

# LDAPQueryAnalyzer – Manual

LDAPQueryAnalyzer – Manual	1
LDAPQueryAnalyzer	5
Fields	5
Domains	5
DCs	5
NCs	6
Base	6
Filter	6
Attributes	6
ASQ Attributes	6
Results	6
Controls	7
History	7
Port	8
LDAP	8
GC	8
Custom	8
BaseType	8
DN	8
PhantomRoot	8
rootDSE	8
operational attributes	8
Scope	8
Base	8
OneLevel	8
SubTree	8
Referrals	8
None	8
External	8
Subordinate	9
Query type	9
Paged	9
Non-Paged	9
Attributes	9
AttributeScoped	9
Sorted	9
Return	9
Results	9
	1

Statistics	9
Search	10
Cancel	10
Query	10
All	10
Restore	10
Menus	11
File	11
Close	11
User	11
WhoAml	11
Restart elevated	11
Run elevated (2nd instance)	11
Restart as	11
Restart as elevated	11
Run as (2nd instance)	11
Run as elevated (2nd instance)	12
Connection	12
Refresh Forest	12
Set Ports	12
LDAP	12
GC	12
Set Timeout (s)	12
Connect Forest	12
Pass Credentials	12
Query	12
Browse (Base)	12
Execute Query	13
Provider	13
LDAP	13
GC	13
Base type	13
DN	13
PhantomRoot	13
rootDSE	13
Query type	13
Paged	13
Non-Paged	14
SearchScope	14
Base	14

OneLevel	14
SubTree	14
Return	14
Results	14
Statistics	14
operational attributes	14
Autoswitch to PagedQuery	14
Value Range Retrieval	15
Attribute Scoped Query	15
Show deleted	15
Show recycled	15
Sort results ascending (client side)	15
Sort results descending (client side)	15
Attribute Scoped Query	15
Sorted Query (server side)	15
Filter	15
Filter Wizard	15
Clear Filter History	15
Attributes	15
Load Attribute List from Schema	15
Hide Attribute List	15
Decode	16
GUIDs	16
SIDs	16
userParameters	16
Resolve Sids	16
SecurityDescriptors	16
OctetStrings	16
ReplicaLinks	16
memberOf includes primaryGroupID	16
To local time	16
Results	16
Copy selected	16
Copy all	16
Remembered results	16
Show first	16
Show previous	16
Show next	16
Show current	16
Clear list	17

Clear Output Clear current result pane.	17
Change Font	17
Tools	17
DynamicTypeBuilder	17
FilterWizard	17
Fields	17
Filter	17
ObjectClasses	17
Attributes	18
Value	19
Controls	19
Open AND group (&	19
Open OR group (	19
Close current group )	19
Close all groups ))	19
UnDo	19
Clear	19
Apply	20
ObjectClasses	20
Equals =	20
Not Equals !=	20
Attributes	20
Equals =	20
Not Equals !=	20
Less or Equals <=	20
Greater or Equals >=	20
Bitwise OR	20
Not Bitwise AND !&	20
Not Bitwise Or !	21
Match in Chain ->>	21
isGuid	21
DynamicTypeBuilder	22
Disclaimer	25

## LDAPQueryAnalyzer

LDAPQueryAnalyzer (MFP-LABS\theboss)

File User Connection Query Filter Attributes Decode Results Tools

ConnectionInfo (mfp-labs.labsetup.org)

Domains: DC=mfp-labs.DC=labsetup.DC=org

DCs: dc1root.mfp-labs.labsetup.org

NCs: DC=mfp-labs.DC=labsetup.DC=org

Load: [Progress Bar]

Query

Base: DC=mfp-labs.DC=labsetup.DC=org

Filter: (& (objectClass=user) (sAMAccountName=theboss) )

History

Port: ☒ LDAP ☐ GC ☐ Custom: 389

Base type: ☒ DN ☐ PhantomRoot ☐ rootDSE ☐ operational attributes

Scope: ☐ Base ☐ OneLevel ☒ Subtree

Referrals: ☒ None ☐ Subordinate ☐ External

Query type: ☐ Paged (auto) ☒ Non-Paged ☐ DirSync

Return: ☒ Results ☐ Statistics

Search

Attributes

Results (1)

DC: dc1root.mfp-labs.labsetup.org:389

Base: DC=mfp-labs.DC=labsetup.DC=org

Filter: (& (objectClass=user) (sAMAccountName=theboss) )

Scope: Subtree

ReferralChasing: None

ResultCount: 1

CN=theboss,OU=Users,OU=AdminBox,DC=mfp-labs,DC=labsetup,DC=org

DN: <CN=theboss,OU=Users,OU=AdminBox,DC=mfp-labs,DC=labsetup,DC=org>

accountexpires: <never> (9223372036854775807)

admincount: <1>

badpasswordtime: <7/7/2017 12:18:47 PM (UTC)> (131439035274299058)

badpwdcount: <0>

c: [unclear]

### Fields

#### Domains

A list of all domain naming contexts (NC) in the current forest. The domain NC of the executing user is displayed after start.

mfp-labs.labsetup.org

child-labs.mfp-labs.labsetup.org

mfp-labs.labsetup.org

parallel-labs.labsetup.org

#### DCs

A list of all domain controllers (DC) in the currently displayed domain.

DC1Root.mfp-labs.labsetup.org

DC1Root.mfp-labs.labsetup.org

DC2Root.mfp-labs.labsetup.org

By selecting context menu item <Show DC Info> you get detailed information about the selected DC into the results pane.

