DCSS V. Wampler
NIHRFC0008 CIT
Category: Best Community Practice February 2008

AD Attribute Data Content and Management: Best Community Practice V1.3

Status of this Memo

This document specifies National Institutes of Health (NIH) architecture best practice for the NIH community for Active Directory (AD) Attribute Data Content Management and requests any suggestions for improvements. AD user object attributes were ratified by the NIH ITMC Architecture Committee on May 25, 2004. The updated version of this document was sent through the NIH ITMC Infrastructure and Operations Committee October, 2007. Please refer to the current edition of NIH "Architecture Standards Process" (NIHRFC 0001) for the standardization state and status of this protocol. Distribution of this memo is intended for the NIH community.

Abstract

This memo documents a set of principles for the creation and maintenance of AD attributes. These principles include:

1. Definition of AD Attributes;
2. AD Account naming convention and content rules;
3. Computer naming conventions;
4. Group Policy naming conventions;
5. Required documentation; and
6. Security auditing.

This memo describes how the NIH Active Directory attribute administration should occur and presents recommended practices for NIH business managers, application designers/developers, and security officers. Additionally, the goal of this BCP is to enable application owners to decide which attributes will best meet their specific application requirements.

Table of Contents

1 Introduction

AD includes accounts for users (that is, an individual person or an administrator), groups, computers, and resource and service accounts. Each attribute for user, group or computer objects is described in detail in the sections that follow. Additionally, naming conventions for other AD objects are established to prevent naming collisions.

In order to facilitate a greater degree of manageability in the creation, identification, and management of AD attributes, this BCP shall address common best practices that will provide a framework to enable NIH application owners to better utilize AD attributes.

All AD user objects will follow NIH Password Policy and NIH Account Policy.

This best practice shall support the NIH Enterprise Architecture principles of "Optimum Enterprise Benefit" and "Standardization of Common Data."

1.1 Identified Needs

- Establish a common content best practice for Active Directory object attributes within NIH and shared with the HHS and other OPDIVS.
- Establish best practices and relevant guidelines required for creating, populating and maintaining Active Directory user and computer object attributes.
- Establish auditing standards for Active Directory attributes.
- Secure executive support and IC buy-in for the Active Directory attribute best practices articulated below.

2 AD User Account Attribute Data Content Principles and Best Practices

The following principles and associated best practices apply to all NIH Active Directory user object attributes.

2.1 Active Directory User Account Principle

An Active Directory user account is created so that a person at NIH can use IT resources and services (i.e. email, VPN, network file and print services). Such a person might be, but is not limited to, one of the following: NIH employee, contractor, tenant of NIH facilities, participant in the NIH visiting programs, registered user of NIH computer facilities, grantee, reviewer, council member, or collaborator. Before each person is issued an AD user account, they must first be registered in the NIH Enterprise Directory (NED) and be assigned a NED ID. Each person is authorized for a single, primary AD account. A person shall not be registered as a Resource account. AD user names are centrally registered at CIT, which ensures naming uniqueness and provides a registry of account names.

2.2 AD User Attribute Data Content Management Rules

2.2.1 Last Name

Common (preferred last name) or legal last name of person; does not include a generation qualifier. May contain spaces, hyphens, and apostrophes.

AD Attribute Name: **sn** (Surname)
Max Length: 64
Example(s): “O’Connell” “della Robbia” “Smith-Davies”

2.2.1.1 First Name

Common (preferred first name) or legal first name of person. May contain spaces, hyphens, and apostrophes.

AD Attribute Name: **givenName**
Max Length: 64
Example(s): “Chou-Chi” “Jim” “Mary Jane”

2.2.1.2 Employee Identifier

The NIH unique identifier assigned to a person by NED in the form of ten digits.

AD Attribute Name: **employeeID**
Max Length: 16
Example: 0010058023

2.2.1.3 Employee Type

Person’s employment status: Employee (all NIH Full-Time Equivalent (FTE)), Fellow, Contractor, Guest, Volunteer, Tenant.

AD Attribute Name: **employeeType**
Max Length: 64
Examples: “Employee” “Fellow” “Contractor” “Guest” “Volunteer” “Tenant”

2.2.1.4 OpDiv Name

Official 2- to 6-letter (needed for SAMHSA) abbreviation for operational division where a person works. All NIH personnel have this set to “NIH”.

AD Attribute Name: **company**
Max Length: 64
Examples: “NIH” “HHS”

2.2.1.5 IC

Official 2- to 5-letter abbreviation of the institute or center (IC) that the person is associated with.

