From Azure AD to Microsoft Entra ID: Unlocking Multicloud Security through a New Era of Comprehensive Identity and Access Management Reimagined

- Praveen

Spotlight on Changes: Essential Takeaways

In the ever-evolving landscape of digital transformation, Microsoft has announced a significant change - Azure Active Directory (Azure AD) is being rebranded to Microsoft Entra ID. This shift is part of Microsoft's ongoing commitment to simplify secure access experiences for everyone, making it easier for users to navigate the unified and expanded Microsoft Entra portfolio.

Seamless Transition: No Action Required

For businesses currently using or deploying Azure AD, the transition to Microsoft Entra ID is seamless. All existing deployments, configurations, and integrations will continue to function as they do today without any action required from you. The service you've come to rely on remains consistent, ensuring uninterrupted operation.

More Than Just a Name Change

While the name is changing, the features and capabilities that have made Azure AD a cornerstone of business operations remain intact. Licensing, terms, service-level agreements, product certifications, support, and pricing remain the same. The change is primarily in the display names for service plans and SKUs, which will be updated on October 1, 2023. For example, Azure Active Directory Free will become Microsoft Entra ID Free, Azure Active Directory Premium P1 will become Microsoft Entra ID P1, and so on.

Consistent Developer and DevOps Experiences

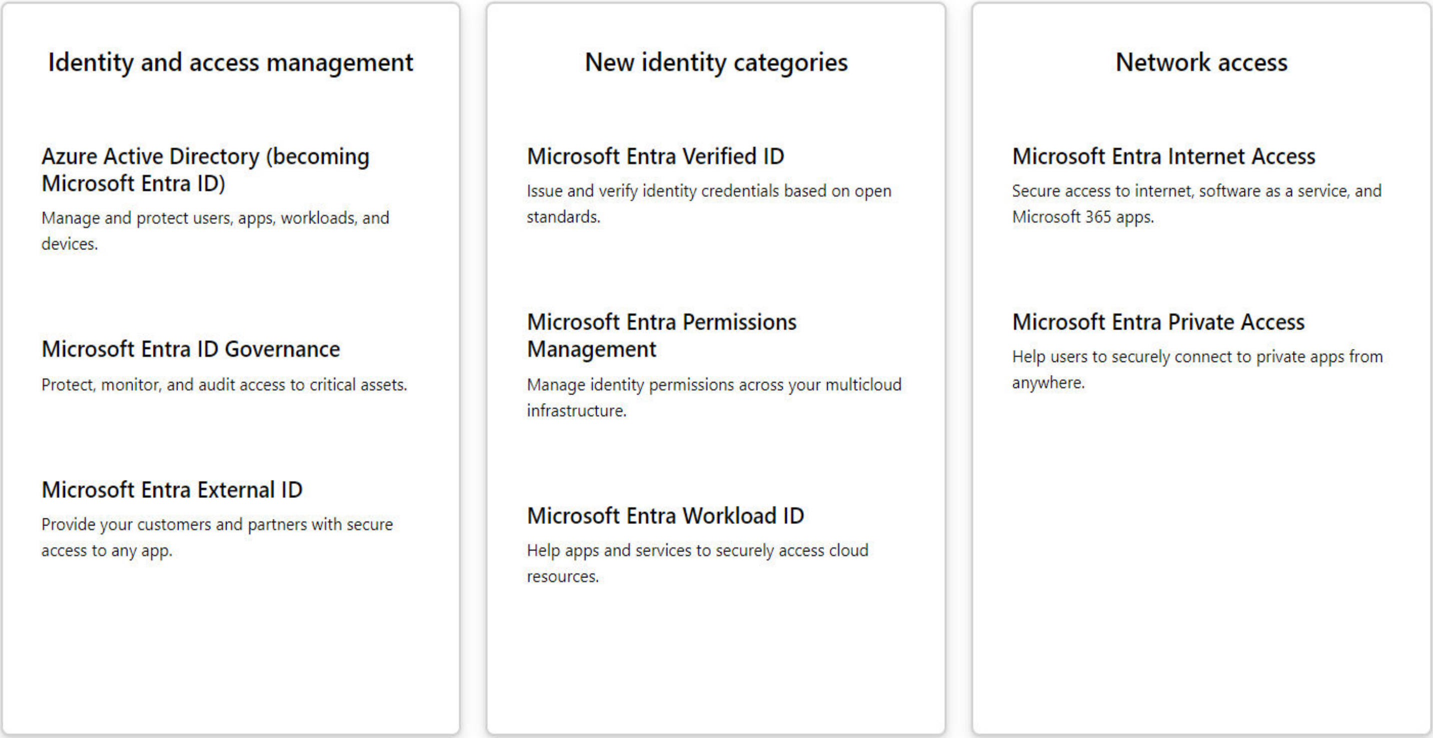
The renaming to Microsoft Entra ID does not affect the developer and DevOps experiences. All existing login URLs, APIs, PowerShell cmdlets, and Microsoft Authentication Libraries (MSAL) stay the same, ensuring a consistent experience. Naming is also not changing for Microsoft Authentication Library (MSAL), Microsoft Graph, Microsoft Graph PowerShell, and other related services.

