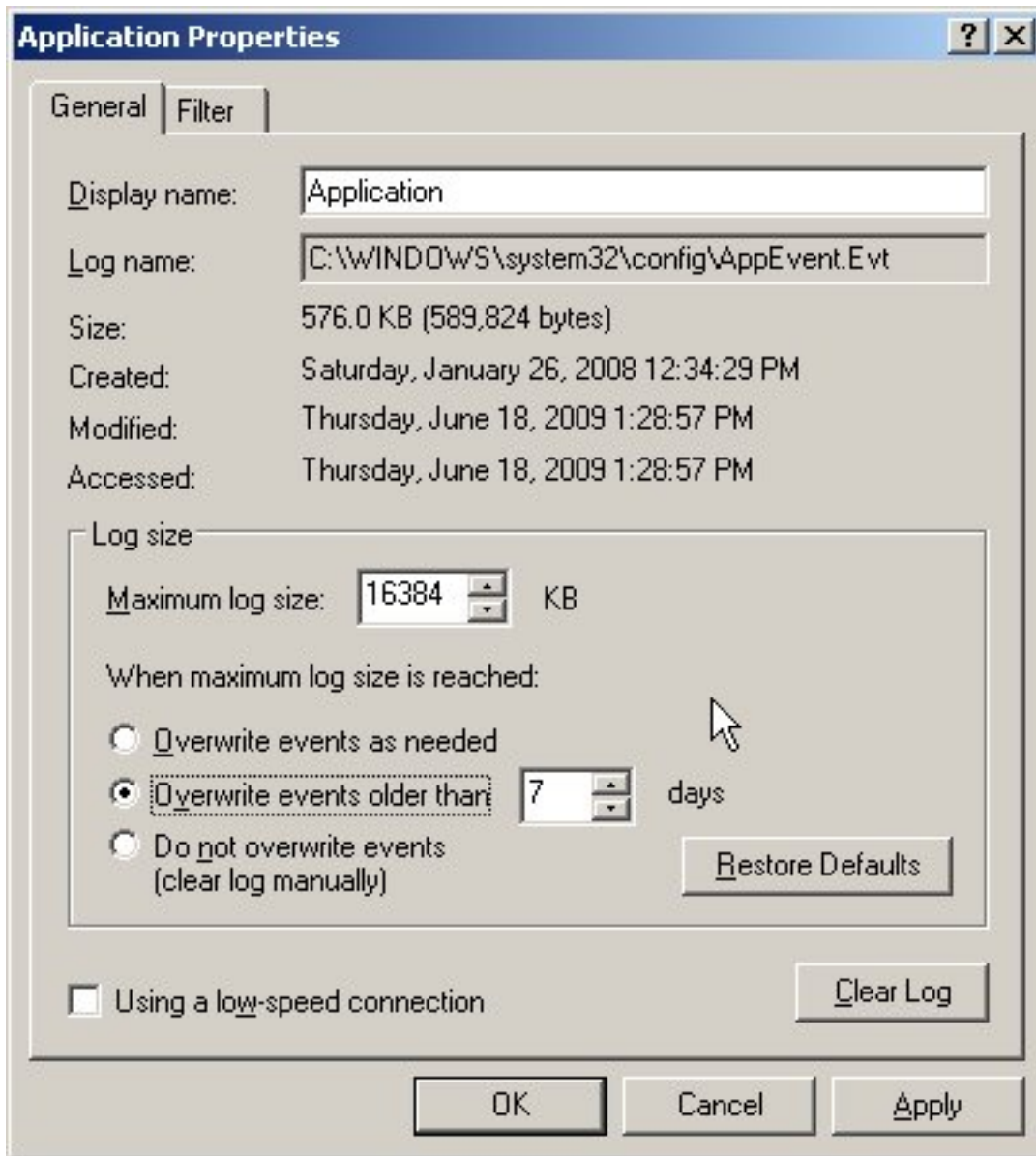


# How to scan for the settings of your Event Viewer Application, Security, or System logs?

Here is a way to scan for the settings of your Event Viewer Application, Security, and System logs?



