SSO in Salesforce (Single Sign-On)

Single Sign-On (SSO) in Salesforce allows users to log in once using an external **Identity Provider (IdP)** and access Salesforce without entering credentials again. It improves security, simplifies authentication, and reduces password fatigue.

How It Works

1. **User tries to access Salesforce.**
2. **Salesforce redirects the user to the Identity Provider (IdP).**
3. **IdP verifies the user's credentials.**
4. **IdP sends a security token (SAML/OAuth) to Salesforce.**
5. **Salesforce validates the token and grants access.**

Types of SSO in Salesforce

- **SAML-Based SSO** – Uses XML-based authentication (for enterprise IdPs like Okta, Azure AD).
- **OAuth/OpenID Connect (OIDC) SSO** – Used for API and mobile authentication.
- **Delegated Authentication SSO** – Uses an external system to validate credentials.
- **Federated SSO** – Allows login via third-party IdPs like Google, Ping Identity, ADFS.

Benefits

✅ **One Login for Multiple Apps** – No need to remember multiple passwords.
✅ **Stronger Security** – Reduces phishing and weak password risks.
✅ **Centralized User Management** – Managed through IdP.
✅ **Faster Access** – Seamless login experience.

Common Identity Providers (IdPs) for Salesforce SSO

🔹 **Okta**
🔹 **Microsoft Azure AD**
🔹 **Google Workspace**
🔹 **Ping Identity**
🔹 **Active Directory Federation Services (ADFS)**

1. General SSO Concepts

Q1: What is Single Sign-On (SSO), and how does it work?

Answer:

Single Sign-On (SSO) is an authentication mechanism that allows users to log in once and gain access to multiple applications without needing to re-enter credentials. It improves security, user experience, and IT efficiency.

How It Works:

1. **User Requests Access** – The user tries to log in to an application (Service Provider, SP).
2. **Redirect to Identity Provider (IdP)** – If the user is not authenticated, the request is sent to the IdP.
3. **User Authenticates** – The IdP verifies the credentials (via username/password, MFA, etc.).
4. **Token Issuance** – If successful, the IdP generates an authentication token (SAML, OAuth, OpenID Connect).
5. **Redirect to SP** – The token is sent back to the SP.
6. **Access Granted** – The SP validates the token and grants the user access.

Example: A user logs into **Okta (IdP)** and can access **Salesforce, Gmail, and Slack** without re-entering credentials.

Q2: What are the main benefits of implementing SSO in an enterprise?

Answer:

✅ **Improved Security** – Reduces password fatigue and phishing risks.
✅ **Better User Experience** – Users log in once and access multiple apps.
✅ **Centralized Access Management** – IT teams control authentication in one place.
✅ **Reduced IT Costs** – Fewer password reset requests.
✅ **Stronger Compliance** – Helps with regulatory requirements (GDPR, HIPAA, etc.).

Example: A company integrates **Azure AD** with **Salesforce, Workday, and ServiceNow**, ensuring seamless and secure authentication.

Q3: What are the key differences between authentication and authorization?

Answer:

Feature	Authentication	Authorization
Definition	Verifies user identity	Determines access level
Process	Login with credentials	Access permissions granted
Handled By	Identity Provider (IdP)	Service Provider (SP) or Role-Based Access Control (RBAC)

Feature	Authentication	Authorization
Example	Entering a username & password to log in	Accessing an admin dashboard after login

Example: Logging into **Salesforce (authentication)** vs. accessing reports based on the user's role (authorization).

Q4: What is an Identity Provider (IdP) and a Service Provider (SP) in SSO?

Answer:

- **Identity Provider (IdP)** – The system that authenticates users and issues access tokens (e.g., **Okta, Azure AD, Google Workspace**).
- **Service Provider (SP)** – The application that users want to access after authentication (e.g., **Salesforce, Slack, Workday**).

How It Works:

1. **User logs into IdP (Okta)** → IdP verifies credentials.
2. **IdP generates a SAML/OAuth token** → Sent to SP (Salesforce).
3. **SP (Salesforce) validates token** → Grants access.

Example: **Okta (IdP)** authenticates users for **Salesforce (SP)** via SAML SSO.

Q5: What are the security risks associated with SSO, and how can they be mitigated?

Answer:

● Risks of SSO:

- **Single Point of Failure** – If the IdP is compromised, all connected apps are vulnerable.
- **Session Hijacking** – Attackers can steal SSO tokens.
- **Phishing Attacks** – Users may be tricked into entering credentials on fake IdP login pages.
- **Token Replay Attacks** – A stolen SAML/OAuth token can be reused.

