Microsoft

Azure Active Directory Identity Governance

Table of contents

Today's hyper-connected world and the ways we work

The world we live in today is hyper-connected and continually changing. It's an evolving and expanding digital network of varied connections and a variety of devices, users, and systems. Organizations of all sizes include a user base of vendors, partners, contractors, and customers who need access to corporate data and information anytime, anywhere, and on any device, including their own. In the modern workforce, the emergence of new trends like hybrid cloud models, IoT devices, and collaborative applications make it easy to share information, data, and files with other internal as well as external systems and users.

This changing landscape creates new business opportunities, but also increases the threat surface. Each point of user access is a possible point of exposure. IT and security departments are struggling with analysis of security policy compliance, situational awareness, and the understanding of threats in real time. Failure to manage users' access to and control of sensitive resources places companies at increased risk for audit failure, fraud, or security data breaches. Most importantly, it calls into question the trust of your brand.

1,903 breaches were reported through March 31, 2019, exposing approximately 1.9 billion records. Compared to Q1 2018, the number of reported breaches was up 56.4 percent, and the number of exposed records was up 28.9 percent from 1.4 billion. The start of 2019 was fueled by credential leaks and compromised email accounts.

Source - Risk Based Security:
Data Breach QuickView Report, First Quarter 2019

Are you effectively controlling access to resources?

As the levels of business insider breaches and fraud increase, it's crucial to manage user identities efficiently and securely while balancing goals for employee and organizational productivity. To keep up with today's ever-changing security and compliance landscape, organizations have to start recognizing new security strategy advancements that can help appropriately manage and govern users' access to corporate resources.

Key questions

- Who has access to what resources?
- Who should have access?
- What are they doing with that access?
- Are there adequate organizational controls to ensure users' access stays compliant?
- Can I show my organization's auditors that the controls are working?

When these critical questions are answered, you can effectively manage user access to crucial resources—and can conceivably ensure that your organization is protected against potential threats.

According to Crowd Research Partners, 90 percent of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).

Source - Crowd Research Partners:
Insider Threat 2018 Report

Identity is the new security perimeter

The security frontier has evolved from a network to an identity. Now, rather than solely focusing on securing your network, security is more about protecting your data, apps, and users. Firms that adopt the right solutions for managing and governing identities across their enterprises are better equipped to grow safely and innovate securely. Automating identity governing processes can minimize the burden on IT teams.

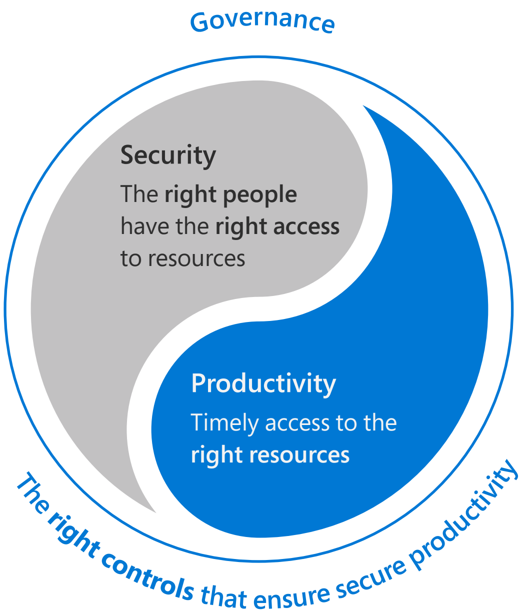
With a centralized and automated identity governance solution, you can quickly deploy standard processes at scale. You can also govern all user access—including employees, contractors, partners, and vendors—to all resources, apps, and data at enterprise scale, with controls to maintain compliance and automate IT tasks to improve operational efficiencies and reduce costs.

Introducing Azure Active Directory Identity Governance

Microsoft Azure Active Directory (Azure AD) Identity Governance is a cloud-based solution that enables organizations to efficiently and securely manage their digital identities by ensuring that the right people have the right access to the right resources. Azure AD Identity Governance, a native capability within Azure AD, helps your organization protect, monitor, and audit access to critical assets while ensuring employee productivity. It's uniquely positioned to meet the needs of customers who lack an effective and complete identity governance solution.

