LDAP Reference

This reference covers LDAP-specific features of DS software.

Standards

Supported standards

Controls

Support LDAP controls

Extended Operations

Supported LDAP extended operations

Localization

Supported locales and languages
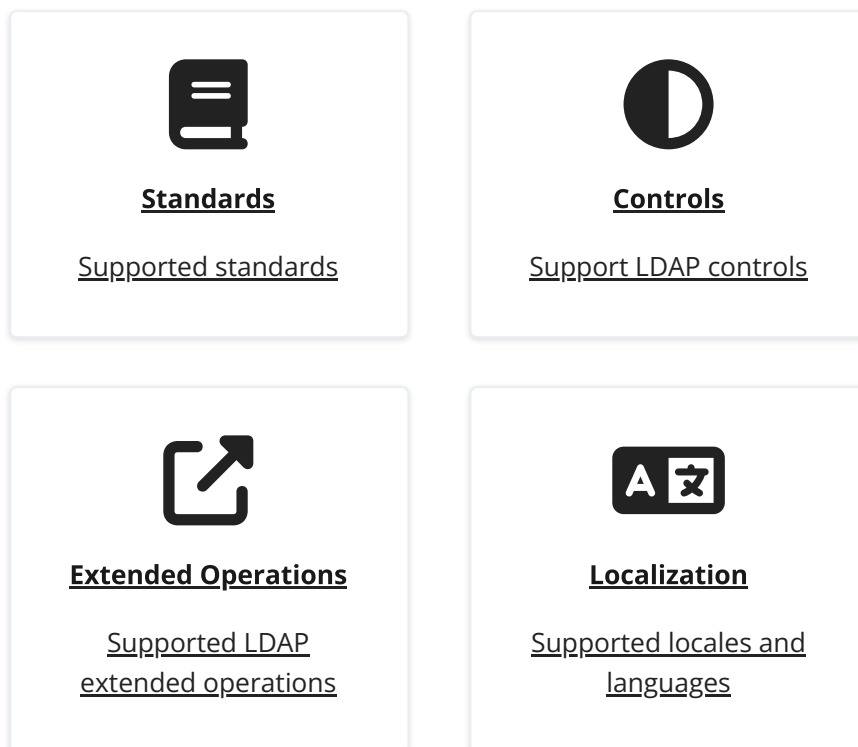
ForgeRock® Identity Platform serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see https://www.forgerock.com ⧉ .

Supported Standards

DS software implements the following RFCs, Internet-Drafts, and standards:

RFC 1274: The COSINE and Internet X.500 Schema ⧉
    X.500 Directory Schema, or Naming Architecture, for use in the COSINE and Internet X.500 pilots.

RFC 1321: The MD5 Message-Digest Algorithm ⧉
    MD5 message-digest algorithm that takes as input a message of arbitrary length, and produces a 128-bit "fingerprint" or "message digest" of the input.

RFC 1777: Lightweight Directory Access Protocol (LDAPv2) ⧉

Provide access to the X.500 Directory while not incurring the resource requirements of the Directory Access Protocol.

Classified as an historic document.

RFC 1778: The String Representation of Standard Attribute Syntaxes ⧉

Defines the requirements that must be satisfied by encoding rules, used to render X.500 Directory attribute syntaxes into a form suitable for use in LDAP. Defines the encoding rules for the standard set of attribute syntaxes.

Classified as an historic document.

RFC 1779: A String Representation of Distinguished Names ⧉

Defines a string format for representing names, which is designed to give a clean representation of commonly used names, while being able to represent any distinguished name.

Classified as an historic document.

RFC 2079: Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs) ⧉

Defines a new attribute type and an auxiliary object class to store URIs, including URLs, in directory entries.

RFC 2222: Simple Authentication and Security Layer (SASL) ⧉

Describes a method for adding authentication support to connection-based protocols.

RFC 2246: The TLS Protocol Version 1.0 ⧉

Specifies Version 1.0 of the Transport Layer Security protocol.

RFC 2247: Using Domains in LDAP/X.500 Distinguished Names ⧉

Defines an algorithm by which a name registered with the Internet Domain Name Service can be represented as an LDAP distinguished name.

RFC 2251: Lightweight Directory Access Protocol (v3) ⧉

Describes a directory access protocol designed to provide access to directories supporting the X.500 models, while not incurring the resource requirements of the X.500 Directory Access Protocol.

RFC 2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions ⧉

Defines a set of syntaxes for LDAPv3, and the rules by which attribute values of these syntaxes are represented as octet strings for transmission in the LDAP protocol.

RFC 2253: Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names ⧉

Defines a common UTF-8 format to represent distinguished names unambiguously.

RFC 2254: The String Representation of LDAP Search Filters⧉

Defines the string format for representing names, which is designed to give a clean representation of commonly used distinguished names, while being able to represent any distinguished name.

RFC 2255: The LDAP URL Format⧉

Describes a format for an LDAP URL.

RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3 ⧉

Provides an overview of the attribute types and object classes defined by the ISO and ITU-T committees in the X.500 documents, in particular those intended for use by directory clients.

RFC 2307: An Approach for Using LDAP as a Network Information Service⧉

Describes an experimental mechanism for mapping entities related to TCP/IP and the UNIX system into X.500 entries so that they may be resolved with LDAP.

RFC 2377: Naming Plan for Internet Directory-Enabled Applications⧉

Proposes a new directory naming plan that leverages the strengths of the most popular and successful Internet naming schemes for naming objects in a hierarchical directory.

RFC 2696: LDAP Control Extension for Simple Paged Results Manipulation⧉

Lets a client control the rate at which an LDAP server returns the results of an LDAP search operation.

RFC 2713: Schema for Representing Java(tm) Objects in an LDAP Directory⧉

Defines a common way for applications to store and retrieve Java objects from the directory.

