Managing Workstations
In an Active Directory Environment at PCC

This document provides information about the implications of implementing Active Directory (AD) on the workstation management functions within TSS. The focus of this information is on the end-user impact as well as the impact to TSS staff responsible for managing workstations.

This is not a technical document or a list of project requirements. Instead, it is a visioning tool to illustrate how things will be different when AD is implemented and the various transitions that we will need to manage throughout the process.

Most of the information presented here was collected from other higher education institutions that have already implemented AD.
## Contents

Overview .................................................................................................................. 3  
User and Workstation Information Synthesized by AD ................................. 4  
Project Structure .................................................................................................. 6  
Active Directory Structure and Workstation Management ............................ 7  
Documentation for OUs and GPs ......................................................................... 9  
Roles and Responsibilities ..................................................................................... 10  
Naming Standards and Governance .................................................................. 11  
Workstation Management Process Changes and New Functionality ............ 12  
Changing Roles for TSS Staff ............................................................................... 13  
Training ............................................................................................................... 15  
Recommendations ............................................................................................... 16
Overview

PCC is currently working on an Active Directory implementation project. The AD project has a wide scope and several associated initiatives. This document specifically pertains to the workstation management piece of the overall AD program. It is also limited to PCC-owned workstations. AD will make it much easier for people to use their own personal computer on our network (domain) but those considerations are not addressed in this document. A subsequent effort will be launched to develop those requirements.

This document also does not cover any of the setup of the data in AD. It assumes that accounts have already been provisioned and that appropriate privileges and system access capabilities have been assigned to users. There is also an assumption that integration processes have been established and the LDAP repository in AD is fully populated and accessible for workstation management purposes.

There are several benefits typically associated with doing an AD project such as centralized management of devices, increased security and data protection, and efficient account management. The California Institute of Technology developed a definition of AD that works well for our environment. “AD is a network directory that provides a single, logical and consistent database in which to store information about the network and all network-based resources.” Perhaps the best way to articulate the benefit of using AD for workstation management is by looking at what we will be able to do when it is implemented.

Benefit Statement

With AD in place, we will be able to synthesize all of the information we have about the workstation with everything we know about the user. We can then use this set of information to provide the most appropriate system access, software, and services for the user.
User and Workstation Information Synthesized by AD

We currently have a lot of information about the workstations in our asset management system. This includes all relevant hardware and software data. Other current systems also have a lot of information about our users including their role, location, department/division, etc. One of our current limitations to efficient workstation management is that we do not have a single authoritative source for both the hardware and user information. Once AD is implemented we will no longer have this limitation.

Here are a couple of examples of using user and machine information together to more effectively manage workstations.

Example 1: We currently use Go-Print to charge students for printing in the CRC. However, Go-Print is attached to the workstation regardless of the user role. If a staff member logs onto a CRC workstation and tries to print a document then they will be presented with the Go-Print charge screen. When AD is implemented, an associated policy will be in place to identify the user as either a student or staff member. When a print request is made from that same CRC workstation, AD will administer the policy requiring payment for printing to the student but not the staff member even though they use the same workstation.

Example 2: We currently maintain a local administrator account on each workstation for maintenance and support. It is typical that a single shared password is used for that local administrator account on numerous workstations. Technicians rely on that account being the same on different computers they manage in order to automate workstation management tasks from all our existing workstation management tools (KBOX, Ghost, Deep Freeze, Sophos). In order to make and keep that account the same they must rely on manual configuration or workstation imaging and there is no telling which technician has done what on any given workstation using that account. When AD is implemented there will be no need to synchronize local administrator accounts – technicians will manage workstations with their own uniquely assigned domain user accounts. This will not only eliminate the overhead of managing local administrator accounts, but will also generate a centralized enterprise-wide audit trail of workstation administration actions that will enhance support team communications and information security.

Example 3: Currently users (student, staff, faculty, TSS Tech) log on to workstations with administrator accounts, with few exceptions. This is due to the need to permit users to customize their computing environment on workstations that know nothing of who they are or what they need. When AD is implemented we can configure workstations upon logon based on user roles, thereby eliminating the need for them to have administrator level access. The issue of legacy software that requires administrator access to run can be addressed using a combination of off-the-shelf software or software-as-a-service that identifies all such software on the network, and PCC’s asset management system that can deploy software based on the AD role of the user logging in.