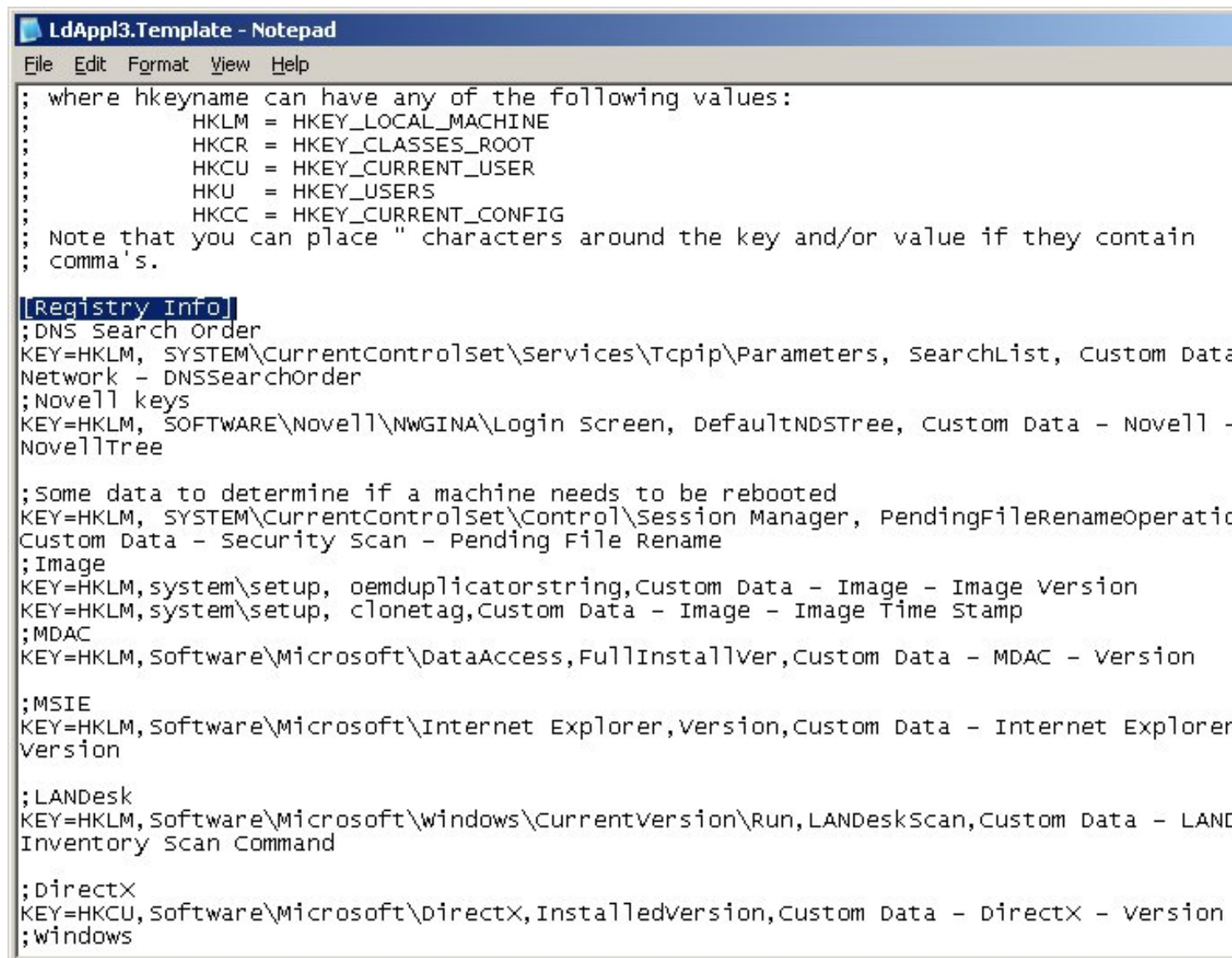
1. The registry keys that holds this information is located:

How to scan for the settings of your Event Viewer Application, Security, or System logs?

- a. HKLM\System\controlset001\services\Eventlog\Application
- b. HKLM\System\controlset001\services\Eventlog\Security
- c. HKLM\System\controlset001\services\Eventlog\System

2. On the core server browse to the Program Files\LANDesk\ManagementSuite\ldlogon directory and open up your ldappl3.template file with notepad.

