

DRAFT DRAFT DRAFT DRAFT

ACTIVE DIRECTORY NAMING STANDARDS

User Account Names

A Windows user object has two names: a user "distinguished name", and an "account name". The account name must be unique within the AD domain, while the user distinguished name, which serves as the Relative Distinguished Name (RDN) of the user in the Active Directory, must be unique within the Active Directory OU in which it resides.

For users with a NetID, the user's AD account name should be identical to the user's NetID.

For non enterprise account users, the AD user account name must be prefixed by bang (!) followed by the org mnemonic, a hyphen (-), and the user id, and must EXCEED 8 characters - For example: !OENG-dowens. This is to ensure that Windows user names will not conflict with NetID-based accounts that may be created in the future. Notre Dame AD user accounts which do not follow this naming standard are subject to removal without notice.

Example: mynetid (NetID-based Notre Dame AD user account name)

Example: !ORG-localname (non-NetID Notre Dame AD user account name)

For enterprise account creation, accounts with a NetID are created from the iPlanet Directory data using `ndpvid' as the `cn', and `uid' as both the `sAMAccountName' and prefix of `userPrincipalName'.

iPlanet Directory

Active Directory

ndPVid
uid
uid

cn
sAMAccountName
userPrincipalName (suffix is ND.EDU)

Security and Distribution Groups

A Windows 2000 Active Directory group may be one of six types. Two broad categories, "security" and "distribution", define the general type of the group. Each of these two types is further defined as either "domain local", "global" or "universal". *See the Microsoft paper Active Directory User, Computers and Groups [1] for a more detailed explanation of Active Directory groups.*

The Notre Dame AD recommended naming standard for Active Directory security and distribution group names is:

ddd-group_name-tt

ddd

Notre Dame AD org mnemonic

tt

type of group (ls, gs, us, ld, gd, ud) See below

group_name

descriptive name which explains the purpose of the group

Active Directory group types are:

group types (tt)

ls domain local security

gs global security

us universal security

ld domain local distribution

gd global distribution

ud universal distribution

Example: LAW-OU Admins-gs

Because Active Directory groups are replicated across the network, they must be populated in ways that minimize network replication. Try to use global and domain local groups where possible. If you have a need to create a universal group, do not populate the universal group with individual users. Instead, use the names of other groups to build the universal group membership.

Note: All group types in AD are displayed with the same group icon, which can be visually confusing. The Active Directory Users and Computers console does show the group type field, however testing has shown that after making changes to an individual group, the user interface no longer displays the group type field description. This can cause confusion and lead to error, which is why we include the group type as part of the group naming scheme. Using this scheme will help prevent Administrators from choosing the wrong group when they are managing groups within groups, in their own domain and across other domains. The following Windows 2000 Server Resource Kit tools may be of assistance when troubleshooting group memberships: ifmember.exe, findgrp.exe, global.exe, local.exe, showgroups.exe, showmbrs.exe.

Group Policy Objects (GPOs)

The naming convention for Group Policy Objects is to use the Notre Dame AD org mnemonic Name as a prefix for all Group Policy names. For instance, "LAW staff policy" or "MCOB lab 3 policy". Using Group Policy names prefixed with your ND AD mnemonic Name will reduce the likelihood that similarly named Group Policy objects will be confused with one-another.

Notre Dame AD org mnemonic Names

We are working on securing a complete list of the Notre Dame AD mnemonic names and prefixes from the data source (HP), in the mean time we are using the following list:

OENG	IT: Operations & Engineering	SCI	Science
OPS	OIT: Operations Staff	CSE	Computer Science
HDSK	OIT: HelpDesk	FOOD	Food Services
DSS	OIT: Distributed Support	LSR	Lab for Social Research
ETS	OIT: Education Technology	LAW	Law School
ENTS	OIT: Enterprise Systems	MCOB	Mendoza College of Business
EDS	Enterprise Directory Services	ALCO	College of Arts & Letters
ENG	Engineering	LIB	University Libraries
		DEVL	Development Office

Computer Names

Windows 2000 computers have two names; a "long" name, and a "pre-Windows 2000", NetBIOS name. In most cases, the two names will be identical. The ADS naming standard is recommended for the "pre-Windows 2000", NetBIOS name and "long" computer names for the new computer being added.

The ADS naming standard for computer names is:

xxx-rest_of_name (or)
xxxrest_of_name

where:

xxx Registered organization prefix, 2 or more characters in length. See the Notre Dame ADS org mnemonic Names section below for directions on obtaining a prefix for your organization. We recommend keeping the prefix length to 4 characters or less. The dash (-) is optional, but recommended for ease of recognition.

rest_of_name

A suffix chosen by the organization creating the computer.

Example: MCOB-EXAMPLE123456789 ("long" computer name)

The "long" computer name is typically used to form the DNS name of the computer, and is also used to form the Distinguished Name (DN) of the computer in the Active Directory. However, the DNS name and the Distinguished Name(DN) for Active Directory are not necessarily the same. As illustrated in the example, a machine with hostname mcob-lab1 with DNS name mcob-lab1.business.nd.edu, has a DNS name different from the DN for Active Directory.

Example 1: Computer with hostname mcob-lab1, DNS name mcob-lab1.business.nd.edu, located in the MCOB OU in Active Directory

COMPUTER NAME: mcob-lab1

DNS NAME: mcob-lab1.business.nd.edu

DN: cn=mcob-lab1,ou=mcob,ou=campus,dc=nd,dc=edu

The "pre-Windows 2000", or NetBIOS, computer name is really the "account" name for the computer, and must be unique within the Windows 2000 domain in which it resides. Because WINS-based browsing services are still being used on campus, choosing a computer name that is unique throughout the entire Notre Dame campus environment is highly recommended, to avoid WINS name collisions. For compatibility with "pre-Windows 2000" operating systems, the length of the "pre-Windows 2000", or NetBIOS, computer name is limited to 15 characters.

Example: MCOB-EXAMPLE123 (NetBIOS name, truncated to 15 characters)

[1]

<http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adusers.asp>