

## *LDAP Search Command Examples*

*Command:*

```
ldapsearch -x -LLL -H ldap://server.example.com -b "dc=example,dc=com"
"(uid=john.doe)" cn mail
```

*Explanation:*

*Search for the user with UID 'john.doe' and return their common name (cn) and email (mail).*

*Command:*

```
ldapsearch -x -H ldap://server.example.com -b "ou=users,dc=example,dc=com"
"(&(objectClass=person)(|(uid=john.doe)(uid=jane.doe)))"
```

*Explanation:*

*Search for entries where the object class is 'person' and the UID is either 'john.doe' or 'jane.doe'.*

*Command:*

```
ldapsearch -x -H ldap://server.example.com -b "dc=example,dc=com" -l 10
"(objectClass=*)"
```

*Explanation:*

*Search for all objects with a time limit of 10 seconds.*

*Command:*

```
ldapsearch -x -ZZ -H ldaps://server.example.com -b "dc=example,dc=com"
"(uid=john.doe)"
```

*Explanation:*

*Use SSL/TLS for security and search for user with UID 'john.doe'.*

*Command:*

```
ldapsearch -x -E pr=1000/noprompt -H ldap://server.example.com -b
"dc=example,dc=com"
"(objectClass=person)"
```

*Explanation:*

*Use simple paging of the results, retrieving 1000 entries at a time without prompting.*

*Command:*

```
ldapsearch -x -LLL -H ldap://server.example.com -b "dc=example,dc=com"
"(uid=john.doe)" +
```

*Explanation:*

*Retrieve operational attributes for the entries along with common name and email.*

*Command:*

```
ldapsearch -Y DIGEST-MD5 -U username -H ldap://server.example.com -b
"dc=example,dc=com"
"(objectClass=*)"
```

*Explanation:*

*Use SASL DIGEST-MD5 mechanism for authentication.*

*Command:*

```
ldapsearch -x -H ldap://server.example.com -b "dc=example,dc=com" "(objectClass=*)"
cn mail -s sub -A
```

*Explanation:*

*Fetch all attributes except 'cn' and 'mail' for entries.*

*Command:*

```
ldapsearch -x -H ldap://server.example.com -b "dc=example,dc=com" -l 30 -z 500
"(objectClass=person)"
```

*Explanation:*

*Set a time limit of 30 seconds and a maximum return size of 500 entries.*

*Command:*

```
ldapsearch -x -E '1.2.840.113556.1.4.319' -H ldap://server.example.com -b
"dc=example,dc=com"
"(objectClass=*)"
```

*Explanation:*

*Utilize the LDAP control with the specified OID.*

## **LDAP Connection and Authentication Arguments**

- **-h {host} / --hostname {host}** — The IP address or resolvable name to use to connect to the directory server. If this is not provided, then a default value of 'localhost' will be used.
- **-p {port} / --port {port}** — The port to use to connect to the directory server. If this is not provided, then a default value of 389 will be used.  
The specified value must not be less than 1 or greater than 65,535.
- **-D {dn} / --bindDN {dn}** — The DN to use to bind to the directory server when performing simple authentication.  
A provided value must be able to be parsed as an LDAP distinguished name as described in RFC 4514.
- **-w {password} / --bindPassword {password}** — The password to use to bind to the directory server when performing simple authentication or a password-based SASL mechanism.
- **-j {path} / --bindPasswordFile {path}** — The path to the file containing the password to use to bind to the directory server when performing simple authentication or a password-based SASL mechanism.  
The specified path must refer to a file that exists.
- **--promptForBindPassword** — Indicates that the tool should interactively prompt the user for the bind password.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- **-Z / --useSSL** — Use SSL when communicating with the directory server.  
This argument is not allowed to have a value. If this argument is included in a set

of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `-q / --useStartTLS` — Use StartTLS when communicating with the directory server.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--defaultTrust` — Use the JVM's default trust store, and optionally an additional trust store specified using the `--trustStorePath` argument, to non-interactively determine whether to trust any certificate chain presented during TLS negotiation. If the chain cannot be trusted based on any of those sources, then negotiation will fail without prompting about whether to trust it.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `-X / --trustAll` — Trust any certificate presented by the directory server.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `-K {path} / --keyStorePath {path}` — The path to the file to use as the key store for obtaining client certificates when communicating securely with the directory server.

- `-W {password} / --keyStorePassword {password}` — The password to use to access the key store contents.

