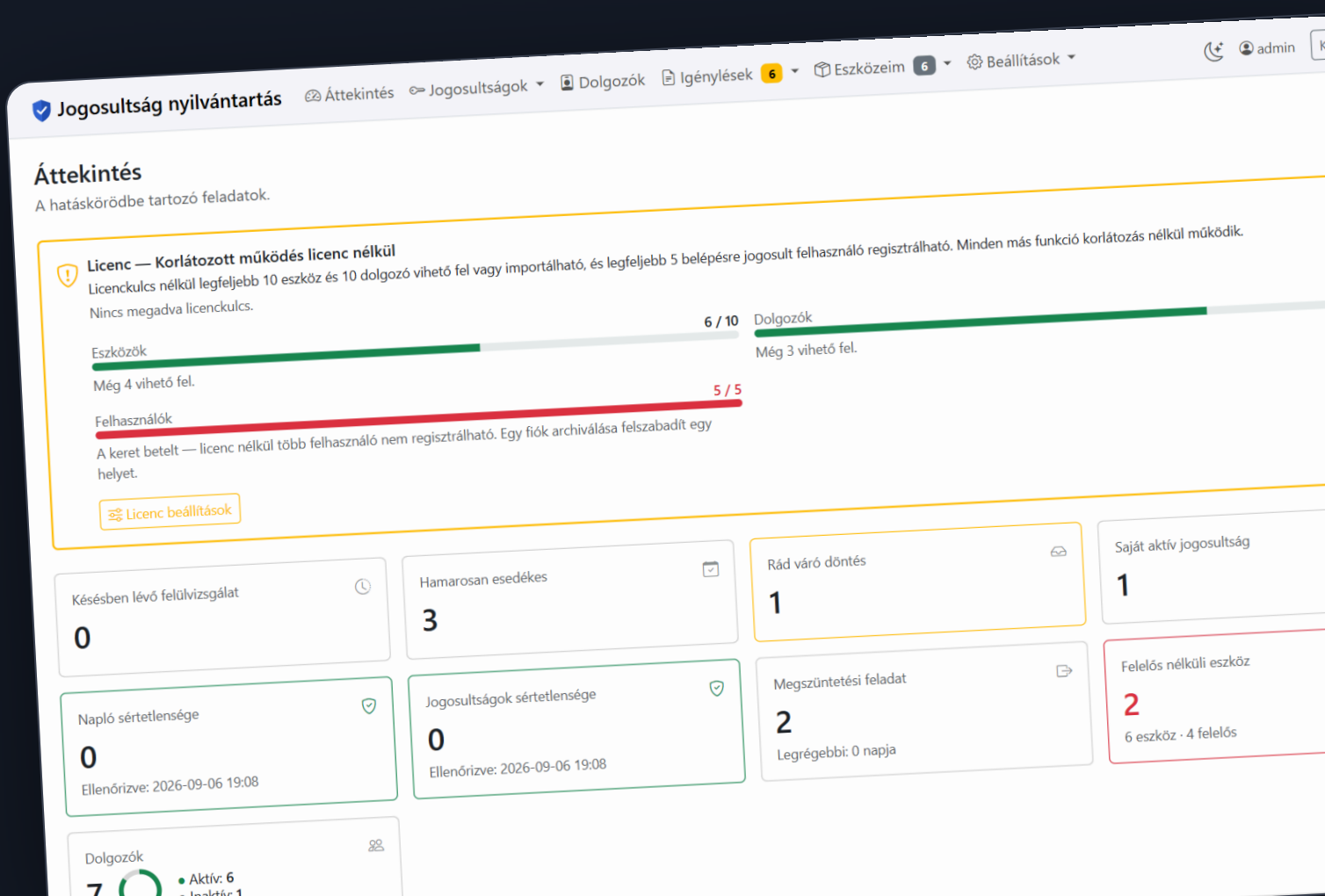
ACCESS RIGHTS REGISTER · NIS2

devnullsec
Borics Krisztián e.v.

