

Attribute Common Name (CN)	LDAP Display Name	Audit Purpose	Description
Account-Expires-Date	accountExpirationDate	Used to determine what accounts have been set to automatically expire.	Date when the user account expires.
Admin-Count	adminCount	Used to determine if account was associated with an administrative group.	User account that was or is currently part of one of the administrative groups.
Assistant	assistant	Used to determine potential role appropriateness.	Name of user's administrative assistant.
Canonical-Name	canonicalName	Used to determine structure of Active Directory.	Name of the object in canonical format, e.g., me.domain.com
Common-Name	cn	Used to uniquely identify employees in Active Directory.	Name of user.
User-Comment	comment	Used to gather contextual information on account.	Comments entered for user's account.
Company	company	Used to determine if account is associated with another company/vendor.	User's company name.
Control-Access-Rights	controlAccessRights	Used to determine additional rights assigned to employee account.	Displays extended control access rights for the object.
Department	department	Used to determine what department an employee works in.	Contains the name for the department in which the user works.
departmentNumber	departmentNumber	Used to categorize employees by department number.	Department number user belongs to.
Description	description	Used to gather contextual information on account.	Description entered for user's account.
Display-Name	displayName	Used to uniquely identify employees in Active Directory.	The user's first name, middle initial, and last name.
Obj-Dist-Name	distinguishedName	Used to determine structure of Active Directory.	Distinguished Name of user account in directory (forest).
Division	division	Used to determine what division an employee works in.	The user's division.
Employee-ID	employeeID	Used to match account with other computer systems and employment records.	ID of an employee.
Employee-Number	employeeNumber	Used to match account with other computer systems and employment records.	Number assigned to an employee other than the Employee ID.
Employee-Type	employeeType	Used to categorize employees.	Job category for an employee.
Generation-Qualifier	generationQualifier	Used to uniquely identify employees in Active Directory.	Indicates a person's generation. For example, Jr. or II.
Given-Name	givenName	Used to uniquely identify employees in Active Directory.	First name of the user.
Comment	info	Used to gather contextual information on account.	Comments for user's account.
Last-Logon-Date	lastLogonDate	Used to determine when the account was last logged in.	Last time user logged into Domain.
E-mail-Addresses	mail	Used to gather contextual information on account. Used to determine employee's email address.	List of email addresses for a contact.
Managed-Objects	managedObjects	Used to determine additional rights assigned to employee account.	List of users accounts or groups that the user has control over.
Manager	manager	Used to gather contextual information on account. Used to determine an employee's manager.	Name of user's manager.
Is-Member-Of-DL	memberOf	Used to determine what groups an employee is assigned to.	List of groups that the user belongs to.
Other-Name	middleName	Used to uniquely identify employees in Active Directory.	Middle name of user.
ms-DS-Allowed-To-Delegate-To	msDS-AllowedToDelegateTo	Used to determine if account can run as a service on another server.	Used to determine if account was given ability to obtain service tickets for Constrained Delegation.
ms-DS-PSO-Applied	msDS-PSOApplied	Used to determine if account is assigned Fine Grain Password Policies.	Microsoft Computed Field at time of query for determining FGPP membership.
ms-DS-Resultant-PSO	msDS-ResultantPSO	Used to determine if account is assigned Fine Grain Password Policies.	Microsoft Computed Field at time of query for determining FGPP membership.
ms-DS-Source-Object-DN	msDS-SourceObjectDN	Used to determine if account is associated with a different forest in Active Directory	Used to determine if user account is associated with another domain.
ms-DS-User-Account-Control-Computed	msDS-User-Account-Control-Computed	Used to determine if account is Locked or has an expired password.	Microsoft Computed Field at time of query for determining user account status, e.g., Normal, Account Locked, Password Expired.
ms-DS-User-Password-Expiry-Time-Computed	msDS-UserPasswordExpiryTimeComputed	Used to determine when the account's password expires.	Microsoft Computed Field at time of query for determining Date/Time of password expiration.
RDN	name	Used to uniquely identify employees in Active Directory.	Name of user.
Organization-Name	o	Used to gather contextual information on account.	Name of the company, organization, vendor.
Object-Sid	objectSid	Used to determine the unique identifier of account.	Unique Identifier for user.
Organizational-Unit-Name	ou	Used to determine structure of Active Directory.	Name of the organizational unit.
Password-Expired	PasswordExpired	Used to determine if account password is expired or not.	Indicates if user's password is expired with a true/false statement.
Password-Last-Set	PasswordLastSet	Used to determine when the employee last changed their password.	Date/Time when password was last set.
Personal-Title	personalTitle	Used to gather contextual information on account. Used to determine employee's title.	User's title.
Primary-Group-ID	primaryGroupID	Used to determine the primary active directory group an employee is assigned.	Primary group assigned to user.
SAM-Account-Name	sAMAccountName	Used to uniquely identify employees in Active Directory.	User Logon name.
See-Also	seeAlso	Used to determine what other accounts are associated with this employee.	List of distinguished names that are related to an object.
Service-Principal-Name	servicePrincipalName	Used to determine additional rights assigned to employee account.	List of principal names used for mutual authentication with an instance of a service on this computer.
SID-History	sIDHistory	Used to determine if account was migrated from another domain.	List of SIDs that user account can use in multiple infrastructures.
Surname	sn	Used to uniquely identify employees in Active Directory.	User's family or last name.
Title	title	Used to gather contextual information on account. Used to determine employee's job title.	User's job title.
uid	uid	Used to gather contextual information on account. Used to determine employee's user ID number.	User ID.
UidNumber	uidNumber	Used to gather contextual information on account. Used to determine employee's user ID number.	User ID to map user to Unix/Linux server.
User-Account-Control	userAccountControl	Used to determine the employee's Active Directory account status.	Specifies user's status in Active Directory e.g., Enabled, Disabled, Password Status.
User-Workstations	userWorkstations	Used to determine if employees are allowed to log in to only certain computers.	Specifies computer(s) that user is allowed to login to.
When-Changed	whenChanged	Used to determine when the account information was last updated.	Date when user account was last updated.
When-Created	whenCreated	Used to determine when the account was last created.	Date when user account was created.