

Learn about security options

Last updated by | Hamza Aqel | Jan 10, 2023 at 7:47 AM PST

Contents

- [Introduction:](#)
- [Information protection and encryption](#)
 - [Data in transit:](#)
 - [Data at rest:](#)
- [Customer managed key](#)
- [Network security](#)
 - [Private access:](#)
 - [Public access:](#)
- [Access management](#)
- [Azure Active Directory Authentication](#)

Introduction:

There are multiple layers of security available to help protect the data on your Azure Database for PostgreSQL server. The following information provides details about these security options, such as requirements for customer-managed keys and the two networking options available when running Azure Database for PostgreSQL - Flexible Server.

Information protection and encryption

Azure Database for PostgreSQL encrypts data in two ways:

Data in transit:

Azure Database for PostgreSQL encrypts in-transit data with Secure Sockets Layer and Transport Layer Security (SSL/TLS). Encryption is enforced by default. See [this guide](#) for more details. For better security, you can choose to enable [SCRAM authentication](#). And, although we don't recommend this, if needed, you have an option to disable TLS/SSL for connections to Azure Database for PostgreSQL - Flexible Server by updating the `require_secure_transport` server parameter to OFF. You can also set the TLS version by setting `ssl_min_protocol_version` and `ssl_max_protocol_version` server parameters.

Data at rest:

For storage encryption, Azure Database for PostgreSQL uses the FIPS 140-2 validated cryptographic module. Data is encrypted on disk, including backups and the temporary files created while queries are running.

The service uses the AES 256-bit cipher included in Azure storage encryption, and the keys are system managed. This is similar to other at-rest encryption technologies, like transparent data encryption in SQL Server or Oracle databases. Storage encryption is always on and can't be disabled.

Customer managed key


Data encryption with customer-managed keys is available in [Azure database for PostgreSQL – Flexible Server](#) .


Make sure that the [requirements](#)  are met before enabling customer managed keys.

Network security

When you're running Azure Database for PostgreSQL - Flexible Server, you have two main networking options:

Private access:

You can deploy your server into an Azure virtual network. Azure virtual networks help provide private and secure network communication. Resources in a virtual network can communicate through private IP addresses. See the [networking overview for Azure Database for PostgreSQL - Flexible Server](#) .


Security rules in network security groups let you filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces. See the overview of [network security groups](#) .

Public access:

The server can be accessed through a public endpoint. The public endpoint is a publicly resolvable DNS address. Access to it is secured through a firewall that blocks all connections by default.

IP firewall rules grant access to servers based on the originating IP address of each request. See the [overview of firewall rules](#) .

Access management


While you're creating the Azure Database for PostgreSQL server, you provide credentials for an administrator role. This administrator role can be used to create more [PostgreSQL roles](#) .

[Audit logging](#)  is also available with Flexible Server to track activity in your databases.

However, Azure Database for PostgreSQL - Flexible Server currently doesn't support Azure Defender protection. ETA is Q1CY23 (Under NDA).

For more information, see [Security in Azure Database for PostgreSQL - Flexible Server](#) .

Azure Active Directory Authentication

Azure Active Directory (Azure AD) Authentication is available in Azure database for PostgreSQL – Flexible server. For more information, see the [concepts guide](#) .

To configure your server with Azure AD, see how to [configure AAD authentication in Azure database for Flexible server](#) .