# Contents

1 - Preface ................................................................................................................................. 4

2 - Definitions ............................................................................................................................ 5

3 - Environment Overview .................................................................................................... 6

3.1 - Current Active Directory environment ............................................................................... 6

3.2 - Consolidated domain organizational structure ................................................................. 6

3.3 - Delegation of Administrative Rights ................................................................................. 6

3.3.1 - OU Admin group ............................................................................................................. 7

3.4 - Identity Manager (IdM) Integration ..................................................................................... 8

3.4.1 - User Account Auto-Provisioning ..................................................................................... 8

3.4.1.1 - Affiliations ..................................................................................................................... 9

3.4.2 - Moving Existing User Accounts ................................................................................... 10

3.4.3 - User Account Deprovisioning Process ......................................................................... 11

3.4.4 - Manual User Account Management Process ................................................................. 11

4 - Active Directory Conventions Overview ....................................................................... 12

4.1 - Naming Convention Overview ......................................................................................... 12

4.1.1 - Common Naming Convention Requirements ................................................................. 12

4.1.2 - Exceptions to Naming Conventions Requirements ....................................................... 12

4.1.2.1 - Procedure for approval ............................................................................................... Error! Bookmark not defined.

4.1.2.2 - Provide information to Information Services ................................................................. 13

4.1.2.3 - Request DuckID reservation for users ........................................................................ 13

4.1.2.4 - Engage Information Services to identify workarounds or migration strategies .......... 13

5 - Active Directory Object Types & Uses ........................................................................... 14

5.1 - User Objects .................................................................................................................... 14

5.1.1 - Managed User Objects (User objects with a DuckID) ................................................... 15

5.1.2 - Unmanaged User Objects (User objects without a DuckID) ....................................... 15

5.1.2 - User Account Passwords ............................................................................................... 16

5.2 - Computer Objects .......................................................................................................... 17

5.2.1 - Servers ......................................................................................................................... 17

5.2.2 - Workstations & Laptops .............................................................................................. 18

5.2.3 - Mac/Linux/Unix ........................................................................................................... 18

5.2.4 - Miscellaneous Devices ............................................................................................... 19

5.3 - Group Objects ............................................................................................................... 19

5.3.1 - Security Groups .......................................................................................................... 19

5.3.2 - Mail-Enabled Security Groups ..................................................................................... 19

5.3.3 - Email Distribution Groups ......................................................................................... 19
Since 2008, Information Services has worked in concert with key stakeholders in the campus IT community to consolidate Active Directory to a single Active Directory forest with users and resources in a single child domain, ad.uoregon.edu. Documentation, instructions, and requirements found in this guide pertain to OU administration within the consolidated child domain, with some consideration to migrations from, and interoperability with, legacy child domains and external forests.
### 2 - Definitions

**Active Directory**
Active Directory is Microsoft’s implementation of LDAP (a directory service) with advanced management and authentication functionality.

**AD**
AD refers to the consolidated ad.uoregon.edu Active Directory domain.

**Domain**
Domain refers to an Active Directory domain in the uoregon.edu forest.

**DuckID**
DuckID refers to the user’s UO username. This is used throughout the document as <duckid> and should be replaced with the actual username anywhere used. This document also uses ‘adm-<duckid>’ to refer to an OU admin account.

**Forest**
Refers to the top-level organization structure in an Active Directory environment. Forests > Trees > Domains > OUs

**Group Policy Object (GPO)**
GPO refers to an Active Directory Group Policy Object.

**Organizational Unit (OU)**
Organizational Unit refers to the classifying/organizing structure of an Active Directory domain. An OU can be thought of as the directory equivalent of a folder. Each unit/department is assigned an OU in which all computers, servers, groups and users are placed.

**OU Admins**
IT staff within a department granted administrative control over a unit/department Organization Unit using dedicated admin accounts.
3 - Environment Overview

The University of Oregon Active Directory environment is composed of a primary Active Directory forest with an empty root domain and a number of child domains. In addition, several stand-alone Active Directory forests (typically with a single domain) exist outside of the primary UO forest.

3.1 - Current Active Directory environment

At this time, the primary Active Directory forest for the University of Oregon contains one empty root domain, 1 consolidated child domain, and fourteen legacy child domains. The fourteen legacy child domains are scheduled for removal by the end of summer 2011, though this is dependent on server/service migrations performed by Domain Admins for these child domains.

3.2 - Consolidated domain organizational structure

Departments/Units participating in the campus Active Directory environment are allocated an Organization Unit in the AD domain. This OU can be found as a sub-OU of the top-level ‘Units’ OU (AD\Units\DeptName\). Each department/unit OU is pre-populated with the following required sub-OUs:

1) **Computers**: Contains all unit Computer objects
2) **Groups**: Contains all unit Group objects
3) **Servers**: Contains all unit Server objects
4) **Users**: Contains two sub-OUs
   a. **Managed**: User objects that are synchronized from the upstream Identity Manager system. These are ‘DuckID’ accounts and are all official UO accounts (faculty, staff, students, and many resource accounts).
   b. **Unmanaged**: User objects that exist *only* in Active Directory. These are typically service accounts, test accounts, or resource accounts for Exchange.

Please note, the Computers, Groups, Servers, and Unmanaged Users OUs may all contain additional sub-OUs for further granularity (delegation, group policy assignment, physical location, etc...). Additionally, it is important to note that top-level department OU structure is defined per IT unit, not by reporting structure.

3.3 - Delegation of Administrative Rights
A key component to the design of the consolidated environment was the implementation of a delegation model to match the decentralized nature of campus IT. To meet this requirement, the OU structure has been organized in such a way as to provide the significant flexibility. As such, several administrative models are supported:

1) One OU per IT unit.
   This is the standard delegation model. A single IT unit (one or many staff working for a single IT organization) is delegated responsibility to the department OU.

2) Many OUs per IT unit.
   In cases where a larger group of IT professionals managed pieces of an organization, a single OU may still be used. In this use case, further delegation granularity is gained by the creation of additional sub-OUs within each of the Computers, Groups, Servers, and Unmanaged Users OUs.

3) One OU for many IT units.
   In cases where a single IT unit supports several departments that are unaffiliated, it may be required to separate those units into individual top-level department OUs.

### 3.3.1 - OU Admin group

Regardless of the delegation model used, each OU has an administrators group following the convention <OUNAME>.OU.ADMIN (ex: IS.OU.ADMIN). This group is used to designate each department’s ‘OU Admins’, or IT staff that have been delegated top-level administrative control for the department’s OU.

This group and its members have several requirements:

1) Regular DuckID users should never be used as OU Admins.
2) Every member of the OU Admins group must be a dedicated administrative user.
3) OU Admin users should be placed in the Unmanaged Users OU.
4) OU Admins should never be mailbox-enabled (i.e. have an Exchange mailbox).
5) OU Admin users should follow the naming convention ‘adm-’ + DuckID, where DuckID is the username of the respective standard user account.
6) OU Admins should have long and complex passphrases. In general, these should be more complex and greater length than the standard DuckID user.