RFC 2714: Schema for Representing CORBA Object References in an LDAP Directory⧉

Define a common way for applications to store and retrieve CORBA object references from the directory.

RFC 2739: Calendar Attributes for vCard and LDAP⧉

Defines a mechanism to locate a user calendar and free/busy time using the LDAP protocol.

RFC 2798: Definition of the inetOrgPerson LDAP Object Class⧉

Defines an object class called inetOrgPerson for use in LDAP and X.500 directory services that extends the X.521 standard organizationalPerson class.

RFC 2829: Authentication Methods for LDAP⧉

Specifies particular combinations of security mechanisms which are required and recommended in LDAP implementations.

RFC 2830: Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security⧉

Defines the Start Transport Layer Security (TLS) operation for LDAP.

RFC 2849: The LDAP Data Interchange Format (LDIF) - Technical Specification⧉
    Describes a file format suitable for describing directory information or modifications made to directory information.

RFC 2891: LDAP Control Extension for Server Side Sorting of Search Results⧉
    Describes two LDAPv3 control extensions for server-side sorting of search results.

RFC 2926: Conversion of LDAP Schemas to and from SLP Templates⧉
    Describes a procedure for mapping between Service Location Protocol service advertisements and LDAP descriptions of services.

RFC 3045: Storing Vendor Information in the LDAP root DSE⧉
    Specifies two LDAP attributes, vendorName and vendorVersion that may be included in the root DSA-specific Entry (DSE) to advertise vendor-specific information.

RFC 3062: LDAP Password Modify Extended Operation⧉
    Describes an LDAP extended operation to allow modification of user passwords, which does not depend on the authentication identity or the password storage mechanism.

RFC 3112: LDAP Authentication Password Schema⧉
    Describes LDAP schema for user/password authentication including the authPassword attribute type. This attribute type holds values derived from the user's password(s) (commonly using cryptographic strength one-way hash).

RFC 3296: Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories⧉
    Details schema and protocol elements for representing and managing named subordinate references in LDAP directories.

RFC 3377: Lightweight Directory Access Protocol (v3): Technical Specification⧉
    Specifies the set of RFCs comprising LDAPv3, and addresses the "IESG Note" attached to RFCs 2251 through 2256.

RFC 3383: Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)⧉
    Provides procedures for registering extensible elements of LDAP.

RFC 3546: Transport Layer Security (TLS) Extensions⧉
    Describes extensions that may be used to add functionality to Transport Layer Security.

RFC 3671: Collective Attributes in the Lightweight Directory Access Protocol (LDAP)⧉
    Summarizes the X.500 information model for collective attributes and describes use of collective attributes in LDAP.

RFC 3672: Subentries in the Lightweight Directory Access Protocol (LDAP)⧉

Adapts the X.500 subentry mechanisms for use with LDAP.

DS servers extend the subtree specification's `specificationFilter` component to allow any search filter.

RFC 3673: Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes⧉
Describes an LDAP extension which clients may use to request the return of all operational attributes.

RFC 3674: Feature Discovery in Lightweight Directory Access Protocol (LDAP)⧉
Introduces a general mechanism for discovery of elective features and extensions, which cannot be discovered using existing mechanisms.

RFC 3712: Lightweight Directory Access Protocol (LDAP): Schema for Printer Services⧉
Defines a schema, object classes and attributes, for printers and printer services, for use with LDAP directories.

RFC 3771: Lightweight Directory Access Protocol (LDAP) Intermediate Response Message⧉
Defines and describes the IntermediateResponse message, a general mechanism for defining single-request/multiple-response operations in LDAP.

RFC 3829: Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls⧉
Extends the LDAP bind operation with a mechanism for requesting and returning the authorization identity it establishes.

RFC 3876: Returning Matched Values with the Lightweight Directory Access Protocol version 3 (LDAPv3)⧉
Describes a control for LDAPv3 that is used to return a subset of attribute values from an entry.

RFC 3909: Lightweight Directory Access Protocol (LDAP) Cancel Operation⧉
Describes an LDAP extended operation to cancel (or abandon) an outstanding operation, with a response to indicate the outcome of the operation.

RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1⧉
Specifies Version 1.1 of the Transport Layer Security protocol.

RFC 4370: Lightweight Directory Access Protocol (LDAP) Proxied Authorization Control⧉
Defines the Proxy Authorization Control, which lets a client request that an operation be processed under a provided authorization identity instead of under the current authorization identity associated with the connection.

RFC 4403: Lightweight Directory Access Protocol (LDAP) Schema for Universal Description, Discovery, and Integration version 3 (UDDIv3)⧉
Defines the LDAP schema for representing UDDIv3 data types in an LDAP directory.

RFC 4422: Simple Authentication and Security Layer (SASL)⧉

Describes a framework for providing authentication and data security services in connection-oriented protocols via replaceable mechanisms.

RFC 4505: Anonymous Simple Authentication and Security Layer (SASL) Mechanism⧉
Describes a new way to provide anonymous login needed within the context of the SASL framework.

RFC 4510: Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map⧉
Provides a road map of the LDAP Technical Specification.

RFC 4511: Lightweight Directory Access Protocol (LDAP): The Protocol⧉
Describes LDAP protocol elements, and their semantics and encodings.

RFC 4512: Lightweight Directory Access Protocol (LDAP): Directory Information Models⧉
Describes the X.500 Directory Information Models as used in LDAP.

RFC 4513: Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms⧉
Describes LDAP authentication methods and security mechanisms.

RFC 4514: Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names⧉
Defines the string representation used in LDAP to transfer distinguished names.

RFC 4515: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters⧉
Defines a human-readable string representation of LDAP search filters that is appropriate for use in LDAP URLs and in other applications.

RFC 4516: Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator⧉
Describes a format for an LDAP URL.

RFC 4517: Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules⧉
Defines a base set of syntaxes and matching rules for use in defining attributes for LDAP directories.

