Final Report
The Feasibility of Consolidating to a Single Account at OSU

January 2010

Table of Contents
Working Group Charge ................................................................................................................................. 2
Executive Summary ....................................................................................................................................... 2
Goal ............................................................................................................................................................... 3
Common Services Used at OSU .................................................................................................................... 3
Consolidation Barriers .................................................................................................................................. 3
  Password Policy ......................................................................................................................................... 3
  Account Management .............................................................................................................................. 4
  Applications Using Centralized Authentication ........................................................................................ 4
  Licensing and Access Control .................................................................................................................... 4
End User Benefits and Drawbacks ................................................................................................................ 4
  Security ..................................................................................................................................................... 4
  Unified Directory ....................................................................................................................................... 5
  One username and password to access resources ................................................................................... 5
  Potential for savings across OSU ............................................................................................................... 5
Consolidation Method .................................................................................................................................. 5
  Multiple Domain Model ............................................................................................................................ 5
  Consolidating to ONID .............................................................................................................................. 5
Administrative Processes Requiring Modification ...................................................................................... 6
  User Impacts ............................................................................................................................................. 6
  Migration Cost .......................................................................................................................................... 6
Efforts Currently in Progress ......................................................................................................................... 7
Summary ....................................................................................................................................................... 7
Committee Members .................................................................................................................................... 7
Appendix ....................................................................................................................................................... 8
  Migration analysis ..................................................................................................................................... 8
  ONID Account Statistics ........................................................................................................................... 8
  Terms used ................................................................................................................................................. 8
Working Group Charge
This ITCC working group will research and document the possibility of merging ONID and departmental based Active Directory (AD) accounts into one account. The team will focus on the following:

- Are there technical barriers to merging the accounts?
- What are the account management ramifications?
- What workflows/university processes will be required to change to make this successful?
- What are the customer benefits and drawbacks to merging these accounts?
- What are the ballpark costs or cost savings?

Executive Summary
Currently, most OSU employees have two Active Directory (AD) accounts: their ONID account which is a hybrid AD and Unix account, and an AD account provided by their department which may include an Exchange email box. Having multiple accounts is redundant and confusing to users. The committee was formed to explore the feasibility of using one user name and password (a single account) for OSU employees and students to access the majority of enterprise and departmental computing resources.

A single account is not the same as single sign on. A single account would still require separate authentication to each system, the same as today, but the same username and password would be used each time.

We took into consideration the existing IT environment and account consolidation projects already underway, especially the migration to ONID authentication for Banner.

We considered two possible consolidation options: a multiple domain model that layers existing Active Directory accounts on top of ONID or consolidating user accounts into the ONID domain. The multiple domain model was ruled out based on the inability of some existing enterprise systems to handle authentication across more than one domain. Consolidating to ONID, while not without its own challenges, appeared to be feasible and was clearly the committee preference. A number of issues will need to be addressed during implementation planning if consolidation is the final decision.

We believe that significant migration costs, primarily in staff hours, would be incurred to make this change. There are no long term costs which we can determine at this time and no foreseeable long term savings; however, changes to processes, automation, and consolidation of hardware or software may positively influence savings.

There are a number of benefits that employees and students would enjoy in a single account environment. The number of times someone has to authenticate will not change, but they will always know which username and password to use. This benefit, and others outlined in this paper, must be tempered with appropriate measures to ensure the security of OSU’s data.

This report details the methods considered, consolidation barriers, end user benefits and drawbacks, and efforts currently in progress.
Goal
The goal of the committee is to explore the feasibility of using one user name and password (a single account) to access the majority of University and departmental computing resources. This is separate from the concept of Single Sign On where logging in once gives you access to multiple resources, which is beyond the scope of this committee and considerably more difficult to achieve for a diverse campus community. This study identifies the drawbacks and benefits to end users, the computing resources affected, the technical and organizational barriers, the procedures that would need to be modified or created, and the areas where we expect to save or incur costs. Lastly, we provide a basic framework that describes how a single account system might function. This framework should not be considered an implementation plan.

Common Services Used at OSU
- Login to computer
- File server access
- Email (Exchange, ONID)
- Modular Messaging (voicemail)
- Banner, Nolij and Data Warehouse
- OSU Online Services
- Blackboard
- Wireless
- Virtual Private Network (VPN)
- Web Applications

Consolidation Barriers
There are a number of barriers to creating a single account for OSU employees and students to use when accessing electronic systems.