Results

DC Info: dc1root.mfp-labs.labsetup.org

Name: dc1root.mfp-labs.labsetup.org

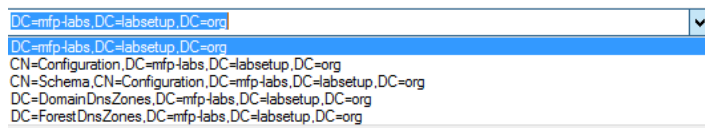
IsGC: True

DomainName: MFP-LABS.LABSETUP.ORG

LdapAdminLimits: MaxValueRange=1000

## NCs

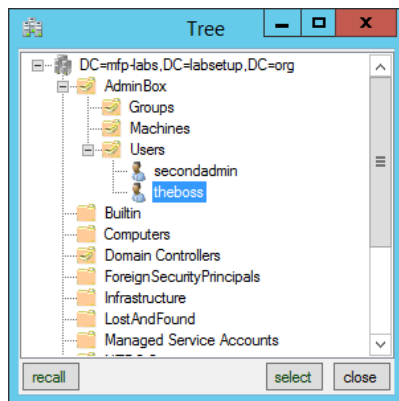
A list of all NCs held by the selected DC.



## Base

The base path to search in – selecting a NC in field NCs updates field Base.

Additionally you may use the context menu <Browse> to load a browsing GUI to find object paths in your AD.

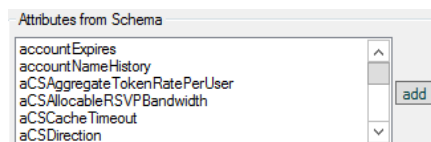


## Filter

Here you define the query filter in LDAP syntax. For the ease of use a FilterWizard is implemented -> context menu Filter Wizard. The FilterWizard will be described later.

## Attributes

The (list of) attributes you want to be returned by the query. You may use the context menu <Load Attributes List> to get a list of all available attributes from the schema (including custom attributes).



If the attribute list contains constructed attributes, LDAPQueryAnalyzer switches to single object path base queries to retrieve the constructed attributes from each object matching the given filter.

You may use 0 or null as attribute to get only the paths of the matching objects returned (no attributes will be requested from the DC).

## ASQ Attributes

The attributes you want to get returned from the objects who are stored via their distinguishedName (DN) in the queried attribute via an Attribute Scoped Query query.

## Results

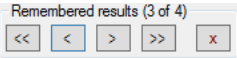
The result output pane. Every query result during runtime is saved in a result cache. If the result cache count exceeds 20 the first result is deleted, and the new result is added at the end of the cache.

You may walk or clear the result cache via the <Remembered results> buttons.

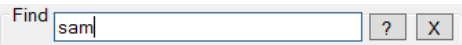
Every query result will display query info.

Example:

DC: dc1root.mfp-labs.labsetup.org:389  
Base: DC=mfp-labs,DC=labsetup,DC=org  
Filter: ( & (objectClass=user) (sAMAccountName=theboss) )  
Scope: Subtree  
ReferralChasing: None  
ResultCount: 1



You may search the query results by pressing Ctrl & F when the result output pane has the focus -> this will show the find dialogue:



Clicking the find button <?> will try to find the first match, pressing <?> button again or pressing F3 will try to find the next match in the query results.

The <x> button will close the find dialogue.

**Controls**

**History**

A list of already successfully executed queries, containing info about:

- Filter used
- Attributes requested
- Was Attribute Scoped Query
- Result should be sorted
- SearchBase
- SearchScope
- DC contacted
- Port used

List can be cleared by selecting context menu <Clear History>. You may also delete single entries by selecting context menu <Delete Current> or delete selected items per <Delete Selected>.

Additionally, you may run bulk queries by selecting the desired items and click <Bulk Query> context menu.

Bulk	Filter	Attributes	ASQ	Sort	Base	DC
<input type="checkbox"/>	( & (objectClass=user) (sAMAccountName=testuser1) )	*	none	none	DC=mfp-labs,DC=labsetup,DC=org	dc4ro
<input type="checkbox"/>	( & (objectClass=user) (! (lastLogonTimestamp=*)) )	none	none	none	DC=mfp-labs,DC=labsetup,DC=org	dc1ro
<input checked="" type="checkbox"/>	( & (objectClass=user) (sAMAccountName=theboss) )	*	none	none	DC=mfp-labs,DC=labsetup,DC=org	dc1ro
<input type="checkbox"/>	( & (objectClass=user) (sAMAccountName=testuser1) )	*	none	none	DC=mfp-labs,DC=labsetup,DC=org	dc1ro
<input type="checkbox"/>	( & (objectClass=user) (sAMAccountName=testuser1) )	lastlogon	none	none	DC=mfp-labs,DC=labsetup,DC=org	dc1ro

☒ Use SearchBase  
☒ User SearchScope  
☒ Use ASQ  
☒ Use Sorting  
☒ Use DC  
☒ Use Port  
☒ Use All  
  
Bulk Query  
  
Delete Current  
Delete Selected  
Clear History

## Port

### LDAP

The LDAP port (default 389) is used for DC connection. Default value can be defined in context menu Define LDAP Port:

### GC

The Global Catalog (GC) port (default 3268) is used for DC connection. Default value can be defined in context menu Define GC Port. This option is only available when the selected DC is also a GC.

### Custom

You may define a custom port to connect to the DC – for example to connect to an AD snapshot instance mounted via dsamain.exe.

## BaseType

### DN

Standard base type -> a distinguishedName (defined by Base field) is used as search base.

### PhantomRoot

Performing a subtree search against the phantom root of the forest (null-DN) with search scope SubTree. Thus, you will be able to find any object in the whole forest – even if you have multiple parallel trees in your forest.

### rootDSE

Send an UDP ping (rootDSE call) against the selected DC with an empty search base and search scope Base.

### operational attributes

If selected you get back the operational attributes when sending an UDP ping (rootDSE call). You may customize the operational attributes to be returned by editing the RootDSE.xml in the folder .\Cache\Settings. To add a new attribute to the operational attributes list just insert a new line like `<string>newAttribute</string>` to the `<OperationalAttributes>` node.

