



[TechNet Home](#) > [Windows Server TechCenter](#) > [Identity and Directory Services](#) > [Active Directory](#) > [Step By Step](#)

Step-by-Step Guide to Active Directory Bulk Import and Export

Published: September 17, 2004

This guide introduces batch administration of the Active Directory® service, using both the Lightweight Directory Access Protocol (LDAP) Data Interchange Format (LDIF) utility and several sample programs written using the Microsoft Visual Basic® Scripting Edition (VBScript) development system.

On This Page

- ↓ [Introduction](#)
- ↓ [Overview](#)
- ↓ [Using VBScript and ADSI](#)
- ↓ [Appendix – Using LDIFDE](#)
- ↓ [Additional Resources](#)

Introduction

Step-by-Step Guides

The Windows Server 2003 Deployment step-by-step guides provide hands-on experience for many common operating system configurations. The guides begin by establishing a common network infrastructure through the installation of Windows Server 2003, the configuration of Active Directory, the installation of a Windows XP Professional workstation, and finally the addition of this workstation to a domain. Subsequent step-by-step guides assume that you have this common network infrastructure in place. If you do not want to follow this common network infrastructure, you will need to make appropriate modifications while using these guides.

The common network infrastructure requires the completion of the following guides.

- [Part I: Installing Windows Server 2003 as a Domain Controller](#)
- [Part II: Installing a Windows XP Professional Workstation and Connecting It to a Domain](#)

Once the common network infrastructure is configured, any of the additional step-by-step guides may be employed. Note that some step-by-step guides may have additional prerequisites above and beyond the common network infrastructure requirements. Any additional requirements will be noted in the specific step-by-step guide.

Microsoft Virtual PC

The Windows Server 2003 Deployment step-by-step guides may be implemented within a physical lab environment or through virtualization technologies like Microsoft Virtual PC 2004 or Microsoft Virtual Server 2005. Virtual machine technology enables customers to run multiple operating systems concurrently on a single physical server. Virtual PC 2004 and Virtual Server 2005 are designed to increase operational efficiency in software testing and development, legacy application migration, and server consolidation scenarios.

The Windows Server 2003 Deployment step-by-step guides assume that all configurations will occur within a physical lab environment, although most configurations can be applied to a virtual environment without modification.

Applying the concepts provided in these step-by-step guides to a virtual environment is beyond the scope of this document.

Important Notes

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, places, or events is intended or should be inferred.

This common infrastructure is designed for use on a private network. The fictitious company name and Domain Name System (DNS) name used in the common infrastructure are not registered for use on the Internet. You should not use this name on a public network or Internet.

The Active Directory service structure for this common infrastructure is designed to show how Windows Server 2003 Change and Configuration Management works and functions with Active Directory. It was not designed as a model for configuring Active Directory for any organization.

[↑ Top of page](#)

Overview

This guide introduces batch administration of the Active Directory service, using both the LDAP Data Interchange Format (LDIF) utility and a simple program you can write using the Visual Basic Scripting Edition (VBScript) development system. Using these tools, you can export, import, and modify objects such as users, contacts, groups, servers, printers, and shared folders.

In this guide, you will perform the following tasks.

- Perform batch operations using the Ldifde.exe utility. Export users into a file format compatible with the LDIF standard format. Perform a batch modification of all the users. Use LDIF to create a new user and delete a user.
- Perform batch operations using Active Directory Service Interfaces (ADSI) and VBScript. Export users into a text file using a script written with ADSI and VBScript. Use VBScript to perform a batch modification of all the users. Use VBScript to create a new user and delete a user.

Prerequisites

- [Part 1: Installing Windows Server 2003 as a Domain Controller](#)
- [Step-by-Step Guide to Setting Up Additional Domain Controllers](#)

Using the Ldifde.exe Utility

The LDIF is an Internet draft standard for a file format that can be used for performing batch operations on directories that conform to the LDAP standards. LDIF can be used to export and import data, allowing batch operations such as Add, Modify, and Delete to be performed in Active Directory. A utility called Ldifde.exe is included in the Windows Server 2003 operating system to support batch operations based on the LDIF standard.

