

Using LDIFDE to import and export directory objects to Active Directory

This article was previously published under Q237677

Article ID	: 237677
Last Review	: February 27, 2007
Revision	: 4.2

On This Page

↓ [SUMMARY](#)

↓ [MORE INFORMATION](#)

↓ [Viewing LDIFDE general parameters](#)

↓ [General Parameters](#)

↓ [Export Specific Parameters](#)

↓ [Import Specific Parameter](#)

↓ [Credentials Parameters](#)

↓ [Using LDIFDE to export and to import directory objects](#)

↓ [Export the organizational units from the source domain](#)

↓ [Export the user accounts from the source domain](#)

↓ [Import the organizational units from Export to Import](#)

↓ [Import the users from Export to Import](#)

↓ [Exporting objects from an entire forest](#)

↓ [Importing multivalued attributes](#)

SUMMARY

The LDAP Data Interchange Format (LDIF) is a draft Internet standard for a file format that may be used for performing batch operations against directories that conform to the LDAP standards. LDIF can be used to export and import data, allowing batch operations such as add, create, and modify to be performed against the Active Directory. A utility program called LDIFDE is included in Windows 2000 to support batch operations based on the LDIF file format standard. This article is designed to help you better understand how the LDIFDE utility can be used to migrate directories.

MORE INFORMATION

Viewing LDIFDE general parameters

1. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, type: **ldifde ?**. The built-in Help file is then displayed as below.

General Parameters

```
-i Turn on Import Mode (The default is Export) -f filename Input or Output
filename -s servername The server to bind to -c FromDN ToDN Replace occurrences of
FromDN to ToDN -v Turn on Verbose Mode -j Log File Location -t Port Number
(default = 389) -? Help
```

Export Specific Parameters

```
-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
```

Import Specific Parameter

```
-k The import will go on ignoring 'Constraint Violation' and 'Object Already
Exists' errors
```

Credentials Parameters

```
-a Sets the command to run using the supplied user distinguished name and
password. For example: "cn=yourname,dc=yourcompany,dc-com password" -b Sets the
command to run as username domain password. The default is to run using the
credentials of the currently logged on user.
```

Note This tool is very flexible and offers a number of command-line switches and arguments. The

utility is included in Windows 2000 Server, but not with Windows 2000 Professional. The LDIFDE program can be copied to a computer running Windows 2000 Professional and be run remotely against the Windows 2000 Server Active Directory.

Using LDIFDE to export and to import directory objects

The following is a step-by-step process to import and export Organizational Units (OUs) and user accounts from one Windows 2000 Active Directory to another. For this example, "Export" is the name of the domain from which objects are exported and "Import" is the name of the domain in which objects are imported. LDIFDE can also be used to import most third-party folders to Active Directory.

Export the organizational units from the source domain

1. Log on as Administrator in the Export domain. If you log on using an account that does not have administrative privileges, you may not be able to perform export and import operations against the Active Directory.
2. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
3. At the command prompt, type:

```
ldifde -f exportOu.ldf -s Server1 -d "dc=Export,dc=com" -p subtree -r  
"(&(objectCategory=organizationalUnit)" -I "cn,objectclass,ou"
```

Running this command exports all OUs except domain controllers into a file named ExportOU.ldf.

Export the user accounts from the source domain

At the command prompt, type:

```
ldifde -f Exportuser.ldf -s Server1 -d "dc=Export,dc=com" -p subtree -r  
"(&(objectCategory=person)(objectClass=User)(givenname=*))" -I  
"cn,givenName,objectclass,samAccountName"
```

Running this command exports all users in the Export domain into a file named Exportuser.ldf. If you do not have all the required attributes, the import operation does not work. The attributes **objectclass** and **samAccountName** are required, but more can be added as needed.

Note Built-in accounts, such as Administrator, do not have a given name. By default, the LDAP filter used above does not export those accounts. LDIFDE does not support exporting passwords.

Note When you omit the **-s** parameter, LDIFDE chooses a global catalog for exports. Depending on the domain controller placement, this server might be a domain controller for a different domain, and exports might fail. You see this when you examine the output of LDIFDE. In this case, specify a local domain controller of the domain in which the objects are hosted.

