ORACLE

Understanding the Timeouts in Oracle Applications Clouds

Timeouts are used to maintain data integrity and security in software applications and application integrations.

Read about the timeout types used in Oracle Applications Cloud and related functional and technical details.

Target Audience

- Implementer
- Application Administrator
- Business Administrator
- Business Manager
- Project Manager

Quick Links to Resources

- My Oracle Support (MOS)
- Oracle Help Center

Other Helpful Links

- System Requirements
- Oracle University
- Oracle Partner Finder

Connect With Us

- Cloud Customer Connect

FOR BUSINESS AUDIENCE

What are Timeouts?

When you sign in to the Oracle Applications Cloud, your authentication is validated, and you are given access to the application. As a security precaution, your authentication is valid for a limited time period and subject to certain conditions. Beyond this time limit, you can experience timeouts, which restrict your access to the application.

Why Do You Need Timeouts?

You can access and use cloud applications from any location using just a web browser. In many cases, applications are integrated with and exchange data with your other business applications, including mobile applications. Security measures are required and built to protect and secure such complex application integrations - timeouts being one such security measure.

Timeouts are not application errors but are intentionally designed and built to ensure business data protection and security. Timeouts relate to aspects such as how long your sign in must remain valid, how long can you be signed in without any activity, how long can you leave your computer unattended while you are signed in, and so on.

When Do You Experience Timeouts?

Oracle applications have various types of timeout rules that run simultaneously. You can experience timeouts if any one of the following occur.

- **Timeout related to your sign in**: Your sign in is authenticated and valid for eight hours only. If you continue to be signed in to the application beyond the authentication validity time period of eight hours, your sign in is revoked, the application times out, and you are asked to sign in again.
- **Timeout related to application inactivity**: If 30 minutes pass since you last performed an action in the application, the application automatically times out. When this happens, you will see a warning on the screen. You must follow the instructions in the warning to continue working in the application.
- **Timeout related to browser inactivity**: If 30 minutes pass since you last performed an action in the browser used to access the application, the application automatically times out. When this happens, you will see a warning on the screen. You must follow the instructions in the warning to continue working in the application.

Notes:

- For more information about the timeout types, see the technical information section in this document.
- The timeout time periods are predefined across all Oracle Cloud applications and cannot be edited.

How Are Timeouts Handled in Application Integrations?

Oracle Applications Cloud supports integrations with other applications, such as Oracle Configure, Price, and Quote Cloud (CPQ), Oracle Eloqua, Oracle Digital Customer Service, Oracle Policy Automation, and so on. Integrations allow Oracle Applications Cloud to access and display information from other applications.

Each application has its own set of specific timeout values, which continue to be used in integrations as well. For example, consider an application page that includes a table for which information is derived from Oracle Digital Customer Service. A timeout displayed on the page, may arise from either of the integrated applications timing out.

Best Practices for Minimizing Timeouts

- Use your credentials to sign in to only one active Oracle application instance.
  - Do not use your credentials to sign in to the Oracle application in multiple browsers simultaneously.
  - Do not use the same credentials to sign in to the Oracle application in multiple tabs of the same browser simultaneously.

FOR TECHNICAL AUDIENCE

Timeout Values in Oracle Applications Cloud

Oracle applications have multiple authentication validity time periods built in to maintain your security. The set time periods cannot be modified.

For reference, you may experience timeouts in any of the following cases:

TIMEOUT TYPE	DESCRIPTION	TIME BEFORE TIMEOUT
Session Lifetime Timeout	Time duration for which the memory of your sign-in activity is reserved on the web server. On sign in, your browser session receives a cookie that is valid for 8 hours. After 8 hours, you are required to sign in again.	8 hours

Idle Session Timeout	Time duration that passes without any application requests or activity from you. When it expires, you are required to click to reinitialize the session. On reinitialize, session timeout duration is reset. If session not reinitialized, you are required to sign in again. Timeout occurs if you do not make any request in the cloud application in 30 minutes.	30 minutes
Inactivity Timeout	Time duration that passes without any browser activity from you. When it expires, you are prompted to sign in again. Timeout occurs if you do not use the browser for 30 minutes.	30 minutes

NOTE: The timeout time periods are predefined across all Oracle Applications Cloud and cannot be edited.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle