

The logo for Microsoft Windows Server 2003 R2, featuring the Microsoft logo icon and the text "Microsoft Windows Server 2003 R2".

Microsoft® Windows Server™ 2003 R2

Step-by-Step Guide to Deploying ADAM

Microsoft Corporation

Published: September 2005

Author: Jim Groves

Editor: Carolyn Eller

Abstract

The Active Directory® Application Mode (ADAM) directory service in Microsoft® Windows Server™ 2003 R2 provides rich integration of directory support and security, scalability, and native Lightweight Directory Access Protocol (LDAP) support to directory-aware applications. ADAM supports a number of LDAP capabilities that are targeted for information technology (IT) professionals and application developers. With this step-by-step guide, you will be able to set up ADAM and get it running quickly on Windows Server 2003 R2, so that you can explore some of its new and important features.

Microsoft

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005 Microsoft Corporation. All rights reserved.

Active Directory, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

Step-by-Step Guide to Deploying ADAM	5
Requirements for ADAM	6
Installing ADAM.....	7
Using the ADAM Administration Tools.....	18
Stopping and Restarting an ADAM Instance	18
Using the ADAM ADSI Edit Administration Tool	19
Configuring the ADAM Schema Snap-in Administration Tool	24
Using ADSchemaAnalyzer	26
Using Active Directory to ADAM Synchronizer.....	28
Setting Up Application Data	29
Step 1: Adding Optional User Classes to the ADAM Schema	30
Step 2: Extending the ADAM Schema to Support an Application	31
Step 3: Importing Application Data into an ADAM Instance	32
Using an Application with ADAM	34
Querying Data with Windows Address Book.....	34
Managing OUs, Groups, and Users in ADAM	39
Step 1: Create an OU	40
Step 2: Create a group	41
Step 3: Create an ADAM user	42
Step 4: Add a user to a group.....	44
Disabling and Enabling ADAM User Accounts.....	47
Managing Directory Partitions in ADAM.....	47
Connecting and Binding to an ADAM Instance Using Ldp.exe	48
Adding an Application Directory Partition	49
Deleting an Application Directory Partition	51
Managing Authorization in ADAM.....	53
Viewing Effective Permissions.....	54
Granting Permissions	55
Denying Permissions.....	56

Managing Authentication in ADAM	58
Binding as a Windows Principal	59
Setting the Password of an ADAM User.....	59
Binding as an ADAM Principal.....	61
Binding Through an ADAM Proxy Object	61
Binding Security and ADAM Proxy Objects	62
Creating and Binding with an ADAM Proxy Object	63
Demonstrating ADAM Proxy Object Functionality	65
Backing Up and Restoring Active Directory Application Mode (ADAM)	66
Backing up an ADAM Instance	66
Removing an ADAM Instance	67
Restoring an ADAM Instance	68
Managing Configuration Sets.....	70
Installing a Replica Using the Active Directory Application Mode Setup Wizard	70
Installing a Replica from Media by Using Unattended Installation	72
Configuring the Replication Schedule	74
Causing Immediate Replication of a Directory Partition	76
Administering ADAM Programmatically	77
Administering ADAM Programmatically Through Visual Basic Scripts	77
Administering ADAM Programmatically Through the System.DirectoryServices API... ..	79
Administering ADAM Proxy Objects Programmatically	81

Step-by-Step Guide to Deploying ADAM

This document is a step-by-step guide for deploying Active Directory Application Mode (ADAM).

The Active Directory® directory service in Microsoft® Windows® 2000 and in Microsoft® Windows Server™ 2003 is the fastest growing directory service for intranets and extranets, as a result of its rich integration of directory support and security, scalability, and native Lightweight Directory Access Protocol (LDAP) support. Active Directory in Windows Server 2003 builds on that success by supporting a number of new LDAP capabilities that are targeted for information technology (IT) professionals and applications developers. ADAM is one of these new capabilities. Organizations, independent software vendors (ISVs), and developers who want to integrate their applications with a directory service now have an additional capability in Active Directory that provides numerous benefits.

With this document, you will be able to set up ADAM and get it running quickly, so that you can explore some of its new and important features.

Specifically, in this scenario you perform the following tasks for this walk-through:

1. Set up the lab environment, where you install and configure ADAM.
2. Install ADAM.

Next, you explore its features for adding and managing data:

1. Set up application data so that you can use ADAM with an application.
2. Query and retrieve the application data that you imported into your ADAM instance.
3. Practice creating and managing organizational units (OUs), groups, and users in ADAM.
4. Manually add and then delete an application directory partition.
5. Grant and deny user permissions.

Finally, you practice administrative tasks:

1. Practice binding to an ADAM instance in several ways.
2. Practice performing the basic functions of using ADAM such as starting and stopping an instance of ADAM.
3. Back up, remove, and restore an ADAM instance.

4. Install replicas of ADAM.
5. Perform ADAM tasks programmatically.

 **Note**

It is recommended that you first use the steps provided in this guide in a test lab environment. Step-by-step guides are not necessarily meant to be used to deploy Windows Server features without accompanying documentation. You should use this guide with discretion when using it as a stand-alone document.

Requirements for ADAM

Before you start using the procedures in this guide, do the following regarding system requirements:

- Have available at least one test computer on which you can install ADAM. For the purposes of following the exercises in this guide, you can install ADAM on computers running any of the following operating systems:
 - Windows Server 2003 R2, Standard Edition
 - Windows Server 2003 R2, Enterprise Edition
 - Windows Server 2003 R2, Datacenter Edition

The computer must have 50 MB free disk space.

 **Note**

You can also run ADAM on computers running Windows XP and earlier versions of Windows Server 2003. The ADAM version that runs on these operating systems is available at "[Windows Server 2003 Active Directory Application Mode](http://go.microsoft.com/fwlink?linkid=17797)" on the Microsoft Web site (<http://go.microsoft.com/fwlink?linkid=17797>).

- Obtain a copy of the ADAM download, which includes lab files for use with this guide. For this exercise, use only the lab files in the download, but install the ADAM application itself from the Windows Server 2003 R2 product CD. The ADAM download is available at the [Microsoft Download Center](http://go.microsoft.com/fwlink?linkid=29359) (<http://go.microsoft.com/fwlink?linkid=29359>). Run the download to extract the lab files required for the exercises in this guide.
- Log on with an administrator account.

- For the purposes of this guide, you can install replica ADAM instances on your first test computer, or you can install them on a second computer, if you have one available.
- If you previously installed an earlier version of ADAM, you must uninstall the earlier version from the computer before installing the new version of ADAM.

Installing ADAM

You can install an ADAM instance either by using the Active Directory Application Mode Setup Wizard or by using the ADAM unattended installation process. In the first exercise, you use the Active Directory Application Mode Setup Wizard to install ADAM. In [Managing Configuration Sets](#), you use an unattended installation to install an ADAM replica.

Note

To install ADAM, you must log on to your computer using an account that belongs to the local Administrators group.

In this exercise, you first install ADAM, and then you install an ADAM instance by using the Active Directory Application Mode Setup Wizard.

To install ADAM

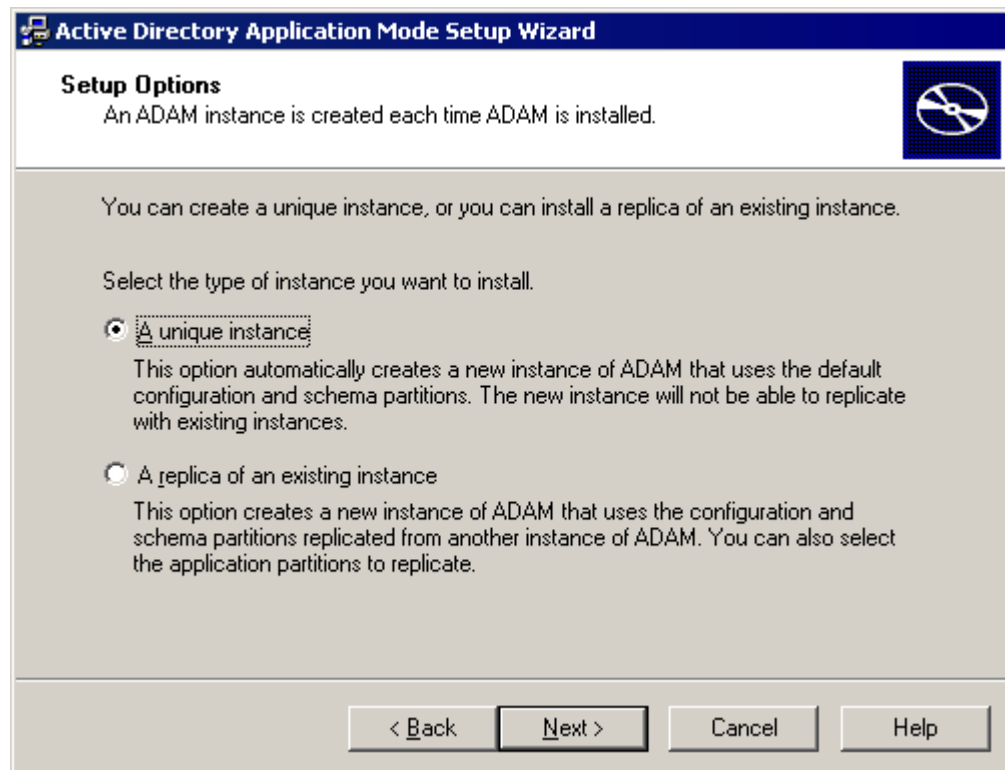
1. To install ADAM, log on as an administrator, click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select the check box next to **Active Directory Services**, and then click **Details**.
4. Select the check box next to **Active Directory Application Mode (ADAM)**, click **OK**, and then click **Next**.
5. Review the message that appears. Based on the contents of message, do one of the following:
 - If the message "You have successfully completed the Windows Component Wizard" appears, click **Finish**.
 - If an error message appears, make a note of the error, click **Finish**, and then review the ADAM event messages in Event Viewer.

► **To install an ADAM instance by using the Active Directory Application Mode Setup Wizard**

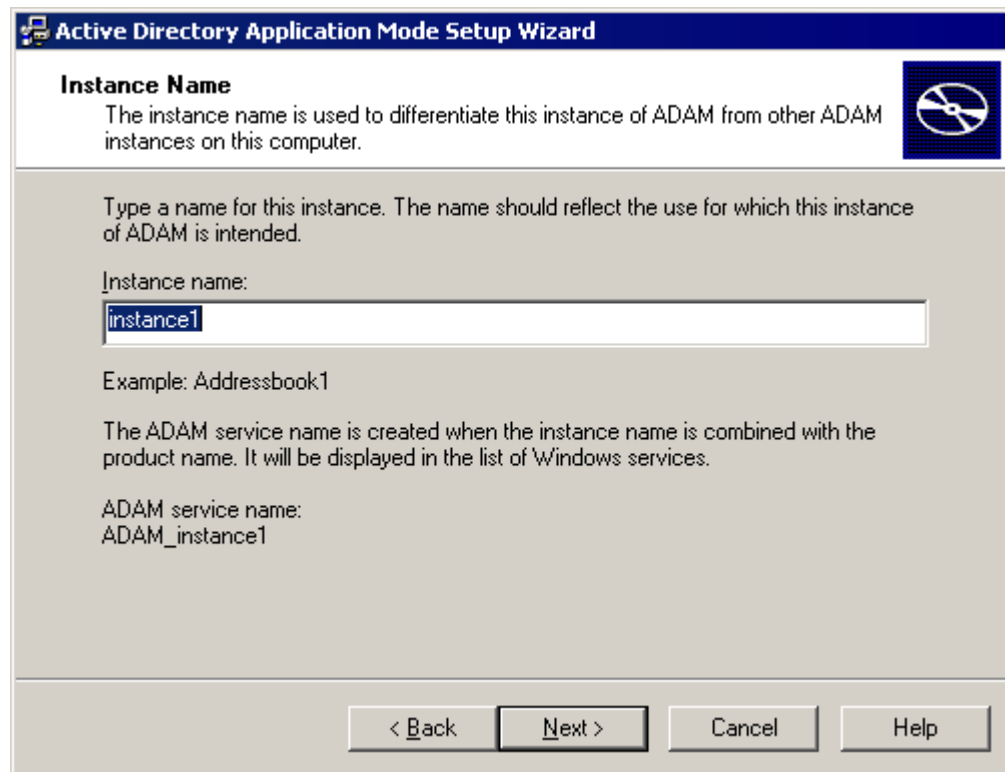
1. To start the Active Directory Application Mode Setup Wizard, click **Start**, point to **All Programs**, point to **ADAM**, and then click **Create an ADAM instance**. The first page of the Active Directory Application Mode Setup Wizard looks like the following:



2. On the **Welcome to the Active Directory Application Mode Setup Wizard** page, click **Next**.
3. On the **Setup Options** page, you can choose whether to install a unique ADAM instance or join an existing configuration set. Because you are installing the first ADAM instance, click **A unique instance** (as shown in the following), and then click **Next**. Later, you will create additional ADAM instances and join them in a configuration set.



4. On the **Instance Name** page, provide a name for the ADAM instance that you are installing. This name is used on the local computer to uniquely identify the ADAM instance. For this exercise, simply accept the default name of instance1, and then click **Next**.



The screenshot shows a Windows-style dialog box titled "Active Directory Application Mode Setup Wizard". The main heading is "Instance Name". Below the heading is a paragraph: "The instance name is used to differentiate this instance of ADAM from other ADAM instances on this computer." To the right of this text is a blue square icon with a white circular arrow. Below the paragraph is a text box with the label "Instance name:" and the text "instance1" entered. Underneath the text box is the text "Example: Addressbook1". Below that is another paragraph: "The ADAM service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services." Below this is the text "ADAM service name:" followed by "ADAM_instance1". At the bottom of the dialog box are four buttons: "< Back", "Next >", "Cancel", and "Help".

5. On the **Ports** page, specify the communications ports that the ADAM instance uses to communicate. ADAM can communicate using both LDAP and Secure Sockets Layer (SSL); therefore, you must provide a value for each port. For this exercise, accept the default values of 389 and 636, and then click **Next**.

Ports

Computers will connect to this instance of ADAM using specific ports on all of the IP addresses associated with this computer.

The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

If you plan to install Active Directory on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number:

SSL port number:

< Back Next > Cancel Help

 **Note**

If you install ADAM on a computer where either of the default ports is in use, the Active Directory Application Mode Setup Wizard automatically locates the first available port, starting at 50000. For example, Active Directory uses ports 389 and 636, as well as ports 3268 and 3269 on global catalog servers. Therefore, if you install ADAM on a domain controller, the Active Directory Application Mode Setup Wizard provides a default value of 50000 for the LDAP port and 50001 for the SSL port.

- On the **Application Directory Partition** page, you can create an application directory partition (or naming context) by clicking **Yes, create an application directory partition**. Or, you can click **No, do not create an application directory partition**, in which case you must create an application directory partition manually after installation. For this exercise, click **Yes, create an application directory partition**. When you create an application directory partition, you must provide a distinguished name for the new partition. For this exercise, type **o=Microsoft,c=US** as the distinguished name (as shown below), and then click **Next**.

Active Directory Application Mode Setup Wizard

Application Directory Partition
An application directory partition stores application-specific data.

Do you want to create an application directory partition for this instance of ADAM?

No, do not create an application directory partition
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.

Yes, create an application directory partition
Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name:
CN=Partition1,DC=Woodgrove,DC=CDM

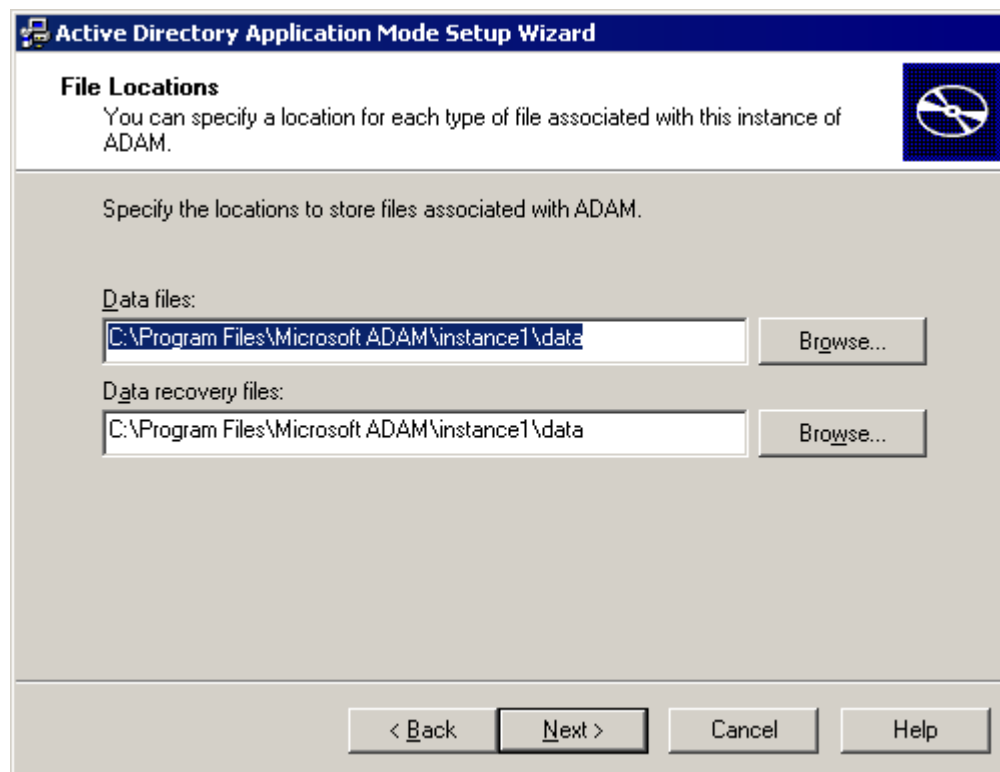
Partition name:
o=Microsoft,c=US

< Back Next > Cancel Help

 **Note**

ADAM supports both X.500-style and Domain Name System (DNS)-style distinguished names for top-level directory partitions.

7. On the **File Locations** page, you can view and change the installation directories for ADAM data and recovery (log) files. By default, ADAM data and recovery files are installed in %ProgramFiles%\Microsoft ADAM*instancename*\data, where *instancename* represents the ADAM instance name that you specify on the **Instance Name** page. For this exercise, click **Next** to accept the default file locations.



Important

When installing ADAM on a computer running Windows XP, you must install these files on the same logical volume. When installing ADAM on Windows Server 2003 and Windows Server 2003 R2 in a production environment, it is recommended that you install the files on separate physical disks.

Note

ADAM setup installs program files and administration tools in %windir%\ADAM.

8. On the **Service Account Selection** page, you select an account to be used as the service account for ADAM. The account that you select determines the security context in which the ADAM instance runs. Unless you are installing ADAM on a domain controller, the Active Directory Application Mode Setup Wizard defaults to the Network Service account. For this exercise, click **Next** to accept the **Network service account** default. Or, if you are installing ADAM on a domain controller, click **This account**, and then select a domain user account to use as the ADAM service account.

Active Directory Application Mode Setup Wizard

Service Account Selection
 ADAM performs operations using the permissions associated with the account you select.

Set up ADAM to perform operations using the permissions associated with the following account.

Network service account
 ADAM has the permissions of the default Windows service account.

This account:
 ADAM has the permissions of the selected account. Ensure that the account you select is set up to run as a service.