3. Scroll down till you see the [Registry Info] section:



```
LdAppl3.Template - Notepad
File Edit Format View Help
; where hkeyname can have any of the following values:
;
;     HKLM = HKEY_LOCAL_MACHINE
;     HKCR = HKEY_CLASSES_ROOT
;     HKCU = HKEY_CURRENT_USER
;     HKU  = HKEY_USERS
;     HKCC = HKEY_CURRENT_CONFIG
; Note that you can place " characters around the key and/or value if they contain
; comma's.

[Registry Info]
;DNS Search Order
KEY=HKLM, SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, SearchList, Custom Data -
Network - DNSSearchOrder
;Novell keys
KEY=HKLM, SOFTWARE\Novell\NWGINA\Login screen, DefaultNDSTree, Custom Data - Novell -
NovellTree

;Some data to determine if a machine needs to be rebooted
KEY=HKLM, SYSTEM\CurrentControlSet\Control\Session Manager, PendingFileRenameOperatio
Custom Data - Security Scan - Pending File Rename
;Image
KEY=HKLM,system\setup, oemduplicatorstring,Custom Data - Image - Image Version
KEY=HKLM,system\setup, clonetag,Custom Data - Image - Image Time Stamp
;MDAC
KEY=HKLM,Software\Microsoft\DataAccess,FullInstallVer,Custom Data - MDAC - Version

;MSIE
KEY=HKLM,Software\Microsoft\Internet Explorer,Version,Custom Data - Internet Explorer
Version

;LANDesk
KEY=HKLM,Software\Microsoft\windows\CurrentVersion\Run,LANDeskScan,Custom Data - LAND
Inventory Scan Command

;DirectX
KEY=HKCU,Software\Microsoft\DirectX,InstalledVersion,Custom Data - DirectX - Version
;windows
```

4. At the end of the [Registry Info] section paste in the following lines. You can modify them so the information is stored in a different location than the custom directoy if you wish, but this is where I put them:

How to scan for the settings of your Event Viewer Application, Security, or System logs?

;Event Viewer Application settings

KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,MaxSize,Custom Data -  
Event Viewer Settings - Application Max Size

KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,Retention,Custom Data -  
Event Viewer Settings - Application Retention

;Event Viewer Security settings

KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Security,MaxSize,Custom Data -  
Event Viewer Settings - Security Max Size

KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Security,Retention,Custom Data -  
Event Viewer Settings - Security Retention

;Event Viewer System settings

KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\System,MaxSize,Custom Data -  
Event Viewer Settings - System Max Size

KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\System,Retention,Custom Data -  
Event Viewer Settings - System Retention

How to scan for the settings of your Event Viewer Application, Security, or System logs?

```
LdAppl3.Template - Notepad
File Edit Format View Help
KEY=HKLM,Software\Microsoft\windows\CurrentVersion\Run,LANDeskScan,Custom Data - LAN
Inventory Scan Command

;DirectX
KEY=HKCU,Software\Microsoft\DirectX,InstalledVersion,Custom Data - DirectX - Version
;windows
KEY=HKLM,Software\Microsoft\windows\CurrentVersion\NetCache,Enabled,Custom Data - win
Offline Files Status

;vulscan deferred tasks
KEY=HKLM,Software\landesk\Managementsuite\winclient\vulscan,DeferredTasks,Custom Data
LANdesk - Deferred Repair Task

;Event Viewer Application settings
KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,MaxSize,Custom Data - Eve
Viewer Settings - Application Max Size
KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,Retention,Custom Data - E
Viewer Settings - Application Retention

;Event Viewer Security settings
KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Security,MaxSize,Custom Data - Event
Settings - Security Max Size
KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Security,Retention,Custom Data - Even
Viewer Settings - Security Retention

;Event Viewer System settings
KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\System,MaxSize,Custom Data - Event V
Settings - System Max Size
KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\System,Retention,Custom Data - Event
Settings - System Retention

; DMI Info section - map DMI information to LANdesk class/attributes
; Key=<dmi class>, <attribute id>, <attribute in the database>
;
; or
; Key=<dmi component>, <dmi class>, <attribute id>, <attribute in the database>
; An example is like the following:
; Key=DMTF|Processor|011, 2, Processor - Type
```

5. Here is a break down of what this line means so you can put the information in different locations, name the folders differently etc.

a. **KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,MaxSize,Custom Data - Event Viewer Settings - Application Max Size**

This is the first location. Although they list the HKCU (HKEY\_CURRENT\_USER) in this list in the ldappl3 file, we can't bring information back from here.

