



Operating System

Managing the Active Directory

Beta 3 Technical Walkthrough

Abstract

This walkthrough introduces you to administration of the Microsoft® Windows® 2000 Active Directory™ directory service. The procedures in this document demonstrate how to use the Active Directory Users and Computers snap-in to add, move, delete, and alter the properties for objects such as users, contacts, groups, servers, printers, and shared folders.

© 1999 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, Windows, Windows NT and the Windows logo are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA
0599*

CONTENTS

INTRODUCTION	1
Installation Requirements	1
Walkthrough Tasks	1
USING THE ACTIVE DIRECTORY DOMAINS AND TRUSTS SNAP- IN	2
Starting the Active Directory Domains and Trusts Snap-in	2
Changing the Domain Mode	3
USING THE ACTIVE DIRECTORY USERS AND COMPUTERS SNAP-IN	5
Starting the Active Directory Users and Computers Snap-in	5
Navigating the Active Directory Users and Computers Snap-in	5
Description of Active Directory Objects	6
Adding an Organizational Unit	7
Creating a User Account	8
Adding Information about the User	9
Moving a User Account	10
Creating a Group	11
Adding a User to a Group	12
Publishing a Shared Folder	13
Publishing a Printer	16
Windows 2000 Printers	16
Non-Windows 2000 Printers	17
Creating a Computer Object	19
Managing Computers	19
Renaming, Moving, and Deleting Objects	20
Nested Groups	21
FINDING SPECIFIC OBJECTS	23
FILTERING A LIST OF OBJECTS	24
FOR MORE INFORMATION	26
Before You Call for Support	26
Reporting Problems	26

INTRODUCTION

This document introduces you to administration of the Microsoft® Windows® 2000 Active Directory and the Active Directory Users and Computers snap-in.

This snap-in allows you to add, move, delete, and alter the properties for objects such as users, contacts, groups, servers, printers, and shared folders.

Installation Requirements

You must have installed the Beta 3 release of Windows 2000 Server (including the Active Directory) on a server in your network. You can run the administration tools from the server, or you can run the tools from a Beta 3 release of Windows 2000 Professional.

The administration tools are installed by default on all Windows 2000 domain controllers. On Windows 2000 stand-alone servers or workstations, the Active Directory administration tools are optional and can be installed from the Optional Windows 2000 components package.

Walkthrough Tasks

In this walkthrough you will perform the following tasks.

Common Administrative Tasks

- Creating Organizational Units
- Creating Users and Contacts
- Creating Groups and adding members to Groups

Advanced Administrative Tasks

- Publishing shared network resources, such as shared folders and printers in the directory.
 - Moving Users, Groups, and Organizational Units in the directory
 - Using Filters and Searches to retrieve objects from the directory
-

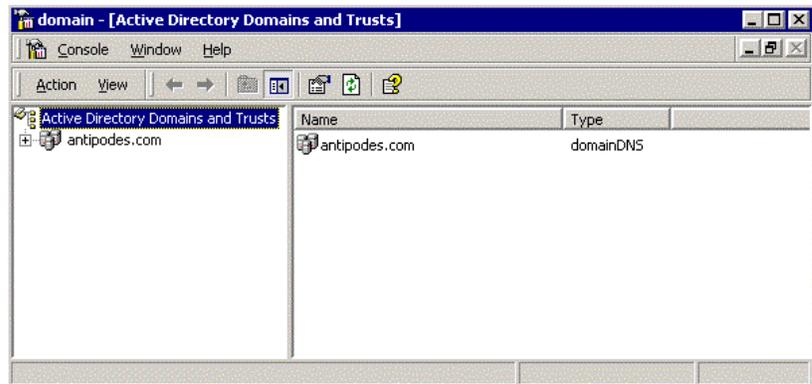
USING THE ACTIVE DIRECTORY DOMAINS AND TRUSTS SNAP-IN

The Active Directory Domains and Trusts snap-in provides a graphical view of all domain trees in the forest. Using this tool, an administrator can manage each of the domains in the forest, manage trust relationships between domains, configure the mode of operation for each domain (Native or Mixed Mode), and configure the alternative User Principal Name (UPN) suffixes for the forest.

Starting the Active Directory Domains and Trusts Snap-in

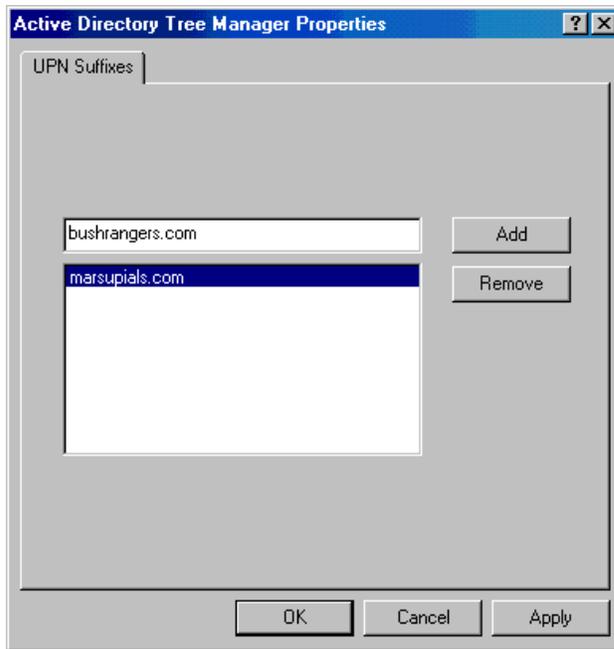
To start the Active Directory Domains and Trusts snap-in

1. Log on as an Administrator. If you log on using an account that does not have administrative privileges, you may not be able to manage the Active Directory.
2. Click the **Start** button, point to **Programs**, and then click **Administrative Tools**.
3. Click **Active Directory Domains and Trusts**. A window similar to the following appears.



