

# Provisioning and De-provisioning of Common Credentials and User Maintenance of Common Credential Attributes in a Higher Education setting

OHECC, 2009

**UNIVERSITY OF CINCINNATI**

2008

Authored by: Kevin L. McLaughlin & Quinn R. Shamblin

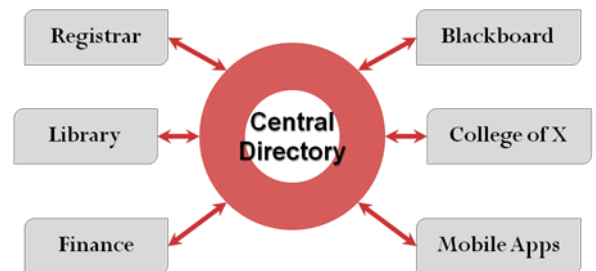
# Provisioning and De-provisioning of Common Credentials and User Maintenance of Common Credential Attributes in a Higher Education setting

OHECC, 2009

## Identity Management

Identity Management (IDM) helps bring order to chaos by centrally managing the identity life cycle

- Creation
  - Describes the identity by optionally assigns one or more attributes
- Auto provision, distribution, role assignment
- Management of identity attribute information by the user
  - Allows user to change one or more attributes
- Role-based access, re-assignment
- Deletion
- Auto de-provision



Addresses the tenacious “N+1” problem by encouraging the consolidation of directories

From an IT perspective, identity management focuses connecting systems together that provide an individual with the ability to make use of a service. This is a technical execution perspective and, as was shown in the presentation (the IT Identity management slide), the IT view can be confusing.

From a business and community member perspective, a person sees him- or herself as just one person who should therefore have a single organizational identity **No Matter How Many Systems He or She Uses!** When we get to the point where a person has only one identity in the organization, we are making use of *Common Credentials*.

In today's complex world, technology is used extensively to enable the ever-growing list of things that have become an integral part of our everyday lives: ID cards, credit cards, and Internet based services, to name a few. In all cases where a personalized service is involved, proof is required that you are who you portray yourself to be. Because services have evolved organically, originating from an unlimited number of sources, we find ourselves with hosts of unique user identities, usually amounting to one per person, per service that is used. To address the ever-growing concern over protecting one's personal identity from unauthorized use, and to improve the way we conduct business at the University of Cincinnati, we have started implementing a highly secure, centralized IDM system, as the authoritative source of information about

what systems and data a person is authorized to access. Our centralized IDM also reduces the number of unique credentials a person needs to conduct business using UC systems.

Typical IDM Functionality consists of both user and system features:

- The user can update personal information with self-service tools. He or she can also change or reset his or her password
- The system incorporates automation and workflow components that that improve the efficiency and accuracy of identity provisioning and deprovisioning

Prior to implementation of IDM at the University of Cincinnati, we had a chaotic hodgepodge of systems which required community members to manage multiple IDs, each with their own attributes, in order to use the systems.

- This was the heterogeneous result of almost 200 years of growth
- Central university functions: Registrar, Administration & Finance, UCit
- Sixteen (16) colleges, each with their own systems
- Hundreds of applications at all levels

Personnel at UC had different passwords for every application and had to manage each password manually. The project goal was to move UC to a world where a single identity is centrally managed and a single username and password will grant access to all applications to which the person is permitted access.

It took a great effort to coordinate efforts to bring all these diverse identities into an orderly whole that allowed a community member to use common credentials, and the attributes thereof, to access all UC systems.

An identity attribute is any field containing information about the user. Some attributes, such as current address, phone number, email address, and password, should be maintained by the user with provided tools. Other attributes, such as the roles to which a person is assigned and the access that he or she is permitted, must be controlled by the system and designated administrators.

