Cyolo | Last_Mile

CASE STUDY

How Lillehammer Municipality Improved the Security of its Water and Wastewater Operations

A growing number of Norway's water and wastewater facilities are managed digitally. Many of these systems were built in an earlier era and no longer meet today's requirements for security and stability, let alone remote access.

When older infrastructure such as mobile communications systems, servers, and firewalls needs to be replaced, municipalities face an important choice: simply rip and replace the old solution — or take the opportunity to build safer and more future-ready alternative?

Lillehammer Municipality's Water and Wastewater Department chose the latter. Now, they are sharing their experience and advice for others facing the same decision.

Why Remote Access via VPN Was No Longer Secure Enough

Lillehammer Municipality manages around 80 pumping stations and facilities via remote access, and the risk of cyberattacks had grown too high to ignore.

Knut Olav Bakke, Automation Engineer for Water and Wastewater, recognized that their old VPN-based remote access solution, which relied on a single password, was not sufficient to prevent attacks or meet emerging regulatory requirements such as NIS2.

"We know that other water and wastewater organizations in Norway have been attacked. That is a reality we have to take seriously," said Bakke.

As the requirement for stronger security grew more pressing, the municipality decided that a new solution would need to include, at a minimum, two-factor authentication for all remote access.

From Outdated Technology to a Future-Ready Solution

Remote communications technology has evolved over many years. In the case of the Lillehammer Municipality, the initial goal of remote access was primarily to gain greater visibility and give partners remote access to its OT resources. Today, the focus is increasingly on ensuring stable and secure operations.

With the municipality already planning to upgrade much of its infrastructure, the water and wastewater department took advantage of the chance to make a bigger change.

After a previous unsuccessful attempt with another provider, finding the right partner for the project became crucial.

Why Lillehammer Municipality Chose to Partner with Last Mile and Cyolo

In operational technology, there is no such thing as a "one size fits all" solution. A remote-login tool that works in an office environment will not necessarily meet the needs of a facility that must deliver water around the clock. Such environments require solutions designed specifically for operationally-critical settings — as well as people who truly understand how they need to work in practice.

Lillehammer Municipality's Water and Wastewater Department already had a strong working relationship with Last Mile, including around operations and control-system solutions for OT. This trust, combined with Last Mile's technical understanding, became a decisive factor in the municipality's choice to work with Last Mile and the Cyolo solution for secure remote access.

"Last Mile has a strong understanding of how we work, what our needs are, and they understand both the technology and our day-to-day reality,"
said Bakke.

How Lillehammer Municipality Ensured a Successful Transition

The way Lillehammer Municipality's Water and Wastewater Department managed the transition is a strong example of how to make such a change safely and bring everyone along:

- **Parallel operation:** The old solution was kept as a backup while the new Cyolo remote access solution was rolled out.
- **Gradual rollout:** Instead of training everyone at once, employees were prioritized and trained one by one.
- **Simple training:** Each person needed no more than two hours to become comfortable with the new system.

A More Secure Day-to-Day Experience — Without Extra Work

The change to employees' daily routine after adopting the Cyolo access solution was minimal: they now use a standard web browser and their phone to confirm login.

However, the difference in security and visibility has been significant:

Improved security: Two-factor authentication helps prevent unauthorized users, both external and internal, from gaining access to critical systems. The solution also includes a supervisor function that makes it possible to monitor the entire session in real-time.

Full visibility: A new logging function provides complete control over who has logged into which equipment, and when. In addition, the solution provides control over external files by checking and sanitizing data via internal security mechanisms.

Data sovereignty: The Cyolo solution has a unique decentralized architecture and adheres fully to the zero-trust model, meaning that all information and data remains stored within the municipality's OT network. This is different from other access solutions that may store data in the cloud.

Positive user experience: The solution has worked without issues, and users log in through a standard web browser.

Simpler troubleshooting: The solution makes it much easier to troubleshoot by enabling direct connection to equipment out at the stations, saving significant time.

Non-disruptive deployment: During installation, there was also no need to change the setup of the existing infrastructure, such as firewalls.

Convenient integrations: The solution offers many possibilities through open APIs for integration with other applications, such as logging, SIEM/SOC solutions, Active Directory, and IAM solutions, making it easy to integrate with the municipality's existing systems.

Compliance-readiness: The solution also aligns with both new and establish regulatory requirements and standards, including NIS2, ISO 27001, and IEC 62443.

With the Cyolo remote access solution in place, the team has gained better control over remote access, as well as greater peace of mind in their day-to-day operations.

"The biggest difference now is that we sleep a little better at night. We know we have a more secure solution for ensuring remote access to our most critical systems."

Lillehammer's Advice to Other Municipalities

Based on their experience with Last Mile and Cyolo, Lillehammer Municipality's Water and Wastewater Department has some clear advice for others facing similar challenges around secure remote access:

- **Explore the market:** Start by learning where others have succeeded and who they succeeded with.
- **Know your own systems:** It is important to understand where your vulnerabilities are and what is most important to protect.
- **Start carefully:** Begin on a small scale, then create a strong plan for adoption and internal training.

Considering a More Advanced Secure Remote Access Solution?

Too many water and wastewater organizations are still using solutions that fail to meet today's more stringest security and compliance requirements. Last Mile and Cyolo can help you identify practical next steps — whether you want to start small or take a broader approach.

This case study was written by Stig Mortverdt of Last Mile and is based on an interview with Knut Olav Bakke, Automation Engineer at Lillehammer Municipality.

About Last Mile

Last Mile is Scandinavia's leading provider of communication, IoT, and security solutions for industrial environments on land and at sea. The company delivers its solutions primarily through authorized competence partners across Norway, offering everything from design and products to consulting, managed services, and training. In selected industries, Last Mile also works directly with end customers to deliver tailored solutions for critical infrastructure and operational technology environments.

About Cyolo

Cyolo provides secure remote privileged access for cyber-physical systems (CPS) and operational technology (OT). Our solution enables industrial enterprises to connect employees and third-party vendors to critical assets in a way that's safe, secure, and surprisingly simple. Cyolo delivers improved security, productivity, and operational agility – without compromise.

Request a demo to learn more:

cyolo.io/demo