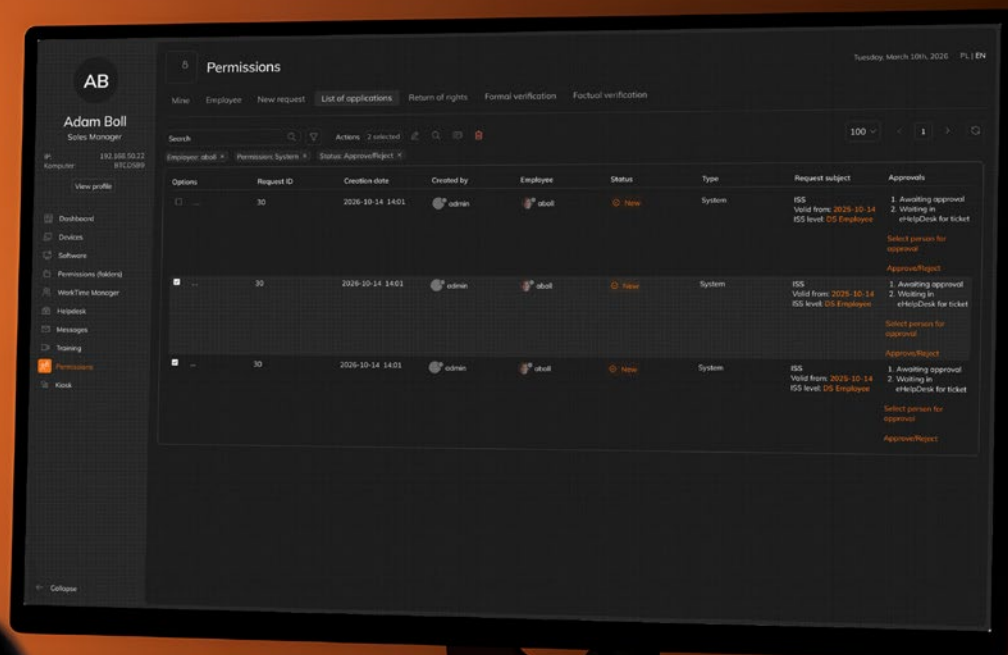




eauditor. IAM

Identity and Access Management System for IT Resources

eAuditor IAM covers the full lifecycle of employee permissions: from the creation of the first account and profile assignment, through temporary role extensions, to the automatic revocation of access upon leaving the company. Everything in one place, fully auditable, with minimal burden on the IT department.

REQUEST • APPROVE • REVOKE • AUDIT

Benefits of implementation



Regulatory compliance

UKSC2 / NIS2 / ISO 27001 / DORA / KRI

The system directly meets the requirements of Article 8 of UKSC2 (access control, MFA), NIS2, ISO 27001, DORA, and the National Interoperability Framework: least privilege principle, recertification, identity lifecycle (JML), 2FA, and a complete audit trail.



Less operational work in IT

Requests are automatically routed to the appropriate person. Approval, execution in Active Directory, and email notifications – all without manual processing by administrators.



Audit-ready at all times

Every change in permissions is recorded. Periodic reminders ensure verification of granted access. Operational and strategic reports can be generated in just a few clicks – ready for auditors and regulators.



Fewer excess privileges

Two-step verification, temporary permissions, and self-service access return by employees reduce privilege creep and orphaned accounts.



Continuity despite absence

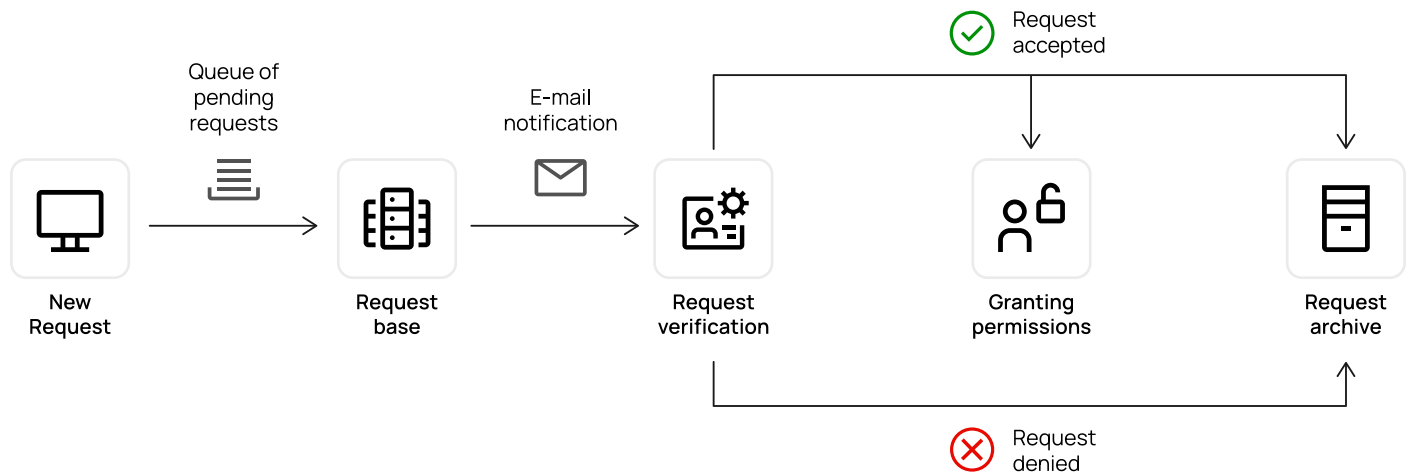
Vacations, sick leave, business trips – the system automatically assigns a substitute and forwards requests and approvals. The process never waits for the decision-maker's return.



