FOCUS: HIPAA

Single Logon: Balancing Security and Healthcare Productivity

ABSTRACT

Mayo Single Logon (MSL) has faced the traditional dilemma that is painful to all IT organizations because it forces the tradeoff between user productivity and security. Recent regulatory initiatives, such as HIPAA, have caused the issue of security to take on more importance, forcing organizations to revisit the balance of security and productivity. MSL is a security application that brokers user credentials and facilitates desktop security. The simple design, functionality and stability have allowed MSL to speed up user productivity, keep satisfaction high and help solve many security initiatives.

MARGARET (PEGGY) J. SAPP AND TERRENCE (TERRY) L. BEHRENS

Mayo Clinic, Rochester, MN, is an integrated, multi-specialty practice. More than 23,000 allied health personnel support 3,200 staff and resident physicians. The Rochester campus includes both outpatient and inpatient practice and has three hospitals: Saint Mary’s Hospital, Rochester Methodist Hospital and Generose Hospital. About 20,000 workstations are part of the technology infrastructure used to support the practice.

Mayo is a physician-run institution with physician-led committees in which consensus rules. Decisions are driven by Mayo’s primary value that the needs of the patient come first.

Mayo’s single logon faced the traditional dilemma that all

KEYWORDS

Mayo Single Logon (MSL)  HIPAA  Security  Access  Implementation  Persistent  Password management  Compliance
IT organizations struggle with because it represents the tradeoff between user productivity and security. In most cases, security and security features have received less visibility, while user productivity and satisfaction have received the most attention.

The imbalance between productivity and security has led to many issues, such as users selecting generic IDs and sharing user names and passwords, as well as an overall lack of security at the workstation level. Recent regulatory initiatives, particularly HIPAA, have raised the importance of security and have caused organizations to revisit the balance of security and productivity.

**Project Background**

The Mayo Single Logon (MSL) project has two objectives. First, it is intended to provide fast, easy and secure access to clinical and non-clinical applications. Secondly, it is intended to provide software that facilitates processes to meet Mayo Foundation and HIPAA security requirements for patient electronic medical records and business information.

In early 2001, a vendor’s product was being implemented at Mayo. Prior to implementation, an analysis of workflow processes indicated that the use of the new system would cause a practice change for many users. Stability issues became apparent even though the vendor’s product had been deployed to only 1,500 of the 20,000 workstations. At the same time, the parent company of the vendor was sold to another company that had little interest in supporting the product.

This led to Mayo’s participation in a due diligence process. This process looked at products from other vendors, the existing product and a solution created in-house. Mayo elected to adopt the in-house single logon product based on its design, cost and supportability. The experiences gained in preparing to deploy the vendor product were used to shape the homegrown product.

In addition, the MSL technical team developed a password management strategy to help users utilize a true “single password” in their workflow and a help desk diagnostic tool to help identify and correct any issues that occurred during deployment or routine use.

**Design Elements and Ancillary Tools**

The in-house single logon and related password management project had to have four components to meet HIPAA requirements: an enforced secure screensaver, automatic logoffs after periods of inactivity, workstation logging and auditing capabilities and password expiration capabilities.

A usability study found other features that were important to users. These included:

- A password synchronization tool that could be used by the individual versus going through a help desk.
- A rapid way to log off or lock the workstation (See Figure 1).
- “Persistent” applications that remain on between user logons to increase the speed of accessing applications.
- The ability to individually customize which applications would launch when a user logs in to a workstation.
- The need for tools at the help desk to resolve user issues.
- The need for a tool for security personnel to query information that was centrally logged.

During the design phase, many practice groups at Mayo were interviewed to identify key design elements for a single logon application. From these interviews, the team developing the software determined that the software should contain all workstation features that HIPAA would require, always be available, be modular in design, be adaptable, function quickly, use Mayo’s existing infrastructure, be layered above the Microsoft operating system, and use the application communication interface that existed with the former product.

MSL is designed to be modular in nature, with each module having specific functionality and responsibility. This modular design concept enables easier debugging, faster interoperability, a smaller footprint and the ability to do plug and play. The modular design encapsulates functionality to specific pieces of code. For example, the modular design allows any type of biometric identification system to be used by creating a dynamic link library that works between the device and MSL by using a standard set of application program interfaces. An implementation that used a proximity badge reader was designed as a “proof of concept.”