Behind every access, there is a decision, and you can prove it.

The Access Rights Register follows every permission through its whole life, from the request to its removal from the real system, with an audit log sealed by HMAC, so that at your next audit you can show instead of explain.

Request and approval · Periodic review · Deprovisioning tasks · Tamper-evident audit log



WHY YOU NEED IT

A spreadsheet is not evidence.

NIS2 does not ask whether you have a list of permissions. It asks who decided on each access, when someone last reviewed it, and whether a leaver's access was really removed from the actual system as well. A hand-kept spreadsheet can only promise answers to these questions, while this system gives you evidence.

5

stages on one timeline

Request, approval, active permission, review and termination, each with a name and a date.

6

termination reasons, handled automatically

On expiry, departure, account lockout or asset retirement, the system revokes on its own and opens a task.

30'

background sweep every 30 minutes

Expiring and due permissions move to the right branch even without human intervention.

What the system covers from the NIS2 access management requirements

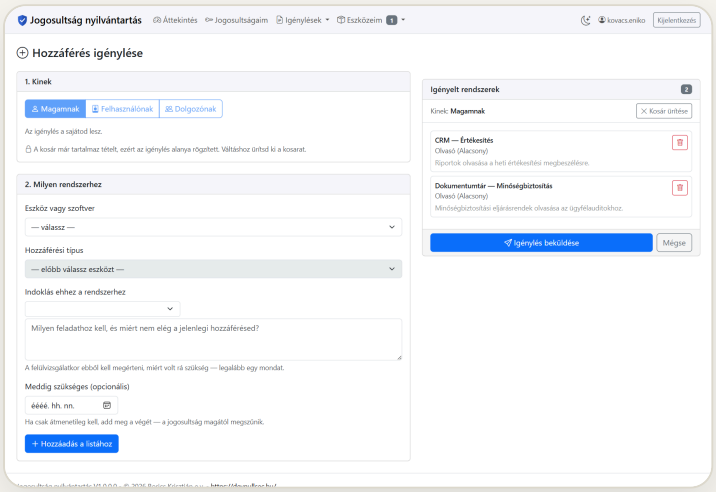
- ✓ **Asset catalogue** with an owner, a deputy and a criticality level for every system that requires a login.
- ✓ **Request and approval** with justification and a conflict-of-interest rule, so nobody decides on their own case.
- ✓ **Access and asset matrices** that are always up to date and export to Excel.
- ✓ **Periodic and campaign-based reviews** on the asset owners' task lists.
- ✓ **Deprovisioning task list** that stays open until the access has also been removed from the real system.
- ✓ **HMAC-sealed audit log** whose integrity can be verified at any time, even in front of the auditor.
- ✓ **Critical security events** reported immediately: MFA policy changes, integrity failures, blocked IP addresses.
- ✓ **Subcontractor management** per company, tied to the contract end date.

> An audit reveals whether a register is actually used or merely kept. This system was built for the former.

THE LIFE OF A PERMISSION

From the request to the actual removal.

1	2	3	4	5
Request	**Approval**	**Active**	**Review**	**Termination**
for myself, a colleague or an employee	the approver decides, with justification	in the matrix, sealed with HMAC	keep or revoke	a task, until it is gone from the real system



Basket-style request: several systems for one person at once, each with its own justification.