User name:

Password:

< Back Next > Cancel Help

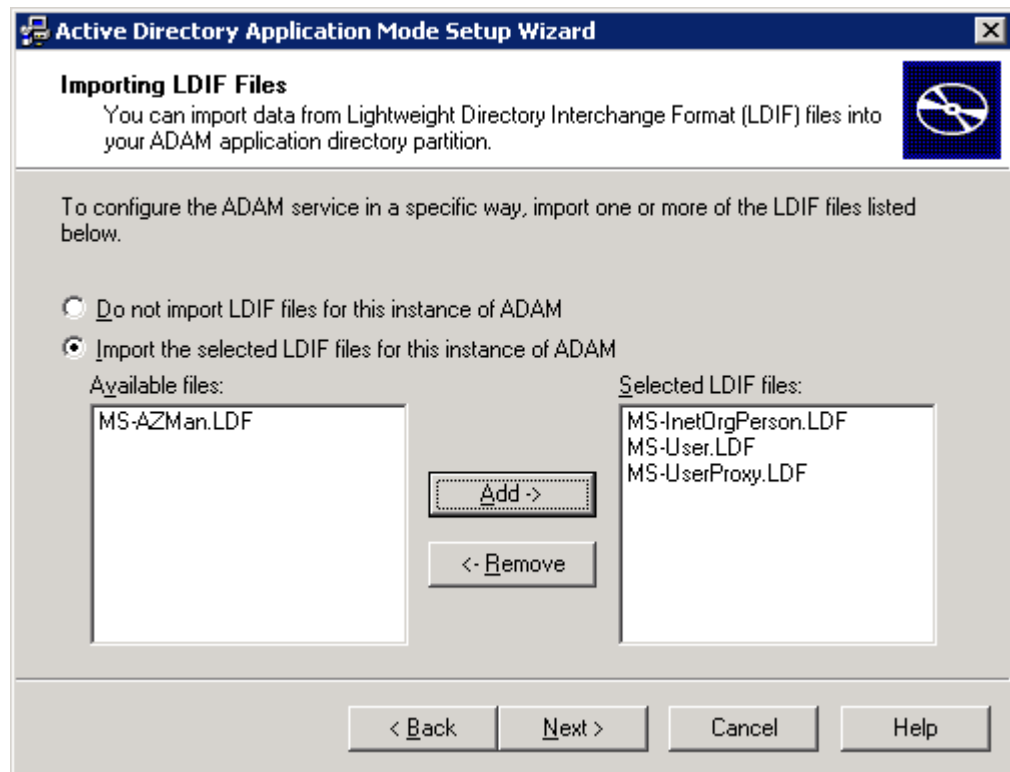
 **Note**

You can change the ADAM service account after ADAM is installed by using the Dsmgmt command-line tool. When you install ADAM on a domain controller, you must select a domain user account as the ADAM service account.

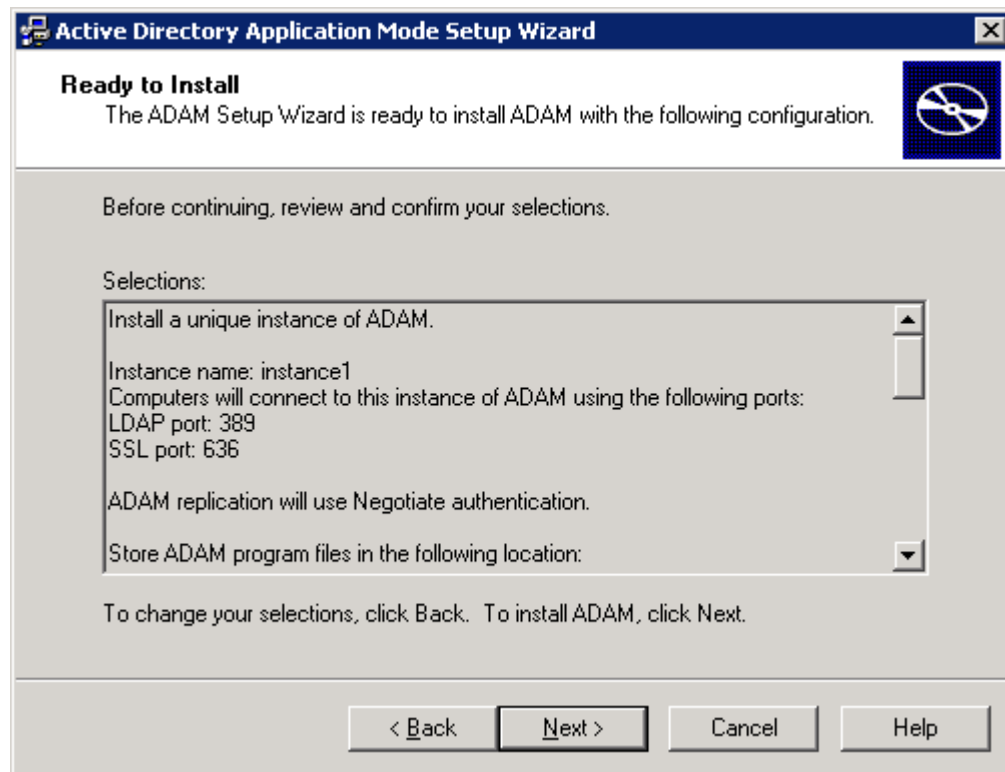
9. On the **ADAM Administrators** page, you select a user or group to become the default administrator for the ADAM instance. The user or group that you select will have full administrative control of the ADAM instance. By default, the Active Directory Application Mode Setup Wizard specifies the currently logged on user. You can change this selection to any local or domain account or group on your network. For this exercise, click the default value of **Currently logged on user**, and then click **Next**.



10. On the **Importing LDIF Files** page, you can import into the ADAM schema two .ldf files containing **user** class object definitions. Importing these **user** class object definitions is optional. However, these object definitions are required later in this guide so, you should import these definitions now:
- Click **Import the selected LDIF files for this instance of ADAM.**
 - Click **MS-InetOrgPerson.LDF**, and then click **Add.**
 - Click **MS-User.LDF**, and then click **Add.**
 - Click **MS-UserProxy.LDF**, click **Add**, and then click **Next.**



11. The **Ready to Install** page gives you an opportunity to review your installation selections. After you click **Next**, the Active Directory Application Mode Setup Wizard begins copying files and setting up ADAM on your computer.



12. When the Active Directory Application Mode Setup Wizard finishes installing ADAM, it displays this message: “You have successfully completed the Active Directory Application Mode Setup Wizard.” When the **Completing the Active Directory Application Mode Setup Wizard** page appears, click **Finish** to close the wizard.

 **Note**

If the Active Directory Application Mode Setup Wizard does not complete successfully, an error message describing the reason for the failure appears on the Summary page.

If an error occurs in the Active Directory Application Mode Setup Wizard before the **Summary** page, you can review the error message that appears. In addition, you can click **Start**, click **Run**, and type either of the following:

%windir%\Debug\adamsetup.log

%windir%\Debug\adamsetup_loader.log

The Adamsetup.log and Adamsetup_loader.log files contain information that can help you troubleshoot the cause of an ADAM setup failure.

Using the ADAM Administration Tools

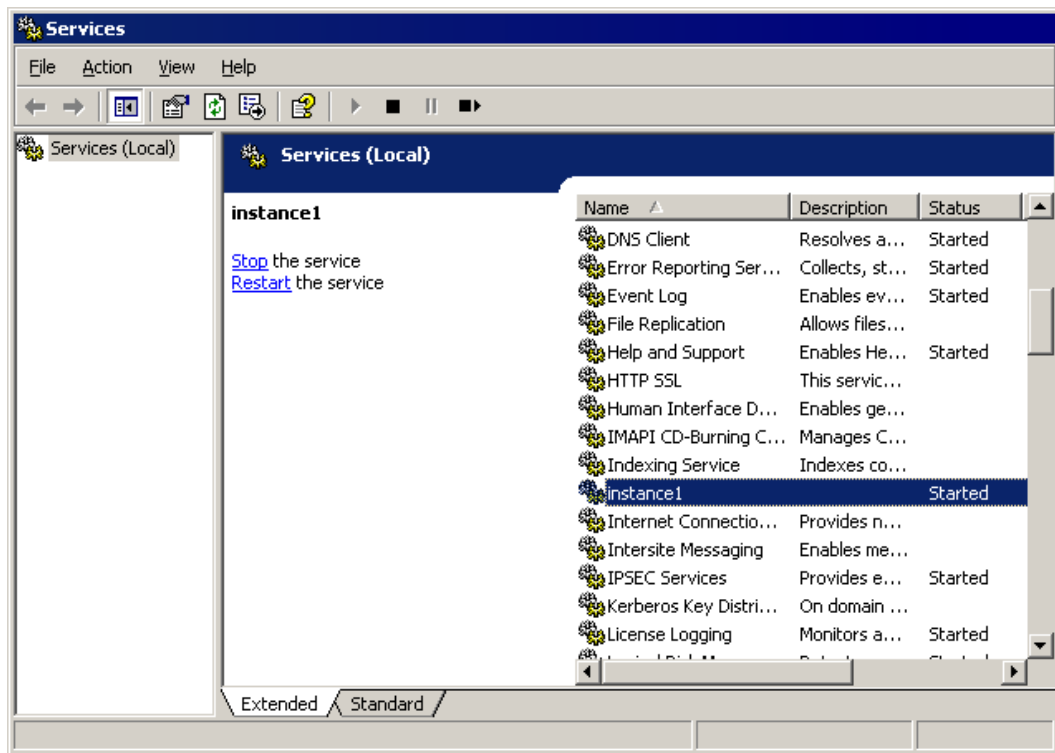
An ADAM instance runs as a standard user service, rather than as a system service, and it can be stopped and started through the Services snap-in in Microsoft Management Console (MMC). In addition, ADAM includes several administration tools for general administration tasks. In the following exercises, you:

- Use the Services snap-in to stop and restart your ADAM instance.
- Use ADAM ADSI Edit (ADAM-adsiedit.msc) to browse your directory.
- Configure the ADAM Schema snap-in.
- Use ADSchemaAnalyzer to produce a file that can be used to extend a schema with elements from another schema.
- Use Active Directory to ADAM Synchronizer to copy data from Active Directory to an ADAM instance.

Stopping and Restarting an ADAM Instance

▶ To stop and restart an ADAM instance by using the Services snap-in

1. Click **Start**, point to **Administrative Tools**, and then click **Services**.
2. The ADAM instance that you just installed is listed in the details pane of the Services snap-in, along with other services on the computer. ADAM instances are listed in Services by their name, which in this case is instance1. Click the ADAM instance that you installed, as shown in the following:



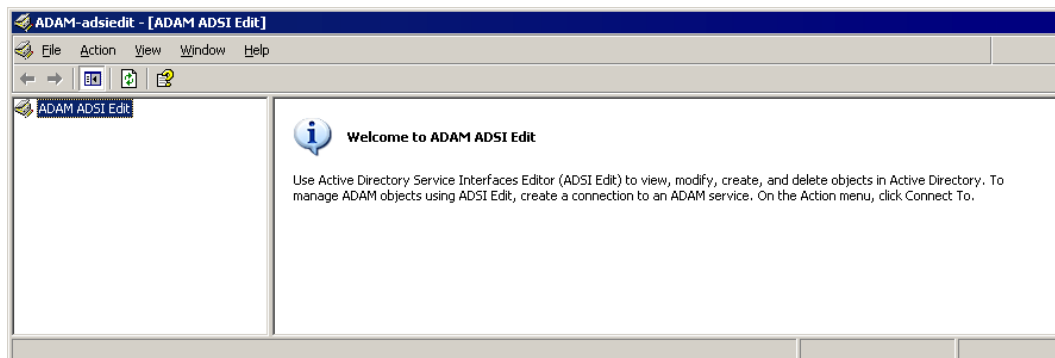
3. To stop the ADAM instance, on the **Action** menu, click **Stop**.
4. After the ADAM instance is stopped, on the **Action** menu, click **Start** to restart the ADAM instance.

Using the ADAM ADSI Edit Administration Tool

The main administration tool for ADAM is ADAM ADSI Edit. In this exercise, you use ADAM ADSI Edit to bind to, view, and browse your ADAM instance.

► To bind to, view, and browse an ADAM instance using ADAM ADSI Edit

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM ADSI Edit**.
2. In the console tree, click **ADAM ADSI Edit**. The **ADAM ADSI Edit** snap-in looks like the following:



3. On the **Action** menu, click **Connect to**. The **Connection Settings** dialog box appears.
4. In **Connection name**, you can type a label under which this connection will appear in the console tree of ADAM ADSI Edit. For this connection, type:

ADAM demo

5. In **Server name**, type the host or DNS name of the computer on which the ADAM instance is running.

 **Note**

Because, in this exercise, ADAM is running on the local computer, you can use localhost as the server name.

6. In **Port**, type the LDAP or SSL communication ports in use by ADAM. Or, as in this case, accept the default value of 389.

 **Note**

To list the port numbers used by ADAM instances, click **Start**, point to **All Programs**, point to **ADAM**, click **ADAM Tools Command Prompt**, and then, at the command prompt, type: **dsdbutil "list instances" quit**

7. Under **Connect to the following node**, you can connect to a well-known naming context, such as the configuration or schema directory partition, or you can specify the distinguished name of a partition to which you want to connect. For this exercise, click **Distinguished name (DN) or naming context**, and type:

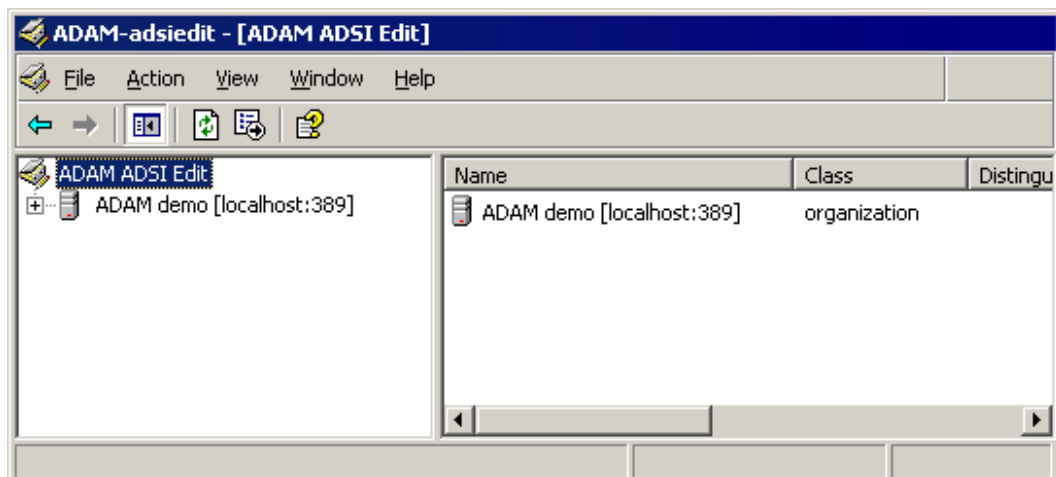
o=Microsoft,c=US

This is the distinguished name of the application partition that you created during setup.

8. Under **Connect using these credentials**, click **The account of the currently**

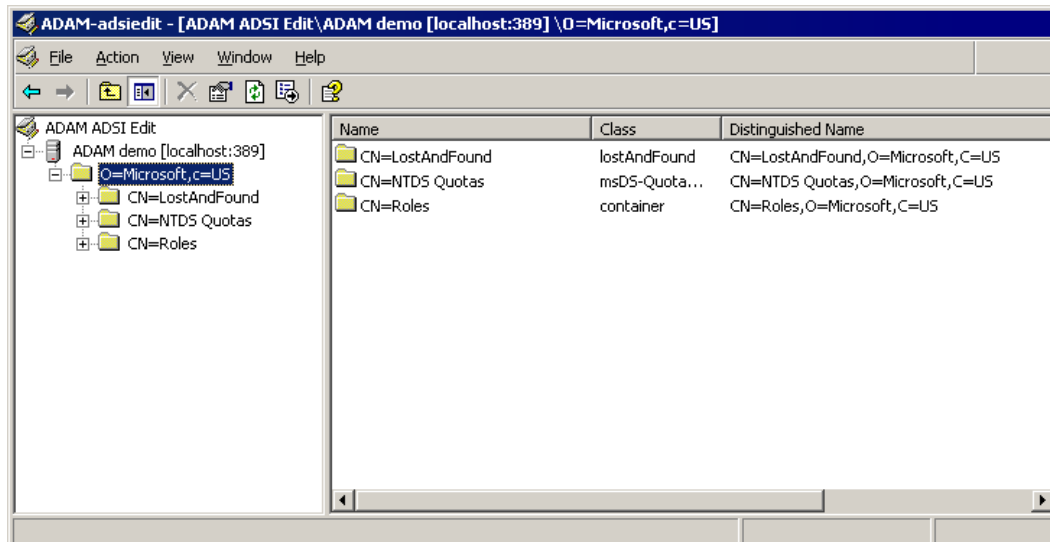
logged on user. The **Connection Settings** dialog box now looks like the following:

9. Click **OK**. The **ADAM ADSI Edit** snap-in looks like the following:



10. In the console tree, double-click **ADAM demo**, and then double-click

O=Microsoft,c=US. The **ADAM ADSI Edit** snap-in now shows the application directory partition:



11. In the console tree, click any container to view the objects in that container. For example, click **CN=Roles**.
12. To open a different directory partition on the ADAM instance, in the console tree, click **ADAM ADSI Edit**, and then, on the **Action** menu, click **Connect to**.
13. Fill out the **Connection Settings** dialog box as shown, and then click **OK**.

Connection Settings

Connection name:

Server name: Port:

Connect to the following node:

Distinguished name (DN) or naming context:

Well-known naming context:

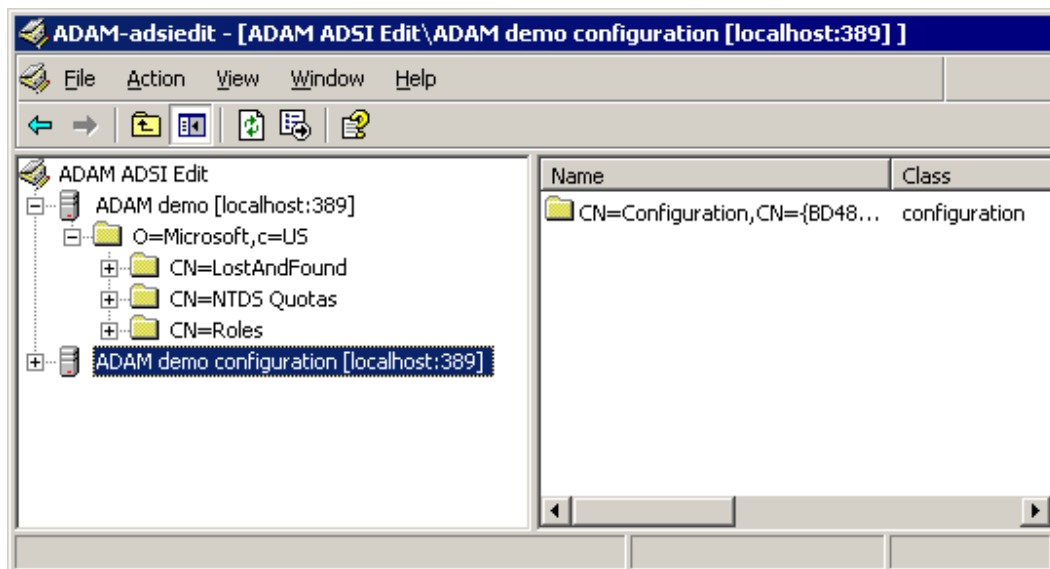
Connect using these credentials:

The account of the currently logged on user

This account:
 User name: Password:

OK Cancel

The **Connection Settings** dialog box now looks like the following:



You can now browse the contents of the configuration directory partition of your ADAM instance.

