ldifde.exe

>> File Path: `C:\Windows\SysWOW64\ldifde.exe`

>> Description: NT5DS

Hashes

Type	Hash
MD5	`979DE101F5059CEC1D2C56967CA2BAC0`
SHA1	`86A22C76679FB4F7A0F99C555BBB3DAAA1B4C060`
SHA256	`355A746E33B0DF2F834FDEF913DDCFDBD83F59A17FFD3A9F2AFA48EEE7BE7E71`
SHA384	`37EBF2285FCC6EC88ACD0E2FE359ED02621D41471ABBD1E6A0B04629DA75C79DAEB4C0217C231B808B8FEE228B983580`
SHA512	`2242C7CE33620C01D55196B15B7FD126940AA31FC1B8347EF7C7E46171F8D1FA9AFC5181EA6763AF58D01DCA11A54E545ABC2841BA4184C3C899FBA992975C1A`
SSDEEP	`1536:LXoPCAhD2F8pUP+d5TolJUS8Ze3tP4k/HIwCB1:LXozTmWLKrtP4nr`

Runtime Data

Usage (stdout):

```
Invalid Parameter: Input file name required

LDIF Directory Exchange

General Parameters
==================
-i              Turn on Import Mode (The default is Export)
-f filename     Input or Output filename
-s servername   The server to bind to (Default to DC of computer's domain)
-c FromDN ToDN  Replace occurences of FromDN to ToDN
                If either FromDN or ToDN ends with #attributeName, the
                attribute value will be looked up in rootDSE and used to
                replace #attributeName.  See example for "Macro expansion
                in DNs".
-v              Turn on Verbose Mode
-j path         Log File Location
-t port         Port Number (default = 389)
-u              Use Unicode format
-w timeout      Terminate execution if the server takes longer than the
                specified number of seconds to respond to an operation
                (default = no timeout specified)
-h              Enable SASL layer signing and encryption
-?              Help

Export Specific
===============
-d RootDN       The root of the LDAP search (Default to Naming Context)
-r Filter       LDAP search filter (Default to "(objectClass=*)")
-p SearchScope  Search Scope (Base/OneLevel/Subtree)
-l list         List of attributes (comma separated) to look for
                in an LDAP search
-o list         List of attributes (comma separated) to omit from
                input.
```

```
-g              Disable Paged Search.
-m              Enable the SAM logic on export.
-n              Do not export binary values
-x              Include deleted objects (tombstones)
-1              Retain only the important replPropertyMetadata

Import
======
-k              The import will go on ignoring 'Constraint Violation'
                and 'Object Already Exists' errors
-y              The import will use lazy commit for better performance
                (enabled by default)
-e              The import will not use lazy commit
-q threads      The import will use the specified number of threads
                (default is 1)
-z              Continue importing irrespective of errors.
-x              Enable tombstone reanimation support (passes deleted
                objects control with ldap modify requests)
```

```
Credentials Establishment
=========================
Note that if no credentials is specified, LDIFDE will bind as the currently
logged on user, using SSPI.

-a UserDN [Password | *]            Simple authentication
-b UserName Domain [Password | *]   SSPI bind method

Example: Simple import of current domain
    ldifde -i -f INPUT.LDF

Example: Simple export of current domain
    ldifde -f OUTPUT.LDF

Example: Export of specific domain with credentials
    ldifde -m -f OUTPUT.LDF
           -b USERNAME DOMAINNAME *
           -s SERVERNAME
           -d "cn=users,DC=DOMAINNAME,DC=Microsoft,DC=Com"
           -r "(objectClass=user)"

Example: Macro expansion in DNs
    ldifde -f export.ldf -c "#configurationNamingContext" "cn=configuration,dc=x"
    ldifde -i -f import.ldf -c "cn=configuration,dc=x" "#configurationNamingContext"
```

```
No log files were written.  In order to generate a log file, please
specify the log file path via the -j option.
```

Loaded Modules:

Path
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\System32\wow64.dll
C:\Windows\SysWOW64\ldifde.exe

Signature

- Status: Signature verified.
- Serial: `33000001C422B2F79B793DACB20000000001C4`
- Thumbprint: `AE9C1AE54763822EEC42474983D8B635116C8452`

>> Issuer: CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

>> Subject: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

File Metadata

>> Original Filename: ldifde.exe.mui

>> Product Name: Microsoft Windows Operating System

>> Company Name: Microsoft Corporation

>> File Version: 10.0.17763.1 (WinBuild.160101.0800)

>> Product Version: 10.0.17763.1

>> Language: English (United States)

>> Legal Copyright: Microsoft Corporation. All rights reserved.

Possible Misuse

*The following table contains possible examples of `ldifde.exe` being misused. While `ldifde.exe` is **not** inherently malicious, its legitimate functionality can be abused for malicious purposes.*

Source	Source File	Example	License
sigma	proc creation win apt judgement panda gtr19.yml	`- '\ldifde.exe -f -n '`	DRL 1.0