4. Add alternate User Principal Name suffixes. The User Principal Name (UPN) provides an easy-to-use naming style for users to log on to the Active Directory. The style of the UPN is based on Internet standard RFC 822, which is sometimes referred to as a *mail address*. The default UPN suffix is the forest DNS name, which is the DNS name of the first domain in the first tree of the forest. In this walkthrough, the default UPN suffix is **antipodes.com**.
5. Select the root node of the **Active Directory Domains and Trusts**, right-click, and select **Properties**.
6. Add the following UPN suffixes:

marsupials.com
bushrangers.com



7. You can manage each of the domains shown in the tree view by starting the Active Directory Users and Computers snap-in. Select the domain node for **antipodes.com**, right-click, and select **Manage**.

To continue with managing objects in the directory, see the section, “Using the Active Directory Users and Computers Snap-in,” in this document.

Changing the Domain Mode

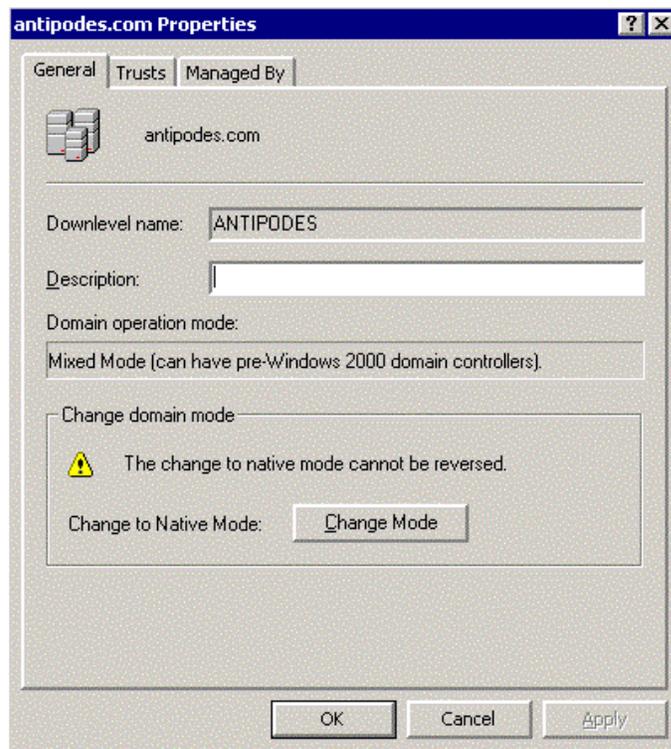
Windows 2000 domains operate in either of two modes:

- *Mixed Mode*, which allows domain controllers running both Windows 2000 and earlier versions of Windows NT Server to co-exist in the domain. In mixed mode, the domain features from previous versions of Windows NT Server are still enabled, while some Windows 2000 features are disabled.
- *Native Mode*, in which all the domain controllers must run Windows 2000 Server. In Native Mode, you can take advantages of new features such as Universal groups, nested group membership, and inter-domain group membership.

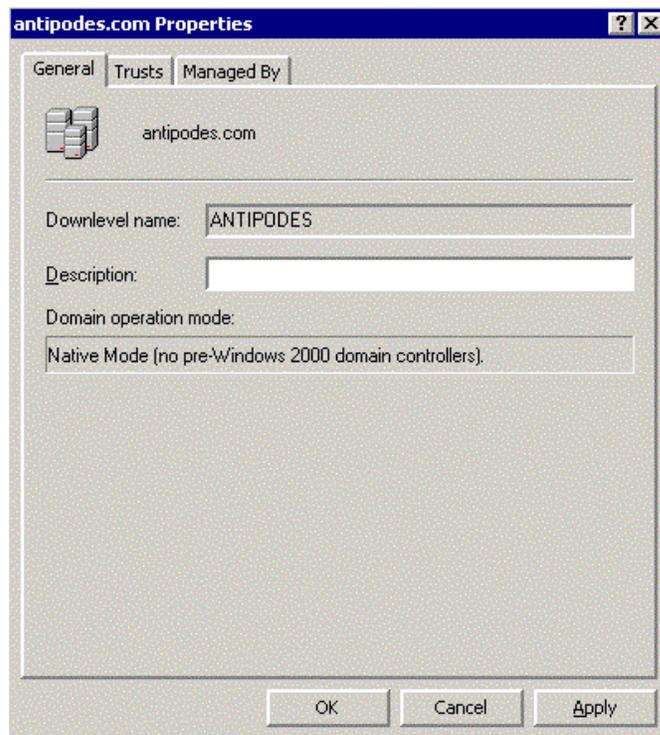
When a domain is first installed, it is in mixed mode. The mode of operation can be changed from mixed mode to native, but this is not reversible. In native mode, downlevel Windows NT 4.0 Domain Controllers are not supported.

To switch to native mode

1. Make sure all domain controllers in your domain are running Windows 2000 Server.
2. Right-click the domain object, and then click **Properties**. A window similar to the following appears.



3. Click the **Change Mode** button.
4. Restart the domain controller.



USING THE ACTIVE DIRECTORY USERS AND COMPUTERS SNAP-IN

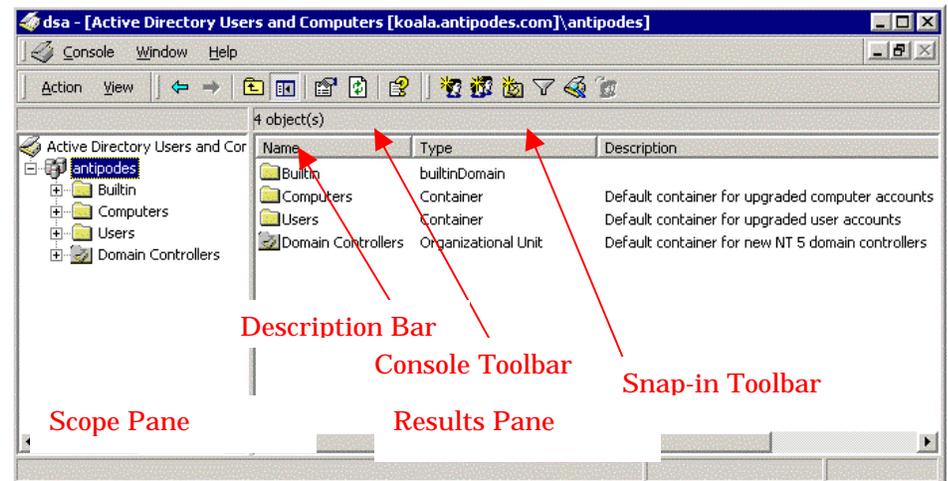
Starting the Active Directory Users and Computers Snap-in