14. To close ADAM ADSI Edit, on the **File** menu, click **Exit**.

Configuring the ADAM Schema Snap-in Administration Tool

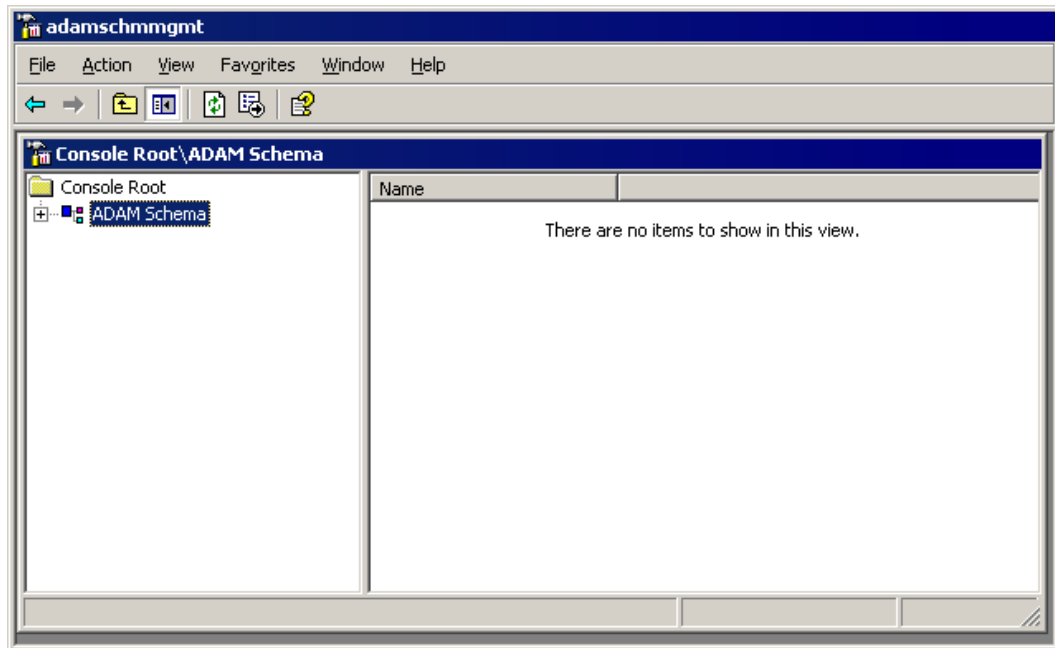
You can use another ADAM administration tool, the ADAM Schema snap-in, to administer the ADAM schema. If you have ever used the Active Directory Schema snap-in, the ADAM Schema snap-in should look very familiar to you. Before you can use the ADAM Schema snap-in, you need to create an MMC file for it, as described in this procedure.

▶ To create an MMC file for the ADAM Schema snap-in

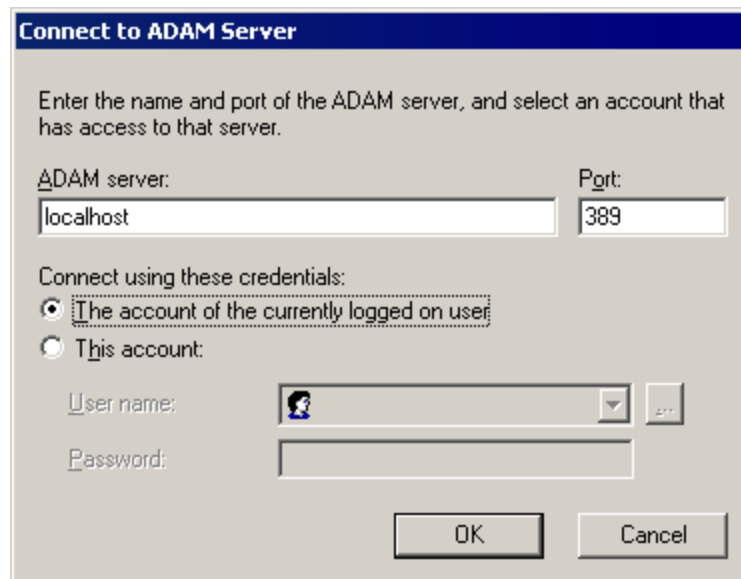
1. Click **Start**, click **Run**, type **mmc /a**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In **Available Standalone Snap-ins**, click **ADAM Schema**, click **Add**, click **Close**, and then click **OK**.
4. To save this console, on the **File** menu, click **Save**.
5. In **File name**, type the following, and then click **Save**.

%windir%\system32\adamschmmgmt.msc

The **ADAM Schema** snap-in looks like the following:

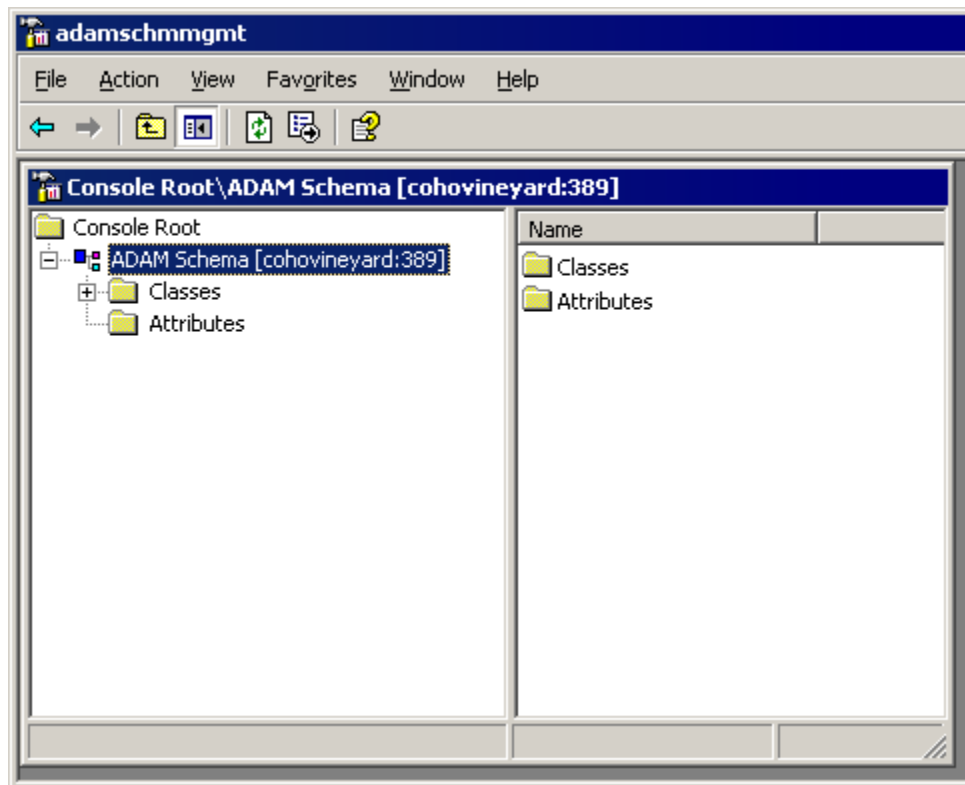


- To connect to your ADAM instance through ADAM Schema, in the console tree, right-click **ADAM Schema**, click **Change ADAM Server**, and then complete the dialog box as follows:



- Click **OK**. The ADAM Schema snap-in now looks like the following. You can browse

and view the ADAM schema classes and attributes:



8. To create a shortcut for the ADAM Schema snap-in on your **Start** menu:
 - a. Right-click **Start**, click **Open All Users**, double-click the **Programs** folder, and then double-click the **ADAM** folder.
 - b. On the **File** menu, point to **New**, and then click **Shortcut**.
 - c. In the **Create Shortcut Wizard**, in **Type the location of the item**, type **adamschmmgmt.msc**, and then click **Next**.
 - d. On the **Select a Title for the Program** page, in **Type a name for this shortcut**, type **ADAM Schema**, and then click **Finish**.

Using ADSchemaAnalyzer

You can use ADSchemaAnalyzer to help migrate the Active Directory schema to ADAM, from one ADAM instance to another, or from any LDAP-compliant directory to an ADAM instance. You can use ADSchemaAnalyzer to load a target (source) schema, mark the

elements you want to migrate, and then export them to the base ADAM schema. You can also compare the two schemas.

Important

When using ADSchemaAnalyzer to create an LDIF file, you should load both a target and a base schema. Otherwise, the resulting LDIF file might not be usable by the Idifde tool

To create an LDIF file with ADSchemaAnalyzer

1. Click **Start**, point to **All Programs**, point to **ADAM**, click **ADAM Tools Command Prompt**, and then, at the command prompt, type:
adschemaanalyzer
2. To load a target schema, click **File**, and then click **Load target schema**, and then do one of the following:
 - To load the domain Active Directory schema as the target schema, in the dialog box, type your user name, password, and domain, and then click **OK**.
 - To load a different schema (such as the schema of an Active Directory forest or an another LDAP-compliant directory), in the dialog box, type the server name and port of the directory containing the target schema, type your user name ,password, and domain as needed, and then click **OK**.
3. To load the schema of your ADAM instance as the base schema, click **File**, click **Load base schema**, and then in **Server[:port]**, type the server name and port of the ADAM instance.
4. In the dialog box, click **OK**.
5. In the resulting tree, mark all elements that you want to export to your base schema by right-clicking the element and selecting one of the following options:
 - **Auto** automatically marks an element as included or excluded in the export. If an element is marked as **Auto (included)**, you can right-click that element, and then click **Why auto included?** to see the reverse dependency tree for the element.
 - **Included** marks an element so that it is included in the export. ADSchemaAnalyzer marks all related elements, such as superclasses, auxClasses, must/may contains, defaultObjectCategory, and possSuperiors. ADSchemaAnalyzer includes propsets for included attributes and back-links for links.

- **Excluded** marks an element so that it is not included in the export. You can block certain paths in the dependency graph. For example, you might want to import `domainDns`, but not `samAccountDomain` (which is an `auxClass` of `domainDns`). You can exclude a complete element, such as the `samAccountDomain` class, or you can exclude a relationship; for example, you can remove the `auxClass` reference from the `domainDns` class. If you exclude a relationship, any other classes that reference that element continue to include it.
- **Present** means that the element is present on the target server. By default, the top class is marked as present.

6. To create the LDIF file, click **File**, and then click **Create LDIF file**.

You can use the `ldifde` command at the ADAM tools command prompt to import the target schema elements in the LDIF file into the base ADAM schema. The beginning of the LDIF file contains complete instructions for performing this task.

Using Active Directory to ADAM Synchronizer

Active Directory to ADAM Synchronizer is a command-line tool that synchronizes data from an Active Directory forest to a configuration set of an ADAM instance.

Important

Active Directory to ADAM Synchronizer does not synchronize user passwords between Active Directory and ADAM.

There are two prerequisites before Active Directory to ADAM Synchronizer can synchronize data:

- The schema in the ADAM instance must be extended to match schema objects in the Windows Server 2003 Active Directory forest.
- The schema in the ADAM instance must be extended for schema objects that are required by Active Directory to ADAM Synchronizer.

Note

You must use the `-t port_number` option with `ldifde` if the ADAM instance uses a port other than the default port 389.

To use Active Directory to ADAM Synchronizer for the first time

1. Click **Start**, point to **All Programs**, click **ADAM**, and then click **ADAM Tools**

Command Prompt to open a command window in the ADAM directory.

- To extend the ADAM schema to match the default Windows Server 2003 schema objects in Active Directory, at the command prompt, type the following command on a single line, and then press ENTER:

```
Ldifde -i -s localhost -c CN=Configuration,DC=X
#ConfigurationNamingContext -f MS-AdamSchemaW2k3.ldf
```

- To extend the ADAM schema to include schema objects that are required by Active Directory to ADAM Synchronizer, at the command prompt, type the following command on a single line, and then press ENTER:

```
Ldifde -i -s localhost:389 -c CN=Configuration,DC=X
#ConfigurationNamingContext -f MS-AdamSyncMetadata.ldf
```

- Modify the configuration file MS-AdamSyncConf.xml with the appropriate parameters.



Important

Do not delete any unused fields from this file.

- Install the configuration file. At a command prompt, typing the following command, and then press ENTER:

```
ADAMSync /install localhost:389 %windir%\ADAMMS-AdamSyncConf.xml
```

- Synchronize the data from the Active Directory forest to the ADAM configuration set. At a command prompt, typing the following command, and then press ENTER:

```
ADAMSync /sync localhost:389 "o=microsoft,c=US"
```

Use ADAM ADSI Edit to verify that the data has been synchronized.

Setting Up Application Data

In most cases, you extend the ADAM schema with object class and attribute definitions for the kinds of data that you want an application to store. Just as with Active Directory, the schema in ADAM is extensible. You can extend the ADAM schema programmatically or with the Ldifde.exe command-line tool.

In the following exercises, you:

- Step 1: Add optional user classes to the ADAM schema.
- Step 2: Extend the ADAM schema to support an application.
- Step 3: Import application data into an ADAM instance.

 **Note**

You will use the application data that you import in these exercises later with the Windows Address Book application.

Step 1: Adding Optional User Classes to the ADAM Schema

You can add the optional user classes that are provided with ADAM during ADAM setup, or you can add them manually using the Ldifde.exe command-line tool. If you imported the user class definition .ldf files when you ran the Active Directory Application Mode Setup Wizard, you can skip this procedure.

 **To manually add optional user classes to the ADAM schema**

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type the following command, and then press ENTER:

```
ldifde -i -f ms-inetorgperson.ldf -s servername:portnumber -k -j . -c  
"CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
```

where *servername:portnumber* represents the computer name and LDAP communication port of your ADAM instance. Because the ADAM instance is running on your local computer, you can also use localhost as the computer name.

 **Note**

Be sure to use the copy of Ldifde.exe that came with Windows Server 2003 R2, rather than a copy that came with an earlier ADAM release or with Windows Support Tools.

The **ADAM Tools Command Prompt** window should now look like the following:

```

C:\WINDOWS\ADAM>ldifde -i -f ms-inetorgperson.ldf -s localhost:389 -k -j . -c "cn=
n=schema,cn=configuration,dc=x" #schemanamingcontext
Connecting to "localhost:389"
Logging in as current user using SSPI
Importing directory from file "ms-inetorgperson.ldf"
Loading entries.....
-----
67 entries modified successfully.

The command has completed successfully

C:\WINDOWS\ADAM>

```

3. Type the following command, and then press ENTER:

```

ldifde -i -f ms-user.ldf -s servername:portnumber -k -j . -c
"CN=Schema,CN=Configuration,DC=X" #schemaNamingContext

```

The ADAM Tools Command Prompt window now looks like the following:

```

C:\WINDOWS\ADAM>ldifde -i -f ms-user.ldf -s localhost:389 -k -j . -c "cn=schema,
cn=configuration,dc=x" #schemanamingcontext
Connecting to "localhost:389"
Logging in as current user using SSPI
Importing directory from file "ms-user.ldf"
Loading entries.....
-----
67 entries modified successfully.

The command has completed successfully

C:\WINDOWS\ADAM>_

```

After you run these commands, the ADAM schema includes the ADAM and inetOrgPerson user object classes. You can verify this by viewing the ADAM schema with the ADAM Schema snap-in.

Step 2: Extending the ADAM Schema to Support an Application

In this exercise, you extend the ADAM schema again by adding a contacts object class, again by using the ldifde command-line tool.

► **To extend the ADAM schema**

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type the following, and then press **ENTER**:

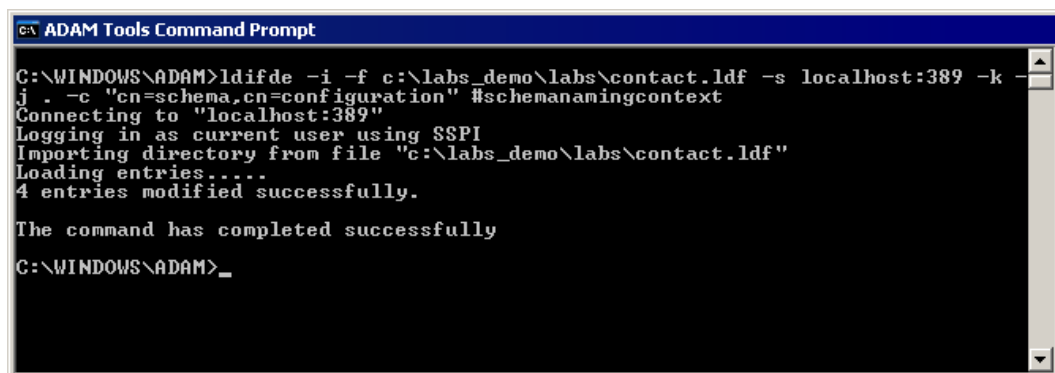
```
ldifde -i -f drive:\path\labs_demo\labs\contact.ldf -s servername:portnumber-k -j . -c "CN=Schema,CN=Configuration" #schemaNamingContext
```

where *drive:\path* represents the location where you saved the ADAM download, and *servername:portnumber* represents the computer name and LDAP communications port of your ADAM instance. Because the ADAM instance is running on your local computer, you can also use localhost as the computer name.

📌 **Note**

Be sure to use the copy of Ldifde.exe that came with the ADAM release, rather than a copy that came with an earlier ADAM release or with Windows Support Tools.

After the command runs, the **ADAM Tools Command Prompt** window looks like the following:



```
C:\WINDOWS\ADAM>ldifde -i -f c:\labs_demo\labs\contact.ldf -s localhost:389 -k -j . -c "cn=schema,cn=configuration" #schemanamingcontext
Connecting to "localhost:389"
Logging in as current user using SSPI
Importing directory from file "c:\labs_demo\labs\contact.ldf"
Loading entries....
4 entries modified successfully.

The command has completed successfully

C:\WINDOWS\ADAM>_
```

Now your ADAM schema also includes the contacts object class, and it is ready for some application data.

Step 3: Importing Application Data into an ADAM Instance

In this exercise, you import some sample data into your ADAM instance using the Ldifde command-line tool. This data is provided with the ADAM download.

▶ **To import application data**

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type the following:

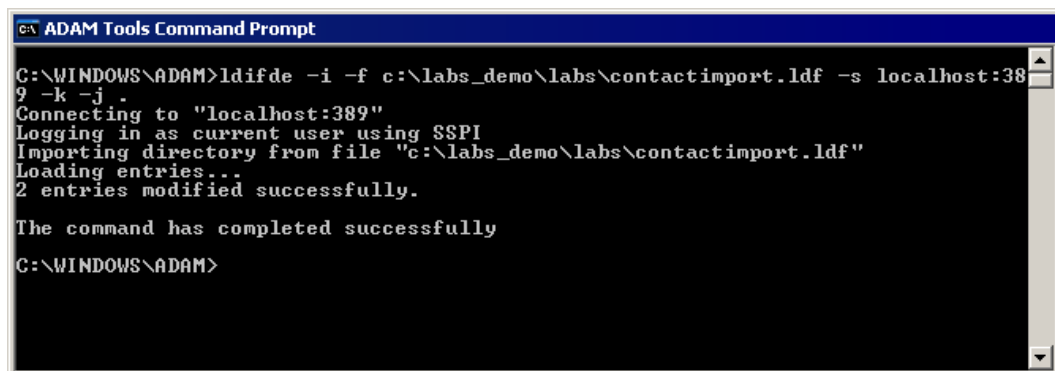
```
ldifde -i -f drive:\path\labs_demo\labs\contactimport.ldf -s  
servername:portnumber-k -j .
```

where *drive:\path* represents the location where your ADAM files are located, and *servername:portnumber* represents the computer name and LDAP communications port of your ADAM instance.

 **Note**

Be sure to use the copy of Ldifde.exe that came with the ADAM release, rather than a copy that came with an earlier ADAM release or with Windows Support Tools.

After the command runs, the **ADAM Tools Command Prompt** window looks like the following:



```
C:\WINDOWS\ADAM>ldifde -i -f c:\labs_demo\labs\contactimport.ldf -s localhost:389 -k -j .  
Connecting to "localhost:389"  
Logging in as current user using SSPI  
Importing directory from file "c:\labs_demo\labs\contactimport.ldf"  
Loading entries...  
2 entries modified successfully.  
  
The command has completed successfully  
C:\WINDOWS\ADAM>
```

 **Note**

Ldifde always reports the number of entries that are imported into the directory. In this case, you can see from the Ldifde output that contactimport.ldf contains two records. For more information about Ldifde, type **ldifde /?** at the command prompt.

