

# Outbound Firewall Rules - Configuration

Last updated by | Subbu Kandhaswamy | Mar 9, 2022 at 10:26 AM PST

## Contents

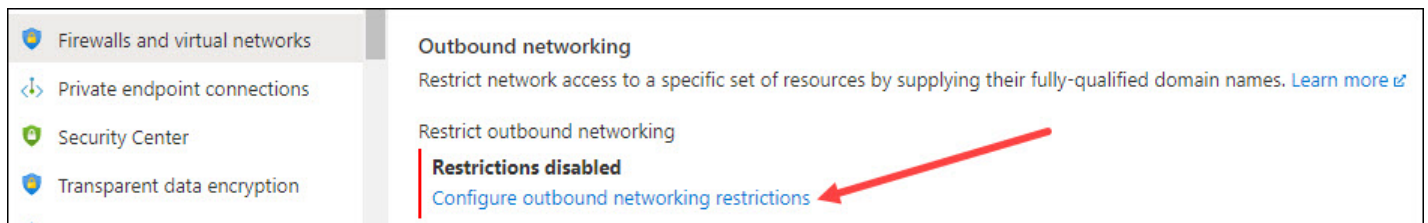
- [Introduction](#)
- [Configuring OFR in the Azure Portal](#)
- [Configuring using PowerShell](#)
- [Configuring OFR using Azure CLI](#)
- [Troubleshooting](#)
  - [Checking enforcement of Outbound Firewall Rules](#)
  - [Auditing](#)
  - [Vulnerability Assessment](#)
  - [I/E Service](#)
  - [Kusto Query](#)
- [Common Errors and Cause](#)

## Introduction

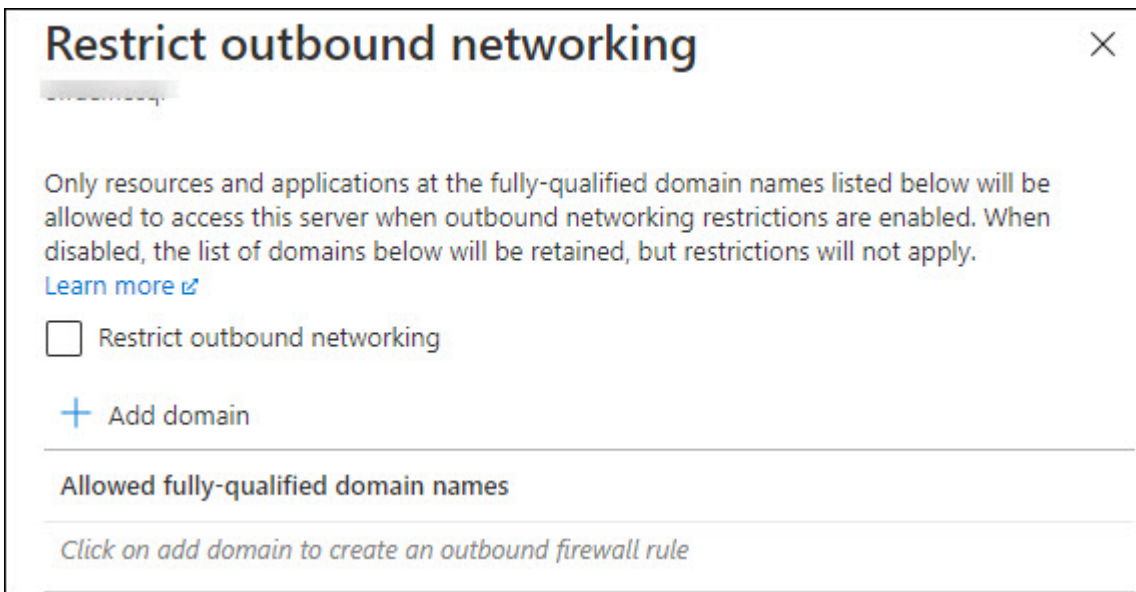
Outbound Firewall Rules limits network traffic from Azure SQL to a customer defined list of Storage accounts and any attempt to access Storage accounts that are not in this list is denied. The following Azure SQL DB features support this feature Auditing, Vulnerability Assessment, I/E Service, OpenRowset, Elastic Query and Bulk Insert.

