**Manage Sensitive Data with Dynamic Data Masking and Data Encryption**

**Create a Sample Database**

**A screenshot of a computer

Description automatically generated**

1. The Essentials section will list important info about the database; find Server name listed there, then click the link below it.
2. On the SQL server page that opens, under the Security section in the left-hand menu, click on Firewalls and virtual networks to begin adding your IP address to the firewall.
3. Near the top of the page, just below the header, click on + Add client IP. This will automatically add your IP to the list of whitelisted IPs. Other settings on this page will be left as default, so no other changes are necessary.
4. Click on Save to save the change.

A screenshot of a computer

Description automatically generated

**Create an SQL User Account**

At Globomantics Corporation, power users like the data analyst are not allowed to view sensitive customer details like email, phone number, or Tax Identification Number (TIN). Before you implement these policies, you will create a user account and login for the data analyst (data\_analyst for the Data Analyst) that will demonstrate different access capabilities. The user accounts can only be created from the master database which is currently not available in Query editor (preview) on the Azure portal. So, for this challenge you will need to use Azure Data Studio. You could also accomplish these tasks with SQL Server Management Studio (SSMS) if you're familiar with it.

1. In the Azure portal, click on Overview in the left pane to view details for your SQL server. Copy the Server name to your clipboard, it will look something like globomantics-prod-server-1341998.database.windows.net .

A screenshot of a computer

Description automatically generated

1. Open Azure Data Studio, then in the Servers section of the left pane, click the New Connection button to connect to the SQL database. Fill in the Connection Details with these settings:

* Connection type: Microsoft SQL Server
* Server: Paste in the server name
* Authentication type: SQL Login
* User name: globomantics\_admin
* Password: 4-v3ry-53cr37-p455w0rd

1. Click Connect, and once connected you should see the globomanticsDB and master SQL databases listed in the table. Note that, in the navigation pane on the left, the master DB will be listed under Databases > System Databases.
2. Right click on the master database, then click New Query.
3. In the query editor, paste in this script, then click Run.

--run in master

CREATE LOGIN [data\_analyst] WITH PASSWORD = 'wb#rR1Aks4ZGv2S#'

GO

CREATE USER [data\_analyst] FOR LOGIN [data\_analyst];

Upon successful execution of the above script, you should see the following output: Commands completed successfully.

A screenshot of a computer

Description automatically generated

1. Open a new query editor for the **globomanticsDB** database.
2. Execute the following script in the **globomanticsDB** database.

A screenshot of a computer

Description automatically generated

1. execute as user = 'data\_analyst'

select top 5 CustomerID,EmailAddress,CompanyName,phone,PasswordHash,PasswordSalt from SalesLT.Customer

A screenshot of a computer

Description automatically generated

**Set up Dynamic Data Masking from the Azure Portal**

Data analysts at Globomantics Corporation are not privileged to see the account numbers, tax amounts, email addresses and usernames of customers. As a data engineer, you will apply the necessary masking rules to these columns to hide this sensitive data.

1. Back in the Azure portal, use the search bar to navigate to the **globomanticsDB** SQL database page.
2. Under the **Security** section of the navigation pane, click on **Dynamic Data Masking**. This page shows the list of tables and columns in the database that are recommended for masking.
3. For each of these three columns, click the respective **Add mask** button to mask the columns using the default Dynamic Data Masking function: **Phone**, **PasswordHash,** **PasswordSalt**.

A screenshot of a computer

Description automatically generated

1. Click on **Save** to apply the masking.
2. To mask the tables which are not part of the recommendations, in the Azure portal click on + Add mask, then configure the settings as follows:

* Schema: SalesLT
* Table: Customer
* Column: EmailAddress
* Masking field format: Email

1. Click on Add at the top.
2. Click on Save to save changes.
3. If you run the script from task 5 above again, the EmailAddress column should now be masked with the email masking rule.
4. In case you want to change the default masking format to another masking format, in the Azure portal click on one of the masking rules in the Masking rules table (eg SalesLT\_Customer\_EmailAddress).
5. Select the Masking field format you want, then click Update.
6. Click on Save.

A screenshot of a computer

Description automatically generated

**Mask String Values with a Custom Format**

The data analysts are not privileged to access customer addresses. Company policy requires that non-privileged  users only see the first two and last four characters of customer addresses. As a data engineer you will design and implement this preferred format to meet this business requirement.

1. Back in the Azure portal on the **Dynamic Data Masking** page for the **globomanticsDB** database, click on **+ Add mask** to add a new custom mask, then configure the settings as follows:

* Schma: **SalesLT**
* Table: **Address**
* Column: **AddressLine1**
* Masking field format: Select **Custom string**
* Exposed prefix: 2 to expose the first two characters
* Exposed suffix: 4 to expose the last four characters

1. Click **Add** then **Save**.

A screenshot of a computer

Description automatically generated

1. Execute this query against the **globomanticsDB** database:

select top 10 \* from SalesLT.Address

A screenshot of a computer

Description automatically generated

﻿

The results should show that the masking rule has been applied to the *AddressLine1* column – you'll see just the first two and last four characters.

**Grant Access to Users to View Masked Data**

When masking is applied on columns, administrators and database owners can see the data on masked columns as usual. The data analysts at Globomantics Corporations, due to their reporting work, now need to have elevated privileges to see all data columns. In addition, the **PasswordHash** column we masked in the previous step is no longer needed since data contained in the column is already hashed. Follow the below steps to meet these business requirements.

1. To give access to the data analysts,  enter data\_analyst in the text box just under the **Masking rules** section.
2. To remove masking on the **PasswordHash** column, click on the masking rule **SalesLT\_Customer\_PasswordSalt**.
3. In the **Edit Masking rule** window, click on the **Delete** button, and then click **Save**.
4. Now run this query against **globomanticsDB**:

A screenshot of a computer

Description automatically generated

execute as user = 'data\_analyst'

select top 5 CustomerID,EmailAddress,CompanyName,phone,PasswordHash,PasswordSalt from SalesLT.Customer

A screenshot of a computer

Description automatically generated

**Manage Transparent Data Encryption in Azure Portal**

Transparent data encryption (TDE) is an encryption mechanism to help you protect Azure Synapse Analytics and Azure SQL database. It protects your Azure Synapse Analytics against threats of malicious offline activity by encrypting data at rest. TDE performs real-time encryption as well as decryption of the database, associated backups, and transaction log files at rest without you having to make changes to the application. In order to use TDE for Azure Synapse Analytics, you will have to manually enable it.

1. On the **globomanticsDB** SQL database page in the Azure portal, in the left pane under the **Security** section, click on **Transparent data encryption**. This page shows whether data encryption is enabled or not.
2. By default the service-managed TDE is used and therefore a TDE certificate is automatically generated for the server that contains that database. Toggle Data encryption **ON** if it is off, the click **Save**.