LDAP Attributes / SecureAuth IdP Profile Properties Data Mapping

Use this guide as a reference to map the SecureAuth® Identity Platform (formerly SecureAuth IdP) profile properties to LDAP attributes in the directory.

You can integrate an LDAP directory with the Identity Platform to assert or manage user identity information.

The mapping table details the LDAP attribute requirements for each profile property. The table includes examples of specific Active Directory fields which can be used in configurations.

Prerequisites

- Access to an LDAP directory store
- Service account with read access, and optional write access to enable various features. In the table below, the **True Writable** options are not be available if the service account only has read access.
- Grant permissions to the directory fields that are required to be writable (if providing write access to the service account)
- LDAP directory integration with Identity Platform

Contents

Identity Platform profile properties

The following table lists all available profile properties; however it does not require that every property be mapped.

Any property that is specifically used in the realm for authentication and post-authentication must be mapped to an LDAP directory field.

The **AD Field** column in the table provides an *example* of a valid directory field to use in the configuration; however, you can use any field that fulfills the requirements.

Profile Property	Definition	LDAP attribute requirements	Example of AD-specific field
First Name	First name of user	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when First Name is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when First Name is set to Show Enabled	givenName
Last Name	Last name of user	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Last Name is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Last Name is set to Show Enabled	sn

Groups	Groups to which a user belongs	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable False	memberOf
Phone 1 (Work)	Primary phone number associated with user; typically a work number	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Phone 1 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Phone 1 is set to Show Enabled	telephoneNumber
Phone 2 (Mobile)	Secondary phone number associated with user; typically a mobile number	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Phone 2 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Phone 2 is set to Show Enabled	mobile
Phone 3 (Alternate)	Alternate phone number associated with user	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Phone 3 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Phone 3 is set to Show Enabled	See DirectoryString List below for options
Phone 4 (Alternate)	Alternate phone number associated with user	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Phone 3 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Phone 3 is set to Show Enabled	See DirectoryString List below for options
Email 1 (Work)	Primary email address associated with user; typically a work email	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Email 1 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Email 1 is set to Show Enabled	mail

Email 2 (Personal)	Secondary email address associated with user; typically a personal email	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Email 2 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Email 2 is set to Show Enabled	See DirectoryString List below for options
Email 3 (Alternate)	Alternate email address associated with user	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Email 3 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Email 3 is set to Show Enabled	See DirectoryString List below for options
Email 4 (Alternate)	Alternate email address associated with user	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – in **Account Management (Help Desk)** realm configuration, when Email 4 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Email 4 is set to Show Enabled	See DirectoryString List below for options
Aux ID 1 to Aux ID 10	Placeholder properties that can be mapped to any LDAP attribute and extracted for authentication or asserted to resource	LDAP Syntax Depends on LDAP attribute Format Support Depends on LDAP attribute Writable • True – in **Account Management (Help Desk)** realm configuration, when Aux ID # is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Aux ID # is set to Show Enabled	Appropriate LDAP Attribute
PIN	Static personal identification number (PIN) associated with the user account	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 1024 Multi-valued False Format Support – Plain text (based on selection in Multi-Factors Methods tab) Writable is True – in **Account Management (Help Desk)** realm configuration, when PIN is set to Show Enabled Format Support – standard hash (based on selection in Multi-Factors Methods tab) Writable is True – in **Self-service Account Update** realm configuration, when PIN is set to Show Enabled	otherLoginWorkstations

