

SecureAuth IdP Salesforce

Secure and Simple Access to Salesforce

SecureAuth IdP is an Identity Provider that secures and simplifies access to Salesforce.com, the Force.com Platform, other cloud and on-premise web applications, and VPNs. Unlike other products, SecureAuth IdP delivers integrated SSO, Identity Access Management, and Versatile Authentication Services (VAS) that can be easily configured to meet the security and productivity requirements for your Salesforce.com or Force.Com implementation.

SecureAuth IdP SSO enables a user to log onto Salesforce.com and Force.com with one set of credentials. This eliminates multiple usernames and numerous passwords that are normally required. SecureAuth IdP automatically connects Salesforce.com applications and the Force.com Platform to the enterprise's Active Directory; and SecureAuth's Security Token Service (STS) asserts the extracted identity in the artifact that the apps require.

SecureAuth IdP Authentication (VAS) ensures users are really who they say they are, which is critical for remote users. SecureAuth IdP can be easily configured to deliver diverse types of authentication for Salesforce applications and the Force Platform to meet corporate and/or industry regulations. Unlike other SSO solutions that stop short of development and require partners for authentication, SecureAuth's Versatile Authentication (Group Policies, Certificates, SMS OTP, Telephony OTP, Username/Password) is based on the "Three Rs": Roles (who is the User), Resources accessed (confidentiality of the information), and Regulations (PCI, FFIEC, NCUA, HIPAA, etc.).

Ensure Interoperability of User Credentials

SecureAuth IdP provides secure, transparent user access by enabling identities to be shared securely across diverse applications and computing platforms, including Salesforce.com, the Force.com Platform, on-premise web, VPN, and mobile resources. This is achieved with SecureAuth IdP's built-in Security Token Service (STS), which creates, validates, signs, and exchanges one type of security token for another that is not dependent on any one mechanism (such as the Kerberos protocol or X.509 to secure messages). STS handles the translation on the fly so you can comfortably mix protocols and all applications will work together seamlessly. For Salesforce.com, the token is usually a SAML assertion, but SecureAuth also supports OpenID, OAuth, and other protocols.



Bridge the Access and Security Gap of Salesforce and On-premises Applications

SecureAuth IdP provides transparent SSO access to Salesforce.com, the Force.com Platform, and other applications. With credentials securely stored on-premise in your directory, SecureAuth IdP delivers an SSO experience using the Security Access Markup Language (SAML) protocol. SAML doesn't perform the authentication required; and unlike other cloud SSO systems that rely on third-party authentication, SecureAuth includes VAS that is designed for SaaS applications.

User Self-Services and Rapid Deployment

One of the most time-consuming processes is getting users provisioned. SecureAuth's user self-enrollment system is simple, self-explanatory, and does not require help desk or administrative support. An administrator simply selects the authentication method to be used before a user is allowed to continue with the sign-on process. Once authenticated, users can update and manage their own profile. In addition, SecureAuth IdP enables users to securely reset their own password when forgotten, which saves enterprises hundreds of thousands of dollars a year in wasted time and labor.

SecureAuthIdP can be deployed in days, not weeks or months. SecureAuth has eliminated APIs and the need to write custom code by building a system that can be easily configured to work with your existing infrastructure and applications. Our development team has addressed all of the intricacies of directory integration, SAML, and certificate authorities, so your staff does not need to understand SAML or certificate authorities. The result is a reduced deployment time for Salesforce.com.

Key Features of SecureAuth IdP for Salesforce.com

Integrated Single- or 2-Factor Authentication, SSO, and Identity Access Management Services

- 20+ Authentication Mechanisms
- SSO to Salesforce and other SaaS, Mobile, Web, and Network Apps
- Logging and Auditing
- 1-Touch Revocation

Point-and-Click Configurations

- Eliminates APIs and Integration

User Self-services

- 2-Factor Authentication Enrollment
- Profile Maintenance
- Password Reset
- Self/Device Revocation

Single Set of Credentials for All Resources

- On-premises
- Cloud
- Mobile

Rapid Deployment

Lowers TCO for cloud and on-premises applications by reducing management overhead and calls to the help desk.

75% cost savings over stand-alone hardware token or SSO products.

Streamlines user experience

Increases security with federated identities and multi-factor authentication.

SecureAuth IdP is ideal for Salesforce and all other resources

Integration with Popular SaaS Apps:

- Salesforce
- Google Apps
- WebEx
- SuccessFactors
- Workday, and more

Web Apps:

- .NET
- J2EE
- SharePoint
- WebSphere, and more

Mobile Apps:

- iOS, Android
- Windows, Blackberry

Network Resources:

- Cisco
- Juniper
- F5
- Microsoft UAG



2-Factor Access Control for the Mobile Enterprise