Membership in the OU Admin group will grant the following rights on the OU:

<table>
<thead>
<tr>
<th>UNIT.OU.ADMIN Granted Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create User Objects Inside the Unmanaged OU</td>
</tr>
<tr>
<td>Full Control Over User Objects in the Unmanaged OU</td>
</tr>
<tr>
<td>Modify Non-IdM User Attributes For Users in the Managed OU</td>
</tr>
<tr>
<td>Full Control of Computer Objects</td>
</tr>
<tr>
<td>Full Control of Group Objects</td>
</tr>
<tr>
<td>Full Control of OU Objects (with the exception of the Managed OU)</td>
</tr>
<tr>
<td>Create Group Policy Objects</td>
</tr>
<tr>
<td>Modify GPOs When Admin is the Creator</td>
</tr>
<tr>
<td>Delete GPOs When Admin is the Creator</td>
</tr>
<tr>
<td>Link GPOs within OU structure</td>
</tr>
</tbody>
</table>

The following rights have been revoked to all:

<table>
<thead>
<tr>
<th>UNIT.OU.ADMIN Revoked Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create User Objects Inside the Managed OU</td>
</tr>
<tr>
<td>Modify IdM-managed User Attributes in the Managed Users OU</td>
</tr>
</tbody>
</table>
3.4 - Identity Manager (IdM) Integration

The IdM system is the authoritative source for all accounts that are represented with a DuckID. These include all student, staff, faculty, and sponsored users; along with other departmental and affiliated accounts. The IdM system will provision and de-provision these accounts, as well as populate and maintain specific attributes. When provisioning, the IdM system will choose an object’s location in the directory based on information populated in University HR and employee databases; when information in these sources changes, IdM will re-evaluate the objects OU location.

All modifications to a user object in AD by the IdM system will include logging information appended to the user’s ‘info’ attribute. This logging information will contain the date along with a single line describing the change that occurred.

3.4.1 - User Account Auto-Provisioning

All user objects with a DuckID will be provisioned into AD through the IdM system. IdM will create the user, populate the user attributes, move the user to their destination OU; and if that destination is in a department OU, IdM will email the unit.ou.admin group notifying them of the new user.

The following are key attributes and their population by IdM:

<table>
<thead>
<tr>
<th>Information</th>
<th>IdM Attribute</th>
<th>AD Attribute(s)</th>
<th>Reason</th>
<th>OU Admin Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>DuckID</td>
<td>Uid</td>
<td>cn, sAMAccountName, displayName, name</td>
<td>Basic User Info</td>
<td>No</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
<td>givenName</td>
<td>Basic User Info</td>
<td>No</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>sn</td>
<td>Basic User Info</td>
<td>No</td>
</tr>
<tr>
<td>Middle Name</td>
<td>&lt;none&gt;</td>
<td>middleName</td>
<td>Not stored in IdM</td>
<td>No</td>
</tr>
<tr>
<td>Logon Name</td>
<td><a href="mailto:uid@ad.uoregon.edu">uid@ad.uoregon.edu</a></td>
<td>universalPrincipalName</td>
<td>Basic User Info</td>
<td>No</td>
</tr>
<tr>
<td>Email Address</td>
<td>&lt;none&gt;</td>
<td>mail</td>
<td>Set by mail- enable scripts in Active Directory</td>
<td>Yes</td>
</tr>
<tr>
<td>Manager Name</td>
<td>&lt;none&gt;</td>
<td>manager</td>
<td>Not stored in IdM</td>
<td>Yes</td>
</tr>
<tr>
<td>Office Phone</td>
<td>telephoneNumber</td>
<td>telephoneNumber</td>
<td>Basic User Info</td>
<td>No</td>
</tr>
<tr>
<td>Building/Office</td>
<td></td>
<td>physicalDeliveryOfficeName</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Postal Street Address</td>
<td></td>
<td>streetAddress</td>
<td>Basic User Info</td>
<td>Yes</td>
</tr>
<tr>
<td>Postal State</td>
<td></td>
<td>st</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Postal Zip Code</td>
<td></td>
<td>postalCode</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Country</td>
<td></td>
<td>co</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Password expiry Status</td>
<td></td>
<td>expirePassword</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>
Initial OU placement will be decided based on the same data that populates faculty and staff information in the UO directory. This system is based on employee home org codes that are associated with job information, and each code corresponds to a department/unit, which in turn matches an OU location in AD.

When Users have multiple org codes (jobs in multiple units), their employee home org will be used to decide which OU they are placed in. This data is held in the custom AD user attribute ‘UOAD-UoHomeDept’. If a user has incorrect org code data, the unit HR representative should look at updating the user’s employment data. If the org code is correct, but the user is still located in an inappropriate OU, the accounts clerk can create an over-ride to ensure the user is located in the correct AD container.

Individual unit OUs will have all faculty and staff populated into their Managed OU. This includes student workers and GTFs. If these users have an org code that does not match an existing OU, they will be provisioned into the Auth-Only OU at the top of the directory. OU admins can manually add these users to security groups or query for department information using the custom AD user attributes UOAD-EmplDept1 and UOAD-EmplDept2.

Students who have no job affiliation (no employee home org code) will be populated into the Students OU at the top of the directory. OU admins will have the ability to query students for major and minor status using the custom AD user attributes UOAD-UoStudMajor and UOAD-UoStudMinor (both attributes will hold all applicable department affiliations). Admins can utilize this data to identify by itself or to populate security groups for granting access to resources.

### 3.4.1.1 - Affiliations

Each user with a DuckID has at least one registered affiliation with the UO. Affiliations identify the type of user and in turn the amount of access to UO systems. Many users have multiple affiliations and when that occurs, the greatest amount of access takes precedence. The definition of these affiliations can be found at [http://ccadmin.uoregon.edu/idm/?q=node/1](http://ccadmin.uoregon.edu/idm/?q=node/1). The following list includes recognized affiliations along with the dates that AD services are provisioned and deprovisioned:

<table>
<thead>
<tr>
<th>Affiliation Type</th>
<th>Beginning Date of AD Service</th>
<th>Ending Date of AD Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Faculty</td>
<td>2 Weeks Prior to Appointment</td>
<td>End of Employment</td>
</tr>
</tbody>
</table>
### 3.4.2 - Moving Existing User Accounts

#### 3.4.2.1 - Changing Departments

When an existing user changes their employee home org code, their location in AD might need to change as well. IdM will detect an org code change and move the user to their new OU if applicable. When a user object is moved in or out of a unit OU the IdM system will send an email notification to the unit.ou.admin group.

#### 3.4.2.2 - Changing Affiliation

Changes in affiliation affect duration that users have access to AD resources following the end of their affiliated status with the University. When users have multiple affiliations, the affiliation with the greatest level of access takes precedence when deprovisioning accounts. When the greatest level of affiliation expires, the user is disabled in AD and an email message is sent to the unit.ou.admin group.

