Active Directory at the University of Michigan

The Michigan Way
Since 2000
Introductions

• Who I am: Christina Fleming (cmhf)
• Who you are:
  • Your Name
  • Your Department
  • How long have you worked with AD?
  • What is your Department is doing with AD?
  • What would you like to get out of this learning?
What is the Michigan Way?

- 19 Schools and Colleges with the same football team.
- Administrators want control over their own IT resources.
- We are smarter than everyone else so we should do it differently.
- 8th layer of the OSI model – Politics.
What’s in a Name?

- What is the DNS name of the Active Directory Forest?
  - adsroot.itcs.umich.edu
- Why?
  - 8th layer of the OSI model – Politics.
- Why not umich.edu?
  - Already an MIT Kerberos realm with that name.
- Why not ad.umich.edu?
  - No services allowed at DNS root – Politics. This decision has since been reversed.
- What is the NetBIOS name of the Forest?
  - UMROOT
UMROOT Design

- KERBEROS
  - umich.edu
- LIMROOT
  - adsroot.itcs.umich.edu
  - mpathways.umich.edu
  - bf.umich.edu
  - ENGIn
    - ad.engin.umich.edu
  - HOUSING
    - housing.adsroot.itcs.umich.edu
  - LSA
    - lsa.adsroot.itcs.umich.edu
- UMICHe
  - ads.itcs.umich.edu
- BUS
  - bus.ads.itcs.umich.edu
- DPS
- MCIT
- ISR
AD Stats (as of July 2010)

- Participating U-M units: 165
- Representation from all 20 of the Schools and Colleges, University Libraries, numerous business units and institutes on the Ann Arbor central campus in addition to the Schools and Colleges from U-M Dearborn
- Unique logons per month: 63,380 (high water mark)
- Total Centrally Managed Users: 413,252

![Growth of the UMRoot Forest](chart.png)
AD Stats (as of July 2010)

- Exchange Mailboxes: 16,968 (11,652 standard mailboxes, 5,316 voice mailboxes)
AD Stats (as of July 2010)

- Birthday: July 7, 2000, 10:11 pm
- Total Objects in the directory: 512,006
- Unit managed centrally created users (Accounts OU): 9796
- Unit Created Users (Orgs OU): 6,140
- Groups: 16,042
- Organizational Units: 4,815
- Group Policies: 3,389
- Workstations: 23172 (57% XP, 22% Vista, 10% Windows 7, < 1% Mac and Linux)
- Servers: 989 (54% Server 2003, 33% Server 2008, 12% Server 2008 R2)
- Sample of Applications Managed through AD: VaaS, Exchange, Sharepoint, OCS, Shared Desktop Image, VDI, Mainstream Storage, CPPM, Campus Computing Sites
UMROOT Domain
Active Directory Users and Computers
People OU

• Real time and daily feed from UMOD to People OU.

• UMOD feed includes all U-M Faculty, Staff, Students, Alumni, etc.

• Only ITCS Admins can administer People OU. This limits the usefulness of these accounts.

UMROOT
adsroot.itcs.umich.edu

UMOD Feed
300K users
Pass-thru Authentication

- One way trust between UMROOT and UMICH.EDU Kerberos Realm.

- Uniqnames in both UMROOT and UMICH.EDU Kerberos.

- User can log on to UMROOT workstation with UMICH.EDU Kerberos credentials instead of UMROOT credentials.

- User receives Kerberos tickets to both UMROOT and UMICH.EDU Kerberos realm.
Pass-thru Authentication

• This is used mostly for CampusComputing Sites logons, but some other units are using it.

• Requires special registry key to be set on domain joined workstations.
• Each department/unit has their own fully delegated Organizations OU.

• Any type of object can be created, users, groups, computers, etc.

• Naming convention requires a department prefix, i.e. dept-user1, dept-computer1, etc.

