LDAP Attributes / SecureAuth IdP Profile Properties Data Mapping

Introduction

Use this guide as a reference to appropriately map SecureAuth IdP Profile Properties to LDAP Attributes in the directory.

SecureAuth IdP integrates with on-premises directories for user profile mapping to validate and extract information without storing any data on the appliance to effectively authenticate and assert end-users.

The table below exemplifies the LDAP Attribute requirements for each Profile Property, and provides Active Directory-specific examples that can be utilized in configurations.

Prerequisites

1. Have an LDAP directory store
2. Create a service account for SecureAuth IdP with read access, and optional write access to enable various features

    In the table below, the **True Writable** options will not be available if the service account has only read access

3. Grant permissions to the directory fields that are required to be writable (if providing write access to the service account)
4. Integrate an on-premises LDAP directory with SecureAuth IdP (see **Data Tab Configuration** for specific configuration steps)

SecureAuth IdP Profile Properties

This list includes all available Profile Properties; however, not every Property is required to be mapped

Only the Properties that are specifically utilized in the realm (for authentication and/or post-authentication) need to be mapped to an LDAP directory field

The **AD Field** listed in the table is an *example* of a valid directory field to use in the configuration, but any field that fulfills the requirements can be utilized

SecureAuth IdP Profile Property	Definition	LDAP Attribute Requirements				Writable	AD-specific Field Example
		LDAP Syntax	Size (RangeUpper)	Multi-valued	Format Support		
Groups	Groups to which user belongs	2.5.5.12 (Directory String)	N / A	False	Plain Text	False	memberOf
First Name	User's first name	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **First Name** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **First Name** dropdown on the Self-service Configuration Page	givenName
Last Name	User's last name	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Last Name** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Last Name** dropdown on the Self-service Configuration Page	sn
Phone 1	User's primary phone number, typically corporate number	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Phone 1** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Phone 1** dropdown on the Self-service Configuration Page	telephoneNumber

Phone 2	User's secondary phone number, typically mobile phone number	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Phone 2** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Phone 2** dropdown on the Self-service Configuration Page	mobile
Phone 3	User's additional phone number	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Phone 3** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Phone 3** dropdown on the Self-service Configuration Page	See **DirectoryString List** below for options
Phone 4	User's additional phone number	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Phone 4** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Phone 4** dropdown on the Self-service Configuration Page	See **DirectoryString List** below for options
Email 1	User's primary email address, typically corporate email	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Email 1** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Email 1** dropdown on the Self-service Configuration Page	mail
Email 2	User's secondary email address, typically personal email	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Email 2** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Email 2** dropdown on the Self-service Configuration Page	See **DirectoryString List** below for options
Email 3	User's additional email address	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Email 3** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Email 3** dropdown on the Self-service Configuration Page	See **DirectoryString List** below for options
Email 4	User's additional email address	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show Enabled** is selected from the **Email 4** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Email 4** dropdown on the Self-service Configuration Page	See **DirectoryString List** below for options
PIN	User's static Personal Identification Number	2.5.5.12 (Directory String)	1024	False	Plain Text (based on selection in Registration Methods tab) Standard Hash (based on selection in Registration Methods tab)	True for **Account Management Page** realm if **Show Enabled** is selected from the **PIN** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **PIN** dropdown on the Self-service Configuration Page	otherLoginWorkstations
KB Questions	User's knowledge-based questions, e.g. In what city did you grow up?	2.5.5.12 (Directory String)	32768 Recommended (dependent on number and length of KBQs)	False	Base64 Encoding (based on selection in Registration Methods tab) Encryption (based on selection in Registration Methods tab)	True for **Account Management Page** realm if **Show** is selected from the **Clear KBQ-KBA CheckBox** dropdown on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **KBQ-KBA** dropdown on the Self-service Configuration Page	houseIdentifier
KB Answers	User's answers to knowledge-based questions, e.g. Irvine	2.5.5.12 (Directory String)	4096 Recommended (dependent on number and length of KBAs)	False	Base64 Encoding (based on selection in Registration Methods tab)	True for **Account Management Page** realm if **Show** is selected from the **Clear KBQ-KBA CheckBox** dropdown on the Help Desk Configuration Page	homePostalAddress