Frequently Asked Questions

The name change is set to happen starting after a 30-day notification period from July 11, 2023. The reason for the name change is to simplify secure access experiences, aligning with the expanded vision of Microsoft Entra, a product family that includes Microsoft Entra ID and other solutions.

Exceptions to Azure AD Name Change

It's important to note that products or features that are being deprecated aren't being renamed. These products or features include Azure AD Authentication Library (ADAL), Azure AD Graph, and Azure Active Directory PowerShell for Graph, which have been replaced by other services.



Identity and access management

Azure Active Directory (becoming Microsoft Entra ID)

Manage and protect users, apps, workloads, and devices.

Microsoft Entra ID Governance

Protect, monitor, and audit access to critical assets.

Microsoft Entra External ID

Provide your customers and partners with secure access to any app.

New identity categories

Microsoft Entra Verified ID

Issue and verify identity credentials based on open standards.

Microsoft Entra Permissions Management

Manage identity permissions across your multicloud infrastructure.

Microsoft Entra Workload ID

Help apps and services to securely access cloud resources.

Network access

Microsoft Entra Internet Access

Secure access to internet, software as a service, and Microsoft 365 apps.

Microsoft Entra Private Access

Help users to securely connect to private apps from anywhere.

What is Microsoft Entra?

Microsoft Entra is a comprehensive suite of multicloud identity and network access solutions. It's designed to secure access to any resource for every user or digital workload across your entire environment. Here are the key components of Microsoft Entra:

Identity and Access Management

Azure Active Directory (becoming Microsoft Entra ID):

Formerly known as Azure Active Directory, Microsoft Entra ID is a cloud-based identity and access management service. It helps your employees sign in and access resources seamlessly.

With features like single sign-on, multi-factor authentication, and device management, it ensures that your organization's data is secure and accessible only to authorized personnel.

Microsoft Entra ID Governance:

Microsoft Entra ID Governance provides a risk-based approach to managing access to your organization's resources. It ensures that only the right people have the right access to the right resources.

With features like access reviews, privileged identity management, and entitlement management, it helps you maintain control over who has access to what within your organization. This component helps protect, monitor, and audit access to critical assets.

Microsoft Entra External ID:

Managing identities and access for external users can be a challenge. Microsoft Entra External ID is a comprehensive solution for this. It provides secure and seamless access experiences for your customers and partners.

With features like self-service sign-up and sign-in, progressive profiling, and unified customer identity, it enhances the user experience while maintaining security.. This provides your customers and partners with secure access to any app.

New Identity Categories

Microsoft Entra Verified ID:

In the digital age, verifying identity credentials is crucial. Microsoft Entra Verified ID provides a way to issue and verify identity credentials based on open standards. It enhances security and privacy by enabling users to control their own identity data. This issues and verifies identity credentials based on open standards.

Microsoft Entra Permissions Management:

Managing identity permissions across a multicloud infrastructure can be complex. Microsoft Entra Permissions Management simplifies this process.

It helps you discover and right-size permissions, ensuring least privilege access for any identity. This manages identity permissions across your multicloud infrastructure.

Microsoft Entra Workload ID:

Securing the connections between your apps, services, and resources is crucial. Microsoft Entra Workload ID is a solution for this. It helps you manage and secure service identities, application identities, and data plane identities. This helps apps and services to securely access cloud resources.

Network Access

Microsoft Entra Internet Access:

Microsoft Entra Internet Access provides secure access to internet, software as a service, and Microsoft 365 apps.