Some users with the special affiliations of ‘Retired’ and ‘Emeritus’ can have accounts that do not allow login to machines, but are for email only; this status must be requested by department admins. No automated movement or deprovisioning occurs when a user achieves these special affiliations.

<table>
<thead>
<tr>
<th>Role</th>
<th>Duration Prior to</th>
<th>Duration After</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate</td>
<td>2 Weeks Prior to Appointment</td>
<td>End of Appointment</td>
<td></td>
</tr>
<tr>
<td>Courtesy</td>
<td>2 Weeks Prior to Appointment</td>
<td>End of Appointment</td>
<td></td>
</tr>
<tr>
<td>Emeritus</td>
<td>By Request</td>
<td>Death</td>
<td></td>
</tr>
<tr>
<td>Faculty</td>
<td>1 Term Prior to Appointment</td>
<td>1 Term after Appointment</td>
<td></td>
</tr>
<tr>
<td>Fixed Term Enduring Faculty</td>
<td>2 Weeks Prior to Appointment</td>
<td>1 Term after Appointment</td>
<td></td>
</tr>
<tr>
<td>Fixed Term Short Term Faculty</td>
<td>2 Weeks Prior to Appointment</td>
<td>1 Term after Appointment</td>
<td></td>
</tr>
<tr>
<td>GTF</td>
<td>2 Weeks Prior to Appointment</td>
<td>1 Term after Appointment</td>
<td></td>
</tr>
<tr>
<td>Retired</td>
<td>By Request</td>
<td>Death</td>
<td></td>
</tr>
<tr>
<td>Sponsored</td>
<td>At Sponsorship Creation</td>
<td>Upon Expiry or Departure</td>
<td></td>
</tr>
<tr>
<td>Staff</td>
<td>2 Weeks prior to Start</td>
<td>End of Employment</td>
<td></td>
</tr>
<tr>
<td>Student</td>
<td>1 Term Prior to Enrollment</td>
<td>1 Term after Enrollment</td>
<td></td>
</tr>
<tr>
<td>Student Employee</td>
<td>2 Weeks Prior to Employment</td>
<td>1 Term after Employment</td>
<td></td>
</tr>
<tr>
<td>Temporary Employee</td>
<td>2 Weeks prior to Start</td>
<td>End of Employment</td>
<td></td>
</tr>
</tbody>
</table>
### 3.4.3 - User Account Deprovisioning Process

When a user’s access to AD resources expires (based on their affiliation), the account is disabled in AD for 75 days. An email is sent to the unit.ou.admin group to notify them of the change. After 75 days IdM will automatically remove disabled user accounts from AD, again notifying the unit.ou.admin group. If a disabled user needs temporary access to retrieve files or email, they should contact the accounts clerk who can re-enable their account for a fixed duration.

IdM will not modify Exchange attributes if a unit has their own Exchange server. Instead the unit will need to monitor those mailboxes and remove them based on their own policy.

#### 3.4.3.1 - Removing Exchange Mailboxes and attributes after user moves

In cases where a user has lost affiliation with your department, you will be unable to remove attributes set on the user.

### 3.4.4 - Manual User Account Management Process

The campus IdM system is the authoritative source for provisioning and deprovisioning DuckID based accounts in AD. All new accounts that are based on a DuckID will be created in AD by the IdM system. Users without current affiliation can be setup as a sponsored account through IdM.

There will be cases in which administrators will need accounts that are not users, but are used to run services or provide access to mail/room/resource objects. These accounts can be created in the AD Users and Computers MMC inside of the Unmanaged OU underneath the Users OU. All service accounts should follow the naming convention stated earlier.
4 - Active Directory Conventions Overview

The new Active Directory (AD) domain will be separated into OUs to ease the delegation of management for unit administrators. Each OU will represent a logical unit (or department) and all users that work for that unit will be present within the OU container (users in the same department will not be spread between different OUs). There may be cases in which a unit has IT related operations managed by staff in a different OU. In that instance their OU will be nested underneath a parent OU to allow delegated authority to propagate down.

AD will be structured so that the top level contains only the Units OU as well as the following built-in OU containers: Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, and Users. The Units OU will house all departmental unit OUs as well as Students and Auth-Only. All administration of objects not located in a Unit OU will be done by Information Services.

Unit OUs will be named based on an abbreviation of the actual campus unit they represent. To ease with management and naming we will try to keep abbreviations between 2-5 characters (CAS, SA, IS, LIB, LCB, etc). Each unit OUs will be structured with the following OU containers: Computers, Servers, Groups, and Users; the Users OU will also contain child OUs called Managed and Unmanaged. Unit OUs will also have a mail-enabled universal security group called unit.admin.ou.

4.1 - Naming Convention Overview

As all Active Directory objects now reside in the same AD domain, the potential for naming conflicts and added difficulty in tracking down poorly named objects is that much greater. To mitigate these potential risks in the shared environment, several required naming conventions have been instituted, along with a number of recommendations for each object type. This section will provide the basic Naming requirements that apply to all object types (users, computers, groups, GPOs). Additionally, the following sections of this guide will include requirements and recommendations for naming conventions that are specific to each object type.

4.1.1 - Common Naming Convention Requirements

All objects within a department’s OU, with the exception of *Managed* User objects, should meet a few minimum naming requirements, regardless of type. This convention has the following pattern:

<UNIT_Prefix><\ .><object_name_suffix>

< UNIT_Prefix > should match the department’s/unit’s OU name.

<object_name_suffix> should contain the functional description or name of the object.

The prefix and suffix sections should be separated by either a dash or a period. In Information Services, periods are used with Groups, but dashes are used with computers, servers, and unmanaged users.

Examples: IS-TestUser1, IS-CC-SERVER01, IS.SYSTEMS.STAFF

In cases where the OU name is too long to be used as a prefix value (ex: Library, PRINTING, Research), the preferred prefix should be unique across the domain (i.e. no two departments should use the same prefix) and used consistently across the OU.

Please refer to sub-sections for each object type in section 5 for additional requirements and recommendations on object naming conventions.

4.1.2 - Exceptions to Naming Conventions Requirements

While adhering to the naming conventions outlined in this guide are considered requirements for domain membership, there are cases in which this may not be possible. This may be allowed pending review by Information Services.

Exceptions to the naming convention requirements must be reviewed by Information Services.

The following steps must be taken for approval:
4.1.2.2 - Provide information to Information Services

The following information must be provided to Information Services:

1) The object(s) that cannot meet the naming requirement.

2) The business needs driving the non-conforming name(s).

3) The duration of time the business need(s) will require the non-conforming name.

4.1.2.3 - Request DuckID reservation for users

If the non-conforming object is either an unmanaged user, a DuckID reservation must be requested by contacting the Identity Management group in Information Services (idmhelp@ithelp.uoregon.edu).