AD Attribute Name: **department** (Department)
Max Length: 64
Examples: “CIT” “NCI” “OD”

2.2.1.6 Lab/Branch/Office

Official abbreviations of the Lab/Branch/Office that the person is associated with. 64 maximum characters, separated by slashes as needed.

AD Attribute Name: **physicalDeliveryOfficeName**
Max Length: 64
Example(s): “CIT/DCSS/BOSB” “OD/OST/IRTP”

2.2.1.7 sAMAccountName

Unique name that represents a person who uses network resources and services. (NOTE: AD user names will be centrally registered at CIT. This will ensure naming uniqueness and provide a registry of account names to owners.)

Formula using AD attributes: **sn** + first initial of (and one or more letters, as needed) of **givenName** + first initial (optional, if needed) of **middleName** + digits (if needed for NIH-wide uniqueness, not only within an IC).

20 maximum characters, truncate surname if necessary. Characters are a-z, A-Z, and 0-9 only, no special characters allowed. Resolve NIH-wide duplicates with a digit starting with 2. Capitalize first letter in each name attribute used. Because of the large number of technical dependencies, a person should only be issued one sAMAccountname during their tenure at NIH. However, if there is a legal name change, a person can have a new sAMAccount created and associated with their old NED ID.

AD Attribute Name: **sAMAccountName**
Max Length: 20
Examples: If: **sn**=Doe, **givenName**=Joseph, **middleName**=W, then: “DoeJ” “DoeJW” “DoeJW2” “DoeJo” “DoeJos” “DoeJose” “DoeJosep” “DoeJoseph” “DoeJosephW” “DoeJosephW2” etc.

2.2.1.8 userPrincipalName

Identifier for a person that is an Internet-style login name based on the Internet standard RFC 822, uses AD attribute **sAMAccountName** plus “**@**”suffix and domain address.

AD Attribute Name: **userPrincipalName**
Max Length: 64
Examples: “doejw@mail.nih.gov” “doejw@nih.gov”

2.2.1.9 Proxy Email Address

All supported electronic messaging addresses of a person.

Formula for email: “smtp: mailNickname@mail.nih.gov” is then sent to **mail** attribute. Additional email addresses can be added (otheraddress@ic.nih.gov).

Attribute Name: **proxyAddresses** (Proxy-Addresses)

Max Length: 256

Example: “doej@nih.gov” “John.Doe@nih.gov” “John.Doe@nih.hhs.gov”

2.2.1.10 Email Address

Primary SMTP email address (default reply-to) for a person as represented by Central Email Service (CES) at NIH. Same rules as above **proxyAddresses**; pulled from **proxyAddresses** if

populated. The primary smtp address will be generated by Exchange's Recipient Update Service (RUS) at AD user account creation.

AD Attribute Name: **mail**
Max Length: 256
Example: "doej@mail.nih.gov"

2.2.1.11 Street Address

The first line is NIH Mailstop. The physical address of the person's office (street address of building) will continue on the second line.

AD Attribute Name: **streetAddress** (Street-Address)
Max Length: 1,024
Example: "12 SOUTH DR"

2.2.1.12 Location (2003)

Name of building/room number.

AD Attribute Name: **roomNumber,** and **msExchangeAssistantName**
Max Length: 256
Example: "12A/2025"

2.2.1.13 City

The city, locality, or geographical area name.

AD Attribute Name: **l** *(lower-case "L")* (Locality-Name)
Max Length: 128
Example(s): "Bethesda" "Triangle Park" "Rockville"

2.2.1.14 State

State or province postal abbreviation of location of the person's office.

AD Attribute Name: **st** (State-Or-Province-Name)
Max Length: 128
Examples: "MD" "PR" "AE" "QC"

2.2.1.15 Country

This attribute uses the ISO numeric-3 code

AD Attribute Name: **countryCode**
Max Length: 3
Examples: "(840) United States" "(296) Kiribati"

2.2.1.16 Postal Code

US Postal Service ZIP code or foreign postal code. May use a maximum of 40 and a minimum of 5 characters.

AD Attribute Name: **postalCode** (Postal-Code)
Max Length: 40
Examples: "22171" "20814-5512" "MK4 1B4"

2.2.1.17 Office Telephone Number

Office telephone number with area code or country and local area codes separated by periods. Extension if any noted by space x followed by extension number. 64 maximum characters.