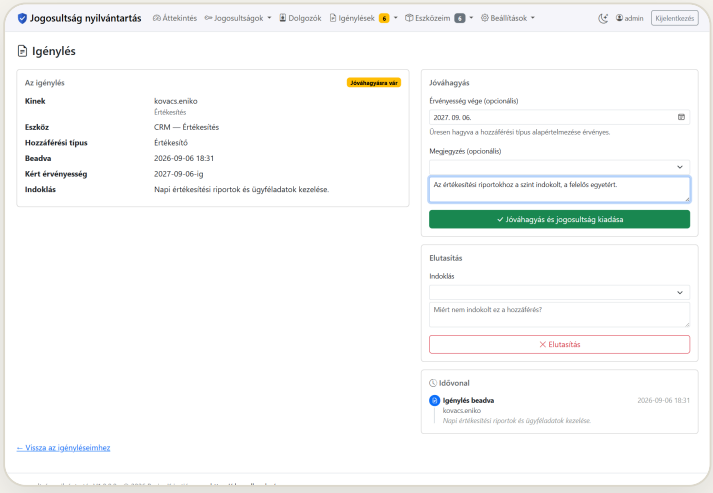
Requests that still make sense six months later

The requester collects a person's complete access package in one basket, so the approver sees at once how much access is being granted. Behind the scenes a separate request is created per system, so one rejection does not take the others with it.

- ✓ Mandatory justification, sped up with templates
- ✓ Time-limited access that expires on its own
- ✓ Can be requested for employees without an account and for subcontractors
- ✓ The subject is locked in the basket, so it cannot be swapped by accident

One screen for the decision

The approval queue shows the items the signed-in approver is allowed to decide on. The system excludes their own requests and those concerning them, and an approval immediately issues the access and adds it to the matrix.

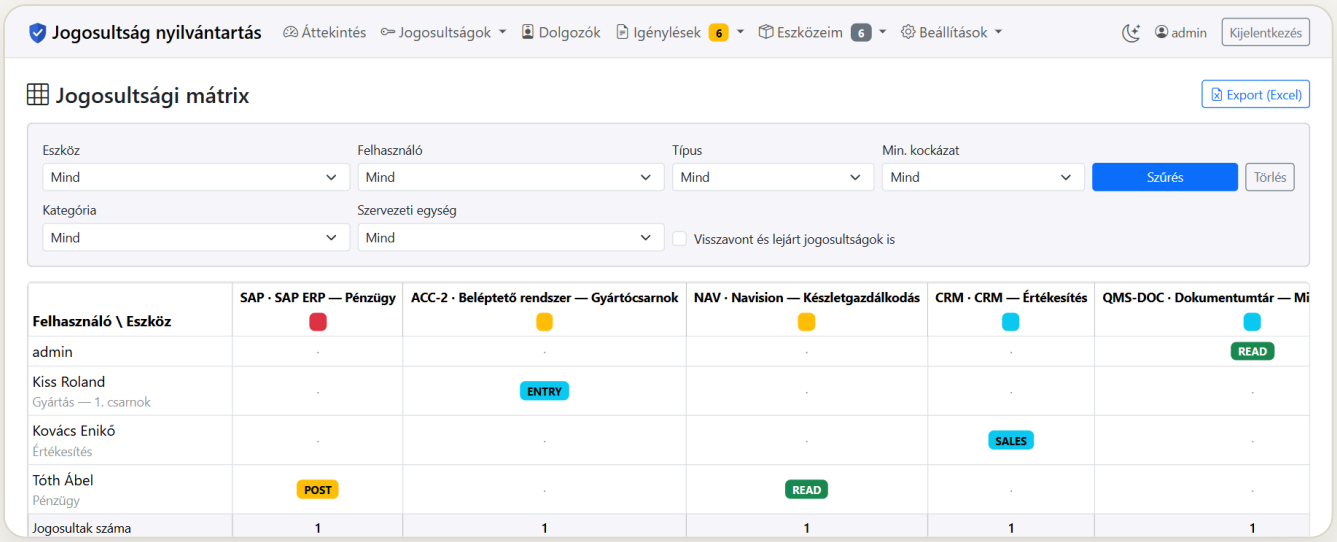


Reviewing a request with an expiry date and a note.

TRANSPARENCY

One glance shows who can access what.

The access matrix sets users against assets, colour-coded by risk. The asset matrix shows who owns each system and where a deputy is missing. Both can be filtered and exported to Excel with a single click.