Password Policy
We must agree on a common password policy to consolidate accounts. The National Institute of Standards and Technology (NIST) Electronic Authentication Guidelines (http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf) are federal standards that OSU can use to develop a password policy that satisfies our account security requirements. NIST establishes four levels of identity assurance. The assurance level must be chosen based on the risks of an authentication error. OMB 04-04 (http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf) provides guidance to select the appropriate assurance level.

A detailed review of the OMB 04-04 guidelines is beyond this committee's scope. A cursory review indicates the following:

- NIST Level 1 assurance is adequate for most users
- NIST Level 2 assurance is appropriate for users with access to sensitive or protected information
**Account Management**

Delegated account creation is necessary. Many units have situations involving students, employees, and collaborators who require accounts that are not generated automatically under the current ONID system. Situations that must be accommodated include:

- Employees that require email accounts before their actual OSU start date
- Graduate students arrive and start their research before enrolling
- Students and employees continue to collaborate after their employment (ends e.g. writing papers)
- Visiting faculty, domestic and international
- Collaborators from federal, state, and county agencies or from private industry
- Others as identified

The ability to quickly disable accounts in the event of phishing, violation of acceptable use policies, etc. also needs to be delegated; however, this will require communication and coordination between account administrators. Policies and procedures for disabling accounts need to be developed.

**Applications Using Centralized Authentication**

Existing applications using Active Directory or LDAP authentication may need to be rewritten or modified as accounts are consolidated. Applications currently using Active Directory authentication should require only minor modifications.

Requests For Proposal (RFP) should include specific wording to ensure that new applications will work with OSU's authentication system and prevent adding additional authentication credentials.

OSU developers should ensure that applications will work with OSU’s authentication system.

**Licensing and Access Control**

We need to consider the effect of consolidation for software which is licensed on a per-user, per-FTE, or per-student basis. For example, some library databases are licensed and restricted to only OSU employees and students. When we add additional accounts, we may violate the license terms if there is no method to restrict access. Additional groups must be created in ONID. Some of these groups can be populated automatically from Banner, such as college and major, while others must be manually maintained.

**End User Benefits and Drawbacks**

There are a number of benefits and drawbacks of a single account environment compared to the current status quo. This section will outline both benefits and drawbacks without labeling them as such since they may be perceived differently depending on the point of view of the reader.

**Security**

Users with multiple passwords to remember often resort to insecure methods of keeping track of them. This is a serious risk to the University but we believe it is less likely to happen with a single account. Having a single account to maintain would have benefits for system administrators, including the ability to disable accounts, remove old or abandoned accounts, and respond to attacks.

One major risk of consolidating to a single account occurs when the account is compromised. An account may be compromised by malware infection of the local desktop computer, brute force guessing
attack, or social engineering (phishing). Currently, if a user’s desktop login account is compromised, their other accounts may still be safe. When a single account is used to access all systems, then a compromise affects all systems. This may increase the risk of exposure of sensitive data.

NIST guidelines may be an appropriate starting point for choosing the appropriate assurance levels. Low level Information Technology (IT) security training may also be necessary for those with access to sensitive information in order to help reduce the number of successful human engineered attacks against the university.

**Unified Directory**
Currently there are two directories used at OSU, the OSU Online Directory ("Find Someone") and the Outlook Address Book. Users may need to search both directories to find all of the desired contact information.

Most OSU employees have two entries in the Outlook Address Book, one from their ONID account and one from their department account. Consolidating to a single account would remove this duplication and confusion.

**One username and password to access resources**
Users may use many different accounts to access all the systems required for their jobs. Simplifying this access is the primary motivation for consolidating to a single account.

The current multiple account environment is complex, with a number of unique accounts including ONID ID, Banner ID, OSU ID, Active Directory ID, and maybe other applications that use yet another account.

**Potential for savings across OSU**
We believe there are no long-term IT costs or savings with consolidation. There will be significant one time migration costs, primarily in IT support hours, during the consolidation to a single account.

The University could see a reduction of implementation and development costs for new enterprise wide systems if authentication was consolidated. A single account may save users time and reduce the number of password resets due to forgotten passwords.

