

# Novell Account Management for Windows 2000

1.0

[www.novell.com](http://www.novell.com)

INSTALLATION AND  
ADMINISTRATION GUIDE



**Novell®**

## Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1993-2001 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent Nos. 5,608,903; 5,671,414; 5,677,851; 5,758,344; 5,784,560; 5,794,232; 5,818,936; 5,832,275; 5,832,483; 5,832,487; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,913,025; 5,919,257; 5,933,826. U.S. and Foreign Patents Pending.

Novell, Inc.  
1800 South Novell Place  
Provo, UT 84606  
U.S.A.

[www.novell.com](http://www.novell.com)

Account Management for Windows 2000 Administration Guide  
April 2001  
103-000114-001

**Online Documentation:** To access the online documentation for this and other Novell products, and to get updates, see [www.novell.com/documentation](http://www.novell.com/documentation).

**Novell Trademarks**

ConsoleOne is a trademark of Novell, Inc.

DirXML is a trademark of Novell, Inc.

eDirectory is a trademark of Novell, Inc.

NDS is a registered trademark of Novell, Inc., in the United States and other countries.

NDS Manager is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Client is a trademark of Novell, Inc.

Novell Directory Services is a registered trademark of Novell, Inc., in the United States and other countries.

**Third-Party Trademarks**

All third-party trademarks are the property of their respective owners.



# Contents

	<b>Account Management for Windows 2000</b>	<b>7</b>
<b>1</b>	<b>Installation</b>	<b>9</b>
	Minimum System Requirements . . . . .	9
	Hardware Requirements . . . . .	9
	Before Installation . . . . .	11
	Installing Account Management . . . . .	12
	Updating Windows 95/98 and Windows NT/2000 Clients . . . . .	12
	Installing Account Management for Windows 2000 . . . . .	13
	Synchronizing Active Directory with NDS eDirectory . . . . .	14
	Installing ConsoleOne . . . . .	14
	Uninstalling Account Management . . . . .	14
	Upgrading from Account Management for Windows NT . . . . .	15
	Uninstalling Account Management for Windows NT . . . . .	15
<b>2</b>	<b>Overview</b>	<b>17</b>
	Benefits . . . . .	17
	Simplified Login to the Network . . . . .	18
	Additional Management Capabilities of NDS eDirectory . . . . .	18
	Creating an eDirectory Replica on a Windows 2000 Server . . . . .	19
	Administration of User and Group Components from a Single Database . . . . .	20
	Management Capabilities . . . . .	21
	Components . . . . .	24
	ConsoleOne Objects . . . . .	25
<b>3</b>	<b>Managing Active Directory Accounts in NDS eDirectory</b>	<b>29</b>
	Managing Domains . . . . .	29
	Configuring Domain Identification . . . . .	30
	Adding an NDS User to a Windows 2000 Domain . . . . .	30
	Deleting a User from a Windows 2000 Domain . . . . .	32
	Configuring Index Servers . . . . .	32
	Managing User Accounts . . . . .	34
	Adding an NDS User to a Windows 2000 Domain . . . . .	34
	Deleting a User from a Windows 2000 Domain . . . . .	35
	Adding an NDS User to a Group . . . . .	36
	Deleting an NDS User from a Group . . . . .	37
	Setting a User's Primary Group . . . . .	38
	Configuring User Domain Settings . . . . .	38
	Managing Groups . . . . .	39
	Configuring Group Identification . . . . .	39

Creating a New Group . . . . .	40
Adding an NDS User to a Group. . . . .	41
Deleting an NDS User from a Group . . . . .	42
Deleting a Group. . . . .	43
Setting a User's Primary Group . . . . .	43
Managing Organizational Units . . . . .	43
Creating an Active Directory Organizational Unit . . . . .	44
Modifying an Active Directory Organizational Unit. . . . .	45
Deleting an Active Directory Organizational Unit . . . . .	45
<b>4 Password Synchronization</b>	<b>47</b>
Overview . . . . .	48
Changing a User Password in NDS eDirectory . . . . .	48
Changing a User Password in Active Directory . . . . .	49
Synchronizing User Passwords . . . . .	50
Configuring Domain Providers. . . . .	50
Configuring Password Filters . . . . .	51
Configuring Service Options . . . . .	53

## **6 Account Management for Windows 2000 Administration Guide**

## Account Management for Windows 2000

Novell® Account Management is a directory-enabled application that simplifies and unifies the management of user profiles on Windows\* 2000 networks. It leverages all the scalability, utility, and extensibility of NDS® eDirectory™ and adds crucial integration capability and password synchronization functionality. With Account Management, you can eliminate many of the complexities of administering a mixed-platform network while smoothing over compatibility issues and centralizing your management of user accounts stored in eDirectory and Active Directory\*.

This manual contains information on how to install, configure, and manage Account Management on Windows 2000 servers.

**8** Account Management for Windows 2000 Administration Guide



# 1

## Installation

This section describes how to install Novell® Account Management for Windows\* 2000.

**IMPORTANT:** In order to install Novell Account Management for Windows 2000, you must have NDS® eDirectory™ 8.5 installed on your Windows 2000 server.

### Minimum System Requirements

- Windows 2000 Server or Windows 2000 Advanced Server with NDS eDirectory 8.5
- Active Directory\*
- Novell Client™ 4.8 or later

### Hardware Requirements

Hardware requirements depend on the specific implementation of NDS and Active Directory.

For example, a base installation of NDS eDirectory with the standard schema requires about 74 MB of disk space for every 50,000 users. However, if you add a new set of attributes or completely fill in every existing attribute, the object size grows. These additions affect the disk space, processor, and memory needed.

Two factors increase performance: more cache memory and faster processors.

The following table illustrates typical system recommendations for NDS eDirectory.

Objects	Processor	Memory	Hard Disk
100,000	Pentium* III 450-700 MHz (single)	384 MB	144 MB
1 million	Pentium III 450-700 MHz (dual)	2 GB	1.5 GB
10 million	Pentium III 450-700 MHz (2 to 4)	2 GB +	15 GB

Requirements for processors might be greater than the tables indicate, depending upon additional services available on the computer, as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor-intensive.

Of course, faster processors improve performance. Additional memory also improves performance because eDirectory can then cache more of the directory into memory.

Microsoft\* recommends the following hardware requirements for Windows 2000 Servers:

- ◆ 133 MHz or higher Pentium-compatible CPU.
- ◆ 256 MB of RAM (128 MB minimum supported; 4 GB maximum).
- ◆ 2 GB hard disk with a minimum of 1 GB of free space.
- ◆ Windows 2000 Server supports up to four CPUs on one machine.

Microsoft recommends the following hardware requirements for Windows 2000 Advanced Servers:

- ◆ 133 MHz or higher Pentium-compatible CPU.
- ◆ 256 MB of RAM (128 MB minimum supported; 8 GB maximum).
- ◆ 2 GB hard disk with a minimum of 1 GB of free space.
- ◆ Windows 2000 Advanced Server supports up to eight CPUs on one machine.