The single logon was devised as a client/server application that only uses the server for data storage. There is no “true” central server used for credentials for MSL because the application relies on Microsoft domain authentication first and then does a lookup in a series of tables that reside on a dedicated server. The lookup checks additional permissions for individual users and to get additional identifiers. This design approach helps increase high availability and enables the use of structured query language that is not linked to any particular vendor.

Wherever possible, MSL was designed to use existing Mayo and Microsoft infrastructure to save time, money and incorporate any future changes. MSL does not use a
central application server, but instead it adds additional links to the workstation and then reroutes the application links from the start menu to these links based on whether MSL is installed or not. This scheme enables applications that are both MSL-aware and non-aware to co-exist on the workstation and for MSL to be installed on individual systems under the same policy without disrupting other machines.

All essential system settings are either delivered by Microsoft policy (screen saver and auto-logoff timeouts) or by registry settings that can be manipulated remotely.

MSL supports a mode of application management called persistence, which enables particular applications to be started when the computer is turned on and then remain running. If these applications are MSL-aware, they receive logon and logoff messages from MSL. Persistent applications also can be non-MSL aware and can continue to run even though the computer may automatically log a user off after a certain period of inactivity. These types of applications might be long-running report-generators or machine interfaces.

MSL also supports an ancillary tool called Auto Start Manager that enables users to start applications at logon, based on their profiles. These auto-start options can be set either for roaming or for individual logons to specific machines.

Reducing Potential Problems

Other features were incorporated in the product to help minimize the number of assistance requests to the help desk. Features like self-diagnostics and auto-update help to meet the design concept of high availability and help with the change management process.

The MSL design team also expanded the available interfaces to include remote procedure calls, screen scrape and created a Common Object Method (COM) control that is installed on each workstation client to facilitate communications between Web-based applications, Visual Basic and Java. These interfaces are secured with session keys to secure the communications between an application and MSL, preventing spoofing. User credentials are passed in encrypted formats to applications.

MSL code was written with Microsoft Compiler in straight “C” language for the sake of speed, for portability across various Microsoft operating platforms and for stability when working with the graphical identification and authentication module.

Several steps were taken to minimize the impact of the deployment and to minimize the impact of any potential problems. Microsoft Premier support analyzed and reviewed the architecture to ensure that it did not interfere with the operating system.

A service level agreement was created after testing scenarios were created and tested. This agreement defines exactly which team is responsible for each part of the application. This process helps document the flow, and each party involved can turn to the agreement to help troubleshoot any problems that occur.

The client code also has been modified to help alleviate any outages. All calls to the server store procedures have timers on them. The logging is kept on a separate server and is handled in traditional transaction management architecture.

Password management was handled as a separate project to help get passwords down to one. It involved the development of three interfaces to one piece of code: a Web-based user self-service page, a help desk master resetter and the MSL.

Device Doctor for Help Desk was used as a launch pad for tools, and it displays information that enables speedy diagnosis and repair.

The usability lab demonstrated that users wanted a fast way to log off or lock the workstation just as much as they sought a fast way to log on. Therefore, mouse options for these functions were introduced on the desktop. To save time and enable the physician to focus on the patient, users also wanted user-controlled auto-started applications that could be varied depending on the work location. For example, some wanted a different set of applications to start up in the inpatient setting, and another set that would start during outpatient rounds or procedures.

The Implementation Strategy

Microsoft Project was used to help the team recognize and keep track of tasks and timelines. The development team met on a weekly basis with the implementation team to review progress, make assignments and adjust the plan.

Within the project plan, a template or checklist by practice was developed. These also ensured that steps were not skipped or forgotten.

Three options were considered for deploying a single logon approach. Because the tool by itself did not force practice change, it could have been installed on each workstation in a big bang approach. However, stability issues with the previous vendor caused Mayo to consider a different approach. Mayo was eager to have single logon available for users who were beginning to use more online clinical applications during the course of patient
FOCUS: HIPAA

care. Therefore, a fast-track implementation approach was chosen.

Mayo’s Board of Governors endorsed the project and implementation plan, and that provided support to the plans, which was important in nudging some practices that were not eager to embrace individual logon accountability.