To start the Active Directory Users and Computers snap-in

1. Log on as an Administrator. If you log on using an account that does not have administrative privileges, you may not be able to create several directory objects.
2. Start the Active Directory Users and Computers snap-in. There are several methods for starting this snap-in:
 - You can invoke the Active Directory Users and Computers snap-in from the Active Directory Domains and Trusts snap-in (as described in the previous section), or
 - You can load the snap-in from the Administration Tools menu. From the **Start** button, point to **Programs**, and then click **Administrative Tools**. Click **Active Directory Users and Computers** to start the snap-in.

Navigating the Active Directory Users and Computers Snap-in

The following illustration and table identify the key components of the Active Directory Users and Computers snap-in.



Object	Description
Scope Pane	Shows all of the container objects.
Results Pane	Shows all objects contained within the selected object in the scope pane.
Console Toolbar	Toolbar associated with the Management Console.
Snap-In Toolbar	Toolbar associated with the Active Directory Users and Computers snap-in.
Description Bar	Indicates whether snap-in is operating in Advanced or Normal Mode,

	whether a filter is applied, and the number of objects displayed in the results pane.
Context Menu	Lists actions that can be performed on selected object/
Wizard	Consists of a series of dialogs to guide you through a number of steps.
Property Sheets	Tabbed dialogs used to display the attributes of an object.

Description of Active Directory Objects

The objects described in the following table are created during installation of the Active Directory, either during a fresh installation or upgrade of a Windows NT 4.0 domain.

Icon	Folder	Description
	Domain	The root node of the snap-in represents the domain being administered.
	Computers	Contains all Windows NT and Windows 2000 computers that join a domain. This includes computers running Windows NT versions 3.51 and 4.0, as well as those running Windows 2000. If you upgrade from a previous version, Active Directory migrates the machine account to this folder. You can move these objects.
	System	Contains Active Directory systems and services information, such as RPC, WinSock, and other information.
	Users	Contains all the users in the domain. In an upgrade, all users from the previous domain will be migrated. Like computers, the user objects can be moved.

You can use the Active Directory to create the following objects.

Icon	Object	Description
	User	A user object is an object that is a security principal in the directory. A user can log on to the network with these credentials and access permissions can be granted to users.
	Contact	A contact object is an account that does not have any security permissions. You cannot log on to the network as a contact. Contacts are typically used to represent external users for the purpose of e-mail.
	Computer	An object that represents a computer on the network. For Windows NT workstations and servers, this is the machine account.



Organizational Unit

Organizational units are used as containers to logically organize directory objects such as users, groups, and computers in much the same way that folders are used to organize files on your hard disk.



Group

Groups can contain users, computers, and other groups. Groups simplify the management of large numbers of objects.



Shared Folder

A shared Folder is a network share that has been published in the directory.



Shared printer

A shared printer is a network printer that has been published in the directory

Adding an Organizational Unit

The following procedure creates an organizational unit in the **antipodes** domain. Note that you can create nested organizational units, and there is no limit to the nesting levels.

To add an organizational unit (OU)

1. Right-click a domain object.
2. Either select **New**, and click **Organizational Unit**, or use the **New Organizational Unit** toolbar button. Type the following as the name of your new organizational unit:

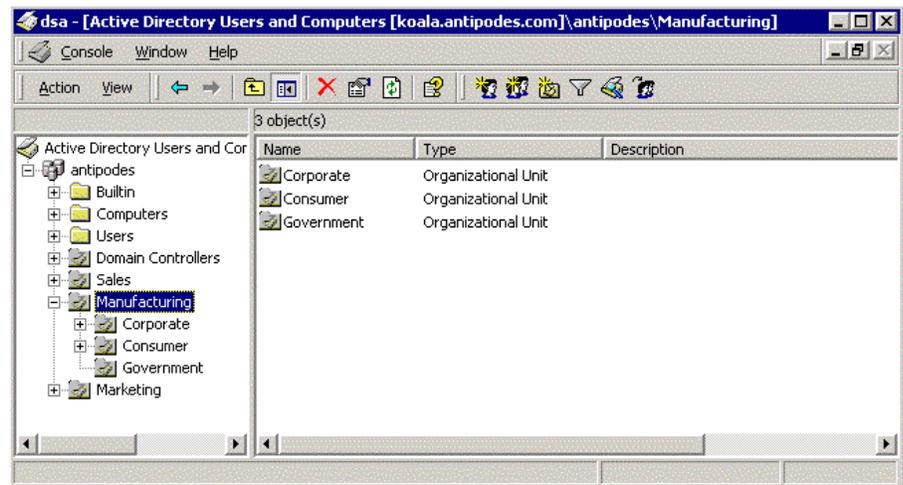
Sales

3. Click **OK**.

For the rest of the exercises in this walkthrough, please repeat steps 1 and 2 above to create additional organizational units, as follows:

- Create another organizational unit called **Marketing** under your domain.
- Create another organizational unit called **Manufacturing** under your domain.
- Create another organizational unit called **Consumer** under the **Manufacturing** organizational unit. (To do this, right-click **Marketing**, click **New**, and then click **Organizational Unit**.)
- Create two more organizational units called **Corporate** and **Government** under the **Manufacturing** organizational unit.

