

ESIS

One of Denmark's largest education IT providers finally solved permanent admin rights across 10,000 endpoints

ESIS is one of Denmark's largest providers of IT services to the educational sector, supporting 17 schools that together span around 60 locations, and keeping the digital infrastructure running that Danish students and teachers depend on every day.

Industry:

Education / IT Services

Number of Employees:

ca. 6,000

Operating System:

Windows & macOS, distribution varies across schools

Endpoints on ABR:

10,000

ESIS
ERHVERVSSKOLERNES IT SAMARBEJDE

The Challenge

Before Admin By Request, every user at ESIS had full local admin rights: employees, teachers, and students, all the time. Students installed whatever caught their eye, teachers experimented with course software, and machines drifted from their configured state within days. IT had no visibility into what was running and no log to investigate with when something broke. The practical cost was constant reimaging, with entire sets of classroom machines rebuilt every month, burning IT time on work that served no educational purpose.

The risk went deeper than housekeeping. Schools aren't high-value targets, but they're accessible ones, and attackers use a compromised school machine as a springboard, exploiting admin rights to move laterally toward the next target. With every user a local admin on every machine, one compromise put the whole estate in reach, something ESIS's sister institutions had already lived through.

ESIS had tried to fix this before. One earlier tool was binary, admin or not, which fails where teachers need course software, IT educators need real capability, and students need some access but not all of it. Another was little more than a button that handed over admin rights with no

approval, no log, and no visibility, barely different from permanent rights.

The Solution

What made Admin By Request fit was the ability to move past all-or-nothing. Its sub-policy architecture lets each group get exactly what it needs: administrative staff get modest elevation, teachers install course software without calling IT while keeping autonomy over their own machines, IT educators get more capability, students are limited but not blocked, and kiosk PCs are locked down completely. No previous tool could tell those populations apart on the same network.

The rollout was deliberately permissive at the start. Rather than clamping down on day one, policies let users request elevation and state a reason, giving IT immediate data on what people actually needed. That data drove the tightening over time: pre-approving what was genuinely needed, restricting what wasn't. The transition felt gradual to users instead of an overnight removal of something they'd always had.

All privileged access now runs through the tool as the single gateway to admin rights, which closes the gaps other approaches leave open. When the Print Nightmare vulnerability landed, requiring admin rights to install printer drivers across 10,000 machines, ESIS simply pre-approved driver installation: the user clicks yes, the driver installs, and no admin rights are left behind. A problem that could have paralyzed printing estate-wide was handled quietly.

Rolling out across the first 6,000 to 7,000 clients took about six months, and the technical side was never the bottleneck. The time went into convincing schools and local IT teams to change how they'd worked for years, after which deployment moved fast, with local staff managing their own environments inside ESIS's framework. The Inventory module became an unexpected win too, turning into a core tool for security analysis and, during the Windows 10 to 11 migration, a live view of progress nothing else could match.

The Impact

Classroom machines that once needed monthly rebuilds are no longer a worry. As Mads Schack Kahl put it: "We have almost no problems with endpoint compromise now. And when something does happen, it's something trivial, a browser pop-up, nothing that's actually been installed. That's not what we're worried about anymore." The lateral movement risk is gone at the root, because a user who isn't a permanent admin can't move freely across the network.

The bigger payoff is time. In education, IT resources are perpetually thin, since schools invest in teaching, not IT headcount, so every hour spent reimaging a classroom is an hour not spent helping a teacher whose laptop died before a lesson. With endpoint management now running largely on its own, local IT has that time back.

"The core task is helping the people out in the schools, teachers and students who need support. That's what they're there for. If they spend all their time on infrastructure, they don't have time to help anyone when it actually matters."
~ Mads Schack Kahl, System Consultant, ESIS

Removing admin rights from an estate this varied had long been considered undoable at ESIS, because the binary tools on offer meant either locking people out or leaving security gaps that made the effort pointless. Admin By Request made a previously impossible objective



achievable without adding IT resources to sustain it. ESIS isn't subject to NIS2 but operates under GDPR and the Danish state's minimum IT security requirements, one of which requires that users aren't administrators on their own machines, a rule long impossible to meet in practice and now met as a matter of course.

Moving Forward

Attention is turning to the server side. ESIS manages more than 700 virtual servers, and external consultants like heating and building-management engineers regularly need access to them through openings wider than they should be. ESIS has already seen what happens when a supplier is compromised and that reaches inward, so giving those consultants precisely the access they need, for exactly as long as they need it, with a full audit trail, is on the list.

Connected to that, remote support today relies on a tool that makes local IT read out a long alphanumeric code before every connection, friction that adds up across 700 servers and daily requests. Since the Admin By Request client is already deployed everywhere, Secure Remote Access offers a way to cut the step entirely: IT initiates, the user confirms, and the session opens.

Longer term, ESIS is also weighing Linux support as data sovereignty rises up the EU agenda, valuing the option to manage Windows, macOS, and Linux under one tool and to put machines too old for Windows or macOS back into service as the student loaners it's legally required to provide.

> “Before Admin By Request, we were reimaging entire sets of classroom computers every month. Today, we almost never have problems with endpoint compromise.
> Our local IT staff used to spend a disproportionate amount of their time just getting machines back to a working state. Now they can focus on what they are actually there for: being available when a teacher or student needs help. And all of that was achieved without adding a single extra resource to IT. In an education sector that is permanently understaffed, that makes all the difference.”
>
> Mads Schack Kahl, System Consultant, ESIS

Admin By Request
ZERO TRUST PLATFORM