RFC 4518: Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation⧉
Defines string preparation algorithms for character-based matching rules defined for use in LDAP.

RFC 4519: Lightweight Directory Access Protocol (LDAP): Schema for User Applications⧉
Provides a technical specification of attribute types and object classes intended for use by LDAP directory clients for many directory services, such as white pages.

RFC 4523: Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates⧉

Describes schema for representing X.509 certificates, X.521 security information, and related elements in LDAP directories.

RFC 4524: COSINE LDAP/X.500 Schema⧉
Provides a collection of LDAP schema elements from the COSINE and Internet X.500 pilot projects.

RFC 4525: Lightweight Directory Access Protocol (LDAP) Modify-Increment Extension⧉
Describes an LDAP extension to the LDAP modify operation that supports an increment capability.

RFC 4526: Lightweight Directory Access Protocol (LDAP) Absolute True and False Filters⧉
Extends LDAP to support absolute True and False filters based upon similar capabilities found in X.500 directory systems.

RFC 4527: Lightweight Directory Access Protocol (LDAP) Read Entry Controls⧉
Specifies an LDAP extension to let the client read the target entry of an update operation.

RFC 4528: Lightweight Directory Access Protocol (LDAP) Assertion Control⧉
Defines the LDAP Assertion Control, which lets a client specify that a directory operation should only be processed if an assertion applied to the target entry of the operation is true.

RFC 4529: Requesting Attributes by Object Class in the Lightweight Directory Access Protocol (LDAP)⧉
Extends LDAP to support a mechanism that lets LDAP clients request the return of all attributes of an object class.

RFC 4530: Lightweight Directory Access Protocol (LDAP) entryUUID Operational Attribute⧉
Describes the LDAP/X.500 entryUUID operational attribute and associated matching rules and syntax.

RFC 4532: Lightweight Directory Access Protocol (LDAP) "Who am I?" Operation⧉
Provides an LDAP mechanism for clients to obtain the authorization identity that the server has associated with the user or application entity.

RFC 4616: The PLAIN Simple Authentication and Security Layer (SASL) Mechanism⧉
Defines a simple plaintext user/password SASL mechanism called the PLAIN mechanism.

RFC 4634: US Secure Hash Algorithms (SHA and HMAC-SHA)⧉
Specifies Secure Hash Algorithms, SHA-256, SHA-384, and SHA-512, for computing a condensed representation of a message or a data file.

RFC 4752: The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism⧉

Describes the method for using the GSS-API Kerberos V5 in SASL, called the GSSAPI mechanism.

RFC 4876: A Configuration Profile Schema for Lightweight Directory Access Protocol (LDAP)-Based Agents ⧉
Defines a schema for storing a profile for agents that use LDAP.

RFC 5020: The Lightweight Directory Access Protocol (LDAP) entryDN Operational Attribute ⧉
Describes the LDAP/X.500 entryDN operational attribute, which provides a copy of the entry's DN for use in attribute value assertions.

RFC 5802: Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms ⧉
Describes SASL SCRAM.

RFC 5803: Lightweight Directory Access Protocol (LDAP) Schema for Storing Salted Challenge Response Authentication Mechanism (SCRAM) Secrets ⧉
Describes how an LDAP directory server stores passwords for use in SCRAM SASL binds.

RFC 7677: SCRAM-SHA-256 and SCRAM-SHA-256-PLUS Simple Authentication and Security Layer (SASL) Mechanisms ⧉
Registers mechanisms for SASL SCRAM, updating RFC 5802.

FIPS 180-1: Secure Hash Standard (SHA-1)
Specifies a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file.

FIPS 180-2: Secure Hash Standard (SHA-1, SHA-256, SHA-384, SHA-512)
Specifies four Secure Hash Algorithms for computing a condensed representation of electronic data.

DSMLv2: Directory Service Markup Language ⧉
Provides a method for expressing directory queries and updates as XML documents.

JavaScript Object Notation ⧉
A data-interchange format that aims to be both "easy for humans to read and write," and "easy for machines to parse and generate."

RFC 7643: System for Cross-domain Identity Management: Core Schema ⧉
Platform neutral schema and extension model for representing users and groups in JSON and XML formats. DS supports the JSON format.

The LDAP Relax Rules Control (Internet-Draft) ⧉
Experimental LDAP control allowing a directory client application to request temporary relaxation of data and service model rules.

This control relaxes LDAP constraints, allowing operations that are not normally permitted, such as modifying read-only attributes. To prevent misuse, restrict access to this control to limited administrative accounts.

Supported LDAP Controls

LDAP controls provide a mechanism to extend the semantics and arguments of existing LDAP operations. One or more controls may be attached to a single LDAP message. A control only affects the semantics of the message it is attached to. Controls sent by clients are called *request controls*. Controls returned by servers are called *response controls*.

DS software supports the following LDAP controls:

Account Usability Control
    Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.8

    Sun Microsystems control to determine whether a user account can be used to authenticate to the directory.

Active Directory change notification control
    Object Identifier: 1.2.840.113556.1.4.528

    Microsoft Active Directory control for a client application to register with the directory to receive change notifications.

Assertion request control
    Object Identifier: 1.3.6.1.1.12

    RFC: RFC 4528: Lightweight Directory Access Protocol (LDAP) Assertion Control⊠

Authorization Identity request control
    Object Identifier: 2.16.840.1.113730.3.4.16

    RFC: RFC 3829: Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls⊠

Authorization Identity response control
    Object Identifier: 2.16.840.1.113730.3.4.15

    RFC: RFC 3829: Lightweight Directory Access Protocol (LDAP) Authorization Identity Request and Response Controls⊠

Entry Change Notification response control
    Object Identifier: 2.16.840.1.113730.3.4.7

Internet-Draft: draft-ietf-ldapext-psearch: Persistent Search: A Simple LDAP Change Notification Mechanism ⧉

Get Effective Rights request control
Object Identifier: 1.3.6.1.4.1.42.2.27.9.5.2

Internet-Draft: draft-ietf-ldapext-acl-model: Access Control Model for LDAPv3 ⧉

Internal Modifications control
Object Identifier: 1.3.6.1.4.1.36733.2.1.5.3

ForgeRock control that provides additional modifications to a request for internal operations.