You can also use the Ldifde.exe utility to extend the schema, export Active Directory user and group information to other applications or services, and populate Active Directory with data from other directory services.

Note: The Ldifde.exe utility is the recommended method for pushing tested schema extensions into a production environment.

Exporting Objects

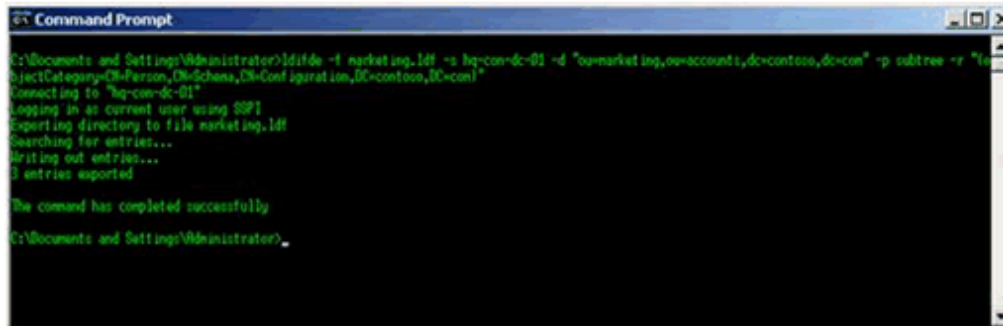
You can use the Ldifde.exe utility to export all objects in the Marketing organizational unit (OU), created in "[Step-by-Step Guide to Common Infrastructure Part 1](#)". This example searches the OU for certain objects and creates a file containing the names of those objects.

To export objects using LDIF

1. Log on as a **Domain Administrator**.
2. Click the **Start** button, point to **All Programs**, point to **Accessories**, and then click **Command Prompt**.
3. At the **command prompt**, type:

```
ldifde -f marketing.ldf -s hq-con-dc-01 -d "ou=marketing,ou=accounts,dc=contoso,dc=com" -p
subtree -
r "(objectCategory=CN=Person,CN=Schema,CN=Configuration,DC=contoso,DC=com)"
```

4. Press **Enter**. Your results should be similar to those shown in Figure 1.



```
Command Prompt
C:\Documents and Settings\Administrator>ldifde -f marketing.ldf -s hq-con-dc-01 -d "ou=marketing,ou=accounts,dc=contoso,dc=com" -p subtree -r "(objectCategory=CN=Person,CN=Schema,CN=Configuration,DC=contoso,DC=com)"
Connecting to "hq-con-dc-01"
Logging in as current user using SSP1
Exporting directory to file marketing.ldf
Searching for entries...
Writing out entries...
3 entries exported

The command has completed successfully
C:\Documents and Settings\Administrator>
```

Figure 1. Exporting Directory Data

[See full-sized image](#)

The previous command creates an LDIF file named Marketing.ldf, by connecting to the server named HQ-CON-DC-01 and executing a subtree search of the Marketing OU for all objects of the category Person. The output file will be located in the root of the Documents and Settings directory of the current user.

Note: objectCategory is an indexed attribute designed to enhance search performance.

You can use this LDIF file to perform a batch import of all the objects from the Marketing OU into any other LDAP-compatible directory. Some attributes may not be applicable to other implementations of LDAP. In particular, if you use this mechanism to import the objects into another Active Directory, some attributes must be omitted because they are automatically generated during object creation. (If they are not specifically omitted, the operation will fail.)

For example, the LDIFDE command that is used to omit these attributes is identical to the previous command, except for the addition of the **-m** parameter.

```
ldifde -f marketing.ldf -s hq-con-dc-01 -d "ou=marketing,ou=accounts,dc=contoso,dc=com" -p
subtree -
r "(objectCategory=CN=Person,CN=Schema,CN=Configuration,DC=contoso,DC=com)" -m
```

Modifying Objects

In the following example, the entire Marketing organization has moved to a new office address. LDIF is used to perform a batch modification for all user objects in the Marketing organization by altering the state, street, locality, and postal code attributes.