## Scope

### Base

Performing a base search against the object path defined in Base.

### OneLevel

Performing a one level search against the object path defined in Base.

### SubTree

Performing a subtree search against the object path defined in Base.

## Referrals

### None

Never chase the referred-to server. Setting this option prevents the app from contacting other servers in a referral process.

### External

Chase external referrals.



## Subordinate

Chase only subordinate referrals which are a subordinate naming context in a directory tree.

## Query type

### Paged

The requested query will be send as paged query. Useful if you expect more results to be returned as the MaxPageSize value defined in IDAPAdminLimits. Caveat – query index intersection in this case results in the usage of only one indexed attribute in the query even though there would be more indexed attributes used in the query - possible performance impact.

Therefore, the switch Autoswitch to PagedQuery was implemented in the Menu Query - see description in option Non-Paged below.

### Non-Paged

We first try to send a non-paged query. If the result count exceeds the MaxPageSize value defined in IDAPAdminLimits we only return the results up to MaxPageSize.

Per default the switch <Autoswitch to PagedQuery> from the Menu <Query> is activated. This will resend the query as a paged query and we get all results returned.

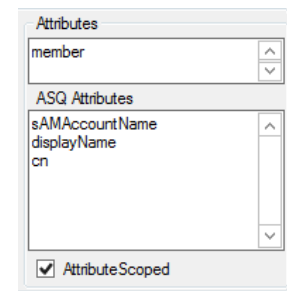
## Attributes

### AttributeScoped

Attribute scoped queries (ASQ) can be send against any linked attribute pair member, like for example:

- member / memberOf
- manager / directReports

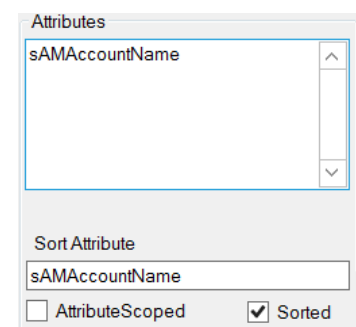
An ASQ must be send against the path of an object that holds this attribute as a base search. In the Attributes field, we need the attribute we want to do the ASQ against as only entry in the list. The attributes in the field ASQ Attributes define the attributes you want to get returned from the objects who are stored via their distinguishedName (DN) in the queried attribute.



The screenshot shows a dialog box titled "Attributes". It has two main sections. The top section, labeled "Attributes", contains a list box with "member" selected. The bottom section, labeled "ASQ Attributes", contains a list box with "sAMAccountName", "displayName", and "cn" listed. Below these list boxes, there is a checkbox labeled "AttributeScoped" which is checked.

### Sorted

Will instruct the NTDS on the DC to sort the query results ascending before returning them. You must define an attribute for sorting. You may use the context menu <Load Attributes List> to get a list of all available attributes from the schema (including custom attributes).



The screenshot shows a dialog box titled "Attributes". It has two main sections. The top section, labeled "Attributes", contains a list box with "sAMAccountName" selected. The bottom section, labeled "Sort Attribute", contains a text box with "sAMAccountName" entered. Below these, there are two checkboxes: "AttributeScoped" (unchecked) and "Sorted" (checked).

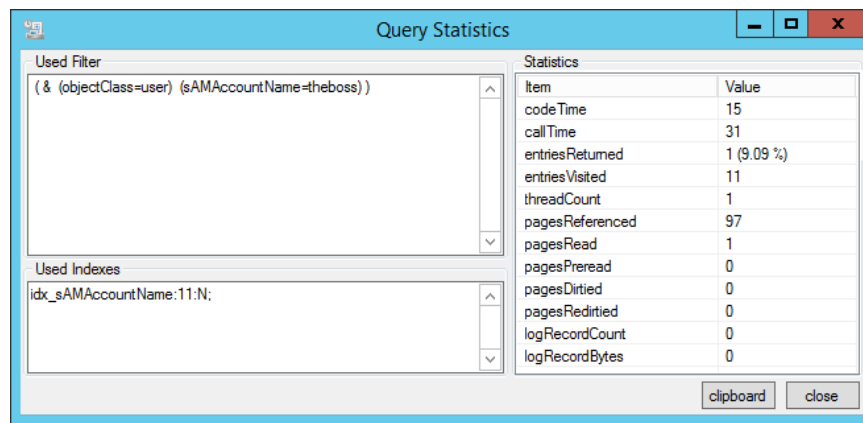
## Return

### Results

Select to display the query results in the results pane.

### Statistics

Select to retrieve query statistics for your query from the DC. To be able to retrieve the information from a DC you need to have the DebugPrivilege assigned to the calling user on the DC.



### Search

Send the query to the selected DC.

### Cancel

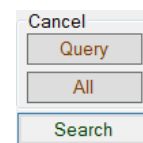
Only displayed while executing a query.

### Query

Cancel query call but handle already received results.

### All

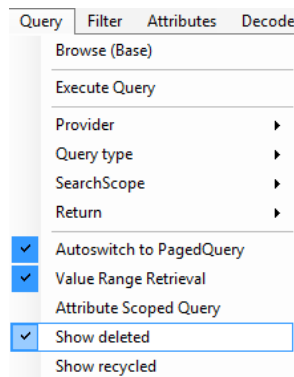
Cancel query call and handling of already received results.



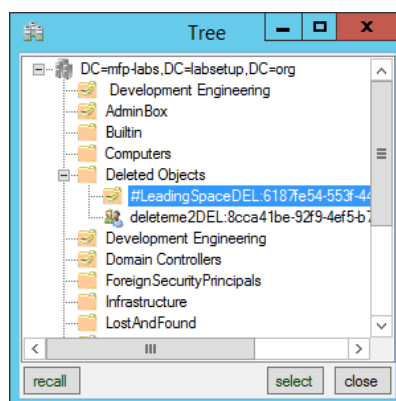
### Restore

Restore a deleted, non-recycled object. Note – you must run the app elevated.

