Working Smarter with Identity Management Modernization

State of Minnesota — Minnesota IT Services

CATEGORY:
Business Process Innovations

CONTACT:
Emily Shimkus
Director of Communications
emily.shimkus@state.mn.us
(O) 651-201-1011
(C) 651-485-1354

INITIATION DATE:
May 2017

END DATE:
June 2018

MINNESOTA IT SERVICES

Executive Summary

One of the basic tenants of ITIL is to always look for process improvement opportunities; "work smarter, not harder." Since Minnesota IT Services (MNIT) is an ITIL shop, our teams embarked on a project to better serve business partners at the Department of Transportation (MnDOT) by automating the process of updating personnel information for MnDOT's enormous staff and creating a self-serve password reset application.

Personnel data was already entered and stored in the state's employment system called SEMA4. It was not, however, connected to any other systems, and moving the data from one to the other was a manual, time-consuming process fraught with error. By using MNIT's expertise in Active Directory and the Outlook Address Book, we set out to find a way to update Active Directory auto-magically (in technical terms) with the data that was already available in SEMA4, the state's system that houses information such as employee titles, phone numbers, work locations, departments or offices.

Previously, MNIT and MnDOT spent a lot of time updating basic user information in Active Directory records, and again updating the same information in the Outlook Address Book. Entering the information into another application wasted resources and increased the risk of typos and errors. The information was already in one state database, so why not take advantage of that and use it to update other state systems automatically?

The new MnDOT Identity Manager (MIM) uses Microsoft Forefront Identity Manager (FIM). It allows us to take advantage of SEMA4 nightly updates and use them to synchronize data within Active Directory and Outlook and the Global Address Book. This saves IT resources from having to manually update this information as employees come and go, or move between offices. The process is automatic, accurate, and timely, and not prone to human error.

Another common task performed by IT staff is password resets and account unlocks. Similar to commercially available systems, the Self-Service Password Reset (SSPR) module in FIM provides users with the ability to unlock their own network accounts by pre-registering the answers to five out of ten security questions beforehand. The answers are stored, and then randomly presented when a user needs to reset their own password. They can do it securely at any time, any day, from anywhere in the world, using an Internet browser.

Another opportunity we discovered involved managing consultant network access. MnDOT manages about 1,000 consultants on an annual basis. Not all workers log into the network on a daily basis, and a common problem we faced involved consultant accounts expiring unexpectedly for them. As a result, expensive consultant time was wasted while supervisors worked to get the expired accounts re-enabled, and the consultant back to work. MNIT and MnDOT used to spend a lot of IT resources re-enabling and extending consultant expiration dates. We built a workflow in MIM that continuously monitors the status of all consultants' expiration dates, and provides email notification to the consultant and their supervisor. MIM uses a simple, intuitive interface that allows supervisors to extend their own consultants when needed.

Currently, our MNIT teams are planning future projects to enhance MIM and give MnDOT Human Resources staff an even more on-demand and responsive experience. We are committed to building partnerships that ensure success, providing solutions that benefit all Minnesotans, and delivering quality IT solutions on time and on budget.

Exemplar

MIM **utilized existing MnDOT data** to automatically update Active Directory in a more responsive and timely manner. This allows us to update other IT systems in a more efficient and less expensive manner. Additionally, it has given stakeholders and resource owners more **direct control and management** of MnDOT applications and network resources.

Concept

Thousands of MNIT staff hours were consumed annually to update information in Active Directory and the Outlook Address Book with information that was already present and being maintained within the SEMA4 system. MNIT staff and MnDOT's Human Resources staff were **duplicating efforts with manual processes** to update the same information in multiple, separate systems, resulting in thousands of separate transactions per year per system.

The **purpose** of the MIM project was to **eliminate the manual, redundant processes** between SEMA4, Active Directory, Outlook, and the MnDOT Warehouse, and replace them with **automated processes** that connected existing data to the corresponding employee and consultant information stored in Active Directory records and the Outlook Address Book. The MnDOT Warehouse data was also being used to generate business reports and update selected business applications.

Research and technical articles indicated that there was a Microsoft product, Forefront Identity Manager (FIM) that could be used to update fields in Active Directory automatically from data already being stored in the MnDOT Warehouse.

The proposal was to use the information stored in the Warehouse to update employee Active Directory information using Microsoft's **Forefront Identity Management (FIM) System**. The process would be automatic, more efficient, and it would have the advantage of eliminating errors and typos which were inherent to manual data entry. Private employee data was not within the scope of the project.