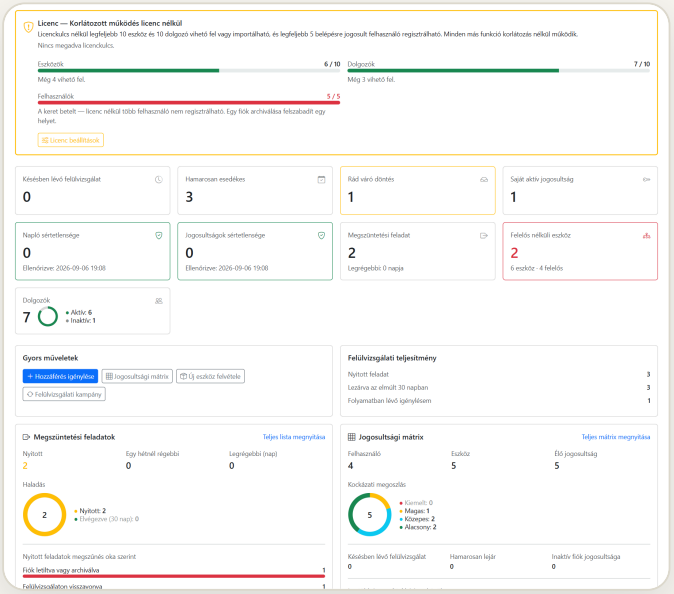


Access matrix: a red frame marks an overdue review, the hourglass marks access that will expire soon.

Five minutes each morning on the Overview

The personalised dashboard only shows the cards the user actually has work on: decisions waiting for them, overdue reviews, open deprovisioning tasks and the two integrity indicators.

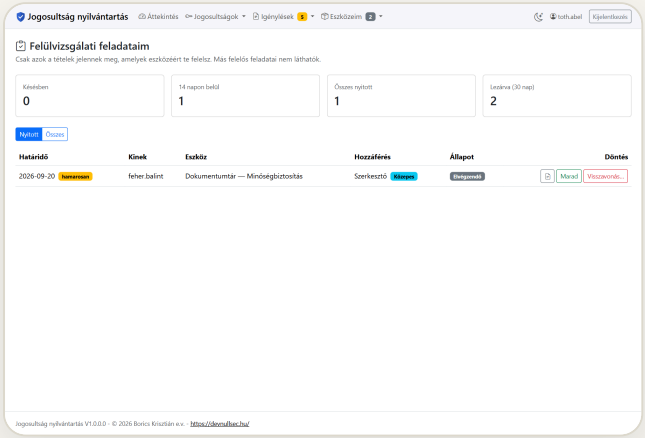
- ✓ Need-to-know filtering in every view
- ✓ Assets without an owner highlighted
- ✓ Live list of signed-in users



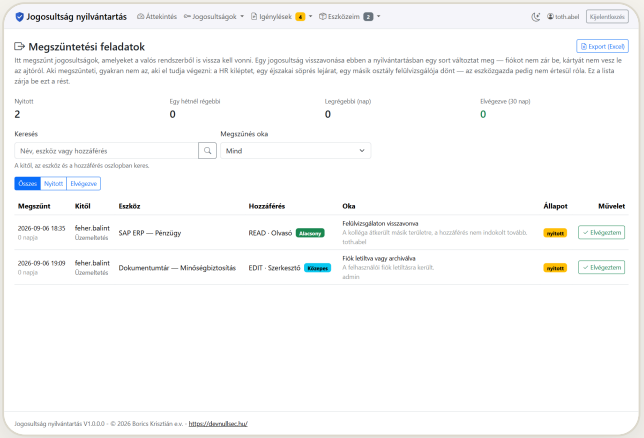
CONTINUOUS CONTROL

Revoking is not the same as removing.

Most registers stop exactly where the real risk begins: at changing a row. Here a revocation opens a deprovisioning task for the asset owner, and the access only counts as terminated once someone has actually removed it from AD, the ERP or the application.