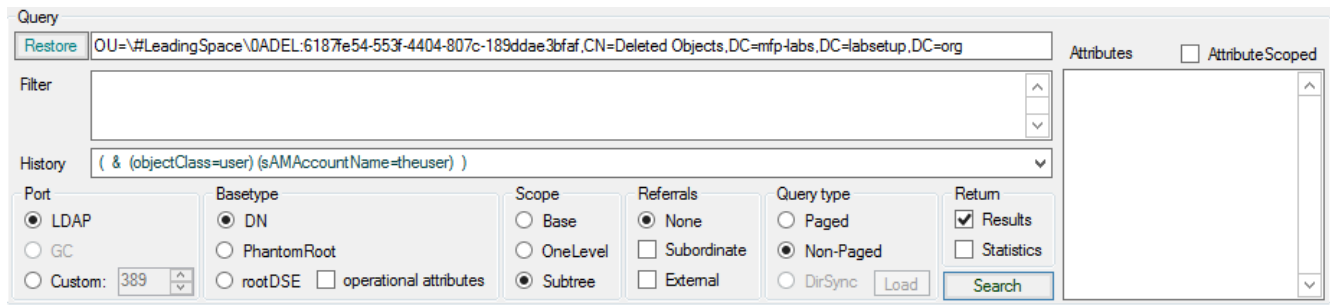
To do so you must first enable ShowDeletedControl in the Query menu:



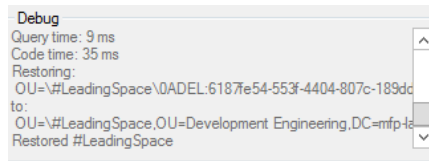
Then click <Browse> menu item from Base field context menu and select the object to be restored in the tree view:



Now you will find the <Restore> button besides the Base field (and the Base field context menu item <Restore> as enabled):



Clicking the button restores the object if possible.



If you enabled ShowRecycledControl as well and select a recycled object, the option to restore will not be available.

## **Menus**

### **File**

#### **Close**

Close app.

### **User**

#### **WhoAmI**

Displays information about the calling user's group memberships and assigned privileges for the machine the tool is executed on in the results pane. Additionally, when running elevated, the tool tries to list User Rights Assignment on the local machine and the targeted DC.

#### **Restart elevated**

Restart app elevated (UAC). Only available if the executing user has the Administrators group disabled in his token.

#### **Run elevated (2nd instance)**

Run app elevated (UAC) in a new instance. Only available if the executing user has the Administrators group in his token.

#### **Restart as**

Restart app as a different user.

#### **Restart as elevated**

Restart app elevated (UAC) as a different user.

#### **Run as (2nd instance)**

Restart app as a different user in a new instance.

### Run as elevated (2nd instance)

Restart app elevated (UAC) as a different user in a new instance.

## Connection

### Refresh Forest

Recall forest info collection for current forest.

### Set Ports

#### LDAP

Define the LDAP port (default 389) used for DC connection.

#### GC

Define the GC port (default 3268) used for DC connection.

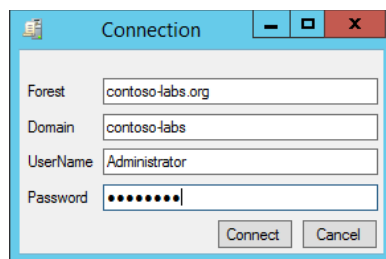
### Set Timeout (s)

Set timeout for DC connections to establish and queries to return results.

### Connect Forest

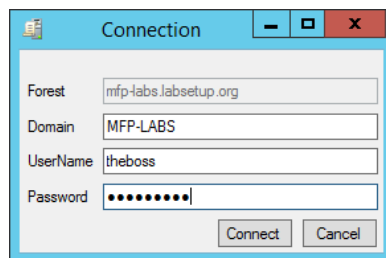
Connect to a different forest with the possibility to pass different credentials than the executing user.

If Password field is empty, the executing user's credentials are used to connect.



### Pass Credentials

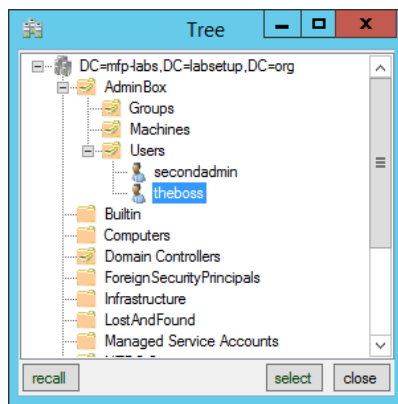
Reconnect current forest with given credentials.



## Query

### Browse (Base)

Load a browsing GUI to find object paths in your AD and set path in Base field.



### Execute Query

Send the query to the selected DC.

### Provider

#### LDAP

The LDAP port (default 389) is used for DC connection. Default value can be defined in context menu Define LDAP Port.

#### GC

The Global Catalog (GC) port (default 3268) is used for DC connection. Default value can be defined in context menu Define GC Port. This option is only available when the selected DC is also a GC.

### Base type

#### DN

Standard base type -> a distinguishedName (defined by Base field) is used as search base.

#### PhantomRoot

Performing a subtree search against the phantom root of the forest (null-DN) with search scope SubTree. Thus, you will be able to find any object in the whole forest – even if you have multiple parallel trees in your forest.

#### rootDSE

Send an UDP ping (rootDSE call) against the selected DC with an empty search base and search scope Base.