Load Balancer Connection Affinity control
Object Identifier: 1.3.6.1.4.1.36733.2.1.5.2

ForgeRock control that provides a value for connection affinity when using a load balancer from the LDAP SDK.

When you use a DS SDK load balancer that does not support connection affinity, attach this control to LDAP operations that require affinity load balancing.

Manage DSAIT request control
Object Identifier: 2.16.840.1.113730.3.4.2

RFC: RFC 3296: Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories ⧉

Matched Values request control
Object Identifier: 1.2.826.0.1.3344810.2.3

RFC: RFC 3876: Returning Matched Values with the Lightweight Directory Access Protocol version 3 (LDAPv3) ⧉

No-Op Control
Object Identifier: 1.3.6.1.4.1.4203.1.10.2

Internet-Draft: draft-zeilenga-ldap-noop: LDAP No-Op Control ⧉

Password Expired response control
Object Identifier: 2.16.840.1.113730.3.4.4

Internet-Draft: draft-vchu-ldap-pwd-policy: Password Policy for LDAP Directories ⧉

Password Expiring response control
Object Identifier: 2.16.840.1.113730.3.4.5

Internet-Draft: draft-vchu-ldap-pwd-policy: Password Policy for LDAP Directories ⧉

Password Policy response control

Object Identifier: 1.3.6.1.4.1.42.2.27.8.5.1

Internet-Draft: draft-behera-ldap-password-policy: Password Policy for LDAP Directories ⬀

Password Quality Advice controls

Object Identifier: 1.3.6.1.4.1.36733.2.1.5.5

ForgeRock controls that are used for requesting and returning structured password quality advice. The request and response controls share the same OID.

Interface stability: *Evolving*.

Permissive Modify request control

Object Identifier: 1.2.840.113556.1.4.1413

Microsoft defined this control that, "Allows an LDAP modify to work under less restrictive conditions. Without it, a delete will fail if an attribute does not exist, and an add will fail if an attribute already exists. No data is needed in this control." (source of quote ⬀)

Persistent Search request control

Object Identifier: 2.16.840.1.113730.3.4.3

Internet-Draft: draft-ietf-ldapext-psearch: Persistent Search: A Simple LDAP Change Notification Mechanism ⬀

Post-Read request control

Object Identifier: 1.3.6.1.1.13.2

RFC: RFC 4527: Lightweight Directory Access Protocol (LDAP) Read Entry Controls ⬀

Post-Read response control

Object Identifier: 1.3.6.1.1.13.2

RFC: RFC 4527: Lightweight Directory Access Protocol (LDAP) Read Entry Controls ⬀

Pre-Read request control

Object Identifier: 1.3.6.1.1.13.1

RFC: RFC 4527: Lightweight Directory Access Protocol (LDAP) Read Entry Controls ⬀

Pre-Read response control

Object Identifier: 1.3.6.1.1.13.1

RFC: RFC 4527: Lightweight Directory Access Protocol (LDAP) Read Entry Controls ⬀

Proxied Authorization v1 request control

Object Identifier: 2.16.840.1.113730.3.4.12

Internet-Draft: [draft-weltman-ldapv3-proxy-04: LDAP Proxied Authorization Control](#)⬈

Proxied Authorization v2 request control
    Object Identifier: 2.16.840.1.113730.3.4.18

    RFC: [RFC 4370: Lightweight Directory Access Protocol (LDAP) Proxied Authorization Control](#)⬈

Public Changelog Exchange Control
    Object Identifier: 1.3.6.1.4.1.26027.1.5.4

    DS control for using the bookmark cookie when reading the external change log.

Real Attributes Only Request Control
    Object Identifier: 2.16.840.1.113730.3.4.17

    Netscape control indicating that the request is only for attributes actually contained in the entry. Do not return virtual attributes even if they are explicitly requested.

    The control has no value.

Replication Context control
    Object Identifier: 1.3.6.1.4.1.36733.2.1.5.4

    ForgeRock control that is used internally to provide some replication-related context to requests. This control may be removed in the future.

Replication repair control
    Object Identifier: 1.3.6.1.4.1.26027.1.5.2

    DS control that is used to modify the content of a replicated database on a single server without impacting the other servers that are replicated with this server.

Server-Side Sort request control
    Object Identifier: 1.2.840.113556.1.4.473

    RFC: [RFC 2891: LDAP Control Extension for Server Side Sorting of Search Results](#)⬈

Server-Side Sort response control
    Object Identifier: 1.2.840.113556.1.4.474

    RFC: [RFC 2891: LDAP Control Extension for Server Side Sorting of Search Results](#)⬈

Simple Paged Results Control
    Object Identifier: 1.2.840.113556.1.4.319

    RFC: [RFC 2696: LDAP Control Extension for Simple Paged Results Manipulation](#)⬈

Subentries request controls
    Object Identifier: 1.3.6.1.4.1.4203.1.10.1

RFC: <u>Subentries in the Lightweight Directory Access Protocol (LDAP)</u> ⧉

Object Identifier: 1.3.6.1.4.1.7628.5.101.1

Internet-Draft: <u>draft-ietf-ldup-subentry: LDAP Subentry Schema</u> ⧉

Subtree Delete request control
Object Identifier: 1.2.840.113556.1.4.805

Internet-Draft: <u>draft-armijo-ldap-treedelete: Tree Delete Control</u> ⧉

Transaction ID control
Object Identifier: 1.3.6.1.4.1.36733.2.1.5.1

ForgeRock control that enables Common Audit to associate an ID with a request. The ID is recorded with audit events, and can be used to correlate and track user interactions as they traverse the components of the ForgeRock platform.

