

Mendix on Azure FAQ

Overview

What is Mendix on Azure?

Mendix on Azure is a fully managed solution deployed within your Azure environment that configures, manages, and operates all the necessary services to deploy Mendix applications. It leverages Azure Marketplace capabilities to simplify deployment and ongoing maintenance.

Who is Mendix on Azure a good fit for?

- Organizations with highly sensitive data or strict security requirements.
- Customers needing compliance with regulations such as SOC2.
- Businesses integrating legacy systems hosted or reachable on Azure.
- Those requiring control over geographical data residency with deployments in 25+ Azure regions.
- Existing Azure customers wanting quick Mendix adoption with minimum setup burden.

Deployment and Setup

How quickly can Mendix on Azure be deployed?

Customers can deploy Mendix applications within approximately 30 minutes when starting from scratch.

Can the product be hosted in the customer's own Azure subscription?

Yes, the solution must be deployed in the customer's Azure subscription, ensuring data remains within their security perimeter.

How does Mendix on Azure differ from Mendix on Kubernetes?

Deploying Mendix on Kubernetes requires extensive setup of AKS, ACR, databases, storage, monitoring systems (Grafana, Prometheus), DNS, certificates, and Mendix operator. This manual setup takes about 140 hours initially plus quarterly maintenance. Mendix on Azure automates all this, offering faster deployment and simplified management.

Can customers make an app private with no public endpoint?

Yes, apps can be configured without a public endpoint.

Can customers deploy apps to a private virtual network (VNet)?

Yes, deployment to private VNets is a default feature of the product.

Will customers be able to peer with other VNets in their Azure tenant? What are the limitations?

Yes, VNet peering is supported within the customer's Azure tenant.

Can customers add multiple replicas of an app without additional Mendix fees?

Yes, multiple app replicas can be added without additional fees charged by Mendix.

Maintenance and Updates

Who is responsible for updates and maintenance?

Mendix ensures all solution components remain up-to-date by programmatically pushing quarterly updates, relying on Microsoft's managed Azure services for infrastructure components.

How does automatic scaling work?

Mendix on Azure automatically scales infrastructure based on the aggregate capacity configured across app environments. Database capacity can be manually configured and shared by all Mendix apps within the environment.

Security and Data Access

How will security credentials be managed on the Mendix side?

Access uses cross-tenant role assignments with controlled permissions. This means no customer credentials are shared with Mendix at all.

How will Mendix guarantee that Ops staff does not access customer data in the Postgres database?

Mendix has implemented strict controls and limited access through service principals. Only specified automated systems and a very limited number of named resources handle environment access.

Will Mendix have access to my databases?

No, Mendix does not have direct access to customer databases.

How is app data secured?

App data is fully stored within the customer's Azure subscription, using private endpoints and Workload Identity to ensure security without public internet exposure.

How is communication secured between Mendix-managed services and the customer environment?

All communication uses Azure Private Link to eliminate public internet traffic.

Is DDoS Protection required for Mendix on Azure?

No. Microsoft DDoS Protection is optional. Mendix on Azure deploys with built-in security controls that follow Azure best-practice baselines; you add DDoS Protection only if you want stronger safeguards for public-facing endpoints.

Where does DDoS Protection sit, and which tier should we choose?

DDoS Protection is applied outside the AKS cluster—it's enabled on the Virtual Network or individual public IP addresses that front your Mendix apps. It augments the free, always-on platform DDoS defense Azure already provide

Can we place DDoS Protection between the Mendix Platform and the AKS cluster?

No. That channel is outbound-only, has no public endpoint, and therefore isn't a DDoS target. DDoS Protection should be scoped to the public-facing load balancer or Application Gateway that exposes your Mendix apps, not to the internal control-plane traffic.

Database and Resources

Does Mendix on Azure come with backup & restore functionality?

Yes, Mendix on Azure provides full backup & restore capabilities modeled on what we offer on Public Mendix Cloud. This includes automated nightly backups and the ability to upload and download backup snapshots for archival and/or migration purposes. All backups are also stored on the customer's account.

Can customers access the underlying Mendix application database?

Yes, read-only access to the PostgreSQL database is as an optional feature. This can be used for analytics or data warehousing purposes.

Can customers choose Azure SQL instead of PostgreSQL?

No, PostgreSQL is the only supported database option. In case another database is required, Mendix on Kubernetes is the recommended solution.

How can customers tune database and compute resources?

Customers can adjust total database capacity via the Mendix on Azure portal and configure CPU/memory allocations per container to optimize costs.

How are resources like Grafana and Prometheus licensed?

Azure resources are billed through the customer's Azure subscription.

Development and CI/CD

Are the available CI/CD APIs for Mendix on Azure the same as Mendix on Kubernetes?

Yes, the APIs are the same. Some Mendix on Kubernetes-specific APIs (e.g., cluster or namespace creation) are not applicable in Mendix on Azure and thus not available.

Does Mendix on Azure support private GIT servers or GIT repositories like Azure DevOps?

Mendix on Azure requires Mendix Teamserver. Private GIT servers like Azure DevOps are not supported.

Can local CI/CD pipelines be integrated with Mendix APIs?

Yes, integration with Mendix APIs for local CI/CD is possible.

Monitoring and Observability

Will customers have access to logs and metrics similar to Mendix Public Cloud?

Yes, Mendix on Azure provides a Grafana dashboard with equivalent monitoring and metric visibility.

Is there support for Datadog, Dynatrace, or other monitoring tools?

No, these third-party monitoring tools are not supported out of the box.

Connectivity

Can Mendix apps connect to other Azure resources?

Yes, all Mendix connectors for Azure resources are supported, with Azure Private Endpoints ensuring traffic does not traverse the public internet.

Geography and Availability

Why are not all Azure regions available for Mendix on Azure?

Not all Azure regions offer the full set of services required for Mendix on Azure. As of November 2025, 26 Azure regions are available.

Licensing and Pricing

How does licensing work for Mendix on Azure?

Mendix on Azure can be deployed free of charge via Azure Marketplace. This will automatically start a 120-day free trial per app environment. When the trial is about to expire, Mendix will reach out to discuss commercial licensing.

Azure resource costs are billed through the customer's Azure subscription by Microsoft.

Support and Future Plans

Is this like the “former” Mendix Cloud Dedicated offering?

No. Although both run in the customer's environment, their technical architectures and support models differ significantly.

Will there be more customization or flexibility in the future?

Possibly, but Mendix limits customization to ensure scalability and maintain ease of adoption.

Are there plans to offer Mendix on AWS?

This is still under consideration.

Usability

Can non-IT users deploy and manage Mendix on Azure?

Yes, the user interface is designed for ease of use and requires minimal IT or cloud expertise.