## 10 Account Management for Windows 2000 Administration Guide

## Before Installation

Novell Account Management for Windows 2000 lets you use ConsoleOne™ to manage the structure of Active Directory domains, users, and groups from within NDS eDirectory. During installation, you will create several Active Directory objects in NDS. Before the installation, you may want to do the following:

- ◆ Create a container in eDirectory to hold the Windows 2000 Forest object.

You will be asked during the Installation to specify a location for the Forest object. This object must be located in a container. It cannot be created at the root of your tree.

- ◆ Determine where in your NDS tree you want to place the Password Synchronization object

See “Password Synchronization Object” on page 26 for more information.

- ◆ Determine the placement of eDirectory partitions and replicas.

To synchronize changes to objects, the server on which you install Account Management for Windows 2000 requires a master or read/write replica of the NDS eDirectory partition.

- ◆ Create filtered replicas.

Filtered replicas contain a filtered set of objects or object classes along with a filtered set of attributes and values for those objects. You might want to consider creating a filtered replica if you only want to synchronize specific objects or attributes.

For more information, see "Filtered Replicas" in *NDS eDirectory 8.5 Administration Guide* (<http://www.novell.com/documentation/lg/ndsedir/docui/index.html>).

- ◆ Create an index.

NDS eDirectory uses indexes to significantly improve query performance and ConsoleOne display time.

When ConsoleOne displays the contents of a container within a domain, it sends the query to an index server. When Account Management for Windows 2000 is installed, an index is automatically created on the server on which the product is installed. If there are multiple servers in the tree, it may be useful to create an index on one or more additional servers.

For more information, see "Index Manager" in *NDS eDirectory 8.5 Administration Guide* (<http://www.novell.com/documentation/lg/ndsedir/docui/index.html>).

## Installing Account Management

To install Account Management for Windows 2000, perform the following procedures:

- ◆ "Updating Windows 95/98 and Windows NT/2000 Clients" on page 12
- ◆ "Installing Account Management for Windows 2000" on page 13
- ◆ "Synchronizing Active Directory with NDS eDirectory" on page 14
- ◆ "Installing ConsoleOne" on page 14

The initial installation of Novell Account Management for Windows 2000 requires eDirectory 8.5 to be already installed on the same Windows 2000 server or domain controller that Account Management will be installed on. However, you are not required to install eDirectory 8.5 on every Windows 2000 server. A second or third domain controller can be set up for synchronization by running `/WINNT/SYSTEM32/DIRLINK.EXE` found on each Windows 2000 server where eDirectory and Account Management for Windows 2000 have been installed.

When installing to a remote domain, an account is created on the remote domain so that the DirXML driver can authenticate to that domain. The name of the account is `NAM_DomainName` (where *DomainName* is the name of the remote domain). For security purposes, the password for this account is randomly generated. If this account is modified (renamed, password changed, or group memberships changed), the DirXML driver will not synchronize with the remote domain.

## Updating Windows 95/98 and Windows NT/2000 Clients

In order for the Account Management for Windows 2000 Password Synchronization feature to work properly, you should update your Novell Windows 95/98 and Windows NT/2000 Clients on the server on which you will be installing Account Management for Windows 2000 and on all machines running the Novell Client whose passwords you want synchronized.

To update your Novell Clients, make sure you have the latest Client (\NT\I386\SETUPNW.EXE on the Novell Account Management for Windows 2000 CD), then run the following:

OS	File
Windows 95/98	PATCHES\ACMGTC\ENU\PRODUCTS\WIN95\IBM_ENU\SETUPSP.EXE
Windows NT/2000	PATCHES\ACMGTC\ENU\PRODUCTS\WINNT\I386\SETUPSP.EXE

For more information on password synchronization, see Chapter 4, “Password Synchronization,” on page 47.

## Installing Account Management for Windows 2000

- 1** At the Windows 2000 Server, log in as Administrator or as a user with administrative privileges.
- 2** Determine the location in eDirectory where the Active Directory forest object will reside.  
  
A replica of this partition must be added to the eDirectory/Windows 2000 server before you install Account Management. You should also place replicas of the partitions holding the users who will be synchronized with Active Directory on the eDirectory/Windows 2000 server.
- 3** Run SETUP.EXE from the product CD or downloaded file.
- 4** Select from the following components (you can install the components separately or together):
  - ◆ Synchronize Active Directory with eDirectory  
  
Installs software that synchronizes Active Directory and NDS eDirectory. This also installs software that can synchronize the passwords of the associated NDS and Active Directory users. See “Synchronizing Active Directory with NDS eDirectory” on page 14 for more information.
  - ◆ Install ConsoleOne  
  
Installs ConsoleOne 1.2d and additional snap-ins for managing Novell Account Management for Windows 2000. See “Installing ConsoleOne” on page 14 for more information.

## Synchronizing Active Directory with NDS eDirectory

- 1 Follow the online instructions in the Installation Wizard.
- 2 If you are not already connected, you will be required to log in to your NDS tree as Administrator or an equivalent.

If the schema has already been extended, you don't have to log in as Administrator at the root of the tree. If the container administrator has rights to the NDS Users that will be synchronized with Active Directory, you can log in as a container administrator.

- 3 You can create new NDS users who will be associated with the existing domain users, or you can associate existing NDS users with the domain users.

You can also choose to install the password filter during the installation process or after it has completed. You will be required to reboot the computer in order to use this filter.

## Installing ConsoleOne

- 1 Follow the online instructions in the Installation Wizard to install ConsoleOne 1.2d and Account Management snap-ins.

## Uninstalling Account Management

You must remove the Password Synchronization NT Provider and all associated filters prior to uninstalling Account Management for Windows 2000. The Password Synchronization NT Provider can be found in Control Panel > Password Synchronization.

See "Deleting a Password Filter" on page 52 for more information on removing password filters.

- 1 On the Windows taskbar, click Start > Settings > Control Panel > Add/Remove Programs.
- 2 Remove the following components:
  - ◆ Account Management for Windows 2000 Driver  
This uninstalls DirXML™ and the Active Directory DirXML driver.
  - ◆ Account Management for Windows 2000

### 14 Account Management for Windows 2000 Administration Guide

This uninstalls Account Management for Windows 200 and removes the Password Synchronization and Forest objects from your NDS tree.

- ◆ ConsoleOne 1.2d

## Upgrading from Account Management for Windows NT

You can upgrade to Account Management for Windows 2000 from the following products:

- ◆ NDS for NT
- ◆ NDS eDirectory Corporate Edition
- ◆ Account Management 2.1 for Windows NT

To upgrade your system to Account Management for Windows 2000:

- 1** Uninstall NDS for NT, NDS eDirectory Corporate Edition, or Account Management 2.1 for Windows NT.

**IMPORTANT:** Use the Uninstall NDS for NT and Include New NDS Information in the NT Domain option when uninstalling Account Management for Windows NT.

See “Uninstalling Account Management for Windows NT” on page 15 for more information.

- 2** Reboot your Windows NT server.
- 3** Install Windows 2000 Server or Windows 2000 Advanced Server.
- 4** Install Active Directory.
- 5** Install Account Management for Windows 2000.

See “Installing Account Management” on page 12 for more information.