The control's value is the UTF-8 encoding of the transaction ID.

Virtual List View request control
Object Identifier: 2.16.840.1.113730.3.4.9

Internet-Draft: <u>draft-ietf-ldapext-ldapv3-vlv: LDAP Extensions for Scrolling View Browsing of Search Results</u> ⧉

Virtual Attributes Only Request Control
Object Identifier: 2.16.840.1.113730.3.4.19

Netscape control indicating that the request is only for virtual attributes. Do not return real attributes contained in the entry even if they are explicitly requested.

The control has no value.

Virtual List View response control
Object Identifier: 2.16.840.1.113730.3.4.10

Internet-Draft: <u>draft-ietf-ldapext-ldapv3-vlv: LDAP Extensions for Scrolling View Browsing of Search Results</u> ⧉

Supported LDAP Extended Operations

LDAP extended operations define additional operations for services not already available in the protocol.

DS software supports the following LDAP extended operations:

Cancel Extended Request

Object Identifier: 1.3.6.1.1.8

RFC: [RFC 3909: Lightweight Directory Access Protocol (LDAP) Cancel Operation](#)⬀

Get Connection ID Extended Request
Object Identifier: 1.3.6.1.4.1.26027.1.6.2

DS extended operation to return the connection ID of the associated client connection. This extended operation is intended for DS internal use.

Password Modify Extended Request
Object Identifier: 1.3.6.1.4.1.4203.1.11.1

RFC: [RFC 3062: LDAP Password Modify Extended Operation](#)⬀

Password Policy State Extended Operation
Object Identifier: 1.3.6.1.4.1.26027.1.6.1

DS extended operation to query and update password policy state for a given user entry.

Start Transport Layer Security Extended Request
Object Identifier: 1.3.6.1.4.1.1466.20037

RFC: [RFC 4511: Lightweight Directory Access Protocol (LDAP): The Protocol](#)⬀

Who am I? Extended Request
Object Identifier: 1.3.6.1.4.1.4203.1.11.3

RFC: [RFC 4532: Lightweight Directory Access Protocol (LDAP) "Who am I?" Operation](#)⬀

Support for Languages and Locales

DS software stores data in UTF-8 format. You can store and search for localized directory data for many locales.

Locales and Language Subtypes

DS software supports the following locales with their associated language and country codes, and their collation order object identifiers. Locale support depends on the Java Virtual Machine used at run time. The following list reflects all supported locales.

Locales

Afrikaans

Code tag: af
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.1.1

Albanian
Code tag: sq
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.127.1

Amharic
Code tag: am
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.2.1

Arabic
Code tag: ar
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.3.1

Arabic (Algeria)
Code tag: ar-DZ
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.6.1

Arabic (Bahrain)
Code tag: ar-BH
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.5.1

Arabic (Egypt)
Code tag: ar-EG
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.7.1

Arabic (India)
Code tag: ar-IN
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.8.1

Arabic (Iraq)
Code tag: ar-IQ
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.9.1

Arabic (Jordan)
Code tag: ar-JO
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.10.1

Arabic (Kuwait)
Code tag: ar-KW
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.11.1

Arabic (Lebanon)
Code tag: ar-LB
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.12.1

Arabic (Libya)

Code tag: ar-LY
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.13.1

Arabic (Morocco)
Code tag: ar-MA
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.14.1

Arabic (Oman)
Code tag: ar-OM
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.15.1

Arabic (Qatar)
Code tag: ar-QA
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.16.1

Arabic (Saudi Arabia)
Code tag: ar-SA
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.17.1

Arabic (Sudan)
Code tag: ar-SD
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.18.1

Arabic (Syria)
Code tag: ar-SY
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.19.1

Arabic (Tunisia)
Code tag: ar-TN
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.20.1

Arabic (United Arab Emirates)
Code tag: ar-AE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.4.1

Arabic (Yemen)
Code tag: ar-YE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.21.1

Armenian
Code tag: hy
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.89.1

Bangla
Code tag: bn
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.24.1

Basque

Code tag: eu
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.70.1

Belarusian
Code tag: be
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.22.1

Bulgarian
Code tag: bg
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.23.1

Catalan
Code tag: ca
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.25.1

Chinese
Code tag: zh
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.143.1

Chinese (China)
Code tag: zh-CN
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.144.1

Chinese (Hong Kong SAR China)
Code tag: zh-HK
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.145.1

Chinese (Macau SAR China)
Code tag: zh-MO
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.146.1

Chinese (Singapore)
Code tag: zh-SG
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.147.1

Chinese (Taiwan)
Code tag: zh-TW
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.148.1

Cornish
Code tag: kw
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.99.1

Croatian
Code tag: hr
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.87.1

Czech

Code tag: cs
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.26.1

Danish

Code tag: da
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.27.1

Dutch

Code tag: nl
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.105.1

Dutch (Belgium)

Code tag: nl-BE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.106.1

Dutch (Netherlands)

Code tag: nl-NL
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.105.1

English

Code tag: en
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.34.1

English (Australia)

Code tag: en-AU
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.35.1

English (Canada)

Code tag: en-CA
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.36.1

English (Hong Kong SAR China)

Code tag: en-HK
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.38.1

English (India)

Code tag: en-IN
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.40.1

English (Ireland)

Code tag: en-IE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.39.1

English (Malta)

Code tag: en-MT
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.41.1

English (New Zealand)

Code tag: en-NZ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.42.1

English (Philippines)

Code tag: en-PH

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.43.1

English (Singapore)

Code tag: en-SG

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.44.1

English (South Africa)