					Encryption (based on selection in Registration Methods tab)	True for **Self-service Account Update** realm if **Show Enabled** is selected from the **KBQ-KBA** dropdown on the Self-service Configuration Page	
Aux ID 1 - 10	Placeholder Properties that can be mapped to any LDAP attribute and extracted for authentication or asserted to resource	Dependent on LDAP Attribute				True for **Account Management Page** realm if **Show Enabled** is selected from the **Aux 1 - 10** dropdown(s) on the Help Desk Configuration Page True for **Self-service Account Update** realm if **Show Enabled** is selected from the **Aux 1 - 10** dropdown(s) on the Self-service Configuration Page	Appropriate LDAP Attribute
Cert Serial Number	Certificate that is generated by SecureAuth IdP and stored in user profile	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for all **Certificate Enrollment** realms	See **DirectoryString List** below for options
Cert Reset Date	Certificate revocation date – certificates delivered before this date are invalidated	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management** realm if **Show Enabled** is selected from the **Cert Rev Field** on the Help Desk Configuration Page	See **DirectoryString List** below for options
Certificate Count	Number of certificates in user's profile	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for all **Certificate Enrollment** realms True for **Account Management Page** realm if **Show Enabled** is selected from the **Cert Count Field** dropdown and / or if **Show Enabled is selected from the Cert Rev Field** on the Help Desk Configuration Page	See **DirectoryString List** below for options
Certificate Expiration	Date on which user's certificate expires	2.5.5.12 (Directory String)	1024 Recommended	False	Plain Text	True for all **Certificate Enrollment** realms in which **Email Notification** is **Enabled** in the **Certificate / Token Properties** section (Workflow tab)	See **DirectoryString List** below for options
Mobile Reset Date	Mobile cookie revocation date – cookies delivered before this date are invalidated	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Account Management Page** realm if **Show** is selected from the **Mobile Rev** dropdown on the Help Desk Configuration Page	See **DirectoryString List** below for options
Mobile Count	Number of mobile cookies in user's profile	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for all realms in which **Mobile Enrollment and Validation** is selected from the **Integration Mode** dropdown on the Workflow tab True for **Account Management Page** realm if **Show** is selected from the **Mobile Rev** dropdown on the Help Desk Configuration Page	See **DirectoryString List** below for options
iOS Devices	Unique ID of iOS devices stored for use in Fingerprinting	2.5.5.12 (Directory String)	N / A	False	Plain Text	True	See **DirectoryString List** below for options
Ext. Sync Pwd Date	Date on which Google Apps and LDAP directory passwords synchronize	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for realms in which **Google Apps Functions** are enabled for the **Sync Password** feature, and in which the password synchronizes on a specific date rather than on every login	See **DirectoryString List** below for options
Hardware Token	Yubikey information used for 2-Factor Authentication	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for **Yubikey Provisioning** realm	See **DirectoryString List** below for options
OATH Seed	Seed used to generate OATH One-time Passwords (OTPs)	2.5.5.12 (Directory String)	4096 (or higher) Required	False	Advanced Encryption	True for **OATH Provisioning** realm	postalAddress
One Time OATH List	List of valid OATH OTPs to increase security during offset duration	2.5.5.12 (Directory String)	N / A	False	Plain Text	True for all realms in which OATH OTPs are **Enabled** for second factor (Registration Methods tab) and in which the One Time OATH List feature is enabled	See **DirectoryString List** below for options

The **Fingerprints, **Push Notification Tokens**, and **Access Histories** Properties have distinct LDAP attribute requirements based on the select **Format Support** (Plain Binary vs. JSON)**

**Fingerprints	Values created from unique characteristics of a user's desktop, browser, or mobile device	2.5.5.10 (Octet)	8 kB (or higher) per Fingerprint Record Required If the **Total FP Max Count** is set to -1 (no limit), then the size must be **unlimited** **NOTE:** The **FP's access records max count** data is also stored in the **Fingerprints** Property and increases the size	True	Plain Binary	True	audio

		2.5.5.12 (Directory String)	No Limit / Undefined		JSON		accountNameHistory
**Push Notification Tokens	Registered devices to receive PUSH Notifications	2.5.5.10 (Octet)	4096 (or higher) Required	True	Plain Binary	True	jpegPhoto
		2.5.5.12 (Directory String)			JSON		altSecurityIdentities
**Access Histories	IP Address, geo-location, and last access time of user for Adaptive Authentication comparison	2.5.5.10 (Octet)	1024 (or higher) per Access History Record Required The Access History setting can be configured in the web.config file: **<add key="AccessHistoryMaxCount" value="5" />**	True	Plain Binary	True	photo
		2.5.5.12 (Directory String)			JSON		otherMailbox

DirectoryString List

These are Active Directory DirectoryString (2.5.5.12) options that can be used for the Profile Properties noted above; but any DirectoryString attribute that fulfills the other requirements can be utilized as well

- extensionName
- facsimileTelephoneNumber
- info
- ipPhone
- otherFacsimileTelephoneNumber

- otherHomePhone
- otherIpPhone
- otherLoginWorkstations
- otherMobile
- otherPager

- otherTelephone
- pager
- postOfficeBox
- street
- streetAddress