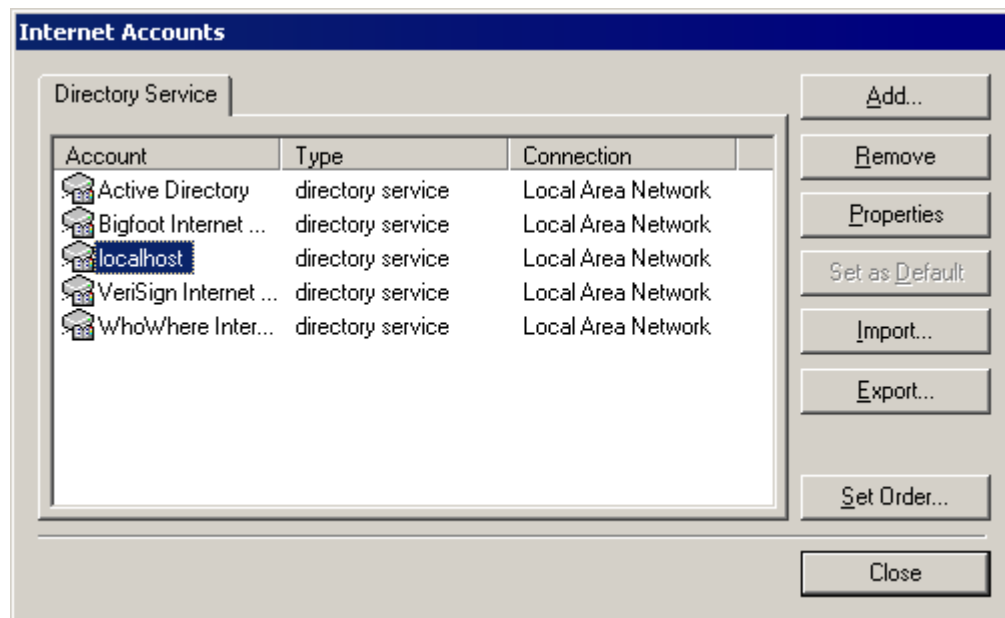
Using an Application with ADAM

In this exercise, you use Windows Address Book, an LDAP-based application, to query and retrieve the application data that you imported into your ADAM instance.

Querying Data with Windows Address Book

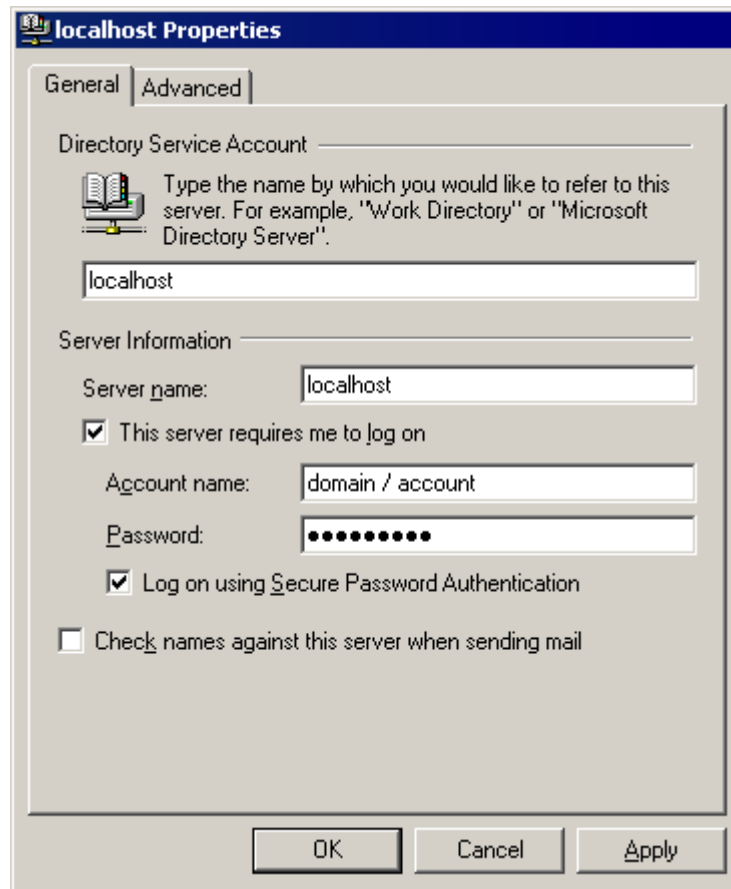
► **To query data with Windows Address Book**

1. Click **Start**, click **Run**, type **wab.exe**, and then click **OK**.
2. On the **Tools** menu, click **Accounts**, and then click **Add**. The Internet Connection Wizard appears.
3. In **Internet directory (LDAP) server**, type **localhost**, click **Next** twice, and then click **Finish**.
4. In the **Internet Accounts** dialog box, on the **Directory Service** tab, double-click **localhost**, as shown in the following:

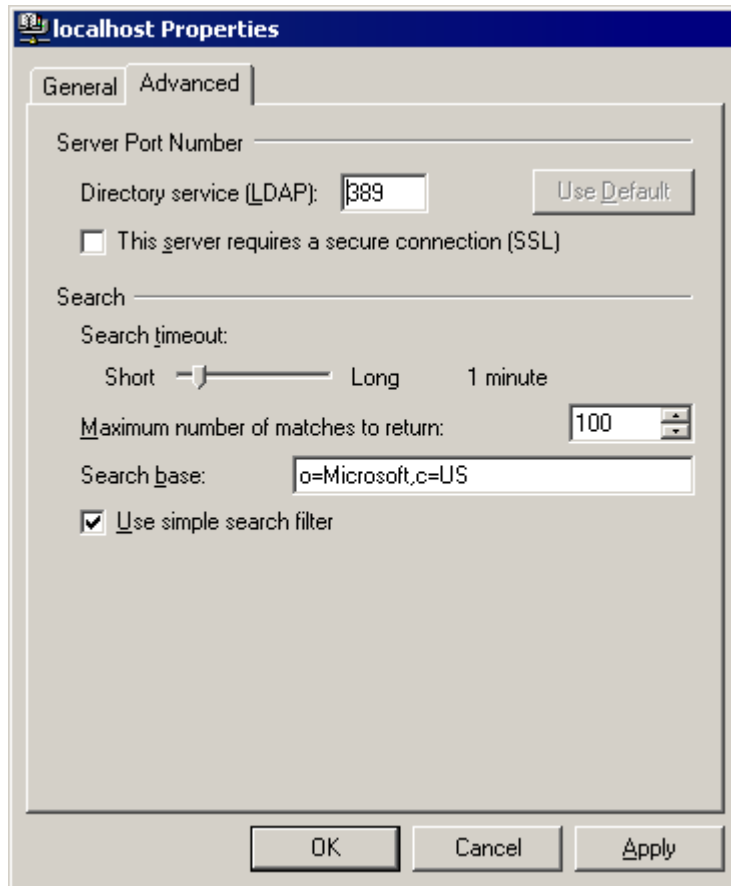


5. Complete the **General** tab in the **localhost Properties** dialog box as shown in the following figure, using the account with which you are currently logged on to the computer. Be sure to select both the **This server requires me to log on** check box

and the **Log on using Secure Password Authentication** check box.



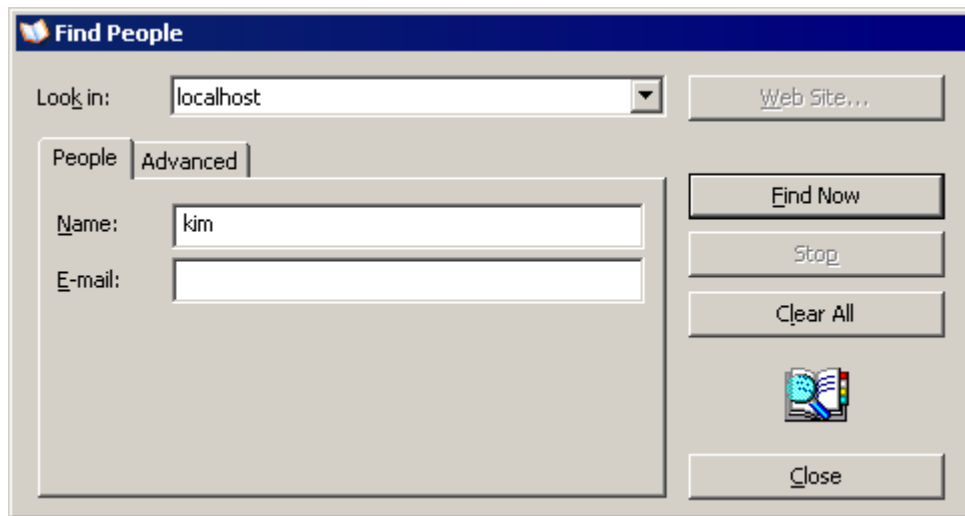
6. Click the **Advanced** tab, and then select the **Use simple search filter** check box. In **Search base**, type **o=Microsoft,c=US** as shown in the following, click **OK**, and then click **Close** in the **Internet Accounts** dialog box.



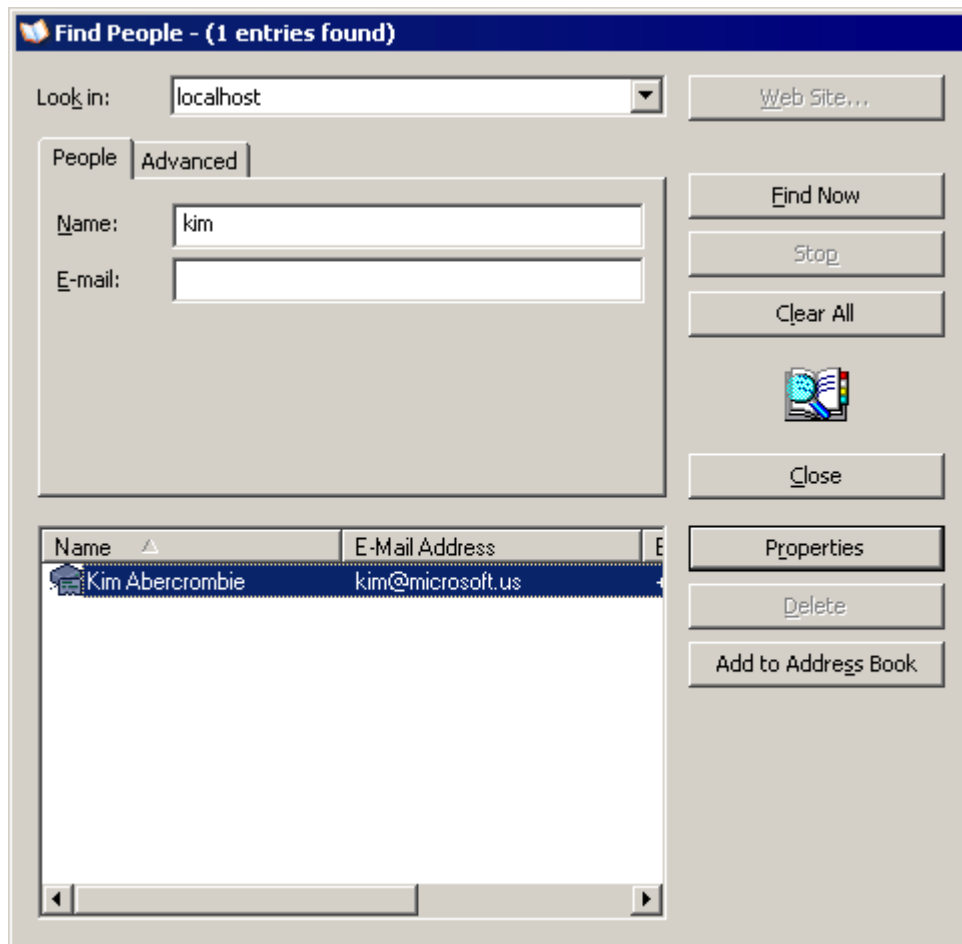
7. In Windows Address Book, click **Find People** on the toolbar. In **Look in**, click **localhost**, and then, in **Name**, type:

kim

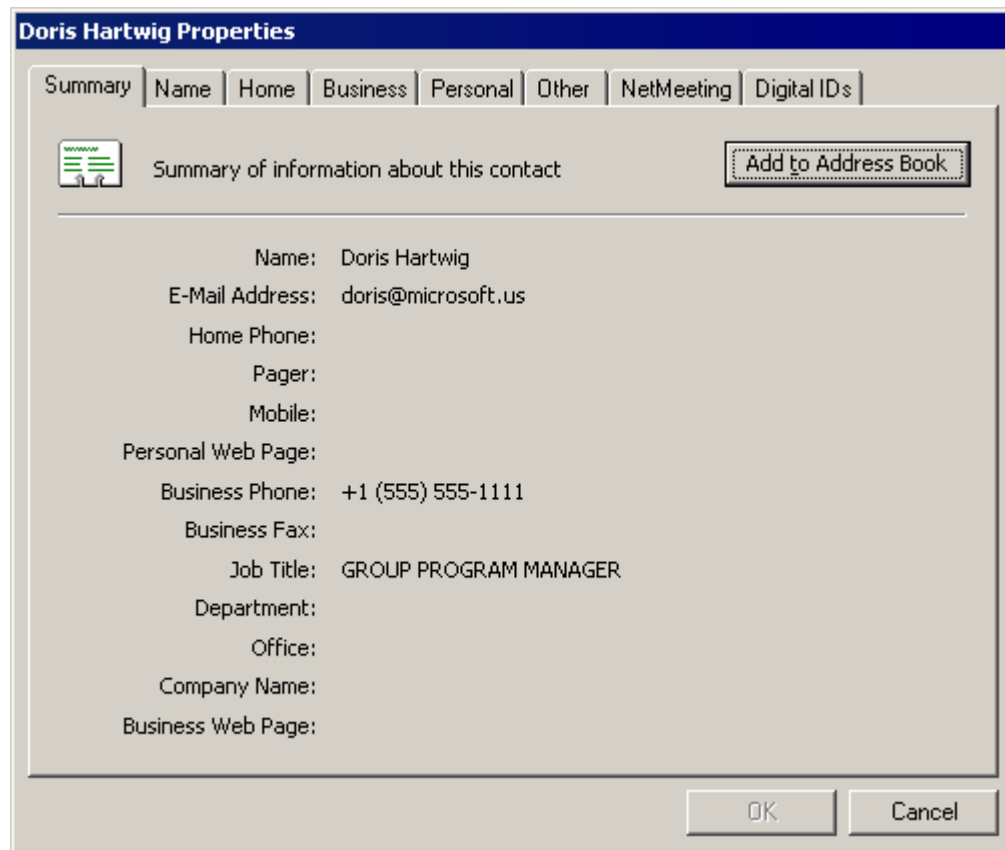
The **localhost Properties** dialog box looks like the following:



8. Click **Find Now**. Your search should return one entry from the ADAM directory, as shown in the following:



9. Double-click the name to view the search result details.
10. On the **Organization** tab, you can view the reporting relationship. Double-click the manager's name to view the associated contact details, which looks like the following:



Managing OUs, Groups, and Users in ADAM

ADAM is used most often to store information about users and the organizations and other groups they belong to. In these exercises, you create an organizational unit (OU) called "ADAM users" in the o=Microsoft,c=US application directory partition and add a group in ADAM called "ADAM testers," and you create an ADAM user named Mary Baker with one of the user object classes that you imported earlier. Using ADAM ADSI Edit, you:

- Step 1: Create an OU.
- Step 2: Create a group in the new OU.

- Step 3: Create an ADAM user.
- Step 4: Add an ADAM user to the ADAM users group.

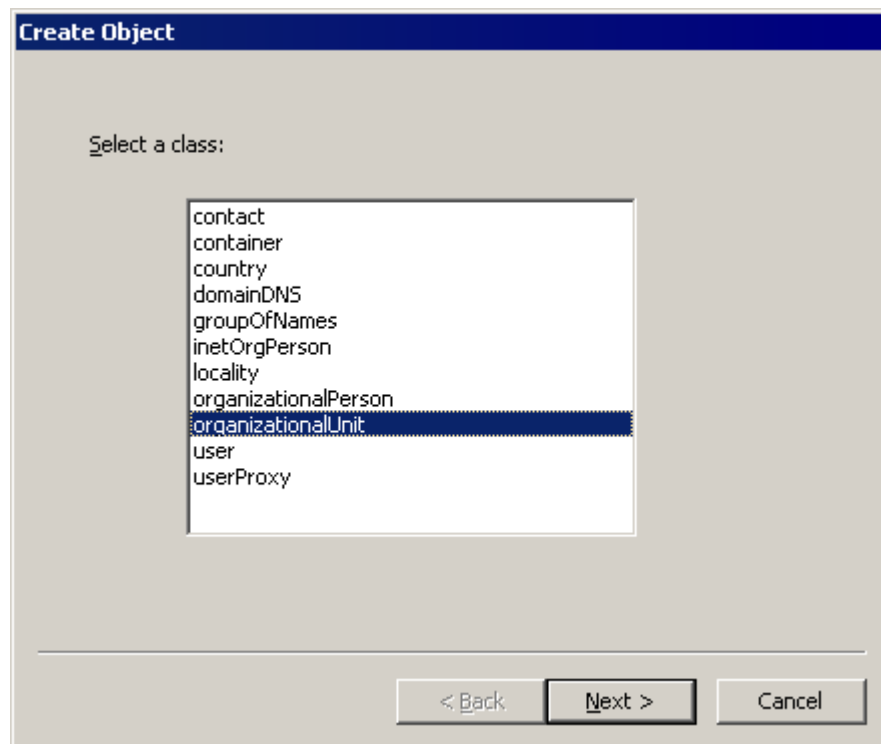
In addition you learn how to enable and disable ADAM user accounts.

Step 1: Create an OU

In this exercise, you create an OU.

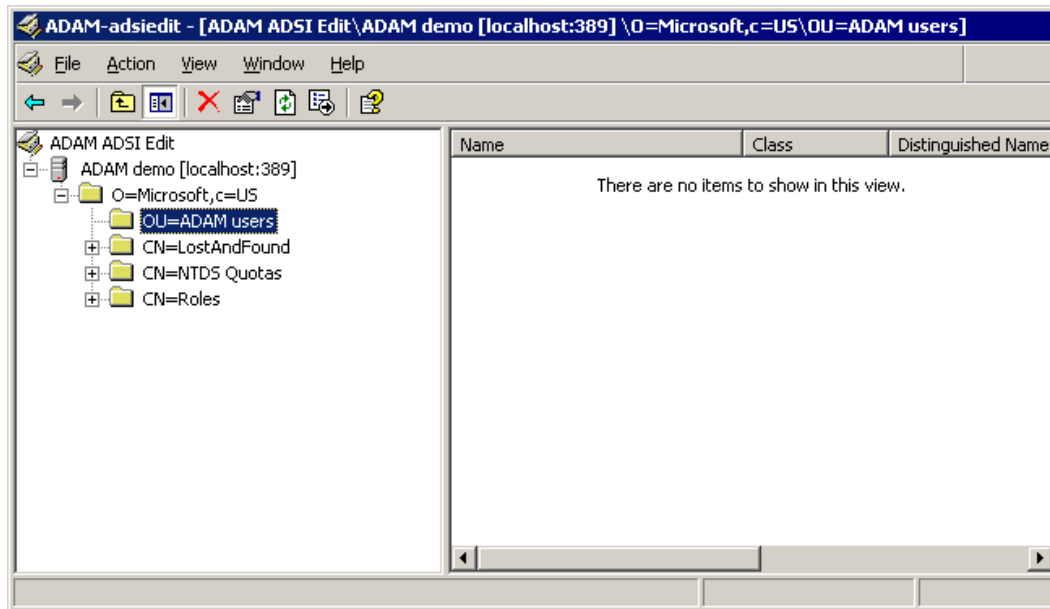
▶ To create an OU

1. If it is not open already, open ADAM ADSI Edit, and then connect to the o=Microsoft,c=US application directory partition, as described in the procedure “To bind to, view, and browse an ADAM instance using ADAM ADSI Edit” in [Using the ADAM Administration Tools](#).
2. In the console tree, right-click **O=Microsoft,c=US**, point to **New**, and then click **Object**. The **Create Object** dialog box looks like the following:



3. In the **Select a class** list, click **organizationalUnit**, and then click **Next**.

4. In **Value**, type **ADAM users**, and then click **Next**.
5. On the next page, you can click **More attributes** to edit additional attributes on the object that you are creating. For this exercise, simply click **Finish**.
6. In the console tree, double-click **O=Microsoft,c=US**. The **ADAM ADSI Edit** snap-in looks like the following:



Step 2: Create a group

In this exercise, you create a group in the OU.