Knowledge-based questions (KBQ)	Knowledge-based questions for the user; for example, what city did you grow up?	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 32768 recommended; dependent on number and length of KBQs Multi-valued False Format Support – Base64 encoding (based on selection in Multi-Factors Methods tab) Writable is True – in **Account Management (Help Desk)** realm configuration, when Clear KBQ-KBA CheckBox is set to Show Format Support – Encryption (based on selection in Multi-Factors Methods tab) Writable is True – in **Self-service Account Update** realm configuration, when KBQ-KBA is set to Show Enabled	houseIdentifier
Knowledge-based answers (KBA)	Knowledge-based answers from the user; for example, Irvine	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 4096 recommended; dependent on number and length of KBAs Multi-valued False Format Support – Base64 encoding (based on selection in Multi-Factors Methods tab) Writable is True – in **Account Management (Help Desk)** realm configuration, when Clear KBQ-KBA CheckBox is set to Show Format Support – Encryption (based on selection in Multi-Factors Methods tab) Writable is True – in **Self-service Account Update** realm configuration, when KBQ-KBA is set to Show Enabled	homePostalAddress
Cert Serial Number	Certificate generated by SecureAuth IdP and stored in user profile	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable 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	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable True – in **Account Management (Help Desk)** realm configuration, when Cert Rev Field is set to Show Enabled	See DirectoryString List below for options
Certificate Count	Number of certificates in user profile	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – for all **Certificate Enrollment** realms • True – in **Account Management (Help Desk)** realm configuration, when Cert Count Field is set to Show Enabled • True – in **Account Management (Help Desk)** realm configuration, when Cert Rev Field is set to Show Enabled	See DirectoryString List below for options
Certificate Expiration	Date on which certificate expires for the user	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 1024 recommended Multi-valued False Format Support Plain text Writable True – for all **Certificate Enrollment** realms (Workflow tab > Certificate / Token Properties section), in which Email Notification is set to Enabled	See DirectoryString List below for options

Mobile Reset Date	Mobile cookie revocation date – cookies delivered before this date are invalidated	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable True – in **Account Management (Help Desk)** realm configuration, when Mobile Rev is set to Show	See DirectoryString List below for options
Mobile Count	Number of mobile cookies in the profile associated with the user	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable • True – for all realms (Workflow tab > Device Recognition Method section) in which Integration Method is set to Mobile Enrollment and Validation. • True – in **Account Management (Help Desk)** realm configuration, when Mobile Rev is set to Show	See DirectoryString List below for options
iOS Devices	Unique ID of iOS devices stored for use in Fingerprinting	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable True	See DirectoryString List below for options
Ext. Sync Pwd Date	Date on which Google Apps and LDAP directory passwords synchronize	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable True for realms in which the Sync Password feature has Google Apps Functions enabled, and in which the password synchronizes on a specific date rather then on every login.	See DirectoryString List below for options
Hardware Token	YubiKey information used for multi-factor authentication (MFA)	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable True for YubiKey provisioning realm	See DirectoryString List below for options
OATH Seed	Seed used to generate OATH One-time Passwords (OTPs)	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 4096 (or higher) required Multi-valued False Format Support Advanced encryption Writable True for OATH provisioning realm	postalAddress
One Time OATH List	List of valid OATH OTPs to increase security during offset duration	LDAP Syntax 2.5.5.12 (Directory String) Multi-valued False Format Support Plain text Writable True for all realms (Multi-Factor Methods tab) in which OATH OTPs are set to Enabled for second factor, and realms in which the One Time OATH List feature is enabled	See DirectoryString List below for options

Behavior Biometrics	Behavior profile used in behavioral biometrics authentication (Authentication API)	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) No limit / undefined Multi-valued False Format Support Plain text Writable True	comment

** The following table contains distinct LDAP attribute requirements based on the selected **Format Support** (plain binary vs JSON)

Profile Property	Definition	LDAP attribute requirement	Example of AD-specific field
Fingerprints ** (Plain binary)	Values created from unique characteristics of desktop, browser, or mobile device associated with the user	LDAP Syntax 2.5.5.10 (Octet) Size (RangeUpper) • 8 kB (or higher) per Fingerprint record required • If the Total FP Max Count is set to -1 (no limit), then the upperRange must be unlimited NOTE: Fingerprint access records max count data is also stored in the Fingerprints Property and increases the size Multi-valued True Format Support Plain binary Writable True	audio
Fingerprints ** (JSON)	Values created from unique characteristics of desktop, browser, or mobile device associated with the user	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) No limit / undefined Multi-valued True Format Support JSON Writable True	accountNameHistory
Push Notification Tokens ** (Plain binary)	Devices registered to receive push notifications	LDAP Syntax 2.5.5.10 (Octet) Size (RangeUpper) 4096 (or higher) required Multi-valued True Format Support Plain binary Writable True	jpegPhoto
Push Notification Tokens ** (JSON)	Devices registered to receive push notifications	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 4096 (or higher) required Multi-valued True Format Support JSON Writable True	altSecurityIdentities