## Uninstalling Account Management for Windows NT

Use the following procedure to uninstall any of the following products:

- ◆ NDS for NT
- ◆ NDS eDirectory Corporate Edition
- ◆ Account Management 2.1 for Windows NT

To uninstall Account Management for Windows NT and save any changes made while the domain was redirected to NDS, the NT server must have a

working connection to an NDS server holding a replica of the partition that holds the Domain object.

**IMPORTANT:** You must first remove Account Management from your backup domain controller (BDC) before you can remove it from your primary domain controller (PDC). If you uninstall from the PDC first, you won't be able to access your BDC.

Back up your PDC before completing the following steps.

- 1** Log in to the BDC as an administrative user.
- 2** In the Windows taskbar, click Start > Programs > Novell > Domain Object Wizard.
- 3** Follow the online instructions.
- 4** After the BDC reboots, perform Steps 1-3 on any remaining BDCs.
- 5** Log in to the PDC as an administrative user and log in to your NDS tree as Administrator or an equivalent.
- 6** In the Windows taskbar, click Start > Programs > Novell > Domain Object Wizard.
- 7** Select Uninstall NDS for NT and Include New NDS Information in the NT Domain

This option reads the current NT domain information from NDS and moves it to the Windows NT domain. If you have added users and other objects to NDS since moving the NT domain to NDS, those objects are added to the NT domain. Any objects that were originally in the NT domain but were not moved to NDS are no longer in the domain.

- 8** Follow the online instructions.

You can still uninstall and revert to the original domain state without a NetWare<sup>®</sup> connection. Any changes or additions made during the domain migration, however, are not reverted.

## **16** Account Management for Windows 2000 Administration Guide



# 2

## Overview

Novell Account Management for Windows\* 2000 lets you manage Active Directory\* objects (such as users, groups, containers, and domains) with both the Novell® and Microsoft\* management consoles. Account Management for Windows 2000 does this by allowing for the placement of Windows 2000 domains in the NDS® eDirectory™ tree, thereby creating a single management point for both directories.

The Installation Wizard lets you create new eDirectory user accounts in eDirectory for existing Active Directory users, or link existing Active Directory accounts with ones that already exist in eDirectory. After installation, any user you create in Active Directory is created in eDirectory in the container you specify. Users created in eDirectory are created in Active Directory only if you choose to add them to a Windows 2000 domain.

Account Management for Windows 2000 also provides a secure solution for synchronizing user passwords. This means that your users can log in to both Active Directory and eDirectory with the same password. Any change made to a user password in one directory is automatically made in the other directory as well.

The underlying integration functionality of Account Management for Windows 2000 is based on DirXML™ technologies. However, the Installation Wizard configures the DirXML driver for you. No manual DirXML configuration is necessary.

## Benefits

Account Management for Windows 2000 provides the following benefits:

- ◆ “Simplified Login to the Network” on page 18
- ◆ “Additional Management Capabilities of NDS eDirectory” on page 18

- ◆ “Creating an eDirectory Replica on a Windows 2000 Server” on page 19
- ◆ “Administration of User and Group Components from a Single Database” on page 20

## Simplified Login to the Network

Without Account Management for Windows 2000 integration, a user must log in as an eDirectory user to authenticate to eDirectory, then log in as a Windows 2000 user to access the Windows 2000 network.

After integration, a user can authenticate to both platforms using the same password. To access all authorized network services, including Windows 2000 domains, the user can log in to both accounts using a synchronized password.

Every change made to a password, in either eDirectory or Active Directory, is synchronized so that you only make the change once. The user does not have to remember two passwords, and you don't have to make password changes in two different databases.

For more information, see Chapter 4, “Password Synchronization,” on page 47.

## Additional Management Capabilities of NDS eDirectory

The addition of eDirectory to a Windows 2000 server gives you several management capabilities not available in a Windows 2000 domain network. These include:

- ◆ “Security Determination from a Single User Account” on page 18
- ◆ “Easy Movement of User Accounts” on page 19

### Security Determination from a Single User Account

In the eDirectory database, each user account exists only once. Because all network resources are in the same database, you do not need to create a user account on each server or domain a user needs to access. As a result, you can determine from a single location what group membership access rights a user has to any network resource.

NDS eDirectory also allows you to remove access to all network resources by deleting a single user account. You can be assured that there are no other accounts (security holes) residing on other servers or domains for that user.

Having a single User object in eDirectory does not create a single point of failure for network access. Because the eDirectory database that the user resides in can be partitioned and replicated to as many servers as needed on the network, the user object should always be available.

### **Easy Movement of User Accounts**

Moving a user account from one domain to another is a cumbersome task under the Windows 2000 domain system. It involves recording user information on a piece of paper, deleting the user account, and then re-creating that account in another domain.

In eDirectory, user accounts reside in an administrative container called an Organizational Unit (OU). An Organizational Unit contains users in a workgroup and all other network resources for that workgroup. Moving a user from one Organizational Unit to another is a simple procedure.

For example, if Bill moves from marketing to engineering, you can move Bill's user account from the Marketing Organizational Unit to the Engineering Organizational Unit. Because the user account was not deleted, all the properties associated with Bill's user account are maintained.

In eDirectory, users do not need to be moved from one 2000 domain to another. Windows 2000 domains are treated as entities to which eDirectory users can belong. A user can be a member of as many domains as needed.

### **Creating an eDirectory Replica on a Windows 2000 Server**

Account Management for Windows 2000 requires you to place an eDirectory replica on your Windows 2000 server. The replica can be a master replica or a read/write replica. When you install the replica on a Windows 2000 server, the server becomes an NDS Server object in eDirectory.

For more information on eDirectory replicas, see "Managing Partitions and Replicas" in *NDS eDirectory 8.5 Administration Guide* (<http://www.novell.com/documentation/lg/ndsedir/docui/index.html>).

## Administration of User and Group Components from a Single Database

Putting domain user accounts into eDirectory allows for a single point of administration, which provides you with the following benefits:

- ◆ “Simplified User and Group Administration” on page 20
- ◆ “Reduced Administration Costs” on page 20

### Simplified User and Group Administration

Account Management for Windows 2000 extends eDirectory so that it contains selected attributes and objects of the Windows 2000 domain. This provides you with a single database from which to administer all components of the network.

Account Management for Windows 2000 synchronizes changes made to the most common domain attributes and objects—the objects and attributes you use on a daily basis to administer your domains. This approach eliminates the need to administer two separate databases or to manually synchronize databases. You can administer all your users and groups inside eDirectory and have your changes synchronized in Active Directory.

For example, you can use ConsoleOne™ to create a user, then make that user a member of a domain or a member of a group in that domain. For more information on how to do this, see Chapter 3, “Managing Active Directory Accounts in NDS eDirectory,” on page 29.

### Reduced Administration Costs

By providing a single point of administration for users and groups in a mixed environment, Account Management for Windows 2000 greatly simplifies the entire network administration process and substantially reduces the cost of owning and managing your heterogeneous network.

Combining eDirectory and domain user accounts reduces the cost of administering a mixed environment by eliminating duplicate work on accounts.

Managing user accounts in eDirectory also allows you to use cost-saving features such as templates. This simplifies processes such as creating new user accounts.

## Management Capabilities

Account Management for Windows 2000 manages users, groups, and Organizational Units. It does not manage other similar objects found in both eDirectory and Active Directory (such as workstations and printers), nor does it manage Windows 2000 file system rights.