4.1.2.4 - Engage Information Services to identify workarounds or migration strategies

An important step to the DuckID exception process is to contact Information Services to discuss workarounds and business needs driving exceptions. Contact IS Systems by sending an email to adhelp@ithelp.uoregon.edu to begin this process.
### 5 - Active Directory Object Types & Uses

The below table lists all the object types that exist in the domain and their planned uses.

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Uses</th>
<th>Access</th>
<th>Purpose</th>
<th>IdM Managed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Faculty &amp; Staff</td>
<td>Domain login, Exchange email, dept resources</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>User</td>
<td>Student</td>
<td>Domain login, dept resources</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>User</td>
<td>GTF</td>
<td>Domain login, Exchange email, dept resources</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>User</td>
<td>Computer Labs</td>
<td>Domain login</td>
<td>Used by systems to run services under a domain security context</td>
<td>No</td>
</tr>
<tr>
<td>User</td>
<td>Service Account</td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>User</td>
<td>Contractor / Consultant</td>
<td>Domain login</td>
<td>Student workers,</td>
<td>Yes</td>
</tr>
<tr>
<td>User</td>
<td>Shared login</td>
<td>Domain login, Exchange email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Retirees</td>
<td>Exchange Email only</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>User</td>
<td>Resource</td>
<td>Exchange Email only</td>
<td>Conference Rooms, projects, shared computers</td>
<td>No</td>
</tr>
<tr>
<td>Contact</td>
<td>Allow GAL/Email outside exchange</td>
<td></td>
<td>Non-exchange recipients</td>
<td>No</td>
</tr>
<tr>
<td>Security Group</td>
<td>Grant resource access to users</td>
<td></td>
<td>Provide access to secured resources</td>
<td>No</td>
</tr>
<tr>
<td>Email Group</td>
<td>Email list</td>
<td></td>
<td>Email group of users</td>
<td>No</td>
</tr>
<tr>
<td>Email-enabled Security Group</td>
<td>Email list that can grant resource access</td>
<td></td>
<td>Email group of users or provide access to secured resources</td>
<td>No</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>Organize objects</td>
<td></td>
<td>To allow delegation of authority, apply matching policy</td>
<td>No</td>
</tr>
</tbody>
</table>

#### 5.1 - User Objects

AD requires that specific attributes for a user be unique. As such, a username will be consistent across the following attributes on a single user object: cn, name, and samaccountname.

User objects should always have a comment in the notes attribute stating the date of creation, the creator, and the purpose of the account. In ADUC this attribute can be edited under the telephones tab.
5.1.1 - Managed User Objects (User objects with a DuckID)

All users with a DuckID will utilize the DuckID as their username in Active Directory. A user’s displayname in AD will match their displayname in IdM. This is usually the same as the username.

5.1.1.2 - Mailbox-enabled and Mail-enabled Users

OU Admins that are also Exchange Admins may mailbox-enable/disable and mail-enable/disable managed user objects in the department/unit OU.

Managed user email addresses should match the username of the user. Typically, the SMTP domain should be set as ‘@uoregon.edu’, though this configuration is dependent on the Exchange Server’s configuration, not the Active Directory user object.

Importantly, OU Admins may not mailbox-enable/disable or mail-enable/disable users that are not in their OU.

5.1.1.3 - Managed User Naming

As Managed User objects are populated by IdM, all naming conventions follow UO standards for DuckID accounts. OU Admins do not have direct edit access to username values on Managed User objects.

5.1.2 - Unmanaged User Objects (User objects without a DuckID)

The use of common prefixes and separators should be used to identify accounts that do not have a DuckID. In this guide, the word unit always means the 2-5 letter OU abbreviation for that unit/department in AD.

5.1.2.1 - Service Accounts

Service accounts can be created by OU admins using the AD Users and Computers MMC. Service accounts will reside in the unmanaged OU of the specific unit, under the Users OU. To help other admins identify service accounts, service accounts should be named with to provide sufficient insight into its functions, though the complexity of this name falls to the OU Admin to decide.

The recommended convention used in Information Services is: <unit>-SVC-<APP_AND_ADD'L_INFO>.

Ex: DEV-SVC-MSSQL (The service account used to run SQL services in Development).

5.1.2.2 - Lab Accounts

Lab accounts can be created by OU admins using the AD Users and Computers MMC. Lab accounts will reside in the unmanaged OU of the specific unit, under the users OU. To help other admins identify lab accounts, they should be named following the scheme of ‘unit.lab.labname’ (example CAS.LAB.SSIL223).

While lab accounts such as these can be created by OU administrators, they are not recommended. Most lab accounts of this type are legacy accounts that were required prior to general usage of Active Directory for all users with valid DuckID credentials.

5.1.2.3 – Kiosk Accounts

Kiosk accounts are accounts created to allow public access to resources without login to a workstation.

5.1.2.3 - Exchange Resource Accounts

Exchange Resource Accounts are mailbox objects that are Exchange mailboxes that refer to resources (e.g. rooms, equipment, vehicles) rather than real people. These accounts are typically used to control access to unit resources like conference rooms, projectors, and vehicles. These accounts will be provisioned with email address suffixes of ‘@ad.uoregon.edu’ and can receive email from internal UO users only.

Exchange accounts have two names of importance: the email address prefix, and the display name. The following naming conventions are targeted at the email prefix as a way to avoid naming conventions and to show resource ownership. While it is
generally advisable to have both display name and email prefix be similar, moderate deviation from the naming convention may be appropriate for the display name to aid users with GAL lookups.

Exchange Resource Accounts can be created by OU admins using the AD Users and Computers MMC. These accounts should reside in the unmanaged OU of the specific unit, under the users OU. To help other admins identify Exchange Resource Accounts, the email addresses should be named following the scheme of `unit.location.resource` (example IS.CC.projector3). The display name for this resource would be `IS CC Projector 3`.

For resource accounts that represent a room the email address prefix should be formatted like `unit.building.room number` (example AAA.LA.321). The room display names however will be looked up from the GAL, and should be more user friendly. Display names should follow same naming convention but without abbreviations like ‘AAA Lawrence Room 321’. In cases where a department is the designated authority for scheduling the room AND Exchange is the authoritative calendar (i.e., the room is not scheduled using R25 or some other solution), the room can be labeled as `building.room number` (example LA.321) with display name like ‘Lawrence Room 321’.

In cases where the account is used for more than merely calendaring (for instance a shared email box for unit IS support staff) a more fitting name would be `unit.mbox.use` (example SA.MBOX.ITVOICEMAIL).

### 5.1.2.4 - External Users

External Users such as contractors and consultants should be created as sponsored accounts and given a DuckID so that they may be provisioned through the IdM system. The provisioning process will allow the sponsoring staff member to choose a username for the guest through the IdM web interface. The interface will make suggestions based on the guest’s name and common UO DuckID naming conventions, but the sponsoring employee can utilize any name that does not conflict with an existing account.

### 5.1.2 - User Account Passwords

DuckID and AD passwords are synchronized so that users have a single credential to use regardless of the resource they are accessing.