✓ **Azure AD Identity Governance is a native solution in Azure AD.**

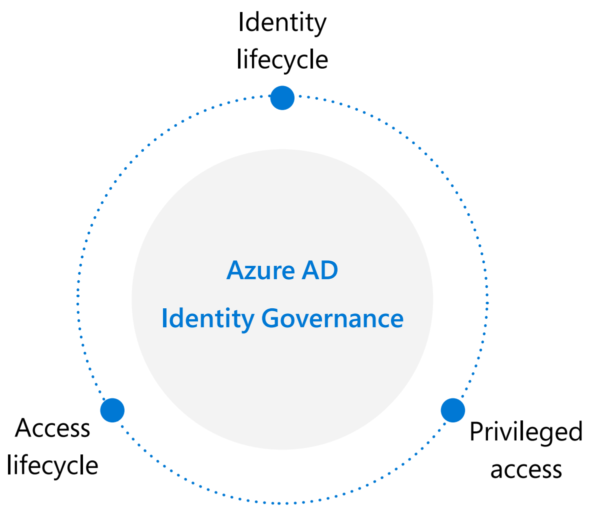
With Azure AD Identity Governance, IT can gain more visibility into who has—and who should have—access to what resources in the organization and on what devices. They can better control what users can do with that access and can restrict access according to company and regulatory policies.


Governance
Security
The right people have the right access to resources
Productivity
Timely access to the right resources
The right controls that ensure secure productivity

Sign in to the Azure portal as an administrator and go to the **Azure Active Directory** > **Identity Governance** section to try Enterprise Mobility + Security (EMS) E5 and evaluate **Azure AD Identity Governance capabilities.**

Azure AD Identity Governance capabilities

With identity as your control plane with Azure AD, you can unlock various new governance capabilities, such as automatic account provisioning and de-provisioning, conditional access controls, access reviews, entitlement management and compliance policies, secure collaboration with partners, and more. To begin, let's define the three core elements that can shape the thought process around identity governance as a whole.



Azure AD Identity Governance gives organizations the ability to:

- Govern the identity lifecycle
- Govern the access lifecycle
- Govern privileged access

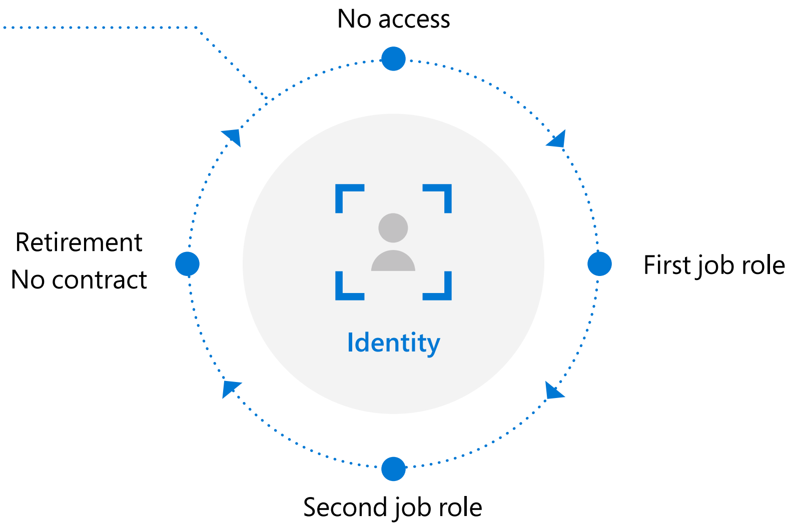
Governing the identity lifecycle

Every organization needs to ensure quick user, partner, or vendor onboarding and provide them access to the resources they legitimately need to make them productive without compromising access to systems beyond that requirement.

To balance the security and productivity requirements, IT needs to keep track of a user's identity throughout its lifecycle. The user identity may change over time based on the user's role and status in the organization. For example, a user or partner might be hired as a contractor, then become a full-time employee, and finally leave the organization. Across all these stages, the organization identity should be updated, and even after retirement, a record of the account should exist for auditing purposes.

