SQL Sentry Azure SQL Database and Azure Synapse SQL Pools Security

Last Modified on 21 November 2022

In this article:

Account Permissions

The monitoring service requires the **server admin** account for Azure SQL Database and Azure Synapse SQL Pool targets.

The credentials provided for an Azure SQL Database target must be the server account configured in the Azure Portal for the Azure SQL Server so that **full access** is available for monitoring.

Authentication Methods

The following authentication methods are supported when adding Azure SQL Database target types:

- SQL Server
- Azure Active Directory - Password
- Azure Active Directory - Integrated

Multi-Factor Authentication

Using service accounts that require Multi-Factor Authentication (MFA) is not currently supported for connecting the SQL Sentry monitoring service to Azure SQL Database targets. It is recommended that generalized service accounts are used for configuring connection credentials rather than accounts that are directly linked to users. For environments that require MFA for Azure Active Directory users, a service account can be excluded from the MFA requirement by using an exclusion for conditional access.

Additional Information: See the Use Azure AD access reviews to manage users excluded from Conditional Access policies article on Microsoft Docs for guidance on how to set up exclusions for MFA.

Firewall

The Microsoft Azure SQL Database and Azure Synapse SQL Pools services are protected by a firewall because both services are exposed on the internet. The **Azure SQL Firewall** is in place to help protect access to your data. When creating a new Azure SQL Database or Azure Synapse SQL Pools target, the connectivity verification ensures that an **Azure SQL Firewall** rule is correctly configured and indicates a warning if it's not.

Azure SQL Database and Azure Synapse SQL Pools Firewall Configuration

It is important to *allowlist* the IP address of the server hosting the SQL Sentry monitoring service via the Azure Portal. Depending on the software version, this may be called the SentryOne monitoring service.

The **Azure SQL Firewall** settings are configured using the Azure Portal, through the command line utilities on **PowerShell,** or through the **Cross Platform CLI** tool. For more information about the **Azure SQL Firewall** and configuring it, see the How to configure an Azure SQL database firewall documentation from Microsoft.

⚠ **Important:** Because the **Azure SQL Firewall** rules can change, the monitoring service can lose access. If this occurs, notifications appear in the **System Status** and on the **Dashboard** as a warning.

While the firewall is blocking the monitoring service, no data is retrieved from the target.