "session" with a `sessionID` that is unique to a visit and will last the duration of the visit. Only Authenticated visitors have an associated `sessionId`.
- sendSignOut—Send this event when the user logs out of the website.

  Note: The `sessionId` lasts for the duration of the authenticated user's visit to your website. It is stored in a cookie and sent with every event that occurs between SignIn and SignOut, and is changed automatically after every SignIn event.
- sendUserInfo—Send this event when the user visits your website after closing the browser window on an authenticated session. For details, see Recognized Visitors.

Visitor Event Timeline

The figure below shows the timeline for events that take place when a visitor browses your website.



Visitor Event Timeline

All visitors to you website are identified with a `visitorId`, which can be used to associate the visitor to events, such as `PageEntered` or `PageExited`, during the span of the visit.

Accessing Visitor Information

The History REST API is a RESTful interface that allows you to manage a collection of JSON objects using `POST` and `GET` HTTP requests. You can create or access visitor information in the Backend Server database at any point during the event timeline by using the History REST API resources:

- The visit resource contains information about a visit that is started when a visitor navigates to your website. This visit is associated with the flow of pages visited (entered and then exited) by the visitor.

The visit ends when the visitor closes the browser or leaves the website.

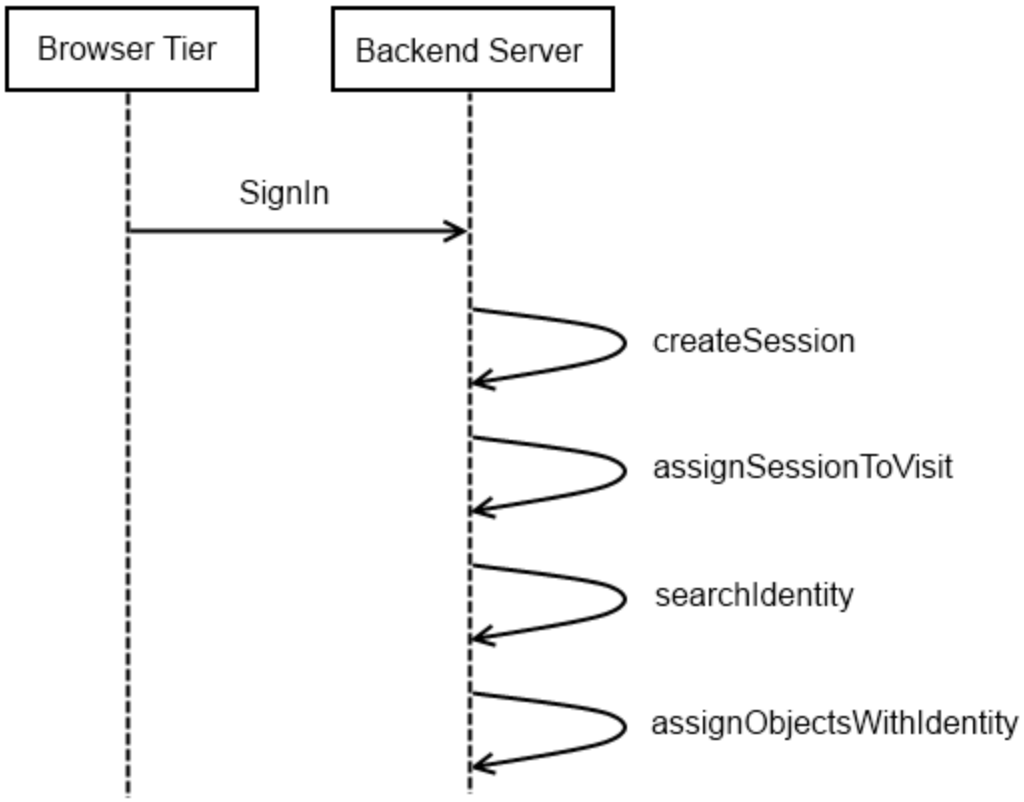
- The identity resource contains information for an authenticated visitor.
- The session resource contains information about the events and pages involved in the visitor's browsing activity during the time between SignIn and SignOut.
- The page resource contains information for a specific page entered at a given time. If the visitor leaves the page and then later revisits the page, a new page resource is created.
- The event resource contains information about SYSTEM and BUSINESS events.

When a visitor begins a visit on the website (a browser session is opened for the website), the Backend Server creates a visit resource and records the browsing history related to the visit by creating a page resource for each page entered and then exited. These events are also recorded as a collection of events associated with the visit and the pages.

Authenticated Visitors

When the visitor is Authenticated on the website, you should use the `sendSignIn` event so that Genesys Web Engagement can start a new session. When the Backend Server receives this event, it creates a session resource and an identity resource to store the visitor information. The identifying information used to login (for instance, the e-mail address) is available in the `SignIn` event and is used to:

- Create the `identityId` or search the visitor's identity resource.
- Associate the visitor with a contact in the Genesys Solution.



GWE SignIn event.png

The `SignOut` and `UserInfo` events are used to manage the collections of additional information. These collections, called `contacts` and `useridentifications`, are introduced in the Backend Server database.

- The `contacts` collection maintains the association between the `identityIds` and the `sessionId`, `visitId`, and `globalVisitId`.
- The `useridentifications` collection store all of the SYSTEM events.

Recognized Visitors

When an Authenticated visitor closes the browser window without signing out and then later revisits your site, you can use the sendUserInfo event to tell Genesys Web Engagement that the visitor is now Recognized.

You will need to send the `userId` in the `sendUserInfo` event. How you track the `userId` depends on your website. For example, you could create a persistent cookie to store the `userId` when a visitor logs in to you website. Then when a visitor first browses your site, you could check the cookie and call the `sendUserInfo` event if the cookie contains the `userId`. There are many possible scenarios - the best implementation is entirely dependent on your website and its workflow.

Note: The visitor's identity cannot be guaranteed in the Recognized state. For instance, another

member of the visitor's family could be browsing the website with the same computer.

Anonymous Visitors

If the visitor is not Authenticated or Recognized, no identity is created. The visitor's activity on the website, including events and pages visited, are still associated with the visit.