Code tag: en-ZA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.46.1

English (U.S. Virgin Islands)

Code tag: en-VI

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.45.1

English (United Kingdom)

Code tag: en-GB

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.37.1

English (United States)

Code tag: en-US

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.34.1

English (Zimbabwe)

Code tag: en-ZW

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.47.1

Esperanto

Code tag: eo

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.48.1

Estonian

Code tag: et

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.69.1

Faroese

Code tag: fo

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.75.1

Finnish

Code tag: fi

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.74.1

French

Code tag: fr
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.76.1

French (Belgium)
Code tag: fr-BE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.77.1

French (Canada)
Code tag: fr-CA
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.78.1

French (France)
Code tag: fr-FR
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.76.1

French (Luxembourg)
Code tag: fr-LU
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.80.1

French (Switzerland)
Code tag: fr-CH
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.79.1

Galician
Code tag: gl
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.82.1

German
Code tag: de
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.28.1

German (Austria)
Code tag: de-AT
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.29.1

German (Belgium)
Code tag: de-BE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.30.1

German (Germany)
Code tag: de-DE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.28.1

German (Luxembourg)
Code tag: de-LU
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.32.1

German (Switzerland)

Code tag: de-CH
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.31.1

Greek

Code tag: el
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.33.1

Gujarati

Code tag: gu
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.83.1

Hebrew

Code tag: iw
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.85.1

Hindi

Code tag: hi
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.86.1

Hungarian

Code tag: hu
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.88.1

Icelandic

Code tag: is
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.91.1

Indonesian

Code tag: in
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.90.1

Irish

Code tag: ga
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.81.1

Italian

Code tag: it
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.92.1

Italian (Switzerland)

Code tag: it-CH
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.93.1

Japanese

Code tag: ja
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.94.1

Kalaallisut

Code tag: kl
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.95.1

Kannada
Code tag: kn
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.96.1

Konkani
Code tag: kok
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.98.1

Korean
Code tag: ko
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.97.1

Latvian
Code tag: lv
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.101.1

Lithuanian
Code tag: lt
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.100.1

Macedonian
Code tag: mk
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.102.1

Maltese
Code tag: mt
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.104.1

Manx
Code tag: gv
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.84.1

Marathi
Code tag: mr
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.103.1

Norwegian
Code tag: no
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.107.1

Norwegian (Norway)
Code tag: no-NO-NY
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.108.1

Norwegian Bokmål

Code tag: nb
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.110.1

Norwegian Nynorsk
Code tag: nn
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.109.1

Oromo
Code tag: om
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.111.1

Oromo (Ethiopia)
Code tag: om-ET
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.112.1

Oromo (Kenya)
Code tag: om-KE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.113.1

Persian
Code tag: fa
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.71.1

Persian (India)
Code tag: fa-IN
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.72.1

Persian (Iran)
Code tag: fa-IR
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.73.1

Polish
Code tag: pl
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.114.1

Portuguese
Code tag: pt
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.115.1

Portuguese (Brazil)
Code tag: pt-BR
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.116.1

Portuguese (Portugal)
Code tag: pt-PT
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.115.1

Romanian

Code tag: ro

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.117.1

Russian

Code tag: ru

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.118.1

Russian (Russia)

Code tag: ru-RU

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.118.1

Russian (Ukraine)

Code tag: ru-UA

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.119.1

Serbian

Code tag: sr

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.128.1

Serbo-Croatian

Code tag: sh

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.120.1

Slovak

Code tag: sk

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.121.1

Slovenian

Code tag: sl

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.122.1

Somali

Code tag: so

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.123.1

Somali (Djibouti)

Code tag: so-DJ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.124.1

Somali (Ethiopia)

Code tag: so-ET

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.125.1

Somali (Kenya)

Code tag: so-KE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.126.1

Somali (Somalia)

Code tag: so-SO
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.123.1

Spanish
Code tag: es
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.49.1

Spanish (Argentina)
Code tag: es-AR
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.50.1

Spanish (Bolivia)
Code tag: es-BO
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.51.1

Spanish (Chile)
Code tag: es-CL
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.52.1

Spanish (Colombia)
Code tag: es-CO
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.53.1

Spanish (Costa Rica)
Code tag: es-CR
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.54.1

Spanish (Dominican Republic)
Code tag: es-DO
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.55.1

Spanish (Ecuador)
Code tag: es-EC
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.56.1

Spanish (El Salvador)
Code tag: es-SV
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.65.1

Spanish (Guatemala)
Code tag: es-GT
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.57.1

Spanish (Honduras)
Code tag: es-HN
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.58.1

Spanish (Mexico)

Code tag: es-MX
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.59.1

Spanish (Nicaragua)
Code tag: es-NI
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.60.1

Spanish (Panama)
Code tag: es-PA
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.61.1

Spanish (Paraguay)
Code tag: es-PY
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.64.1

Spanish (Peru)
Code tag: es-PE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.62.1

Spanish (Puerto Rico)
Code tag: es-PR
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.63.1

Spanish (Spain)
Code tag: es-ES
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.49.1

Spanish (United States)
Code tag: es-US
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.66.1

Spanish (Uruguay)
Code tag: es-UY
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.67.1

Spanish (Venezuela)
Code tag: es-VE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.68.1

Swahili
Code tag: sw
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.131.1

Swahili (Kenya)
Code tag: sw-KE
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.132.1

Swahili (Tanzania)

Code tag: sw-TZ

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.133.1

Swedish

Code tag: sv

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.129.1

Swedish (Finland)

Code tag: sv-FI

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.130.1

Swedish (Sweden)

Code tag: sv-SE

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.129.1

Tamil

Code tag: ta

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.134.1

Telugu

Code tag: te

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.135.1

Thai

Code tag: th

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.136.1

Tigrinya

Code tag: ti

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.137.1

Tigrinya (Eritrea)

