Netherland’s Top Research University Consolidates and Streamlines Privileged Password Management Processes using Password Manager Pro

Wageningen UR replaces traditional, hardcopy password management practices using ManageEngine Password Manager Pro; achieves improved operational efficiency & internal controls.

WAGENINGEN UNIVERSITY
WAGENINGEN UR

Business Challenge

Wageningen University and Research Centre (Wageningen UR), an institution of international repute in the sphere of Life Sciences, has many partners in both education and research in more than 70 countries across the globe. With over 6500 staff and 10,000 students, Wageningen UR has an innovative and sprawling campus.

For better integration of knowledge and exchange of ideas among academicians, students, researchers, research institutions, businesses and government agencies, Wageningen UR has been equipped with state-of-the-art Information and Communication Technology (ICT) tools, backed by a huge IT infrastructure comprising servers, databases and numerous IT applications.

Just like any other higher educational institution, Wageningen UR also deals with a huge collection of intellectual property, scientific literature, confidential data, research records, details about the staff and students and a host of other sensitive information. Needless to say, the IT department of Wageningen UR is tasked with the challenge of safe upkeep of disparate IT infrastructure, combating cyber-attacks, ensuring information security and network availability.

Fast Facts

Organization: Wageningen UR

Industry: Education

Location: The Netherlands

Business Challenge: Manual Password Management Processes like maintaining privileged passwords on paper in a safe proved highly inefficient and drove users to create individual password management solutions

Solution: ManageEngine Password Manager Pro

Why Password Manager Pro?

- Highly easy-to-use and cost-effective
- Rock-solid security; proven encryption standards
- Automatically resets passwords across remote systems enforcing standards
- Provision to selectively share passwords among administrators
- High-availability architecture

While ensuring uninterrupted access to courses, systems and research database across the globe for researchers, Wageningen UR's IT department had to keep in mind the potential security threats to intellectual property and other sensitive data. With security incidents looming large, effectively tracking and controlling privileged access to the IT assets became imperative.

"The privileged passwords that grant unrestricted access to disparate IT assets, had been kept on paper in a safe, which resulted in lack of centralized access controls. With many administrators working in the ecosystem, the admin access to shared resources could not be tracked to specific users. Enforcing standard password management practices became resource intensive and cumbersome. Above all, maintaining synchronization between the passwords on paper and remote resources was a big pain," explains Remon Klein Tank, Security Architect at Wageningen UR.

Being an active member of international security bodies like CERT, FIRST and others, Remon was well aware of the potential security threats associated with the practice of individual users creating their own means of storing passwords due to the restricted accessibility of the paper-based store in the vault.

"Before things went out of control, we wanted to replace the traditional, insecure practices and bolster internal controls," points out Remon.

Remon Klein Tank

Security Architect – IT Infrastructure,
Wageningen UR

> *"We are highly impressed by the rich functionality, ease-of-use, performance and security aspects of Password Manager Pro. It has turned out to be the winning choice for us and we would recommend Password Manager Pro to any IT department"*

The Solution

Remon and his team realized that controlling access to privileged passwords and automating the password management processes by deploying a Privileged Password Management Solution was the best thing to do to tackle the problems on hand.

When they started looking for a solution, they had some important considerations on mind. They expected rock-solid security, proven encryption standards, flexible-yet-powerful authentication options (including two factor authentication with support for hardware tokens) and high availability architecture, in addition to the capability to solve all their password management owes.

"Moreover, we wanted the solution to be highly easy-to-use and cost-effective," says Remon.

After an initial evaluation, Remon and team shortlisted two vendors – ManageEngine Password Manager Pro and Cyber-Ark Enterprise Password Vault. Following a careful evaluation and test deployment, they zeroed-in on Password Manager Pro.

"Though both the products were equally capable and met all our requirements, we chose Password Manager Pro as it proved highly intuitive for our password users," remarks Remon.

"We were highly impressed by the rich functionality, ease-of-use, performance and security aspects of Password Manager Pro. The top-notch technical support enabled us deploy the product to production in quick time," recalls Remon.