1. HKLM = HKEY\_LOCAL\_MACHINE
2. HKCR = HKEY\_CLASSES\_ROOT

How to scan for the settings of your Event Viewer Application, Security, or System logs?

3. HKCU = HKEY\_CURRENT\_USER

4. HKU = HKEY\_USERS

5. HKCC = HKEY\_CURRENT\_CONFIG

b. KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,MaxSize,Custom Data - Event Viewer Settings - Application Max Size

1. This is the path to the key. It is only to the folder so you won't be putting the key name in this section.

c. KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,MaxSize,Custom Data - Event Viewer Settings - Application Max Size

1. This is the name of the key that you are trying to bring back

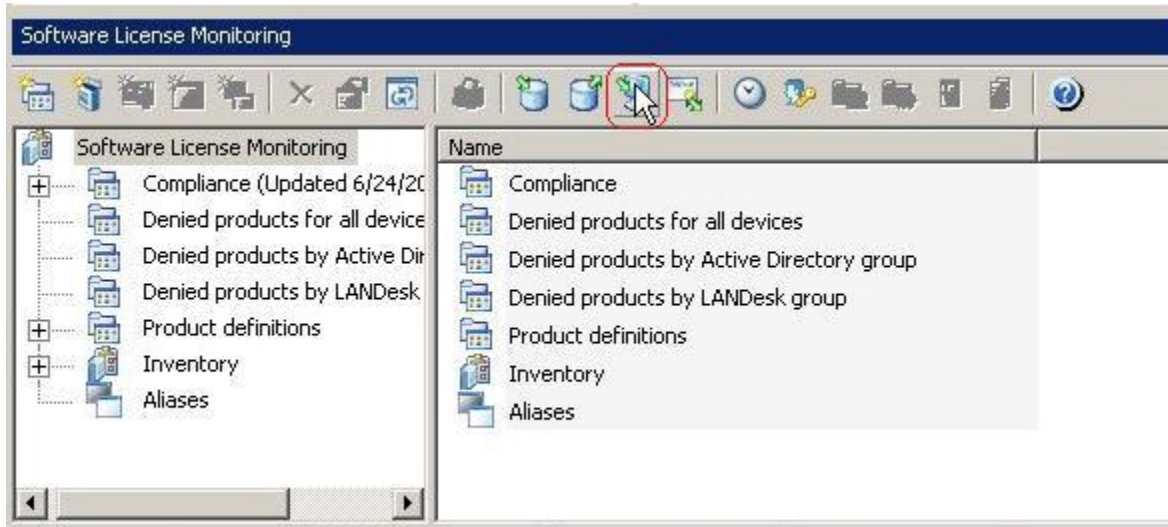
d. KEY=HKLM,SYSTEM\ControlSet001\Services\Eventlog\Application,MaxSize,Custom Data - Event Viewer Settings - Application Max Size

1. This is the location you will see the information in your inventory and queries.

6. Save your Idappl3.template

7. Log into your console and go to Tools > Report / Monitoring > Software License Monitoring and click on the 'Make Available to Clients'.

How to scan for the settings of your Event Viewer Application, Security, or System logs?

