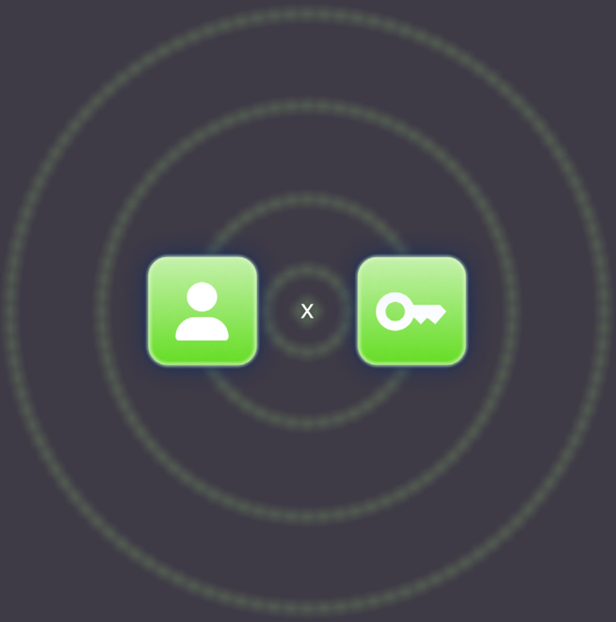
ConductorOne

# Identity Management vs Access Management



The core functions of identity security asks: “Who is this user?” and “What are they allowed to do?” Identity management is the discipline that answers the first question, while access management answers the second. This relationship directly mirrors authentication and authorization: a system must first verify an identity before it can grant access to a resource.

For IT and security teams, this requires a dual focus: they must accurately manage the lifecycle of every account (identity management) and enforce the **principle of least privilege** for those accounts (access management).

Getting both right is critical for enabling productivity while securing the organization against threats like orphaned accounts and permission sprawl.

While identity and access management are interdependent, they cover distinct responsibilities. To understand how these functions operate in practice, let’s break down the key aspects of each.

## What is identity management?

Identity management is the function that oversees the digital identities of all entities, including people and systems, within an organization. It is the authoritative framework for managing user accounts and ensuring that the identity information associated with them is accurate and trustworthy.

## Key components

At its core, identity management establishes and governs the entire lifecycle of a digital identity. This process includes:

- **Creation**: A unique digital identity is created when a user or system joins the organization. This identity is populated with key attributes and roles, such as job title, department, and initial permissions.
- **Modification**: Throughout the identity's lifecycle, identity management ensures data remains accurate during events like promotions, departmental transfers, or other role changes.
- **Deletion**: When a user leaves the organization, their identity is securely and completely de-provisioned to remove all access rights.

## How it works

The primary operational function of identity management is to enable secure and convenient authentication for authorized users. Authentication is the process of verifying that an entity is who or what it claims to be. A robust identity management system provides the foundation upon which all authentication decisions are made.

## Tools and technologies

IdM is powered by a set of integrated technologies that work together to manage and secure identities. These include:

- **Centralized identity platforms**: Often called Identity Providers (IdPs), these systems act as the single source of truth for all identity data and provide the core infrastructure for authentication.
- **Single sign-on (SSO)**: SSO platforms, often using standards (like SAML and OpenID Connect), allow a user to authenticate once and gain access to multiple apps and services, which centralizes control and simplifies the user experience.
- **Robust authentication methods**: To move beyond legacy password management, identity management leverages stronger authentication methods like multi-factor authentication (MFA), biometrics, and one-time passwords (OTPs).
- **User provisioning systems**: These tools automate the granting and revoking of access based on established roles and policies, ensuring users get appropriate access when they need it—and lose it when they no longer do.

By establishing and maintaining an accurate, verifiable digital profile for every user, identity management provides the fundamental layer of trust required to make subsequent security and access decisions.

# What is access management?

If identity management confirms users are who they say they are, access management dictates what they are allowed to do. It is the comprehensive process of granting, modifying, and revoking user permissions for specific data and resources. After a user's identity is authenticated, access management is the function that enforces the specific privileges they have.

## Key components

Access management **controls the permissions** linked to an established digital identity. It mitigates the challenge of tracking and enforcing varying access levels based on an individual's specific position, role, and responsibilities. This means specifying exactly who has access to particular data, applications, or functionalities within a system.

## How it works

The core process of access management is authorization—the act of allowing or denying a requested action based on a user's permissions. Specialized software and policies are used to regulate these permissions across various systems, such as file servers, databases, and collaboration platforms, ensuring an authenticated user is actually entitled to the resource they are trying to use.