Account Management for Windows 2000 synchronizes users and Organizational Units between eDirectory and Active Directory, including the following attributes:

<b>NDS eDirectory Attribute</b>	<b>Active Directory Attribute</b>
<b>User Creation</b>	
Name	<User Name>
Surname	Last Name
Unique ID	Display Name
<b>General/Identification</b>	
Given Name	First Name
Last Name	Last Name
Full Name	Display Name
Middle Initial	Initials
Title	Title
Telephone	Telephone Number
Fax Number	Fax
E-Mail Address	E-mail
Description	Description
<b>General/Postal Addresses</b>	
Street	Street
Post Office Box	P.O. Box
City	City

<b>NDS eDirectory Attribute</b>	<b>Active Directory Attribute</b>
State	State/Province
Zip Code	Zip/Postal Code
<b>Domain/Access</b>	
User Name	<User Name>
Login Name	User Logon Name (Pre Windows 2000)
Group Membership	Member of
Add	Add
Remove	remove
Set Primary	Set Primary
<b>Domain/Setting</b>	
User Profile Path	Profile Path
Login Script Name	Logon Script
Home Directory	Home Folder
Local Path	Local Path
Connect	Connect
User May Log On To	Log On To
All Workstations	All Computers
These Workstations	The Following Computers
<b>User Profile/Personal Information</b>	
First	First Name
Middle Initial	Initials
Last	Last Name
Full	Display Name

## 22 Account Management for Windows 2000 Administration Guide

<b>NDS eDirectory Attribute</b>	<b>Active Directory Attribute</b>
<b>User Profile/Business Information</b>	
Job Title	Title
Phone	Telephone Number
Fax	Fax
Email	E-mail
Street	Street
City	City
State/Prov	State/Province
Zip/Postal	Zip/Postal Code
<b>Restrictions/Login Restrictions</b>	
Account Disabled	Account Is Disabled
Account Has Expiration Date	Account Expires
Chart	Hours

Account Management for Windows 2000 also lets you manage all three types of Active Directory groups (Global, Domain Local, and Universal) within the ConsoleOne management utility. These group management capabilities include:

- ◆ Creating Active Directory groups
- ◆ Deleting Active Directory groups
- ◆ Modifying Active Directory groups
- ◆ Adding Active Directory group members
- ◆ Deleting Active Directory group members

For more information on managing Active Directory groups in ConsoleOne, see “Managing Groups” on page 39.

Account Management for Windows 2000 doesn’t automatically synchronize schema and schema extensions, although it is possible through minor modifications in the DirXML™ drivers and style sheets to synchronize new

schema extensions. Account Management for Windows 2000 also does not synchronize directory access controls and permissions.

Account Management for Windows 2000 does not eliminate the need to design and deploy Active Directory domains or other components of Active Directory, such as the Active Directory global catalog server.

## Components

There are six basic components of Account Management for Windows 2000:

- ◆ DirXML

DirXML is the Novell meta-directory solution for eDirectory. DirXML provides the synchronization engine and rules system for managing objects between eDirectory and Active Directory.

DirXML maintains synchronization rules and information in eDirectory, and then bi-directionally synchronizes the information with other systems, such as Active Directory, through DirXML drivers.

- ◆ Active Directory DirXML driver

The Active Directory DirXML driver is a small Win32\* service that uses ADSI and LDAP to communicate changes to and from Active Directory.

You will need one Active Directory DirXML driver per domain. The driver is installed on your Windows 2000 server running eDirectory. The Windows 2000 server does not have to be a domain controller.

- ◆ Account Management for Windows 2000 Setup Wizard

The Account Management for Windows 2000 Setup Wizard transparently installs and configures DirXML and the Active Directory DirXML driver after asking a few configuration questions.

The Account Management for Windows 2000 Wizard creates objects in eDirectory for your existing Active Directory groups and OUs, and lets you select users for synchronization.

- ◆ ConsoleOne snap-in

Account Management for Windows 2000 includes a set of ConsoleOne snap-ins for viewing and managing the Active Directory attributes of synchronized users.



- ◆ Password synchronization service

The password synchronization service keeps eDirectory and Active Directory user passwords synchronized whenever a password is changes from within Active Directory management utilities or at the Windows desktop.

Each managed domain has one Windows 2000 server running the password synchronization service.

- ◆ Password filter

The password filter needs to be installed on all Active Directory domain controllers for every managed domain.

The password filter intercepts any Active Directory password changes, forwards this information to the Windows 2000 server running the password synchronization service, which in turn updates eDirectory with the new password.







A wizard automatically deploys and configures the Password Synchronization Agent on the Active Directory domain controller.

For more information on installing password filters, see “Installing a Password Filter” on page 51.

## ConsoleOne Objects

Account Management for Windows 2000 is represented by objects defined in eDirectory. The base eDirectory schema has been extended to accommodate this

information. The new object types are listed in the following table:

Object Icon	Description
	Windows 2000 Forest object
	Windows 2000 Domain object
	Password Synchronization object
	Password Provider object
	Active Directory User object
	Active Directory Group object

### Windows 2000 Forest Object



The Forest object represents a collection of one or more Windows 2000 domains that share a common schema, configuration, and global catalog and are linked with two-way transitive trusts.

### Windows 2000 Domain Object



The Domain object represents a group of computers that are part of a network and share a common directory database. A domain is organized in levels and is administered as a unit with common rules and procedures. Each domain has a unique name.

For more information, see “Managing Domains” on page 29.

### Password Synchronization Object



The Password Synchronization object represents the Novell Password Synchronization Service installed during the Account Management for Windows 2000 installation. This service controls the synchronization of passwords between eDirectory and Active Directory.

For more information, see Chapter 4, “Password Synchronization,” on page 47.

### Password Provider Object



The Password Provider object represents domains specified in the Password Synchronization Applet. In order for the Novell Password Synchronization Service to work, a domain provider must be selected and a password filter must be installed on all Windows 2000 domain controllers in the domain.

For more information, see “Installing a Password Filter” on page 51.


### Active Directory User Object



The Active Directory User object represents a person in your organization linked to a user in Active Directory. An Active Directory user account enables a user to log in to computers and domains with an identity that can be authenticated and authorized for access to domain resources.

For more information, see “Managing User Accounts” on page 34.

## Active Directory Group Object

 The Active Directory Group object represents a collection of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail. Security groups are used both to grant access to resources and as e-mail distribution lists.

For more information, see “Managing Groups” on page 39.

**28** Account Management for Windows 2000 Administration Guide

# 3

## Managing Active Directory Accounts in NDS eDirectory

This chapter describes how to integrate Active Directory\* with your NDS® eDirectory™ network

Using the Account Management for Windows\* 2000 snap-in to ConsoleOne™, you can create container, Group, and User objects. You can also add users to or remove users from Group objects or container objects. This means that you don't have to learn different applications to manage users, groups, and domains.

- ♦ “Managing Domains” on page 29
- ♦ “Managing User Accounts” on page 34
- ♦ “Managing Groups” on page 39
- ♦ “Managing Organizational Units” on page 43

### Managing Domains

Each Windows 2000 domain is represented by a Domain object in ConsoleOne. This object is a container object that operates similarly to a Group object in that it not only holds information about the domain and users who are members of the domain, but the Domain object also contains member objects, such as containers and Groups, just like an actual domain.