With features like secure web gateway, firewall as a service, and cloud access security broker, it ensures that your organization's internet access is secure and controlled. This secures access to internet, software as a service, and Microsoft 365 apps.

Microsoft Entra Private Access:

Microsoft Entra Private Access is a solution for securely connecting your users to your private apps from anywhere. It provides zero trust network access for your private apps without exposing them to the public internet. This helps users to securely connect to private apps from anywhere.

Microsoft Entra is a comprehensive suite of solutions designed to secure access to any resource for every user or digital workload across your entire environment. It helps you protect and verify every identity, manage permissions, enforce intelligent access policies, and simplify the user experience.

With Microsoft Entra, you can ensure that your organization's data is secure and accessible only to authorized personnel. These components work together to provide a comprehensive solution for identity and access management, ensuring secure access to resources across a multicloud environment.

Analogy: Think of Microsoft Entra as the entire theme park management system.

Identity and Access Management

Azure Active Directory (becoming Microsoft Entra ID):

This is like the ticketing system at the entrance of the park. It checks the tickets (identities) of the visitors (users) and allows them to enter the park (access resources).

Microsoft Entra ID Governance:

This is like the park's surveillance system. It monitors and audits the activities within the park (access to critical assets) to ensure everyone is following the rules.

Microsoft Entra External ID:

This is like the guest pass system. It allows guests (customers and partners) to access certain rides or attractions (apps) within the park.

New Identity Categories

Microsoft Entra Verified ID:

This is like the VIP pass system. It issues and verifies special passes (identity credentials) based on certain criteria (open standards).

Microsoft Entra Permissions Management:

This is like the park's access control system. It manages who can access which rides or attractions (identity permissions) within the park (multicloud infrastructure).

Microsoft Entra Workload ID:

This is like the park's maintenance system. It ensures that all the rides and services (apps and services) can securely access the resources they need to function properly.

Network Access

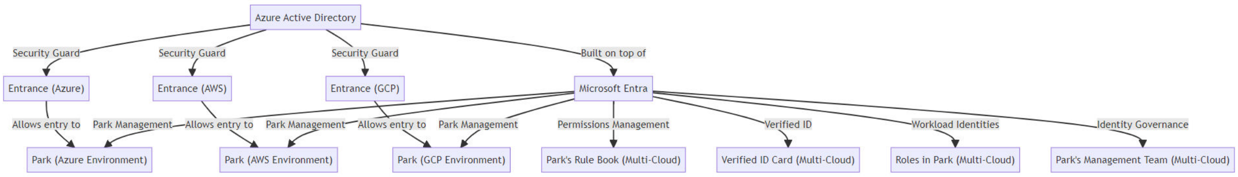
Microsoft Entra Internet Access:

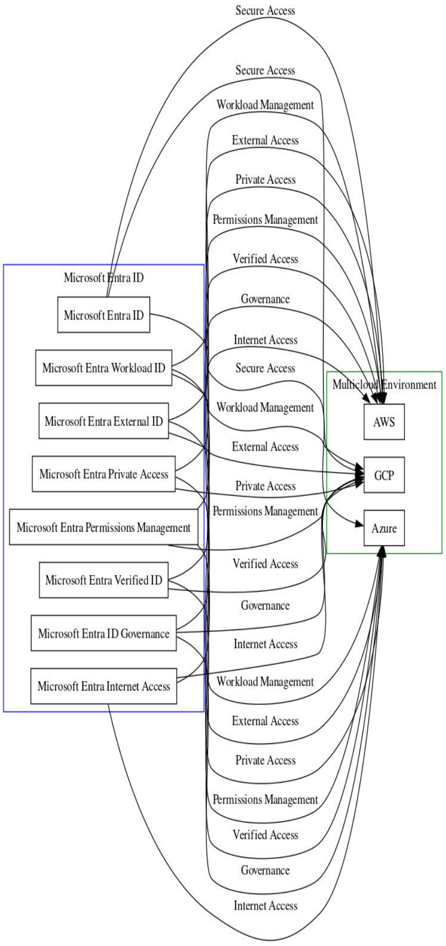
This is like the park's Wi-Fi system. It provides secure internet access to visitors, allowing them to access online services and apps.

Microsoft Entra Private Access:

This is like the park's VIP lounge access. It allows certain visitors to securely connect to private areas (apps) from anywhere in the park.