The manual process for managing this identity lifecycle scenario is not effective at scale. IT needs to automate the lifecycle and provisioning process and ensure it remains accurate, even as user communities, applications, and business requirements change. Azure AD offers various capabilities and supports numerous scenarios to govern and manage the identity lifecycle across employees and guests.

Identity lifecycle



Managing the employee identity lifecycle

Azure AD enables automated, policy-based provisioning and de-provisioning of user accounts from Workday Human Capital Management (HCM), other cloud Human Resources (HR), or on-premises HR systems. For typical organizations, the identity lifecycle for employees is a representation of that person derived from information in an HCM system. For organizations using Workday HCM, Azure AD ensures user accounts are automatically provisioned and de-provisioned. The Workday HCM workflows supported by the Azure AD user provisioning service enable automation of various scenarios, including profile updates and employee hires, terminations, and rehires.

Azure AD Premium also includes Microsoft Identity Manager (MIM), which can import records from on-premises HCM systems, such as SAP, Oracle eBusiness, and Oracle PeopleSoft, and manage the users, credentials, policies, and access within an organization's on-premises resources.

Granting partner access to resources

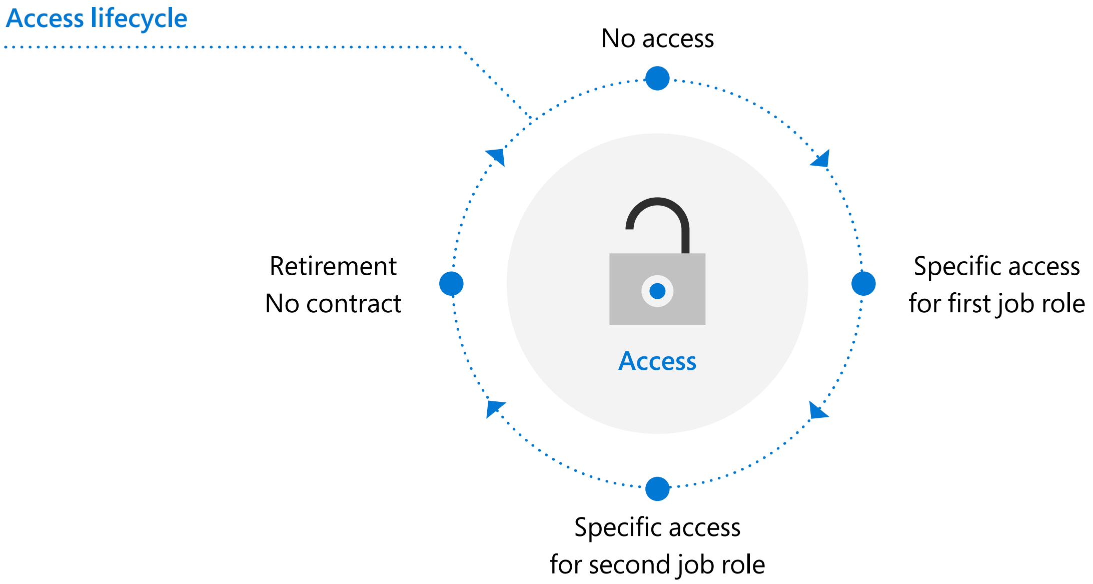
Azure offers Azure AD Business-to-Business (B2B) collaboration without losing control of corporate data. Azure AD B2B capabilities simplify how users from other firms—including partners, contractors, and suppliers—access an organization's resources. An employee can invite a guest user for collaboration, or the guest user can request access and be approved through a workflow. Once invited or approved, the guest user can sign in with their own Azure AD identity, their organization's identity provider, or a social account—meaning they don't need to remember and maintain yet another password.

Directed by the organization's security policy, Azure AD admins can set multi-factor authentication (MFA) policies for guest users and can enable self-service guest user provisioning from another non-Azure AD tenant using federation. Users can be automatically provisioned across applications, teams, and sites, while access is regularly reviewed. This helps to ensure collaboration remains effective and inactive guests are removed from the directory when access is no longer needed.