Reviews from the asset owner's view: "Keep" is one click, while revoking always asks for a reason.



An open deprovisioning task: SAP access revoked in a review, still waiting to be removed.

Recertification that comes full circle

At an interval matched to the asset's criticality, the task appears on the owner's list by itself. After a reorganisation, an ad hoc campaign can be started for one asset or for the whole catalogue.

Six reasons, one list

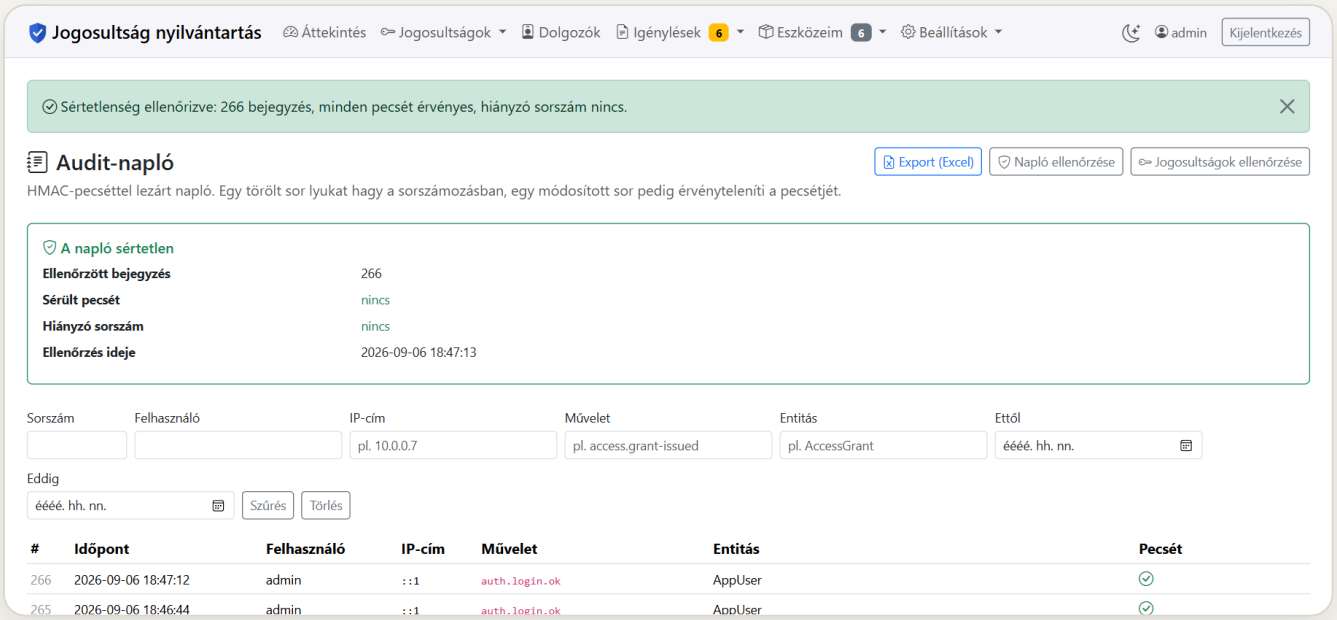
Manual revocation, expiry, a review decision, account lockout, an employee leaving or an asset being retired: whichever happens, the asset owner is notified, and the closing note is written to the log.

> Automatic closure would only prove that the program ran. A human closure states that someone actually checked.

INTEGRITY

A register that notices when someone tampers with it.

Every request, decision, revocation and settings change enters the audit log with an HMAC seal. A deleted row leaves a gap in the sequence numbers, a modified row invalidates its own seal, and the system recalculates all of it at the press of a button.



Integrity check: 266 entries, every seal valid, no missing sequence numbers.

Mandatory MFA

A global switch for authenticator-app two-factor authentication, with recovery codes shown only once.

Encrypted fields

Names, e-mail addresses and TOTP keys encrypted at field level, with managed key rotation and key destruction.

