

Policies for Notre Dame OU Administrators

DRAFT

Updated: 06/16/2003

1. Introduction
2. How to Join the Notre Dame Forest
3. Joining as an Organizational Unit (OU)
4. Computer Accounts
5. User Accounts
6. Group Policy Objects (GPOs)
 - 6.1 GPO Naming Conventions
 - 6.2 GPO Processing
 - 6.3 GPO Delegation
 - 6.4 GPO Security
7. Authentication
8. Passwords
9. Software License Compliance
10. Network Services
11. Internet Information Server IIS
12. Distributed File System (DFS)
13. Encrypted File System (EFS)
14. Enterprise Administration Responsibilities
15. Local Administration Responsibilities

1. Introduction

We anticipate that many departments and units, large and small, on the Notre Dame Campus will elect to join the Notre Dame forest. Most of the administrative responsibilities in the forest will be delegated to local administrators in these departments and units. Being a local administrator in the Notre Dame forest carries certain responsibilities and expectations. These policies are meant to delineate appropriate standards within the Notre Dame forest.

This policy is subordinate to the Responsible Use Policy (RUP) and the RUP takes precedence if in conflict. All participants must maintain conformity to the RUP and subsequent revisions thereof.

All local administrators in the Notre Dame forest must read and agree to the following policies, prior to being given an administrative account. Any local administrator who creates an administrative account for another local administrator must make sure the new administrator has read and agreed to these policies.

All Notre Dame local administrators (or their proxy) are expected to participate in the Notre Dame Active Directory Steering Committee (ADSC) and attend its meetings.

2. How to Join the Notre Dame Forest

- Familiarize yourself with these policies and the Notre Dame Naming Standards.
- Schedule a meeting with the ADSC by sending e-mail to AD Team. The ADSC will discuss your requirements with you.
- Agree to the Notre Dame policies and complete a Service Level Agreement (SLA)
- Provide the name of a mailing list for your local administrators that can be added to the Active Directory administrators listserv.
- Provide the NetID of the first administrator for the new OU.
- Provide the DNS name of the first computer that will join the new OU.
- Participate in the ADSC.

3. Joining as an Organizational Unit (OU)

Departments and units are encouraged to join the Notre Dame Active Directory as an Organizational Unit (OU). OUs are directory containers for directory objects (i.e., user, computer, and policy objects). The primary purpose of an OU is to make administration easier in terms of management and delegation. Control of an OU in the Notre Dame forest will be delegated to an OU administrator group who shall have the ability to manage users, computers, local security groups, and Group Policy Objects (GPOs) in their OU and sub-OUs. GPOs are a set of common configuration settings, like distributing software or changing the user environment, to help manage directory objects such as computers and users. OU administrators will only be allowed to apply GPOs for their OU.

4. Computer Accounts

In general, people who experience problems with a particular service should speak to their local administrator first. If the issue can't be resolved, then the local administrator can raise the issue to the appropriate support group. (See 16 Local Administration Responsibilities below).

Notre Dame naming standards are recommended for computer account names. Naming conflicts are left to local administrators to resolve. Priority will generally go to the OU that first used the name in the forest.

All workstations should keep "nd.edu" or other existing domain suffixes as their primary domain suffix. All workstations must be registered properly in the campus DNS. Use the existing DNS names (if legal Windows names). All workstations must have an Active Directory DNS name that matches their registered campus DNS name. The hostname component of the FQDN becomes the legacy short-name alias. Workstations in the forest must be configured to turn off DDNS registration. This is enforced by a site GPO which should not be blocked.

5. User Accounts

Notre Dame naming standards are recommended for user account names.

1. Local administrators are responsible for the local support of their user accounts. As a local administrator, it is up to you to educate your users on a regular basis so as to avoid common problems. The majority of issues you deal with will probably concern failed logins and security in the distributed Windows environment

Establish which security group the members of your department should always use for access to local shared folders. Document the process step-by-step, so users can follow it easily.

Enterprise data replicated into the Notre Dame campus domain from the EDS Directory (e.g., name fields, etc.) will be subject to automatic updating and should not be altered locally. Local administrators must take appropriate security precautions to protect user account data.

Local administrators should make every effort to delete expired or unused local user accounts in their OUs.

6. Group Policy Objects (GPOs)

Group Policy Objects are directory objects used to apply common configuration settings on computers and user objects. GPOs are associated with directory containers, and are thus applied indirectly to all user or computer objects within that container. Using GPOs, local administrators can perform tasks such as assigning a particular software installation to a set of computers, enforce security settings, or assign configuration options.

6.1 GPO Naming Conventions

The use of Notre Dame naming standards are strongly recommended for GPOs.

6.2 GPO Processing

- Group Policy template settings should be configured to process unchanged Group Policy settings.
- Be sure that a GPO has fully replicated before making further changes to it.
- The use of the No Override and Block Inheritance options on Enterprise policies is restricted and requires ADSC approval.
- Filtering of permissions on GPOs is generally not recommended.
- Even if local administrators are exempt from a GPO affecting normal users, they will be subject to some specialized GPO that governs security settings.
- Synchronous processing of Group Policy is recommended over asynchronous processing.
- The default Group Policy refresh rates should not be significantly decreased or increased.

6.3 GPO Delegation

- Use caution when delegating Group Policy to groups other than Administrators.
- Assign Group Policy permissions to security groups and not individual users.
- Full Control is not necessary to manage links or modify GPOs; assign the fewest

permissions needed.