## Tools and technologies

A variety of technologies are used to enforce access control policies. The goal is to ensure the right individuals have the right access to the right resources. These technologies include:

→ **Access control models**: These are the frameworks that define how permissions are assigned. Common models include **role-based access control** (RBAC) and **attribute-based access control** (ABAC).

→ **Access control lists**: These are tables that tell a system which users or groups have permission to access a specific object and what operations they are allowed to perform.

→ **Privileged access management (PAM)**: These solutions are specifically designed to manage, monitor, and secure the elevated access used by administrators and other privileged accounts that control critical infrastructure.

→ **Permission reporting and cleanup tools**: These technologies provide a clear overview of who has access to what, helping teams identify and remove excessive, unnecessary, or outdated permissions that create risk.

Access governance platforms: These systems help ensure that access policies align with business objectives and regulatory requirements by providing tools for access reviews, policy management, and reporting.

## A resource-centric approach to security

Access management focuses on controlling and **monitoring user access** to prevent unauthorized use or data breaches. The fundamental principle is to ensure that access rights are explicitly and correctly granted based on need, rather than being open by default.

# Identity Management vs. Access Management: A Direct Comparison

While identity management and access management are interdependent, they solve distinct technical challenges within an **IAM framework**. Identity management focuses on authentication—verifying who a user is—while access management handles authorization—determining what an authenticated user is permitted to do.

The following table breaks down the key operational differences.

| Parameter | Identity Management | Access Management |
|---|---|---|
| **Scope of operation** | Manages the full lifecycle of a digital identity, from creation to deletion. It is focused on the user profile. | Controls the permissions and privileges assigned to a verified identity. It is focused on what the user can do. |
| **Granularity of control** | Operates with broad controls, assigning users to high-level roles and groups (e.g., Engineer, Contractor). | Enforces fine-grained, specific permissions, defining what actions a role can perform on a resource (e.g., read-only vs. admin). |
| **Core approach** | Its purpose is to create and maintain an accurate, trustworthy profile for each user or entity. | It ensures the correct, verified user is connected to a specific resource with the appropriate permissions. |
| **Primary objective** | To provide secure and streamlined authentication by establishing a verifiable digital profile. | To enforce correct authorization by ensuring an authenticated user has the necessary permissions and nothing more. |
| **Security function** | Prevents risks like orphaned accounts by ensuring identity data is accurate and accounts are properly managed. | Enforces the principle of least privilege, monitors access, and controls permissions to prevent data breaches. |

## Scope of operation

Identity management focuses on the identity itself. Its scope covers the entire lifecycle of a user account from creation and modification to eventual deletion. It is concerned with establishing and overseeing the digital profile.

Access management, in contrast, focuses on permissions. Its scope is to control and regulate the privileges linked to an established identity, specifying who can access what data or functionality.

### Granularity of control

Identity management operates with broader controls, often dealing with high-level user profiles, roles, and groups (e.g., assigning a user to the “Engineer” or “Finance” role).

Access management provides much more granular and specific control. It defines the precise permissions for those roles, such as allowing the “finance” role to access accounting software but not production databases.

### Primary objective: authentication vs. authorization

The primary objective of identity management is to enable a streamlined and secure user authentication process. By creating a robust and precise digital profile, it provides the trusted foundation needed to verify a user’s identity.

The primary objective of access management is to enforce correct authorization. It ensures that once a user is authenticated, they have tailored access only to the resources they need, which minimizes security gaps and preserves data integrity.

### Core use cases

The use cases for each function highlight their differences:

- **Identity management** is central to employee lifecycle events, including onboarding, offboarding, and managing user profile changes.
- **Access management** is applied in the day-to-day securing of applications, systems, and data to prevent unauthorized access and actions.

### Security function

Both are critical to security:

- **Identity management** enhances security by ensuring user identity data is accurate and that accounts are properly managed, preventing issues like orphaned accounts.
- **Access management** strengthens security by enforcing the principle of least privilege, controlling permissions, and monitoring user access to stop unauthorized entry and data breaches.

## How identity management and access management work together

Identity management and access management are sequential and interdependent. For secure access to be granted, authentication must always precede authorization. This two-step process forms the core of a modern IAM strategy.

The flow works as follows:

1. A user first attempts to access a system. The identity management function handles the **authentication** to verify the user's identity.
2. Once the user is successfully authenticated, the access management function takes over. It performs **authorization** by checking the permissions associated with that specific identity to determine if they have the appropriate access rights to the requested resource.

Here is practical example:

Consider a member of an accounting team who logs into their corporate network.

→ **Authentication**: The user provides their credentials (e.g., username, password, and an MFA token). The identity management system verifies these credentials and confirms the user's identity.