Communications and other implementation tasks were standardized for every medical specialty department and division. A standard checklist was built into the project plan for quality control.

During the development and testing phase of the project, communications began with various practice chairs, administrators and front-line managers. Previous experience had shown that it was helpful to have some local early adopters who could provide feedback and help support others in their work areas during implementation. A Web site was established to address frequently asked questions and provide online training and other implementation information.

Implementing a project of this size involved considerable infrastructure challenges, which included:

- Distributing software to different platforms.
- Updating software.
- Modifying workstation policies to have the correct values for settings.
- Developing a strategy for “spot” installations.
- Creating a knowledge base for frequently asked questions.
- Creating a strategy to reinstall MSL on computers with rebuilt hard drives.
- Creating a strategy to handle MSL on several different classes of workstations.
- Creating a development, integration and production server environment.
- Creating an automated build process and automated version checking.
- Creating a process for testing fail-over quarterly.
- Creating a process for automated user enrollment.

These challenges were handled by establishing weekly meetings with the MSL technical team and the support teams from Mayo for infrastructure processes.

Challenges Encountered

Many clinical applications could not be modified to stay active between user sessions. This meant users had to wait for the applications to launch at each logon. The next version of the application is expected to resolve this issue.

Many times, the team filled an educational role by introducing security and accountability expectations to new users. Although MSL does not force individual logons and logoffs, this was new territory for those who were used to having someone else on their patient care team logon to the workstation. Even today, individuals who see a higher volume of patients find it difficult to logon and logoff for themselves.

Many users carry bad memories of the previous product, which was unstable, and it has taken time to build their confidence so that they understand that whenever something goes wrong, it is not necessarily caused by MSL.

Measuring the Performance

So far, MSL is deployed to more than 15,000 workstations on the Rochester campus. Most of those implementations took place in the first four months.

The 27,000 users of the system have found MSL to be extremely stable. MSL has caused very little interruption of service for most users. Since initial implementation, generic logon accounts have been eliminated. However, the new application by itself does not force individual logons and logoffs.

The purpose of the tool is to facilitate access and security with the least amount of disruption. Its use has reduced the amount of multiple logons, thus reducing the time needed to activate and use applications. Because applications are more readily available at logon, synergies will develop in using various applications online during patient care activities and result in reduced dependence on paper medical records.

After implementing MSL, the average single logon time was 31.2 seconds faster than the average time before implementation (See Figure 2), nearly a 75 percent improvement (SD=10.48).

Several qualitative, non-measurable effects of MSL were reported. They included achieving compliance with regula-

![Figure 2: Measurement - baseline and post implementation workstation access speed (31% improvement)](image)

**Average of 31 second improvement (75%)**

<table>
<thead>
<tr>
<th>Descriptive Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>Time</td>
</tr>
<tr>
<td>Time</td>
</tr>
<tr>
<td>Time</td>
</tr>
</tbody>
</table>

T-Tests

| Variable | Method | Variances | DF | t Value | Pr > |t| |
|----------|--------|-----------|----|---------|------|----|
| Time | Satterthwaite | Unequal | 18.8 | 9.42 | <.0001 |
tions; improving account control; facilitating security of workstations and the electronic health record; developing a central point for logging workstation activity; better securing applications that are not among Mayo’s integrated clinical systems and do not require logon; assuring expandability to allow use of biometric devices; and enabling users to customize auto-start applications.

An evaluation survey conducted two months after the implementation indicates that 92 percent of 337 care providers have an average to excellent opinion of MSL. Some 63 percent indicated that the adaptation to using MSL in their practice was relatively easy with few negative effects. Another 32 percent indicate that the transition had been somewhat difficult, but that they were adjusting (See Figure 3).

Lessons Learned from Implementation

Several factors helped make the MSL implementation a successful one.

Knowledge of the Practice. Those implementing MSL knew the Mayo practice over several years, and the workflow analysis completed for the implementation of the previous product enabled a quick implementation of the single logon application.