To modify objects using LDIF and Notepad

1. Click the **Start** button, point to **All Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the **command prompt**, type the following command to extract the required entries.

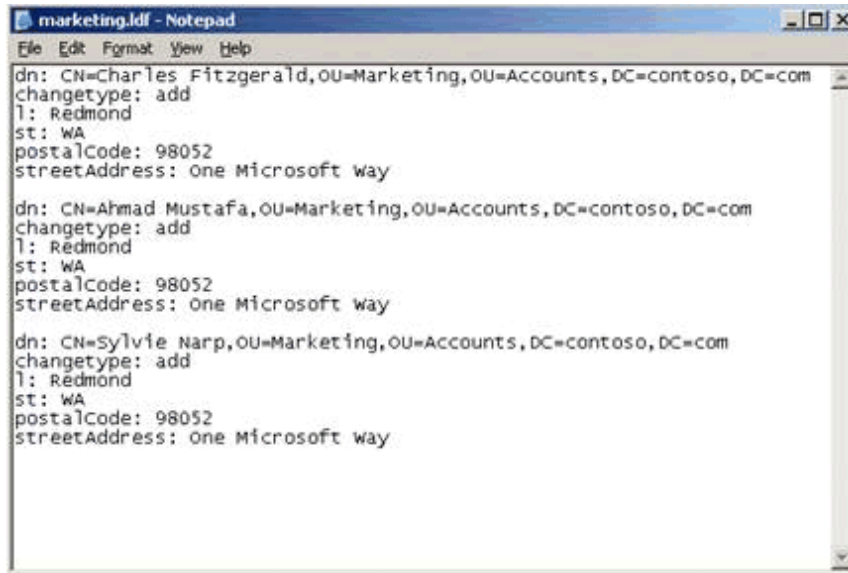
```
ldifde -f marketing.ldf -s hq-con-dc-01 -d "ou=marketing,ou=accounts,dc=contoso,dc=com" -p
subtree -r
"(objectCategory=CN=Person,CN=Schema,CN=Configuration,DC=contoso,DC=com)" -l
"1,st,streetaddress,postalcode"
```

Note: Entries for City, State, Address, and PostalCode have not been defined in the common network infrastructure guides for the user objects within the Marketing OU. It is advisable to populate these fields

for each user object in the Marketing OU prior to performing this export.

3. Press **Enter**.
4. Open the **marketing.ldf** file with **Notepad**.

Note: If you populated each user object with data, your results should be similar to those shown in Figure 2.

A screenshot of a Notepad window titled 'marketing.ldf - Notepad'. The window contains three entries for user objects in LDIF format. Each entry starts with a 'dn:' line, followed by 'changetype: add', and then several attribute-value pairs: 'l:', 'st:', 'postalCode:', and 'streetAddress:'. The entries are for Charles Fitzgerald, Ahmad Mustafa, and Sylvie Narp, all located in the Marketing OU of the Accounts department at contoso.com. The address for all three is 'One Microsoft way' in Redmond, WA 98052.

