

Enable Security for an Azure SQL Database

Understand the scenario

You are an Azure® administrator. You need to enable security for an Azure SQL database. First, you will create an Azure SQL database. Next, you will enable Azure Defender for SQL, and then you will perform a vulnerability assessment. Finally, you will enable database auditing by using a storage account for the audit log.

Understand your environment

You will be using an Azure resource group named corp-datalod26434675 that contains no resources.

# **Create an Azure SQL database**

* Sign in to the Azure portal

Select the Copy to clipboard icon to copy the text string to the clipboard.

A cloud slice is a subset of an Azure subscription that has been assigned to a user account that was provisioned for you for the duration of this challenge lab. A cloud slice provides temporary access to a subset of resources available in a cloud subscription so that you can learn the concepts in this challenge lab without having to configure your own subscription.

A cloud slice has restrictions on the types of administrative activities that are allowed. Please follow the instructions carefully, especially with regard to names and other configuration details.

* 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-datalod26434675** |
| Database name | db26434675 |
| Server name | sql26434675 |
| Server admin login | AzureAdmin |
| Password | AzPwd26434675! |
| 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** |
| Enable Azure Defender for SQL | **Not now** |
| Use existing data | **Sample** |

* Expand this hint for guidance on creating an Azure SQL database.
  + Review the documentation on [creating an Azure SQL database](https://docs.microsoft.com/en-us/azure/azure-sql/database/single-database-create-quickstart?tabs=azure-portal" \o "Create an Azure SQL database" \t "_blank).
* Log in to the **db26434675** database as AzureAdmin using AzPwd26434675! 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 using the query editor in the Azure portal.

* + Review the documentation on using the [query editor](https://docs.microsoft.com/en-us/azure/azure-sql/database/connect-query-portal" \o "Use the query editor in the Azure portal to query an Azure SQL database" \t "_blank) in the Azure portal.

If you are prompted for a certificate, select **Cancel**.

## Check your work

Verify that you have created an Azure SQL database.

Verify that you have created a new logical SQL server.

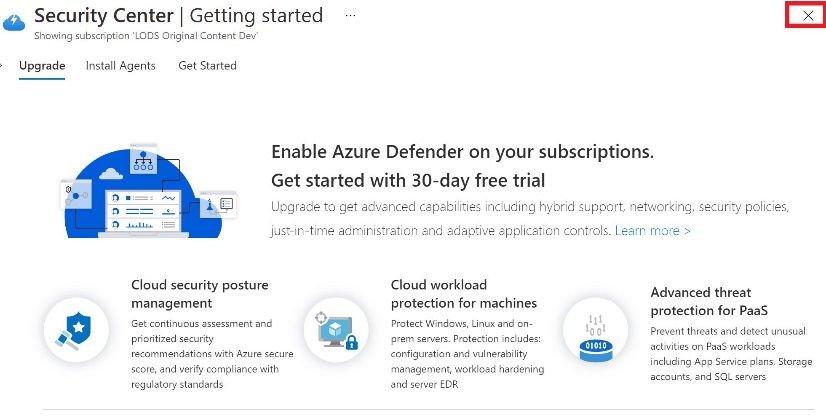
# **Enable Azure Defender for SQL**

* Enable Azure Defender for SQL for the **db26434675** database.

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

* + Review the documentation on [enabling Azure Defender for SQL](https://docs.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql" \l "enable-azure-defender-for-azure-sql-database-at-the-resource-level" \o "Enable Azure Defender for Azure SQL Database" \t "_blank).

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



* Perform a vulnerability assessment for the **db26434675** database.

Expand this hint for guidance on performing a vulnerability assessment.

* + Review the documentation on [performing a vulnerability assessment](https://docs.microsoft.com/en-us/azure/azure-sql/database/sql-vulnerability-assessment" \o "The SQL vulnerability assessment documentation" \t "_blank).

The vulnerability assessment scan may take a few minutes to fully register in Azure.

## Check your work

Verify that you have enabled Azure Defender for SQL.

Verify that you have performed a vulnerability assessment.

# **Enable database auditing**

* Enable database auditing on the **db26434675** database, and then store the audit log in the existing storage account in the challenge subscription.

Expand this hint for guidance on enabling auditing for Azure SQL Database.

* + Review the documentation on [enabling auditing for Azure SQL Database](https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview" \o "Auditing for Azure SQL Database" \t "_blank).
* Log in to the **db26434675** database as AzureAdmin using AzPwd26434675! as the password.
* Attempt to drop the SalesLT.Customer table by using the [DROP TABLE](https://docs.microsoft.com/en-us/sql/t-sql/statements/drop-table-transact-sql) statement, and then review the error message.

Expand this hint for guidance on attempting to drop a table.

* + Review the documentation on [attempting to drop a table](https://docs.microsoft.com/en-us/sql/t-sql/statements/drop-table-transact-sql" \l "examples" \o "Dropping a table in the current database" \t "_blank).

You should see the following error message:

Failed to execute query. Error: Could not drop object 'SalesLT.Customer' because it is referenced by a FOREIGN KEY constraint.

* Review the audit log for the **db26434675** database, and then review the audit record of the failed DROP TABLE statement.

Expand this hint for guidance on reviewing the audit log for a database.

* + Review the documentation on [reviewing the audit log for a database](https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview" \l "subheading-3" \o "Analyze audit logs and reports" \t "_blank).

## Check your work

Verify that you have enabled database auditing.

Congratulations, you have completed the **Can You Enable Security for an Azure SQL Database?** challenge.

You have accomplished the following:

* Created an Azure SQL database.
* Enabled Azure Defender for SQL.
* Performed a vulnerability assessment.
* Enabled database auditing.