When you are finished, you should have the following hierarchy:



Creating a User Account

The following procedure creates the user account **John Smith** in the **Sales** organizational unit.

To create a new user account

1. Right-click the **Sales** organizational unit, click **New**, and then click **User**, or use the **New User** toolbar button.
2. Type the following user information:

In this Text Box	Type this
First Name	John
Last Name	Smith
Full Name	John Smith
Logon Name	jsmith

Create New Object - (User)

Create in: antipodes.com/Sales

First name: John

Last name: Smith

Full name: John Smith

User logon name: jsmith @antipodes.com

Downlevel logon name: ANTIPODES/ jsmith

< Back Next > Cancel

3. Type a password in both the **Password** and **Confirm password** boxes, and select the appropriate account options.

Create New Object - (User)

Create in: antipodes.com/Sales

Password: xxxxxxxx

Confirm password: xxxxxxxx

User must change password at next logon

User cannot change password

Password never expires

Account disabled

< Back Next > Cancel

4. Accept the confirmation dialog. You have now created an account for John Smith in the Sales organizational unit.

Adding Information about the User

To add user information

1. Right-click the user object, and click **Properties**.
2. Add more information about the user (as shown in the following illustration), and

click **OK**.

The image shows a Windows XP dialog box titled "John Smith Properties". The "General" tab is active, displaying a user profile for John Smith. The fields are as follows:

First name:	John
Last name:	Smith
Description:	Senior Sales Representative
Office:	Regional Headquarters 12/1054
Telephone:	(206) 874 1288
E-Mail:	jsmith@antipodes.com
Home page:	http://www.antipodes.com/emplo

Buttons for "OK", "Cancel", and "Apply" are located at the bottom of the dialog box.

Moving a User Account

Users can be moved from one organizational unit to another in the same domain or a different domain. For example, in this procedure, John Smith moves from the Sales division to the Marketing division.

To move the user account

1. Select the **Sales** organizational unit.
2. Select John Smith's user account, **right-click**, and select **Move**.
3. Click **Browse**, select the **Marketing** organizational unit, and click **OK**.



Note: Drag-and-drop administration of users is not supported in this Beta release.

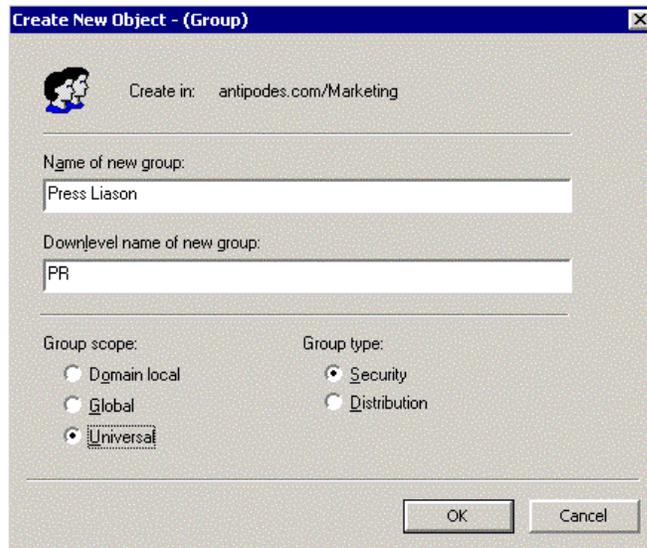
If you upgrade from a previous version of Windows NT Server, you may want to move existing users from the **Users** folder to some of the organizational units that you have created.

Creating a Group

To create a group

1. Either right-click the **Marketing** organizational unit, click **New**, and then click **Group**, or select the **Create New Group** button on the toolbar.
2. In the **Name of New Group** text box, type

`Press Liaison`



3. Select the appropriate **Group type** and **Group scope**:

- The **Group type** indicates whether or not the group can be used to assign permissions to other network resources, such as files and printers. Both security and distribution groups can be used for e-mail distribution lists.
- The **Group scope** determines the visibility of the group and what type of objects can be contained within the group.

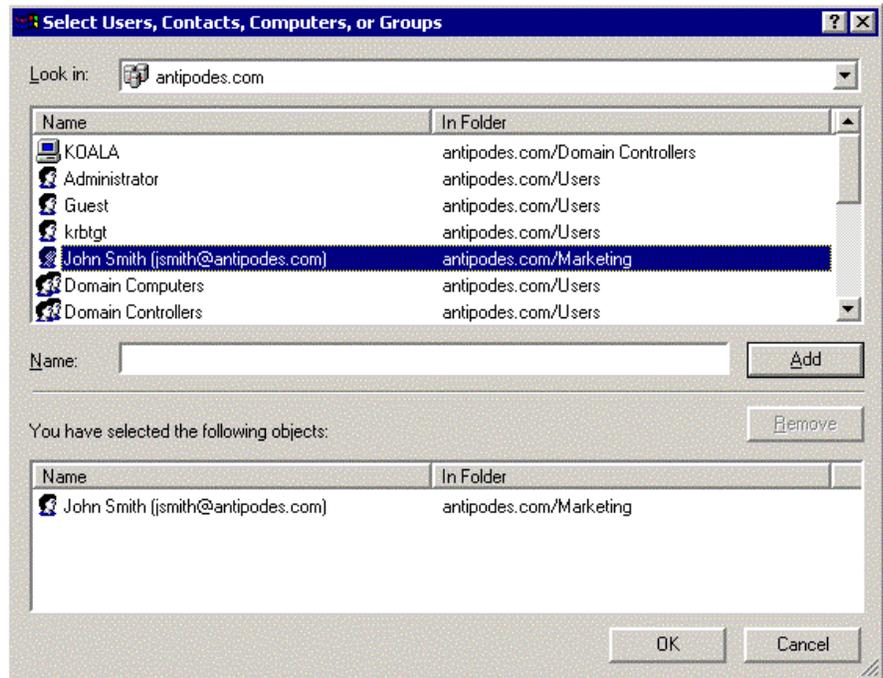
Scope	Visibility	May contain
Domain Local	Domain	Users, Global, or Universal Groups
Global	Tree	Users or Global groups
Universal	Forest	Users, Global, or Universal Groups