Governing the access lifecycle

Go beyond merely giving users birthright access when they're onboarded. Instead, maintain a process that enables your users' access to change with their needs. For example, guest users may be unaware of the handling requirements for data in an organization to which they have been invited. Likewise, they may not know what access rights they need or what to do when they no longer need access. To best meet both business and user needs, organizations should maintain an efficient process that enables users' access to change as their roles do.

Organizations can automate access and enforce access policies through Azure AD Identity Governance to ensure users have the right access. With tools like entitlement management and dynamic groups with SaaS apps, it's possible to reduce the burden on IT and business decision makers by turning access management into an automated access process. The user's rights can be reviewed and adjusted regularly during access reviews. Selecting reviewers who can approve or deny a user's continued access is especially important when it comes to guest users.



Access lifecycle
No access
Specific access for first job role
Specific access for second job role
Retirement No contract
Access

Access lifecycle automation (access requests, fulfillment, and workflow)

Using Azure AD entitlement management, resource owners can create packages containing Azure AD-integrated apps, Azure AD groups, Office 365 groups, and SharePoint Online sites. They can define user access governance policies across these resources with access packages. Resource owners can also define policies for escalating requests, generating multistage approvals, and managing access expiration, among others. Separate policies can be defined for access by employees or by business partners and collaborators.

Azure AD offers tools like dynamic groups that allow IT admins to automate the critical task of granting, modifying, and removing users' access to connected apps and systems based on user profile data. This not only ensures users have correct permissions, but also reevaluates user profile changes.

For more information on entitlement management and how to use it, visit the Azure AD entitlement management documentation page.

Access enforcement (policy and role management)

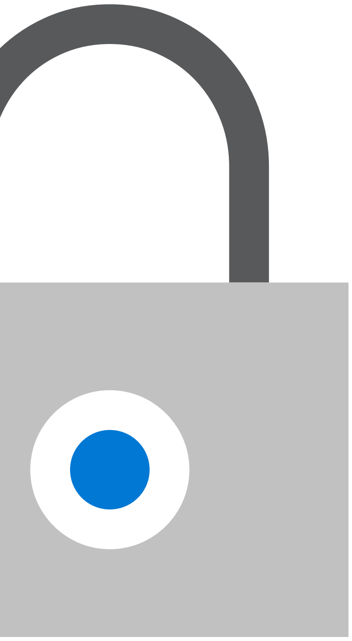
Using Azure AD, administrators can define the conditional access policies for runtime access to applications and data. It enforces policies that implement automated access control decisions for accessing apps based on various conditions like sign-in risk, network location, and more.

Azure AD conditional access policies can include displaying terms of use to end users as well as ensuring users have agreed to those terms before being able to access applications and data. This approach ensures that users see relevant disclaimers for legal or compliance requirements.

Access reviews

With Azure AD access reviews, organizations can ensure that only users who need access actually have access. IT can enable recurring or one-time access review campaigns for guests and employees who have a continued need for access to groups, enterprise applications, and administrative role assignments.

Reviews can be delegated to the resource owner or specific people, or users can be allowed to self-attest their need for access. Further, reviewers receive intelligent recommendations on whether to approve or deny users. With Azure AD access reviews, end users and partners can collaborate more freely and effectively while ensuring their access is periodically reviewed.