System Flexibility

Full configurability during implementation – records, permission definitions, and approval workflows can be created without programming. The system supports access not only to applications, but also to production machines, rooms, or equipment.

System features



Access management

Access request

A form with dynamic fields, application or permission profile selection, validity period (from-to), and change history. Approval via the dashboard or directly from an email.

Approval templates

Definable approval paths based on Active Directory data (login, position, department). A single template can handle multiple request types and automatically identifies the appropriate decision-maker.

Initial access audit

Import of existing permissions from source systems and Active Directory, with two-step verification (formal approval by a manager, actual verification by IT).

Periodic Recertification

A schedule of automated access reviews. The system reminds managers to verify current access rights of their teams. Each cycle ends with a report.

Automation and integration

Automatic permission provisioning

Once the application is approved, the system runs PowerShell scripts that grant access—from domain accounts to resources and email inboxes.

Two tools in one – IAM and eHelpDesk

Once the application is accepted, the system automatically generates an implementation request to the appropriate support group – without copying data between systems.

Access and continuity

Employee Panel

A web-based application accessible from the computer's desktop—no need to log in again. Domain SSO recognizes the logged-in user. Employees can view their permissions, submit applications, and track their status.

Absence and substitution module

Absence calendar with automatic designation of a replacement and linking to the request approval process. For fixed-term employees, the system blocks requests that extend beyond the employment period.

What does the implementation look like?

1

We get to know your organization

We meet to determine which systems should be covered by access management, who approves requests, and what the decision-making workflows look like in your organization. The result is a process map tailored to your needs.

2

We implement the system in your environment

The installation is carried out remotely within your infrastructure (on-premise). We configure records, permission definitions, and processes.

3

We conduct the “initial inventory” – baseline audit

We collect current permissions from source systems and Active Directory and perform two-step verification. After this stage, for the first time in the organization, you gain clear visibility into who has which access – and who actually should have it.

4

We support you after go-live (SLA Support)

In the months following production launch, we provide support services including ongoing system monitoring, handling service requests, configuration adjustments, and fine-tuning processes to match organizational needs. The goal of this stage is full stabilization of the implementation.

Integrations

- Microsoft Active Directory – organizational structure, users, domain authentication (SSO)
- LDAP, CAS – external authentication
- Two-factor authentication (2FA) and two-step email verification
- eHelpDesk – routing requests to support groups and shared Employee Panel
- Databases: MS SQL, MySQL, PostgreSQL, Oracle – employee data import
- Source files: CSV, Excel, XML, TXT – also via ODBC

Technical Requirements

- Deployment model: on-premises – installation within the client's infrastructure
- Server OS: Ubuntu / Debian / RHEL / CentOS / Windows Server
- Environment: JDK 8 (OpenJDK), Apache Tomcat 10.x
- Database: PostgreSQL 16.x
- Hardware (minimum): 4-core CPU, 8 GB RAM, 20 GB disk space
- Client: any modern browser (Chrome, Firefox, Edge) – no installation required

Licensing model

The system is offered under a perpetual license model. The price depends on the number of system administrators (accounts authorized to manage the system) and the number of users involved in processes (typically equal to the number of accounts in MS Active Directory).

Contact us!

Get in touch with our IAM Sales Managers to schedule a free demo or receive an offer tailored to your organization.

Wojciech Jakubowski
IAM Sales Manager

wjakubowski@btc.com.pl
tel.: +48 91 481 72 26
mob.: +48 500 114 607

Daria Lorek
IAM Sales Manager

dlorek@btc.com.pl
tel.: +48 91 481 72 21
mob.: +48 797 440 524

Learn more



www.eauditor.eu/en/IAM