Introducing Microsoft Entra Workload Identities

What are Workload Identities?

Just like users, a software workload needs an identity to access resources. Two common scenarios in Microsoft Entra today for workload identities are:

- **Managed identities** (also known as managed service identities) use a managed service such as Azure AD Identity Protection or Azure Storage.
- **Application identities** provide access to resources when it’s desirable or necessary to use a service account, as is the case for applications.

Workload identities are part of machine identities for software workloads, such as applications, scripts, and containers that require authentication and authorization as they access resources in cloud environments.

Challenges in securing workload identities

Human users typically have a single identity that is used to access a broad range of resources. Unlike a human user, a software workload may have multiple credentials to access different resources and those credentials need to be stored securely. It’s also hard to track when a workload identity is created or when it should be revoked.

Microsoft Entra Workload Identities helps resolve issues when securing workload identities

With Entra Workload Identities, you strengthen deployment of Zero Trust, empowering you to protect secrets, sensitive data, and other resources via the workload identity. Workload Identities evolves continuously. More features come available often to help provide a clear view into the security of your secrets, assets, and other resources.

Need for securing workload identities

Today, workload identities are part of machine identities for software workloads, such as applications, services, scripts, or containers that require authentication and authorization to access resources in cloud environments.

Managed identities can be used to provision access to an Azure resource such as Azure Key Vault or Azure Storage.

Application identities enable access to resources when IT admins or developers deploy apps in their environment.

Challenges in managing workload identities

Human users typically have a single identity that is used to access a broad range of resources. Unlike a human user, a software workload may have multiple credentials to access different resources and those credentials need to be stored securely. It’s also hard to track when a workload identity is created or when it should be revoked.

Microsoft Entra Workload Identities helps resolve issues when securing workload identities

With Entra Workload Identities, you strengthen deployment of Zero Trust, empowering you to protect secrets, sensitive data, and other resources via the workload identity. Workload Identities evolves continuously. More features come available often to help provide a clear view into the security of your secrets, assets, and other resources.

Microsoft Entra Workload Identities helps resolve issues when securing workload identities

- **Secure access with adaptive policies**
- **Comprehensive logging for workload identities**
- **Multi-factor authentication**
- **Intelligently detect compromised identities**
- **Simplify lifecycle management**
- **Simplify identity management**
- **Workload identity federation**

Microsoft Entra Workload Identities evolves continuously. More features come available often to help protect other areas of the security of your secrets, assets, and other resources.

To date, no single solution addresses today’s challenges in managing workload identities. Enterprises risk their applications or services being exploited or breached because of difficulties in securing workload identities.