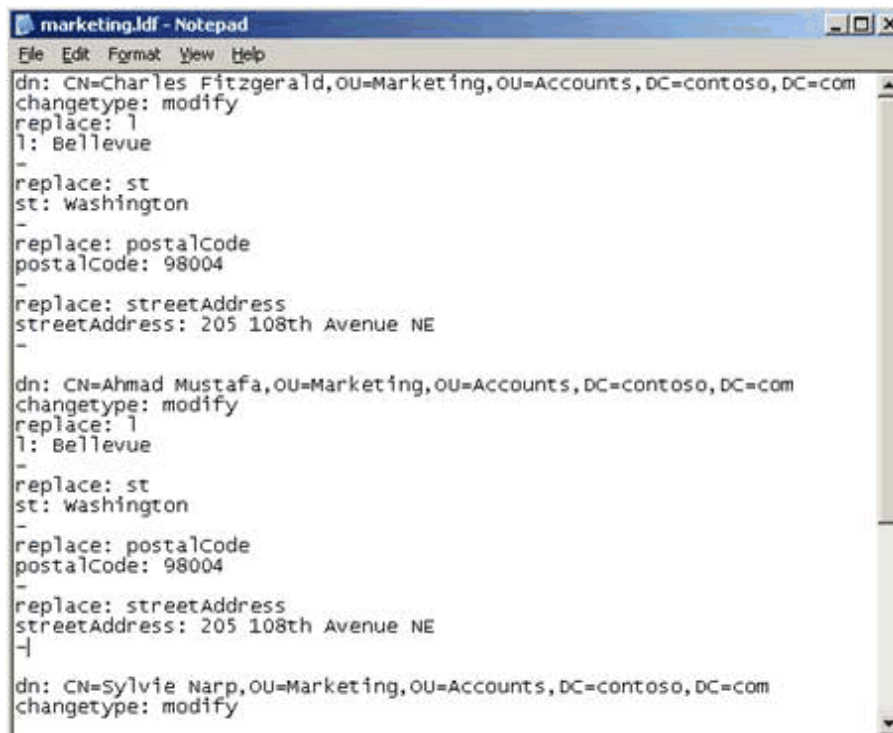
```
marketing.ldf - Notepad
File Edit Format View Help
dn: CN=Charles Fitzgerald,OU=Marketing,OU=Accounts,DC=contoso,DC=com
changetype: add
l: Redmond
st: WA
postalCode: 98052
streetAddress: One Microsoft way

dn: CN=Ahmad Mustafa,OU=Marketing,OU=Accounts,DC=contoso,DC=com
changetype: add
l: Redmond
st: WA
postalCode: 98052
streetAddress: One Microsoft way

dn: CN=Sylvie Narp,OU=Marketing,OU=Accounts,DC=contoso,DC=com
changetype: add
l: Redmond
st: WA
postalCode: 98052
streetAddress: One Microsoft way
```

Figure 2. Reviewing an LDF File

5. In **Notepad**, modify each user object entry in **Marketing.ldf** so that it is similar to Figure 3. **Note:** You must save the file as an .ldf file.

A screenshot of a Notepad window titled 'marketing.ldf - Notepad'. The window shows the same three user object entries as in Figure 2, but they have been modified. The 'changetype' is now 'modify', and the 'l:', 'st:', 'postalCode:', and 'streetAddress:' attributes have been replaced with new values: 'Bellevue', 'Washington', '98004', and '205 108th Avenue NE' respectively. The entries are for Charles Fitzgerald, Ahmad Mustafa, and Sylvie Narp.

```
marketing.ldf - Notepad
File Edit Format View Help
dn: CN=Charles Fitzgerald,OU=Marketing,OU=Accounts,DC=contoso,DC=com
changetype: modify
replace: l
l: Bellevue
-
replace: st
st: Washington
-
replace: postalCode
postalCode: 98004
-
replace: streetAddress
streetAddress: 205 108th Avenue NE
-

dn: CN=Ahmad Mustafa,OU=Marketing,OU=Accounts,DC=contoso,DC=com
changetype: modify
replace: l
l: Bellevue
-
replace: st
st: Washington
-
replace: postalCode
postalCode: 98004
-
replace: streetAddress
streetAddress: 205 108th Avenue NE
-

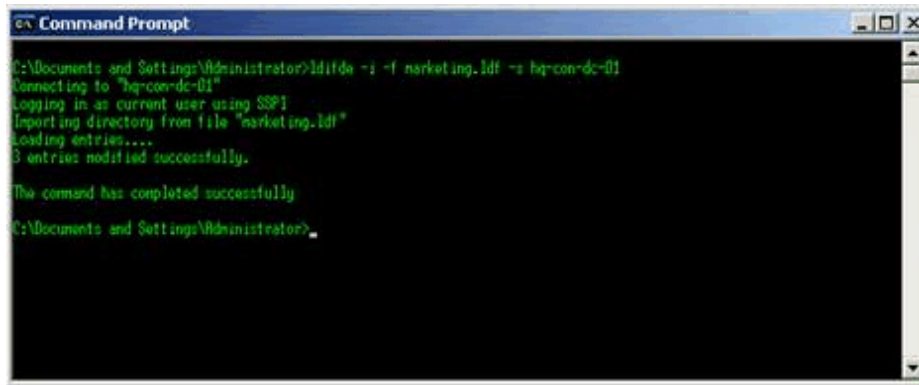
dn: CN=Sylvie Narp,OU=Marketing,OU=Accounts,DC=contoso,DC=com
changetype: modify
```