### Query type

#### Paged

The requested query will be send as paged query. Useful if you expect more results to be returned as the MaxPageSize value defined in IDAPAdminLimits. Caveat – query index intersection in this case results in the usage of only one indexed attribute in the query even though there would be more indexed attributes used in the query - possible performance impact.

Therefore, the switch <Auto switch to PagedQuery> was implemented in the Menu Query - see description in option Non-Paged below.

### Non-Paged

We first try send a non-paged query. If the result count exceeds the MaxPageSize value defined in IDAPAdminLimits we only return the results up to MaxPageSize.

Per default the switch <Auto switch to PagedQuery> from the Menu Query is activated. This will resend the query as a paged query and get all results returned.

### SearchScope

#### Base

Performing a base search against the object path defined in Base.

#### OneLevel

Performing a one level search against the object path defined in Base.

#### SubTree

Performing a subtree search against the object path defined in Base.

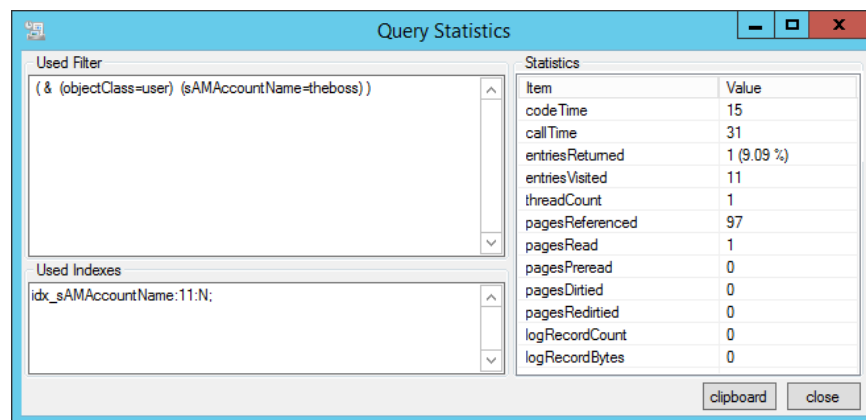
### Return

#### Results

Select to display the query results in the results pane.

#### Statistics

Select to retrieve query statistics for your query from the DC. To be able to retrieve the information from a DC you need to have the DebugPrivilege assigned to the calling user on the DC.



Item	Value
codeTime	15
callTime	31
entriesReturned	1 (9.09 %)
entriesVisited	11
threadCount	1
pagesReferenced	97
pagesRead	1
pagesPreread	0
pagesDirtied	0
pagesRedirtied	0
logRecordCount	0
logRecordBytes	0

### operational attributes

If selected, you get back the operational attributes when sending an UDP ping (rootDSE call). You may customize the operational attributes to be returned by editing the RootDSE.xml in the folder: .\Cache\Settings. To add a new attribute to the operational attributes list just insert a new line like <string>newAttribute</string> to the <OperationalAttributes> node.

### Autoswitch to PagedQuery

When selected - if the result count exceeds the MaxPageSize value defined in IDAPAdminLimits we do not only return the results up to MaxPageSize - we will resend the query as a paged query and get all results returned.

### Value Range Retrieval

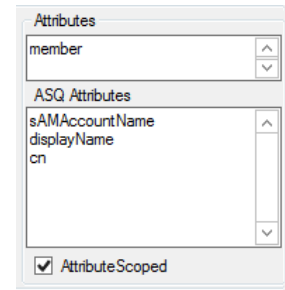
If you ask for a multivalued attribute to be returned and the value count exceeds MaxValRange value defined in IDAPAdminlimits we return the values up to MaxValRange. If selected, we do a value range retrieval and get back all values.

### Attribute Scoped Query

Attribute scoped queries (ASQ) can be send against any linked attribute pair member, like for example:

- member / memberOf
- manager / directReports

An ASQ must be send against the path of an object that holds this attribute as a base search. In the Attributes field, we need the attribute we want to do the ASQ against as only entry in the list. The attributes in the field below define the attributes you want to get returned from the objects who are stored via their distinguishedName (DN) in the queried attribute.



The screenshot shows a dialog box titled 'Attributes'. It has two main sections. The top section, labeled 'Attributes', contains a list box with 'member' selected. The bottom section, labeled 'ASQ Attributes', contains a list box with 'sAMAccountName', 'displayName', and 'cn' listed. At the bottom of the dialog, there is a checkbox labeled 'AttributeScoped' which is checked.

### Show deleted

If selected we also return deleted objects in the query results. Additionally, you will find deleted objects in the browser GUI for base field as well.

### Show recycled

If selected we also return recycled objects in the query results. Additionally, you will find recycled objects in the browser GUI for base field as well.

### Sort results ascending (client side)

Returned result set is sorted ascending (in code, not on DC) by distinguishedName

### Sort results descending (client side)

Returned result set is sorted descending (in code, not on DC) by distinguishedName

### Attribute Scoped Query

Returned

### Sorted Query (server side)

Returned result set is sorted ascending. Sorting is done on the DC from NTDS.

!Caution: this will affect DC performance dramatically!

## Filter

### Filter Wizard

Call the FilterWizards which helps you to create LDAP filters.

### Clear Filter History

Clear the remembered filters in the filter history.

## Attributes

### Load Attribute List from Schema

Show a list of all available attributes from the schema (including custom attributes).

### Hide Attribute List

Hide the list of all available attributes from the schema.

## Decode

### GUIDs

Decode GUID attributes from byte arrays to String-GUIDs

### SIDs

Decode\_SID\_attributes from byte arrays to String-SIDs

### userParameters

Decode RAS- and TerminalServices-Settings from userParameters attribute.

### Resolve Sids

Resolve SIDs to names.

### SecurityDescriptors

Display decoded SecurityDescriptor (SD) instead of displaying SDDL-String of SD. If Resolve Sids is selected, the trustees in the ACLs are resolved to names.