Using Organizational Units within a domain helps you manage the accounts and resources in the domain. The users and groups associated with the domain are represented as objects beneath the Domain object. By making NDS User objects members of the domain rather than actually residing within the domain, you can place the User objects anywhere in the tree and still give users access to specific domains.

Domain objects are created in eDirectory during the Account Management for Windows 2000 installation.

Use ConsoleOne to perform the following domain tasks:

- ◆ “Configuring Domain Identification” on page 30
- ◆ “Adding an NDS User to a Windows 2000 Domain” on page 30
- ◆ “Deleting a User from a Windows 2000 Domain” on page 32
- ◆ “Configuring Index Servers” on page 32

## Configuring Domain Identification

- 1** In ConsoleOne, right-click a Domain object.
- 2** Click Properties > General Identification.
- 3** Select from the following options:

Option	Description
Description	Describes the selected Domain object
Default User Creation Context	Describes where new NDS User objects are created when a corresponding User object is created in Active Directory

- 4** Click Apply > OK.

## Adding an NDS User to a Windows 2000 Domain

You can add an NDS user to a Windows 2000 domain or an Organizational Unit within a domain in any of the following ways:

- ◆ “Adding an NDS User to a Windows 2000 Domain through the NDS User Object” on page 31
- ◆ “Adding an NDS User to a Windows 2000 Domain through the Domain Object” on page 31
- ◆ “Adding an NDS User to an Organizational Unit within a Domain” on page 31
- ◆ “Creating a New NDS User” on page 31

### 30 Account Management for Windows 2000 Administration Guide

**Adding an NDS User to a Windows 2000 Domain through the NDS User Object**

- 1** In ConsoleOne, right-click the NDS User object you want to add to the domain.
- 2** Click Properties > Domain Access.
- 3** Click the Domain drop-down list > select a domain or a container within the domain.
- 4** Click Add.
- 5** Specify an Active Directory container, user name, and login name.
- 6** Click OK.
- 7** Click Apply > OK.

**Adding an NDS User to a Windows 2000 Domain through the Domain Object**

- 1** In ConsoleOne, right-click the Domain object you want to add an NDS User object to.
- 2** Click Properties > General Identification.
- 3** Click Add Users to browse to and select the NDS User objects you want to add to the domain.
- 4** Click Select > OK.
- 5** Click Apply > OK.

**Adding an NDS User to an Organizational Unit within a Domain**

- 1** In ConsoleOne, right-click the Organizational Unit you want to add an NDS User object to.
- 2** Click Properties > General Identification.
- 3** Click Add Users to browse to and select the NDS User objects you want to add to the domain.
- 4** Click Select > OK.
- 5** Click Apply > OK.

**Creating a New NDS User**

- 1** Right-click the container you want to add the user to.
- 2** Click New > User.

- 3** Enter information for the user > click Add This User to an Active Directory Domain.
- 4** Click OK.

## Deleting a User from a Windows 2000 Domain

Deleting an Active Directory User object in eDirectory from a domain deletes the Active Directory user from Active Directory. The corresponding NDS User object is not automatically deleted. You must delete this User object separately.

You can delete an NDS user from a Windows 2000 domain in either of the following ways:

- ◆ “Deleting an Active Directory User from a Domain through the User Object” on page 32
- ◆ “Deleting an Active Directory User from a Domain through ConsoleOne” on page 32

### Deleting an Active Directory User from a Domain through the User Object

- 1** In ConsoleOne, right-click the User object you want to delete from a domain.
- 2** Click Properties > Domain Access.
- 3** Click the Domain drop-down list > select the domain you want to delete the user from.
- 4** Click Remove.
- 5** Click Apply > OK.

### Deleting an Active Directory User from a Domain through ConsoleOne

- 1** In ConsoleOne, right-click the User object you want to delete.
- 2** Click Delete.

## Configuring Index Servers

NDS eDirectory uses database indexes to significantly improve query performance. If you have multiple servers in your domain, you need to specify which servers hold your indexes.



When ConsoleOne displays the contents of a container within a domain, it sends the query to one of these index servers. When Account Management for Windows 2000 is installed, an index is automatically created on the server where the product is installed. If there are multiple servers in the tree, it may be useful to create an index on one or more additional servers. When you add a server to the list using ConsoleOne, and there is no index on the server, ConsoleOne will create one automatically. Deleting the server from the list does not delete the index from the server.

For more information on indexes and index management, see "Index Manager" in *NDS eDirectory 8.5 Administration Guide* (<http://www.novell.com/documentation/lg/ndsedir/docui/index.html>).

Use ConsoleOne to perform the following tasks:

- ◆ "Adding Index Servers" on page 33
- ◆ "Deleting Index Servers" on page 33

### **Adding Index Servers**

- 1** In ConsoleOne, right-click a Domain object.
- 2** Click Properties > General Index Servers.
- 3** Click Add.
- 4** Browse to and select a server object.
- 5** Click OK.
- 6** Click Apply > OK.

### **Deleting Index Servers**

- 1** In ConsoleOne, right-click a Domain object.
- 2** Click Properties > General Index Servers.
- 3** Select the index server you want to delete.
- 4** Click Delete.
- 5** Click Apply > OK.

## Managing User Accounts

Use ConsoleOne to perform the following tasks:

- ◆ “Adding an NDS User to a Windows 2000 Domain” on page 34
- ◆ “Deleting a User from a Windows 2000 Domain” on page 35
- ◆ “Adding an NDS User to a Group” on page 36
- ◆ “Deleting an NDS User from a Group” on page 37
- ◆ “Setting a User's Primary Group” on page 38
- ◆ “Configuring User Domain Settings” on page 38

For more information on managing eDirectory users, see ConsoleOne User Guide (<http://www.novell.com/documentation/lg/consol12d/docui/index.html>).

### Adding an NDS User to a Windows 2000 Domain

You can add an NDS user to a Windows 2000 domain or an Organizational Unit within a domain in any of the following ways:

- ◆ “Adding an NDS User to a Windows 2000 Domain through the NDS User Object” on page 31
- ◆ “Adding an NDS User to a Windows 2000 Domain through the Domain Object” on page 31
- ◆ “Adding an NDS User to an Organizational Unit within a Domain” on page 31
- ◆ “Creating a New NDS User” on page 31

#### Adding an NDS User to a Windows 2000 Domain through the NDS User Object

- 1** In ConsoleOne, right-click the NDS User object you want to add to the domain.
- 2** Click Properties > Domain Access.
- 3** Click the Domain drop-down list > select a domain or a container within the domain.
- 4** Click Add.
- 5** Specify an Active Directory container, user name, and login name.

- 6** Click OK.
- 7** Click Apply > OK.

### **Adding an NDS User to a Windows 2000 Domain through the Domain Object**

- 1** In ConsoleOne, right-click the Domain object you want to add an NDS User object to.
- 2** Click Properties > General Identification.
- 3** Click Add Users to browse to and select the NDS User objects you want to add to the domain.
- 4** Click Select > OK.
- 5** Click Apply > OK.

