Genesys Security Deployment Guide

Inactivity Timeout

4/3/2025

Inactivity Timeout

Contents

The inactivity timeout is a configurable period of time during which a user can be inactive (that is, not interact with the system in any way) without any impact on their session. After the timeout expires, the user is locked out of the session, and in some cases, all session displays are minimized. The user must log back in to continue with the session. Alternatively, anyone (not just the owner of the session) can close the session completely, without logging back in.

> **Important**
>
> For purposes of this feature, *activity* is defined at screen level, regardless of the application in focus, and includes: using the mouse (clicking, moving, or scrolling), pressing a key, changing the state of a window between active and inactive, or acknowledging any warning that might be generated by the operating system's own timeout functionality. Watching the progress of an activity, as when a progress indicator appears on the screen, for example, is not interpreted as inactivity. Therefore, the inactivity timeout is not triggered in this case.

Security Benefits

If a user is distracted while logged in to a session, causing them to either turn away or walk away from their computer, that session is available for anyone (authorized or not) to access. The Inactivity Timeout feature minimizes the possibility of that second party viewing or accessing the system. It is a best effort because the length of the timeout is a trade-off between the inconvenience to the logged-in user of having to log in repeatedly, and the risk of exposing the system to other people.

Supporting Components

The following components support this feature:

- Configuration Manager
- Genesys Administrator Extension
- Solution Control Interface
- Genesys Rules System - Genesys Rules Authoring Tool (GRAT)
- Interaction Routing Designer
- Outbound Contact Manager
- Pulse - See Genesys Pulse Configuration Options for more information.
- Workspace Web Edition
- Workspace Desktop Edition (formerly known as Interaction Workspace) also supports this feature, but configures it differently than described in this section. For configuration details of this feature in Workspace Desktop Edition, refer to the *Workspace Desktop Edition Deployment Guide*.
- Genesys Customer Experience Insights. (GCXI) - See KB33832: How does the User Session Idle Timeout

work in MicroStrategy for more information.

- SIP Feature Server
  - (For Web based access inactivity timeout (when no user action is there), the session will be disconnected after 10 minutes. This is a configurable value of GAX. For Telephony User Interface inactivity timeout (when no input is given by user), the session will be disconnected after 30 seconds (after 3 attempts of 10 seconds each).

Feature Description

When a user is inactive for the period of time equal to the inactivity timeout, all display screens are minimized (with the exception of some modal dialog screens), and a re-login dialog box is displayed. The connection to the server should be preserved. However, if the connection is lost for some reason, the High Availability (HA) functionality of the application will attempt to reestablish it automatically.

In the re-login dialog box, the user can do one of the following:

- Enter their password, and click **OK**. The user is then authenticated. One of two situations occurs:
  - If this user is not the original user, access will not be permitted.
  - If this user is the original user, that user will be logged back in, and the session state will be restored as much as possible.
- Click **Cancel** to close the application. A confirmation dialog box appears, requesting that the user verify that the application is to be closed.

In any case, the user must be re-authenticated before accessing the current session.

Password Changes

Genesys Administrator, Configuration Manager, and Interaction Routing Designer permit an authorized individual to change a user's password for that Application. If this occurs while the user is logged in, and before the inactivity timeout expires should the user become inactive, the user must use the new password in the re-login dialog box. The old password will be interpreted as an invalid password and access will not be permitted.

In Genesys Administrator or Configuration Manager, a system administrator can also change a user's password for another Application. If this occurs while the user is logged in, and before the inactivity timeout expires should the user become inactive, the user must use the old password in the re-login dialog box. The new password will be interpreted as an invalid password and access will not be permitted.

Feature Configuration

> **Important**
>
> This section describes a standard configuration method for this feature, as used by most components. Some components, such as those identified in Supporting Components, might implement this feature differently. In this case, see the product documentation for details.

The inactivity timeout is configured at the Application level, so can differ between applications. By default, the feature is disabled, and the timeout must be set to a non-zero value to enable the feature.

The inactivity timeout is specified by setting the **inactivity-timeout** option in the **[security]** section of the options of the GUI Application object. Application templates, if they exist, contain this option set to the default value. Refer to the *Framework Configuration Options Reference Manual* for a full description of this option.