Directory integrations

Introduction

SecureAuth IdP integrates with your company's on-premises, corporate directories and data stores for end-user authentication, completion of the post authentication assertion process, and / or usage by identity management resources such as the self-services account update tool. User profiles remain in your data store and are never saved on SecureAuth IdP, keeping data in your control, with no duplicate content to manage elsewhere.

The New Experience user interface lets you connect your company's Active Directory and / or SQL Server directory to SecureAuth IdP. You configure the directory as a user data membership directory to validate a company's active users, or as an authentication data profile directory to provide and update user profile information required by a realm or application added on SecureAuth IdP. The directory connection is saved as a membership directory object or as a profile directory object which can be associated with any number of realms or applications added on SecureAuth IdP.

When adding a profile directory connection, you are prompted to map attributes to AD properties, or define the data format of attributes supplied to SQL service providers / tables. The attribute mapping or data format definitions, and the directory connection profile, are collectively saved in the object that can be associated with realms and applications. Re-using this object is a configuration time-saver and prevents AD mapping errors since a property can only have one attribute mapped to it on the directory connection.

You can associate multiple directory objects with a single post authentication resource. In this scenario, you specify additional second factor authentication workflows to be used and do not need to configure each individual realm to be used in a realm-chaining configuration.

The SecureAuth IdP version 9.3 Web Admin user interface supports AD and SQL directory integrations only. The Classic Web Admin user interface supports LDAP, Azure AD, Oracle, Tivoli, ODBC, ASP.NET, and NetIQ (Novell) eDirectory, in addition to AD and SQL directory integrations.

NOTE: A directory integration configured and saved on the New Experience user interface cannot be edited on the Classic Experience user interface since the directory configuration is stored in the cloud and not on the SecureAuth IdP appliance.

Prerequisites

- SecureAuth IdP version 9.3 installed and running.
- On-premises Active Directory / SQL Server (membership directory / profile directory). The directory will be integrated with SecureAuth IdP so that end-user information can be extracted from the directory's data store to complete authentication and assertion functionality.
- Service account set up for SecureAuth IdP to access the data store. The account should be granted read privileges and optionally write privileges to update end-user information.

NOTE: Credentials used to access the integrated directory are stored in a secure, storage component in the on-premises SecureAuth IdP which keeps credentials encrypted.

Select the directory integration type

Active Directory integration

SQL Server integration