How-To Library

# How to Use the Security Rule Set Simulator for Microsoft Azure SQL Database

© Copyright Informatica LLC 2019. Informatica, the Informatica logo, and PowerExchange are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html

# Abstract

Use the Security Rule Set Simulator to test security rules and regular expressions for Microsoft Azure SQL Database.

# Supported Versions

- Dynamic Data Masking 9.9

# Table of Contents

Overview. . . . . 2
Running the Security Rule Set Simulator. . . . . 2
Testing the Security Rule for the Dynamic Data Masking Administrator Role. . . . . 3
Testing the Security Rule for the Dynamic Data Masking User Role. . . . . 3
Determining the Value for the AUTH_EXEC_USER Symbol. . . . . 3

# Overview

Use the Security Rule Set Simulator to test security rules that prevent unauthorized access to data.

To prevent unauthorized access, you create a security rule that prevents non-privileged users from viewing sensitive employee data. To test the security rule, you run a simulation from the Security Rule Set Simulator.

Access the Security Rule Set Simulator from the Rule Editor on the Management Console. To set up the simulation, specify the database and database user information, define symbols, and enter an SQL statement that will test the new security rule. The simulator tests the rule and displays the results as a log file. Review the results to verify if the security rule masks data correctly.

To gather more information on the simulation, run the Security Rule Set Simulator in debug mode.

# Running the Security Rule Set Simulator

Run the Security Rule Set Simulator to test a rule, a rule folder, or a rule set.

Open the Security Rule Set Simulator from the **Action** menu in the Rule Editor. Select **Action** > **Security Rule Set Simulator**.

Run the Security Rule Set Simulator on the following rule tree nodes:

**Rule**

To run the simulator on a rule, select the rule in the Rule Editor and open the Security Rule Set Simulator. The simulator tests only the rule, even if the rule uses the Continue processing action.

**Rule Folder**

To run the simulator on the rules in a rule folder, select the rule folder in the Rule Editor and open the Security Rule Set Simulator. The simulator tests all the rules in the folder. The simulator stops running after it tests the last rule in the rule folder, even if the last rule uses the Continue processing action.

**Rule Set**

To run the simulator on the rules in a rule set, select the rule set in the Rule Editor and open the Security Rule Set Simulator. The simulator tests the rules in the rule set and applies the processing actions.

## Testing the Security Rule for the Dynamic Data Masking Administrator Role

Test security rules for data on Microsoft Azure SQL Database using the Dynamic Data Masking administrator role.

1. In the **DDM Database Name** field, enter the Azure SQL Database name that you defined in the Management Console.
2. In the **DBA Username** field, enter the user name of the Dynamic Data Masking administrator.
3. In the **DBA Password** field, enter the password for the Dynamic Data Masking administrator.
4. In the **Symbol Definition** section, enter a value in the **Symbol Value** column for AUTH_CURRENT_DATABASE.

   The symbol value for AUTH_CURRENT_DATABASE is the database name in Microsoft SQL Server that the user can access.
5. In the **SQL Statement** field, enter a SQL statement to test the rule.
6. Click **Run**.

   The simulator tests the rule and displays the results in the **Log output** section.
7. To view the detailed log, click **Debug Mode**. The detailed log displays additional information about the connection and the Dynamic Data Masking server.
8. To save the Security Rule Set Simulator parameters and log output to a file, click **Save File**. You can load the saved parameters and log output to a new instance of the Security Rule Set Simulator.
9. To exit the Security Rule Set Simulator, click **Close**.

## Testing the Security Rule for the Dynamic Data Masking User Role

Test security rules for data on Microsoft Azure SQL Database using the Dynamic Data Masking user role.

1. In the **DDM Database Name** field, enter the Azure SQL Database name that is defined in the Management Console.
2. In the **DBA Username** field, enter the user name of the Dynamic Data Masking user.
3. In the **DBA Password** field, enter the password for the Dynamic Data Masking user.
4. In the **Symbol Definition** section, enter a value for the following symbols:
   - AUTH_CURRENT_DATABASE
   - AUTH_USERNAME
   - AUTH_EXEC_USER
5. In the **SQL Statement** field, enter a SQL statement to test the rule.
6. Click **Run**.

   The simulator tests the rule and displays the results in the **Log output** section.
7. To view the detailed log, click **Debug Mode**. The detailed log displays additional information about the connection and the Dynamic Data Masking server.
8. To save the Security Rule Set Simulator parameters and log to a file, click **Save File**. You can load the saved parameters and log to a new instance of the Security Rule Set Simulator.
9. To exit the Security Rule Set Simulator, click **Close**.

## Determining the Value for the AUTH_EXEC_USER Symbol

1. Log in to Microsoft Azure SQL Database with the Dynamic Data Masking user account that you want to test.

2. Run the following query: `SELECT CURRENT_USER`

   The value appears. Use this value for the **AUTH_EXEC_USER** symbol on the **Security Rule Set Simulator** page.

## Author