- Limit the use of sensitive snap-ins, such as the Group Policy, Security Templates, and Security Configuration and Analysis snap-ins.
- In the case of non-administrative users, define GPOs that deny access to all snap-ins except those deemed necessary and explicitly listed as permitted.
- At a minimum, it is recommended that normal, non-administrative users not be allowed access to the Security Templates and Security Configuration and Analysis snap-ins. Access to these templates could allow a user to view all of the intended security settings of a system and perform an analysis to determine if the system is vulnerable to attack.

6.4 GPO Security

- It is recommended that computers within a Windows 2000 domain be grouped into separate OUs based on their role in the domain. For example, workstations will be in their own OU, member servers in another OU, and domain controllers in the Default Domain Controllers OU. Within this type of organization, GPOs containing security settings individualized for each type of computer can be easily applied.
- Group related settings in a single GPO.
- Set a strong Local Group Policy for computers that are not part of a domain. For domain computers, a good LGPO can compensate for holes in subsequently applied Active Directory GPOs.
- Use loopback processing only when necessary.
- Do not use legacy clients in a Windows 2000 network
- Enable Group Policy diagnostic logging temporarily when troubleshooting is required.

7. Authentication

“Cleartext” authentication is not allowed in the Notre Dame infrastructure. “Cleartext” authentication will be turned off on all domain controllers.

8. Passwords

Please refer to the recommended passphrase characteristics contained on the Change Password web page.

9. Software License Compliance

Participation in the Notre Dame forest does not entitle departments to licenses for operating systems or other software for departmental systems. The Notre Dame service includes only licenses for software required to operate the Notre Dame forest and Domain Controllers. Departments should ensure that systems participating in the Notre Dame forest are properly licensed for software running on their systems, including operating system or server software.

10. Network Services

Windows DNS Server Services must NOT be installed on any computer within the Notre Dame forest without prior consultation with OIT Networking Services and ADSC approval. Windows machines must be configured to turn off DDNS registration. OIT does not generally support DDNS for security reasons. A site-wide GPO automatically disables DDNS registration for members of the forest. This policy should not be blocked. All Notre Dame computers in the Notre Dame forest must have their primary DNS suffix name correctly entered, and must be registered in DNS to communicate properly in the forest. To conform to campus networking standards, all computers must have a DNS name that matches their registered node.

DHCP services must be coordinated with OIT Networking Services before joining the forest.

11. Internet Information Server (IIS)

By default, IIS services are turned off through Notre Dame Group Policy. This helps to ensure that local workstations cannot start 'rogue' IIS web servers. Local administrators can override the Notre Dame GPOs governing IIS in order to implement a well-managed IIS web service.

12. Distributed File System (DFS)

DFS is supported in the Notre Dame forest. Please contact Core Middleware Services if you wish to run this service.

13. Encrypted File Services (EFS)

By default, EFS services are turned off through Notre Dame Group Policy. Please be sure to understand the risks relating to lost encryption keys if you choose to override this policy.

14. Enterprise Administration Responsibilities

The Notre Dame Infrastructure is composed of many different computing, administrative and consulting services. This section provides a brief description of these services and specific contact information for each. In general, people who experience problems with a particular service should speak to their local Notre Dame administrator first. If the issue can't be resolved, then the local administrator raises the issue to the appropriate support group.

The OIT installs and maintains the server and support machines which run Active Directory for the ND domain. A group within OIT, Core Middleware service as Enterprise Administrators (EA). They install, configure, and maintain the Active Directory domain controllers for the AD domain that support the Notre Dame infrastructure. Urgent problems related to domain controllers or infrastructure services should be reported by calling the **OIT Help Desk** at **631-8111**. For general discussion, this group can be contacted via e-mail at AD Team.

The responsibilities of the Enterprise Administrators are:

- Install and maintain the Active Directory domain controllers in the AD domain that support the Notre Dame infrastructure.
- Notre Dame Enterprise Administrators are currently on duty Monday-Friday, from 8 a.m. to 5 p.m.
- Manage the flow of information from the EDS Directory to AD. The EA group also manages the replication of directory information within the Active Directory, and makes any enterprise level changes to the AD directory, such as schema modifications.
- Communicate all enterprise-wide changes to domain and OU administrators via the Notre Dame Change Management System. The NDCMS serves as the primary vehicle for the notification, coordination, authorization, and archiving of notable changes. The AD Team listserv will also be used as an email communication tool.
- Have administrator privileges on all domain controllers and OUs, in order to support and maintain the infrastructure's domain controllers and directory services.
- Assume a "hands-off" approach to local domain and OU administration. The EA group is not responsible for the administration of locally created user accounts. Only when faced with an enterprise-wide emergency, where no adequate alternative exists and every attempt has been made to contact appropriate support personnel and relevant managers first, will an Enterprise Administrator take action at the domain or OU level.

15. Local Administration Responsibilities

The responsibilities of local administrators are:

- Agree to the policies and guidelines for Notre Dame OU Administrators.
- Provide support for local users and services. In general, people who experience problems with a particular service should speak to their local Notre Dame administrator first. If the issue can't be resolved, then the local administrator can raise the issue to the appropriate central support group.
- The local administrator that requested the top-level Notre Dame OU for their unit will be the person responsible for designating which administrators will be added to this local administrative group account. Local OU administrators are required to maintain a mailing list for administrators who are active in their OU and provide the Enterprise Administrators with the name of the mailing list.
- Local OU administrators must keep themselves informed about domain-wide changes via the Notre Dame Change Management System.
- Local Notre Dame Administrators must join and participate in ADSC.
- Local administrators should make every effort to delete expired or unused user accounts in their OUs.