### **UC IDM Project Milestones**

- Deploy one central repository of identity information that is designated as the authoritative source
- Create the “central directory” service
  - This is comprised of two directories:
    - LDAP (Novell Identity Vault) in which passwords expire, and
    - An Active Directory (Microsoft) in which passwords do not expire. This second directory is provided for systems that must have AD or do not support password expiration
  - The two directories are synchronized bi-directionally to ensure that the information in both is kept accurate and up-to-date in real time
- Synchronize all central IT application and system directories with the “central directory”. This includes systems such as Email, Blackboard, and Remote Access (VPN)
- Improve the security and quality of passwords in use at UC by requiring complex passwords.

- Synchronize distributed IT application and system directories with the “central directory”. If a college operates its own IT infrastructure, they may now use the central system for authentication, thus allowing their students to use the same password for their local systems as they do for their email, and to have that password update automatically on password change or reset
- Drive standardization of data needs and structures. Consolidate directories
- Implement single sign-on

## UC Password Complexity

Due to conflicting limitations in Novell Identity Vault and Microsoft Active Directory with respect to capabilities to define complex password requirements, UC finalized on these rules:

- Passwords must contain:
  - At least one lowercase letter
  - At least one uppercase letter
  - At least one number
- Must be a minimum length of eight characters
- May not contain an form of a person’s name or username

## Project Challenges

- Establishing Proper Communication Channels – By far the biggest challenge we faced was one of communication. The proper crafting of the message, the vehicles for message distribution and the timing of the messages were all factors in the successful communication of each new phase throughout the release process.
- Password Challenges
  - Novell Identity Vault and Microsoft Active Directory have different features. They have different limitations and requirements. If you implement “complex passwords” in AD, the requirements may be different than what can be achieved in Novell. Therefore, unless the password requirements are carefully chosen and the password changing tool carefully written, a user’s new password may be accepted by one and rejected by the other. This would result in the system not being able to keep in synch.
  - Software functionality limitations. Some software packages do not have facilities for warning of an upcoming password expiration date. If a user uses these packages exclusively and never logs into another system that can provide such a warning, the user may suddenly find him- or herself locked out of his or her software when the password expires. This issue often arises with mobile applications (i.e., those accessed via mobile phone). This issue makes desirable a second central directory — one that does not expire passwords — and a system to alert such users that their passwords are about to expire.
  - Password Self-Service.

- During the initial rollout of the system you will like get pushback on having the system at all if the system requires enrollment (such as answering security questions), but this resistance fades quickly.
- No matter how carefully you chose the security questions you ask, you will get people that think you made bad choices. Our solution to this was to pick standard questions that people can remember and then to always encrypt the answers.
- Case sensitivity. Be certain that your selected system supports case sensitivity for the passwords. Otherwise, a person can type “letmeinpleaz” when the password is supposed to be “LetMeInPleaz” and the system will let the person log in.
- Ensuring that *only* the owner can change their password, or any of the attributes associated with their identity
- Scope Creep – As the project proceeds, management will often want to wrap more and more features into the scope of the effort. Use good project management techniques to control the scope and manage expectations over the length of the project.

## Key Learnings

- Pick the right team
- Pick the right technology
- Phase it in
- You can’t over communicate
- Don’t underestimate how difficult change is for a percentage of your community members.
- Pick questions that are easy to remember and consider making the challenge responses non-case sensitive.
- Educate the community members on how to pick a password/passphrase that they will have an easier time remembering.
- Train the help desk and make sure they know when implementation is going to take place.

## Change

Of course no system can be put into operation without considering the impact that change, of any type, has on members of the effected community. As a community, UC is change adverse and has proven resistant to the implementation of an IDM policy and process. As a community of higher education professionals, we would do well to remember what Charles Darwin eloquently explained: “It is not the strongest of the species that survives nor the most intelligent, but the one most responsive to change.” We should also always remember that “there are risks and costs to a program of action. But they are far less than the long-range risks and costs of comfortable inaction.” (Paraphrasing John F. Kennedy)

Information Security procedures, like an IDM solution move people from comfort zones and are often challenged as un-necessary or over-kill. Nothing could be farther from reality. We are a world in cyber-

crisis and our personal data is being stolen almost at a laughable (if it wasn't so serious) rate. In order to move forward with corrective action, we need to change the way we are doing things.

Change requires action, not inaction.