**Consolidation Method**
We believe it is technically feasible to consolidate user accounts to a single user domain. We considered the following options:

**Multiple Domain Model**
We explored the feasibility of layering accounts from existing Active Directory domains on top of ONID. We discarded this solution because most of OSU's enterprise systems (Banner, OSU Online Services, Data Warehouse, Blackboard, VPN, wireless, web applications) are not multiple-domain aware and would not function in this model. Fundamentally, this model does not achieve the committee's goal.

**Consolidating to ONID**
Users would be consolidated onto existing ONID accounts in the ONID Active Directory domain. Administrative, service and resource accounts could remain in the existing departmental domains or could migrate to the ONID domain. This consolidation would require attaching existing resources, such
as Exchange mailboxes and desktop profiles, to ONID accounts. Active Directory groups which grant
access to central and departmental resources would also need to be updated. Departments would be
delegated control over the ONID accounts belonging to people in their department.

The ability for departments to create new users in the ONID domain would be regulated (probably via a
web interface) to prevent the creation of users that would conflict with current or future ONID users.
Non OSU employees, who are not eligible for ONID accounts, would be prefixed with a department
identifier in the username, such as "tss_", "for_", or "eng_".

Active Directory computer objects and groups could remain in the existing departmental domain or be
migrated to a delegated structure within the ONID domain.

Administrative Processes Requiring Modification
To consolidate user accounts into the ONID domain, we must come up with a process for creating
accounts for people that do not currently qualify for ONID, including people that will be eligible for ONID
in the future (early accounts). See the Account Management section for more details.

There are two mutually exclusive solutions we have identified to address people who do not qualify for
an ONID account:

1. Create DINO (non-ONID) accounts for non-employees and early account creations. When an
   official ONID account is eventually created, manually reconcile the two accounts. This is not an
   ideal long term solution due to the manual reconciliation and should only be considered as a
   short term solution.
2. Create Banner SPRIDEN records for everyone, including non-employees, and some means in
   Banner to trigger the creation of an ONID account for these additional people. This would
   require Banner access for department IT staff to create an ONID account with a turn-around
time of less than two hours to meet department’s expectations.

Solution #2 would be the ideal solution in that all information would be in one place and there could be
one university wide process. However this would require approval from the Banner data custodians as
well as modifications to Banner forms and processes. Solution #1 would only be recommended as a
short term solution.

Both solutions would benefit from a more widely used Employee Fast-Track ID form to populate Banner
with incoming employees on a timely basis.

User Impacts
Users may need to learn a new username if their current departmental account does not match the
ONID account or they do not use one of the enterprise applications requiring an ONID account such as
VPN or BlackBoard.

There would be temporary disruptions in access to resources during the migration process.

Migration Cost
Department IT staff would be involved in migrating from existing departmental accounts to ONID
accounts. They will have to visit each workstation to migrate desktop profiles. They will also have to re-
assign resources and permissions to the ONID account.
Additional resources would be required to re-write existing departmental applications. This could be significant depending on the complexity of the application.

**Efforts Currently in Progress**
Enterprise Computing Services is migrating to ONID authentication for Banner, OSU Online Services, Banner Data Warehouse, Appworx (Banner job submission), and Touchnet ([http://mybill.oregonstate.edu](http://mybill.oregonstate.edu)). This migration is still in the testing phase. The target for implementation is sometime before summer 2010.

UHDS (University Housing & Dining Services) is planning and testing the migration of their Active Directory accounts, and associated resources such as exchange accounts, from the FS_MAIL domain to the ONID domain.

**Summary**
It is technically feasible to consolidate to a single account. There are significant upfront costs to consolidation. There are no long term costs or savings, but employees and students should enjoy some benefits from having a single account to access the majority of enterprise and departmental resources assuming an appropriate balance between security and usability can be found.

If the decision is made to consolidate accounts, we recommend establishing an implementation committee to address the following outstanding issues:

1. **Administrative processes**
   a. Determine the best method to integrate people not currently eligible for ONID accounts
   b. Identify resources and processes requiring modification
2. **Security requirements**
   a. Identify systems housing sensitive data
   b. Work with OSU Data Custodians to determine if a single account will necessitate additional security measures to access data under their purview.
   c. Implement appropriate security
3. Provide migration cost analysis
4. Propose migration plan and timeline

This assumes an ongoing process exists among all IT units to ensure needs are being met.