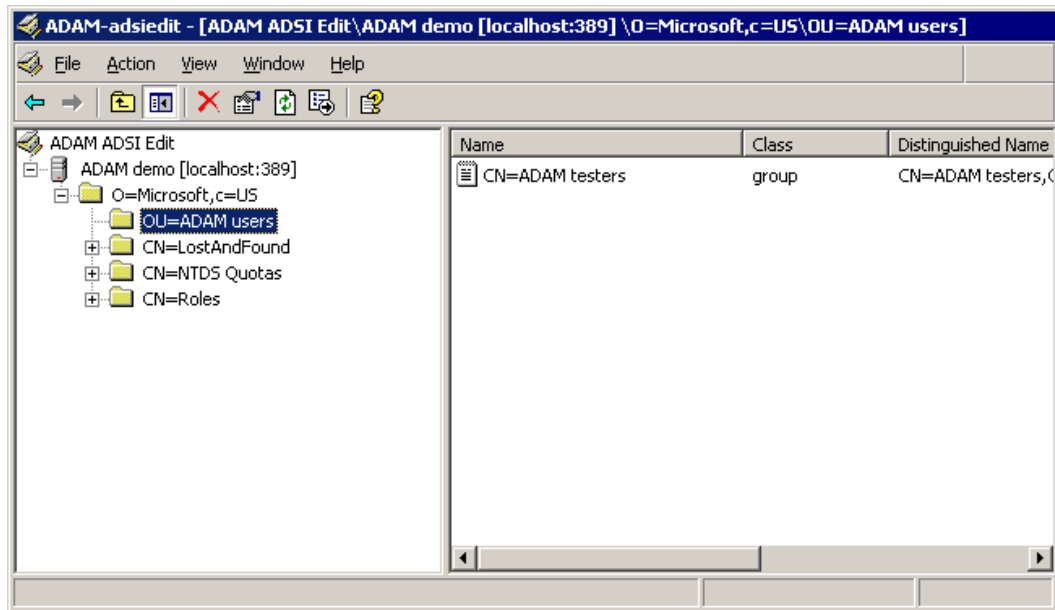
▶ To create a group in an OU

1. In the console tree, right-click **OU=ADAM Users**, point to **New**, and then click **Object**.
2. In **Select a class**, click **group**, and then click **Next**.
3. In **Value**, type **ADAM testers**, and then click **Next**.
4. In **Value**, type **2147483650** (equivalent to 0x80000002 hexadecimal, which signifies an account group), click **Next**, and then click **Finish**.

 **Note**

For more information about the **groupType** attribute, see "[Group-Type](http://go.microsoft.com/fwlink?linkid=51093)" on the Microsoft Web site (<http://go.microsoft.com/fwlink?linkid=51093>).

The **ADAM ADSI Edit** snap-in looks like the following:



Step 3: Create an ADAM user

In this exercise, you create an ADAM user in the ADAM Users OU, and then you add the user to the ADAM Testers group.

Note

The new user account is disabled by default because it has no associated password.

To create an ADAM user

1. If it is not already open, open ADAM ADSI Edit.
2. Connect and bind to your ADAM instance, as described in the procedure "To bind to, view, and browse an ADAM instance using ADAM ADSI Edit" in [Using the ADAM Administration Tools](#). Then, in the console tree, double-click the ADAM instance.
3. Double-click the **O=Microsoft,c=US** application directory partition.
4. Right-click the **OU=ADAM Users** container that you created previously, point to **New**,

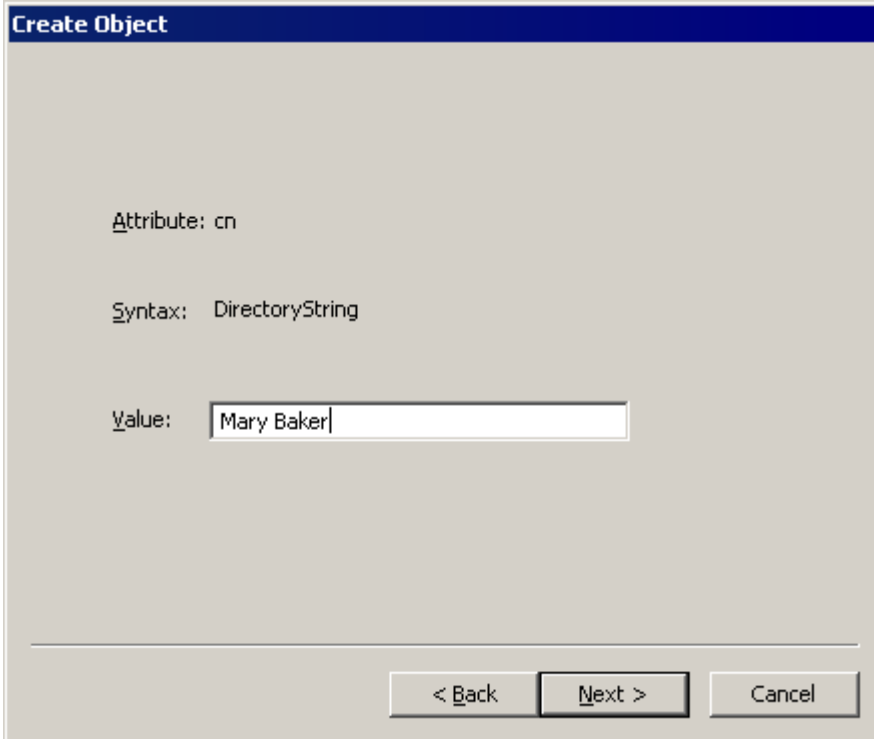
and then click **Object**.

5. In **Select a class**, click **user**, and then click **Next**.

 **Note**

If you did not close ADAM ADSI Edit before importing the Adamuser.ldf user class object definitions, you may receive the following warning message during this step: “An invalid directory pathname was passed.”

6. In **Value**, type **Mary Baker** as the common name (cn) for the new user, as shown below, and then click **Next**.



The screenshot shows a dialog box titled "Create Object". It contains the following text:

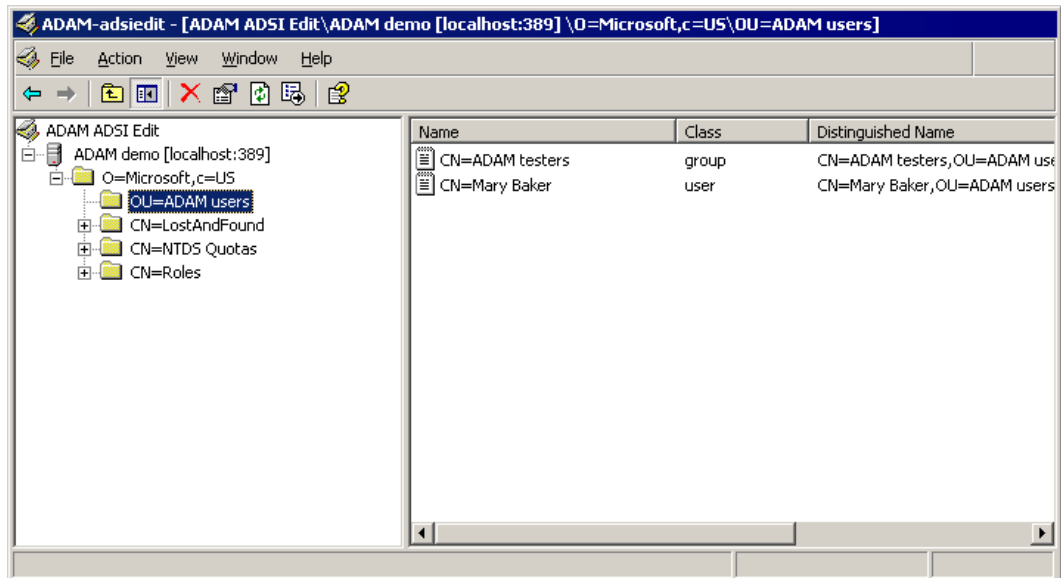
Attribute: cn

Syntax: DirectoryString

Value:

At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

7. Click **Finish**. The **ADAM ADSI Edit** snap-in looks like the following:

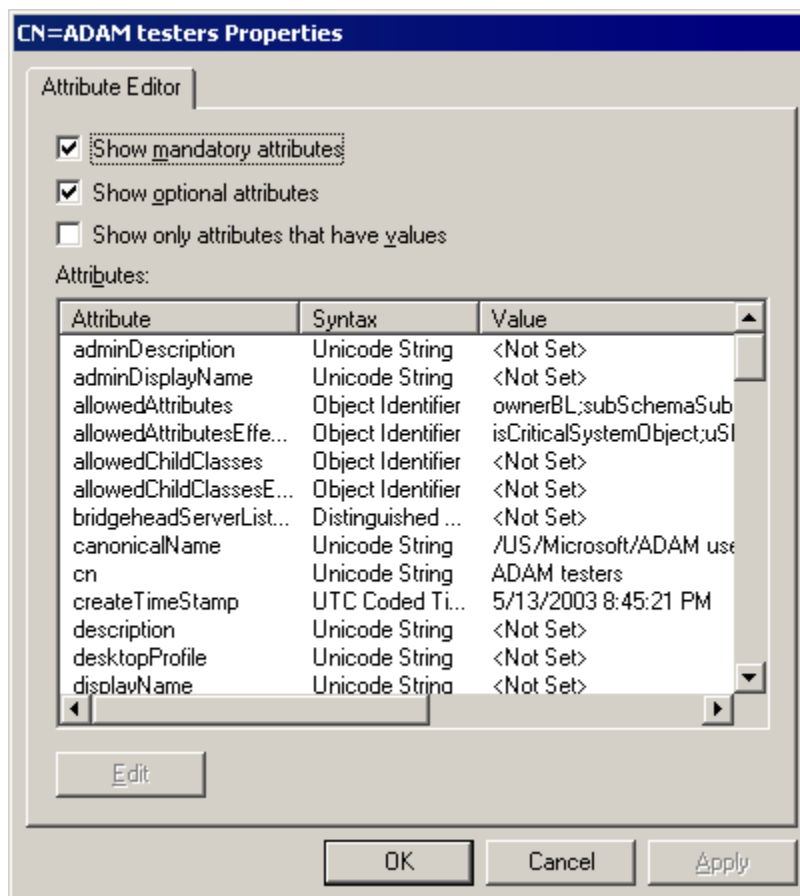


Step 4: Add a user to a group

You can add both ADAM users and Windows users to ADAM groups, as described in this exercise. First, you add Mary Baker, the user that you just created, to the ADAM testers group.

▶ To add a user to a group

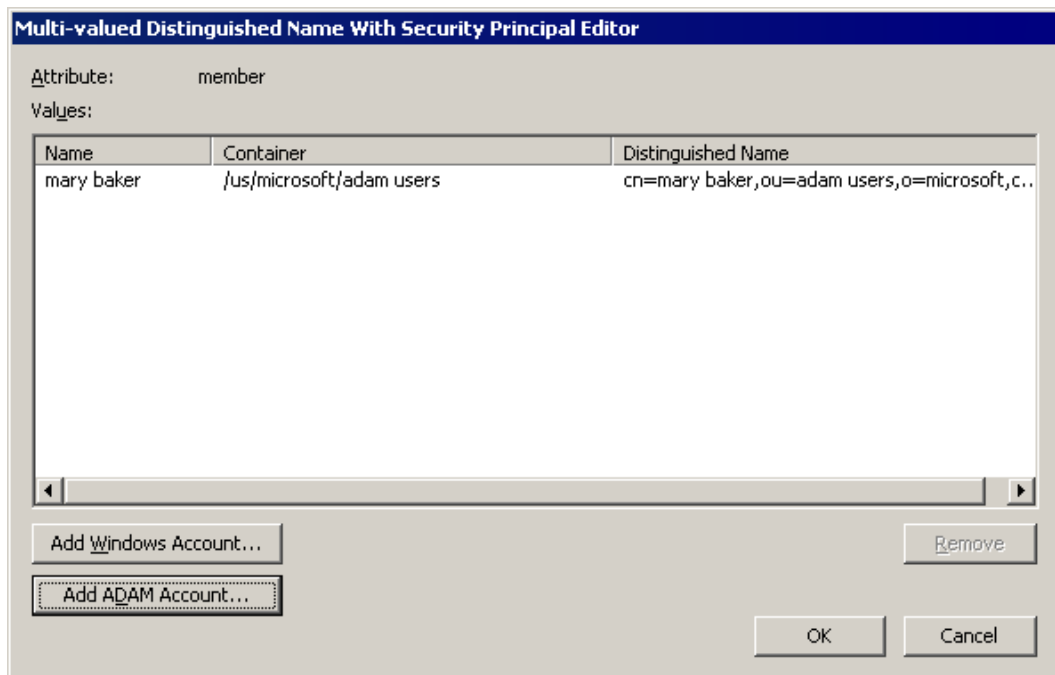
1. In the details pane of ADAM ADSI Edit, right-click **CN=ADAM testers**, and then click **Properties**. The **CN=ADAM testers Properties** dialog box looks like the following:



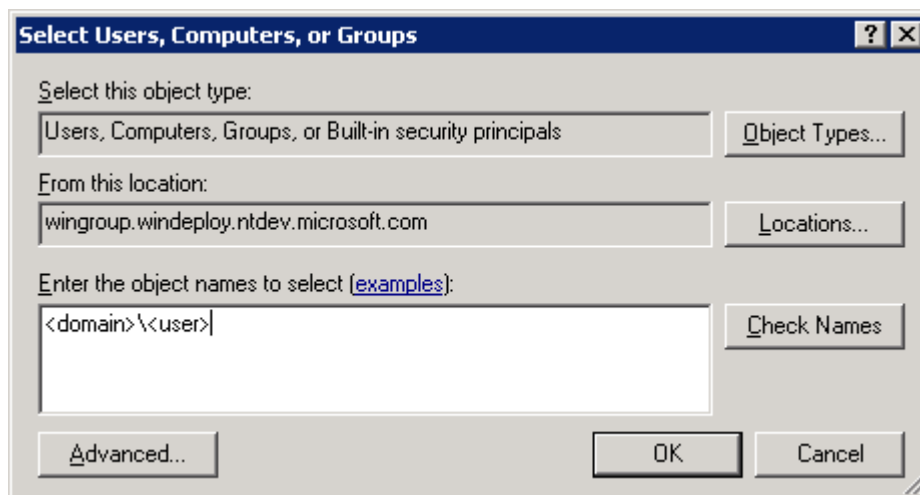
2. In **Attributes**, click **Member**, and then click **Edit**.
3. Click **Add ADAM Account**, type the following as the distinguished name, and then click **OK**:

CN=Mary Baker,OU=ADAM users,O=Microsoft,C=US

The **Multi-valued Distinguished Name with Security Principal Editor** dialog box looks like the following:



4. You can also add Windows users to an ADAM group. In the **Multi-valued Distinguished Name With Security Principal Editor** dialog box, click **Add Windows Account**. The **Select Users, Computers, or Groups** dialog box looks like the following:



5. In the **Select Users, Computers, or Groups** dialog box, add a Windows user from your computer or domain to the ADAM testers group. In **Enter the object names to**

select (examples), type an account name using the computer\account or domain\account format.

6. Click **OK**. The new user name appears in the **Multi-valued Distinguished Name With Security Principal Editor** dialog box as a member of the group.
7. Click **OK** twice to return to ADAM ADSI Edit.

Disabling and Enabling ADAM User Accounts

You can disable and enable ADAM user accounts by using the ADAM ADSI Edit snap-in. In this exercise, you disable the Mary Baker account and then enable it again.

▶ To enable or disable an ADAM user account

1. In ADAM ADSI Edit, connect and bind to an ADAM instance as described in the procedure “To bind to, view, and browse an ADAM instance using ADAM ADSI Edit” in [Using the ADAM Administration Tools](#).
2. In the console tree, double-click the **O=Microsoft,c=US** application directory partition.
3. In the console tree, click the **OU=ADAM Users** container.
4. In the details pane, right-click **CN=Mary Baker**, and then click **Properties**.
5. In **Attributes**, click **msDS-UserAccountDisabled**, and then click **Edit**.
6. Click **True**, and then click **OK**. The Mary Baker account is now disabled.
7. To enable the Mary Baker account, edit **msDS-UserAccountDisabled** again, and this time set the attribute to **False**.

Managing Directory Partitions in ADAM

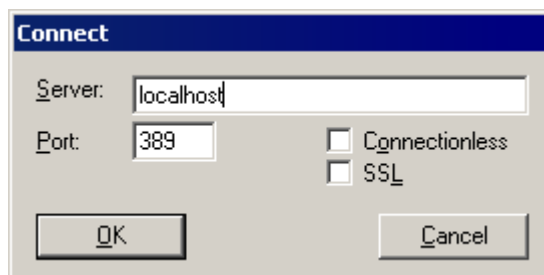
The following exercises help you become familiar with an additional ADAM administration tool, Ldp.exe. Ldp is installed as part of the ADAM administration tool set. In these exercises, you use Ldp to connect and bind to an ADAM instance, and then you use Ldp to manually add and then delete an application directory partition. (Remember, you can also create an application directory partition by using the ADAM setup wizard.)

Connecting and Binding to an ADAM Instance Using Ldp.exe

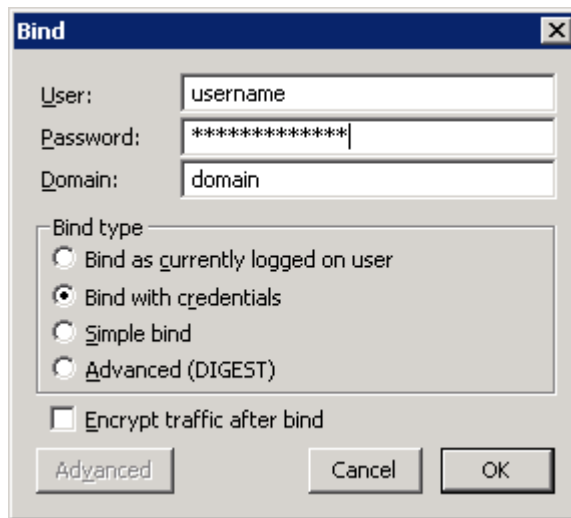
To begin this exercise, you connect and bind to your ADAM instance using Ldp.exe.

▶ **To connect and bind to an ADAM instance using Ldp.exe**

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type **ldp**, and then press ENTER.
3. On the **Connection** menu, click **Connect**.
4. In **Server**, type the host or DNS name of the computer running ADAM. When the ADAM instance is running locally, you can also type **localhost**.
5. In **Port**, type the LDAP or SSL communication port number for the ADAM instance to which you want to connect, and then click **OK**.



6. On the **Connection** menu, click **Bind**.
7. Do one of the following:
 - To bind using the credentials you logged on with, click **Bind as currently logged on user**.
 - To bind using a domain user account, click **Bind using credentials**, type the user name, password, and domain name (or the computer name, if you are using a local workstation account) of the account that you are using, and then click **OK**, as in the following.



- To bind using just a user name and password, click **Simple bind**, type the user name and password of the account that you are using, and then click **OK**.
 - To bind using an advanced method (NTLM, DPA, negotiate, or digest), click **Advanced (method)**, click **Advanced**, in **Method**, select the desired method, set other options as needed, and then click **OK** twice.
8. When you are finished specifying bind options, click **OK**.

Adding an Application Directory Partition

Now, you are ready to add an application directory partition.

▶ To add an application directory partition using Ldp.exe

1. On the **Ldp Browse** menu, click **Add child**.
2. In **Dn**, type **cn=test,o=testpartition,c=us** as the distinguished name for the new application directory partition.
3. Under **Edit Entry**, type the following, and then click **Enter**:
 - In **Attribute**, type **ObjectClass**.
 - In **Values**, type **container**.
4. Under **Edit Entry**, type the following, and then click **Enter**:

- In **Attribute**, type **InstanceType**.
- In **Values**, type **5**.