Code tag: ti-ER

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.138.1

Tigrinya (Ethiopia)

Code tag: ti-ET

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.139.1

Turkish

Code tag: tr

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.140.1

Ukrainian

Code tag: uk

Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.141.1

Vietnamese

Code tag: vi
Collation order object identifier: 1.3.6.1.4.1.42.2.27.9.4.142.1

Language Subtypes

- Afrikaans, af

- Albanian, sq

- Amharic, am

- Arabic, ar

- Armenian, hy

- Bangla, bn

- Basque, eu

- Belarusian, be

- Bulgarian, bg

- Catalan, ca

- Chinese, zh

- Cornish, kw

- Croatian, hr

- Czech, cs

- Danish, da

- Dutch, nl

- English, en

- Esperanto, eo

- Estonian, et

- Faroese, fo

- Finnish, fi

- French, fr

- Galician, gl

- German, de

- Greek, el

- Gujarati, gu

- Hebrew, iw

- Hindi, hi

- Hungarian, hu

- Icelandic, is

- Indonesian, in
- Irish, ga
- Italian, it
- Japanese, ja
- Kalaallisut, kl
- Kannada, kn
- Konkani, kok
- Korean, ko
- Latvian, lv
- Lithuanian, lt
- Macedonian, mk
- Maltese, mt
- Manx, gv
- Marathi, mr
- Norwegian, no
- Norwegian Bokmål, nb
- Norwegian Nynorsk, nn
- Oromo, om
- Persian, fa
- Polish, pl
- Portuguese, pt
- Romanian, ro
- Russian, ru
- Serbian, sr
- Serbo-Croatian, sh
- Slovak, sk
- Slovenian, sl
- Somali, so
- Spanish, es
- Swahili, sw
- Swedish, sv
- Tamil, ta
- Telugu, te

- Thai, th

- Tigrinya, ti

- Turkish, tr

- Ukrainian, uk

- Vietnamese, vi

Localization Support

DS software supports localization, but it is not fully localized. Many messages and some tools are available only in English.

Some messages are localized for the following languages:

- Catalan

- French

- German

- Japanese

- Korean

- Polish

- Simplified Chinese

- Spanish

- Traditional Chinese

LDAP Result Codes

An operation result code as defined in RFC 4511 section 4.1.9 is used to indicate the final status of an operation. If a server detects multiple errors for an operation, only one result code is returned. The server should return the result code that best indicates the nature of the error encountered. Servers may return substituted result codes to prevent unauthorized disclosures.

Result Code	Name	Description
-1	Undefined	The result code that should only be used if the actual result code has not yet been determined. Despite not being a standard result code, it is an implementation of the null object design pattern for this type.
0	Success	The result code that indicates that the operation completed successfully.
1	Operations Error	The result code that indicates that the operation is not properly sequenced with relation to other operations (of same or different type). For example, this code is returned if the client attempts to StartTLS [RFC4346] while there are other uncompleted operations or if a TLS layer was already installed.
2	Protocol Error	The result code that indicates that the client sent a malformed or illegal request to the server.
3	Time Limit Exceeded	The result code that indicates that a time limit was exceeded while attempting to process the request.

Result Code	Name	Description
4	Size Limit Exceeded	The result code that indicates that a size limit was exceeded while attempting to process the request.
5	Compare False	The result code that indicates that the attribute value assertion included in a compare request did not match the targeted entry.
6	Compare True	The result code that indicates that the attribute value assertion included in a compare request did match the targeted entry.
7	Authentication Method Not Supported	The result code that indicates that the requested authentication attempt failed because it referenced an invalid SASL mechanism.
8	Strong Authentication Required	The result code that indicates that the requested operation could not be processed because it requires that the client has completed a strong form of authentication.

Result Code	Name	Description
10	Referral	The result code that indicates that a referral was encountered. Strictly speaking this result code should not be exceptional since it is considered as a "success" response. However, referrals should occur rarely in practice and, when they do occur, should not be ignored since the application may believe that a request has succeeded when, in fact, nothing was done.
11	Administrative Limit Exceeded	The result code that indicates that processing on the requested operation could not continue because an administrative limit was exceeded.
12	Unavailable Critical Extension	The result code that indicates that the requested operation failed because it included a critical extension that is unsupported or inappropriate for that request.
13	Confidentiality Required	The result code that indicates that the requested operation could not be processed because it requires confidentiality for the communication between the client and the server.

Result Code	Name	Description
14	SASL Bind in Progress	The result code that should be used for intermediate responses in multi-stage SASL bind operations.
16	No Such Attribute	The result code that indicates that the requested operation failed because it targeted an attribute or attribute value that did not exist in the specified entry.
17	Undefined Attribute Type	The result code that indicates that the requested operation failed because it referenced an attribute that is not defined in the server schema.
18	Inappropriate Matching	The result code that indicates that the requested operation failed because it attempted to perform an inappropriate type of matching against an attribute.
19	Constraint Violation	The result code that indicates that the requested operation failed because it would have violated some constraint defined in the server.

Result Code	Name	Description
20	Attribute or Value Exists	The result code that indicates that the requested operation failed because it would have resulted in a conflict with an existing attribute or attribute value in the target entry.
21	Invalid Attribute Syntax	The result code that indicates that the requested operation failed because it violated the syntax for a specified attribute.
32	No Such Entry	The result code that indicates that the requested operation failed because it referenced an entry that does not exist.
33	Alias Problem	The result code that indicates that the requested operation failed because it attempted to perform an illegal operation on an alias.
34	Invalid DN Syntax	The result code that indicates that the requested operation failed because it would have resulted in an entry with an invalid or malformed DN.
36	Alias Dereferencing Problem	The result code that indicates that a problem was encountered while attempting to dereference an alias for a search operation.