## Configuring OFR in the Azure Portal

- Browse to the Outbound networking section in the Firewalls and virtual networks blade for your Azure SQL Database and select Configure outbound networking restrictions.



This will open up the following blade on the right-hand side:



## Restrict outbound networking

Only resources and applications at the fully-qualified domain names listed below will be allowed to access this server when outbound networking restrictions are enabled. When disabled, the list of domains below will be retained, but restrictions will not apply.

[Learn more](#)

☐ Restrict outbound networking

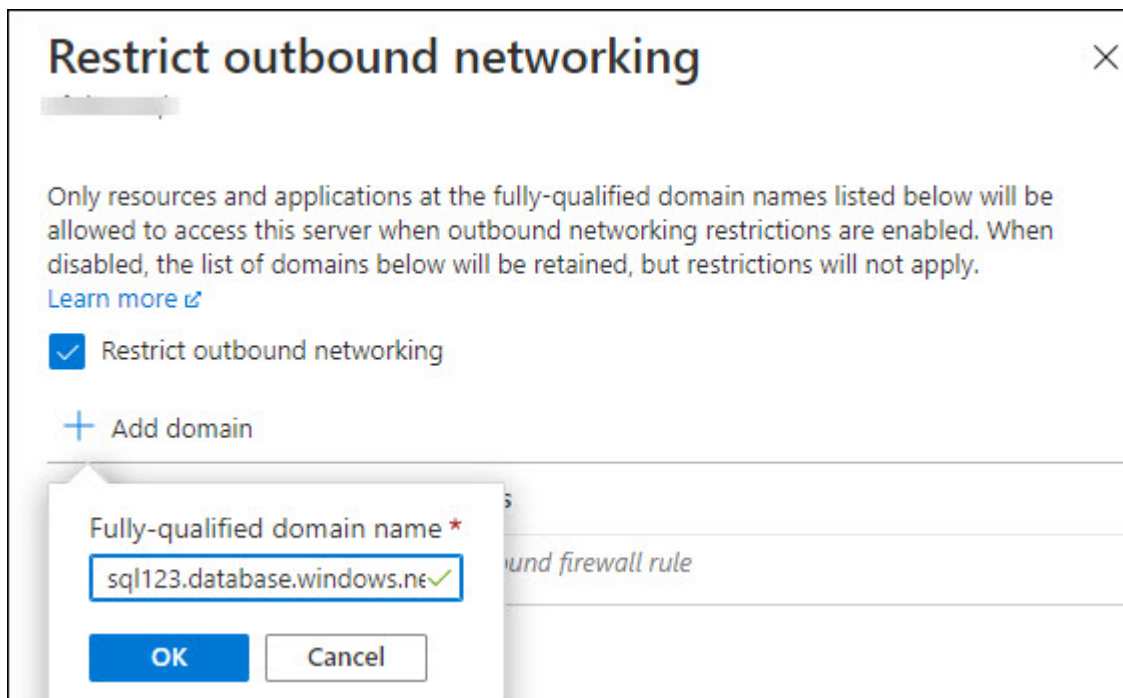
+ Add domain

---

**Allowed fully-qualified domain names**

*Click on add domain to create an outbound firewall rule*

- Select the check box titled Restrict outbound networking and then add the FQDN for the Storage accounts (or SQL Databases) using the Add domain button.



## Restrict outbound networking

Only resources and applications at the fully-qualified domain names listed below will be allowed to access this server when outbound networking restrictions are enabled. When disabled, the list of domains below will be retained, but restrictions will not apply.

[Learn more](#)

☒ Restrict outbound networking

+ Add domain

Fully-qualified domain name \*

sql123.database.windows.net ✓

OK Cancel

---

*Click on add domain to create an outbound firewall rule*

- After you're done, you should see a screen similar to the one below. Select OK to apply these settings

## Restrict outbound networking

Only resources and applications at the fully-qualified domain names listed below will be allowed to access this server when outbound networking restrictions are enabled. When disabled, the list of domains below will be retained, but restrictions will not apply.



