SecureAuth IdP 8.0.x Identity Management

SecureAuth IdP Identity Management

SecureAuth IdP makes managing identities easy and secure by integrating with existing, corporate directories, providing administrative and user self-services IdM Tools, and enabling auditing of all authentication events for review. Many of SecureAuth IdP's IdM features enable customers to make identity modifications through SecureAuth IdP that are then applied to their directory or other parts of their environment.

Each SecureAuth IdP **realm** can be configured with distinct directories, point to specific IdM pages, and employ necessary logging functions to create diverse access abilities for any user or groups of users.

Directory Integrations

SecureAuth IdP can integrate with various directories, including LDAP, SQL, Oracle, ASP.NET, and other data stores. Customers can employ one or multiple directories in each realm to create frictionless access and minimize the number of realms used by utilizing SecureAuth's Web Service Multi-Data Store configuration (see the configuration guide in the list below) or by integrating various directories as profile providers. In a SecureAuth IdP realm, there are two directory integration requirements configured in the **Data** tab (see the configuration guide in the list below): Membership Connection and Profile Provider. One directory can be used for both; or one can be used for Membership Connection and others can be used to provide profile data (with or without the membership directory included). This addresses use cases in which membership information is stored in one directory (say, Active Directory), and profile information is stored in another (SQL Server, for example).

The Web Service Multi-Data Store option enables SecureAuth IdP to call to other realms on the same or different servers to locate user information. This is especially helpful if there are multiple directories for different user types, e.g. internal employees, contractors, customers, etc.

The **Data** tab also contains Profile Property mapping, which enables companies to map directory attributes to SecureAuth IdP Properties without storing sensitive information on the appliance. The properties are then used in authentication and assertion actions, calling back to the directory to pull the relevant information.

Identity Management (IdM 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 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. Refer to the specific configuration guides in the list below.

Actions that are completed through certain tools, such as Help Desk or Self-service Account Update, are made on SecureAuth IdP client-side pages, but then applied to the corporate directory. This enables easy account management without having to manually modify information in the data store.

Logging and Auditing

SecureAuth IdP enables the logging and auditing of all authentication events, which can then be reviewed to find suspicious activity, debug errors, analyze user access, and other helpful functions. In the **Logs** tab (refer to the configuration guide in the list below) of each realm, Audit, Debug, Error, Event, and Text logs can be enabled, and integrations with SysLog and Database logs can be completed. The logs can be reviewed in the Web Admin, or downloaded for further inspection.

Configuration Guides

Data Tab Configuration – integrate a corporate directory(ies) with SecureAuth IdP for membership information (membership connection directory integration) to validate users' existence in the data store, and profile data (profile provider directory integration) to abstract information for authentication and assertion purposes. This also includes Profile Property mapping to directory attributes to enable connection between IdP and the directory without profile information being stored on the appliance. Select the appropriate directory integration from the list below, which include guides on how to integrate for membership connection purposes and for profile provider purposes.

- **Active Directory (sAMAccountName) Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Active Directory (UPN) Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Lightweight Directory Services (AD-LDS) Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Lotus Domino Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Novell eDirectory Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Sun ONE Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Tivoli Directory Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Open LDAP Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Other LDAP Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **SQL Server Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **ODBC Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **ASPNETDB Membership Connection Directory Integration** and **Profile Provider Directory Integration**
- **Web Service (Multi-Data Store) Membership Connection Directory Integration** and **Profile Provider Directory Integration**

LDAP Attributes and SecureAuth IdP Profile Properties – review a list of SecureAuth IdP Profile Properties and their requirements for LDAP attribute mapping

SQL User Data Store Tables and Stored Procedures – create the required tables and stored procedures to enable SecureAuth IdP functions

SecureAuth IdP Out-of-the-box Identity Management (IdM) Tools

- **Account Management (Help Desk) Page Configuration Guide** – configure the help desk page for administrative account management
- **Create User Page Configuration Guide** – enable users to self-create or help desk to create users through SecureAuth IdP, and then write them to the corporate directory
- **Forgot Username Configuration Guide** – allow users to securely request their usernames if lost / forgotten
- **Password Reset Page Configuration Guide** – configure the self-services password reset page, which enables users to securely reset their own passwords
- **Revoke Certificate Page Configuration Guide** – enable administrators to quickly and securely revoke user certificates
- **Secure Portal Configuration Guide** – configure the SSO landing page that enables users to securely access all resources with a single set of credentials
- **Self-service Account Update page configuration**– configure the user account update page for user self-service account management

Reporting Page Configuration Guide – create a landing page for administrators to review and log authentication events

Logs Tab Configuration – enable and configure error, debug, info, and other logs that track SecureAuth IdP events for review