Import the organizational units from Export to Import

1. Log on as an Administrator in the Import domain. If you log on using an account that does not have administrative privileges, you may not be able to perform export and import operations against the Active Directory.
2. Open the file Exportou.ldf using Notepad.
3. In Notepad, on the **Edit** menu, click **Replace**.
4. In the **Find what** box type, **Export**. In the **Replace with** box type, **Import**.
5. Click **Replace All**.
6. After you verify that the domain names are replaced, save, and then close the file.
7. At the command prompt, type:

```
ldifde -i -f ExportOU.ldf -s Server2
```

You should see a message stating the number of entries that have been modified and that the command completed successfully.

Note In this situation, you must complete the first step prior to completing the second step so that the OUs are available to contain the users.

Import the users from Export to Import

1. Open the file Exportuser.ldf using Notepad.

- In notepad, open the **Edit** menu and click **Replace**.

Note Remember that in this example, "Export" is the name of the domain from which objects are exported and "Import" is the name of the domain to which objects are imported. You will replace "Export" with the name of the domain you exported from and you will have to replace "Import" with the domain you are importing to.

- In the **Find what** box type, **Export**. In the **Replace with** box, type **Import**.
- Click **Replace All**.
- After you verify that the domain names are replaced, save, and then close the file.
- At the command prompt, type:

```
ldifde -i -f Exportuser.ldf -s Server2
```

- View the newly created contacts using either the Active Directory Users and Computers snap-in tool or using the Windows Address Book.

NOTE: Because LDIFDE does not export passwords, when the users are imported into the directory, the account is disabled and the password is set to null. This is done for security reasons. Also, the account option "User must change password at next logon" is selected.

Exporting objects from an entire forest

If you need to export OUs, users, and groups from an entire forest, you may either run the above LDIFDE export commands against each domain in the forest, or alternatively, run the query once against the global catalog (GC). To do this, ensure that the domain controller that is specified by the `-s` switch is a GC, and additionally, specify the GC port using the `-t` switch. The GC port number is 3268.

For example, to perform the export operation outlined against a GC, the LDIFDE command would be:

```
ldifde -f Exportuser.ldf -s Server1 -t 3268 -d "dc=Export,dc=com" -p subtree -r  
"(&(objectCategory=person)(objectClass=User)(givenname=*))" -l  
"cn,givenName,objectclass,sAMAccountName"
```

Note To Modify attributes in AD it is very important that the following format be followed for the import file, especially the "-" on a single line followed by a completely blank line on the next line. To import this file all you need to do is run: `ldifde -i -f Import.ldf -s Server`.

Sample Import/Modify File Format:

```
dn: CN=Jane Doe,OU=Staff,DC=microsoft,DC=com changetype: modify replace:  
extensionAttribute1 extensionAttribute1: Staff - dn: CN=John  
Doe,OU=Staff,DC=microsoft,DC=com changetype: modify replace: extensionAttribute1  
extensionAttribute1: Staff -
```

Importing multivalued attributes

Import files with multivalued attributes have the form of:

```
dn: distinguishedName  
changetype: modify  
replace: attribute  
modify replace: attribute [this is the attribute to be changed]  
attribute: value1  
attribute: value2  
attribute: valueN [where N is the next value] - [hyphen, required to terminate input file]
```

example:
dn: CN=Connector for Lotus Notes (EX1),CN=Connections,CN=First Routing Group,CN=Routing Groups,CN=First Administrative Group,CN=Administrative Groups,CN=VINC,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=vinc,DC=biz changetype: modify replace:
msExchExportContainersLinked msExchExportContainersLinked: OU=GroupWise Users,DC=vinc,DC=biz
msExchExportContainersLinked: OU=AD Users,DC=vinc,DC=biz msExchExportContainersLinked:
CN=Users,DC=vinc,DC=biz

APPLIES TO

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

Keywords: kbhowto KB237677

© 2007 Microsoft Corporation. All rights reserved.