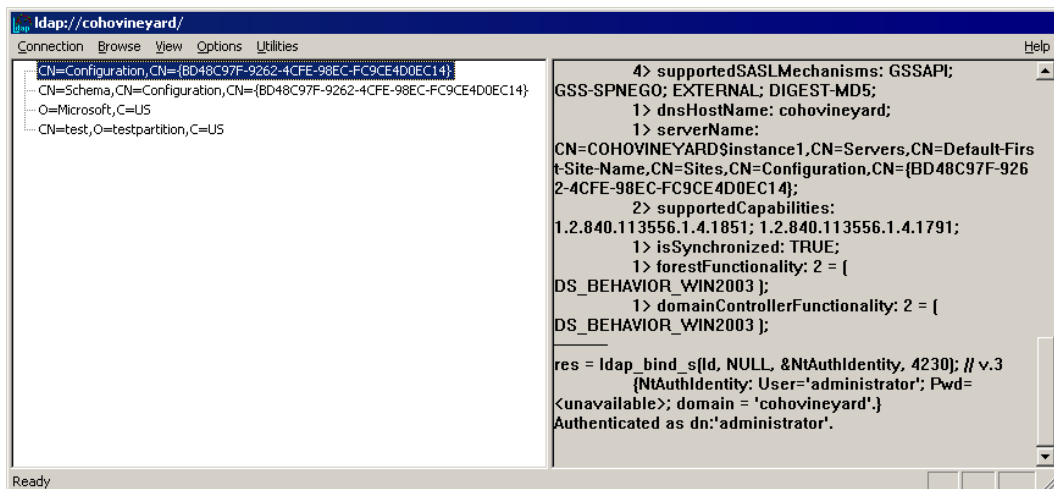
The **Add** dialog box looks like the following:

5. Click **Run**. After the new application directory partition is added, the following result appears in the details pane:

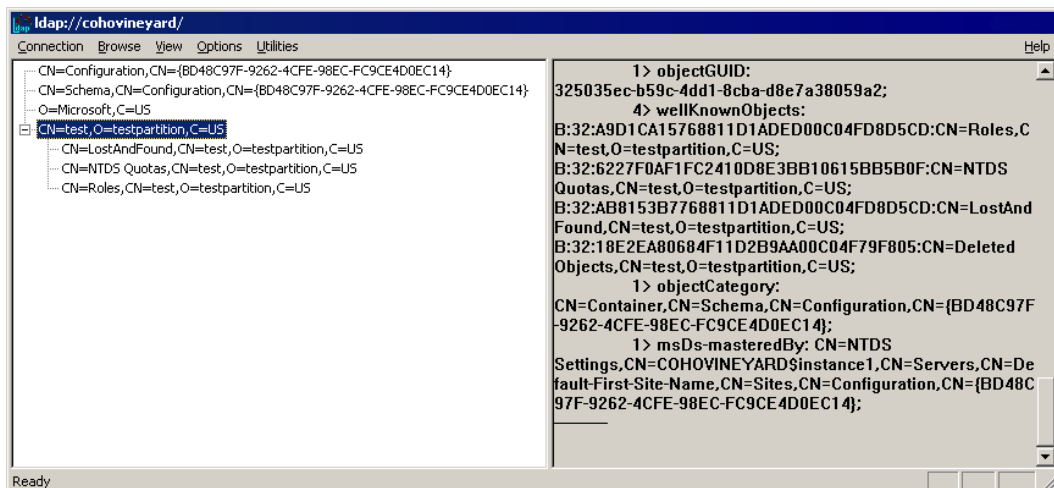
```
***Calling Add...
ldap_add_s(ld, "cn=test,o=testpartition,c=us", [2] attrs)
Added {cn=test,o=testpartition,c=us}.
```

6. Click **Close**.
7. To refresh Ldp and view your new directory partition, you must disconnect and then bind again to the ADAM instance. On the **Connection** menu, click **Disconnect**.
8. Bind to your ADAM instance as you did previously. On the **Connection** menu, click **Bind**.
9. To view the directory tree in Ldp, on the **View** menu, click **Tree**.

10. To view all directory partitions on the ADAM instance, leave **BaseDN** blank, and then click **OK**. The **Ldp** window looks like the following:



11. To view your new directory partition and its default containers and objects, double-click **CN=test,O=testpartition,C=US** in the console tree. The **Ldp** window looks like the following:

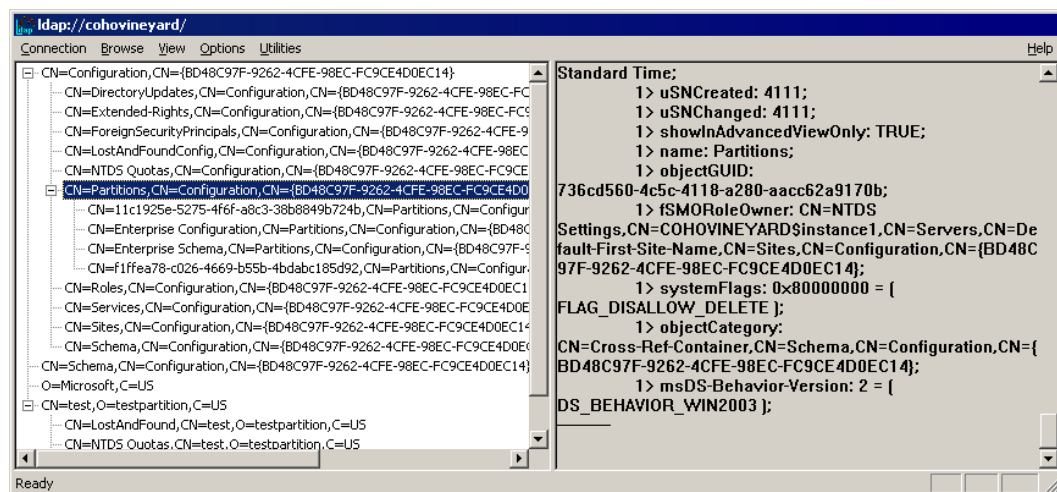


Deleting an Application Directory Partition

In this exercise, you delete the application directory partition that you just created.

► **To delete an application directory partition using Ldp.exe**

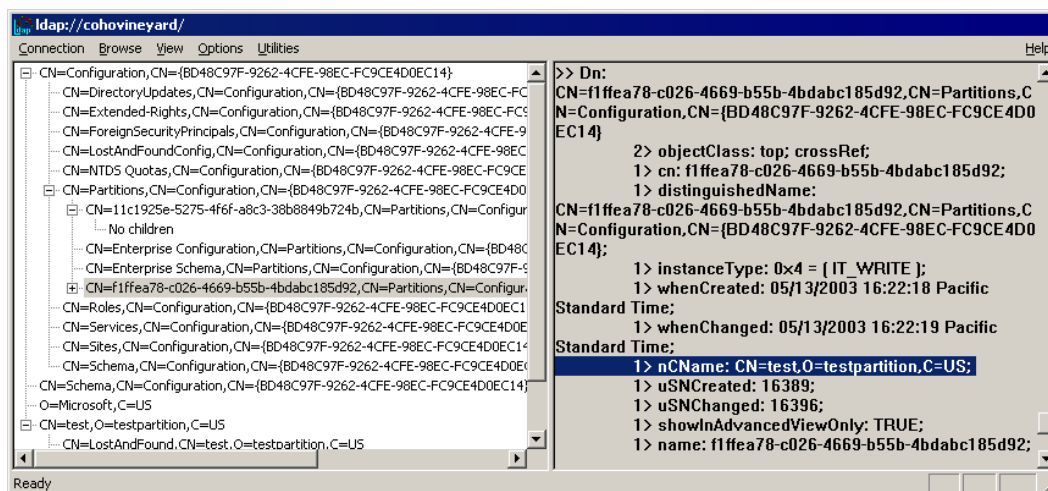
1. In the Ldp console tree, double-click the configuration directory partition **CN=Configuration,CN={GUID}**, where *GUID* is the unique identifier that is assigned by ADAM.
2. To view the cross-reference objects for the directory partitions on your ADAM instance, in the console tree, double-click the partitions container **CN=Partitions**. The **Ldp** window looks like the following:



3. In the console tree, under the partitions container **CN=Partitions**, double-click the cross-reference object for which the value of **nCNName** (as viewed in the details pane) is equal to **CN=test,O=testpartition,C=US**, as shown in the following:

📌 **Note**

To clear the details pane in Ldp without disturbing your bind or connection, on the **Connection** menu, click **New**.



- To delete this cross-reference object (and, therefore, the associated directory partition), in the console tree, right-click the appropriate cross-reference object in the partitions container, click **Delete**, and then click **OK**.

Caution

You cannot undo a partition deletion after you click **OK**.

After you delete the cross-reference object, output similar to the following appears in the details pane:

```
ldap_delete_s(ld, "CN=56c5aea2-5cb1-450a-96f0-5622cd949791,CN=Partitions,CN=Configuration,CN={90BF4692-0FF5-4410-8835-DCBBEE6E08B1}");
Deleted "CN=56c5aea2-5cb1-450a-96f0-5622cd949791,CN=Partitions,CN=Configuration,CN={90BF4692-0FF5-4410-8835-DCBBEE6E08B1}"
```

Note

For more information about Ldp, see ADAM Help. To open ADAM Help, click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Help**.

Managing Authorization in ADAM

Authorization refers to the process of determining which users have access to which directory objects. As with Active Directory, access control lists (ACLs) on each directory object determine which users have access to that object. By default, the only ACLs in ADAM reside in the top-level container of each directory partition. All objects in a given

directory partition inherit these ACLs. Using the Dsacls.exe command-line tool, you can view and modify the default ACLs in ADAM, and you can add additional ACLs. In the following exercises, you view and modify ADAM ACLs.

Note

You may have directory-enabled applications that implement their own custom authorization schemes. These applications generally disregard the ACLs on ADAM directory objects.

Viewing Effective Permissions

In this exercise, you view the effective permissions on the o=Microsoft,c=US directory partition.

To view effective permissions

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type the following, and then press ENTER:

```
dsacls \\servername:portnumber\O=Microsoft,C=US
```

where *servername:portnumber* is the computer name and the LDAP communications port of your ADAM instance.

This command lists all the permissions that are currently set on the directory partition object. Your screen should contain output similar to the following:

```
Access list:
Effective Permissions on this object are:
Allow CN=Instances,CN=Roles,CN=Configuration,CN={C98CA450-AC25-4BC1-AC3C-
C3BEC88B335E}
                                SPECIAL ACCESS
                                READ PERMISSONS
                                LIST CONTENTS
                                READ PROPERTY
                                LIST OBJECT
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                                SPECIAL ACCESS
                                READ PERMISSONS
                                LIST CONTENTS
                                READ PROPERTY
                                LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                                FULL CONTROL
Allow CN=Instances,CN=Roles,CN=Configuration,CN={C98CA450-AC25-4BC1-AC3C-
```

```

C3BEC88B335E}
                                Replicating Directory Changes
Allow CN=Instances,CN=Roles,CN=Configuration,CN={C98CA450-AC25-4BC1-AC3C-
C3BEC88B335E}
                                Replication Synchronization
Allow CN=Instances,CN=Roles,CN=Configuration,CN={C98CA450-AC25-4BC1-AC3C-
C3BEC88B335E}
                                Manage Replication Topology
Allow CN=Instances,CN=Roles,CN=Configuration,CN={C98CA450-AC25-4BC1-AC3C-
C3BEC88B335E}
                                Replicating Directory Changes All

Permissions inherited to subobjects are:
Inherited to all subobjects
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                                SPECIAL ACCESS
                                READ PERMISSONS
                                LIST CONTENTS
                                READ PROPERTY
                                LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                                FULL CONTROL

The command completed successfully

```

Granting Permissions

In this exercise, you grant the Delete permission on the ADAM testers group object to the Mary Baker account.

▶ To grant the Delete permission

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type the following:

```
dsacls "\\servername:portnumber\CN=ADAM testers,OU=ADAM
users,O=Microsoft,C=US" /G "CN=Mary Baker,OU=ADAM
users,O=Microsoft,C=US":SD;;
```

where *servername:portnumber* represents the computer name and LDAP communications port of your ADAM instance. Be sure to use an uppercase G when typing the **/G** parameter, and use quotation marks as shown.

Your screen should contain output similar to the following:

```

Access list:
Effective Permissions on this object are:
Allow CN=Mary Baker,OU=ADAM users,O=Microsoft,C=US
                SPECIAL ACCESS
                DELETE
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                SPECIAL ACCESS <Inherited from parent>
                READ PERMISSONS
                LIST CONTENTS
                READ PROPERTY
                LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                FULL CONTROL <Inherited from parent>

Permissions inherited to subobjects are:
Inherited to all subobjects
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                SPECIAL ACCESS <Inherited from parent>
                READ PERMISSONS
                LIST CONTENTS
                READ PROPERTY
                LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                FULL CONTROL <Inherited from parent>

The command completed successfully

```

Denying Permissions

In this exercise, you deny Delete permissions for the currently logged on user in the ADAM testers group. This is done in two phases:

- Deny delete permissions on the parent container of the ADAM testers group
- Deny delete permissions on the group itself

▶ To deny the Delete permissions on the parent container of a group

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. To deny the Delete, Delete Child, and Delete Tree permissions on the parent container of the ADAM testers group, which is the ADAM users OU. At the command prompt, type the following:

```
dsacls "\\servername:portnumber\OU=ADAM users,O=microsoft,C=US" /D
domain\administrator:SDDCDT;;
```

where *servername:portnumber* represents the computer name and LDAP communications port of your ADAM instance, and *domain\administrator* represents the account with which you are currently logged on. Be sure to use an uppercase D when typing the **/D** parameter, and use quotation marks as shown.

Your screen should contain output similar to the following:

```

Access list:
Effective Permissions on this object are:
Deny domain\account          SPECIAL ACCESS
                             DELETE
                             DELETE CHILD
                             DELETE TREE
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                             SPECIAL ACCESS <Inherited from parent>
                             READ PERMISSONS
                             LIST CONTENTS
                             READ PROPERTY
                             LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                             FULL CONTROL <Inherited from parent>

Permissions inherited to subobjects are:
Inherited to all subobjects
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                             SPECIAL ACCESS <Inherited from parent>
                             READ PERMISSONS
                             LIST CONTENTS
                             READ PROPERTY
                             LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                             FULL CONTROL <Inherited from parent>

The command completed successfully

```

▶ To deny delete permissions on the group

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. To deny the Delete permission on the ADAM testers group for the currently logged on user, at the command prompt, type the following:

dscls "\servername:portnumber\CN=ADAM testers,OU=ADAM users,O=microsoft,C=US" /D domain\administrator:SDDCDT;;

where *servername:portnumber* represents the computer name and LDAP communications port of your ADAM instance, and *domain\administrator*

represents the account with which you are currently logged on. Be sure to use an uppercase D when typing the */D* parameter, and use quotation marks as shown.

Your screen should contain output similar to the following:

```
Access list:
Effective Permissions on this object are:
Deny  domain\account                SPECIAL ACCESS
                                           DELETE
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                                           SPECIAL ACCESS  <Inherited from parent>
                                           READ PERMISSONS
                                           LIST CONTENTS
                                           READ PROPERTY
                                           LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                                           FULL CONTROL    <Inherited from parent>

Permissions inherited to subobjects are:
Inherited to all subobjects
Allow CN=Readers,CN=Roles,O=Microsoft,C=US
                                           SPECIAL ACCESS  <Inherited from parent>
                                           READ PERMISSONS
                                           LIST CONTENTS
                                           READ PROPERTY
                                           LIST OBJECT
Allow CN=Administrators,CN=Roles,O=Microsoft,C=US
                                           FULL CONTROL    <Inherited from parent>

The command completed successfully
```

Managing Authentication in ADAM

With ADAM, you can bind as a Windows principal, as an ADAM principal, or through an ADAM proxy object. In the following exercises, you:

- Complete a bind as a Windows principal.
- Set a password for the ADAM user account Mary Baker, which you created earlier.
- Complete a bind as an ADAM principal.
- Complete a bind through an ADAM proxy object.

In addition, you test the permissions that you set by using Dsacls.exe command-line tool in the exercises in [Managing Authorization in ADAM](#).

Binding as a Windows Principal

In this exercise, you bind to an ADAM instance as a Windows principal and then test the bind.

▶ To bind as a Windows principal and test the bind

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM ADSI Edit**.
2. Using ADAM ADSI Edit, bind to your ADAM instance using the Windows principal that you are logged on as, and connect to the O=Microsoft,c=US directory partition.
3. In the details pane, browse to the ADAM testers group, on which you denied the Delete permission to your current Windows account.
4. Right-click the ADAM testers group, and then click **Delete**. An “Access denied” message appears, confirming that the Delete permission has been successfully denied to your Windows account.

Setting the Password of an ADAM User

Before logging on to the ADAM instance with the Mary Baker user account, you first set a password on the account.

📌 Note

In addition to using Ldp as described in this procedure, you can also use ADAM ADSI Edit to set or modify passwords: right-click the directory object representing the ADAM security principal in ADAM ADSI Edit, and then click Reset Password.

▶ To set a password on an ADAM user account

1. Click **Start**, point to **All Programs**, point to **ADAM**, and click **ADAM Tools Command Prompt**.
2. At the command prompt, type **ldp**, and then press **ENTER**.
3. On the **Connection** menu, click **Connect**, and then connect to your ADAM instance.
4. On the **Options** menu, click **ConnectionOptions**.
5. In **Option Name**, click **LDAP_OPT_SIGN**, type **1** in **Value**, and then click **Set**.

6. In **Option Name**, click **LDAP_OPT_ENCRYPT**, type **1** in **Value**, click **Set**, and then click **Close**.
7. On the **Connection** menu, click **Bind**, and then bind to your ADAM instance.
8. On the **View** menu, click **Tree**, leave **BaseDN** blank, and then click **OK**.
9. In the console tree, locate the O=Microsoft,C=US directory partition. Double-click **O=Microsoft,C=US**, and then double-click **OU=ADAM Users,O=Microsoft,C=US**.
10. Right-click the **CN=Mary Baker** user object, and then click **Modify**. The following dialog box appears:

The screenshot shows a 'Modify' dialog box with the following fields and controls:

- Dn:** CN=Mary Baker,OU=ADAM users,O=Microsoft
- Edit Entry** section:
 - Attribute:** (empty text box)
 - Values:** (empty text box)
- Operation** section:
 - Add
 - Delete
 - Replace
 - Insert file
 - Enter
- Entry List** section:
 - (Empty list box)
 - Edit
 - Remove
- Bottom section:
 - Synchronous
 - Extended
 - Close
 - Run

11. In **Attribute**, type **userpassword**, and then, in **Values**, type a password for the account.
12. Click **Enter**, and then click **Run**. The details pane in Ldp should contain output similar to the following:

```
***Call Modify...
```

```
ldap_modify_s(ld, 'CN=Mary Baker,OU=ADAM users,O=Microsoft,C=US',[1]
```

```
attrs);  
  
Modified "CN=Mary Baker,OU=ADAM users,O=Microsoft,C=US".
```

 **Note**

When ADAM runs on a computer running Windows Server 2003, it enforces the password policy and account lockout settings of the computer, organizational unit, or domain, whichever is in effect.

Binding as an ADAM Principal

In this exercise, you bind to an ADAM instance as an ADAM principal and then test the bind.

 **To bind as an ADAM principal and test the bind**

1. Using Ldp, bind to your ADAM instance using CN=Mary Baker,OU=ADAM users,O=Microsoft,C=US as the account, along with the password that you just assigned to this account.
2. To confirm that you are logged on as Mary Baker and that the Delete permission that you granted earlier is effective, in the Ldp console tree, browse to the ADAM testers group and delete it. To delete the ADAM testers group, right-click the **CN=ADAM testers** object, and then click **Delete**.

 **Note**

By default, new ADAM users (such as Mary Baker) are granted Read access to the top-level container of a given directory partition, a permission which is inherited by all objects on the partition. But, because you explicitly assigned the Delete permission to Mary Baker on the ADAM testers group object, the delete operation succeeded. For more information about access control and default permissions in ADAM, see ADAM Help. To view ADAM Help, click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Help**.