- `-u {path} / --keyStorePasswordFile {path}` — The path to the file containing the password to use to access the key store contents.

The specified path must refer to a file that may or may not exist.

- `--promptForKeyStorePassword` — Indicates that the tool should interactively prompt the user for the password to use to access the key store contents.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--keyStoreFormat {format}` — The format (e.g., JKS, PKCS12, PKCS11, BCFKS, etc.) for the key store file.

- `-P {path} / --trustStorePath {path}` — The path to the file to use as trust store when determining whether to trust a certificate presented by the directory server.

- `--trustStorePassword {password}` — The password to use to access the trust store contents.

- `-U {path} / --trustStorePasswordFile {path}` — The path to the file containing the password to use to access the trust store contents.

The specified path must refer to a file that may or may not exist.

- `--promptForTrustStorePassword` — Indicates that the tool should interactively prompt the user for the password to use to access the trust store contents.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--trustStoreFormat {format}` — The format (e.g., JKS, PKCS12, PKCS11, BCFKS, etc.) for the trust store file.
- `--verifyCertificateHostnames` — Indicates that the tool should verify that the hostname or IP address used to establish connections to the LDAP server matches an address for which the server's TLS certificate was issued. This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-N {nickname} / --certNickname {nickname}` — The nickname (alias) of the client certificate in the key store to present to the directory server for SSL client authentication.
- `--enableSSLDebugging` — Enable Java's low-level support for debugging SSL/TLS communication. This is equivalent to setting the 'javax.net.debug' property to 'all'. This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-o {name=value} / --saslOption {name=value}` — A name-value pair providing information to use when performing SASL authentication.
- `--useSASLExternal` — Use the SASL EXTERNAL mechanism to authenticate. This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--helpSASL` — Provide information about the supported SASL mechanisms, including the properties available for use with each. This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

### Operation Arguments

- `-b {dn} / --baseDN {dn}` — Specifies the base DN that should be used for the search. If a filter file is provided, then this base DN will be used for each search with a filter read from that file. This argument must not be provided if the `--ldapURLFile` is given. If no base DN is specified, then the null base DN will be used by default. A provided value must be able to be parsed as an LDAP distinguished name as described in RFC 4514.
- `-s {base|one|sub|subordinates} / --scope {base|one|sub|subordinates}` — Specifies the scope that to use for search requests. The value should be one of 'base', 'one', 'sub', or 'subordinates'. If this argument is not provided, a default of 'sub' will be used. The provided value should be one of 'base', 'one', 'sub', or 'subordinate'.
- `-z {value} / --sizeLimit {value}` — Specifies the maximum number of entries that the server should return for each search. A value of zero (which is the default if this argument is not used) indicates that no client-side size limit should be imposed. Note that the server may impose its own limit on the number of entries that may be returned for a search. The specified value must not be less than 0 or greater than 2,147,483,647.

- `-l {value} / --timeLimitSeconds {value}` — Specifies the maximum length of time in seconds that the server should spend processing each search. A value of zero (which is the default if this argument is not provided) indicates that no client-side time limit should be imposed. Note that the server may impose its own time limit for search requests.

The specified value must not be less than 0 or greater than 2,147,483,647.

- `-a {never|always|search|find} / --dereferencePolicy {never|always|search|find}` — Specifies the alias dereferencing policy to use for search requests. The value should be one of 'never', 'always', 'search', or 'find'. If this argument is not provided, a default of 'never' will be used.

A provided value should be one of the following: 'always', 'never', 'search', 'find'.

- `-A / --typesOnly` — Indicates that the server should only include the names of the attributes contained in the entry rather than both names and values.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--requestedAttribute {attr}` — Specifies an identifier that indicates which attribute(s) should be included in entries that match the search criteria. The value may be an attribute name or OID, a special token like '\*' to indicate all user attributes or '+' to indicate all operational attributes, or an object class name prefixed by an '@' symbol to indicate all attributes associated with the specified object class. This may be provided multiple times to specify multiple requested attributes, and it may be provided instead of or in addition to the set of requested attributes in the set of trailing arguments. If this is not specified, then the server will behave as if all user attributes had been requested.

- `--filter {filter}` — Specifies a filter to use when processing a search. This may be provided multiple times to issue multiple searches with different filters. If this argument is provided, then the first trailing argument will not be interpreted as a search filter (all trailing arguments will be interpreted as requested attributes). A provided value must be able to be parsed as an LDAP search filter as described in RFC 4515.