### OctetStrings

Not implemented yet.

### ReplicaLinks

Not implemented yet.

### memberOf includes primaryGroupID

Every SecurityPrincipal which is not a group in AD has a group RID (Relative identifier – last sequence of the SID) set in primaryGroupID.

This group is added to the memberOf list when logging on with a SecurityPrincipal.

When selected the primaryGroupID is translated to the name of the group and added to the memberOf list displayed.

### To local time

Not implemented yet.

## Results

### Copy selected

Copy selected result pane content into clipboard.

### Copy all

Copy result pane content into clipboard.

### Remembered results

#### Show first

Jump to the first result in the remembered results cache.

#### Show previous

Move to the previous result in the remembered results cache.

#### Show next

Move to the next result in the remembered results cache.

#### Show current

Move to the last result in the remembered results cache.



### Clear list

Clear results cache list.

### Clear Output

Clear current result pane.

### Change Font

Change display font in result pane.

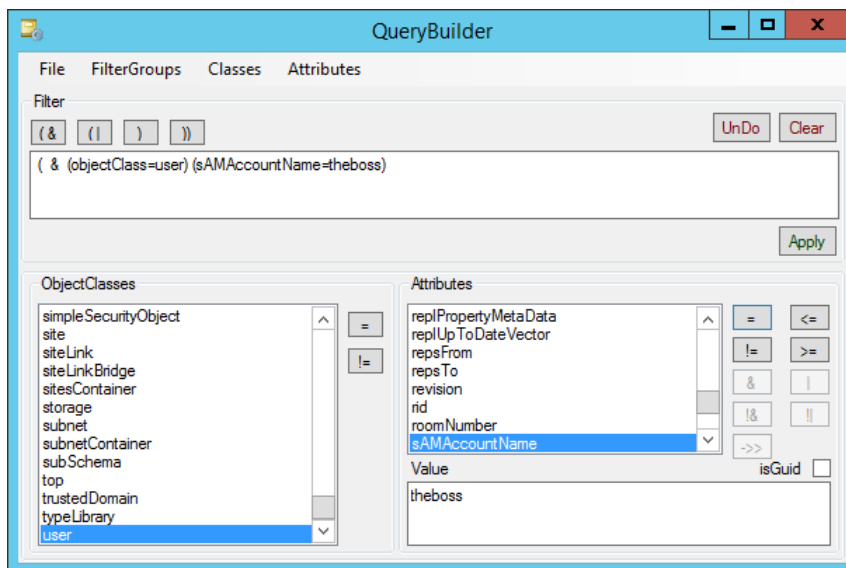
## Tools

### DynamicTypeBuilder

The tool has no hardcoded translations for attribute syntax. We collect information from the Schema and cache this in a XML. Every time the modifiedTimeStamp of the Schema in a forest is updated we refresh the Schema cache.

Since many attributes are enums, OID strings or blobs we implemented a way to dynamically decode those attributes. See detailed description of DynamicTypeBuilder.

## FilterWizard



## Fields

### Filter

Auto-filled textbox showing the currently configured filter. Trailing group closing brackets from auto generated groups are closed automatically when applying filter to main window.

### ObjectClasses

A list of all available classSchema objects in the current forest's schema. Read from schema cache xml.

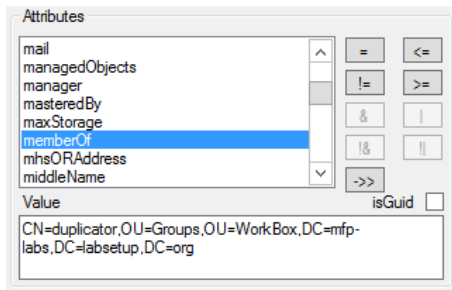
## Attributes

A list of attributes assigned to the selected classSchema object and its sub classes.

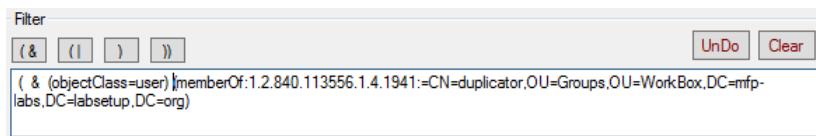
If the selected attribute is defined as part of a linked attribute pair the ->> control (Match In Chain) will be enabled.

Syntax of <Value> must be a distinguishedName.

This adds the :1.2.840.113556.1.4.1941: operator to the filter for this attribute.



The 'Attributes' dialog box shows a list of attributes on the left: mail, managedObjects, manager, masteredBy, maxStorage, memberOf (highlighted), mhsORAddress, and middleName. To the right of the list are several operator buttons: =, <=, !=, >=, &, |, !&, and !|. Below the list is a text field labeled 'Value' containing the distinguished name 'CN=duplicator,OU=Groups,OU=WorkBox,DC=mfplabs,DC=labsetup,DC=org'. There is also a checkbox labeled 'isGuid'.



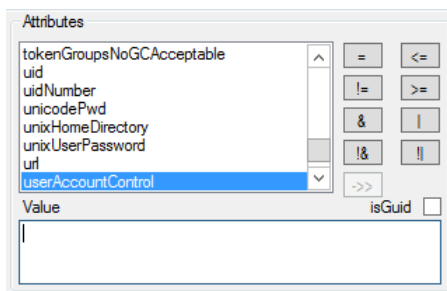
The 'Filter' dialog box shows a list of filter operators: (&), (!), (), and ()). To the right are 'Undo' and 'Clear' buttons. The main text area contains the filter expression: '(& (objectClass=user) | memberOf:1.2.840.113556.1.4.1941:=CN=duplicator,OU=Groups,OU=WorkBox,DC=mfplabs,DC=labsetup,DC=org)'. The '(&)' operator is selected.