### **Adding an NDS User to an Organizational Unit within a Domain**

- 1** In ConsoleOne, right-click the Organizational Unit you want to add an NDS User object to.
- 2** Click Properties > General Identification.
- 3** Click Add Users to browse to and select the NDS User objects you want to add to the domain.
- 4** Click Select > OK.
- 5** Click Apply > OK.

### **Creating a New NDS User**

- 1** Right-click the container you want to add the user to.
- 2** Click New > User.
- 3** Enter information for the user > click Add This User to an Active Directory Domain.
- 4** Click OK.

### **Deleting a User from a Windows 2000 Domain**

Deleting an Active Directory User object in eDirectory from a domain deletes the Active Directory user from Active Directory. The corresponding NDS User object is not automatically deleted. You must delete this User object separately.

You can delete an NDS user from a Windows 2000 domain in either of the following ways:

- ◆ “Deleting an Active Directory User from a Domain through the User Object” on page 32
- ◆ “Deleting an Active Directory User from a Domain through ConsoleOne” on page 32

### **Deleting an Active Directory User from a Domain through the User Object**

- 1** In ConsoleOne, right-click the User object you want to delete from a domain.
- 2** Click Properties > Domain Access.
- 3** Click the Domain drop-down list > select the domain you want to delete the user from.
- 4** Click Remove.
- 5** Click Apply > OK.

### **Deleting an Active Directory User from a Domain through ConsoleOne**

- 1** In ConsoleOne, right-click the User object you want to delete.
- 2** Click Delete.

## **Adding an NDS User to a Group**

You can add an NDS user to a group in either of the following ways:

- ◆ “Adding an NDS User to a Group through the NDS User Object” on page 41
- ◆ “Adding an NDS User to a Group through the Group Object” on page 42

### **Adding an NDS User to a Group through the NDS User Object**

- 1** In ConsoleOne, right-click the NDS User object you want to add to the group.
- 2** Click Properties > Domain Access.
- 3** In the Group Membership area, click Add.
- 4** Select a group > click OK.
- 5** Click Apply > OK.

## **36 Account Management for Windows 2000 Administration Guide**

### Adding an NDS User to a Group through the Group Object

- 1 In ConsoleOne, right-click the group you want to add an NDS User object to.
- 2 Click Properties > Members > Add.
- 3 Select the member you want to add to the group.
- 4 Click Select > OK.
- 5 Click Apply > OK.

### Deleting an NDS User from a Group

You can delete an NDS user from a group in either of the following ways:

- ♦ “Deleting an NDS User from a Group through the User Object” on page 42
- ♦ “Deleting an NDS User from a Group through the Group Object” on page 42

### Deleting an NDS User from a Group through the User Object

- 1 In ConsoleOne, right-click the user you want to delete from a group.
- 2 Click Properties > Domain Access.
- 3 In the Group Membership area, select the group you want to delete the user from.

A user cannot be removed or deleted from its primary group. The name of the user's primary group is displayed in the Primary Group field in the Group Membership area.

- 4 Click Remove.
- 5 Click Apply > OK.

### Deleting an NDS User from a Group through the Group Object

- 1 In ConsoleOne, right-click the group you want to delete a user from.
- 2 Click Properties > Members.
- 3 Select the user you want to delete.
- 4 Click Remove.
- 5 Click Apply > OK.

## Setting a User's Primary Group

To belong to a domain, a user must be a member of at least one group within that domain. Users cannot be deleted from their primary group. This primary group is displayed on the Domain Access page in the Primary Group field in the Group Membership area. By default, the Domain Users group is set as the primary group.

- 1** In ConsoleOne, right-click the user whose primary group you want to change.
- 2** Click Properties > Domain Access.
- 3** In the Group Membership area, select the group you want to set as the new primary group.

When the current primary group (displayed in the Primary Group field in the Group Membership area) is selected, the Set Primary button is disabled.

- 4** Click Set Primary.

The selected group becomes the primary group and is displayed in the Primary Group field in the Group Membership area.

- 5** Click Apply > OK.

## Configuring User Domain Settings

You can enter or view a user's group and user profile path, login script name, home directory, and workstation access.

- 1** In ConsoleOne, right-click a User object.
- 2** Click Properties > Domain Settings.
- 3** Enter the path to the directory containing the domain member's user and group profiles.
- 4** Enter the filename of the user's login script.
- 5** Set the user's home directory.

Option	Description
Local Path	Specify the location of the domain user's local home directory.

Option	Description
Connect To	Specify a location on the network (a drive and a Windows 2000 Server share).

**6** Specify the workstations the user can long on to.

Option	Description
All Computers	Allows the user access from all workstations.
The Following Computers	Allows the user access from certain workstations only. You can specify up to sixty workstations.

**7** Click Apply > OK.

## Managing Groups

Use ConsoleOne to perform the following group tasks:

- ◆ “Configuring Group Identification” on page 39
- ◆ “Creating a New Group” on page 40
- ◆ “Adding an NDS User to a Group” on page 41
- ◆ “Deleting an NDS User from a Group” on page 42
- ◆ “Deleting a Group” on page 43
- ◆ “Setting a User's Primary Group” on page 43

For more information on managing eDirectory groups, see ConsoleOne User Guide (<http://www.novell.com/documentation/lg/consol12d/docui/index.html>).

## Configuring Group Identification

- 1** In ConsoleOne, right-click a Group object.
- 2** Click Properties > General Identification.
- 3** Enter or view information about the selected Group object.

## Creating a New Group

- 1 In ConsoleOne, right-click the domain or container you want the new group created in.
- 2 Click New > Group.
- 3 Specify the group name.
- 4 (Optional) Specify a group description.
- 5 Select one of the following Group Scope options:

Option	Description
Global	A group that can be granted rights and permissions and can become a member of local groups in its own domain, the member servers and workstations, and trusting domains. A global group can contain user accounts only from its own domain. Global groups provide a way to create sets of users from inside the domain, available for use both in and out of the domain.
Domain Local	A security or distribution group that can contain universal groups, global groups, and accounts from any domain in the domain tree or forest. A domain local group can also contain other domain local groups from its own domain. Rights and permissions can be assigned only at the domain containing the group.
Universal	<p>A security or distribution group that can be used anywhere in the domain tree or forest.</p> <p>A universal group can have members from any Windows 2000 domain in the domain tree or forest. It can also include other universal groups, global groups, and accounts from any domain in the domain tree or forest. Rights and permissions must be assigned on a per-domain basis, but can be assigned at any domain in the domain tree or forest.</p> <p>Universal groups can be members of domain local groups and other universal groups but cannot be members of global groups. Universal groups contain primarily global groups.</p>



**6** Select one of the following Group Type options:

Option	Description
Security	A group that can be listed in discretionary access control lists (DACLS) used to define permissions on resources and objects. A security group can also be used as an e-mail entity. Sending an e-mail message to the group sends the message to all the members of the group.
Distribution	A group that is used solely for e-mail distribution and that is not security-enabled.  Distribution groups cannot be listed in discretionary access control lists (DACLS) used to define permissions on resources and objects. Distribution groups can be used only with e-mail applications to send e-mail to collections of users. If you do not need a group for security purposes, create a distribution group instead of a security group.