→ **Authorization**: Now authenticated, the user tries to open the company's accounting software. The access management system checks their role ("accountant") and grants access. Later, if the same user attempts to access the engineering team's source code repository, the AM system will see they are not authorized for that resource and will deny access.

This collaboration ensures that only verified entities with the correct, explicit permissions can gain access to corporate resources, which is fundamental to maintaining security and data integrity.

## Choosing an IAM strategy: standalone vs. unified solutions

The decision to implement a standalone identity or access management solution versus a unified IAM platform depends on an organization's specific needs, including its size, number of user accounts, and the complexity of its permissioning structure.

While specific scenarios might call for a targeted solution, most modern businesses require an integrated approach.

→ **Access management solutions** can be effective for smaller organizations with a limited number of user accounts but highly complex data access structures that require granular permissioning and reporting.

→ **Identity management tools** may suffice for organizations that need to manage a large number of accounts but have a simple permissioning model without the need for intricate access adjustments between different user groups.

Ultimately, because authentication and authorization are so deeply intertwined, most businesses find they need the capabilities of both to operate securely and efficiently across their hybrid IT environment.

### Benefits of a unified IAM solution

For most organizations, integrating identity and access management into a single, unified IAM solution provides the most robust security and operational benefits. This approach:

→ **Safeguards sensitive information**: It enables granular access control, ensuring that sensitive data is protected and that the principle of least privilege can be effectively enforced.

- → **Ensures compliance**: A unified platform provides detailed logs and reports on all access activity, which is essential for security audits and meeting regulatory compliance standards.
- → **Increases operational efficiency**: Automating user and permission management workflows saves significant time for IT and security teams, reducing the manual effort involved in onboarding, offboarding, and access requests.
- → **Enables scalable policy enforcement**: It allows for the consistent application of access control models like role-based-access-control (RBAC), where access privileges are automatically assigned based on user attributes.
- → **Provides centralized management**: A single IAM platform serves as the central hub for managing identities and access across the entire technology stack, including on-premises systems, cloud-based services, and third-party apps.

ConductorOne

## Unifying identity and access management with ConductorOne

A modern, unified IAM platform brings identity and access management into a single control plane, automating the entire access lifecycle while enforcing the principle of least privilege. **ConductorOne** is an identity security platform designed to address these challenges for security and IT teams.

Here's how **ConductorOne** provides a unified solution:

- → **Centralizes identity and access data**: By integrating with identity providers, HR systems, and the full spectrum of an organization's applications, ConductorOne acts as a single source of truth for who has access to what.
- → **Automates the access lifecycle**: ConductorOne automates access changes for joiner, mover, and leaver events. It streamlines onboarding by granting access based on roles and seamlessly adjusts or revokes permissions as roles change or when an employee departs.
- → **Enforces modern access policies**: The platform enables teams to move beyond static permissions by implementing security policies like just-in-time **(JIT)** access, which grants temporary, audited access to sensitive systems only when needed. This enforces least privilege without creating friction for users.
- → **Streamlines access reviews**: ConductorOne automates periodic access review campaigns. It provides reviewers with the context they need to make intelligent decisions, detects excessive or unused permissions, and creates a complete audit trail for compliance purposes.
- → **Provides deep visibility and reporting**: With a complete view of all permissions and access activities, the platform generates curated reports that show who has access to what systems. This visibility is essential for managing security risks and making informed security decisions.

To see how a unified platform can help you **automate access control** and enforce least privilege in your environment, book a demo today.

## Identity vs access management FAQs

### What is the single biggest difference between identity management and access management?

Identity management focuses on authentication (verifying a user is who they say they are), while access management focuses on authorization (determining what an authenticated user is allowed to do). You can't have effective authorization without first having reliable authentication.

### Why is a standalone identity management system not enough for security?

An identity management system can confirm a user's identity, but it doesn't control what that user can do once they are in the system. Without access management, even a correctly authenticated user could have excessive permissions, creating significant security risks and vulnerabilities.

### What is the principle of least privilege and which function handles it?

The principle of least privilege is a foundational cybersecurity concept stating that users should only be granted the minimum access rights necessary to perform their job functions. This is a core responsibility of access management.

### How does a unified IAM platform improve security posture?

IAM tools improve security posture by providing a single, centralized view of all identities and their access rights. This allows organizations to automate user access reviews, enforce consistent security policies like least privilege, and quickly identify and remediate security risks like excessive or unused permissions.

### How does IAM relate to a Zero Trust architecture?

IAM is the foundation of a Zero Trust security model. Zero Trust operates on the principle of "never trust, always verify," which requires continuously authenticating and authorizing every access request, regardless of where it originates. A robust IAM system provides the continuous identity verification and granular access control necessary to implement a Zero Trust strategy effectively.