#### 5.1.2.1 - Password Policy

The password policies for both AD and DuckID are identical.

The policy is as follows:

- Minimum Password Length: 8 characters
- Maximum Password Length: 128 characters
- Password History: 3 passwords remembered
- Maximum Password age: 180 days
- Minimum Password age: 0 days
- May not include the user’s DuckID, First Name, or Last Name.
- Must contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
5.1.2.2 - Password Change Mechanisms

The IdM/AD synch mechanism allows for bi-directional password synchronization. This means that a user can change their password through the IdM web interface or through their local workstation and it will propagate to both systems.

Because DuckID passwords offer access to a larger scope of resources, OU admins will not be able to change passwords or unlock accounts by default. Instead OU admins can apply to become a “Credentialing Agent” which gives them access to change passwords within their local OU. Please refer to the section ‘5.9 - Managing DuckID passwords as a Credential Agent’ in this guide for more information.

5.2 - Computer Objects

In this context, ‘Computer Objects’ specifically refers to Desktops, Laptops, and Server objects stored in the Units\UNITNAME\Computers and Units\UNITNAME\Servers OUs or a sub-OU of one of these.

5.2.1 - Servers

Department servers joined to the Active Directory should be placed in the department’s ‘Servers’ OU, one of the 4 top-level OUs for each department.

Server computer objects may be placed in sub-OUs of ‘Servers’ to provide additional granularity in applying policies or delegating permissions. The degree to which an OU Admin granularly separates servers into separate OUs depends entirely on the business needs of the department.

Examples:
- Ad.uoregon.edu\Units\<dept>\Servers - Standard OU for department servers
- Ad.uoregon.edu\Units\<dept>\Servers\Web Servers - OU for Web Servers
- Ad.uoregon.edu\Units\<dept>\Servers\Database Servers - OU for Database Servers

Servers are identified as server-class systems by the Operating System installed (Windows Server 2003/2008, Mac OS X Server, etc...).

In cases where workstation-class hardware (i.e. a desktop computer) is installed with a server Operating System and is used as a server, this computer should still be placed in the ‘Servers’ OU.

5.2.1.1 – Server Naming

Servers are often visible to a much larger audience and should have a more specific naming scheme. This will allow easy identification of servers and what resources they provide. It is recommended that servers are named based on the following logic (in order from least to most specific):

Unit OU Abbreviation - Location – <Service>Numerical Separator

- IS-CC-MSSQL01 (an IS server in the Computing Center running MS SQL)
- SA-OH-WEB04 (a Student Affairs server in Oregon Hall running web services)
- JWJ-WS-FS01 (a Finance and Administration server in White Stag operating as a file server)

In some cases, including server clustering, high availability, and public accessibility, a server should have a friendly name that makes its services more easily accessible. In these cases, the server should be named following the guidance above and a DNS CNAME should be registered for the friendly name.

In some environments there is a high likelihood that a server location may change or that additional applications and/or services will be installed. In these cases a naming scheme based on location or specific service does not make sense and should be replaced by
something simple like Unit-Purpose, like FS-App1 (A general application server in Facilities Services) or SA-OIP (A Student Affairs server that serves multiple purposes for the Office of International Programs).

### 5.2.2 – Workstations & Laptops

Department workstations & laptops should be placed in the department’s ‘Computers’ OU, one of the 4 top-level OUs for each department.

Computer objects may be placed in sub-OUs of ‘Computers’ to provide additional granularity in applying policies or delegating permissions. Computers may be placed in sub-OUs of the ‘Computers’ OU to meet a department’s business needs. A frequent usage is to separate computers in to OUs based upon supported departments.

Examples:
- ad.uoregon.edu\IS \Computers\ - Standard OU for department computers
- ad.uoregon.edu\IS\Computers\ACAD\ - Computer OU for Academic Services computers in IS
- ad.uoregon.edu\IS\Computers\EAA\Laptops\ - Computer OU for EAA Laptop computers in IS

#### 5.2.2.1 – Workstations & Laptop Naming

With many units residing in the same domain structure, workstations should be named with the department’s unique OU abbreviation, or a suitable and globally unique alternative, as a prefix.

Additionally, the following recommendations are offered:

1) Workstations and laptops should be denoted with ‘WKS’ and ‘LAP’ respectively, or a similarly suitable qualifier. A single letter (e.g. ‘W’ (workstation), ‘D’ (desktop), ‘L’ (laptop)) may be more appropriate depending on the department prefix length.

2) As many departments on campus purchase Dell computers, it is recommended that the Service Tag or serial number is used as the suffix.

3) Computer names should be kept at 15 characters or less in length. Longer names will function, but may cause unexpected results in certain situations.

Examples:
- IS-WKS-32KP8N (A Dell workstation in IS)
- SA-LAP-W43329GH (A laptop in Student Affairs)
- ORSA-L-HJ1233I (A laptop in ORSA)

It is important to note that some departments will use friendly names for workstations/laptops to indicate assigned users, room numbers, or other values. Again, however, the department/unit prefix is mandatory.

Examples:
- LCB-HarrysLaptop (A computer from the College of Business that does not specify chassis)
- LIB-WS-RM233 (A computer in the Library room 233, denoted as a workstation)

### 5.2.3 - Mac/Linux/Unix

Non-Windows clients may also participate in Active Directory for both authentication and management. While several methods are available to join a non-Windows client to Active Directory, the supported method is through the commercial product Likewise Enterprise.
For more information on Likewise Enterprise, please refer to the Likewise Enterprise service description:

http://it.uoregon.edu/systems/services/ad/likewise

Available on this page is the Administrator’s guide for University of Oregon OU Admins. This guide covers, in depth, Mac/Linux/Unix administration concepts with Likewise Enterprise and Active Directory.

### 5.2.3.1 – Mac/Linux/Unix Naming

Mac, Linux, and Unix systems should follow appropriate naming conventions for their device type, as detailed above. Note, however, that it may be appropriate to use an alternate indicator to denote a Mac Desktop/Laptop from a PC. Additionally, as Mac serial numbers are too longer for the 15 character limit, it is recommended to truncate or use an alternate naming convention.

Example:
IS-MAC-W8742342 (A Mac computer in IS)

### 5.2.4 – Miscellaneous Devices

Although mobile device access to Active Directory resources is now fairly minimal, it will most likely increase in the future. To assist administrators in tracking access and troubleshooting issues, mobile devices should follow the same naming scheme as workstations with the unit OU abbreviation used as a prefix.

### 5.3 - Group Objects

Group objects can be created by OU admins in AD Users and Computers and will not be managed by IdM. To help ensure that AD group names don’t conflict with IdM group names all AD groups should follow a common naming scheme. This will also assist ad admins in identifying who owns a specific group and its purpose.

#### 5.3.1 - Security Groups

Security Groups are the preferred method to assign access to resources. Groups can be created to apply the whatever level of granularity on resources required by a department.