**7** Click OK.**Adding an NDS User to a Group**

You can add an NDS user to a group in either of the following ways:

- ◆ “Adding an NDS User to a Group through the NDS User Object” on page 41
- ◆ “Adding an NDS User to a Group through the Group Object” on page 42

**Adding an NDS User to a Group through the NDS User Object**

- 1** In ConsoleOne, right-click the NDS User object you want to add to the group.
- 2** Click Properties > Domain Access.
- 3** In the Group Membership area, click Add.
- 4** Select a group > click OK.
- 5** Click Apply > OK.

### Adding an NDS User to a Group through the Group Object

- 1 In ConsoleOne, right-click the group you want to add an NDS User object to.
- 2 Click Properties > Members > Add.
- 3 Select the member you want to add to the group.
- 4 Click Select > OK.
- 5 Click Apply > OK.

### Deleting an NDS User from a Group

You can delete an NDS user from a group in either of the following ways:

- ◆ “Deleting an NDS User from a Group through the User Object” on page 42
- ◆ “Deleting an NDS User from a Group through the Group Object” on page 42

### Deleting an NDS User from a Group through the User Object

- 1 In ConsoleOne, right-click the user you want to delete from a group.
- 2 Click Properties > Domain Access.
- 3 In the Group Membership area, select the group you want to delete the user from.

A user cannot be removed or deleted from its primary group. The name of the user’s primary group is displayed in the Primary Group field in the Group Membership area.

- 4 Click Remove.
- 5 Click Apply > OK.

### Deleting an NDS User from a Group through the Group Object

- 1 In ConsoleOne, right-click the group you want to delete a user from.
- 2 Click Properties > Members.
- 3 Select the user you want to delete.
- 4 Click Remove.
- 5 Click Apply > OK.

## Deleting a Group

- 1 On ConsoleOne, right-click the group you want to delete.
- 2 Click Delete.

## Setting a User's Primary Group

To belong to a domain, a user must be a member of at least one group within that domain. Users cannot be deleted from their primary group. This primary group is displayed on the Domain Access page in the Primary Group field in the Group Membership area. By default, the Domain Users group is set as the primary group.

- 1 In ConsoleOne, right-click the user whose primary group you want to change.
- 2 Click Properties > Domain Access.
- 3 In the Group Membership area, select the group you want to set as the new primary group.

When the current primary group (displayed in the Primary Group field in the Group Membership area) is selected, the Set Primary button is disabled.

- 4 Click Set Primary.

The selected group becomes the primary group and is displayed in the Primary Group field in the Group Membership area.

- 5 Click Apply > OK.

## Managing Organizational Units

You can create Organizational Unit container objects to subdivide your domain.

Organizational Units can contain other Organizational Units and leaf objects such as User objects.

Normally, the Organizational Unit object represents a department, which holds a set of objects that commonly need access to each other. A typical example is a set of users, along with the printers, volumes, and applications that those users need.

At the highest level of Organizational Unit objects, each Organizational Unit can represent each site (separated by WAN links) in the network.

The way you use Organizational Unit objects in your domain depends on the size and structure of your network. If the network is small, you probably don't need any Organizational Units.

For larger networks, you can create Organizational Unit objects under the Organization to make resources easier to locate and manage. For example, you can create Organizational Units for each department or division in your company. Remember that administration is easiest when you keep User objects together in the Organizational Unit with the resources they use most frequently.

For networks with multiple sites, you can create an Organizational Unit for each site under the Organization object. That way, if you have (or plan to have) enough servers to partition the directory, you can do so logically along site boundaries.

Use ConsoleOne to perform the following tasks:

- ◆ “Creating an Active Directory Organizational Unit” on page 44
- ◆ “Modifying an Active Directory Organizational Unit” on page 45
- ◆ “Deleting an Active Directory Organizational Unit” on page 45

## Creating an Active Directory Organizational Unit

- 1** In ConsoleOne, right-click a Domain object or a container you created.

The creation of Active Directory containers in eDirectory follows the Microsoft Management Console (MMC) standards. For more information, see [www.microsoft.com](http://www.microsoft.com) (<http://www.microsoft.com>).

- 2** Click New > Organizational Unit.
- 3** Enter a name for the Organizational Unit.
- 4** (Optional) Enter a description.

**5** Select from the following options:

Option	Description
Default User Creation Context	Describes where new NDS User objects are created when a corresponding User object is created in Active Directory.
Create a New Container in This Context	Check this check box to create another Organizational Unit in this container as soon as you are done creating this one.

**6** Click OK.

## Modifying an Active Directory Organizational Unit

- 1** In ConsoleOne, right-click the Active Directory Organizational Unit you want to modify.
- 2** Click Properties.
- 3** Enter or edit a description of the object.
- 4** Click Add Users to add users to an Active Directory domain.
- 5** Click Apply > OK.

## Deleting an Active Directory Organizational Unit

Deleting an Active Directory Organizational Unit in ConsoleOne deletes all users and subcontainers within that container.

- 1** In ConsoleOne, right-click the Active Directory Organizational Unit you want to delete.
- 2** Click Delete Object.

**46** Account Management for Windows 2000 Administration Guide

# 4

## Password Synchronization

This chapter describes how to synchronize user passwords in Active Directory\* and NDS® eDirectory™.

You can install and configure password synchronization during the Novell® Account Management for Windows\* 2000 installation. Passwords changes will not be synchronized unless the Novell Password Synchronization Service is running. Therefore, a hardware failure or reboot of the machine where the service is running will result in the loss of password synchronization while the service is down. To avoid this temporary loss of password synchronization, the Novell Password Synchronization Service can be installed to additional Windows 2000 domain controllers or servers for fault tolerance and to ensure that user passwords remain synchronized.

To install the Novell Password Synchronization Service independent of the Account Management for Windows 2000 installation, run the following from the WIN2000\DIRXML\ADMGMGT directory:

```
SETUP.EXE /pwsync
```

Follow the installation steps to configure password synchronization for the domain.

Novell Client™ 4.8 and the client patch, delivered with this product, need to be installed prior to the installation of the Novell Password Synchronization Service. See “Updating Windows 95/98 and Windows NT/2000 Clients” on page 12 for more information.

After installation, changes to password synchronization can be made using the Password Synchronization utility. You should also use the Password Synchronization utility to add a filter to new Active Directory domain controllers you add to your Windows 2000 forest.

## Overview

Password synchronization consists of provider, notification, and filter DLLs and a Windows 2000 service. A Password Synchronization object is created in NDS eDirectory with subordinate Provider objects for each directory being synchronized. The Windows 2000 service authenticates to eDirectory as the Password Synchronization object.

