Web Services and Applications Deployment Guide

Web Services authentication flow

5/12/2025

Web Services authentication flow

Web Services provides authentication in the following sequence:

1. Salesforce Authentication

- Enters here if a request contains two specific headers (Salesforce Session ID and Salesforce Identity URL).
- If successful, the user is authenticated and execution flow proceeds to the authorization stage.
- If authentication headers are not present or authentication fails, execution flow proceeds to the next step.

2. Configuration Server Authentication

- Enters here if a request contains basic authentication header and Configuration Server authentication is enabled for this contact center.
- If successful, user is authenticated and execution flow proceeds to the authorization stage.
- If authentication headers are not present, Configuration Server authentication is disabled, or authentication fails, execution flow proceeds to the next step.

3. Web Services Authentication

- Enters here if a request contains basic authentication header.
- If successful, user is authenticated and execution flow proceeds to the authorization stage.
- If authentication headers are not present or authentication fails, execution flow proceeds to the next step.

4. Security Assertion Markup Language (SAML) Authentication

- Enters here if SAML is enabled and configured.
- An attempt is made to authenticate user through the standard SAML authentication flows.
- If successful, the user is authenticated and execution flow proceeds to the authorization stage.
- If not successful, the user receives an anonymous authentication, which means this users is only given access to unprotected endpoints.

Next step

- Back to Configuring security