Example 4: Every year we replace a large number of workstations for staff and faculty. It is a challenge to identify all of the workstations for a specific department/division and associate each workstation to the corresponding user. In the AD environment our workstation
replacement planning will be greatly simplified. Consistent logon procedures will allow us to associate the user with the corresponding workstation. Departmental workstation replacement planning will be very straightforward because each department/division will already be set up in AD.

A full set of use cases will be developed to cover TSS tech staff and user processing needs. These use cases will become the elements of the overall test plan. Several features can be utilized in AD that leverage the synthesis of user and workstation information. The Alabama Cooperative Extension System supported by Auburn University and Alabama A & M came up with a great list.

1. Authentication based on standard username (user information)
   - Requiring username and password for login to any workstation
   - Allowing users the flexibility of logging into any PCC machine securely
   - Ability to restrict access to machines by certain users

2. Structured policy settings (rules) to be used for workstation management (workstation information)
   - Automating Windows updates and other patches
   - Setting and locking security configurations
   - Making software available via "Add/Remove Programs"
   - Automatically mapping network drives
   - Providing granular management of sub-groups, such as labs and workgroups

3. Easier Printer Sharing.
   - Printers appear automatically under "Printers and Faxes tab."
   - Ability to print to any printer within the domain no matter the physical location

These are just some of the benefits that we will realize under AD. The complete list of workstation management capabilities that AD will provide is extensive and will grow over time. Some of these capabilities will replace our existing processes and others will be new to us.
Project Structure

The project for managing workstations in an AD environment will be in four phases. Each phase is planned for 6 months. There will be a brief overlap of one month between phases to provide a smooth transition and continuity between phases. The phases are:

1) AD Technical Infrastructure Implementation,
2) AD Services and Features Configuration and Standards,
3) AD Workstation Management Pilot,
4) AD Workstation Management Production.

A different team will lead each phase. Phase 1 is led by Server Administration. Phase 2 is led by Solution Services. Phase 3 is led by the Campus Teams. Phase 4 will be a rollout to non-TSS staff for delegated workstation management tasks. Once in production, ongoing management and administration of the AD services and features will be done centrally by Solution Services.

The Workstation Management in an AD Environment project is a sub-project of the overall AD initiative. This structure will require a high degree of coordination, communication, and collaboration with the other AD related projects. The overall project team will include all areas of TSS, vendors and consultants, users, and trainers.
Active Directory Structure and Workstation Management

There is a vast amount of documentation and literature related to AD. A brief explanation of the structure and architecture of AD is helpful in understanding the changes to workstation management that will occur. AD has a hierarchical structure. According to Wikipedia, “The forest, tree, and domain are the logical divisions in an Active Directory network.” Within each domain are Organizational Units (OU). Outside of the OU structure are Groups that contain a set of user accounts. Each group is controlled by one or more Group Policies (GPs). An example of the structure for a higher education institution was developed by UIC.

In an AD environment, users are typically assigned to one or more groups. Rules controlling system access and privileges, GPs, are applied to groups as opposed to individual users. For example, a group policy could be established that requires user passwords to be changed every month. That group policy could then be assigned to all TSS Staff members.

AD is a hierarchical system and GPs are applied in a hierarchical manner with higher-level GPs overriding lower-level policy settings. The example of requiring TSS password changes every month can be used to illustrate the operation of the hierarchy of GPs. For example, a policy could be set at the campus level requiring passwords to be changed every 6 months for all staff members on the campus. The district-wide setting for monthly TSS password changes would override the local campus policy but only applied to TSS staff on that campus.

For the most part, the Domain will contain a structure of OUs that will be pretty close to our existing Organizational Charts for Administrative Departments and Academic Programs. All users will be a member of one or more groups. The services, software, and access for the users will be controlled by rules setup in the group policies. The architecture for the Domain and OUs will likely be set by the larger AD project managed by Server Administration and verified by the
Workstation Management in an AD Environment sub-project. This is a critical step in the project design phase and has to be vetted across all of the sub-projects and stakeholders.

Documentation for the structure of our AD environment is an important deliverable from the early phases of the project. This will set the blueprint for service delivery, delegated authority, and policy implementation. A great model depicting the AD structure was produced by the team from The California Institute of Technology.

**Figure 2** - The hierarchical structure of Active Directory allows for easy delegation of authority, and application of administrative and security policies (Group Policies).

![Diagram of Active Directory structure](image)

This model depicts a single domain AD architecture. Although there is an ability to utilize a structure with multiple domains, this document uses the simple example of a single domain structure. Once the PCC structure is defined we can update the assumptions and modify the AD requirements for workstation management.