- `-f {path} / --filterFile {path}` — Specifies the path to a file containing the search filters to issue. Each filter should be on a separate line. Blank lines and lines beginning with the '#' character will be ignored. This argument may be provided multiple times to specify multiple filter files. If a filter file is provided, then the first trailing argument will not be interpreted as a search filter (all trailing arguments will be interpreted as requested attributes).

The specified path must refer to a file that exists.

- `--ldapURLFile {path}` — Specifies the path to a file containing LDAP URLs that define the search requests to issue. The LDAP URLs will specify the base DN, scope, filter, and attributes to return for each search (any hostnames and port numbers included in the URLs will be ignored). Each URL should be on a separate line. Blank lines and lines beginning with the '#' character will be ignored. This argument may be provided multiple times to specify multiple LDAP URL files.

The specified path must refer to a file that exists.

- `--followReferrals` — Attempt to follow any referrals and search result references encountered during search processing. If this is not provided, then referrals and search references will be displayed in the output.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--retryFailedOperations` — Indicates that, if a search fails in a way that indicates the connection to the server may no longer be valid, the tool should automatically create a new connection and re-try the search before reporting it as a failure.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-c / --continueOnError` — Continue processing searches even if an error is encountered. If this is not provided, then processing will abort after the first failed search.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-r {num} / --ratePerSecond {num}` — Specifies a maximum search rate that the tool should be permitted to achieve. Note that this limit applies only to the rate at which the client issues search requests and not to the rate at which the server may send matching entries.  
The specified value must not be less than 1 or greater than 2,147,483,647.
- `--useAdministrativeSession` — Indicates that the tool should attempt to use an administrative session to process all operations using a dedicated pool of worker threads. This may be useful when trying to diagnose problems in a server that is unresponsive because all normal worker threads are busy processing other requests.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-n / --dryRun` — Indicate which searches would be issued but do not actually send them to the server.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--countEntries` — Indicates that the tool exit code should represent the number of entries returned during search processing. If this is not provided, or if an error is encountered while processing the search, then the tool exit code will reflect the LDAP result code received during search processing (or an appropriate client-side result code if a problem was encountered before sending any searches). Note that because some operating systems do not allow exit code values greater than 255, that will be the maximum exit value for this tool even if more than 255 entries are returned. Also note that this argument can only be used when processing a single search.  
This argument is not allowed to have a value. If this argument is included in a set

of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

## Data Arguments

- `--wrapColumn {value}` — The column at which long lines in the LDIF representation of an entry should be wrapped. A value of zero indicates that no wrapping should be performed. If this is not provided, then the wrap column will be based on the width of the terminal used to run the tool.  
The specified value must not be less than 0 or greater than 2,147,483,647.
- `-T / --dontWrap` — Indicates that no line wrapping should be performed when displaying the LDIF representations of matching entries.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--suppressBase64EncodedValueComments` — Indicates that the tool should not include any comments that attempt to provide a human-readable representation of any base64-encoded attribute values in the search results. If this argument is not provided, then any attribute value whose LDIF representation requires base64 encoding will be immediately followed by a comment that attempts to provide a human-readable representation of the raw bytes that comprise that base64-encoded value.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--outputFile {path}` — Specifies the path to the file to which search results should be written. If this argument is not provided then results will be written to standard output.  
The specified path must refer to a file which may or may not exist, but whose parent directory must exist.
- `--compressOutput` — Indicates that the output should be gzip-compressed. This can only be used if the `--outputFile` argument is provided and the `--teeResultsToStandardOut` argument is not provided.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--encryptOutput` — Indicates that the output should be encrypted with a key generated from a provided password. This can only be used if the `--outputFile` argument is provided and the `--teeResultsToStandardOut` argument is not provided. If the `--encryptionPassphraseFile` argument is provided, then that file will be used to specify the encryption passphrase; otherwise, the passphrase will be interactively requested.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--encryptionPassphraseFile {path}` — The path to a file that specifies the passphrase to use to encrypt the output. This can only be provided if the `--encryptOutput` argument is given, but if that argument is given and no passphrase file is specified, then the passphrase will be interactively requested.

If a file is specified, then that file must exist and must contain exactly one line comprised entirely of the passphrase.

The specified path must refer to a file that exists.