In 2017, the proposal was approved, the **software purchased**, and a consultant with expertise in Microsoft's FIM was hired to assist in the initial setup and configuration of the system. The **cost of the consultant's services** was approximately $30,000. In addition to initial setup and configuration, the contract included assistance in development of custom workflows to:

- Automatically detect employee separation, retirement, or the decease status of a MnDOT employee, and automatically disable the employee's network account.
- Monitor consultant expiration dates. FIM could send email notifications with two-week, one-week, and day-of notice to consultants and their supervisors when accounts are due to expire, with instructions about reactivation steps.

Plans are underway to **implement future updates** and enhancements to the application.

Our MNIT project team met with numerous **MnDOT stakeholders**, including Human Resources representatives, in addition to MNIT staff responsible for updating and maintaining information in the MnDOT Data Warehouse.

MNIT staff **monitor and maintain the IT systems**, and are responsible for the oversight and outcomes of the project.

Since this was an internal project that affect MnDOT and MNIT staff, we used a **personalized communications approach** to socialize the project and the new processes. Educational briefings were held with Human Resources and MNIT Service Delivery staff to explain which SEMA4 fields were being used to update Active Directory records and the Outlook Address Book. MNIT Service Delivery staff **maintain instructional documentation** and share information with customers so they know how to make corrections to information in Active Directory records and Outlook.

Significance

All MnDOT staff benefit from having current, accurate information available in the Outlook Address Book. **MNIT support staff benefit** from more expedient processes and less time needed to update records.

The **project scope** included only the public information of MnDOT employees and consultants that must be maintained in Active Directory.

The MnDOT Identity Management modernization process uses information updated in SEMA4 to automatically update the corresponding information within Active Directory and the Outlook Global Address Book. This effort reduced staff resources needed to maintain the same information in other systems, while at the same time increases timeliness, and reduces errors and typos.

We saw **successful implementation** for employee information updates and in the self-service password reset portion of the project. Successful implementation is seen when SEMA4 data updates Active Directory information within 24 hours, and the information is identical to the SEMA4 data.

In the **Self-Service Password Reset** portion, success was gauged by **significant reduction in calls** to the Service Desk for password resets. This service allows all MnDOT customers to have the ability to unlock and reset their own passwords securely when they need to, 24 hours a day, 7 days a week, and 365 days a year, from anywhere in the world, using a browser with Internet access–without the need to involve MNIT staff.

The **primary beneficiaries** of the MIM system are the MNIT staff who are responsible for maintaining the information, however, all MnDOT users benefit from more accurate information in state systems, including the Outlook Address Book that is available for everyone.

The MIM project aligns with policies and priorities across the state and with our agency business partners by providing state employees with accurate, timely information, and on-demand access anytime, from anywhere. **Productivity increases** when employees have more flexible access to state networks. MNIT staff involved with the project have provided **documentation** to use in creating and building a similar system. MNIT and MnDOT business leadership have been included in discussions concerning MIM enhancement and growth. The Self-Service Password Reset service **significantly reduced employee downtime** caused by locked network accounts.

Additionally, the MNIT team expanded business partner participation in Active Directory security group management to control applications, and access to network folders and resources. This will move direct management of many network applications and resources closer to the business customer more efficiently.

Impact

In short, **MNIT and MnDOT are now doing more with less!** The MIM Project reduced the number of resources necessary to update information in Active Directory and Outlook, enabling IT staff to work on other projects. It has improved the accuracy of the information contained in Active Directory and the Outlook Address Book, which provides better, more accurate and timely information to our MnDOT customers.

Prior to implementation of the MIM project, **MNIT staff spent thousands of hours** annually updating employee information in Active Directory and the Outlook address book using information that Human Resources staff had already updated in SEMA4. This manual, duplicative process of updating the same personnel information was slow, resource intensive, and incurred a significant delays.

The immediate impact of the initiative was to **reduce turnaround time** to present the updated SEMA4 information, from two weeks to one day (24 hours). In addition, as an automated process utilizing the same SEMA4 transaction information, the implementation of this project created an opportunity for a more efficient, streamlined process to **update employee information across different platforms**, which increased the turnaround time for updating critical information and **improved the accuracy** of current information while reducing errors and typos.

The primary justification for the MIM project is that it is based on the obvious **strengths of automation** – the **speed, accuracy, and efficiency** of computers to duplicate and distribute data between systems. To maximize efficiency, MNIT and MnDOT took advantage of data already stored in state information systems. Automation is a logical choice when considering the direct labor cost involved in manually update the same personnel information, which involves thousands of transactions per year.

The Self-Service Password Reset (SSPR) service has **improved network availability** to our MnDOT customers during off-hours, and provides **better customer service**, as users can now unlock their own network accounts when needed. It has **reduced on-call staff time** to resolve password issues.