onelogin
by ONE IDENTITY

OneLogin + One Identity delivering IAM together. **Learn more →**

HOME / IDENTITY AND ACCESS MANAGEMENT 101 / **WHAT IS IDENTITY AND ACCESS MANAGEMENT (IAM)?**

What is Identity and Access Management (IAM)?

Identity and access management concepts

What Does Identity and Access Management Mean?

Identity and access management (IAM) ensures that the right people and job roles in your organization (identities) can access the tools they need to do their jobs. Identity management and access systems enable your organization to manage employee apps without logging into each app as an administrator. Identity and access management systems enable your organization to manage a range of identities including people, software, and hardware like robotics and IoT devices.

Why IAM?

Companies need IAM to provide online security and to increase employee productivity.

- **Security.** Traditional security often has one point of failure - the password. If a user's password is breached - or worse yet, the email address for their password recoveries - your organization becomes vulnerable to attack. IAM services narrow the points of failure and backstops them with tools to catch mistakes when they're made.

- **Productivity.** Once you log on to your main IAM portal, your employee no longer has to worry about having the right password or right access level to perform their duties. Not only does every employee get access to the perfect suite of tools for their job, their access can be managed as a group or role instead of individually, reducing the workload on your IT professionals.

Learn the Signs

Does IAM Improve Regulatory Compliance?

Security is also a matter of law, regulation, and contracts. Data protection standards like Europe's General Data Protection Regulation and HIPPA and the Sarbanes-Oxley Act in the U.S. enforce strict standards for data security. With an IAM solution, your users and organization can ensure that the highest standards of security, tracking, and administrative transparency are a matter of course in your day-to-day operations.

How Does IAM Work?

Identity management solutions generally perform two tasks:

1. IAM confirms that the user, software, or hardware is who they say they are by authenticating their credentials against a database. IAM cloud identity tools are more secure and flexible than traditional username and password

solutions.

2. Identity access management systems grant only the appropriate level of access. Instead of a username and password allowing access to an entire software suite, IAM allows for narrow slices of access to be portioned out, i.e. *editor*, *viewer*, and *commenter* in a content management system.

What Does IAM Do?

IAM systems provide this core functionality:

TASK	TOOLS
Manage user identities	IAM systems can be the sole directory used to create, modify, and delete users, or it may integrate with one or more other directories and synchronize with them. Identity and access management can also create new identities for users who need a specialized type of access to an organization's tools.
Provisioning and deprovisioning users	Specifying which tools and access levels (editor, viewer, administrator) to grant a user is called provisioning. IAM tools allow IT departments to provision users by role, department, or other grouping in consultation with the managers of that department. Since it is time consuming to specify each individual's access to every resource, identity management systems enable provisioning via policies defined based on role-based access control (RBAC). Users are assigned one or more roles, usually based on job function, and the RBAC IAM system automatically grants them access. Provisioning also works in reverse; to avoid security risks presented by ex-employees retaining access to systems, IAM allows your organization to quickly remove their access.
Authenticating users	IAM systems authenticate a user by confirming that they are who they say they are. Today, secure authentication means multi-factor

	authentication (MFA) and, preferably, adaptive authentication.
Authorizing users	Access management ensures a user is granted the exact level and type of access to a tool that they're entitled to. Users can also be portioned into groups or roles so large cohorts of users can be granted the same privileges.
Reporting	IAM tools generate reports after most actions taken on the platform (like login time, systems accessed, and type of authentication) to ensure compliance and assess security risks.
Single Sign-On	Identity and access management solutions with single sign-on (SSO) allow users to authenticate their identity with one portal instead of many different resources. Once authenticated, the IAM system acts as the source of identity truth for the other resources available to the user, removing the requirement for the user to remember several passwords.

What is the Difference Between Identity Management and Access Management?

Identity management confirms that you are you and stores information about you. An identity management database holds information about your identity - for example, your job title and your direct reports - and authenticates that you are, indeed, the person described in the database.

Access management uses the information about your identity to determine which software suites you're allowed access to and what you're allowed to do when you access them. For example, access management will ensure that every manager with direct reports has access to an app for timesheet approval, but not so much access that they can approve their own timesheets.

Cloud Versus On-Premises IAM

In the past, most identity and access management was managed by a server on the physical premises of an organization, which was called on-prem. Most IAM services are now managed by a provider in the cloud to avoid physical maintenance costs to the organization, as well as to ensure uptime, distributed and redundant systems, and short SLAs.