Frequent Meetings of Various Groups. Throughout the project, the technical team and implementation team conducted frequent meetings. Originally, the two teams met together on a weekly basis. When the groups discovered that their issues were not always critical to each group, they began meeting separately. Special meetings were held if something needed to be discussed by both groups. E-mail was used for communication between meetings. In addition, two physician proponents were assigned to the project to provide guidance and to help provide the department and division demonstrations. They jointly led a subgroup that held meetings every two weeks. Members of the subgroup included several other infrastructure workforces at Mayo, and that helped to break down barriers if support was required from other workforces.

Beta Users and Super-Users. During the testing phase, several physicians and allied health personnel were asked to be beta users. This group of about 25 individuals provided important feedback and validated the design, and they continue to help as enhancements are developed. In addition, several super-users were identified in each department or division. They were trained and received single logons for their workstations before implementation in their areas. They were able to tell developers how the single logon would fit into their practice, and they were able to answer their colleagues’ questions.

Early Education Services Involvement. Two project team members were from microcomputer education services, a branch of Mayo’s human resources department assigned to train personnel on workstation and applications. Their involvement from the time when the usability study was conducted throughout implementation enabled them to develop ways to train users. They developed online tutorials in addition to quick reference guides, which were useful in training for other applications.

Providing Demonstrations. Each department or division received a demonstration during one of their regular meetings, which generally attracted participation from physician staff and allied health managers. It is doubtful that so many staff would have willingly attended some other meeting added to their busy schedules.

Saturation Communication. Several approaches were used to communicate information about single logon and password synchronization. Staff developed a Web page that included links to the online tutorial, quick reference guides, a password synchronization tool, a list of frequently asked questions, tips and tricks and the implementation schedule. Kiosks were strategically placed at entrances to employee cafeterias. A PowerPoint slide presentation was played continuously, showing screen shots and text to identify important features, and quick reference guides were available by the kiosk. Flyers were posted in workrooms and employee break rooms when the date of application implementation approached.

Implementation Partners. To support implementation to a large number of users, staff working on other projects were “borrowed” and assigned to various sites at the time of implementation. They provided a physical presence and were able to report any issues back to the implementation team. Team members and implementation partners then met at midday to develop a list of items and make assign-
ments for follow up. This helped to discover recurring problems that needed to be resolved before implementation began at the next site.

Areas for Improvement

Not everything went perfectly with the implementation. Staff found several areas they would have done differently.

Change Management. MSL was deployed knowing it was a tool to facilitate security, but the fast-paced implementation did not leave appropriate time to help some areas adjust to the paradigm shift of expecting individuals to log on and log off.

Project Team—Application Team Communication. Hopes that various clinical applications would remain launched between logons and logoffs proved unrealistic because it was not technically feasible for some applications. This had not been communicated to the MSL team until shortly before implementation. IT leadership had to step in to mediate the situation. Physician leadership compromised. The unavailability of this feature prevents users from experiencing additional time savings when they access those applications.

Demonstrations to Physician Leadership. Typically, one physician proponent attended department or division demonstrations. However, they were not available in two of four areas, necessitating follow-up by them to reinforce the message that the implementation was board-directed. Peer-to-peer discussions often are more productive and should be used earlier rather than later to resolve conflicts.

Future Plans

MSL is a tool of simple design. It is stable, provides single logon benefits and contains flexible features for users to help balance security with productivity. It facilitates meeting workstation security goals for both HIPAA and the Foundation. However, in some practices, the balance of security and productivity still has not been achieved.

Future enhancements will include a feature to help some work environments increase productivity. Plans are under way to communicate and build training plans for the rollout of Version 3 with the new feature. With the ability to retain patient context between care team members logging on—termed rapid user switch—the organization anticipates improved individual accountability and thus a closer balance of security and productivity.

Efforts are under way to expand the password management suite to include all servers and departmental applications that are housed on those servers.

Steps are in place to implement single logon for more non-clinical, business workstation users. In addition, single logon is being expanded into Mayo Health System sites. And looking to the future, the MSL technical team also is preparing for a Web-based logon to a suite of applications.

About the Authors

Margaret (Peggy) J. Sapp is systems and procedures analyst for the Mayo Foundation. She can be contacted at Sapp.margaret@mayo.edu.

Terrence (Terry) L. Behrens is team leader for the Workstation Security and Access. He can be contacted at Tlbehrens@mayo.edu.