It is recommended that groups are created to grant access to resources following the principle of least privilege.

#### 5.3.2 - Mail-Enabled Security Groups

Security Groups can be mail enabled, giving them an email address and allowing them to be utilized for email distribution to list members. Mail Enabled Security Groups can be published in the Global Address Book and sent email from within the UO Exchange Organization only. With regards to naming, these groups are equivalent to Security Groups.

#### 5.3.3 - Email Distribution Groups

Email Distribution Groups are used only for emailing users and contacts, and can’t be used to assign permissions to resources. These groups can be listed in the Global Address List and can be sent to from within the UO Exchange Organization only. These groups should be named following the scheme of ‘unit.email.groupname’. An example would be lib.email.librarians is an email list for librarians in the Library OU.

#### 5.3.4 – Delegation of Group Managed with the ‘Managed By’ attribute

A common delegation scenario is one where a user or group of users has a need to be able to directly manage membership of a group, but should have no other permissions outside of editing membership. This scenario is exactly what the ‘Managed By’ attribute is designed to accomplish.
To assign a group manager, do the following:

1) In Active Directory Users & Computers, find the group that you wish to assign a manager to.
2) Right-click and select Properties.
3) Select the ‘Managed By’ tab.
4) Select the ‘Browse’ button next to the ‘Managed By’ text box.
5) Find the user or group that should be assigned as manager.
6) Ensure that the ‘Manager can update list membership’ checkbox is checked.
7) Click ‘Ok’ to close.

At this point, the user (or all users in the group) will have privilege to edit membership of this group, either via Active Directory Users & Computers or Outlook 2003/2007/2010 if the group is mail-enabled.

### 5.3.5 – Group Naming

Similar to other object types, groups must also follow the minimum naming requirement of a department/unit prefix, a dash or period, followed by the name/function of the group.

The following additional recommendations are also given:

These groups will be named following the scheme of ‘unit.typeofresource.resourcename.access’.

Examples:

**LCB.FS.FILESERVER.FINANCE.RWM** - Provides Read, Write, and Modify (RWM) access to the finance folder on a share from a server named ‘fileserver’ in LCB.

**IS.SP.AD-INFO.KBASE.R** - this group provides Read access to a knowledge base page on a Sharepoint site called ad-info within IS.

<table>
<thead>
<tr>
<th>Dept OU</th>
<th>Type of Resource</th>
<th>Resource Location</th>
<th>Resource Name</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>The abbreviation used to name the OU.</td>
<td>The logical resource name in a 2-3 letter abbreviation. Examples: FS -&gt; Fileshare</td>
<td>The server name or public name of the resource like IS-Fileserver or Shell.</td>
<td>The location where access is given on the resource, usually a folder, site, or web directory.</td>
<td>R -&gt; Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Some security groups are created to encompass a broad spectrum of users and purposes (such as a security group for an entire unit or division). In these cases a detailed name as proposed above might be replace with something more general as long as it contains the unit prefix. For example the financial aid office is beneath the Enrollment Services OU and might have a group for all employees; an appropriate name might be ENROLL.FINAID.ALLUSERS or ENROLL.FINAIDUSERS.

### 5.4 - Group Policy Objects (GPOs)
Group Policy Objects, or GPOs for short, refer to sets of policy settings that may be ‘attached’ to OUs within the Active Directory domain. The policies include settings and controls for nearly every aspect of Windows, from login scripts to power options to screen saver settings. With the addition of Likewise Enterprise, much of this functionality is also available for many non-Windows clients.

Group Policy Objects are created, edited, and linked to OUs using the Group Policy Management Console.

### 5.4.1 - Domain-wide GPOs

Domain wide group policies will be used to apply consistent settings throughout all departments within ad. Because of the sweeping nature of these policies, IS will only deploy the following security settings for computers domain wide.

The following settings will be applied to all computers connected to the domain:

- **Default Domain Policy**: This policy defines global password, Kerberos, and account policies.
- **AD-DefaultLogonDomain**: This policy sets the default logon domain for all domain-joined workstations and servers to AD.

### 5.4.2 - GPO Copying/Usage

While few policies are applied to all units in ad, most GPOs attached to any department OU are readable by OU Admins. As such, any GPO that an OU Admin can read may be copied, renamed, and reset with appropriate permissions for the OU Admins unit.

There may be instances when an OU Admin in one OU would like to link a policy created by another administrator. While this is technically possible, caution should be taken as the original owner can modify or delete that policy at any time. Because of this, each Unit/Department OU should maintain its own set of group policies.

### 5.4.3 - GPO Permissions

Default permissions on GPOs will be:

- **All Unit Admins**: Read All GPOs, Create GPOs, Link GPOs.
- **GPO Creator**: Modify GPOs, Delete GPOs.

After a GPO is created by an OU Admin, the OU Admin must manually assign their <dept>.OU.ADMIN group with full control of the GPO. If this is not done, other OU Admins from the department may not be able to edit the GPO.

Admins may only link GPOs to OUs within their own department/unit OU structure.

### 5.4.4 - GPO Naming

Group policy objects are stored in a shared area, visible to all OU admins. To help make policy management easier to understand, all group policy objects should follow a unique naming structure to help differentiate them from each other. Policies should be named: `<unit>-<type of policy (comp or user)>-<service or option>-<setting>`

**Examples:**

- **IS-COMP-SMB2-DISABLE** (An IS GPO for computers that disables SMB2)
- **CAS-COMP-WSUS-Desktops** (A CAS GPO for computers to modify desktop WSUS settings)
- **SOJC-USER-Mydocs-Redirect** (A Journalism GPO for users to redirect their My Documents folder)

If departments prefer to combine GPO computer and user settings or prefer a simplified naming scheme, the following would also be appropriate: `<unit>-<type of policy>-<policy name>`

**Examples:**
LIB-BOTH-DOWNSTAIRS (A GPO for both computer and user settings in the Library)

ES-BOTH-FINAD (A GPO for both computer and user settings in the Enrollment Services)

| 5.4.5 - GPOs & WMI Filtering |

IS creates and maintains a set of WMI filters for use by OU Admins to provide additional GPO filtering capabilities. The available WMI filters are focused on filtering policy application by Operating Systems (WinXP vs Win7). The WMI filters may be accessed on the ‘Scope’ tab of the GPO through the Group Policy Management Console (GPMC)

Please note that WMI filters do add an additional cost to GPO processing on the workstation and can impact startup and logon times.
5 - OU Administration Basics

5.1 - Requesting an Organization Unit (OU) for your department

Any department/unit at the University of Oregon with dedicated IT staff is eligible to participate in the campus Active Directory environment. The first step in this process is to contact IS Systems (adhelp@ithelp.uoregon.edu).