Adding a User to a Group

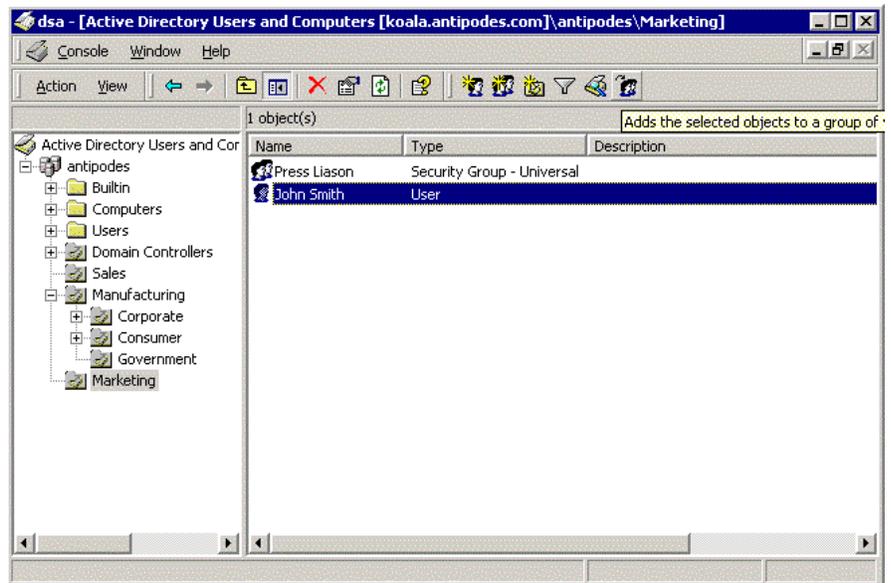
To add a user to a group

1. Right-click the **Press Liaison** group, and click **Properties**.
2. On the **Members** Tab, then click **Add**.
3. This will start the Find dialog. You can use this dialog to scope your query to the forest, a specific domain, or an organizational unit.
4. Click **John Smith**, and click **Add**.

Note: You can select multiple users or groups in this dialog by holding down the CTRL key while you click them. You can also type the name directly. If the name is ambiguous, a further list is displayed to confirm your selection.



Alternatively, you can select the users from the results pane, and then select the **Add to Group** context menu item or toolbar button. This may be more efficient for adding large numbers of members to a group.



Publishing a Shared Folder

Any shared network folder, including a Distributed File System (DFS) folder, can be published in the directory. Creating a Shared folder object in the directory does not automatically share the folder. This is a two-step process: you must first share the folder, and then publish it in the directory.

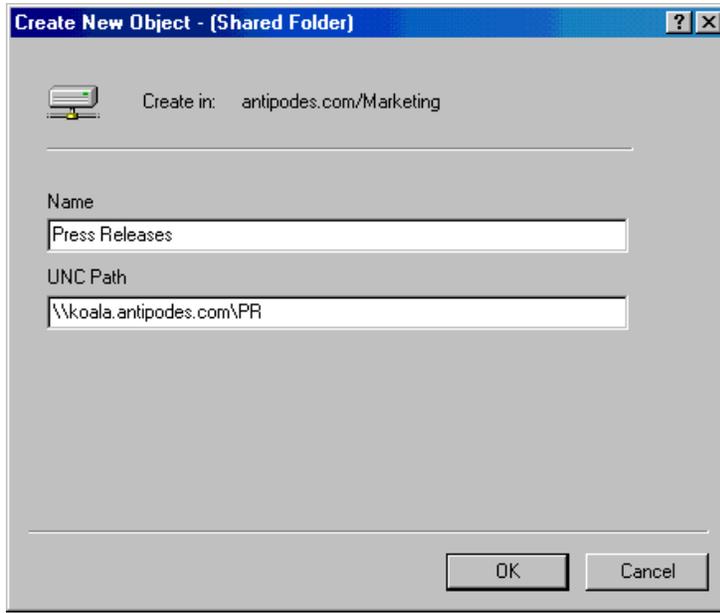
To share a folder

1. Use Windows NT Explorer or the command line to create a new folder called **Press Releases** on one of your disk volumes.
2. In Windows NT Explorer, right-click the folder name, click **Properties**, click the **Sharing** tab, and click **Shared As**.
3. In the **Share Name**, type
`PR`
4. Click **OK**.
5. Populate the folder with files, such as documents, spreadsheets, or presentations.

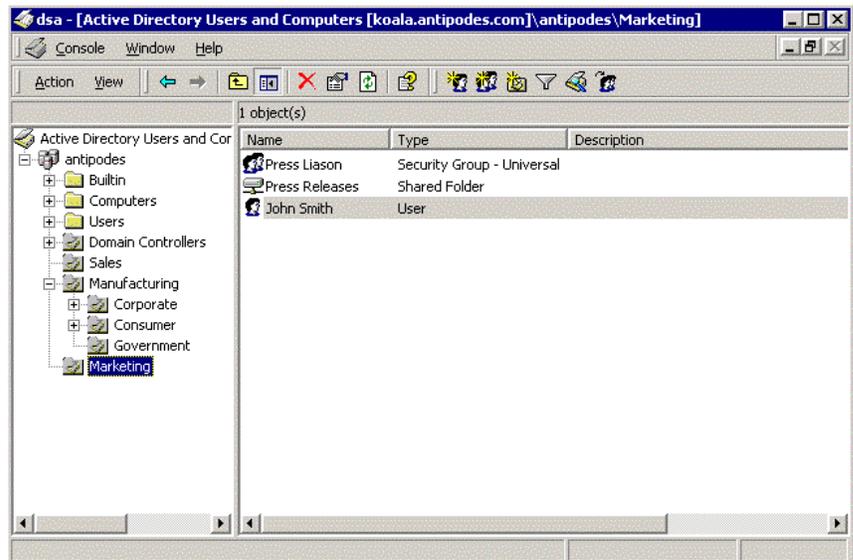
You can also set up a Dfs volume. For more information see the "Distributed File System" walkthrough document.