**Committee Members**
Lucas Turpin, Working Group Lead, Community Network
Jos Accapadi, Central Web Services
Steve Cleveland, College of Engineering
Linda Devenow, Budgets and Fiscal Planning
Steve Fowler, Technology Support Services
Andrew Morgan, Enterprise Computing Services
Curt Onstott, Crop and Soil Sciences
Cary Shufelt, Network Services
Alan Sprague, College of Business
Chris Thompson, College of Engineering
Ken West, College of Forestry
Chris White, University Housing and Dining
Appendix

Migration analysis
The following are some of the steps required to consolidate resources for a single user’s account from a department’s domain to an existing ONID account:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move Exchange mailbox</td>
<td>Migrate existing exchange email to ONID account</td>
</tr>
<tr>
<td>Reassign Groups</td>
<td>Remove departmental user object from existing groups and add ONID account groups granting access to departmental resources</td>
</tr>
<tr>
<td>Fix Departmental Resources</td>
<td>Some departmental resources have permissions granted based on username. For those users that have a different ONID username, those resources will need to be fixed.</td>
</tr>
<tr>
<td>User Data Move - per computer</td>
<td>Once the account is migrated, the user must login to establish their ONID profile. Then IT can step in and move the data from their old departmental profile to the ONID profile. This must be done for each computer the user logs into and stores any data.</td>
</tr>
</tbody>
</table>

The following alternative migration path, still under testing, may require less time and resources.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete ONID AD object</td>
<td>Delete only the Active Directory part of the ONID account</td>
</tr>
<tr>
<td>Move departmental AD object to ONID</td>
<td>Move the departmental AD object from the departments domain to the ONID domain.</td>
</tr>
<tr>
<td>Re-link migrated AD object</td>
<td>Assign appropriate attributes to the Active Directory object required for automated process and linking of accounts.</td>
</tr>
<tr>
<td>Reassign ONID Resources</td>
<td>Re-assign any resources or permissions to the windows side of the reformed ONID account (this may be little to nothing).</td>
</tr>
</tbody>
</table>

ONID Account Statistics
The following are statistics as of January 19, 2010 about the ONID domain.
Total number of ONID accounts 46,656
Total activated ONID accounts 38,976
Accounts activated more than 5 years ago 5,380
Employee ONID accounts 7,149
Activated employee accounts 5,540
Employees for more than 5 years, NOT activated 808
Total number of DINO accounts 337

Terms used
Active Directory
A collection of Windows computer and user objects organized into domains. (Windows equivalent of LDAP). This directory populates the Outlook address book.
DINO (DINO Is Not ONID)
DINO accounts are not ONID accounts. DINO accounts are created in the ONID LDAP directory but are only visible to the services that specifically allow DINO accounts. DINO accounts are not created in Active Directory, do not have file storage, do not have web sites, and do not have email addresses. DINO accounts can be used by any service which uses the ONID LDAP directory for authentication. This includes ONID SSO websites, the OSU VPN service, and more.
LDAP (Lightweight Directory Access Protocol)
A collection of non-windows computer and user objects. This directory populates the OSU Online Directory (Find Someone.)

NIST (National Institute of Standards and Technology)
A federal technology agency that develops and promotes measurement, standards, and technology.
http://www.nist.gov

ONID (OSU Network ID)

OSU Online Services
Banner web portal, also known as Banner Self Service or Banner Web Tailor.

OSU Records Custodians
Records custodians (or owners) have full and final authority for the utilization of, and access to, data under their jurisdiction. Security or access levels for each OSU employee are determined by the custodians. In some instances there are multiple custodians for various sets of data.
Registrar – Kent Kuo
Admissions – Michele Sandlin
Business Affairs – Aaron Howell
Budget and Fiscal Planning – Nancy Heiligman (Mark McCambridge)
Financial Aid – Emilio Vejil
Human Resources – Jacque Rudolph

http://oregonstate.edu/dept/computing/banner/pubs/gpmanual.pdf

Personally Identifiable Information (PII)
Information as identified in Oregon’s Senate Bill 583 (http://oregonstate.edu/net/security/personal-information.php)

SPRIDEN Record
A SPRIDEN record is the unique person record in Banner.

VPN (Virtual Private Network)
VPN provides secure remote access to the OSU network.