A condensed version of the steps involved in the creation of an OU is as follows:

1) DEPT: IT staff from a department request the creation of an OU to adhelp@ithelp.uoregon.edu.
2) DEPT: A name is selected based upon the name (or preferably acronym) of the requesting department.
3) IS: OU provisioning scripts are run to create the parent <dept> OU, the child Computers, Groups, Servers, and Users OUs, the <dept>.OU.ADMIN group, and assign all initial permissions.
4) IS: The first adm-<duckid> is created and added to the <dept>.OU.ADMIN group. This account will be the primary administrative account for the IT staff with the matching DuckID as their standard user. This is the OU Admin account.
5) IS: The password for this new OU Admin account is given to the IT staff that owns the account.
6) IS: An initial computer object is created in the department’s ‘Computers’ OU to match the name of the first Windows admin workstation to be initially used for administration.
7) DEPT: Department ORGN codes are retrieved (generally through the department HR / budget staff). These identify department affiliation on a user.
8) DEPT: ORGN codes are given to IS staff.
9) IS: ORGN codes for the department/unit are mapped in IdM to the new department/unit OU.
10) IS: Accounts matching the ORGN code are manually processed and moved to their new OU location (DEPT\Users\Managed).

5.2 - OU Admin accounts

OU Admin accounts are unmanaged users accounts granted special permission to an OU to perform administrative functions. As these are standard user accounts, additional OU admins may be created at any time and may have their passwords reset by other OU Admins in the department.

5.2.1 - Request a password change for an OU Admin account

As OU Admins are standard user accounts, another OU Admin in an OU may change the password on behalf over an OU Admin. If this is not possible due to vacation or the presence of only a single OU admin in a unit, these password resets may be performed on request by Information Services. OU Admins may be required to come in person for the password to be reset.

5.4 - Preparing an admin Windows workstation

This section details the steps required to setup your Windows XP/7 Admin workstation to manage your Active Directory OU. OU Administration is done with two primary tools: the ‘Active Directory Users & Computers’ console and the ‘Group Policy Management Console’.

1. Identify a Windows workstation currently joined to the AD domain to run the AD Administrative tools.
2. Install the Active Directory User & Computers Console:
   a. Windows XP:
      i. Download adminpak.msi from Microsoft:
         1. http://download.microsoft.com/download/c/7/5/c750f1af-8940-44b6-b9eb-d74014e552cd/adminpak.exe
   b. Windows 7
      i. Download ‘Remote Server Administration Tools for Windows 7
      ii. Enable Active Directory Users & Computers Console
         1. Open ‘Control Panel’
2. Open ‘Programs and Features’
3. Click ‘Turn Windows Features on or off’
4. In the ‘Windows Features’ window
5. Expand ‘Remote Server Administration Tools’
6. Expand ‘Role Administration Tools’
7. Expand ‘AD DS Tools’
8. Check ‘Active Directory Administrative Center’
9. Check ‘AD DS Snap-ins and Command-line Tools’

3. Install the Group Policy Management Console (gpmc.msc)
   a. Windows XP:
      i. Download gpmc.msc from Microsoft:
         1. http://download.microsoft.com/download/a/d/b/adb5177d-01a7-4f04-bfcc-cb7cea8b5bb7/gpmc.msi
   b. Windows 7:
   ii. Enable Group Policy Management Console
       1. Open ‘Control Panel’
       2. Open ‘Programs and Features’
       3. Click ‘Turn Windows Features on or off’
       4. In the ‘Windows Features’ window, browse to ‘Remote Server Administration Tools’ then ‘Feature Administration Tools’
       5. Check ‘Group Policy Management Tools’

5.5 - Running AD Tools from an OU Admin user context

Managing your department’s Active Directory OU has several important considerations:

1. Logon to an admin workstation should be done from a standard user account.
2. All administration should be done from the user account specifically created for AD OU administration (generally ‘adm-username’).
3. Standard, managed user accounts should *never* be granted OU Admin permissions.

To run administrative tools from the security context of your OU Admin user while logged in as a standard user, you may do the following:

1. Click Start > Run
2. Enter: runas /user:ad\adm-<duckid> cmd (where <duckid> is replaced with your DuckID username)
3. Enter the password for your OU Admin account when prompted.
4. In the new CMD window, type the following:
   a. dsa.msc - This will open the Active Directory Users & Computers console in the OU Admin context.
   b. gpmc.msc - This will open the Group Policy Management Console in the OU Admin context.
5. Close the CMD window.

5.6 - Pre-create a computer object in Active Directory

Prior to joining any computer (server, desktop, laptop, etc...) to the domain, the corresponding computer object must be pre-created.

1. On the Windows Admin workstation, open the Active Directory Users & Computers mmc console
   a. Start > Run > dsa.msc, or open Active Directory Users & Computers.
2. Browse to your unit’s Computers OU
   a. Ad.uoregon.edu \ Units \ <unit> \ Computers \\n3. Right-click > New > Computer
4. Enter the name of the computer object
   a. ex: ad.uoregon.edu\Units\IS\Computers\SYS\is-mac-2385fh3
5.7 - Join a Windows computer/server to the AD domain

After the computer account has been pre-created, the computer may be joined to the domain. This may be done either using the GUI (the standard method) or the command line. The GUI method will be covered in this guide.

Using the GUI:

1) Right-click ‘My Computer’
2) In the ‘Computer name, domain, and workgroup settings’ section, click ‘Change Settings’
3) On the ‘Computer Name’ tab in the ‘System Properties’ pop-up, click ‘Change’.
4) In the new window ‘Computer Name/Domain Changes’, select Member of ‘Domain’
5) Enter ad.uoregon.edu in the ‘Domain’ box and click ‘OK’
6) When prompted for credentials, enter the following:
   a. Username: ad\adm-<duckid>
   b. Password: <admin user password>
7) Click OK, then OK

5.8 - Special Considerations for OU Administration

Due to technical requirements and workflow changes, special considerations exist for OU Admins that may not have been an issue in decentralized

5.8.1 - Joining the first computer to an OU

In order to join a computer to a domain, its computer account must usually first be pre-created in Active Directory. However, in order to pre-create an account, you must have an admin console to perform this pre-creation from, which must already be domain-joined.

To work around this catch-22, the first workstation account in a unit’s OU will be pre-created by Information Services during the initial creation of the unit’s OU. This will allow the OU Admin to join the first Windows admin workstation to the domain.

5.8.2 - Send As permissions

Send As permissions on a Mailbox-enabled user object must be requested by sending an email to adhelp@ithelp.uoregon.edu.

Ability to edit this permission cannot be delegated to OU Admins.

5.8.3 - RFC 2307 UNIX Attributes (uid, uidNumber, gidNumber)

RFC 2307 UNIX attributes (uid, uidNumber, gidNumber) are used by non-Windows hosts to uniquely identify users (uid, uidNumber), groups (gidNumber), and primary group membership of users (gidNumber). These are roughly the equivalent of Active Directory user sAMAccountname, SID, and primary group attributes and the group SID. If these fields are not populated, linux/unix/mac hosts may not allow login from Active Directory accounts or use AD groups to assign permission to resources.