To publish the shared folder in the directory

1. In the Directory Management tool, right-click the **Marketing** organizational unit, click **New**, and click **Shared Folder**.
2. In the **Name** edit field, type
`Press Releases`
3. In the **UNC Path** edit field, type
`\\<your machine name>\PR`
for example, type
`\\koala.antipodes.com\PR`



The Marketing organizational unit will now appear as shown in the following illustration.



Users can now see this volume while browsing in the directory.

To browse the directory

1. From the desktop, open **My Network Places**.
2. Click the **Directory**.
3. Click the domain name, and then click **Marketing**.
4. To view the files in the volume, either right-click the **Press Releases** volume, and click **Open**, or double-click **Press Releases**.

Publishing a Printer

This section describes the processes for publishing printers in a Windows 2000 directory.

Windows 2000 Printers

You can publish a printer shared by a computer running Windows 2000 by using the **Sharing** tab of the printer property dialog. By default, the **listed in <directory name>** option is enabled. (This means that the shared printer will be published by default.) The printer is published in the corresponding computer container in the directory. It will be called <server>-<Printer name>.

The print subsystem will automatically propagate changes made to the printer attributes (location, description, loaded paper, and so forth) to the directory.

To share and publish a printer

1. Create a new printer: click **Start**, point to **Settings**, click **Printers**, and then click **Add Printer**. Follow the instructions on your screen to create the printer.
2. Once you have created the printer, select the **Listed in Directory** check box. A window similar to the following will appear.



The Printer object will be published under the Computer object to which it is attached.

Non-Windows 2000 Printers

You can publish printers shared by systems other than Windows 2000 in the directory. The simplest way to do this is to use the **pubprn** script. This script will publish all the shared printers on a given server. It is located in the system32 directory. The syntax is:

```
cscript pubprn.vbs server dspath [trace]
```

For example:

```
Cscript pubprn.vbs prserv1  
"LDAP://ou=marketing,dc=antipodes,dc=com"
```

will publish all the printers on the server \\prserv1, and the printers will be published in the **Marketing** organizational unit. This script copies only the following subset of the printer attributes:

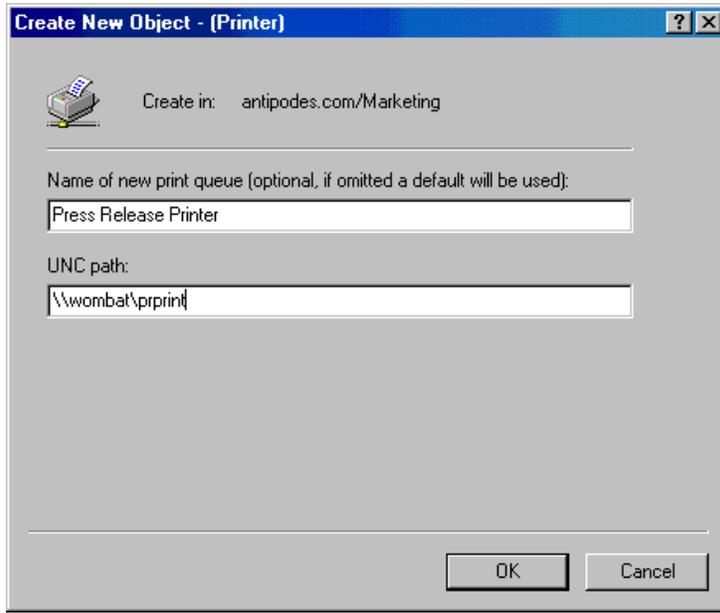
- Location
- Model
- Comment
- UNCPath

You can add other attributes by using the Directory Management snap-in. Note that you can rerun pubprn and it will update rather than overwrite existing printers.

Alternatively you can use the DS MMC snap-in to publish printers on non-Windows 2000 servers.

To use the DS MMC snap-in to publish printers

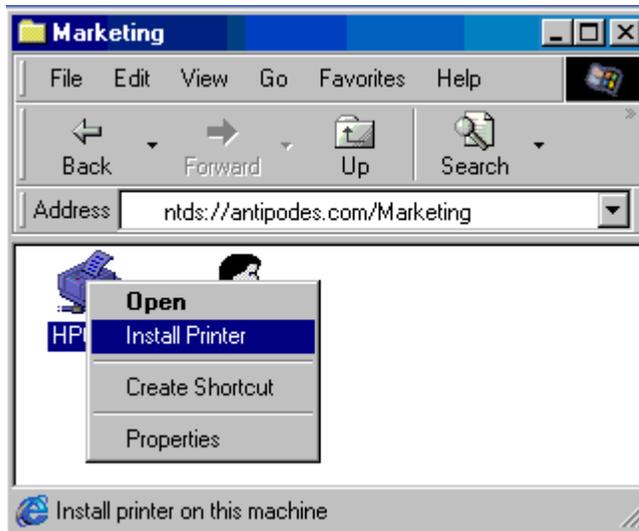
1. Right-click the **Marketing** organizational unit, click **New**, and click **Printer**.
2. In the **Name** field, type
`Press Release Printer`
3. In the **UNC Path** name, type the path to the printer, such as [\\wombat\prprint](http://wombat\prprint).