✓ Mitigation Strategies:

- **Multi-Factor Authentication (MFA)** – Adds an extra security layer.
- **IP-Based Restrictions** – Allows access from trusted locations only.
- **Session Timeout & Token Expiry** – Reduces risk of stolen tokens.
- **SSO Logout (SLO)** – Ensures logging out from one app logs out from all.
- **Federated Identity & Conditional Access** – Enforce policies like device trust checks.

Example: **Salesforce enforces MFA for all users accessing via Okta SSO** to prevent unauthorized access.

2. Salesforce SSO Basics – Detailed Answers

Q1: How does SSO work in Salesforce?

Answer:

Single Sign-On (SSO) in **Salesforce** allows users to log in once using an external **Identity Provider (IdP)** and gain access without entering credentials again. Salesforce acts as a **Service Provider (SP)**, trusting the authentication performed by the IdP.

Step-by-Step Process:

1. **User requests access to Salesforce**
2. **Salesforce redirects the user to the Identity Provider (IdP)**
3. **IdP verifies the user's credentials**
4. **If successful, IdP sends a SAML/OAuth token to Salesforce**
5. **Salesforce validates the token and grants access**

🔹 **SP-Initiated SSO:** The login request starts from **Salesforce** and redirects to the IdP.
🔹 **IdP-Initiated SSO:** The user logs in via the **IdP dashboard**, which then redirects to Salesforce.

Q2: What are the different types of SSO supported by Salesforce?

Answer:

Salesforce supports multiple SSO mechanisms:

SSO Type	Description	Best Used For
SAML-Based SSO	Uses **Security Assertion Markup Language (SAML)** to exchange authentication data	Enterprise IdPs (Okta, Azure AD, ADFS)
OAuth/OpenID Connect (OIDC) SSO	Uses **OAuth 2.0** and **JWT tokens** for authentication	Mobile apps, API-based authentication
Delegated Authentication SSO	Salesforce delegates authentication to an external system via **SOAP API**	Legacy systems, password policies
Federated SSO	Uses third-party IdPs like Google, Microsoft, Okta	Integrating with external identity providers

🔹 **SAML/OAuth is recommended for enterprise security**.

Q3: What is the role of My Domain in Salesforce SSO?

Answer:

My Domain is a **mandatory** requirement for enabling SSO in Salesforce. It provides:
✅ **A custom Salesforce login URL** (e.g., `https://yourcompany.my.salesforce.com`).
✅ **Prevents phishing attacks** by restricting logins to only trusted IdPs.
✅ **Allows SP-Initiated SSO** (users can log in via Salesforce and be redirected to the IdP).

Steps to Set Up My Domain:

1. Navigate to **Setup → My Domain**
2. Enter a unique name (e.g., `yourcompany`)
3. Deploy and test the domain
4. Enable **SSO settings** and restrict login access

🔹 **Without My Domain, SSO will not work in Salesforce.**

Q4: What is the difference between Federated SSO and Delegated Authentication in Salesforce?

Answer:

Feature	Federated SSO	Delegated Authentication
Authentication	Uses **SAML/OAuth** (IdP verifies identity)	Uses **Salesforce API** to authenticate
Credentials Storage	No password stored in Salesforce	External system validates credentials
Security	More secure (token-based)	Dependent on external API security
Setup Complexity	Requires an IdP (Okta, ADFS)	Requires API configuration
Best For	Enterprise SSO with IdP	Custom authentication scenarios

🔹 **Federated SSO is the preferred option for modern authentication.**

Q5: How do you configure SAML-based SSO in Salesforce?

Answer:

To set up **SAML SSO** in Salesforce, follow these steps:

Step 1: Enable My Domain

1. Go to **Setup → My Domain**
2. Choose a unique domain and deploy it

Step 2: Configure SAML in Salesforce

1. Navigate to **Setup → Single Sign-On Settings**
2. Click **New** and select **SAML Enabled**
3. Enter the **Identity Provider (IdP) details**:
    - **Issuer URL** (IdP metadata URL)
    - **SAML Identity Type** (Federation ID / Username)
    - **Entity ID** (Salesforce login URL)
    - **ACS URL** (Assertion Consumer Service URL from Salesforce)
4. Upload the **X.509 Certificate** from the IdP

Step 3: Configure IdP (Okta, Azure AD, etc.)

1. Add **Salesforce as a Service Provider**
2. Enter **Salesforce's ACS URL and Entity ID**
3. Configure the **Federation ID as the identifier**

Step 4: Test SSO

1. Try **SP-Initiated Login** from Salesforce
2. Try **IdP-Initiated Login** from the IdP
3. Use the **SAML Assertion Validator** for debugging

🔻 If authentication fails, check SAML logs and certificate validity.