• Uniqnames **cannot** be used without department prefix (dept-uniqname) or number (uniqname1)
• Each department/unit has their Accounts OU at the same level as the Organizations OU with the same department structure.

• Uniqname users can be moved from the People OU to their departmental/unit Accounts OU where they can be administered by department.

• Moves done by department/unit using a web application called “Windows Central Accounts”
https://umwinca.adsroot.itcs.umich.edu
• Permissions in Accounts OU are less than the full permissions granted in the Organizations OU. Cannot disable accounts, change logon names, restrict workstation or hours, etc.
• Ownership of uniqname accounts is determined by Affiliation data from UMOD.
Why Manage Users in Accounts OU?

- **Exchange**: You want to create your own Exchange mailboxes (Self Serve Exchange)
- **Passwords**: You want to be able to have OU Admins reset passwords for your users.
- **User Attributes**: You want to set other User Attributes for the user.
Why Not Manage Users in Accounts OU?

You do not always need to move users to your Accounts OU:

- **Passwords**: Passwords can be changed by the user at: https://accounts.itcs.umich.edu/password/
- **Home Directories**: Home Drives can be mapped in Logon Scripts.
- **User Attributes**: Most are unnecessary or you don’t have permission to write to them.
- **Group Policy**: Group Policy can be applied to the user with Loopback – more on this later.
- **Groups**: Any user in Active Directory can be added to a group that you create in your Organizations OU and assign permissions to.
Multiple Affiliation Problem

- A user you want to manage may already be managed by another department and was moved to their Accounts OU.
- You can contact that department that is currently managing the user and see if they still need to. If not, they can release the user to the People OU and then you can move it.
- You can choose to leave the user in the current department and have an agreement that the current department will make changes you request.
- If none of the above resolve the problem, we let the user decide who they want managing their user account.
User Attributes
Writable Reserved Attributes

- Department
- DisplayName
- Exchange General, Features, and Advanced tabs
- Email addresses tab
- extensionAttributeX
- Mail
Writable Unrestricted Attributes

- Office
- Address information
- Profile Path
- homeDrive and homeDirectory
- Mobile and IP Phone
- Notes
- Direct Reports
- Manager

- Member of
- Dial-n tab
- Environment tab
- Sessions tab
- Remote Control tab
- Terminal Services Profile tab
Write Protected Attributes

- Live Communications tab
- userPrincipalName
- sAMAccountName
- userAccountControl
- Description
- accountExpires
- userWorkstations
- logonHours
- scriptPath
- Cn
- givenName
- Initials
- Sn

- telephoneNumber
- otherTelephone
- Web Information
- homePhone
- Telephones
- otherHomePhone
- Pager
- otherPager
- facsimileTelephoneNumber
- OtherFacsimileTelephoneNumber
- Company
- altSecurityIdentit
User Attributes
User Attributes (cont’d)
User Attributes (cont’d)
User Attributes (cont’d)
User Attributes (cont’d)
User Attributes (cont’d)
Windows Central Accounts
Web Application
Move Users

- You must be logged on as a department OU Admin, bfly-ouadmin1, to use the Move Users application.
- You must add Affiliations for your department.
- Use the Exception procedure if the user you want to manage does not have the proper affiliations.
- Only move users if necessary to manage specific attributes.
- Passwords can be changed by the user at: https://accounts.itcs.umich.edu/password/
- Any user in Active Directory can be added to a group that you create in your Organizations OU and assign permissions to.
- Group Policy can be applied to the user with Loopback – more on this later.
Windows Central Accounts Home Page
https://umwinca.adsroot.itcs.umich.edu/

University of Michigan
Windows Central Accounts

Users

- Consent for Alternate Windows Administration (U-M CoSign authentication)
  This consent form is required for individuals who are not formally affiliated with a specified U-M department or organizational unit, but nevertheless wish that department or organizational unit to administer their U-M Windows computer and account.