OATH Tokens ** (Plain binary)	Devices provisioned to use OATH Tokens for second factor authentication (contains OATH Seed)	LDAP Syntax 2.5.5.10 (Octet) Size (RangeUpper) 4096 (or higher) required Multi-valued True Format Support Plain binary Writable True	registeredAddress
OATH Tokens ** (JSON and JSON Encrypted)	Devices provisioned to use OATH Tokens for second factor authentication (contains OATH Seed)	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 4096 (or higher) required Multi-valued True Format Support JSON, JSON encrypted Writable True	otherIpPhone
Access Histories ** (Plain binary)	IP Address, geo-location, and last access time of user for adaptive authentication comparison	LDAP Syntax 2.5.5.10 (Octet) Size (RangeUpper) 4096 (or higher) required Multi-valued True Format Support Plain binary Writable True	photo
Access Histories ** (JSON)	IP Address, geo-location, and last access time of user for adaptive authentication comparison	LDAP Syntax 2.5.5.12 (Directory String) Size (RangeUpper) 4096 (or higher) required Multi-valued True Format Support JSON, JSON encrypted Writable True	otherMailbox

When running SecureAuth IdP v9.2 with non-Microsoft AD servers, be sure to verify the attribute syntax for registeredAddress (Octet) since a different syntax is often specified in Open LDAP and other LDAP implementations.

DirectoryString list

The following list contains AD DirectoryString (2.5.5.12) options that can be used for the profile properties noted in the above tables. However, any DirectoryString attribute that fulfills other requirements can be used as well.

- extensionName
- facsimileTelephoneNumber
- info
- ipPhone
- otherFacsimileTelephoneNumber
- otherHomePhone
- otherLoginWorkstations
- otherMobile
- otherPager
- otherTelephone
- pager
- postOfficeBox
- street
- streetAddress

Common profile property mappings to LDAP attributes

The following table contains common mappings to which you can copy and paste.

Profile property	Definition	Multi-valued	Format Support	Writeable	AD-specific field	Active Directory options
Access Histories	IP Address, geo-location, and last access time of user for adaptive authentication comparison	True	Plain binary or JSON	True	photo	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
OATH Tokens	Devices provisioned to use OATH Tokens for second factor authentication (contains OATH Seed)	True	Plain binary or JSON	True	registeredAddress	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
Push Notification Tokens	Devices registered to receive push notifications	True	Plain binary or JSON	True	jpegPhoto	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
Fingerprints	Values created from unique characteristics of desktop, browser, or mobile device associated with the user	True	Plain binary or JSON	True	audio	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager

OATH Seed	Seed used to generate OATH One-time Passwords (OTPs)	False	Advanced encryption	True for OATH provisioning realm	postalAddress	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
Aux ID 2	User's ported phone numbers	Depends on LDAP attribute	Plain text	• True – in **Account Management (Help Desk)** realm configuration, when Aux ID # is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Aux ID # is set to Show Enabled	carlicense	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
Email 1 (Work)	Primary email address associated with user; typically a work email	False	Plain text	• True – in **Account Management (Help Desk)** realm configuration, when Email 1 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Email 1 is set to Show Enabled	mail	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
Email 2 (Personal)	Secondary email address associated with user; typically a personal email	False	Plain text	• True – in **Account Management (Help Desk)** realm configuration, when Email 2 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Email 2 is set to Show Enabled	otherMailbox	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
Phone 1 (Work)	Primary phone number associated with user; typically a work number	False	Plain text	• True – in **Account Management (Help Desk)** realm configuration, when Phone 1 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Phone 1 is set to Show Enabled	telephoneNumber	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager

Phone 2 (Mobile)	Secondary phone number associated with user; typically a mobile number	False	Plain text	• True – in **Account Management (Help Desk)** realm configuration, when Phone 2 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Phone 2 is set to Show Enabled	mobile	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager
Phone 3 (Alternate)	Alternate phone number associated with user	False	Plain text	• True – in **Account Management (Help Desk)** realm configuration, when Phone 3 is set to Show Enabled • True – in **Self-service Account Update** realm configuration, when Phone 3 is set to Show Enabled	houseidentifier	extensionName facsimileTelephoneNumber info ipPhone otherFacsimileTelephoneNumber otherHomePhone otherLoginWorkstations otherMobile otherPager