

Enable Azure Defender for SQL in an Azure SQL Database

Understand the scenario

You are an Azure® administrator for a company that is migrating its primary web app from its on-premises datacenter to Azure. You need to create a new Azure SQL database and enable Azure Defender for SQL. First, you will create an Azure SQL database. Next, you will enable Azure Defender for SQL. Finally, you will verify the security features of Azure Defender for SQL.

Understand your environment

You will be using an Azure resource group named corp-datalod26435737 that contains no resources.

# **Create an Azure SQL Database**

* Sign in to the Azure portal
* Create an Azure SQL database on a new logical SQL server by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26435737** |
| Database name | db26435737 |
| Server name | sql26435737 |
| Server admin login | AzureAdmin |
| Password | AzPwd26435737! |
| Location | **(US) East US** |
| Compute + storage | **Standard S0** |
| DTUs | **10 (S0)** |
| Data max size | **250 GB** |
| Connectivity method | **Public endpoint** |
| Allow Azure services and resources to access this server | **Yes** |
| Add current client IP address | **Yes** |
| Use existing data | **Sample** |
| Enable Azure Defender for SQL | **Not now** |

* Expand this hint for guidance on creating the Azure SQL database.

The sample data will use the AdventureWorksLT sample database.

It will take approximately 3–5 minutes to deploy the Azure SQL database.

[Azure SQL Database](https://docs.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview) is a fully managed database that supports automatic patching, upgrades, and backups.

* Log in to the **db26435737** database as AzureAdmin using AzPwd26435737! as the password, and then create a query to retrieve all of the rows in the SalesLT.Customer table.

Expand this hint for guidance on querying the Azure SQL database.

* + Run the following query to retrieve all of the rows in the SalesLT.Customer table:

SELECT \* FROM SalesLT.Customer

* Close the **Query editor** without saving any changes.

## Check your work

* Confirm that you created an Azure SQL database named db26435737.
* Confirm that you created a new logical SQL server named sql26435737.
* Confirm that you ran a query to retrieve all of the rows in the SalesLT.Customer table.

# **Enable Azure Defender for SQL**

* Enable Azure Defender for SQL for the **db26435737** database.

Expand this hint for guidance on enabling Azure Defender for SQL.

If the Getting Started page is displayed when you open Security Center, close the page in order to continue.

* Perform a vulnerability assessment for the **db26435737** database.

Expand this hint for guidance on performing a vulnerability assessment.

* Review the recommendations provided in the vulnerability assessment for the database.

[SQL Vulnerability Assessment](https://docs.microsoft.com/en-us/azure/azure-sql/database/sql-vulnerability-assessment) is a feature of Azure Defender for SQL that you can use to identify and remediate potential database vulnerabilities.

* Remediate the failing **Auditing should be enabled at the server level** security check by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Enable Azure SQL Auditing | **ON** |
| Audit log destination | **Storage** |
| Storage account | **Create new** |
| Name | sa26435737 |
| Account kind | **StorageV2 (general purpose v2)** |

* Expand this hint for guidance on enabling auditing at the server level.

The [Auditing](https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview" \o "Auditing for Azure SQL Database" \t "_blank) feature for Azure SQL Database records database and server level events and writes them to an audit log which can be hosted in an Azure storage account, a Log Analytics workspace, or an Event Hub.

## Check your work

* Confirm that you enabled Azure Defender for SQL for the db26435737 database.
* Confirm that you enabled auditing at the server level.

# **Manage security recommendations in Azure Defender for SQL**

* Review the **Data Discovery & Classification** recommendations for the **db26435737** database, and then accept all of the recommendations.

Expand this hint for guidance on reviewing the Data Discovery & Classification recommendations.

You can use [Data Discovery & Classification](https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview) to discover and classify sensitive data columns in a database, as well as create custom labels and reports.

* Review the vulnerability assessment recommendations again.

The Auditing at the server level should be enabled and the Sensitive data columns should be classified security checks that were failing may still be displayed. If you perform a scan to update the list, the two vulnerabilities you remediated should be removed from the list of failing security checks.

* Remediate the **Server-level firewall rules should be tracked and maintained at a strict minimum** failing security check.

Expand this hint for guidance on remediating the server-level firewall rules security check.

The Server-level firewall rules should be tracked and maintained at a strict minimum security check identifies a vulnerability that exists because you enabled the Allow Azure services and resources to access this server option and configured the Client IP address firewall rule on the server.

* Perform another scan, and then review the vulnerability assessment recommendations again.
* Review the **'dbo' user should not be used for normal service operation** failing security check, and then approve the current scan result as the Baseline value.

Expand this hint for guidance on setting a Baseline value.

You can select the Approve as Baseline option to indicate that you accept the current settings. The failing security check will not appear in the list of vulnerabilities after the next scan unless you change the current settings.

* Perform another scan, and then review the vulnerability assessment recommendations again.
* Attempt to log in to the **db26435737** database as AzureAdmin using AzPwd26435737! as the password.

Expand this hint for guidance on attempting to log in to the database.

Access should be denied because you removed the Client IP address firewall rule. If access is still allowed, refresh the browser, and then try again.

## Check your work

* Confirm that you accepted the Data Discovery & Classification recommendations for the database.
* Confirm that you reviewed the vulnerability assessment for the database.
* Confirm that you applied selected vulnerability assessment recommendations to the database.

# **Summary**

Congratulations, you have completed the **Enable Azure Defender for SQL in an Azure SQL Database** challenge.

You have accomplished the following:

* Created an Azure SQL database.
* Enabled Azure Defender for SQL.
* Performed a vulnerability assessment.
* Remediated a failing security check.
* Applied Data Discovery & Classification recommendations for the database.