- `--separateOutputFilePerSearch` — Indicates that the tool should generate a separate output file for each search rather than combining all results into a single file.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--teeResultsToStandardOut` — Indicates that search results should be written to standard output as well as to the output file specified via the 'outputFile' argument.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--outputFormat {ldif|json|csv|multi-valued-csv|tab-delimited|multi-valued-tab-delimited|dns-only|values-only}` — Specifies the format that should be used for the output generated by this tool. Allowed values are 'LDIF' (LDAP Data Interchange Format, which is the standard string representation for LDAP data), 'JSON' (JavaScript Object Notation, which is a popular format used by web services), 'CSV' (comma-separated values, which is a commonly used format for text processing, with only a single value per attribute), 'multi-valued-csv' (comma-separated values with a vertical bar between values of multivalued attributes), 'tab-delimited' (another commonly used general text format, with only a single value per attribute), 'multi-valued-tab-delimited' (tab-delimited text with a vertical bar between values of multivalued attributes), 'dns-only' (in which only the DN of each matching entry will be written on a line by itself with no information about the entry's attributes), and 'values-only' (in which each value returned will be written on a line by itself with no attribute names, entry DNs, or delimiters between entries). If either the 'CSV' or 'tab-delimited' format is selected (or one of their multivalued variants), the set of requested attributes must be provided with the '--requestedAttribute' argument, the order in which the attributes are provided on the command line specifies the order in which they will be listed in the output, and if any of those attributes has multiple values then only the first value will be used. Further, the 'CSV' and 'tab-delimited' formats cannot be used in conjunction with the '--ldapURLFile' argument. If no output format is specified, a default of 'LDIF' will be used.

A provided value should be one of the following: 'values-only', 'multi-valued-csv', 'tab-delimited', 'ldif', 'csv', 'multi-valued-tab-delimited', 'json', 'dns-only'.

- `--requireMatch` — Indicates that `ldapsearch` should exit with a nonzero result code, 94 (no results returned), if the search completes successfully but does not return any matching entries. This argument only affects the tool exit code; it will not have any visible effect on the output.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.



- `--terse` — Indicates that the tool should generate terse output. The only thing written to standard output will be search result entries and references, without any summary messages. Standard error will not be affected.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-v / --verbose` — Indicates that the tool should generate verbose output.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

### Control Arguments

- `--bindControl {oid}[:{criticality}]{stringValue}[:{base64Value}]` — Specifies a control that should be included in all bind requests used to authenticate to the server.  
A provided value must be a string representation of a valid LDAP control in the form `{oid}[:{criticality}]{stringValue}[:{base64Value}]`.
- `-J {oid}[:{criticality}]{stringValue}[:{base64Value}] / --control {oid}[:{criticality}]{stringValue}[:{base64Value}]` — Specifies a control that should be included in all search requests sent to the server.  
A provided value must be a string representation of a valid LDAP control in the form `{oid}[:{criticality}]{stringValue}[:{base64Value}]`.
- `--accessLogField {name:value}` — Indicates that all search requests should include an access log field request control to indicate that the server should include a custom field with the specified name and value. The field name must contain only ASCII letters, digits, dashes, and underscores. The field name must be followed by a colon and the field value for that field. This argument may be provided multiple times to request multiple access log fields.
- `--accountUsable` — Indicates that all search requests should include the UnboundID-proprietary account usable request control to request that each search result entry returned include a response control with information about the password policy usability state for the entry.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-E / --authorizationIdentity` — Indicates that all bind requests should include the authorization identity request control as defined in RFC 3829. With this control, a successful bind result should include the authorization identity assigned to the connection.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--assertionFilter {filter}` — A filter that will be used in conjunction with the LDAP assertion request control (as described in RFC 4528) to indicate that the server should only process searches in which the entry specified as the base DN matches this filter.  
A provided value must be able to be parsed as an LDAP search filter as described in RFC 4515.