Result Code	Name	Description
48	Inappropriate Authentication	The result code that indicates that an authentication attempt failed because the requested type of authentication was not appropriate for the targeted entry.
49	Invalid Credentials	The result code that indicates that an authentication attempt failed because the user did not provide a valid set of credentials.
50	Insufficient Access Rights	The result code that indicates that the client does not have sufficient permission to perform the requested operation.
51	Busy	The result code that indicates that the server is too busy to process the requested operation. This is a transient error which means the operation can safely be retried.
52	Unavailable	The result code that indicates that either the entire server or one or more required resources were not available for use in processing the request. This is a transient error which means the operation can safely be retried.

Result Code	Name	Description
53	Unwilling to Perform	The result code that indicates that the server is unwilling to perform the requested operation.
54	Loop Detected	The result code that indicates that a referral or chaining loop was detected while processing the request.
60	Sort Control Missing	The result code that indicates that a search request included a VLV request control without a server-side sort control.
61	Offset Range Error	The result code that indicates that a search request included a VLV request control with an invalid offset.
64	Naming Violation	The result code that indicates that the requested operation failed because it would have violated the server's naming configuration.
65	Object Class Violation	The result code that indicates that the requested operation failed because it would have resulted in an entry that violated the server schema.
66	Not Allowed on Non-Leaf	The result code that indicates that the requested operation is not allowed for non-leaf entries.

Result Code	Name	Description
67	Not Allowed on RDN	The result code that indicates that the requested operation is not allowed on an RDN attribute.
68	Entry Already Exists	The result code that indicates that the requested operation failed because it would have resulted in an entry that conflicts with an entry that already exists.
69	Object Class Modifications Prohibited	The result code that indicates that the operation could not be processed because it would have modified the objectclasses associated with an entry in an illegal manner.
71	Affects Multiple DSAs	The result code that indicates that the operation could not be processed because it would impact multiple DSAs or other repositories.
76	Virtual List View Error	The result code that indicates that the operation could not be processed because there was an error while processing the virtual list view control.
80	Other	The result code that should be used if no other result code is appropriate.

Result Code	Name	Description
81	Server Connection Closed	The client-side result code that indicates that the server is down. This is for client-side use only and should never be transferred over protocol. This is a transient error which means the operation can be retried.
82	Local Error	The client-side result code that indicates that a local error occurred that had nothing to do with interaction with the server. This is for client-side use only and should never be transferred over protocol.
83	Encoding Error	The client-side result code that indicates that an error occurred while encoding a request to send to the server. This is for client-side use only and should never be transferred over protocol.
84	Decoding Error	The client-side result code that indicates that an error occurred while decoding a response from the server. This is for client-side use only and should never be transferred over protocol.

Result Code	Name	Description
85	Client-Side Timeout	The client-side result code that indicates that the client did not receive an expected response in a timely manner. This is for client-side use only and should never be transferred over protocol. This is a transient error which means the operation can be retried.
86	Unknown Authentication Mechanism	The client-side result code that indicates that the user requested an unknown or unsupported authentication mechanism. This is for client-side use only and should never be transferred over protocol.
87	Filter Error	The client-side result code that indicates that the filter provided by the user was malformed and could not be parsed. This is for client-side use only and should never be transferred over protocol.
88	Cancelled by User	The client-side result code that indicates that the user cancelled an operation. This is for client-side use only and should never be transferred over protocol.

Result Code	Name	Description
89	Parameter Error	The client-side result code that indicates that there was a problem with one or more of the parameters provided by the user. This is for client-side use only and should never be transferred over protocol.
90	Out of Memory	The client-side result code that indicates that the client application was not able to allocate enough memory for the requested operation. This is for client-side use only and should never be transferred over protocol.
91	Connect Error	The client-side result code that indicates that the client was not able to establish a connection to the server. This is for client-side use only and should never be transferred over protocol. This is a transient error which means the operation can be retried.
92	Operation Not Supported	The client-side result code that indicates that the user requested an operation that is not supported. This is for client-side use only and should never be transferred over protocol.

Result Code	Name	Description
93	Control Not Found	The client-side result code that indicates that the client expected a control to be present in the response from the server but it was not included. This is for client-side use only and should never be transferred over protocol.
94	No Results Returned	The client-side result code that indicates that the requested single entry search operation or read operation failed because the Directory Server did not return any matching entries. This is for client-side use only and should never be transferred over protocol.
95	Unexpected Results Returned	The client-side result code that the requested single entry search operation or read operation failed because the Directory Server returned multiple matching entries (or search references) when only a single matching entry was expected. This is for client-side use only and should never be transferred over protocol.

Result Code	Name	Description
96	Referral Loop Detected	The client-side result code that indicates that the client detected a referral loop caused by servers referencing each other in a circular manner. This is for client-side use only and should never be transferred over protocol.
97	Referral Hop Limit Exceeded	The client-side result code that indicates that the client reached the maximum number of hops allowed when attempting to follow a referral (i.e., following one referral resulted in another referral which resulted in another referral and so on). This is for client-side use only and should never be transferred over protocol.
118	Canceled	The result code that indicates that a request has been cancelled by a cancel request.
119	No Such Operation	The result code that indicates that a cancel request was unsuccessful because the targeted operation did not exist or had already completed.

Result Code	Name	Description
120	Too Late	The result code that indicates that a cancel request was unsuccessful because processing on the targeted operation had already reached a point at which it could not be canceled.
121	Cannot Cancel	The result code that indicates that a cancel request was unsuccessful because the targeted operation was one that could not be canceled.
122	Assertion Failed	The result code that indicates that the filter contained in an assertion control failed to match the target entry.
123	Authorization Denied	The result code that should be used if the server will not allow the client to use the requested authorization.
16,654	No Operation	The result code that should be used if the server did not actually complete processing on the associated operation because the request included the LDAP No-Op control.

Was this helpful? 👍 👎