CASE STUDY

Product: **HelloID, IAM, PSM, SSPRM, Service Automation** Sector: **Industry** Date: **2020**

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Haas F1 Team
OFFICIAL MACHINE TOOL

A Case Study for Identity & Access Management

Haas Automation is a private manufacturing company in California. During the last 35 years, the company has grown to 1500+ employees and 170 distributors worldwide.

Still, Haas' SAP Security Lead, Vincent Cacaro, considers it a smaller organization. So when he began looking for an IdM solution last year, he immediately ruled out huge vendors like IBM and SAP. He knew they wouldn't fit – on timing or price.

"Their scoping activities alone would take more time than it took us to get Tool4ever's solutions up and running," says Cacaro. "That type of project would be overkill for this company. We wanted a smaller company that could understand our needs, and help us scale at the correct level for our size, industry, and culture. We wanted to get a pilot project rolling that would show fast results."

That's when he found Tools4ever.

Discovery

The discovery process began around identity & access management, single sign-on, and password management.

But like most organizations, their team quickly found other gaps and frustrations. A big one was user lifecycle automation. Both IT and HR were tripping over manual account creation for new employees and contractors. As Cacaro reflects, the two departments weren't always on the same page about "who was working, when they started or terminated, or who was the manager." And once new accounts were created, they had no secure way to disseminate usernames and passwords.

To attack the problem, Haas settled on a phased implementation. They wanted to start with small, quick wins and build from there.

Getting Their Feet Wet

Ken Shannon, IT Infrastructure & Security Manager at Haas, set the stage with a team of committed employees from several departments. Their designated Tools4ever consultant, James Anderson, kicked off the project. He scheduled a bi-weekly call and created a shared to-do list.

Products and Connectors

- IAM (Identity & Access Management)
- PSM (Password Synchronization Manager)
- HelloID (Access Management (SSO) / Service Automation modules)
- SSRPM with Account Claiming (Self-Service Reset Password Manager)

SSO Applications

Jira (Atlassian), SAP, Wrike, UltiPro, DocuSign, Dropbox, KnowBe4, Zoom

IAM Integrations

AD, Exchange, SAP

CASE STUDY

Product: **HelloID, IAM, PSM, SSRPM, Service Automation** Sector: **Industry** Date: **2020**

"We wanted a smaller company that could understand our needs, and help us scale at the correct level for our size, industry, and culture. We wanted to get a pilot project rolling that would show fast results."

Vincent Cacaro
Security Lead at Haas Automation, Inc.

Haas started small, with password synchronization. Several instances in Haas' SAP environment weren't tracking AD credential changes. Developers had to log in to these systems manually, creating piles of burdensome reset tickets for the SAP admins. James drew his sword. After a quick implementation, Tools4ever's Password Synchronization Manager (PSM) began capturing all AD credential changes. It automatically synchronized them into all SAP systems. This generated immediate time savings.

Not All Fun and Games

With PSM in place, the team turned to user directory provisioning via IAM, Tools4ever's on-premises solution.

Well...almost.

The first rule in user provisioning is "garbage in, garbage out." After years of company growth and changing processes, Haas' HR data had become fragmented. So, they took the opportunity to future-proof their systems. This meant a deep dive into their personnel data in SAP. Haas updated everything, and swept out the cobwebs. They fine-tuned department structures and sub-structures. This was a keystone of success. It ensured that IAM could accurately provision every single employee, regardless of their position.

After data cleaning, James began the IAM implementation. He set up automated provisioning of all employees into a single directory system – in this case, Active Directory.

This phase required full buy-in from HR. Cacaro notes, "Without their participation and flexibility, none of this would have been possible." Haas IT Trainer/Documentation Specialist Kim Reed added, "Having HR as a central point of contact for onboarding and offboarding gives us tighter control over who has access. It eliminates the manual processes of creating user accounts or disabling terminated users. Using SAP as the system of record also eliminates errors, which have to be corrected after account creation."

Pause for Password Reset

With all employees now being provisioned from SAP into AD, Haas could tie in Tools4ever's Self-Service Reset Password Manager (SSRPM). They needed a web portal that would work for all employees, anywhere, any time, on any device – even employees without a designated workstation.