Two brakes

Account lockout after five failed attempts, IP blocking after ten, a short idle timeout and silent session extension.

ORGANISATION

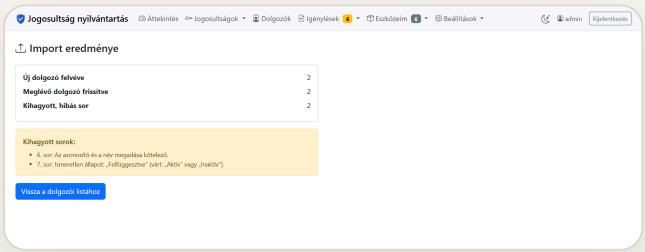
Everyone gets exactly what they need.

Six roles, exactly one per account. The question "what can this person do?" is answered at a glance, with no permissions to add up.

Role	What they can do
User	Requests for themselves and for employees without an account, and reviews as an asset owner.
Key user	Also requests on behalf of colleagues with an account, but does not decide.
Approver	Decides, revokes and sees both matrices.
Administrator	Catalogue, users, settings, audit log, keys and campaigns.
HR	Maintains only the company's own employee list.
Subcontractor HR	Manages the list of a single partner company and sees nothing else.

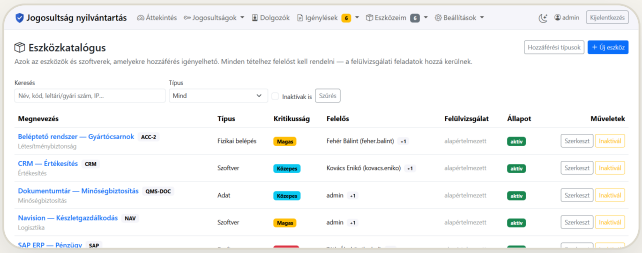
Employee list from Excel

Not every employee needs an account: HR imports the list from Excel, and managers can request access for colleagues without one. When an employee is set to inactive, their permissions end immediately.



Subcontractors tied to their contract

A separate list per partner company, with its own HR account. When the contract expires, the daily sweep closes the company, its people and all their access, and the company name stays visible on the request, in the matrix and in the exports. Subcontractor headcount does not use up licence capacity.



Asset catalogue with type, criticality, owner and review cycle.

AUDIT-READY

Don't claim it is in order. Show it.

An auditor typically picks a few live permissions and traces them back to their origin. The system has a single screen for exactly this: the permission's timeline, with a name and a date at every step. The evidence is handed over in four exportable layers.

State

Who can access what right now? Both matrices in Excel.

Process

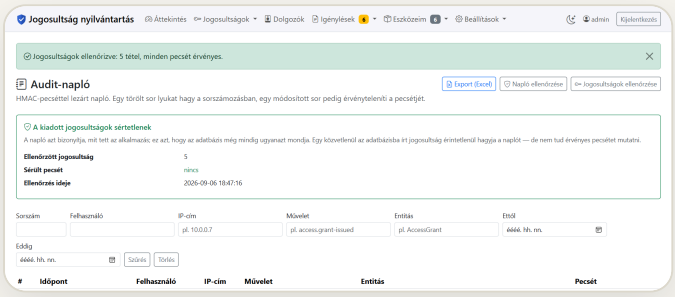
Who decided, when, and on what basis? Requests and reviews.

Log

Is the register authentic? Sealed audit log with export.

Configuration

What rules does it run by? Settings and key inventory.



The strongest moment

Run the integrity check live, in front of the auditor, on both the log and the issued permissions. That is the difference between claiming the register is intact and proving it on the spot.

Try it without a licence

Without a licence key, every feature works without restriction for up to 10 assets, 10 employees and 5 users, so you can start the rollout without risk.

Let's get your access rights in order before your next audit.

Request a demo, and in one hour we will walk through how the system fits the way your organisation works, from setting up the catalogue to the first review campaign.

devnullsec.hu