Password Manager Pro Difference

Of the many features of Password Manager Pro that are proving highly valuable at Wageningen UR, the automatic, remote password synchronization capability is of specific importance. "In our shared IT ecosystem, privileged passwords often remained unchanged. Enforcing password resets proved cumbersome. Now, with Password Manager Pro, all those issues have vanished. Password Manager Pro automatically randomizes and synchronizes passwords of remote, Linux-based IT resources at periodic intervals. We now have a perfectly policy-driven password management approach in place," says Remon.

> *"Password Manager Pro automatically randomizes and synchronizes passwords of remote IT resources at periodic intervals. We now have a perfectly policy-driven password management approach in place"*

Grouping passwords and assigning granular access rights on a per user basis was another critical requirement for Wageningen UR. "Provision to create resource groups and share specific groups with specific users with 'view only' or 'view and modify' permissions is very useful for us. We are now able to easily share a group of passwords to different users and administrators with the required permissions," points out Remon.

The 'password masking' feature of Password Manager Pro is much liked at Wageningen UR. "While talking about information security, we should never overlook the human angle – anti shoulder surfing measure is a necessity. Option to restrict users from viewing the passwords in plain-text while allowing them to launch direct connection to remote resources and permitting users to copy the passwords to the clipboard is very useful in combating shoulder surfing," observes Remon.

Provision to add custom fields has come in handy for Wageningen UR. "By adding custom metadata like password creation date, purpose of account and other labels, we are able to identify the resources easily," adds Remon.

With thousands of students, staff and researchers dependent on network availability and IT services, uninterrupted access to passwords is indispensable. "The high availability architecture with redundant servers is very useful. In addition, the provision to run the software and connect to the web-interface in local machine helps in getting access to passwords even when there is a network failure," explains Remon.

Real-time notifications on password access, modification and other events have helped Wageningen UR get total control on the Privileged Password Management Process. "When a user retrieves a shared password, other admins are instantly notified. The comprehensive audit trails reveal 'who', 'what' and 'when' of all actions. We are in total control," says Remon.

As researchers in Wageningen UR keep turning their attention on the myriad aspects of life sciences, food production, environment and health, lifestyle and livelihood sectors, the IT infrastructure of the institution constantly keeps growing. Strong, secure and efficient IT services has become paramount. "The number of privileged passwords is growing exponentially. Password Manager Pro helps us streamline and consolidate the password management processes with ease," says Remon.

> *"The number of privileged passwords is growing exponentially. Password Manager Pro helps us streamline and consolidate the password management processes with ease"*

“We are very pleased to have Password Manager Pro. Our interactions with the technical support have been very effective. Password Manager Pro not only satisfies all our requirements, but has also resulted in improved operational efficiency and internal controls. Password Manager Pro has turned out to be the winning choice for us and we would recommend Password Manager Pro to any IT department,” declares Remon.

About Wageningen UR

The Wageningen University and Research Centre (Wageningen UR) is an important international player in education and research in the fields of life sciences, natural resources and agriculture. It is a collaboration between Wageningen University, Van Hall Larenstein University of Applied Sciences and the specialised research institutes and is based in Wageningen, the Netherlands. About 6,500 staff and more than 10,000 students from over 100 countries are pursuing research in the domain of healthy food and living environment for governments and the business community-at-large.

www.wur.nl

About Password Manager Pro

Password Manager Pro (PMP) is a web-based, **Shared Account Password Management Solution** for enterprises to control the access to shared administrative passwords of any 'enterprise resource' such as servers, databases, network devices, applications etc. PMP enables IT managers to enforce standard password management practices such as maintaining a central repository of all passwords, usage of strong passwords, frequent changing of sensitive passwords and controlling user access to shared passwords across the enterprise. It is available at costs affordable to SMBs.

www.passwordmanagerpro.com

ManageEngine

Phone: 1-800-425-5558 **Website:** http://www.passwordmanagerpro.com

For Queries: passwordmanagerpro-support@manageengine.com