If the selected attribute is defined as attribute syntax integer or enumeration the controls

- BitWise AND &
- BitWise OR |
- Not BitWise AND !&
- Not BitWise OR !|

will be enabled.

By clicking one of these buttons a list of the existing enum values will be displayed (if enum is defined in the DynamicTypeBuilder). Multi-select in the list is allowed.



The 'Attributes' dialog box shows a list of attributes on the left: tokenGroupsNoGCAcceptable, uid, uidNumber, unicodePwd, unixHomeDirectory, unixUserPassword, url, and userAccountControl (highlighted). To the right of the list are the same operator buttons as in the first image. Below the list is a text field labeled 'Value' which is currently empty. There is also a checkbox labeled 'isGuid'.

Otherwise you may just type the numeric value in the Value field.

This adds the operator :1.2.840.113556.1.4.803 for bitwise AND and :1.2.840.113556.1.4.804: for bitwise OR.

### Value

The value defining the filter for the currently selected attribute.

## **Controls**

### Open AND group (&)

Opens a new AND group to combine filters where all filter clauses grouped here must match for a hit.

If you do not open any group before selecting filter clauses we automatically open an AND group if more than one filter clause is selected.

### Open OR group (|)

Opens a new Or group to combine filter clauses where only one or more of the filter clauses grouped here must match for a hit.

### Close current group )

If you opened a group manually you can close it here.

All automatically opened groups are closed automatically when applying the filter to the main window.

### Close all groups ))

If you opened groups manually you can close them here automatically.

All automatically opened groups are closed automatically when applying the filter to the main window.

### Undo

Remove the last selected filter clause.

### Clear

Remove all selected filter clauses and groups.

## Apply

Apply the constructed filter to the main window.

## ObjectClasses

### Equals =

Adds a filter clause (*objectClass=selected schemaClass*).

### Not Equals !=

Adds a filter clause ( *! (objectClass=selected schemaClass)*  ).

## Attributes

### Equals =

Adds a filter clause (*selected attribute=Value*).

### Not Equals !=

Adds a filter clause ( *! (selected attribute=Value)*  ).

### Less or Equals <=

Adds a filter clause (*selected attribute<=Value*).

Note – we do not offer ‘Not Less or Equals’ -> this is no recommended filter clause – use ‘Greater or Equals’ instead.

### Greater or Equals >=

Adds a filter clause (*selected attribute>=Value*).

Note – we do not offer ‘Not Greater or Equals’ -> this is no recommended filter clause – use ‘Less or Equals’ instead.

### Bitwise AND &

Adds a filter clause (*selected attribute:1.2.840.113556.1.4.803:=Value*).

When this matching rule is used as a clause in a query filter, the clause is satisfied only if all the bits set to '1' in the value included in the clause correspond to bits set to '1' in the value stored in the directory.

### Bitwise OR |

Adds a filter clause (*selected attribute:1.2.840.113556.1.4.804:=Value*).

When this matching rule is used as a clause in a query filter, the clause is satisfied only if at least one of the bits set to '1' in the value included in the clause corresponds to a bit set to '1' in the value stored in the directory.

### Not Bitwise AND !&

Adds a filter clause ( *! (selected attribute:1.2.840.113556.1.4.803:=Value)*  ).

When this matching rule is used as a clause in a query filter, the clause is satisfied only if none the bits set to '1' in the value included in the clause correspond to bits set to '1' in the value stored in the directory.

### Not Bitwise Or !|

Adds a filter clause ( ! ( *selected attribute*:1.2.840.113556.1.4.804:=*Value*) ).

When this matching rule is used as a clause in a query filter, the clause is satisfied only if at none of the bits set to '1' in the value included in the clause corresponds to a bit set to '1' in the value stored in the directory.

### Match in Chain ->>

Adds a filter clause ( *selected attribute*:1.2.840.113556.1.4.1941: =*distinguishedName in Value field*).

Allows you to retrieve for example:

- all direct and nested group memberships of a user
- all direct and nested members of a group
- following the directReports or manager chain
- ...

This is a very expensive call since we must walk the link table of the Active Directory database to find all objects in the link chain.

### isGuid

If the selected attribute is of attribute syntax GUID you can type a string Guid (like bf967a8f-0de6-11d0-a285-00aa003049e2. The GUID will be translated to the hex expression of the GUID to build the proper syntax.

If as GUID attribute is not marked with GUID syntax, you may check isGuid checkbox to get the expected result.

The 'Attributes' dialog box shows a list of attributes on the left, with 'schemaIDGUID' selected. On the right, there are comparison operators: '=', '<=', '!=', '>=', '&', '|', '&&', '||', and '>>'. Below the list, the 'Value' field contains the GUID string 'bf967a8f-0de6-11d0-a285-00aa003049e2'. The 'isGuid' checkbox is checked.

The 'Filter' dialog box shows a filter expression: '( & (objectClass=classSchema) (schemaIDGUID=\8F\7A\96\BF\E6\0D\01\11\A2\85\00\AA\00\30\49\E2)'. There are buttons for 'UnDo' and 'Clear'.

Attribute Type Associator

File

Associations (samaccounttype)

samaccounttype

groupstype

useraccountcontrol

systemflags

searchflags

schemaflagsex

userParameter

Associator type

ENUM

Enum

ADS\_SAMACCOUNT\_TYPE

Dictionary

NONE

BerDecoder

NONE

Save

Discard

Enums

Dictionaries

BerConverter

Enums

Values (ADS\_SAMACCOUNT\_TYPE)

ADS\_GROUP\_TYPE

ADS\_USER\_FLAG

ADS\_SAMACCOUNT\_TYPE

ADS\_SYSTEMFLAG

ADS\_SEARCHFLAG

ADS\_SEARCHFLAGEX

FUNCTIONAL\_LEVEL

DS\_BEHAVIOR

SUPPORTED\_ENCRYPTION\_TYP...