This section explains password synchronization for the following situations:

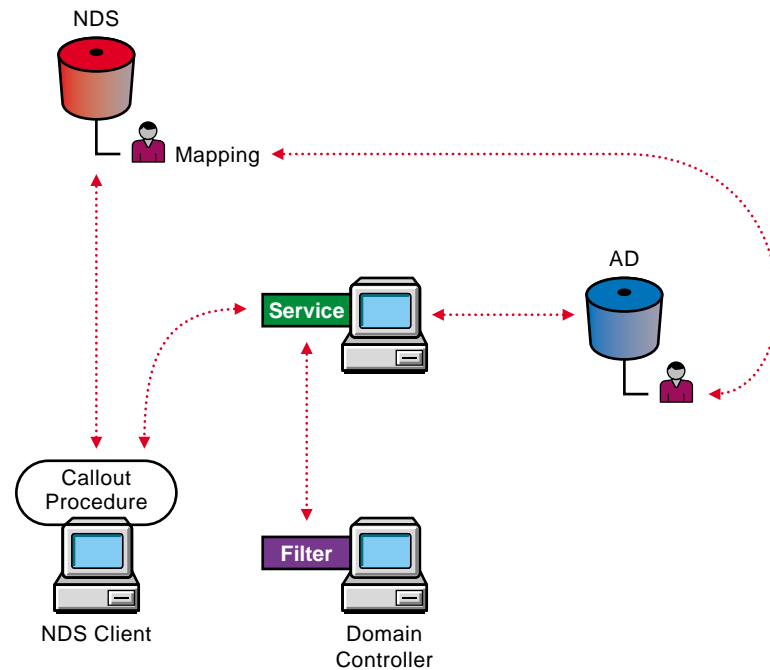
- ◆ “Changing a User Password in NDS eDirectory” on page 48
- ◆ “Changing a User Password in Active Directory” on page 49

## Changing a User Password in NDS eDirectory

When a password change is detected on a Windows box running the Novell® Client™, the username and password are encrypted and sent via RPC to the Windows 2000 service. The Windows 2000 service then walks the list of providers and passes the credential set to each Windows 2000 provider. The Windows 2000 provider verifies the credential set and passes the encrypted credentials via RPC to a password filter installed on the domain controller. The password filter then changes the Windows 2000 credentials.

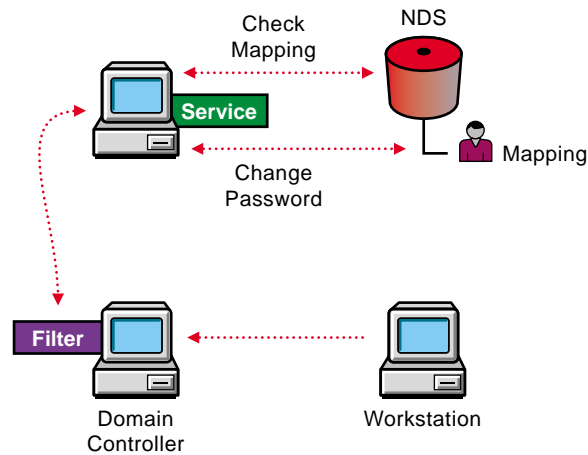


Figure 1 Password Changed in eDirectory



## Changing a User Password in Active Directory

A password change on Windows 2000 comes through the password filter installed on the domain controller. The filter encrypts and passes the credential set to the Windows 2000 service via RPC. The Windows 2000 service walks the list of providers and passes the credential set to each provider. The Windows 2000 provider verifies the credential set and passes the encrypted credentials via RPC to a password filter installed on the domain controller. The NDS provider will verify the credential set, then the Windows 2000 service, which is authenticated to NDS, will change the NDS credentials.

**Figure 2 Password Changed in Active Directory**

## Synchronizing User Passwords

You can use the Password Synchronization utility to select a domain provider and install a password filter on all domain controllers in your domain. To ensure that passwords are always synchronized, you must install a filter on all your domain controllers.

**IMPORTANT:** If your passwords in Active Directory or eDirectory require a certain format (such as a specific password length or type of characters), you should make sure that you establish the same password rules in both directories to ensure that passwords synchronize properly.

Use the Password Synchronization utility to perform the following tasks:

- ◆ “Configuring Domain Providers” on page 50
- ◆ “Configuring Password Filters” on page 51
- ◆ “Configuring Service Options” on page 53

## Configuring Domain Providers

Use the Password Synchronization utility to perform the following tasks:

- ◆ “Installing a Domain Provider” on page 51
- ◆ “Deleting a Domain Provider” on page 51

### Installing a Domain Provider

- 1 On the Windows taskbar, click Start > Settings > Control Panel.
- 2 Click Password Synchronization.
- 3 Click Add.
- 4 Select a domain from the Domains Available for Synchronization list.
- 5 Click OK.

### Deleting a Domain Provider

Before you can delete a domain provider, you must manually remove its password filter. See “Deleting a Password Filter” on page 52 for more information.

- 1 On the Windows taskbar, click Start > Settings > Control Panel.
- 2 Click Password Synchronization.
- 3 Select the domain you want to remove from the Synchronized Domains list.
- 4 Click Remove.

## Configuring Password Filters

Password filters, which are assigned to domain providers, are used to determine how passwords are configured on domain controllers.

Any changes made to a user password go through the password filter before they are actually made.

Every domain controller in the domain should have a password filter.

- ◆ “Installing a Password Filter” on page 51
- ◆ “Checking the Status of a Password Filter” on page 52
- ◆ “Deleting a Password Filter” on page 52

### Installing a Password Filter

Installing a password filter on a domain controller requires you to reboot your domain controller before the installation is complete. You may want to perform this procedure after hours, or select only one domain controller at a time.

- 1** On the Windows taskbar, click Start > Settings > Control Panel.
- 2** Click Password Synchronization.
- 3** Click Filters.
- 4** Select a domain controller > click Setup.

If you are performing a remote install, the domain controller is automatically rebooted after the filter is installed. If you are performing a local install, you must manually reboot the domain controller.

- 5** Click Close.

### Checking the Status of a Password Filter

- 1** On the Windows taskbar, click Start > Settings > Control Panel.
- 2** Click Password Synchronization.
- 3** Click Filters.
- 4** View the status of your domain controllers.

Status	Description
Running	Indicates that the domain controller is currently running.
Installed	Indicates that the domain controller has been installed but is not currently running.
Not Installed	Indicates a domain controller that has just been added to the list of domain providers.

- 5** Click Close.

### Deleting a Password Filter

- 1** On the Windows taskbar, click Start > Settings > Control Panel.
- 2** Click Password Synchronization.
- 3** Click Filters.
- 4** Select a domain controller > click Remove.

If you are performing a remote delete, the domain controller is automatically rebooted after the filter is deleted. If you are performing a local delete, you must manually reboot the domain controller.

**5** Click Close.

## Configuring Service Options

Use the Password Synchronization utility to configure the following service options:

- ◆ “Configuring Error Logging” on page 53
- ◆ “Configuring Retry Lifetime” on page 53

### Configuring Error Logging

Password change events appear in the Windows 2000 Server Event Viewer. You can configure error logging to show all password change events or only the errors.

- 1** On the Windows taskbar, click Start > Settings > Control Panel.
- 2** Click Password Synchronization.
- 3** Select Log Errors.
- 4** Click Close.

### Configuring Retry Lifetime

The Retry Lifetime option lets you specify how many times a password synchronization will be tried before it fails.

- 1** On the Windows taskbar, click Start > Settings > Control Panel.
- 2** Click Password Synchronization.
- 3** Enter a number in the Retry Lifetime field.
- 4** Click Close.

**54** Account Management for Windows 2000 Administration Guide