What is AWS Identity and Access Management?

Amazon Web Services (AWS) identity and access management is simply the IAM system that is built into AWS. By using AWS IAM, you can create AWS users and groups and grant or deny them access to AWS services and resources. AWS IAM is available free of charge.

AWS IAM service provides:

- Fine-grained access control to AWS resources
- AWS multi-factor authentication
- Analysis features to validate and fine tune policies
- Integration with external identity management solutions

What Tools Do I Need to Implement Identity and Access Management?

The tools needed to implement IAM include password-management tools, provisioning software, security-policy enforcement applications, reporting and monitoring apps and identity repositories. IAM tools can include, but are not limited to:

- **MFA**
  Multi-factor authentication means that your IAM provider requires more than one type of proof that you are who you say you are. A typical example is requiring both a password and a fingerprint. Other MFA choices include facial recognition, iris scans, and physical tokens like a Yubikey.
- **SSO**

SSO stands for single sign-on. If your IAM solution provides single sign-on, that means your users can sign in only once and then treat the identity and access management tool as a "portal" to the other software suites they have access to, all without signing in to each one.

What Does an IAM Implementation Strategy Include?

As a cornerstone of a zero trust architecture, an IAM solution should be implemented using zero-trust principles such as least privilege access and identity-based security policies.

- **Central identity management**
  A key principle of zero trust is managing access to resources at the identity level, therefore having centralized management of those identities can make this approach much simpler. This could mean migrating users from other systems or at least synchronizing your IAM with other user directories within your environment such as a Human Resources directory.

- **Secure access**
  Since securing at the identity level is key, an IAM should make sure that it is confirming the identities of those who are logging in. This could mean implementing MFA or a combination of MFA and adaptive authentication to be able to take into consideration the context of the login attempt: location, time, device, etc.

- **Policy-based control**
  Users should only be given authorization to perform their required tasks and no more privilege than is necessary. An IAM should be designed to give users access to resources based upon their job role, their department or any other attributes that seem appropriate. As part of the centrally managed identity solution these policies can then ensure that resources are secure no matter where they are being accessed from.

- **Zero-Trust Policy**
  A zero trust policy means that an organization's IAM solution is constantly monitoring and securing its users identity and access points. In the past, organizations operated on a "once you're in, you have access" policy, but

zero-trust policies ensure that each member of the organization is constantly being identified and their access managed.

- **Secured privileged accounts**
  Not all accounts in an access management system are created equal. Accounts with special tools or privileged access to sensitive information can be provided a tier of security and support that suits their status as a gatekeeper for the organization.

- **Training and support**
  IAM providers provide training for the users who will be most engaged with the product - including users and administrators - and often provide customer service for the long-term health of your IAM installation and its users.

IAM Technologies

An IAM system is expected to be able to integrate with many different systems. Because of this, there are certain standards or technologies that all IAM systems are expected to support: *Security Access Markup Language*, *OpenID Connect*, and *System for Cross-domain Identity Management*.

- **Security Access Markup Language (SAML)**
  SAML is an open standard used to exchange authentication and authorization information between an identity provider system such as an IAM and a service or application. This is the most commonly used method for an IAM to provide a user with the ability to log in to an application that has been integrated with the IAM platform.

- **OpenID Connect (OIDC)**
  OIDC is a newer open standard that also enables users to log in to their application from an identity provider. It is very similar to SAML, but is built on the OAuth 2.0 standards and uses JSON to transmit the data instead of XML which is what SAML uses.

- **System for Cross-domain Identity Management (SCIM)**
  SCIM is standard used to automatically exchange identity information between two systems. Though both SAML and OIDC can pass identity information to an application during the authentication process, SCIM is

used to keep the user information up to date whenever new users are assigned to the service or application, user data is updated, or users are deleted. SCIM is a key component of user provisioning in the IAM space.

Related Resources

Buckle Up for Cybersecurity!

See how IAM can save your customers from a catastrophic breach.

Explore the Infographic →

Calculate Y

Find out how

● ○ →

About

Products

Solutions

Get Started

onelogin

by ONE IDENTITY

Legal | Terms of Use | Privacy Policy | Sitemap

Cookie Preference Center | Cookie Use Policy

United States of America (EN)