The information technology team at Rutgers University has a good suggestion for technology teams. “For other Microsoft recommendations on best practices and setting up AD, take a look at Best Practice Active Directory Design for Managing Windows Networks from Microsoft.”
Documentation for OUs and GPs

The team responsible for workstation management will need to have a complete view into the OU and Group Policy information within AD. This is mentioned by the University of Memphis in their design. “Group Policy is a capability available to AD administrators who need to control the client user experience based upon AD site, domain, OU or group affiliation.”

One of the benefits of AD is the ability to appropriately delegate OU and GP administration to TSS and non-TSS staff. This will be beneficial to the workstation management teams and alleviate any reliance on the central AD support team. GP and OU changes are managed centrally and documented for reference by all stakeholders.

The most important things for the workstation management team are:

1) to have a process for requesting GPs and a template for documenting the requirements needed in a GP,
2) a way to see all of the production GPs in place,
3) a way to see the OU structure, and
4) a process for being notified of changes to OUs.

The need for access to the OU and GP information for the workstation management team is mentioned by Information Services and Technology team from MIT. “GPs can be applied to either users or computers. GPs are applied hierarchically from the least restrictive group to the most restrictive group and are cumulative. GPs for both computer configuration settings and user configuration settings include software settings, Windows settings, and administrative templates.”

In order for the workstation management team to understand what is happening in a user session or predict what will happen, they will need full access to GP and OU documentation. Part of the overall AD project will fully define roles and responsibilities and document which team is ultimately responsible for creating, modifying, and deleting OUs and GPs. During the project implementation phase this will be done by Solution Services.
Roles and Responsibilities

Several teams will need to work together to manage the AD platform. Individual roles based on AD best practices will be defined within each of the teams.

The technical infrastructure will be managed by Domain Administrators on the Server Administration team. The features and services as well as standards will be managed by System Administrators on the Solution Services team. The workstation management for departments and divisions will be done by Organizational Unit Administrators on the Campus Teams.

Domain Administrators will have privileges for all of the roles. System Administrators will have privileges for feature and services management and also all of the authority of the Organizational Unit Administrators. The Organizational Unit Administrators will have privileges for their corresponding OU.

OUs can be embedded in a hierarchy to allow for full functionality by TSS. An example is that an OU may be created for a campus, i.e. RC-OU for Rock Creek, and additional OUs for each department/division at Rock Creek, i.e. RC-MMT, RC-Library, RC-Pavtec. Administrator rights in the RC-OU would be granted to TSS Staff and would allow them to manage any of the embedded OUs. Local department administrators would only have access to their own OU. This structure will allow for centralized management of the overall AD platform by Server Administration and Solution Services and also autonomy on the Campus Teams for their own OUs.
Naming Standards and Governance

The best way to leverage all of the benefit available from the AD architecture is to embrace strict adherence to naming standards and procedures. Naming standards will be established for users, OUs, GPs, workstations, servers, groups, printers, etc. Solution Services will define and document these standards and provide training materials for TSS staff. It is a common best practice in AD environments to produce standard reports identifying components that do not comply with naming standards. These reports are distributed to TSS staff and worked on a daily basis so that components can be appropriately named.

Standard procedures for requesting changes, change management, issue resolution, and system documentation will also need to be in place. Ongoing team meetings will need to be established as part of the production implementation. This group will provide the oversight and governance to the system once the project is done. They will establish change management procedures for changes to AD components. This group will also be responsible for getting information from Server Administration about any updates planned by Domain Admins to the system. Additionally, this team will need to produce updates and status reports to other TSS teams and users related to system changes and plans.

A simple comprehensive communication plan will be developed to plan and track the flow of information.
Workstation Management Process Changes and New Functionality

The AD platform will allow us to change many of the processes related to workstation management. Some of the areas that will change the most are with patches and updates, new machine deployment, and software provisioning.

Windows updates and software patches will be distributed and managed by AD. We will be able to insure that all staff and faculty machines do not have updates and patches disabled. This will also be very beneficial because we will not need to fully re-image classrooms and labs in order to apply updates. With this model in place, our concept of “imaging” which clones hard drives and pushes them across the network will radically change.

In the new process, “images” will actually just be long lists of software that the user or workstation should have. These lists will be used by AD and KBox to deliver the software payload from the nearest storage location. New machine deployment will be greatly automated. The only manual step in the process will be for TSS staff (or delegates) to assign a new machine to a domain in the system deployment console. Once that is done the machine will get a bare metal install of Windows, be joined to the assigned domain, and appropriate Group Policy will initiate the software load to provision packages via the KBox. If necessary, the information from the user’s old machine will be automatically loaded to the new workstation. AD will also control and manage loading new software onto existing workstations. A change will be made to the group policy, or perhaps the OU, and this will trigger the software installation.