- User FAQ and Documentation
  This document provides some background for users of the U-M Windows Central Accounts service.

Administrators

- Request New Delegated OU (U-M CoSign authentication) ... Under Construction
  Prospective Windows delegated OU administrators may request that a new delegated OU be provisioned for their department or organizational unit by filling out the form on this web page.

- Move Users to/from Delegated OU
  An delegated OU administrator may use this web page to move users from the People OU to their delegated OU, or from their delegated OU back to the People OU. Only users who are properly affiliated with the department of the delegated OU may be moved.

- Manage OU Profile
  Delegated OU administrators may use this web page to manage certain properties of their OU.

- Administrator FAQ and Documentation
  This document provides some background for Windows administrators participating in the U-M Windows Central Accounts environment.
Move Users to-from Delegated OU

- Using FSPP as an example.
- Logon as fspp-ouadmin
- Application opens to FSPP Delegated OU.
- Affiliations for FSPP are populated.
- Click on the **Help** button for full documentation.
Move Users to-from Delegated OU

- Type in your email address.
- Add a list of users to Users to Move.
- Click Add Users to Move.
- You can also supply a text file with a list of names.
Move Users to-from Delegated OU

- Names are processed and results are listed.
- All users except mickeymouse were found in AD.
- Check the box next to mickeymouse and click **Remove Checked**.
- Click **Test Move** button.
Move Users to-from Delegated OU

• View the results.
• **nbrack** passed the test and can be moved.
• **ronl** failed because he had already been moved to another OU.
• **tweil** failed because the affiliations don’t match.
• **winweil** has been flagged as a new user without affiliations yet. We allow these new users to be moved.

• Click **Return to Move Users page**.
Move Users to-from Delegated OU

- Table is filled out with names and comments that match results from previous screen.
- winweil and nbrack can be successfully moved.
- ronl cannot be moved because the user is no longer in the People OU. (moved to LSA Physics)
- Select ronl and click Remove checked. We will not process this user.
Requesting an Exception

• For **tweil**, we will request an exception and ask the user for permission.
• Check the box for **tweil**.
• Click **Request Exception**.
Requesting an Exception

- **tweil** has been removed from the list.
- A message indicates the move is pending approval from the user.
Requesting an Exception

- The following email was sent to **tweil** asking permission to allow the user to be moved.
- The user needs to click on the link in the email

---

**Email Content:**

Dear Windows user,

A U-M Windows administrator who is responsible for the administration of the 'FSPP' organizational unit (OU) has requested that your U-M Windows account, 'tweil', be moved to the FSPP OU. This type of request is typically made to improve service to U-M users that are working in, or affiliated with, a U-M department.

Our current records from the U-M Directory indicate that you are not officially affiliated with the 'Ford School of Public Policy' organization. In this case, we need your specific approval to move your Windows account to the FSPP OU. Agreeing to this request will allow the requesting department to manage Windows password changes and other settings for your account that are used on campus Windows networks. Please contact your administrator at , or w2ksupport@umich.edu for further information.

You can accept the request for Alternate Windows Administration by visiting the following web page, and entering the 'I Accept' button. You will be prompted to enter your U-M uniqname and password to identify yourself before the Alternate Windows Administration web page appears.

[https://umprox.adpoint.litcs.umich.edu/w1nc1sent/w1nc1sent.aspx](https://umprox.adpoint.litcs.umich.edu/w1nc1sent/w1nc1sent.aspx)

Sincerely,
The U-M Windows Central Accounts team
Requesting an Exception

- The user needs to authenticate with their U-M Kerberos credentials.
- When the user clicks the I Agree button, the user is moved to the FSPP OU.
Requesting an Exception

- The user will receive a confirmation that the user account has been moved.

U-M Windows Central Accounts

Request Approved and Move Completed

Your request to for Alternate Windows Administration has been approved, and your "test" Windows account has been moved to the "FSUP" Organizational Unit (OU).