Figure 3. Modifying an LDF Import File

6. Close **Notepad**. In the **Command Prompt** window, type:

```
ldifde -i -f marketing.ldf -s hq-con-dc-01
```

7. Press **Enter**. Your results should be similar to those shown in Figure 4.



```

C:\Documents and Settings\Administrator>ldifde -i -f marketing.ldf -s hq-con-dc-01
Connecting to "hq-con-dc-01"
Logging in as current user using SSP1
Importing directory from file "marketing.ldf"
Loading entries....
3 entries modified successfully.

The command has completed successfully.
C:\Documents and Settings\Administrator>

```

Figure 4. Successful Import of an LDF File

8. To confirm that the user object attributes have been modified accordingly, use the Active Directory Users and Computers snap-in. (For help with using this snap-in, see the [Step-by-Step Guide to Managing the Active Directory](#).)

Note: Another utility called Csvde.exe performs the same export functions as the Ldifde.exe utility, but uses a comma-separated file format. Import operations with this utility are "add" only; it does not offer the ability to modify or delete objects. The comma-separated value (CSV) file format is supported by applications such as Microsoft Excel.

Creating and Deleting Objects

In the following examples, LDIF is used to add and delete users from Active Directory.

To create a new user using LDIF

1. Click the **Start** button, click **Run**, type **Notepad Newuser.ldf**, and then click **OK**. When prompted, click **Yes** to create a new file.
2. Add the following text to the file.

```
dn: CN=Pilar Ackerman,OU=Marketing,OU=Accounts,DC=contoso,DC=com
```

```
changetype: add
```

```
cn: Pilar Ackerman
```

```
objectClass: user
```

```
samAccountName: Pilar
```

```
givenName: Pilar
```

```
sn: Ackerman
```

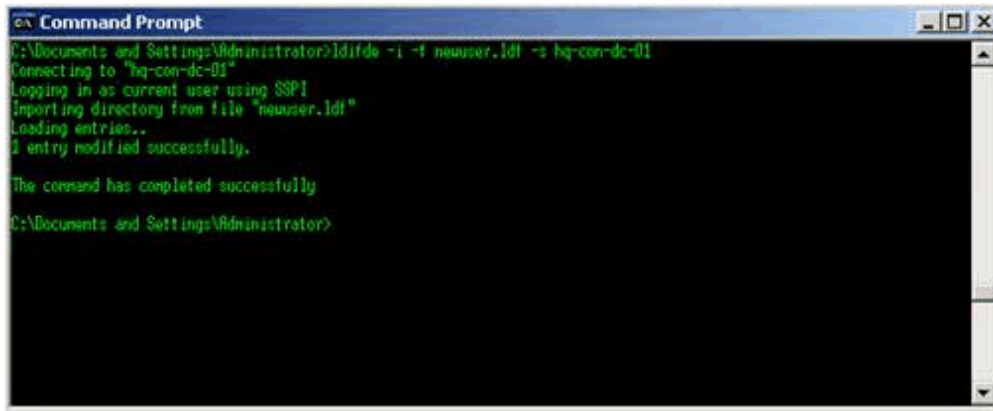
3. Save, and then close the **newuser.ldf** file. Before proceeding with user object creation, verify the file

saved to the Documents and Settings directory.