Microsoft Entra in Multi-Cloud Scenario:





Real-World Use Cases

As a technology specialist we are expected to leverage Microsoft Entra to enhance security, improve operational efficiency, and ensure regulatory compliance.

Here are some real-world use cases:

Multicloud Access Management:

A business with a multicloud environment might struggle to manage access across different cloud platforms. With Microsoft Entra Permissions Management, you can discover and manage permissions across your multicloud infrastructure, ensuring that only authorized users have access to the right resources.

Identity Verification for Secure Interactions:

In a scenario where a business needs to verify the identity of users, devices, or services in a secure and privacy-respecting way, Microsoft Entra Verified ID can be used. This could be useful in industries like finance or healthcare, where verifying identities is crucial.

Managing Workload Identities:

For a business that runs a lot of applications and services, managing their identities and controlling their access to resources can be a challenge. Microsoft Entra Workload Identities can help manage and secure these identities, ensuring that they only have the minimum permissions they need to function.

Regulatory Compliance:

For businesses in regulated industries, meeting compliance requirements can be a significant challenge. Microsoft Entra Identity Governance can simplify operations across on-premises and cloud-based user directories and help ensure compliance with relevant regulations.

Risk Remediation:

Businesses often face risks associated with permissions, such as excessive permissions or unauthorized changes. Microsoft Entra Permissions Management can help identify and fix these risks, enhancing the overall security posture.

Remember, the specific use cases will depend on the business's unique needs and challenges. As an cloud specialist, our role would be to understand these needs and challenges and determine how best to leverage Microsoft Entra to address them.

Is Microsoft Entra is Part of SIEM?

Microsoft Entra is not a Security Information and Event Management (SIEM) solution. Instead, it's a suite of multicloud identity and access products designed to provide secure access to applications and resources. It's built on top of Azure Active Directory (AD), and it extends Azure AD's capabilities to provide more comprehensive identity and access management solutions.

Microsoft's SIEM solution is called Microsoft Sentinel. Microsoft Sentinel is a cloud-native SIEM that provides intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

While Microsoft Entra and Microsoft Sentinel are separate solutions, they can work together as part of a comprehensive security strategy. Microsoft Entra can manage and secure access to resources, while Microsoft Sentinel can monitor and respond to security events related to those resources.

How does Microsoft Entra can help business to reduce cost?

Microsoft Entra, as part of the broader Microsoft Security ecosystem, can help reduce costs in several ways, as highlighted in the blog post you shared:

Simplify Vendor Management:

Managing multiple security solutions from different vendors can be complex and costly. Microsoft Security, including Microsoft Entra, provides a comprehensive security solution that can replace multiple standalone products. This not only simplifies management but can also lead to significant cost savings.

For example, **Rabobank, a financial institution based in the Netherlands, decreased its security vendors from more than 20 to 4**, with Microsoft as its main vendor, **saving €400,000 alone by switching to Microsoft Defender for Cloud**.

Reduce Threats with AI and Automation:

AI and automation can help reduce the workload on IT teams, which are often stretched to the limit due to the increasing number of threats and talent gaps in the industry. AI and automation can help filter events, focus threat investigation on the biggest security issues, and disrupt ransomware attacks.

For instance, **Land O'Lakes** uses AI and machine learning in **Microsoft Sentinel and Microsoft Defender for Cloud to proactively manage threats and reduce alert fatigue**.

Improve Operational Efficiency:

Microsoft Security solutions, including Microsoft Entra, can improve operational efficiency by providing a unified view of security threats and alerts. This can save considerable time for security operations teams.

Frasers Group, a UK sporting goods retailer, was able to keep their security operations center (SOC) team lean by leveraging the automation provided by **Microsoft Sentinel**.

In summary,

Microsoft Entra and the broader Microsoft Security ecosystem can **help organizations "do more with less"** by **simplifying** vendor management, **leveraging** AI and **automation** to reduce threats, and **improving** operational efficiency.

Conclusion

Microsoft Entra is a comprehensive suite of multicloud identity and access products that can help businesses manage identities and access in a complex, multicloud environment.

By providing a unified solution for identity and access management, Microsoft Entra can help businesses enhance security, improve operational efficiency, and ensure regulatory compliance.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/new-name

https://www.microsoft.com/en-in/security/business/microsoft-entra?rtc=1