To exit, either close your browser, or press the link below to return to the U-M Windows Central Accounts home page.

Return to U-M Windows Central Accounts home page
Move Users to-from Delegated OU

- For the remaining users, click **Move Users**.
Move Users to-from Delegated OU

- You will receive a confirmation that the users were moved.
- Click on link to return to menu. Do not click browser back button.
Move Users to-from Delegated OU

- Check AD Users and Computers and you will see the users have been moved including the exception user.
Group Policy
Group Policy

- Group Policies from Active Directory are applied to users and computers that are logged into the domain.
- Download and use the Group Policy Management Console.
- Multiple Group Policies are applied first from the Local Policy, then from the Domain, and then from each OU in the path to the objects.
- In the case of conflicting Group Policies, the last one applied wins.
- The only exception to this is if a Group Policy has been marked as Mandatory.
UMROOT Domain Policies

- There are two Group Policies at the UMROOT domain level.
- The UMROOT Override Domain Policy is applied to all computers in the domain. It has settings we think are useful to everyone, but can be overridden by departments.
- To override a Group Policy, just create another one at a lower level in the OU Structure.
- The UMROOT Mandatory Domain Policy is also applied to all computers in the domain. It contains a small number of very important security settings and can’t be overridden.
There are several policies that restrict certain services from running on computers. Because of past security issues with Code Red, SQL Slammer, etc., IIS, SQL and the Messenger services are set to Disabled. If you want to run one of these services, create a Group Policy that allows these services. You can also link to one of the following centrally managed Group Policies: UMROOT Allow IIS Service Policy UMROOT Allow SQL Server Service Policy Be aware that without an Allow policy, services will start but will be shut down automatically at reboot.
User and Computer Group Policies

- Group Policies contain 2 parts, one part is applied to the user who logs on, the other is applied to the computer they log on from.
- If the user is in a different OU than the computer, a likely situation, 2 different Group Policies will be applied to the user/computer.
- The **user** portion of the Group Policy for the OU the **user** is in will be applied to the **user**.
- The **computer** portion of the Group Policy for the OU the **computer** is in will be applied to the **computer**.
Regular Group Policy Application

- When **user1** logs onto **computer1**:
  - **GPO1-User** is applied to **user1**
  - **GPO2-Computer** is applied to **computer1**
Loopback Group Policies

- We recommend using **Loopback in Replace Mode** applied to the OU your computer is in, not the user’s OU. This is set in the Computer Group Policy.

- In Loopback-Replace Mode, the **user** portion of the Group Policy for the OU the **computer** is in is applied to the **user**.

- The **computer** portion of the Group Policy for the OU the **computer** is in will still be applied to the **computer**.

- This is a best practice because the user who logs onto your computer may not be in your Accounts OU, but you want to apply Group Policy to the user.
Setting Loopback Group Policies
Loopback Group Policy Application

- When **user1** logs onto **computer1**: 
  - **GPO2-User** is applied to **user1**
  - **GPO2-Computer** is applied to **computer1**

```
Dept OU
  Users OU
    user1
  Computers OU
    computer1

GPO1
  GPO1-User
  GPO1-Computer

GPO2
  GPO2-User
  GPO2-Computer
```
Test Your Group Policies

- Group Policies are a great way to shoot yourself in the foot and lock yourself out of a server or computer.
- Group Policies can be complicated and don’t always act the way you would expect.
- Create a Test sub-OU in your Organizations OU and test your policies here first.
- Better yet, try out your Group Policies in the Test Forest.
General OU Admin Information
Joining AD as a Delegated OU

- Fill out the form here.  
  http://www.itcs.umich.edu/windows-forest/
- Select **How To** from main menu
- Select **Joining the U-M Windows Forest as a Delegated OU**
- Choose to join the Test or Production Forest
- Choose the name of a bootstrap computer, the first computer you will join to AD. (Can be a temporary computer)
- Email the form to **windows.support@umich.edu**
- Orgs and Accounts OU will be assigned in addition to OU Admin accounts.
OU Admin Information