4. Type the following in the **Command Prompt** window.

```
ldifde -i -f newuser.ldf -s hq-con-dc-01
```

5. Press **Enter**. When complete, the Command Prompt window will confirm the modification as shown in Figure 5.



```
Command Prompt
C:\Documents and Settings\Administrator>ldifde -i -f newuser.ldf -s hq-con-dc-01
Connecting to "hq-con-dc-01"
Logging in as current user using SSP1
Importing directory from file "newuser.ldf"
Loading entries..
1 entry modified successfully.

The command has completed successfully

C:\Documents and Settings\Administrator>
```

Figure 5. Adding a New User

To delete a user using LDIF

1. Click the **Start** button, click **Run**, type **Notepad Deleteuser.ldf**, and then click **OK**. When prompted, click **Yes** to create a new file.
2. Add the following text to the file.

```
dn: CN=Pilar Ackerman,OU=Marketing,OU=Accounts,DC=contoso,DC=com  
changetype: delete
```

3. Save, and then close the **deleteuser.ldf** file.
4. Type the following in the **Command Prompt** window.

```
ldifde -i -f deleteuser.ldf -s hq-con-dc-01
```

[↑ Top of page](#)

Using VBScript and ADSI

ADSI makes it easy to develop directory-enabled applications. In conjunction with the Windows Script Host, batch directory operations can be scripted using VBScript or Microsoft JScript® development software. In this guide, the procedures that were described in the previous section (which used LDIF) are performed using simple applications written in VBScript.

Note that these scripts do not include any error checking, nor are they meant to provide a programmer's reference to VBScript and ADSI. All of the examples included here assume that you are logged on with the proper credentials on a machine that is a member of the target domain. It is possible in ADSI to explicitly specify credentials and a target domain. After each procedure, confirm that the entries have been modified by checking the Active Directory Users and Computers snap-in.

Exporting Objects

In this example, a text editor, such as Notepad, is used to create a VBScript program. The script searches the

Marketing OU and creates a text file that lists all of the user objects and a subset of their attributes.

To create and execute an export script

1. Click the **Start** button, click **Run**, type **Notepad export.vbs**, and then click **OK**. When prompted, click **Yes** to create a new file. Copy the following text into **export.vbs**.

```
'Global variables
  Dim oContainer
  Dim OutPutFile
  Dim FileSystem
'Initialize global variables
  Set FileSystem = WScript.CreateObject("Scripting.FileSystemObject")
  Set OutPutFile = FileSystem.CreateTextFile("marketing.txt", True)
  Set oContainer=GetObject("LDAP://OU=Marketing,OU=Accounts,DC=contoso,DC=com")
'Enumerate Container
  EnumerateUsers oContainer
'Clean up
  OutPutFile.Close
  Set FileSystem = Nothing
  Set oContainer = Nothing
  WScript.Echo "Finished"
  WScript.Quit(0)
Sub EnumerateUsers(oCont)
  Dim oUser
  For Each oUser In oCont
    Select Case LCase(oUser.Class)
      Case "user"
        If Not IsEmpty(oUser.distinguishedName) Then
          OutPutFile.WriteLine "dn: " & oUser.distinguishedName
        End If
        If Not IsEmpty(oUser.name) Then
          OutPutFile.WriteLine "name: " & oUser.Get ("name")
        End If
        If Not IsEmpty(oUser.streetAddress) Then
          OutPutFile.WriteLine "streetAddress: " & oUser.streetAddress
        End If
        If Not IsEmpty(oUser.l) Then
          OutPutFile.WriteLine "l: " & oUser.l
        End If
        If Not IsEmpty(oUser.st) Then
          OutPutFile.WriteLine "st: " & oUser.st
        End If
        If Not IsEmpty(oUser.postalcode) Then
          OutPutFile.WriteLine "postalcode: " & oUser.postalcode
        End If
      Case "organizationalunit", "container"
        EnumerateUsers oUser
    End Select
    OutPutFile.WriteLine
  Next
End Sub
```

2. Save **export.vbs**, and then close **Notepad**.
3. In the **Command Prompt** window, type **export.vbs**, and then press **Enter**.