In all cases we will have a log of all steps and events that impacted a workstation. This provides a nicely documented audit trail and also the ability to follow-up on any workstation management tasks that did not successfully complete. The logging feature in AD can provide a comprehensive history of all management actions applied to the workstation over the lifecycle from initial deployment through end-of-life.

These are new, efficient ways of doing functions that we currently accomplish with legacy tools and techniques. The new platform will also give us new functionality that we have not had in the past. We will be able to control where user documents are saved through policy settings. This would allow us to move the default “save” location for My Documents to network storage without having to touch the workstation. User data backups will be greatly simplified. Our security capabilities will also be greatly increased in AD. We will also have the opportunity to effectively apply very granular policies and restrictions to workstations based on the user and workstation information.
Changing Roles for TSS Staff

Implementing AD will cause many of the roles related to workstation management to change within TSS. There will also be some new TSS roles created.

TSS desktop support staff will move away from supporting physical devices on the campus. Their work will instead be focused on the AD layer of Group Policies and OUs to support devices.

Software will not be directly loaded on individual machines or built into cloned images. Under AD, software will be packaged and stored in a repository and the commands for loading it managed through policy updates in AD. More time will be focused on correcting errors related to improperly named components, unassigned machines, patching and update failures, and hardware issues.

New roles will also need to be developed for system administration and documentation. There will also be a new role for some staff as they are delegated basic OU administration responsibilities. This will be especially important for the centers (Willow Creek, Newberg, CLIMB, Downtown Center, Metro, Coffee Creek, etc.) that have little or no on-site TSS support.

There are several interesting job descriptions available that illustrate the skills and responsibilities necessary to support AD. Here is one example from a popular internet job site.

SUMMARY:
The Active Directory Analyst – leads the operation, maintenance and further improvement of a multi-site Microsoft Active Directory 2003/2008 cluster environment, supporting up to 15,000 end users. This position is a senior member of the team, with strong leadership and project management skills. This position requires extremely strong Active Directory administration skills.

RESPONSIBILITIES:
• Serves as Microsoft Active Directory technician, providing 3rd level support of Enterprise Microsoft Operating System-based servers
• Manages all Windows platforms providing authentication services for end users
• Monitors, evaluates and troubleshoots the existing Active Directory 2003/2008 implementation(s), developing and implementing solutions for evolution, enhancement, issue resolution and tuning
• Thorough knowledge of Active Directory, DNS, WINS, DHCP, Server 2003/2008, troubleshooting tools such as performance monitor
• Provides continuous support of Microsoft Active Directory and the servers and services that comprise the domain. Tests patches and updates Active Directory servers on an ongoing basis
• Documents standards for naming conventions, Group Policy management, and OU design. Manages GPs and OUs and produces standard operational reports.
• Assists in the development of project plans, implementation timelines, and deployment schedules relating to Active Directory initiatives
• Manages multiple and on-going projects, working closely with team members from various areas of the business
• Balances efforts of the Enterprise Computing team to include an appropriate level of day-to-day problem-solving versus long-term projects and solutions
• Adheres to strict change management policy to ensure timely notification, testing and approval for all system and application related changes that may impact the environment
• Adheres to problem management practices that focus on root cause analysis and prevention of future problems
• Mentors and trains other team members and effectively documents technical and operational procedures
• Works with the Service Desk to resolve user issues that have been escalated in a timely manner
• Pro-actively researches and suggest ways to improve the efficiency of the Operating Systems
• Works closely with members of the Information Technology department from other disciplines to design, maintain and improve systems that cross multiple platforms
We can see from this description that the responsibilities correspond nicely to our Server Administration and Solutions Services teams. Despite all of these role changes to existing staff and the emergence of new AD related roles, our overall staff size in TSS should not increase.
Training

We will need to have a robust training curriculum in order to develop the expertise to manage the system. There will be several different classes for Domain Admins, System Administrators, Support Staff and Technicians, Managers, and Users. This will be a sizable task and will require multiple approaches.

We will undoubtedly send some staff to intensive, week long, full-time training at a vendor location. There is a certification framework for AD skills and this will help us refine the standard curriculum to fit the needs of PCC. We will probably also host some on-site training conducted by a vendor consultant. We can plan for multiple sessions and get the majority of the technical staff trained.