James made quick work of it. With IAM in place, it was easy to flip on SSRPM. Password self-service became available immediately. The IT support team could now divert password reset calls to the self-service solution. Better yet, SSRPM's Account Claiming module gave Haas a new, secure method of disseminating accounts. Now, when a new AD user is provisioned from SAP, SSRPM creates a secure account claim link. New employees can easily use the link to claim their account, set their own password, and enroll in the reset tool.

This was a complete 180 from their original process, says Mike Schilling, System Engineer II. Previously, "the helpdesk manually created a password that expired after the first login. They emailed it to the user. This process wasn't sustainable, especially this past year when the majority of our users were working from home. SSRPM, much like IAM, couldn't have come at a better time."

James reflects, "It was satisfying to hear the team discuss during our meetings that they were using the tools, trusting them, and they were working. Trust the tool!"

Easier Onboarding? There's Logic for That

The next step was to develop account provisioning logic for Haas' most important target systems – Exchange and a handful of SAP targets.

"The helpdesk manually created a password that expired after the first login. They emailed it to the user. This process wasn't sustainable, especially this past year when the majority of our users were working from home. SSRPM, much like IAM, couldn't have come at a better time."

Mike Schilling
System Engineer II at Haas Automation, Inc.

"Exchange was easy," explains James. "We simply built out rules that determine who gets a mailbox." SAP was trickier. "We built connector logic inside IAM that we could reuse across multiple SAP targets. Each employee needed access to a different set of targets." The goal was to create future-proof rules so Haas' team could add new SAP targets and define new triggers on their own.

James collaborated with Haas' SAP admins and developers to customize a handful of other features. He combined his IAM expertise with the team's expertise in Haas' local IT environment. Together, they tackled details, including custom user fields and login retry flows.

Pause for Password Reset

Before finalizing the IAM implementation, Tools4ever assisted Haas with an internal access audit. This allowed a clean mapping of departments onto file shares. It also provided the foundation of a company-wide access governance model. This step ensured all access would be role-dependent, and put an end to resource accumulation and permission creep.

Last Step – Single Sign-On

With users now being automatically provisioned into AD and all target applications, the final step was implementing Single Sign-On (SSO) via Tools4ever's HelloID Access Management module. HelloID allowed one-click access to all of Haas' applications, such as Jira, SAP, UltiPro, DocuSign, and more. And its conditional access policies let users on internal IPs authenticate without any logon at all.

Additionally, James deployed HelloID's Service Automation module to help IT staff add and remove users from AD groups. In the future, Haas plans to use Service Automation's approval workflows for their BYOD automation.

For the finishing touch, James integrated SSRPM's password reset widget into the HelloID dashboard. The team color-coded internal and external applications, a quick and easy convenience feature for end users.

Results

Haas has seen a lot in its 35 years. Their team takes its work seriously. Their responsiveness showed during the twice-weekly check-in calls. "The team was open to talking through processes and asking for ideas, input, or improvements for the future," recalls James. Their excellent communication helped the project succeed.

As a result, Haas is now more efficient in all its IT and HR personnel tasks. Resources are rapidly disseminated. User adoption and acceptance are up. Auditing is easier. User lifecycle management is completely automated. And, there are far fewer opportunities for security holes.

"We eliminated manual data entry. Spreadsheets, post-it notes, memories. . ." says Vince Cacaro. "The time needed for onboarding/offboarding is likely 25% of what it was before – with the added benefit of being correct."

Ken Shannon recalls: "Prior to implementing IAM and HelloID, we struggled with the workload and accuracy of manually creating and managing accounts in all our on-premise and cloud systems. I had considered hiring dedicated staff to handle the growing workload. But those concerns are nowgone. Our team can focus on providing better support to our end users." Kim Reed adds, "With all our employees in AD, we can move on to other solutions, such as Learning Management for our future training campaigns."

Reflecting on the unusual events of 2020, Schilling says, "We've seen a lot of users be put on a leave of absence and then return. IAM has saved us countless hours in user administration. The timing couldn't have been better."

Haas Automation Inc.