Note: Executing **export.vbs** creates the **Marketing.txt** file, which contains a list of users and a subset of their attributes.

With appropriate modification, this script can be used with any application that supports the Microsoft Component Object Model (COM) and Visual Basic technologies. Such applications include Visual Basic, Excel, and Microsoft Access. Scripting is also supported by Internet Explorer and Internet Information Services.

Modifying Objects

In this example, all users address attributes will be changed within the Marketing OU. A simple VBScript program

is used to perform a batch modification for all user objects in the Marketing organization. The script alters the state, street, locality, and postal code attributes.

To create and execute a modify object script

1. Click the **Start** button, click **Run**, type **Notepad modify.vbs**, and then click **OK**. When prompted, click **Yes** to create a new file. Copy the following text into **modify.vbs**.

```
Dim oContainer
  Set oContainer=GetObject("LDAP://OU=Marketing,OU=Accounts,DC=contoso,DC=com")
ModifyUsers oContainer
'cleanup
  Set oContainer = Nothing
  WScript.Echo "Finished"
  WScript.Quit
Sub ModifyUsers(oObject)
  Dim oUser
  oObject.Filter = Array("user")
  For Each oUser in oObject
    oUser.Put "st","Washington"
    oUser.Put "streetAddress","One Microsoft Way"
    oUser.Put "postalCode","98052"
    oUser.Put "l","Redmond"
    oUser.SetInfo
  Next
End Sub
```

2. Save **modify.vbs**, and then close **Notepad**.
3. In the **Command Prompt** window, type **modify.vbs**, and then press **Enter**.

Creating and Deleting Objects

In this example, VBScript is used to add a new user to the Marketing organization. This example illustrates how easy it is to use ADSI and VBScript to programmatically access the directory. Note that in this example, only a limited set of attributes are configured during the user creation.

To create and execute a create object script

1. Click the **Start** button, click **Run**, type **Notepad add.vbs**, and then click **OK**. When prompted, click **Yes** to create a new file. Copy the following text into **add.vbs**.

```
Dim oContainer
Dim oUser
Set oContainer=GetObject("LDAP://OU=Marketing,OU=Accounts,DC=contoso,DC=com")
'Create user
  Set oUser = oContainer.Create("User","CN=Pilar Ackerman")
'Assign values to user attributes
  oUser.Put "samAccountName","Pilar"
  oUser.Put "givenName","Pilar"
  oUser.Put "sn","Ackerman"
  oUser.Put "userPrincipalName","pilar@contoso.com"
  oUser.SetInfo
'Clean up
  Set oUser = Nothing
  Set oContainer = Nothing
  WScript.Echo "Finished"
  WScript.Quit
```

2. Save **add.vbs**, and then close **Notepad**.
3. In the **Command Prompt** window, type **add.vbs**, and then press **Enter**.

To create and execute a delete object script

1. Click the **Start** button, click **Run**, type **Notepad delete.vbs**, and then click **OK**. When prompted, click **Yes** to create a new file. Copy the following text into **delete.vbs**.

```
Dim oContainer
Set oContainer=GetObject("LDAP://OU=Marketing,OU=Accounts,DC=contoso,DC=com")
'Delete user
oContainer.Delete "user","CN=Pilar Ackerman"
'Clean up
Set oContainer = Nothing
WScript.Echo "Finished"
WScript.Quit
```

2. Save **delete.vbs**, and then close **Notepad**.
3. In the **Command Prompt** window, type **delete.vbs**, and then press **Enter**.

[↑ Top of page](#)

Appendix – Using LDIFDE

Syntax

```
Ldifde [-i] [-f FileName] [-s ServerName] [-c String1 String2] [-v] [-j Path] [-t PortNumber] [-d BaseDN] [-r LDAPFilter] [-p Scope] [-l LDAPAttributeList] [-o LDAPAttributeList] [-g] [-m] [-n] [-k] [-a UserDistinguishedName Password] [-b UserName Domain Password] [-?]
```

Parameters

-i

- Specifies import mode. If not specified, the default mode is export.