AD Attribute Name: **telephoneNumber** (Telephone-Number)
Max Length: 64
Example(s): “301.496.1234” “301.555.1234 x25” “55.1.4966.1234”

2.2.1.18 employeeNumber

employeeNumber will have several different data entries depending on the type of user account. All AD user objects will have a value of “primary”, “secondary”, or “resource” in this attribute.

PRIMARY: This setting indicates the primary AD account for a person at NIH. The NED ID will be associated with this account.

SECONDARY: This setting indicates a secondary AD account for a person. The Executive Officer at the person’s IC must request and approve this situation. NED ID is listed for this account.

RESOURCE: This setting indicates a service or resource user account.

2.2.1.19 Display Name

Displayable, “friendly” name, representative of a person.

AD Attribute Name: **displayName** (Display-Name)
Max Length: **256**
Example(s): **“Doe, James (NIH/CIT) [E]”**

Formula *must* use the following AD attributes: **sn**+ “, ” + **givenName** + **(company/department)** + **[**first initial of **employeeType]**

Employee type is abbreviated and placed as a single character between brackets **[ ]**:

[E] Employee, all NIH Full Time Equivalent (FTE)

[F] Fellow

[C] Contractor

[G] Guest

[V] Volunteer

[T] Tenant

Formula may *optionally* use the following AD attributes:

middleName (or first initial of middle name) is optional, place after **givenName**.

generationQualifier is optional, place after **middleName** or if none, after **givenName**.

Titles, such as M.D. or Ph.D. are optional, place after name, before **company.**

Further delineation of labs, branches, and offices is optional, place after “/” after **company/department** within parentheses.

If display name is a duplicate, use digits, beginning with 2, place after name (or generation qualifier or titles, if any).

Example including optional attributes: “Doe, James Carlos III Ph.D. 2 (NIH/CIT/DCSS/EMIB) [C]”

2.2.1.20 Canonical Name (cn)

Attribute often referenced by software applications. Matches **samAccountname**.

AD Attribute Name: **cn**
Max Length: 256
Example: “doej”

2.2.1.21 Middle Name

Common or preferred middle name(s) of person. May contain spaces, hyphens, and apostrophes.

AD Attribute Name: **middleName**
Max Length: 64
Example(s): (as for **givenName**, above)

2.2.1.22 Generation Qualifier

Generation qualifier of person, if any, without periods.

AD Attribute Name: **generationQualifier**
Max Length: 64
Examples: “Sr” “Jr” “III”

2.2.1.23 Fax Telephone Number

Business facsimile (fax) number with area code or country and local area codes separated by periods. Extension if any noted by space x followed by extension number. 64 maximum characters.

AD Attribute Name: **facsimileTelephoneNumber**
Max Length: 64
Examples: “301.496.1235” “55.1.4966.1235”

2.2.1.24 Mobile Telephone Number

Business mobile/cellular telephone number with area code or country and local area codes separated by periods. Extension if any noted by space x followed by extension number. 64 maximum characters.

AD Attribute Name: **mobileTelephoneNumber**
Max Length: 64
Examples: “301.496.1236” “55.1.4966.1236”

2.2.1.25 Pager Number

Business pager telephone number with area code or country and local area codes separated by periods. Extension if any noted by space x followed by extension number. 64 maximum characters.

AD Attribute Name: **pagerTelephoneNumber**
Max Length: 64
Examples: “301.496.1237” “55.1.4966.1237”

2.2.2 Example of Account Using Data Content Rules

This is an example of an NIH AD User account entry:

givenName = James
sn = Doe
employeeID = 0010058023
employeeType = Contractor
company = NIH
department = CIT
physicalDeliveryOfficeName = CIT/DCSS/EMIB
sAMAccountName = DoeJW
userPrincipalName = doejw@nih.gov
mailNickname = doejw
proxyAddresses = doej@mail.nih.gov;
mail = doejw@mail.nih.gov
street = 12 SOUTH DR
msExchangeAssistantName = 12A/2025
roomNumber = 12A/2025
l = Bethesda
st = MD
co = US
countryCode = 840
postalCode = 20892-1234
telephoneNumber = 301.496.1234
displayName = Doe, James (NIH/CIT) [C]
cn = doejw

AD Account names should follow the NIH Appropriate Use Policy http://www3.od.nih.gov/oma/manualchapters/management/2806/, section C.1

2.3 AD Resource and Service Accounts Data Content Management Rules

An entry of this type represents resources or services that are used by persons, groups, or physical machines at NIH. A resource or service account is not a person and therefore does not map to a NED ID.