End users can realize the benefit of printers being published in the directory because they can browse for printers, submit jobs to those printers, and even install the printer drivers directly from the server.

To browse and use printers in the directory

1. From the Desktop, open the **Network Neighborhood**.
2. Click the **Directory**.
3. Click your domain name, then click **Marketing**.
4. Right-click **HPColor**, and then click **Install** to install the printer as a local printer, or click **Open** to see the current printer queue.



Creating a Computer Object

A computer object is created automatically when a computer joins a domain. You can also create the computer object before the computer joins a domain.

To create a computer object

1. Right-click the **Marketing** organizational unit click **New**, then click **Computer**.
2. For the computer name, type

kangaroo

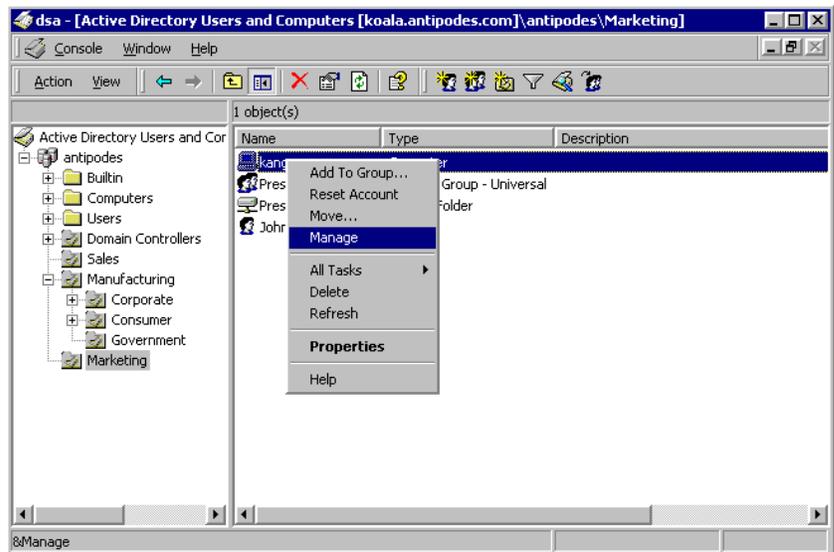
Optionally you can select which users are permitted to join a computer to the domain. This allows the administrator to create the computer account and someone with lesser permissions to install the computer and join it to the domain.

Managing Computers

Now that the computer object has been created, you might want to manage this computer remotely, diagnosing the services running on this computer, looking at the event viewer, and so forth.

To start the Computer Management snap-in

1. In the Directory Management tool, right-click the computer object and click **Manage**.
2. The Computer Management snap-in will start for the selected computer.

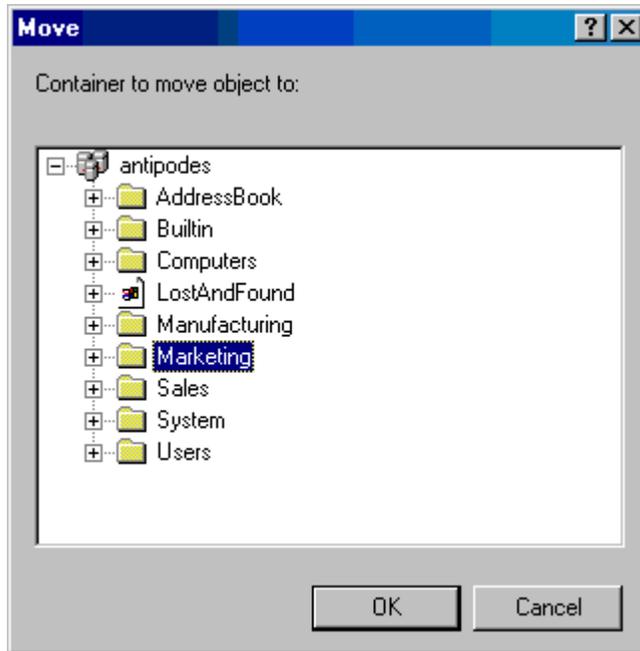


Renaming, Moving, and Deleting Objects

Every object in the directory can be renamed and deleted, and most objects can be moved to different containers.

To move an object

1. Right-click the object, and then click **Move**.
2. Click **Browse**. The Directory Browser will appear, enabling you to select the destination container for the object that you are moving.



Nested Groups

You can use nested groups provided that you are running the Active Directory in Native Mode. Nested groups are easier to manage, and thus reduce administrative overhead.

To create a nested group

1. Create a new group. Right-click the Marketing folder, click **New**, and then click **Group**. Type
All Marketing
as the name for the new group.
2. Right-click the **All Marketing Group** folder, and click **Properties**.
3. Include **Press Liaison** as a member of the group **All Marketing**.



To check the nested groups

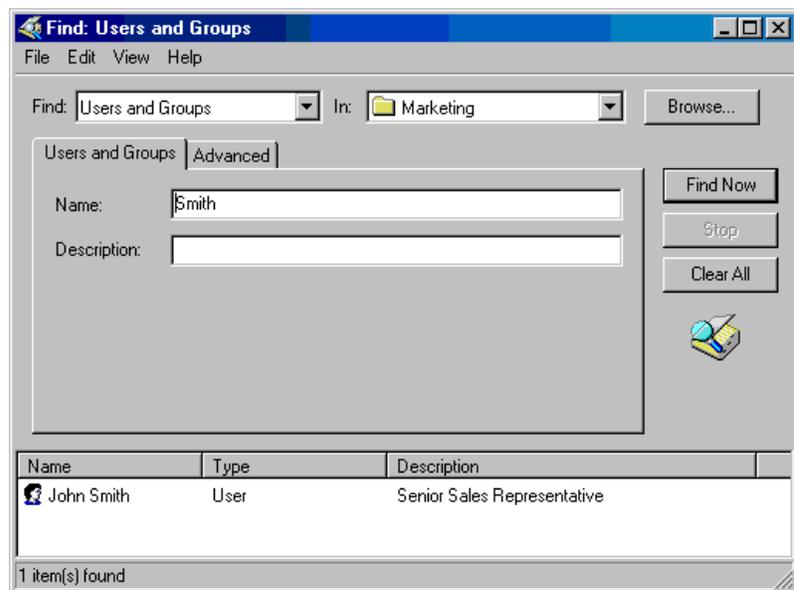
1. Right-click **All Marketing**, click **Properties**, and then click **Membership**. You will see **Press Liaison** as a member of **All Marketing**.
2. Double-click **Press Liaison**, and then click **Membership**. You will see **Press Liaison** listed as a member of the group **All Marketing**.