-f FileName

- Identifies the import or export file name.

-s ServerName

- Specifies the domain controller to perform the import or export operation. By default, Ldifde will run on the domain controller on which Ldifde is installed.

-c String1 String2

- Replaces all occurrences of String1 with String2. This is generally used when importing data from one domain to another and the distinguished name of the export domain (String1) needs to be replaced with that of the import domain (String2).

-v

- Sets verbose mode.

-j Path

- Sets the log file location. The default is the current path.

-t PortNumber

- Specifies an LDAP port number. The default LDAP port is 389. The global catalog port is 3268.

-d BaseDN

- Sets the distinguished name of the search base for data export.

-r LDAPFilter

- Creates an LDAP search filter for data export. For example, to export all users with a particular surname, you can use the following filter -r (and(objectClass=User)(sn=Surname))

-p Scope

- Sets the search scope. Search scope options are Base, OneLevel, or SubTree.

-l LDAPAttributeList

- Sets the list of attributes to return in the results of an export query. If this parameter is omitted, all attributes are returned.

-o LDAPAttributeList

- Sets the list of attributes to omit from the results of an export query. This is typically used when exporting objects from Active Directory and then importing them into another LDAP-compliant directory. If attributes are not supported by another directory, you can omit the attributes from the result set using this option.

-g

- Omits paged searches.

-m

- Omits attributes that only apply to Active Directory objects such as the ObjectGUID, objectSID, pwdLastSet, and samAccountType attributes.

-n

- Omits export of binary values.

-k

- Ignores errors during the import operation and continues processing. The following is a complete list of ignored errors:

- object is already a member of the group
- object class violation (meaning the specified object class does not exist), if the object being imported has no other attributes
- object already exists
- constraint violation
- attribute or value already exists
- no such object

-a UserDistinguishedName Password

- Sets the command to run using the supplied UserDistinguishedName and Password. By default, the command will run using the credentials of the user currently logged on to the network.

-b UserName Domain Password

- Sets the command to run using the supplied UserName Domain Password. By default, the command will run using the credentials of the user currently logged on to the network.

-?

- Displays the command menu.

Remarks

When creating the import file to use with the Ldifde command, use a changeType value to define the type of

changes the import file will contain. The following changeType values are available:

Value	Description
Add	Specifies that new content is contained in the import file.
modify	Specifies that existing content has been modified in the import file.
delete	Specifies that content has been deleted in the import file.

The following is an example of an LDIF import file format using the add value.

```
DN: CN=SampleUser,DC=DomainName
```

```
changetype: add
```

```
CN: SampleUser
```

```
description: DescriptionOfFile
```

```
objectClass: User
```

```
sAMAccountName: SampleUser
```

Examples

To retrieve only the distinguished name, common name, first name, surname, and telephone number of the returned objects, type:

```
-l DistinguishedName, CN, GivenName, SN, Telephone
```

To omit the object GUID, type:

```
-o whenCreated, whenChanged, objectGUID
```

Formatting legend

Format	Meaning
<i>Italic</i>	Information that the user must supply
Bold	Elements that the user must type exactly as shown
Ellipsis (...)	Parameter that can be repeated several times in a command line
Between brackets ([])	Optional items
Between braces ({ }); choices separated by pipe (). Example: {even odd}	Set of choices from which the user must choose only one
Courier font	Code or program output

[↑ Top of page](#)

Additional Resources

For more information, see the following resources.

- The LDAP Data Interchange Format (LDIF) - Technical Specification at <http://www.ietf.org/rfc/rfc2849.txt>
- Microsoft Visual Basic Scripting technologies at <http://msdn.microsoft.com/library/default.asp?url=/library/en->

[us/script56/html/vtorivbscript.asp](#)

- For the latest information about Windows Server 2003, see the Windows Server 2003 Web site at <http://www.microsoft.com/windowsserver2003>

[↑ Top of page](#)

[Manage Your Profile](#)

© 2007 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