INSTANCE\_TYPE

ValueName	Value
DOMAIN_OBJECT	0x0
GROUP_OBJECT	0x10000000
NON_SECURITY_GROUP_OBJECT	0x10000001
ALIAS_OBJECT	0x20000000
NON_SECURITY_ALIAS_OBJECT	0x20000001
USER_OBJECT	0x30000000
MACHINE_ACCOUNT	0x30000001
TRUST_ACCOUNT	0x30000002

Save

Discard

Save

Close

Enums

ADS\_GROUP\_TYPE

ADS\_USER\_FLAG

ADS\_SAMACCOUNT

ADS\_SYSTEMFLAG

ADS\_SEARCHFLAG

ADS\_SEARCHFLAGEX

FUNCTIONAL\_LEVEL

DS\_BEHAVIOR

SUPPORTED\_ENCRYPTION\_TYP...

INSTANCE\_TYPE

Add

Delete

Values (ADS\_SAMACCOUNT\_TYPE)

ValueName	Value
DOMAIN_OBJECT	0x0
GROUP_OBJECT	0x10000000
NON_SECURITY_	0x10000001
ALIAS_OBJECT	0x20000000
NON_SECURITY_	0x20000001
USER_OBJECT	0x30000000
MACHINE_ACCO	0x30000001
TRUST_ACCOUN	0x30000002

Edit

Move up

Move down

Insert

Append

Delete

Save

Discard

Attribute Type Associator

File

Associations (supportedControl)

supportedControl

supportedCapabilities

domainFunctionality

forestFunctionality

domainControllerFunctionality

msds-behavior-version

msds-supportedencryptiontypes

Associator type

Dictionary

Enum

BerDecoder

Dictionary

SUPPORTED\_CONTROL

Save

Discard

Enums

Dictionaries

BerConverter

Dictionaries

SUPPORTED\_CONTROL

SUPPORTED\_CAPABILITIES

KeyValuePairs (SUPPORTED\_CONTROL)

Key	Value
1.2.840.113556.1.4.319	LDAP_PAGED_RESULT_OID_STRING
1.2.840.113556.1.4.521	LDAP_SERVER_CROSSDOM_MOVE...
1.2.840.113556.1.4.841	LDAP_SERVER_DIRSYNC_OID
1.2.840.113556.1.4.1339	LDAP_SERVER_DOMAIN_SCOPE_OID
1.2.840.113556.1.4.529	LDAP_SERVER_EXTENDED_DN_OID
1.2.840.113556.1.4.970	LDAP_SERVER_GET_STATS_OID
1.2.840.113556.1.4.619	LDAP_SERVER_LAZY_COMMIT_OID
1.2.840.113556.1.4.1413	LDAP_SERVER_PERMISSIVE_MODI...

Save

Discard

Save

Close

Dictionaries

SUPPORTED\_CONTROL

SUPPORTED\_CAPABILITIES

Add

Delete

KeyValuePairs (SUPPORTED\_CONTROL)

Key	Value
1.2.840.113556.1.4.319	LDAP_PAGED_RESULT_OID_STRING
1.2.840.113556.1.4.521	LDAP_SERVER_CROSSDOM_MOVE...
1.2.840.113556.1.4.841	LDAP_SERVER_DIRSYNC_OID
1.2.840.113556.1.4.1339	LDAP_SERVER_DOMAIN_SCOPE_OID
1.2.840.113556.1.4.529	LDAP_SERVER_EXTENDED_DN_OID
1.2.840.113556.1.4.970	LDAP_SERVER_GET_STATS_OID
1.2.840.113556.1.4.619	LDAP_SERVER_LAZY_COMMIT_OID
1.2.840.113556.1.4.1413	LDAP_SERVER_PERMISSIVE_MODI...

Edit

Move up

Move down

Insert

Append

Delete

Save

Discard

Attribute Type Associator

File
Associations (StatsData)
grouptype
useraccountcontrol
systemflags
searchflags
schemaflagsex
userParameter
StatsData
Associator type: BERCONVERTER
Enum: NONE
Dictionary: NONE
BerDecoder: StatsData
Save Discard

Enums Dictionaries BerConverter
Converter
StatsData
StatsData
ConversionRule (StatsData)
ia includes Tags
Fields (StatsData)
Field Name Field Type
threadCount System.Int32
callTime System.Int32
entriesReturned System.Int32
entriesVisited System.Int32
filter System.String
Save Discard
Save Close

Converter
StatsData
StatsData
Add
Delete

ConversionRule (StatsData)
ia includes Tags
Fields (StatsData)
Field Name Field Type
threadCount System.Int32
callTime System.Int32
entriesReturned System.Int32
entriesVisited System.Int32
filter System.String
Edit
Move up
Move down
Insert
Append
Delete
Save Discard
Save Close



## **Disclaimer**

```
// =====  
// THIS CODE-SAMPLE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER  
// EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES  
// OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.  
//  
// This sample is not supported under any Microsoft standard support program  
// or service. The code sample is provided AS IS without warranty of any kind.  
// Microsoft further disclaims all implied warranties including, without  
// limitation, any implied warranties of merchantability or of fitness for a  
// particular purpose. The entire risk arising out of the use or performance  
// of the sample and documentation remains with you. In no event shall  
// Microsoft, its authors, or anyone else involved in the creation,  
// production, or delivery of the script be liable for any damages whatsoever  
// (including, without limitation, damages for loss of business profits,  
// business interruption, loss of business information, or other pecuniary  
// loss) arising out of the use of or inability to use the sample or  
// documentation, even if Microsoft has been advised of the possibility of  
// such damages.  
// =====
```