Another full curriculum will have to be developed by our training team. This will be related to PCC standards, best practices, and procedures for working with our implementation of AD. Another session will be developed for users. In some cases we will have users performing delegated functions with the AD system. This would likely include the ability to add a workstation to the domain and perhaps password reset authority.

Training plans and documentation will be developed for all of these skill areas.
Recommendations

This will be an exciting and challenging project. Fortunately, many higher education institutions have already gone through an implementation and have excellent documentation available for us. The technology is mature and robust and will transform our service-delivery capability at PCC. The project will take a long time but there are some simple steps that we can take now to start things off. The list is long but here are just the top five considerations that we need to address.

1. Complete the pre-planning steps. This document is just a discussion piece to define the workstation management piece of AD. We need to create draft versions of the scope document, project plan, status report, training plan, and communication plan for workstation management.

2. Define the project structure. The past few system implementations at PCC have utilized a very effective model. Technical Services (Greg’s teams) builds up the infrastructure platform and establishes the necessary services. Solutions Services (Tammy’s teams) administers the application and completes the configuration. Full documentation, change management procedures, training plans, and communication procedures are developed related to the application. Once that phase is completed, the Stakeholders are given use of the system after it is moved into production. In the workstation management for AD project the stakeholders are primarily the campus teams and some super-users that will have delegated authority. This structure has worked very well for many recent projects including document imaging, Remedy replacement, call center rollout, asset management, and others.

3. Acknowledge that the toughest part of this project is strictly adhering to standards. It is very common for TSS support staff to make decisions and implement changes based on very localized needs. Our challenge will be to centrally manage the system and tightly enforce adherence to standards. Although this will result in a sizable loss of autonomy among the front-line staff, we must keep our focus on the strategic big-picture related to workstation management. We will be better off if we embrace that strategic approach in order to meet the service levels that will be expected of us. This is our best bet for effectively managing our growing number of workstations across an expanding set of locations without increasing our staff size.

4. Get the buy in of the Direct Reports group. In order for us to succeed there must be consensus by the leadership on the path forward. We have to execute this project very well and it will take the support and assistance of everybody in TSS. There is also a large component of the AD project that will impact Media Services and their requirements must be factored in as well. This can be a scope expansion to one of the other AD initiatives or a separate project.

5. Engage a consultant to add expertise to the workstation management for AD project. We have a talented group here in TSS but a little assistance would be great. They can help
us determine our approach, verify our architecture, develop roles and responsibilities, assist with the overall training plan, and get the initial configuration and procedures developed.

We should have no problem completing these steps. This will give us a very good idea of how to move forward. We can establish some milestones, add the project to the project review meetings, and get things started.

Please provide any feedback that you have related to this document to Michael Heuer, TSS Customer Support Manager, Michael.Heuer@pcc.edu.
References

University of Illinois – Chicago
Academic Computing and Communications Center – Active Directory Tech Pages
Managing AD Users and Computers
http://uicad.cc.uic.edu/tech/pctools/index.html

University of Minnesota
Office of Information Technology
UMN Active Directory
http://www.oit.umn.edu/prod/groups/oit/@pub/@oit/@web/@planning/documents/content/oit_conntent_029883.pdf

California Institute of Technology
Information Management Systems and Services
Active Directory FAQ
http://www.imss.caltech.edu/cms.php?op=wiki&wiki_op=view&id=412

The University of North Carolina – Greensboro
Information Technology Services
Active Directory Project Overview
http://its.uncg.edu/Projects/AD/Overview/

Alabama Cooperative Extension System
Alabama A & M and Auburn University
Technology Reference Desk
Active Directory Services
http://www.aces.edu/ctu/techref/networking/ADS.tmpl

North Carolina State University
NCSU Tech Staff Documents
Directory Service and Wolftech Active Directory
http://techies.ncsu.edu/wiki/Directory_service
http://www.wolftech.ncsu.edu/support/support/Active_Directory
Massachusetts Institute of Technology
Information Services and Technology
Windows Server Platforms: Introduction to Group Policy
http://ist.mit.edu/services/servers/windows/group_policy_intro

Georgia Institute of Technology
Office of Information Technology
Georgia Tech Active Directory Policy
http://web-archive.oit.gatech.edu/policies/issue_policies/ad_policy.cfm

Rutgers The State University of New Jersey
Office of Information Technology
Setting Up Active Directory at Rutgers
http://techdir.rutgers.edu/ad.html

Alaska Department of Administration
Enterprise Technology Services
Enterprise Active Directory Project
http://doa.alaska.gov/ets/msAD/