2.3.1 AD Resource/Service User Accounts

Resource accounts are named using the following formula: **sn** = **department** space "**name of resource account**" using 256 maximum characters, a-z, A-Z, and 0-9. No special characters are allowed.

displayName = **sn** space **(company/department)**

For all remaining attributes, use the AD data from the person requesting the Resource Account and fill in the information using the rules as above.

For resource accounts, fill in the following attributes:

sn, company, department, displayName, physicalDeliveryOfficeName

empoyeeNumber: add the word **RESOURCE.**

managedBy: set this to either person who "owns" the account or to a group with multiple members who can answer questions about the account.

Examples of resource accounts: "NHLBI Grants", "NLM ConfRoom", "OD Parking Space", "NIDCD backupexec", "NINDS SQLservice".

2.4 AD Secondary Accounts Data Content Management Rules

An entry of this type represents a secondary or administrative account for a person. This account represents a person and must map to an existing NED ID. AD Resource/Service User Accounts. Data Content definitions can be found in section 2.2 AD User Attribute Data Content Management.

Secondary accounts are created using the following formula:

givenName = first name
sn = last name
employeeID = NED ID
employeeType =
employeeNumber = Secondary
company =
department =
physicalDeliveryOfficeName =
sAMAccountName = aa + sAMAccountname of primary account
userPrincipalName = aa + sAMAccountname@nih.gov
street =
msExchangeAssistantName =
roomNumber =
l =
st =
co =
countryCode =
postalCode =
telephoneNumber =
displayName = AALast name + First name (NIH/Department) [employeeType]
cn = aa + sAMAccountname

2.5 AD User Account Uniqueness

No two AD Accounts in nih.gov shall be named the same (sAMAccount, CN, UPN, and proxy address) and the display name shall reflect this uniqueness. Uniqueness enables the use of the user objects across multiple directories and applications.

2.6 AD Account Audit Principle

All AD user and group object administration shall be audited. Any AD Account or group additions, modifications or deletions will be tracked, recorded and saved in a central repository. Access to audit information shall be made available to group administrators upon request.

3 Reserved AD User Attribute Data Content Principles and Best Practices

The following principles and associated best practices apply to all NIH Active Directory reserved object attributes.

3.1 Reserved AD User Attribute Principle

Active Directory has fifteen unassigned attributes available for use. These attributes are indexed and published in AD's Global Catalogs.

The following AD user Account attributes are reserved due to their use by NIH Enterprise applications (email, fax, archiving) and may not be overwritten or used by any other NIH application or technology.

3.2 Reserved AD User Account Attributes

otherFacsimileTelephoneNumber = used by Enterprise Fax solution

extensionAttribute5 = password self service registered

extensionAttribute7 = Blackberry PIN

extensionAttribute9 = mailboxMove data

extensionAttribute10 = free/busy

4 AD Computer Account Attribute Data Content Principles and Best Practices

The following principles and associated best practices apply to all NIH AD computer attributes.

4.1 AD Computer Account Principle

An Active Directory computer account represents a computer object (workstation, laptop, or server) at NIH. Each computer object needs to be unique and registered to a legal NIH person. The following guidelines are best community practices for creating computer account names.

4.1.1 Required AD Computer Attribute Data Content Management Rules

4.1.1.1 Computer Name

Computer names will have the IC prefix followed by a unique name. For example: "CIT12JoeD". 20 maximum characters. Data Content rules for naming: use characters a-z, A-Z, and 0-9 only, no special characters allowed.

These additional suggestions can be used to develop a unique computer account name:

- Select computer names that are easy for users to remember.
- Identify the owner of a computer in the computer name.
- Select names that describe the purpose of the computer.

NOTE: Where scientific equipment requires the name be hard-coded to the equipment and limited in length, the IC will not have to preface the name with the IC but will work with EMIB to ensure uniqueness.

4.1.1.2 Description

Computer description will be used for server location information.

4.1.1.3 Managed by

Computer Managed by will be used for servers and should note the appropriate person or group responsible for server operation.

5 AD Group Policy Objects Principles and Best Practices

5.1 AD Group Policy Objects Principle

Active Directory Group policy is a feature that provides centralized management and configuration of computers and users in an Active Directory environment.

5.1.1 Required AD Group Policy Objects Data Content Management Rules

5.1.1.1 Group Policy

Group Policies will have the IC prefix followed by a unique name. For example: "CIT Vista Standards". Data content rules for naming: use characters a-z, A-Z, and 0-9 only, no special characters allowed.

