

ANDRITZ GROUP Integrates SSH Solutions for Large Scale Two-factor Authentication

ANDRITZ GROUP integrated SSH MobileID with VPN access to provide an intuitive, administration-free, and tokenless two-factor authentication for its mobile workforce and partners.

ANDRITZ GROUP

ANDRITZ GROUP is a global market leader for customized plant systems, as well as services for hydropower, the pulp and paper, steel and other specialized industries. The Group is headquartered in Graz, Austria with approximately 14,300 employees worldwide. It develops and markets high-tech systems at its production, service, and sales sites all around the world.

Customer Challenge

ANDRITZ employs a global mobile work force and a vast partner network. It manages not only its internal remote users, but also subcontractors and customers who require access to headquarter infrastructure via Virtual Private Network (VPN) remote access.

ANDRITZ faced the challenge of finding a solution to authenticate a large number of users in a manner that was cost-effective and effortless to deploy.

Finding a Solution

One of the benefits of SSL VPN-based remote access products is the ability for an administrator to grant access to anyone, from anywhere, using nearly any device. For a company the size of ANDRITZ, the SSL VPN appliances provided great agility in terms of establishing remote connections, but also created challenges in granting access.

One approach would have been to introduce hardware tokens for remote user authentication, a common solution for companies of all sizes. However, the SSL VPN access would no longer be available anywhere anytime. This drove ANDRITZ to seek not only more agile, but also more cost-effective two-factor authentication methods.



Customer: ANDRITZ GROUP

- **Industry:** Manufacturing
- **Employees:** 14,300
- **<http://www.andritz.com/>**



Meeting ANDRITZ's Requirements

ANDRITZ faced a number of authentication requirements:

- 1. Seamless integration with SSL VPN appliances and leveraged security through the use of two-factor authentication.***

SSH MobileID not only seamlessly integrated with ANDRITZ's SSL VPN appliances, but also with the ANDRITZ GROUP domain controllers, making the migration process virtually free of any IT amendments.

2. On-demand availability with no manual provisioning or activation steps.

Going “on-demand” was one of the key criteria for ANDRITZ, for several reasons, one being the ability to circumvent the heavy administrative costs associated with traditional two-factor authentication methods such as hardware tokens. Another reason was to avoid excessive help desk loads. ANDRITZ’s SSL VPN users are geographically widely dispersed and unless the authentication process was as help desk-free as possible, the overhead involved in servicing end user support requests could have quickly become overwhelming.


SSH MobileID provided ANDRITZ with two SSL VPN authentication methods, both of which are fully on-demand and require no help desk intervention:

- An on-demand one-time password sent via SMS text.
- A list of one-time passwords sent automatically when needed, typically via SMS text.

3. Easy and intuitive to use, with no additional or intrusive authentication steps or downgrades in the existing login experience.

By default, ANDRITZ’s SSL VPN appliances authenticated through domain usernames and passwords. While this was not necessarily the most secure login mechanism, it provided an intuitive and user-friendly way for an end user to log in.

SSH MobileID provides the most intuitive and least disruptive end user login experience. Moreover, end users do not need to remember any new PINs or passwords nor carry any new authentication devices such as key fobs.



“We wanted to improve the level of security in our SSL VPN remote access, but without adding extra overhead on people using the service.”

*Juhani Eronen
Manager, Networks
ANDRITZ Finland*

4. Pricing that allowed changes in user volume.

With new power plants under construction, paper manufacturing lines being installed, projects being completed and closed – all activities that require new users to be added and others to be removed — the number of authenticating SSL VPN users had to adjust to monthly changes, rather than being fixed to a pre-defined volume.

SSH MobileID provided a dynamic subscription model for ANDRITZ. It allows the entire ANDRITZ GROUP to be eligible for SSH MobileID authentication, but only the active users will consume the license. This allows ANDRITZ to effectively circumvent all up-front investments and avoid idle authentication server licenses.

How does it work now?

The end user experience remained simple:

- 1. The user logs in to the SSL VPN using his/her normal domain username and password.**
- 2. If the username and password are correct, the SSL VPN prompts for an additional verification/PIN code.**
- 3. The user receives the verification/PIN code via SMS text message, types it in, and is logged in.**