FINDING SPECIFIC OBJECTS

Rather than browsing the list of objects in the results pane, it is often more efficient to find specific objects that meet a certain criteria. In this example you will find all users who have a surname of “Smith” and are in the Marketing organizational unit.

To find these users

1. Select the **Marketing** organizational unit.
2. Start the Find dialog either by selecting the **Find** toolbar button, or by right-clicking and selecting **Find** from the context menu.
3. In the Name field, type
`Smith`
4. Click the **Find Now** button.



FILTERING A LIST OF OBJECTS

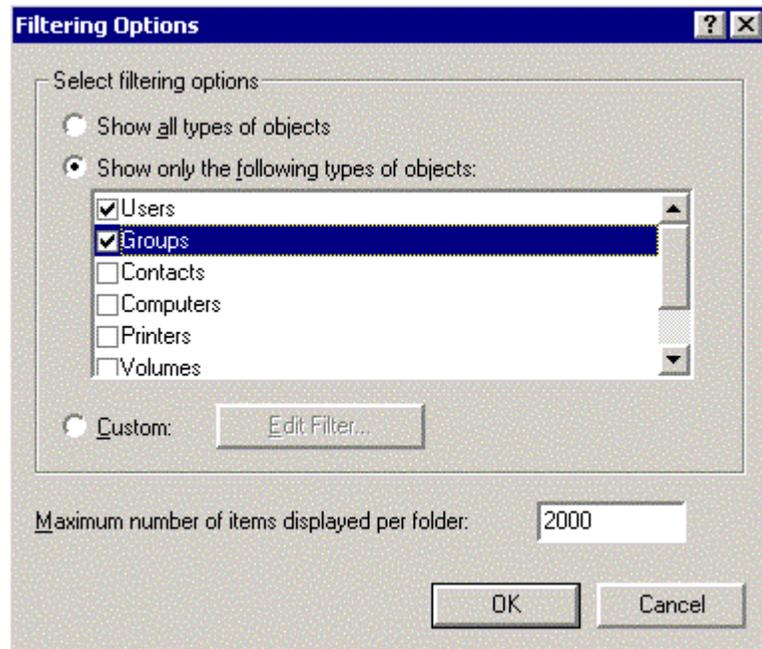
Filtering the list of returned objects from the directory can allow you to manage the directory more efficiently. The filtering option allows you to restrict the types of objects returned to the snap-in—for example, you can choose to view only users and groups, or you may want to create a more complex filter.

In addition, if an organizational unit has more than a specified number of objects, the filter dialog allows you to restrict the number of objects displayed in the results pane. You can use the Filter dialog to configure this option.

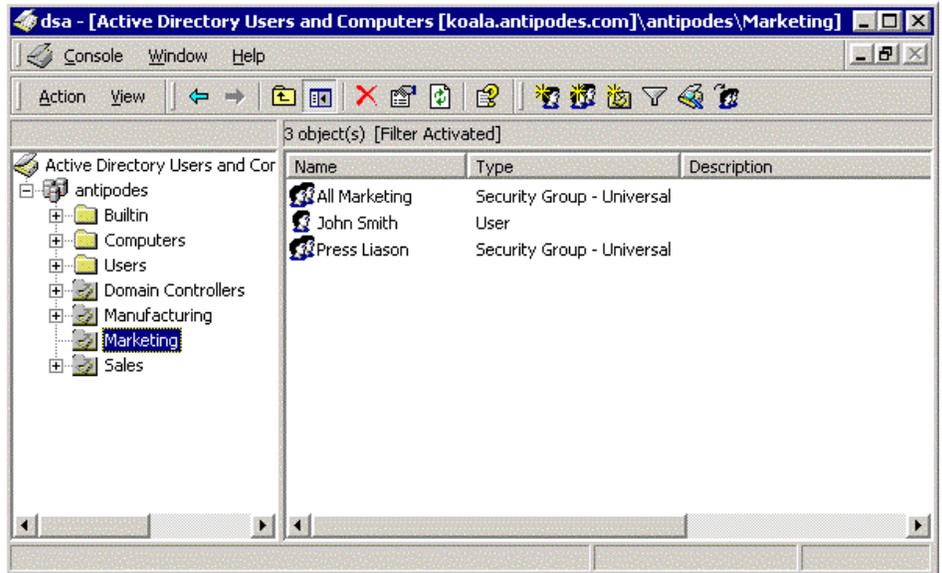
In this example, you will create a filter designed to retrieve users only.

To create the filter

1. Start the filter dialog by either selecting the **Filter** toolbar button or by clicking the **View** menu item and selecting **Filter**.
2. Select the option **Show only the following types of objects**, and then select **Users and Groups**.
3. Click **OK**.



After you click OK, whenever you view a container, it will retrieve user and group objects only. If you also enable the description bar, there will also be a visual indication that a filter has been applied.



FOR MORE INFORMATION

For the latest information on Windows NT Server, visit our World Wide Web site at <http://www.microsoft.com/ntserver> and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows 2000, visit the World Wide Web site at <http://www.microsoft.com/windows/server>

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.