- `--excludeBranch {dn}` — Indicates that all search requests should include the UnboundID-proprietary exclude branch request control to indicate that matching entries below the specified base DN should be excluded from search results. This argument may be provided multiple times if multiple branches should be excluded.  
A provided value must be able to be parsed as an LDAP distinguished name as described in RFC 4514.
- `--generateAccessToken` — Indicates that the bind request should include the generate access token request control, which may be used to request that the server generate and return an access token that can be used to authorize subsequent connections via the OAUTHBEARER SASL mechanism.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--getAuthorizationEntryAttribute {attr}` — Indicates that all bind requests should include the UnboundID-proprietary get authorization entry request control to request that the server return the specified attribute (or collection of attributes, in the case of a special identifier like '\*' to indicate all user attributes or '+' to indicate all operational attributes) from the authenticated user's entry. This argument may be provided multiple times to specify multiple attributes to request.
- `--getBackendSetID` — Indicates that all search requests should include the UnboundID-proprietary get backend set ID request control to request that the Directory Proxy Server include a corresponding get backend set ID response control in each search result entry, indicating the entry-balancing backend set from which that entry was retrieved.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-g {authzID} / --getEffectiveRightsAuthzID {authzID}` — Indicates that all search requests should include the UnboundID-proprietary get effective rights request control to return information about the access control rights the specified user has when interacting with each matching entry.
- `-e {attr} / --getEffectiveRightsAttribute {attr}` — Indicates that all search requests should include the UnboundID-proprietary get effective rights request control to return information about the access control rights that a user has when interacting with each matching entry. This argument may be provided multiple times to specify multiple attributes.
- `--getRecentLoginHistory` — Indicates that all bind requests should include the get recent login history request control to request that the server include a corresponding response control with information about the user's recent login history.  
This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `--getServerID` — Indicates that all search requests should include the UnboundID-proprietary get server ID request control to request that server

include a corresponding get server ID response control in each search result entry, indicating the server from which that entry was retrieved.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--getUserResourceLimits` — Indicates that all bind requests should include the UnboundID-proprietary get user resource limits request control to request that the server return information about resource limits (e.g., size limit, time limit, idle time limit, etc.) imposed for the user.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--includeReplicationConflictEntries` — Indicates that all search requests should include the UnboundID-proprietary return conflict entries request control to indicate that the server may return any replication conflict entries that match the search criteria. Replication conflict entries are normally excluded from search results.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--includeSoftDeletedEntries {with-non-deleted-entries|without-non-deleted-entries|deleted-entries-in-undeleted-form}` — Indicates that all search requests should include the UnboundID-proprietary soft-deleted entry access request control to indicate that the server may return any soft-deleted entries that match the search criteria. Soft-deleted entries are normally excluded from search results. The value for this argument must be one of: 'with-non-deleted-entries' (indicates that both regular and soft-deleted entries should be returned), 'without-non-deleted-entries' (indicates that only soft-deleted entries should be returned), or 'deleted-entries-in-undeleted-form' (returns only soft-deleted entries in the form in the form the entries had before they were deleted).

A provided value should be one of the following: 'with-non-deleted-entries', 'deleted-entries-in-undeleted-form', 'without-non-deleted-entries'.

- `--draftLDUPSubentries` — Indicates that all search requests should include the subentries request control as described in draft-ietf-ldup-subentry to indicate that the server may return any LDAP subentries that match the search criteria. LDAP subentries are normally excluded from search results. This control does not take a value.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--rfc3672Subentries {returnOnlySubentries}` — Indicates that all search requests should include the subentries request control as described in RFC 3672 to indicate that the server may return any LDAP subentries that match the search criteria, optionally including regular entries along with the subentries. LDAP subentries are normally excluded from search results. This control requires a Boolean value of either 'true' or 'false' to indicate whether the server should

return only subentries (if true), or both regular entries and subentries (if false).  
A provided value should be either 'true' or 'false'.

