Single Sign-On Policy

Amadeus Hospitality

HOS LEG – V2.0
Last Update: 4/2025

Federated Single Sign-On Policy

Amadeus Hospitality

If Amadeus provides Customer with federated single sign-on capabilities ("**FSSO**") for the “Applicable Services”, the following provisions will apply:

1. **Authentication Control**: The FSSO will allow the Customer to internally control the authentication process to the Applicable Service. The Customer is fully responsible for determining which users need access to the Amadeus Applicable Service application and the federation service (IdP) as Customer system administrators may access the Applicable Service to perform actions related to user management and role assignment.

2. **Information Exchange**: Customer system administrators must collaborate with the Amadeus team designated by Amadeus to exchange necessary information (e.g., endpoints, public certificates, exchanged attributes, etc.) for setting up and configuring the federation service. This exchange must occur prior to the activation of the FSSO capabilities through secure channels outside of the Amadeus Applicable Service application.

3. **User Authentication**: Subject to Customer compliance with all its obligations included in this FSSO Policy, Amadeus may delegate user authentication (credentials verification) to the Customer. Upon successful authentication, Amadeus may provide access to the Applicable Service.

4. **Customer Responsibilities**:
    - Establishing, implementing, deploying, and overseeing rules, requirements, and procedures for provisioning, de-provisioning, distribution, selection, use, and safeguarding of identifying credentials (such as user IDs and passwords).
    - Verifying the identity of each user and their level of access authorization for each Service.
    - Utilizing at least 'standard industry practices' for password policies, user provisioning and de-provisioning.
    - Enforcing multi-factor authentication for sensitive user accounts.
    - Creating persistent, unique, and static user IDs.

    For clarity, Amadeus will not authenticate users or verify their identity unless a user is FSSO exempt as dictated in written by the Customer.

5. **Amadeus Responsibilities**: Amadeus will: (i) provide Customer system administrators with user management features, including managing users not covered by the FSSO capabilities (if applicable) and managing application-level roles assignment; and (ii) evaluate authorization rules and enforce access control to application resources.

6. **Technical Specifications**: The FSSO capabilities utilize "Security Assertion Mark-up Language 2.0" ("SAML") or OpenId Connect (OIDC). The Customer is solely responsible for procuring all necessary hardware and software to utilize the FSSO.

7. **FSSO Requirements**:
    - SAML version: 2.0

- SAML profile: Web Browser SSO Profile (SP-initiated); Amadeus will provide app-level logout.
- Integration with Identity providers supporting SAML2.0 or OIDC, such as Okta or Azure Active Directory.
- Digital signature for signing assertions.
- Assertion exchange between Customer and Amadeus will use industry-accepted encryption for public networks.
- Amadeus will provide information to be collected, transmitted, and validated as part of the assertion messages under the FSSO.

8. **Coordination**: Amadeus and the Customer will coordinate in good faith the testing and implementation of the FSSO, including idle timeout, account linking, session management, global logout techniques, and end-user support processes.

9. **End-User Support**: Customer end-user support will investigate, and answer inquiries related to the FSSO. In the event of FSSO termination, Amadeus will cooperate with the Customer to convert the provision of continuing Services to Amadeus's standard security authentication systems.

10. **Login Process**: When accessing the web-based Amadeus Applicable Service with FSSO enabled, users will be redirected to their organization's Identity Provider ("**IdP**"). Depending on the security policies defined within the Customer's IdP, users may be prompted to enter their login credentials and/or multi-factor authentication (MFA). Upon successful authentication at the IdP, the user will be redirected back to the Amadeus Service, which will generate a temporary token for the application session. User credentials are never shared with nor stored within Amadeus systems; all subsequent requests will rely on this token until the user session expire..

11. **Indemnification**: The Customer agrees to indemnify and hold harmless Amadeus from any third party claims, costs, losses, damages, or liabilities resulting from the utilization of the FSSO capabilities and/or any unauthorized access to or use of the FSSO systems or services. This obligation is not limited by any liability provisions in the Agreement. Any Customer action or inaction resulting in either a breach of this Policy or a security incident or data breach as defined by applicable law shall be considered a Customer Security Incident under the MSSA. Amadeus disclaims any express, implied, or statutory representations or warranties, including implied warranties of merchantability, title, non-infringement, and fitness for a particular purpose regarding the FSSO.

    "Applicable Service" means the following Amadeus Services provided that Amadeus is granting FSSO capabilities: iHotelier®, Guest Management System and/or Hotsos ®.