6 AD Object Location Management Principle

6.1 AD Object Location Management Principle

In order to facilitate a greater degree of manageability in the creation, identification, and management of AD attributes, the location of AD objects needs to be in a consistent, programmable location. IC technical staff can manipulate and move the AD data objects following their business practices or technical design but the location of those objects shall be under the Organizational Unit (OU) specified. For example, instead of a single "Users" OU under the IC OU, an IC can create OUs (such as "Admin", "Grants", "Budget") that match their organizational structure, for example "CIT Admin", but there must be a Users OU under that level to hold all AD User objects. The AD object location management BCP will provide a framework to enable NIH application owners to better utilize AD attributes for programming and lookups.

6.1.1 AD Object Location Rules

AD User objects: Within AD, the AD user objects are located under an Organization Unit (OU) titled "Users".

AD Computer objects: Within AD, the computer objects are located under an OU titled "Computers".

AD Resource/Service User Accounts: Within AD, the resource accounts are located under an OU titled "OPS" then any OU but ending finally in "Users". (For example: "CIT, OPS, Admin Accounts, Users")

AD Contact objects: Within AD, the AD Contact objects are located under an OU titled "Contacts".

AD Group objects: Within AD, the AD group objects are located under an OU titled "Groups".

AD Distribution List objects: Within AD, the AD distribution list objects are located under an OU titled "Distribution Lists".

AD non-NIH User objects: These are non-NIH accounts that are mail enabled or enabled for VPN. All other non-NIH user objects are located within the NIH External Directory (NED). Non-NIH user objects are located in an OU titled "External".

7 References Section

7.1 NIH Resources

NIH Password Policy

http://cit.nih.gov/ITPolicies

NIH Account Policy

http://cit.nih.gov/ITPolicies

NIH Active Directory Data Standards

outlook:\\Public Folders\All Public Folders\NIH Wide\NIH AD\NIH AD Documents

NIH Active Directory Infrastructure Standards

outlook:\\Public Folders\All Public Folders\NIH Wide\NIH AD\NIH AD Documents

NIH RFC Formatting Standards

https://my.nih.gov/nih/communities/community.asp?UserID=1302641&CommunityID=307&intCurrentPageIndex=0

List of NIH IC

http://www.nih.gov/icd/

NIHRFC002 Person Name standard

http://enterprisearchitecture.nih.gov/ArchLib/AT/IA/Data/NIHRFC0002.htm

7.2 Useful Websites

University of Michigan Network Directory Standards for Novell
http://www.umich.edu/~lannos/novell/standards.html

University of Michigan Network Directory Standards for Microsoft
http://www.umich.edu/~lannos/windows/w2k-namingstandards.html

Microsoft's Technical Article on Users and Groups
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/maintain/adusers.asp

8 Contact

To contact the BCP Editor, send an email message to EnterpriseArchitecture@mail.nih.gov

9 Changes

Version	Date	Change	Authority	Author of Change
0.01	June 2006	Original document	N/A	Valerie Wampler
0.02	October 2007	Added Computer, Resource accounts		Valerie Wampler
0.02	October 2007	Sent to ITMC I&O subcomittee		
.03	November 7, 2007	Edited to indicate fields that receive data via NED	Suggestion of EA team	Valerie Wampler
.04	December 27, 2007	2.1 edited and removed NIH resources, added one primary AD account per person and people are not Resource accounts	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	6.1 provided examples to clarify	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	4.1 added laptop to hardware types, description and managed by as requirements for servers, removed case note	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	5.1 made GPO separate principle	NIHRFC comments	Valerie Wampler
.04	December 27,	2.2.1 removed some	NIHRFC comments	Valerie Wampler

Version	Date	Change	Authority	Author of Change
	2007	data fields as not needed		
.04	December 27, 2007	2.2.2 removed as redundant. It is covered in NIH Account policy	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	2.3 updated	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	2.4 updated	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	2.1.1.20 removed NON-NIH	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	2.1.1.3 edited	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	2.1.1.23 removed	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	Updated header/footer	NIHRFC comments	Valerie Wampler
.04	December 27, 2007	Removed NED/AD flow	NIHRFC comments	Valerie Wampler
1.1	January 4, 2008	English and formatting changes	Valerie Wampler	Katherine Matthews
1.2	January 30, 2008	Added 2.4 Secondary Accounts	Valerie Wampler	Valerie Wampler
1.3	February 1, 2008	Updated header and date	NIHRFC0001	Steve Thornton, NIHRFC Editor

10 Author's Address

Valerie Wampler
NIH/DCSS/CIT/EMIB
301-402-7169
wamplerv@mail.nih.gov