- `--joinRule {dn:sourceAttr|reverse-dn:targetAttr|equals:sourceAttr:targetAttr|contains:sourceAttr:targetAttr}` — Indicates that all search requests should include the join request control to indicate that matching entries should be joined with related entries based on the specified criteria. Allowed values include 'dn:' followed by the name of an attribute in the source entry containing the DNs of the entries with which to join; 'reverse-dn:' followed by the name of an attribute in the target entries whose value is the DN of the source entry; 'equals:' followed by the name of an attribute in the source entry, a colon, and the name of an attribute in target entries that must exactly match the source attribute; or 'contains:' followed by the name of an attribute in the source entry, a colon, and the name of an attribute in target entries that must match or contain the value of the source attribute.
- `--joinBaseDN {search-base|source-entry-dn|{dn}}` — Specifies the base DN to use for searches used to join search result entries with related entries. The value may be one of 'search-base' to use the base DN of the search request, 'source-entry-dn' to use the DN of the source entry as the base DN for join searches, or any valid LDAP DN to use a custom base DN for join searches. If this is not specified, then the default join base DN will be the search base DN.
- `--joinScope {base|one|sub|subordinates}` — Specifies the scope to use for searches used to join search result entries with related entries. The value may be one of 'base', 'one', 'sub', or 'subordinates'. If this is not specified, then the scope of the search request will be used as the join scope.  
The provided value should be one of 'base', 'one', 'sub', or 'subordinate'.
- `--joinSizeLimit {num}` — Specifies the maximum number of entries that the server will permit to be joined with any single search result entry. If this is not provided, the size limit from the search request will be used. Note that the server will impose a maximum join size limit of 1000 entries, so any join size limit greater than that will be limited to 1000.  
The specified value must not be less than 0 or greater than 2,147,483,647.
- `--joinFilter {filter}` — Specifies an additional filter that the server will require target entries to match in order to be joined with the source entry. If this is not provided, no additional join filter will be used.  
A provided value must be able to be parsed as an LDAP search filter as described in RFC 4515.
- `--joinRequestedAttribute {attr}` — Specifies an identifier that indicates which attribute(s) should be included in entries joined with search result entries. The value may be an attribute name or OID, a special token like '\*' to indicate all user attributes or '+' to indicate all operational attributes, or an object class name prefixed by an '@' symbol to indicate all attributes associated with the specified object class. This may be provided multiple times to specify multiple requested attributes. If this is not specified, then the server will behave as if all user attributes had been requested.
- `--joinRequireMatch` — Indicates that the server should not return an entry that matches the search criteria if it is not joined with at least one additional entry. If this is not provided, then entries matching the search criteria will be returned

even if they are not joined with any other entries.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--manageDsaIT` — Indicates that all search requests should include the `manageDsaIT` request control to indicate that any referral entries in the scope of the search should be treated as regular entries rather than causing the server to send search result references.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--matchedValuesFilter {filter}` — Indicates that all search requests should include the matched values request control (as described in RFC 3876) to indicate that search result entries should only include values for a given attribute that match the provided filter. This argument may be provided multiple times to specify multiple matched values filters.

A provided value must be able to be parsed as an LDAP search filter as described in RFC 4515.

- `--matchingEntryCountControl {examineCount=NNN[:alwaysExamine][:allowUnindexed][:skipResolvingExplodedIndexes][:fastShortCircuitThreshold=NNN][:slowShortCircuitThreshold=NNN][:extendedResponseData][:debug]}` — Indicates that all search requests should include the UnboundID-proprietary matching entry count request control, which indicates that the server should return information about the number of entries that match the search criteria. The maximum number of entries to examine must be specified, which helps indicate whether an exact count or an estimate will be returned. If `alwaysExamine` is specified and the number of candidates is less than the examine count, then each candidate will be examined to verify that it matches the criteria and would actually be returned to the client in a search. If `allowUnindexed` is specified, then the count will be allowed to be processed even if the search is unindexed (and may take a very long time to complete). If `extended` is specified, then the client will request extended response data from the server. If `debug` is specified, then additional debug information may be included in the output.
- `--operationPurpose {purpose}` — Indicates that all search requests should include the UnboundID-proprietary operation purpose request control to provide the specified reason for the operation.
- `--overrideSearchLimit {name=value}` — Indicates that search operations should include the override search limits request control with the specified name-value pair. This may be provided multiple times to specify multiple property name-value pairs to include in the control.
- `-C ps[:changetype[:changesonly[:entrychgcontrols]]] / --persistentSearch ps[:changetype[:changesonly[:entrychgcontrols]]]` — Indicates that the search request should include the persistent search request control (as described in draft-ietf-ldapext-psearch) to indicate that the server should return information about changes to entries that match the search criteria as they are

processed. This argument may only be used when processing a single search operation.

- `--permitUnindexedSearch` — Indicates that all search requests should include the UnboundID-proprietary permit unindexed search request control to indicate that the server should process the search operation even if it cannot do so efficiently using server indexes. The requester must have either the unindexed-search or unindexed-search-with-control privilege.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `-Y {authzID} / --proxyAs {authzID}` — Indicates that all search requests should include the proxied authorization request control (as described in RFC 4370) to process the operation under an alternate authorization identity. The authorization ID should generally be specified in the form 'dn:' followed by the target user's DN, or 'u:' followed by the username.