These values are automatically populated on Managed user objects as managed attributes by IdM. These values cannot be edited.

Unmanaged users do not have these values populated by default. The attributes also cannot be edited by OU Admins. Due to this, intervention from Information Services will be required to enable these accounts to login to non-Windows hosts requiring these values.

Additionally, Active Directory group objects also do not have the gidNumber attribute populated.

To request population of UNIX attributes on an unmanaged users or groups, send a request to adhelp@ithelp.uoregon.edu.
Please note that mass population of UNIX attributes on unmanaged users or groups is not supported at this time.

5.8.4 - OU placement of Managed User Objects

The process by which a Managed User object is placed into an OU is based upon data pulled from Banner that indicates a user’s affiliation and department. This means that accounts, depending on the speed and accuracy of paperwork being submitted, may end up in either the wrong OU or may not be moved to a new department OU before the employee begins work.

To help mitigate this issue, please see the following suggestions and comments:

5.8.4.1 - Group Membership

The permissions to add members to a group are entirely based on the OU Admin’s permission on the *Group*, not the user. This means that OU placement of the user object will not adversely affect an OU Admin’s ability add a user to a group.

5.8.4.2 - Mailbox Enabling and Disabling

As adding and removing and Exchange mailbox requires sufficient permissions on the user object, an incorrect OU will adversely affect the OU Admins ability to add or remove and Exchange mailbox from a user.

To add or remove an Exchange mailbox on a user object incorrectly placed in another OU, send an email request to adhelp@ithelp.uoregon.edu.

5.8.4.3 - Removing department specific user attributes

In many units, values are added to user object attributes that are not managed by IdM. These may include department, manager, office, web page, home folder, etc....

If a user has been moved out of the OU Admin’s OU, the OU Admin will be unable to delete these values.

To have these attribute cleaned from a user, send an email to adhelp@ithelp.uoregon.edu to request account cleanup.

5.8.4.4 - GPO Placement - User vs Computer OUs

Given the potential delay on placement of a managed user in a department OU, it is recommended that User Group Policy Objects are assigned to Computer OUs rather than User OUs where possible. This may have a number of implications, including the requirement to enable ‘Loopback processing’ on the GPO.

This setting can be found in the GPO here:

Computer Configuration\Administrative Templates\System\Group Policy\User Group Policy loopback processing mode

Typically, this value should be set to ‘Merge’. ‘Replace’ will cause the computer to ignore all user GPO settings and replace with those in this policy.

5.9 - Managing DuckID passwords as a Credential Agent

The Credentialing Agent roles provides IT staff with the ability reset Duck ID passwords for accounts in their organizational unit through the Identity Manager web interface. This role is not granted by default to OU Admins and requires additional training by the IS IDM team.

For more information on Credentialing Agents: http://ccadmin.uoregon.edu/idm/ca
6 - Server/Service migrations from legacy child domains

Migration of a server/service from a legacy child domain into the consolidated ad.uoregon.edu domain may have a number of complexities, but can be streamlined by performing the following steps (as applicable).

6.1 - Naming Convention Implications

An important requirement of the AD domain is the minimum naming requirements on all computers, servers, groups, and unmanaged users. While this prevents OU admins from impacting the work of other OU admins, it does add complexities to server migrations into the AD domain. As an OU admin, you may need to update DNS records, GPOs, scripts, and other places where the old server name was specified.

6.2 - Pre-creating service accounts

If your service requires an Active Directory user object to run the service, it is important to create a *new* user object in your unit’s Unmanaged Users OU. If given sufficient privileges on the server in the legacy domain, you may be able to switch the service to the new AD service account prior to migrating the server between domains. Doing so will help to minimize the need for last-minute troubleshooting and testing on the day of migration.

6.3 - Pre-creating computer objects

Similar to pre-creating a new computer object before joining a new computer to the domain, you must also create a new computer object in the AD domain for server migrations. For simple server migrations, such as File and Print servers, the steps for migration can be the simple as follows:

1) Create a new computer object in the AD domain following appropriate naming conventions.
2) Confirm the local administrator account on the server has a known username/password.
3) Drop the existing server from the legacy child domain.
4) Login with the local administrator account, change the server to match the new name, and restart.
5) Login with the local administrator account and join the ad.uoregon.edu domain. Use ad\adm-<username> credentials.
6) Update Group Policy objects that map network drives to the old server name.
7) Add/Update DNS records for the new server name.

Please note, servers migrated using automated tools (e.g. Active Directory Migration Tool), will not require pre-creation. However, these migrations must in coordination with Information Services, whereas the Pre-create + drop/join method will not require this degree of coordination.

6.5 - DNS records

As many servers did not historically have a department prefix on the server name, a name change is required for the server to be moved into the AD domain. This may mean that DNS records, scripts, and other direct references to the old computer name will require updating to match the new name.

It is important to note that all computers supporting Dynamic DNS will automatically register in ad.uoreogn.edu via the Active Directory integrated DNS in this domain.

6.6 - Local Server Administration

In many child domains, server administration was performed using the default Administrator account, or another member of the ‘Domain Admins’ group in the child domain. As Domain Admins are added by default as local administrators on each workstation and server in the domain, no additional considerations for administration may have been required.

With the consolidation into the AD domain, this is no longer possible. Each unit has been granted an OU Admin, but this group (or another group depending on requirements), must specifically be granted Administrative access to the host.

The recommended method for doing this in a migration scenario is to do the following:
1) Confirm the local administrator account on the server has both a known username and password.
2) Create a group in the Unit’s OU for server administration, or use the default *.OU.ADMIN group.
3) Add this group to the local ‘Administrators’ group on the computer prior to migration.
4) Migrate the server/workstation.
5) Post migration, all users in this group will still have administrative access.

An alternative to this method is to simply create a Group Policy Object attached to Servers OU that grants local administrative rights. Once the server is migrated to the AD domain and placed in the appropriate server OU, the GPO will grant appropriate administrative access.
In order to maintain a baseline of both security and function, Information Services will perform automated audits on a number of requirements as outlined in this manual. Reports will be sent to OU Admins quarterly. Results from these reports should either be remediated in a timely manner (generally before the next reports are sent). If a business need sets a requirement to do something that violates a rule in one of these reports, the OU Admin must contact Information Services to discuss exceptions and/or alternate strategies for remediation.

Following are a sample of these audits:

### 7.1 - Non-conforming Names

This report pulls all Computers, Servers, Groups, and Unmanaged Users that do not meet at least minimum naming convention requirements.

### 7.2 - OU Admin group membership by non-admin users

This report finds users that are members of the &lt;DEPT&gt;.OU.ADMIN group that are not ‘adm-’ accounts. In particular, this report looks for regular Managed User accounts joined to the OU.ADMIN group as this can be a significant risk and should never be done.

### 7.3 – Mailbox-enabled OU Admin users

This report finds any OU Admin users that have Exchange mailboxes. This can be a significant security risk and should generally not be done.