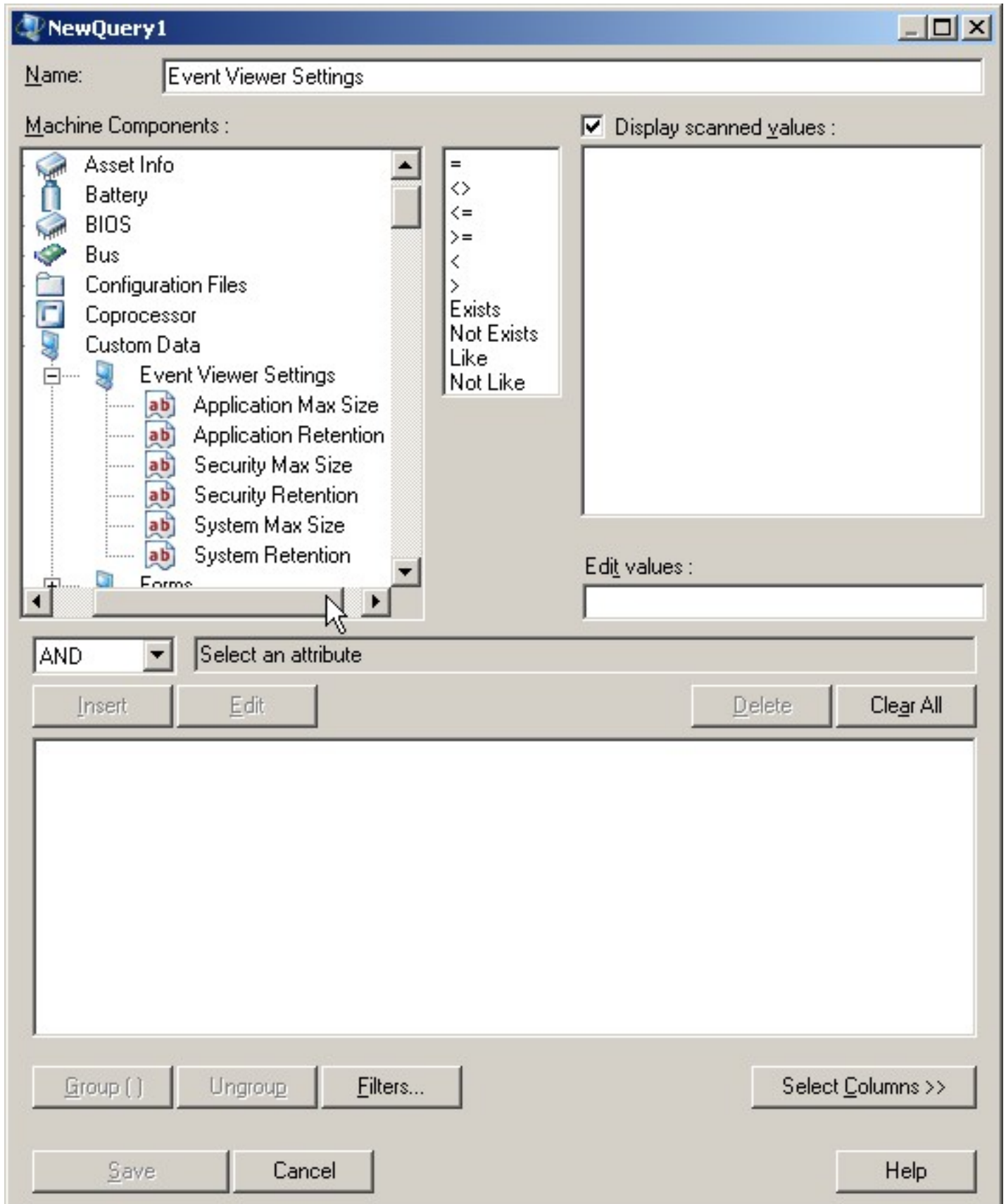


8. On a machine run the inventory scanner with a /F /Sync switches a couple times to make sure a Software scan is done. You can do this from the Start > Run command line if you wish. I would look like this:

```
"C:\Program Files\LANDesk\LDClient\LDISCN32.EXE" /NTT=Your Core name here:5007 /  
S=Your Core name here /l=HTTP://Your Core name here/ldlogon/ldappl3.Idz /V /F /SYNC
```

9. You should now be able to do a query for this information. Since I put mine in the custom data folder this is what it would look like:

How to scan for the settings of your Event Viewer Application, Security, or System logs?



How to scan for the settings of your Event Viewer Application, Security, or System logs?

You can modify what registry keys you bring back, what it is named in the database, and the location if you wish..