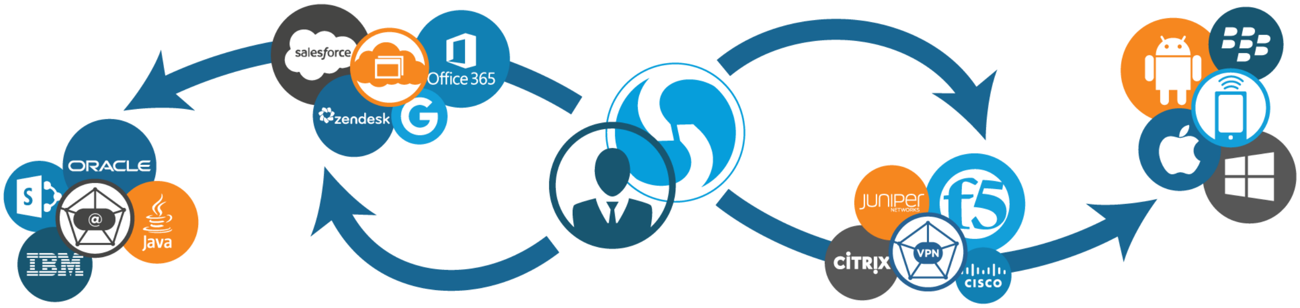
SecureAuth IdP 8.0.x Assertion



SecureAuth IdP Assertion

SecureAuth IdP completes the workflow with various assertion solutions, including integrations with cloud, web, network, and mobile resources, comprehensive IdM tools, and Single Sign-on (SSO) methods. By handling the entire workflow, from acceptance to assertion, SecureAuth IdP creates a more fluid, secure, and user-friendly login process.

The assertion event can be described as the purpose of each SecureAuth IdP **realm**. The other configuration required in the realm is focused on how are and what is brought with users accessing the post-authentication target.

Single Sign-on

SecureAuth IdP provides various SSO options that can be applied to almost any realm. By utilizing shared tokens and validation keys, join realms together to enable secure user access with a single login.

Secure Portal: The secure portal connects SecureAuth IdP realms via a landing page that requires authentication before access is granted. Once users reach the portal page, they can select the resources to which they require access, without being prompted for additional login. Any post-authentication configuration can be included on the secure portal, including SP integrations and IdM Tools.

Transparent SSO: Transparent SSO employs the same configuration requirements as the secure portal option to connect realms; however, no landing page is required. Instead, users can authenticate into one realm (application, VPN, IdM Tool, etc.), and then gain immediate access into another realm without providing additional login information.

Windows Desktop SSO: Leveraging Microsoft's Kerberos Authentication (IWA), SecureAuth IdP can securely assert users to realms without bulky login procedures.

Service Provider Integrations

Service Provider (SP) integrations include cloud, web, mobile, and network-based applications / devices to which SecureAuth IdP enables 2-Factor Authentication and SSO access. SecureAuth IdP supports various industry-standard protocols, including SAML, WS-*, RADIUS, HTTP, OAuth 2.0, and OpenID Connect, making virtually any SP integration possible. Refer to the **Application Integration Guides** and **VPN / Device Integration Guides** from the list below for more information and specific SP integration configuration steps.

Identity Management Tools

SecureAuth's out-of-the-box Identity Management (IdM) Tools include administrative and user self-services account management options, as well as other helpful resources. The IdM Tools can be configured in the **Post Authentication** tab (refer to the configuration guide(s) in the list below) to enable Administrator (Help Desk) Account Management, User Self-services Account Update, Self-services Password Reset, Secure Portal, Account Unlock, Revoke Certificate, Create User, Mobile App Store, Reporting, and other time and cost-saving tools.

Mobile

SecureAuth IdP supports the BYOD and mobile trends with 2-Factor Authentication and SSO SDKs for iOS and Android native, mobile applications; and enables provisioning and certificate delivery and synchronization from appliances to individual mobile devices to alleviate user friction and burdening login procedures.

Configuration Guides

Post Authentication Tab Configuration – configure SecureAuth IdP realms with specific post-authentication (assertion) events

- **SecureAuth IdP Out-of-the-box Identity Management Tools** – configure SecureAuth IdP out-of-the-box administrative and user self-services Identity Management (IdM) Tools, which include Administrative Account Update, Self-services Account Update, Self-services Password Reset, Secure Portal (SSO), Create User, Revoke Certificate, Account Unlock, and others
- **Application Integration Guides** – integrate SecureAuth IdP with cloud and web applications to enable 2-Factor Authentication and Single Sign-on (SSO) access via SAML, WS-*, OpenID Connect / OAuth 2.0, and other industry-standard protocols
- **VPN and Device Integration Guides** – integrate SecureAuth IdP with VPNs and other devices to enable 2-Factor Authentication and SSO access via SAML, certificate delivery, RADIUS, HTTP, and other industry-standard protocols
- **Mobile** – enable mobile provisioning and other mobile post-authentication actions
- **Transformation Engine Guide** – enable on-the-fly changes to SAML assertions, post-authentication to ensure that the SP receives what is required for the integration without modifying or storing additional information in the corporate directory
- **OpenID Connect and OAuth 2.0 configuration** – learn more about how SecureAuth IdP integrates with applications using OpenID Connect / OAuth 2.0 protocols

Transparent Single Sign-on SSO – enable SSO access through the use of a Secure Portal (IdM Tool) or **Transparent SSO**, which leverages the same, authenticated credentials to allow access into multiple applications without requiring a landing page

iOS Mobile SDK Integration Guide (8.0) – enable 2-Factor Authentication and SSO access to native, mobile applications with SecureAuth's SDK for iOS

Android Mobile SDK Integration Guide (8.0) – enable 2-Factor Authentication and SSO access to native, mobile applications with SecureAuth's SDK for Android