Binding Through an ADAM Proxy Object

In addition to binding as a Windows user or as an ADAM user, you can also bind to an ADAM instance by using ADAM bind redirection. When using bind redirection, ADAM can accept and process bind requests to an ADAM proxy object that contains as one of its attributes the security ID (SID) from an Active Directory security principal. With ADAM,

you can use bind redirection to provide Active Directory users with access to both ADAM data and Active Directory data, using Active Directory domain credentials as a single sign-on (SSO). In addition, you can use ADAM proxy objects to store user data that is specific to a particular application in ADAM, while using Active Directory to store more widely used directory data.

Bind redirection enables a user to bind to ADAM by means of a simple bind while still using Active Directory credentials. Other types of binding with Active Directory credentials work without requiring a proxy, but a simple bind does not. Proxy binding works only for a simple bind.

The ADAM .ldf files, which you can import into the ADAM schema during ADAM setup, contain an object definition for the object userProxy, which can be used for bind redirection. This object contains attributes that include a distinguished name and a SID. By creating a userProxy object in ADAM—specifying a distinguished name to be used for binding—and by using a valid SID from an Active Directory user account, you can bind to ADAM using bind redirection. For more information about ADAM authentication, see "[Active Directory Application Mode](http://go.microsoft.com/fwlink/?LinkId=51640)" Technical Reference on the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=51640>).

For the following exercises, it is assumed that you have already imported the optional user classes into the ADAM schema.

Binding Security and ADAM Proxy Objects

By default, binding to ADAM with bind redirection requires an SSL connection. SSL requires the installation and use of certificates on the computer running ADAM and on the computer connecting to ADAM as a client. If you do not have certificates installed in your ADAM test environment, you can, as an alternative, disable the requirement for SSL, as described in the following procedure.

Note

Disabling the requirement for SSL for bind redirection causes the password of a Windows security principal to be passed to the computer running ADAM, without first being encrypted. Therefore, you should only disable the SSL requirement in a test environment.

To disable the SSL requirement for bind redirection

1. As described earlier in the procedure "To bind to, view, and browse an ADAM instance using ADAM ADSI Edit," connect and bind to your ADAM instance using ADAM ADSI Edit, and then, in the console tree, browse to the following container

object in the configuration partition: CN=Directory Service,CN=Windows NT,CN=Services.

2. Right-click **CN=Directory Service**, and then click **Properties**.
3. In **Attributes**, click **msDS-Other-Settings**, and then click **Edit**.
4. In **Values**, click **RequireSecureProxyBind=1**, and then click **Remove**.
5. In **Value to add**, type **RequireSecureProxyBind=0**, click **Add**, and then click **OK**.

Creating and Binding with an ADAM Proxy Object

In these exercises, you create a proxy object for an Active Directory user, and you bind to ADAM using the proxy object.

▶ To bind to ADAM through an ADAM proxy object

1. As described earlier in the procedure “To connect and bind to an ADAM instance using Ldp.exe,” connect and bind to your ADAM instance using Ldp, and then browse to O=Microsoft,C=US.
2. On the Ldp **Browse** menu, click **Add child**.
3. In **Dn**, type **cn=testproxy,o=microsoft,c=us** as the distinguished name for the new userProxy object to be created in the O=Microsoft,C=US container.
4. Under **Edit Entry**, type the following, and then click **Enter**:
 - In **Attribute**, type **ObjectClass**
 - In **Values**, type **userProxy**
5. Again, under **Edit Entry**, type the following, and then click **Enter**:
 - In **Attribute**, type **objectSID**
 - In **Values**, type the valid SID of a user in Active Directory.

The \LABS_DEMO\LABS\bindredirect directory in the ADAM download contains two commands from the Windows Server 2003 Administration Tools Pack, Dsquery.exe and Dsget.exe, to help you retrieve the SID of an Active Directory user. You can run these commands on a computer running Windows Server 2003.

To retrieve the SID of an Active Directory user with these commands, type the following (as a single command) at a command prompt:

dsquery user -samid *domain\account* | dsget user -sid

where *domain\account* represents the user whose SID you want to retrieve. In this command, the results of Dsquery are piped to Dsget.

You can retrieve the SID of the currently logged on user on a computer running Windows Server 2003 by typing the following at a command prompt:

whoami /user

(Some versions of **whoami** require the syntax **whoami /user /sid**.)

6. Click **Run**. This adds the userProxy object, with the attributes that you specified, to the ADAM directory store.
7. To disconnect from your ADAM instance, on the **Connection** menu, click **Disconnect**.

Now, you can bind to your ADAM instance using the ADAM proxy object and bind redirection.

▶ **To bind as an ADAM proxy object through bind redirection**

1. On the **Connection** menu, click **Connect**, and then connect to your ADAM instance on a new connection.
2. On the **Options** menu, click **ConnectionOptions**.
3. In **Option Name**, click **LDAP_OPT_SIGN**, type **1** in **Value**, and then click **Set**.
4. In **Option Name**, click **LDAP_OPT_ENCRYPT**, type **1** in **Value**, click **Set**, and then click **Close**.
5. To bind to your ADAM instance again with Ldp, on the **Connection** menu, click **Bind**.
6. In **User**, type:

cn=testproxy,o=Microsoft,c=us

This represents the proxy object that you just created.
7. Make sure that the **Domain** option is not selected.
8. In **Password**, type the password that is associated with the Active Directory user that you specified in step 5 in the previous procedure, and then click **OK**.

Demonstrating ADAM Proxy Object Functionality

By default, a Windows user binding to an ADAM instance receives membership only in the ADAM groups to which that user has been explicitly added as member. When a user binds to an ADAM instance through a proxy object, the user receives membership in the Users group on each naming context that is held by the ADAM instance.

You can use this difference in group memberships to demonstrate the functional difference between binding to an ADAM instance as a Windows user and binding to an ADAM instance through a proxy object. The following exercise demonstrates this difference.

▶ To demonstrate binding to ADAM through a proxy object

1. In the O=Microsoft,C=US directory partition, add the Users group as a member of the Readers group, following the general directions for adding members to groups as described earlier in the procedure “To add a user to a group.”
2. Bind to your ADAM instance (using Ldp or ADAM ADSI Edit) as an Active Directory user (other than the ADAM administrator, which receives full access to all partitions by default).
3. Attempt to read any object in the O=Microsoft,C=US directory partition. Your attempt should fail, because the Active Directory user does not have access to the partition by default.
4. Bind to your ADAM instance (using Ldp or ADAM ADSI Edit) using the proxy object that you created.
5. Attempt to read any object in the O=Microsoft,C=US directory partition. This time, your attempt should succeed; because users who bind to an ADAM instance through a proxy object automatically receive membership in the Users group. And, because you added the Users group to the Readers group in step 1 of this procedure, binding to the ADAM instance through the proxy object enables you to successfully read the partition.

Note

For more information about bind redirection, see ADAM Help. To view ADAM Help, click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Help**. For information about administering proxy objects programmatically, see [Administering ADAM Programmatically](#) later in this guide.

Backing Up and Restoring Active Directory Application Mode (ADAM)

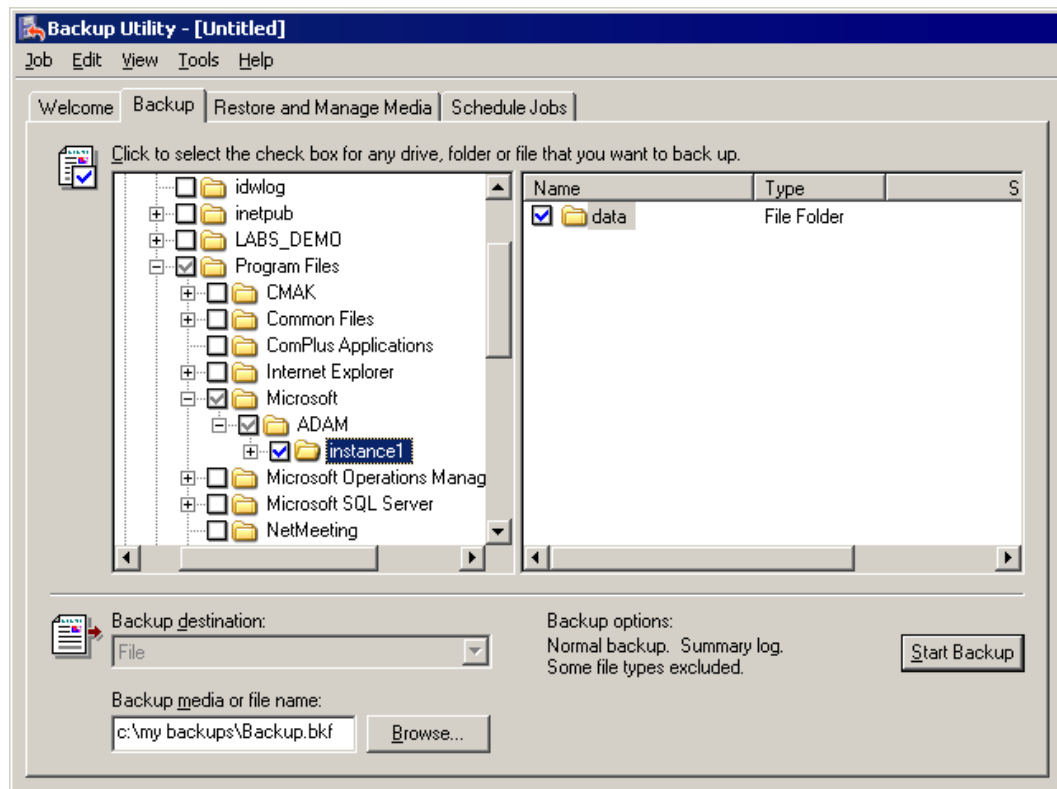
In the following exercises, you back up your ADAM instance. Then, you remove ADAM completely from your computer. Finally, you restore your ADAM instance back to your computer.

Backing up an ADAM Instance

In this exercise, you back up your ADAM instance.

▶ To back up an ADAM instance

1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. In the **Backup or Restore Wizard**, click the **Advanced Mode** link.
3. Click the **Backup** tab, and then, on the **Job** menu, click **New**.
4. Select the check box to the left of your ADAM instance folder, which is, by default, %programfiles%\Microsoft\ADAM\instance1.
5. To back up the ADAM files to a file, in **Backup destination**, click **File**. (If you do not have a tape drive in your computer, **File** is selected by default.) Then, in **Backup media or file name**, type a path and file name for the backup (.bkf) file. Your screen should now appear similar to the following:



6. Click **Start Backup**, and then make any desired changes in the **Backup Job Information** dialog box.
7. If you want to set advanced backup options, such as data verification or hardware compression, in the **Backup Job Information** dialog box, click **Advanced**. When you have finished setting advanced backup options, click **OK**.
8. Click **Start Backup**. After the backup operation is complete, close the backup application.

Removing an ADAM Instance

To simulate an accidental loss of an ADAM instance, you can uninstall your ADAM instance, which removes both the ADAM program files and the ADAM data files.

▶ To uninstall an ADAM instance

1. Click **Start**, point to **Control Panel**, click **Add or Remove Programs**, and then click **ADAM Instance instance1**. If it is the first item in the list, **ADAM Instance**

instance1 will already be selected.

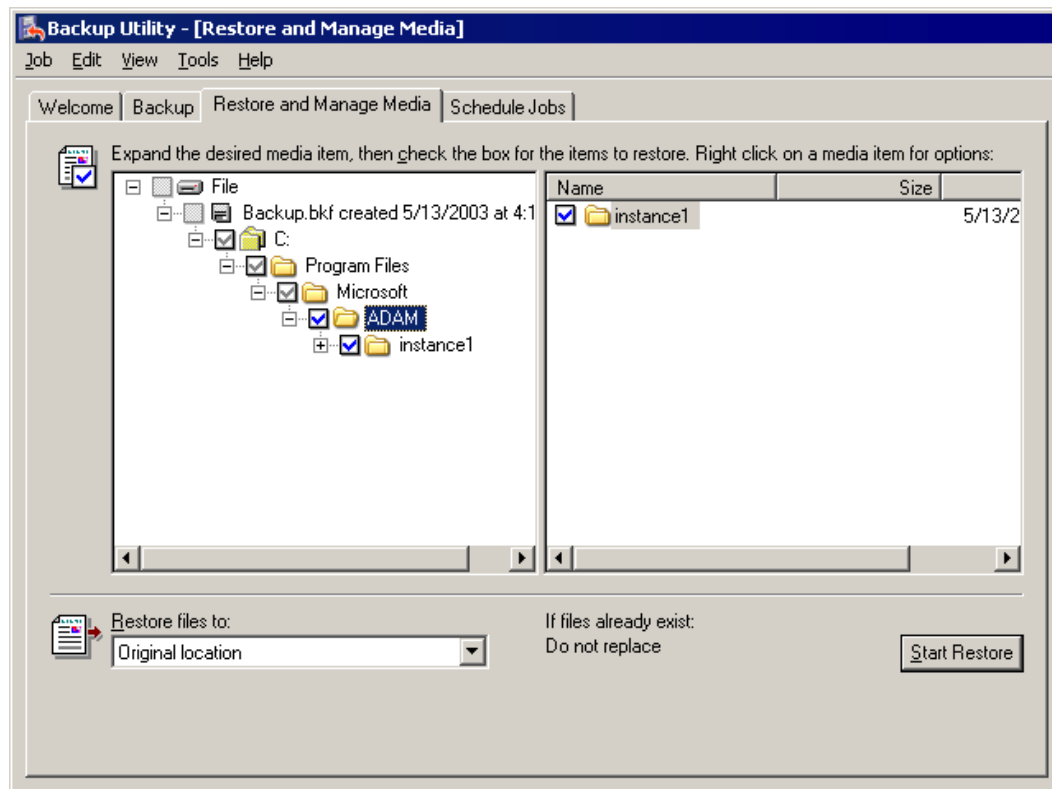
2. Click **Remove**, and then click **Yes**. Active Directory Application Mode is now removed from your computer.

Restoring an ADAM Instance

In this exercise, you restore your ADAM instance from the backup that you made in the previous exercise.

▶ To restore an ADAM instance

1. Create an ADAM instance following the steps in [Installing ADAM](#). Use the same settings as you did during your first ADAM installation except, in this case, do not create an application directory partition during setup. You can restore your original application directory partition from your backup. Therefore, on the **Application Directory Partition** page in the Active Directory Application Mode Setup Wizard, click **No, do not create an application directory partition**.
2. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
3. Click the **Advanced Mode** link in the **Backup or Restore Wizard**.
4. Click the **Restore and Manage Media** tab. To select the ADAM instance that you want to restore, in the details pane, select the check box to the left of the instance1 folder, as shown in the following:



5. In **Restore files to**, click **Original location**.
6. On the **Tools** menu, click **Options**, click the **Restore** tab, click **Always replace the file on my computer**, and then click **OK**.
7. Click **Start Restore**.
8. If you receive a message asking if you want to restart your computer, click **Yes**.
9. After the restore is complete, close the Backup application.
10. To confirm that the data from your original ADAM instance is successfully restored, use ADAM ADSI Edit to confirm that the O=Microsoft,C=US directory partition is restored and that the OU=ADAM users OU and the Mary Baker user account exist in the partition.

Managing Configuration Sets

In the following exercises, you create new ADAM instances by replicating your existing ADAM instance. By doing so, you also create an ADAM configuration set. ADAM instances in a configuration set replicate a common schema partition and configuration partition, and they can also replicate application directory partitions (such as O=Microsoft,C=US) to each other.

In the following exercises, you install two replica ADAM instances. You create the first replica instance by using the Active Directory Application Mode Setup Wizard. You create the second replica instance by using unattended installation. You then configure the replication schedule for your configuration set.

Note

In a production environment, ADAM instances belonging to the same configuration set cannot reside on the same computer. You can have multiple ADAM instances running on a computer, but they must belong to different configuration sets. However, for the purposes of this guide, if you do not have a second computer available, you can install your replica ADAM instances on your first computer.

Installing a Replica Using the Active Directory Application Mode Setup Wizard

You can install an ADAM replica instance by using the Active Directory Application Mode Setup Wizard.

To install an ADAM instance replica by using the Active Directory Application Mode Setup Wizard

1. Start the Active Directory Application Mode Setup Wizard, either on your second computer (if you have one) or on your first computer: click **Start**, click **All Programs**, point to **ADAM**, and then click **Create an ADAM instance**. Follow the steps in the wizard until you reach the **Setup Options** page.
2. On the **Setup Options** page, click **A replica of an existing instance**, and then click **Next**.
3. On the **Instance Name** page, accept the default name instance2 (or instance1, if you are installing ADAM on a second computer), and then click **Next**.

 **Note**

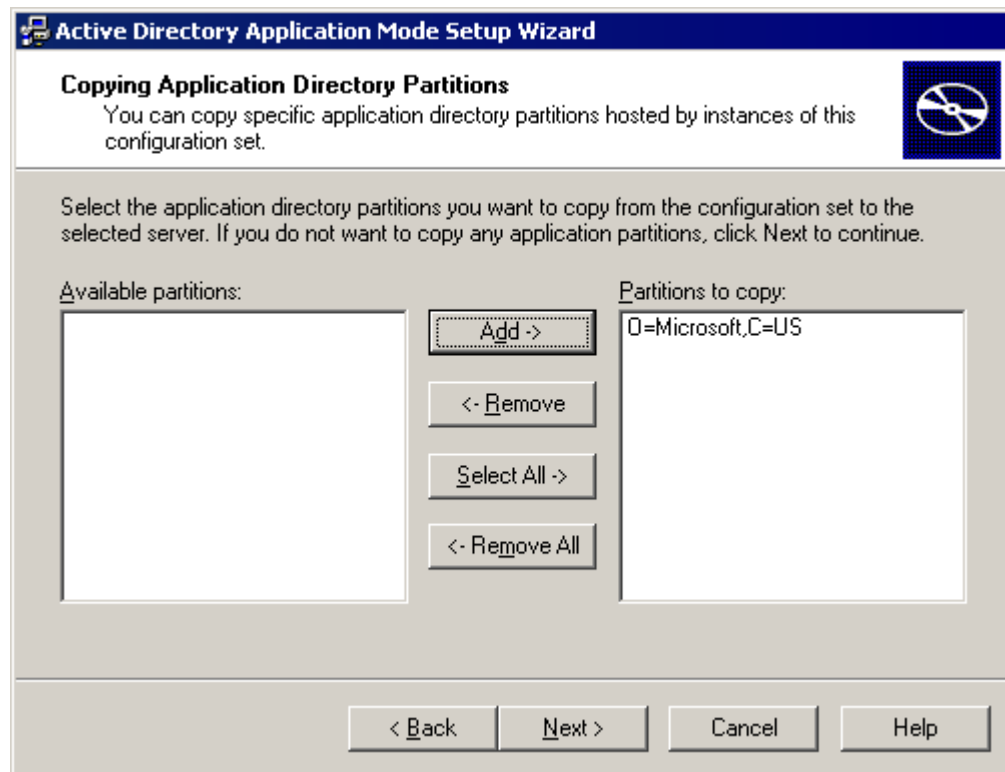
ADAM instance names need to be unique only on a given computer.

4. On the **Ports** page, accept the default values of 50000 and 50001 (if you are installing onto the first computer) or 389 and 636 (if you are installing onto a second computer), and then click **Next**.
5. On the **Joining a Configuration Set** page, in **Server**, type the host name or DNS name of the computer where the first ADAM instance is installed. Then, type the LDAP port number in use by the first ADAM instance (which is 389 by default), and then click **Next**.

 **Note**

You must use a valid host name or DNS name, rather than an IP address or localhost when specifying a server on the **Joining a Configuration Set** page of the Active Directory Application Mode Setup Wizard.

6. On the **Administrative Credentials for the Configuration Set** page, click the account that is used as the ADAM administrator for your first ADAM instance.
7. On the **Copy Application Partition** page, select the application directory partitions that you want to replicate to the new ADAM instance. (The schema and configuration partitions will be replicated automatically.) To select the O=Microsoft,C=US directory partition for replication, in **Available partitions**, click **O=Microsoft,C=US**, and then click **Add**. The **Active Directory Application Mode Setup Wizard** looks like the following:



8. Click **Next**.
9. Accept the default values on the remaining Active Directory Application Mode Setup Wizard pages by clicking **Next** on each page, and then click **Finish** on the Completing the Active Directory Application Mode Setup Wizard page.
10. After the installation is complete, use ADAM ADSI Edit to confirm that the O=Microsoft,C=US directory partition has been replicated to your second ADAM instance.