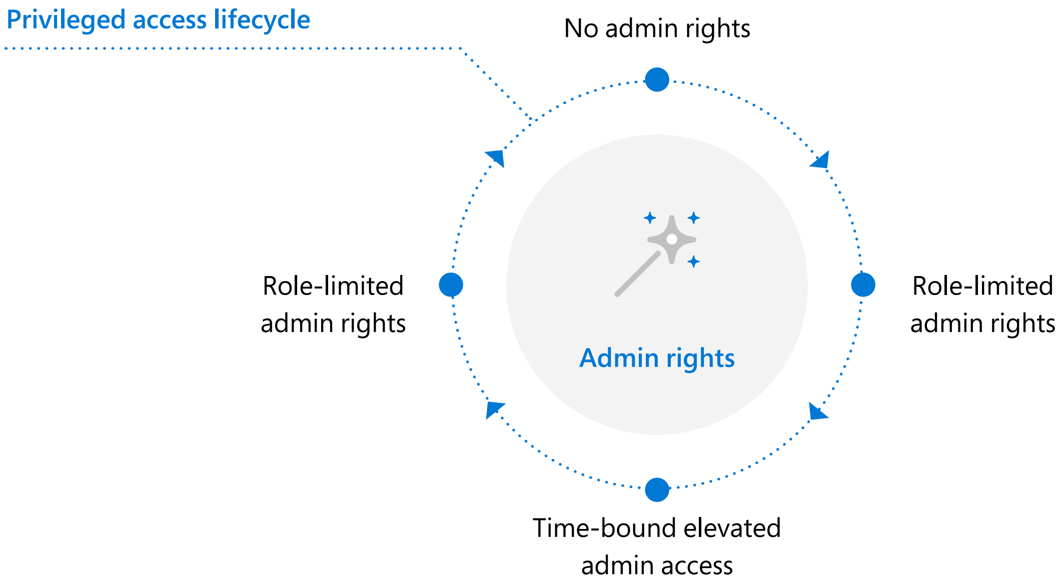


For more information on access reviews and how to use them, visit the Azure AD access review documentation page.

Governing privileged access

Governing privileged access is a vital part of Azure AD Identity Governance, especially given the potential for misuse associated with those administrator rights. It's essential to govern this access to avoid any misuse, whether it's from the organization or an outside resource.

Azure AD enhances system security by governing administrator access and limiting excessive access rights using conditional access policies, MFA, and access reviews. Azure MFA offers an additional layer of security using a second form of authentication and enables strong authentication via a range of easy-to-use methods. Organizations can use Azure AD conditional access policies to make the solution address their specific needs. They can also use access reviews to configure recurring access certification for all users in administrator roles.


Privileged access lifecycle
No admin rights
Role-limited admin rights
Admin rights
Role-limited admin rights
Time-bound elevated admin access

Azure AD Privileged Identity Management

Azure AD Privileged Identity Management (PIM) helps to manage and control privileged administrative roles across Azure AD and Azure resources to ensure compliance with corporate privileged-access policies. It provides solutions for Just-in-Time access, such as limiting the duration of privileged access operations in which users receive temporary permissions to perform privileged tasks.

PIM enforces request approval workflows of a privileged role with fully integrated access reviews, such that potentially malicious activities that might occur while in privileged roles can be identified, uncovered, and prevented in real time. PIM can enforce MFA before a user is allowed to act in a role. It also generates triggers and automated alerts on the PIM dashboard in case of any suspicious or risky activity in the environment. IT can be alerted of admin account creation and can track changes in privileged role assignments and role activation history.

A path forward

A strategic start and well-defined roadmap can help your organization achieve its vision and goals for identity governance. To start, assess your business requirements, discover opportunities, and build business cases for identity governance. Next, perform a gap analysis to evaluate your existing requirements.

Azure AD Identity Governance and Microsoft can help your organization develop a conceptual architecture and detailed roadmap for identity governance adoption. You can improve the overall user experience, streamline technology-focused processes, and migrate identity and governance programs to the next maturity level. Go beyond identity management and start governing identity, access, and administration with Azure AD Identity Governance.

Summary

Identity governance is a continuous journey. Azure AD Identity Governance can help you in this journey with a set of tools and capabilities to ensure that the right users have the right access to the right resources—at the right time. It allows your IT security and audit teams to protect, monitor, and audit access to critical assets while ensuring employee and guest productivity.

Microsoft can help keep you up to date as you navigate the modern IT identity and governance environment. Try a **free trial of EMS E5** to get access to Azure AD and explore Azure AD Identity Governance. Other important resources or documentation include:

- Azure AD Identity Governance documentation
- What is Azure AD Identity Governance?