- `--proxyV1As {dn}` — Indicates that all search requests should include the legacy proxied authorization v1 request control (as described in draft-weltman-ldapv3-proxy-04) to process the search under an alternate authorization identity, specified as the DN of the desired user.

A provided value must be able to be parsed as an LDAP distinguished name as described in RFC 4514.

- `--rejectUnindexedSearch` — Indicates that all search requests should include the UnboundID-proprietary reject unindexed search request control to indicate that the server should not process the search operation if it cannot do so efficiently using server indexes, even if the requester has the unindexed-search privilege. This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--routeToBackendSet {entry-balancing-processor-id:backend-set-id}` — Specifies the ID of an entry-balancing backend set to which the Directory Proxy Server should send all of the search requests. The value should be formatted as the entry-balancing request processor ID followed by a colon and the desired backend set ID for that entry-balancing request processor. This argument can be provided multiple times to specify multiple backend set IDs for the same or different entry-balancing request processors. The request control will be configured to use absolute routing rather than a routing hint.

- `--routeToServer {id}` — Specifies the ID of the backend server to which the Directory Proxy Server should send all search requests.

- `--suppressOperationalAttributeUpdates {attr}` — Indicates that all operations should include the UnboundID-proprietary suppress operational attribute updates request control to indicate that the server should not apply any updates to the specified operational attributes. The value may be one of 'last-access-time', 'last-login-time', 'last-login-ip', or 'lastmod'.

A provided value should be one of the following: 'last-access-time', 'last-login-ip', 'last-login-time', 'lastmod'.

- `--usePasswordPolicyControl` — Indicates that bind requests should include the password policy request control (as defined in draft-behera-ldap-password-

policy-10) to request that the response include password policy-related information about the target entry.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.

- `--realAttributesOnly` — Indicates that all search requests should include the UnboundID-proprietary real attributes only request control to indicate that the server should not include any virtual attributes in entries that are returned. This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-S {value} / --sortOrder {value}` — Indicates that all search requests should include the server-side sort request control (as described in RFC 2891) to request that the server sort results before returning them to the client. The sort order should be a comma-separated list of attribute names, each of which may be optionally prefixed by '+' (to indicate that sorting should be in ascending order for that attribute) or '-' (for descending order), and may be optionally followed by a colon and the name or OID for the ordering matching rule that should be used when sorting. Ascending order will be used if neither '+' or '-' is specified, and if no matching rule ID is given then the attribute type's own ordering rule will be used.
- `--simplePageSize {value}` — Indicates that all search requests should include the simple paged results control (as described in RFC 2696) to indicate that the search should return entries in pages of no more than the specified size. This can be useful for searches that must return a large number of entries but the server restricts the number of entries that may be returned for any search. The specified value must not be less than 1 or greater than 2,147,483,647.
- `--virtualAttributesOnly` — Indicates that all search requests should include the UnboundID-proprietary virtual attributes only request control to indicate that the server should only include virtual attributes in entries that are returned. This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
- `-G {before:after:index:count | before:after:value} / --virtualListView {before:after:index:count | before:after:value}` — Indicates that all search requests should include the virtual list view (VLV) request control (as described in draft-ietf-ldapext-ldapv3-vlv) to indicate that the server should return the specified subset of the sorted search results (and the 'sortOrder' argument must also be given to specify the sort order). The value should be a colon-delimited list indicating which page of results to return, and it may take one of two forms. In either case, the first element specifies the number of elements to return before the entry identified as the start of the results, and the second is the number of entries after the 'start' entry. The third element identifies the start of the result set, and it may be either an integer offset (in which the first entry in the result set has an offset of one), or a string that provides a value for which the server should identify the first entry whose value for the primary sort attribute is greater than or equal to the given string. In the event that an offset is

provided, a fourth element must also be given to indicate the expected number of entries in the result set, or zero if that is not known. For example, a value of '0:9:1:0' indicates that the server should return the first ten entries of the result set (starting at offset 1, which is the first entry, return the zero previous entries and the nine following entries, with no indication of how many entries match the search criteria). Alternately, a value of '0:99:smith' indicates that the server should the first 100 entries in the result set for which the primary sort attribute has a value that is greater than or equal to 'smith'.

- `--useJSONFormattedRequestControls` — Indicates that any request controls should be encapsulated in a JSON-formatted request control. Even if there wouldn't otherwise be any request controls, an empty JSON-formatted request control will be included to indicate that the server should encapsulate any response controls in a JSON-formatted response control.

This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.