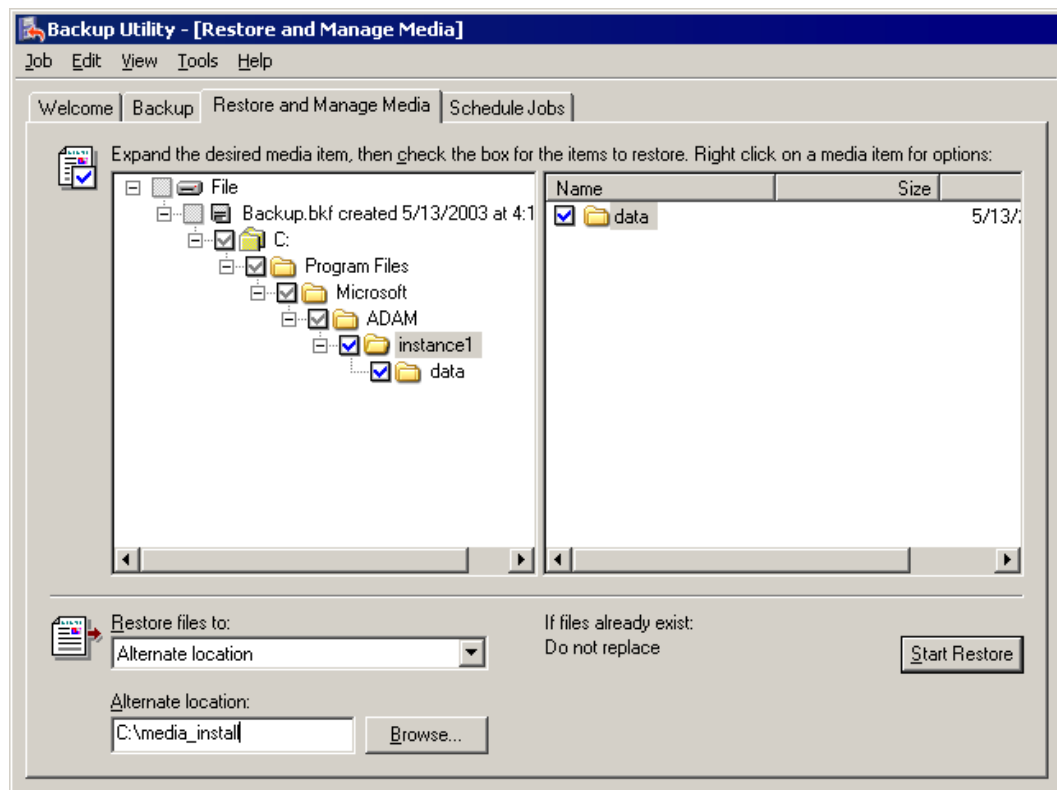
Installing a Replica from Media by Using Unattended Installation

In addition to using the Active Directory Application Mode Setup Wizard, you can also install an ADAM instance replica from media. For this type of installation, you must use a restored copy of an ADAM backup as the media and unattended installation as the installation method.

First, you restore your ADAM instance backup to an alternate location, rather than to the original location, so that you do not overwrite your first ADAM instance. Then you create an answer file and perform the unattended installation.

► **To install an ADAM instance replica by using unattended installation**

1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. Use the Backup application to restore the backup of your original ADAM instance, as you did previously. But this time, in **Restore files to**, click **Alternate location** instead of **Original location**, and then type or browse to an alternate directory path to which you want to restore the files, as shown in the following.



3. After restoring the backup files, create an answer file for the ADAM unattended installation. An answer file provides the values for the ADAM setup options (the same options that are provided in the Active Directory Application Mode Setup Wizard). Using any text editor, create a text file called Answer.txt, and then add the following contents to the file. Be sure to replace *servername* with the host name or DNS name

of the computer on which your first ADAM instance is running. Replace `C:\media_install\Program Files\Microsoft\ADAM\instance1\data` with the path to your restored copy of the first ADAM instance.

```
[ADAMInstall]
; The following line specifies to install a replica ADAM instance.
InstallType=Replica
; The following line specifies the name to be assigned to the new instance.
InstanceName=instance3
; The following lines specify the communication ports to use for LDAP and
SSL.
LocalLDAPPortToListenOn=50002
LocalSSLPortToListenOn=50003
; The following lines specify the directory location of the restored files.
ReplicationDataSourcePath=C:\media_install\Program
Files\Microsoft\ADAM\instance1\data
ReplicationLogSourcePath=C:\media _install\Program
Files\Microsoft\ADAM\instance1\data
; The following lines specify a computer name and ADAM port of an ADAM
instance in the
; configuration set you want to join
; Replace servername with the name of the computer on which your first ADAM
; instance is running
SourceServer=servername
SourceLDAPPort=389
```

4. After saving your Answer.txt file, you are ready to run the unattended installation. At a command prompt, type the following:

```
Drive:\path\adamsetup /c:"adaminstall.exe /answer:drive:\pathname\answer.txt"
```

where the first *drive:\path* is the location of your ADAM download and the second *drive:\pathname* is the location of the Answer.txt file that you created.

5. After running this command, you can confirm by using the Services snap-in that a new ADAM instance is installed and running.2

Configuring the Replication Schedule

Now that you have multiple ADAM instances joined in a single configuration set, you can schedule replication. Scheduling replication is optional. As with Active Directory, ADAM always provides a default replication schedule.

To schedule replication between ADAM instances

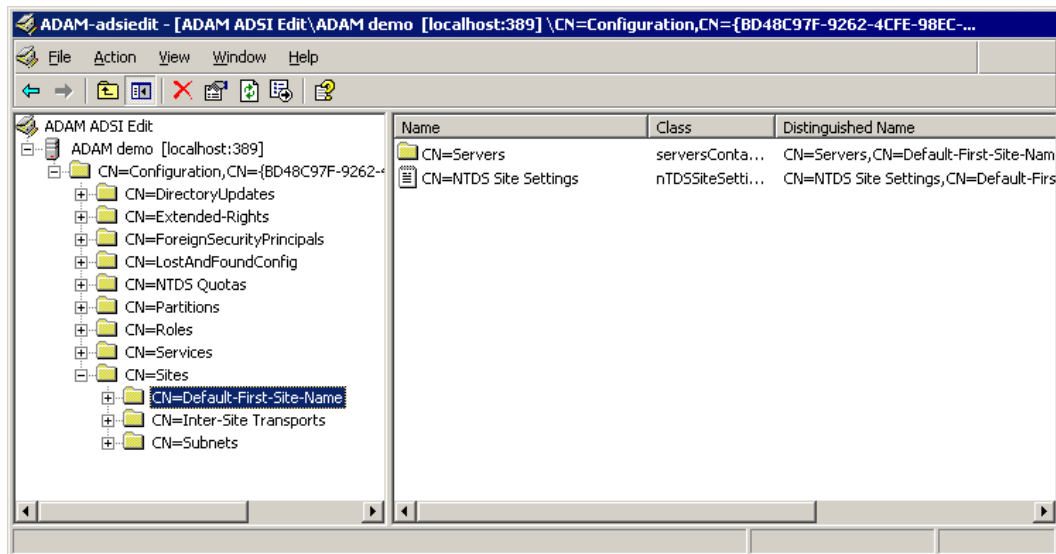
1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM ADSI Edit**.

2. Connect and bind to one of your ADAM instances.

 **Note**

Because all of your ADAM instances belong to the same configuration set, you can schedule replication on any one of them.

3. In the console tree, double-click the configuration partition **CN=Configuration,CN={GUID}**, where **GUID** is the unique identifier assigned during ADAM setup; double-click the sites container, CN=Sites; and then double-click the default sites container, **CN=Default-First-Site-Name**. The **ADAM ADSI Edit** snap-in looks like the following:

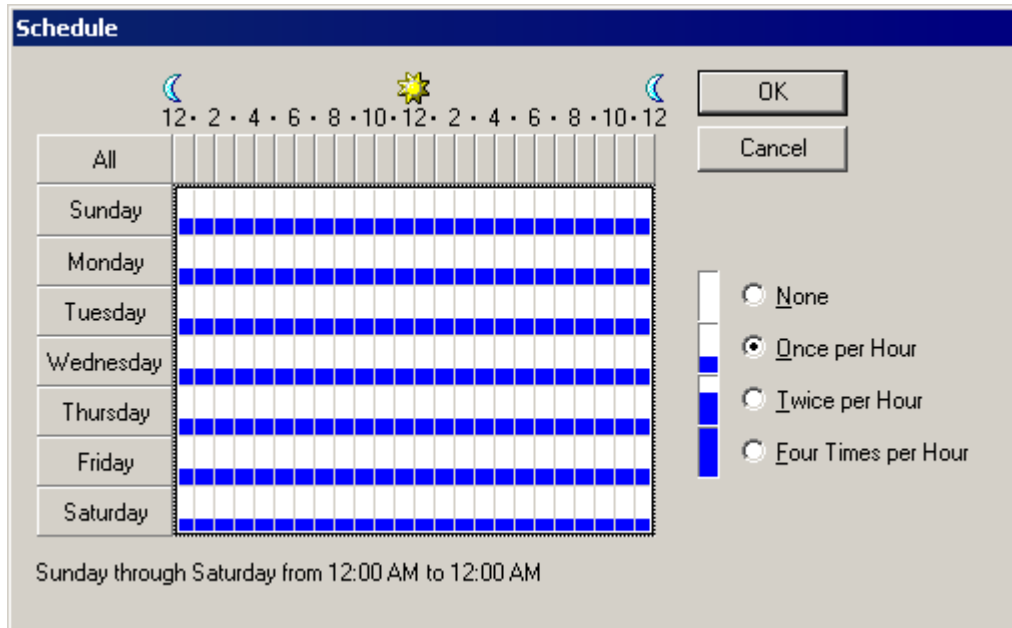


 **Note**

By default, all ADAM instances that you create belong to a single site, Default-First-Site-Name. In this exercise, all your ADAM instances belong to a single site. Therefore, you are scheduling replication within a site, which is called intrasite replication. For more information about ADAM sites, configuration sets, and replication, see the Active Directory Application Mode Administrator's Guide. To view the Active Directory Application Mode Administrator's Guide, click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Help**.

4. In the details pane, right-click **CN=NTDS Site Settings**, and then click **Schedule**.
5. In the **Schedule** dialog box, select the block of time that you want to schedule; click **None**, **Once per Hour**, **Twice per Hour**, or **Four Times per Hour** as the replication

frequency; and then click **OK**. The **Schedule** dialog box looks like the following:



Note

For intrasite replication, ADAM instances replicate changes through update notifications. The replication frequency schedule only affects intrasite replication when no update notifications occur in the specified time.

Causing Immediate Replication of a Directory Partition

The Active Directory Application Mode Setup Wizard installs an ADAM version of Repadmin.exe, which includes the same functionality as the Active Directory version of Repadmin.exe. As with Active Directory, you can cause the immediate synchronization of a directory partition with replication partners by using Repadmin.exe, as described in this exercise.

To cause immediate replication of a directory partition using Repadmin.exe

1. Click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type the following:

reppadmin /syncall localhost:389 o=Microsoft,c=us

 **Note**

For more information about **reppadmin** syntax, at the ADAM Tools Command Prompt, type **reppadmin /?**.

Administering ADAM Programmatically

You can accomplish programmatically many of the tasks that you can complete manually using the ADAM administration tools. The ADAM download includes several sample scripts and some sample code to help get you started.

Administering ADAM Programmatically Through Visual Basic Scripts

The \LABS_DEMO\LABS\VBScript directory in the ADAM download includes sample scripts that are produced in Microsoft® Visual Basic®, Scripting Edition (VBScript), for the following common operations:

- Extend schema to include the contact class. (Adamcontact.vbs)
- Import two contacts. (AdamContactImport.vbs)

The following scripts assume that Adamuser.ldf was imported in a previous exercise:

- Add OU
- Add user
- Add group
- Add user to group
- Delete user
- Get a list of specific objects in a path (Filter_adam.vbs)
- Enumerate users and groups
- Set password

For example, the script for enumerating users and groups contains the following code:

```
! *****
```

```

'
' This script enumerates the users and groups in the passed in OU
' To run: cscript member_adam.vbs [OU] [Group]
' Examples: cscript member_adam.vbs ou=testou,c=us testuser
'
'*****
set Args = Wscript.Arguments
ouName = Args(0)
' If the application OU DN is "ou=adamou,c=us" and the server is "adamhost" and
the port is 389. Then this parameter should be passed
' as follows: "LDAP://adamhost:389/ou=adamou,c=us"

set ou = GetObject(ouName )
wscript.echo "Displaying Groups and Group membership..." & vbcrLf

ou.Filter = Array("group")
for each obj in ou
  wscript.echo "Group : " & obj.Name
  for each member in obj.Members
    wscript.echo "      |"
    wscript.echo "      -- " & member.Name
  Next
  wscript.echo vbcrLf
Next

```

You can run any of these scripts from a command prompt, using the **cscript** command. (For help with **cscript**, at a command prompt, type **cscript /?**.) Each script requires that the distinguished names of both the provider and the host be passed, along with the port specifier.

Note

The Adamcontact.vbs script only requires *servername:portnumber* to be passed, because it extends the schema. You can open the file in Notepad to see the specific syntax. (If you run a script without parameters, the following error message is returned: "Subscript out of range.")

For example, to run the Member_adam.vbs script to enumerate users and groups of an object with a distinguished name of O=Microsoft,C=US, type:

cscript member_adam.vbs "LDAP://servername:portnumber /o=Microsoft,c=us"

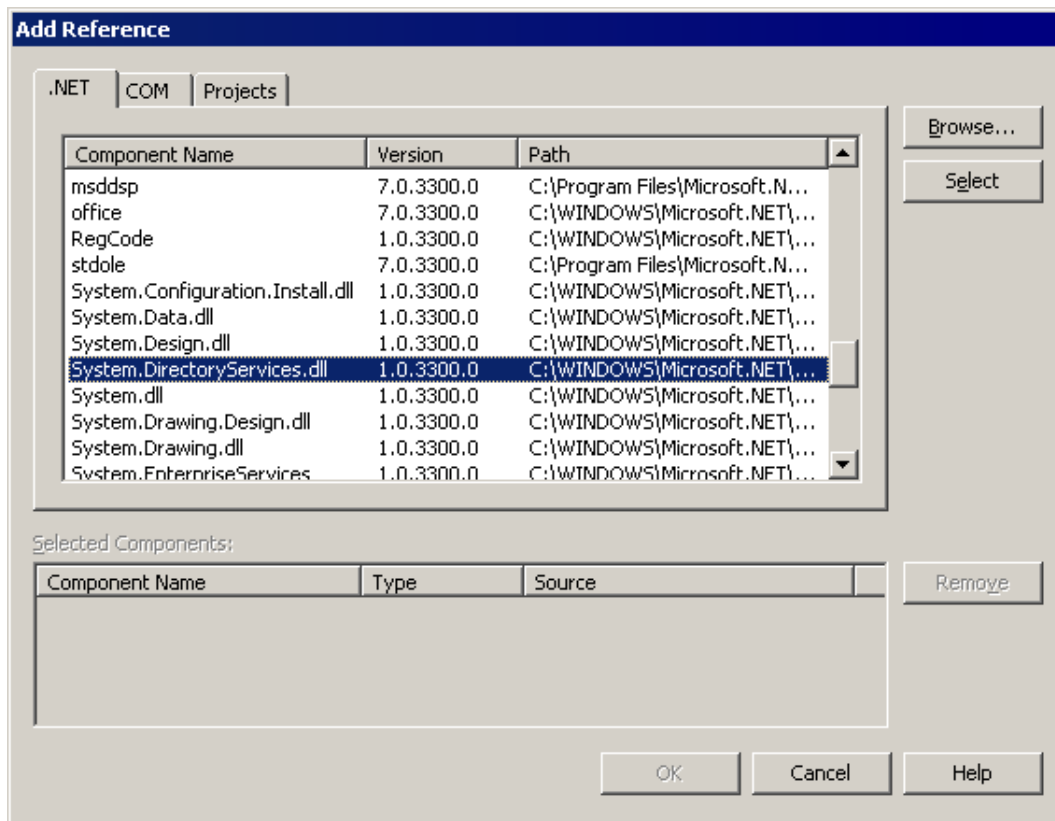
where *servername:portnumber* represents the computer name and LDAP communications port of your ADAM instance.

Administering ADAM Programmatically Through the System.DirectoryServices API

The following exercise requires that you have Microsoft® Visual Studio® .NET installed.

▶ **To access ADAM through the System.DirectoryServices Application Programming Interface (API)**

1. Start Visual Studio .NET.
2. On the **File** menu, click **New**, and then click **Project**.
3. In **Project Types**, click a project type (**C#**, **VB.NET**, and so on).
4. In **Templates**, click a project template (**Console**, **Windows**, and so on).
5. In **Name**, type a name for your project.
6. After the project is created, click **Add Reference** on the **Project** menu.
7. In the **Component Name** column, click **System.DirectoryServices.dll**, as shown in the following.



8. Add the following line at the top of your code:

```
C#:
using System.DirectoryServices;
VB.NET:
Imports System.DirectoryServices;
```

 **Note**

Adding the namespace name is not mandatory, but it is easier than typing a long name. For example instead of `System.DirectoryServices.DirectoryEntry`, use `DirectoryEntry`.

9. To read an ADAM object, add the following code:

```
int portNumber=1025; // put the correct port number here.
String serverName="adam01"; // put the correct servername here.
String partitionDir = "O=Fabrikam"; //put the correct partition
distinguished name.
DirectoryEntry ent = new
    DirectoryEntry("LDAP://" + serverName + ":" + portNumber + "/" + partitionDir);
```

```
Console.WriteLine("Hello World, {0}, with Guid {1}", ent.Name, ent.Guid);
```

Administering ADAM Proxy Objects Programmatically

The \LABS_DEMO\LABS\bindredirect directory in the ADAM download includes sample code for creating, populating, and testing ADAM proxy objects. In addition, the directory includes a compiled, ready-to-run version of this sample code. This sample code illustrates how you can automate the creation of proxy objects, and it completes the steps in the “To bind to ADAM through an ADAM proxy object” procedure in [Using the ADAM Administration Tools](#).

Note

For more information about ADAM bind redirection, see the Active Directory Application Mode Administrator's Guide. To view the Active Directory Application Mode Administrator's Guide, click **Start**, point to **All Programs**, point to **ADAM**, and then click **ADAM Help**.

The code in sampleBindRedirect.c completes all of the following operations programmatically:

- Binds to an ADAM instance using a Windows user account that you provide.
- Reads the **tokenGroups** attribute for the Windows user to retrieve the user's SID.
- Binds to an ADAM instance using the ADAM Administrator's account that you provide.
- With the ADAM administrator account, creates a userProxy object for the Windows user.
- Adds the Users group from any given application directory partition to the Readers group of the same partition.
- Binds to an ADAM instance as the Windows user, to demonstrate that the Windows user cannot read the application directory partition.
- Binds to an ADAM instance through the proxy object, to demonstrate that the application directory partition can be read.
- Deletes the userProxy object.

You can run the compiled version of this sample code, BindRedirect.exe, to observe how the sample code works. For help running the BindRedirect.exe sample program, at a command prompt, type **bindredirect /?**.

 **Note**

This sample code runs with the following requirements:

To run properly, SSL connections to ADAM must be available (which requires the installation of certificates), or the RequireSecureProxyBind attribute on the msds-Other-Settings attribute of nTDSservice object must be set to 0. For more information, see “Binding Security and ADAM Proxy Objects” in [Managing Authentication in ADAM](#).

No foreign security principal object should exist in ADAM for the Windows user that you specify.

When using an SSL connection and binding, you must provide the full DNS name of the computer running ADAM.