- Each department has several dept-ouadminX users that are members of the dept-ouadmins group.
- You can create additional user accounts in your Organizations OU and add them to your dept-ouadmins group.
- Typically admin accounts are created by appending a number to a uniqname, uniqname1.
- Members of the your dept-ouadmins group can reset passwords and reset account lockouts for other dept-ouadminX accounts. They can also add additional members to the group.
Firewall Issues

- Active Directory is only available from campus computers or from the Internet using a VPN client. [http://www.itcom.itcs.umich.edu/vpn/](http://www.itcom.itcs.umich.edu/vpn/)
- A limited number of ports have been temporarily left open to the Internet for convenience to users. These ports will be closed Summer 2009.
  - 636 (LDAP over SSL) and 3269 (Global Catalog over SSL) for use with Entourage directory access to Active Directory.
  - 53 (DNS) access to adsroot.itcs.umich.edu DNS zone.
Test Forest

• The Test Forest closely resembles the production forest. Please consider creating a test OU here and trying things out here before production.
  • Domain DNS: adsroot.itd.umich.edu
  • NetBIOS: ADSROOT
  • Central Accounts: http://umwinca.adsroot.itd.umich.edu
  • Users cannot reset their own passwords with password change web page. Move users to Accounts OU or request password change from window.support@umich.edu.
Windows Server Versions

- Windows 2003 R2 Supported
- Windows 2008 – Supported
- Windows 2008 R2 - Supported
Joining Computers and Servers to the Domain
Joining Computers and Servers to the Domain

- Unlike most other AD implementations, a computer object must be pre-created in your Organizations OU before you can join a computer to the domain.
- You must use the dept-computername naming convention.
- Change the user/group that can join the computer to the domain to dept-ouadmins.
Joining Computers and Servers to the Domain
Joining Computers and Servers to the Domain
Joining Computers and Servers to the Domain

- Add the computer to the domain from the System Properties/Computer Name/Change dialog box.
- Select Domain: adsroot.itcs.umich.edu
- Logon with a dept-ouadminX account
Joining Computers and Servers to the Domain

[Images of computer name change windows showing the process of changing computer names and member of domains.]
Other Services
Other Active Directory Services

- Exchange mailboxes - $5/month
- Live and Office Communication Server
- KMS, key management server
- WINS servers
- DNS servers
- DFS
- Time Servers for domain
- DHCP Servers – departmental servers need to be authorized
- WSUS servers maintained by LSA & Library
Other LANNOS Services

• Connected Backup for workstations (PC and MAC) - $
• CIFS File Storage Pilot - $
Resources
Resources - Web

- LANNOS Web Site:
  http://www.itcs.umich.edu/windows-forest/
- Select How To section
  Getting Started with Active Directory Section
    - Joining the U-M Windows Forest as a Delegated OU
    - Installing Windows Server 2003
    - Setting up your Active Directory Environment
    - Logon Script Basics
    - Active Directory Users, Groups and OUs
    - Windows File Sharing
Resources - Support

- Contact LANNOS Admins
  windows.support@umich.edu
- Contact Campus Admins - Free
  win2000@listserver.itd.umich.edu
  Quarterly Windows Admin Meeting
- Windows Hi-Ed List – Free
  windows-hied@mailman.stanford.edu
- Contact Microsoft - $
  msamembers listserv
  $1500
Resources - Tools

- Move Users Web Site
  http://umwinca.adsroot.itcs.umich.edu

- Password Change Web Page:
  https://accounts.itcs.umich.edu/kpasswd/
Resources - References

- Safari Books Online via www.lib.umich.edu
- Mastering Windows Server 2003 – Mark Minasi
- Inside Windows Server 2003 – Bill Boswell
- Group Policy – Jeremy Moskowitz