

## Case Study: Brandeis University

---

### GENERAL AUTHENTICATION

Brandeis University has a predominantly centralized service based on a combination of Lightweight Directory Access Protocol (LDAP) directory authentication, UNIX accounts for e-mail, and Active Directory for desktop logins. This centralized authentication is true for all but a few systems. A typical authentication scenario is student or staff members logging on to their desktop, and then accessing and authenticating to different systems (e.g. PeopleSoft, e-mail) as needed.

We are currently engaged in a project to rollout USB-based PKI tokens to first systems administration and DBA staff. This group will be followed by: desktop support personnel, our PeopleSoft developers, and then by administrative users. Our current plan does not include any additional groups.

### POLICY

We have an informal policy requiring use of a consolidated AuthN service for most applications, and there is no written policy requiring the use of either the central LDAP or Active Directory. Our usage policies are documented, which include sharing and reset:

<http://its.brandeis.edu/about/policies/computingpolicies.html>.

Brandeis offers informal multiple levels of assurance. Three user groups encompass the following accounts:

1. Administrative accounts - with carefully maintained authorizations; each user is personally known,
2. Non-administrative accounts - significantly less access and oversight, and
3. Sponsored accounts - have almost no vetting; authorizations are limited to e-mail and desktop login functionality.

In addition, we do mandate processes and practices relating to security, such as prohibiting the use of clear text passwords to our primary systems. We eliminated these by first providing SSH/SSL mechanisms where clear text passwords were being used in conjunction with marketing campaigns urging migration to SSH/SSL. For a three-month period, we monitored the systems for clear text logins and individually contacted each of these users to assist them in the use of the SSH/SSL tools.

Afterwards, we eliminated the clear text mechanisms and dealt with the few remaining clear-text users through our help desks.

### ISSUING IDENTIFIERS

Electronic identifiers and passwords/tokens for access into computer-based systems and services are fully-automated, dynamically generated from source systems. Brandeis initially assigns identifiers at the time of application, hire, or sponsorship. On average, two login credentials are assigned to each person in the system. Students who receive financial aid will get an additional ID for PowerFAIDS (our financial aid system) and another after becoming an alumna or alumnus. Faculty and staff have a second set of credentials for Oracle Calendar. We have recently overcome a technical roadblock with PowerFAIDS so that we can construct URLs for a particular user as if already logged in, so that second ID for students can disappear. We've kept the Oracle Calendar namespace separate from our all-powerful UNet account out of concerns over the applications security model. Current versions of Oracle Calendar seem to have eliminated those concerns, but more research is needed.

Distribution of identifiers and passwords employ different methods associated with different business processes. Users are allowed to choose their login ID. Under special circumstances, we do send out a mass mailing that contains a username and "ticket" that can be used to initiate the account creation process.

During the on-line account creation process, user-chosen IDs and passwords are checked dynamically against the already allocated IDs to ensure they adhere to our strength rules. Currently, the login identifier

is persistent and never reassigned; however, this policy is coming up for debate within the next six months.

Our LDAP directory uniquely identifies each person, including employees, students and non-students, with many attributes (e.g., name, SSN), and is tightly coupled with our PeopleSoft systems of record.

Identity proofing is the collective responsibility of the following: Human Resources(HR), Registrar, Campus Police, Parking, Badging services, and Campus Card Office. HR engages in fairly rigorous identity proofing for faculty and staff as per federal hiring requirements. The Registrar meets the ISSO requirements for foreign students but is more lax otherwise, particularly for continuing education students. The campus police require a driver's license and registration for parking permits, and the campus card office checks for some form of ID on issuing a campus identification card.

### **PASSWORD MANAGEMENT**

Our passwords are largely self-maintained for changes, and are reset via some basic scripts accessible, on <https://unet.brandeis.edu/cgi-bin/passwd>. The password strength rules, documented on the site, are enforced at password creation/change.

Our policy, as described above, covers password length, life cycle, syntax, history, pre-crack, and pass phrase. This system enforces a maximum password length.

Passwords are stored by means of MD5 hashing within LDAP, UNIX hashing in the UNIX file systems, and also in Active Directory. Active Directory and UNIX credentials are fed from LDAP, so although there are three technologies, they all function as single login/password. Users will use the same userid/password pair to log into each application, except for those noted above. This is true even to the extent that the MS-Windows password expiration is disabled, and the password changing mechanism that one accesses (via ctrl-alt-del) is disabled (i.e., "grayed out") to ensure that all password changes are first made in the central LDAP directory and then supplied to Active Directory.