# SQL Database - Threat Detection

**Overview**

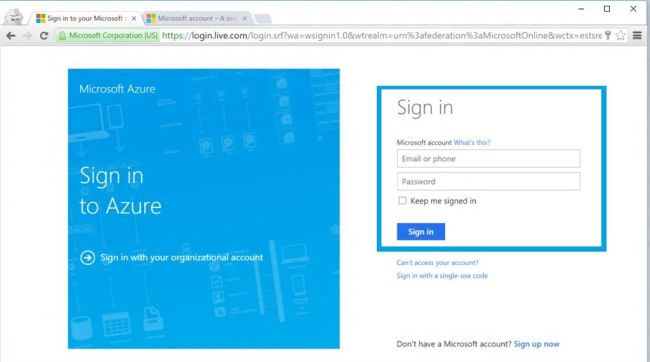
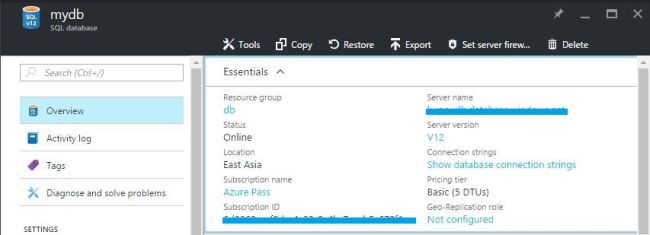
Threat detection detects abnormal database activities indicating potential security threats to the database and offers a new layer of security, which enables the customers to detect and respond to the potential threats as they occur by providing security alerts on abnormal activities. The customers can explore suspicious events, using Azure SQL database auditing to determine, if they result from an attempt to access, breach or exploit the data in the database. Threat detection makes it simple to address possible threats to the database without the need to be a security expert or manage advanced security monitoring systems.

For example, Threat detection detects certain abnormal database activities, thereby specifying the potential SQL injection attempts. SQL injection is one of the common Web Application security problems on the Internet, used to attack data-driven Applications. The attackers take advantage of the Application vulnerabilities to inject malicious SQL statements into Application entry fields, for breaching or modifying the data in the database.

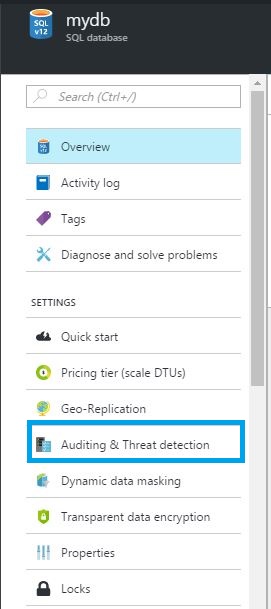
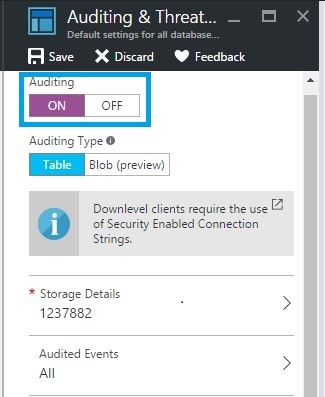
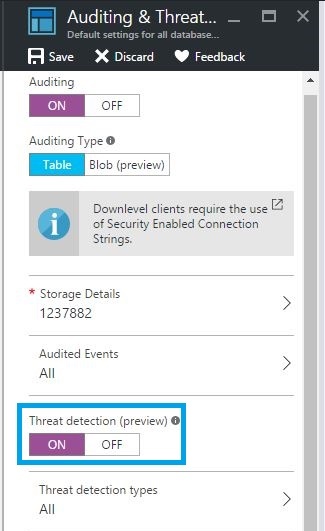
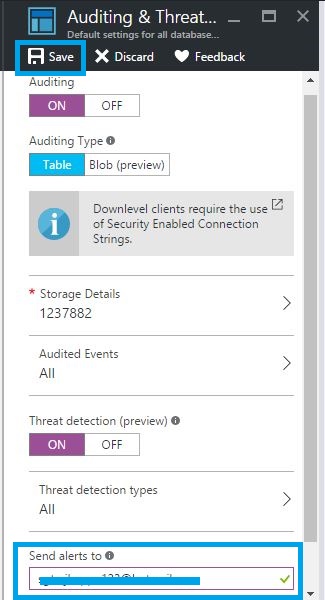
**Prerequisites**

* Azure account.

Now, let's get started with the steps, given below-

**Step 1-**Sign in to the online [Microsoft Azure Portal](https://portal.azure.com/).  
  
  
  
On SQL Servers blade, navigate to the configuration blade of SQL database.  
  


Choose auditing & threat detection option.

  
  
In the auditing & threat detection configuration blade, turn ON auditing, which will display the threat detection settings.  
  
  
  
Turn ON threat detection.  
  
  
  
Finally, type Email ID to get the thread information. Click save in the auditing & threat detection configuration blade to save the new or updated auditing and threat detection policy.  
  
  
  
We will receive an Email notification upon the detection of unusual database activities.  
  
The Email will give the information on the suspicious security event, including the nature of the anomalous activities, database name, Server name and the event time.