Columbus

# Access Management

It is more important than ever that only authorized users are accessing your resources, systems, and applications. Access management is controlling exactly that: Who has access to what resources, systems, and applications within your organization.

# Hackers don’t break in.
# They log in.

The requirements for Access Management solutions are constantly increasing. The phrasing **“Hackers don’t break in. They log in”** is well known and indicates that, for instance, the passwords that we thought were keeping us safe are now easy for hackers to breach.

A strong Access Management solution provides secure access in a way that end users will perceive as smooth and easy. At the same time, it will make it as complicated as possible for the hackers to sneak their way in.

## The basics of an ACCESS MANAGEMENT SYSTEM

### USER AUTHENTICATION

Identity Verification - User Credentials Check

Verifying the identity of a user, often through a username and password, but it can also include biometric authentication methods such as fingerprint or facial recognition.

### USER AUTHORIZATION

Role-based Access Control - Access Policy Enforcement

Determine what resources that user is authorized to access, based on their role or permissions.

# Access Management key features

There are several key features of an Access Management solution, including:

- **Authentication** Verifies the identity of a user, often through a username and password, but it can also include biometric authentication methods such as fingerprint or face recognition.
- **Authorization** Determines what resources a user is authorized to access, based on his or her role or permissions.
- **Single Sign-On (SSO)** Allows users to access multiple applications and resources with a single set of credentials, streamlining the login process and improving security. If an employee leaves the organization, access to all applications will automatically be removed in one go.
- **Multi-Factor Authentication (MFA)** Using authenticators such as Google and Microsoft as an extra layer of protection.
- **Access policies** Administrators can create policies that define which resources users can access and under what circumstances.
- **Audit trails and reporting** Access Management solutions provide detailed logs of user activity, allowing administrators to track who accessed what resources and when.
- **Integration with other security solutions** Access Management solutions can integrate with other security solutions, such as Identity and Access Governance solutions, to provide a comprehensive security strategy.

These features, offered by Access Management solutions, work together to ensure that users can access the resources they need, while also maintaining security and compliance.

# Additional Access Management services

ICY Security offers a range of services around Access Management to deliver the features described above.

## Assessment

Typically, we start with an assessment of the current environment. We will conduct several workshops with key stakeholders in your organization such as IT management, architects and solution owners to understand your requirements and needs.

## Action plan

Based on the assessment we will deliver a detailed action plan, complete with a well-defined roadmap and milestones for the Access Management implementation.

ICY Security supports both agile and hybrid-agile approaches.

Together with you, we assess and agree on which approach supports the implementation process best in your organization.

Columbus

Columbus®

kontakt.dk@columbusglobal.com