[Learn more](#)

☒ Restrict outbound networking

+ Add domain

---

Allowed fully-qualified domain names

sql123.database.windows.net	
ofrstore.blob.core.windows.net	

## Configuring using PowerShell

Azure SQL Database still supports the PowerShell Azure Resource Manager module, but all future development is for the Az.Sql module. For these cmdlets, see AzureRM.Sql. The arguments for the commands in the Az module and in the AzureRm modules are substantially identical. The following script requires the Azure PowerShell module.

The following PowerShell script shows how to change the outbound networking setting (using the RestrictOutboundNetworkAccess property):

```
# Get current settings for Outbound Networking
(Get-AzSqlServer -ServerName <SqlServerName> -ResourceGroupName <ResourceGroupName>).RestrictOutboundNetworkAc

# Update setting for Outbound Networking
$SecureString = ConvertTo-SecureString "<ServerAdminPassword>" -AsPlainText -Force

Set-AzSqlServer -ServerName <SqlServerName> -ResourceGroupName <ResourceGroupName> -SqlAdministratorPassword $
```

Use these PowerShell cmdlets to configure outbound firewall rules

```
# List all Outbound Firewall Rules
Get-AzSqlServerOutboundFirewallRule -ServerName <SqlServerName> -ResourceGroupName <ResourceGroupName>

# Add an Outbound Firewall Rule
New-AzSqlServerOutboundFirewallRule -ServerName <SqlServerName> -ResourceGroupName <ResourceGroupName> -Allowe

# List a specific Outbound Firewall Rule
Get-AzSqlServerOutboundFirewallRule -ServerName <SqlServerName> -ResourceGroupName <ResourceGroupName> -Allowe

#Delete an Outbound Firewall Rule
Remove-AzSqlServerOutboundFirewallRule -ServerName <SqlServerName> -ResourceGroupName <ResourceGroupName> -All
```

## Configuring OFR using Azure CLI

The following CLI script shows how to change the outbound networking setting (using the RestrictOutboundNetworkAccess property) in a bash shell:

```
# Get current setting for Outbound Networking
az sql server show -n sql-server-name -g sql-server-group --query "RestrictOutboundNetworkAccess"

# Update setting for Outbound Networking
az sql server update -n sql-server-name -g sql-server-group --set RestrictOutboundNetworkAccess="Enabled"
```

Use these CLI commands to configure outbound firewall rules

```
# List a server's outbound firewall rules.
az sql server outbound-firewall-rule list -g sql-server-group -s sql-server-name

# Create a new outbound firewall rule
az sql server outbound-firewall-rule create -g sql-server-group -s sql-server-name --outbound-rule-fqdn allowe

# Show the details for an outbound firewall rule.
az sql server outbound-firewall-rule show -g sql-server-group -s sql-server-name --outbound-rule-fqdn allowedF

# Delete the outbound firewall rule.
az sql server outbound-firewall-rule delete -g sql-server-group -s sql-server-name --outbound-rule-fqdn allowe
```

## Troubleshooting

### Checking enforcement of Outbound Firewall Rules

The following section demonstrates how to check enforcement of Outbound Firewall Rules on the SQL DB specific features. As a pre-requisite for this you need to have done the following

1. Set flag on the logical Sql Server instance to enable Outbound Firewall Rules
  - Refer to PUT RestrictOutboundNetworkAccess to Yes
2. Create an Outbound Firewall Rule for a specific storage account
  - Refer to PUT an Outbound Firewall Rule

*For purposes of illustration I have setup and OFR allowing traffic from ofrdemosql to ofrdemostorage1. I have another storage account ofrdemostorage2 that is in the same resource group and not covered by any OFR – hence will be blocked for any network traffic from ofrdemosql*


### Auditing

When you attempt to setup Auditing to a storage account that is not covered by OFR ( e.g. ofrdemostorage2) the following error will be raised as follows

 Save  Discard  Feedback

## Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. [Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing 


Audit log destination (choose at least one):

☒ Storage

Subscription \*

Storage account \*


[Create new](#)

 Advanced properties

## Error configuring Auditing for OFR

*Failed to save server Auditing settings Failed to save Auditing settings for server: ofrdemosql. Storage account 'ofrdemostorage2' is not in the list of allowed FQDNs on the Azure SQL Server. Please add the target to the list of allowed FQDNs on server 'ofrdemosql' and retry the operation.*

[More events in the activity log →](#)

[Dismiss all](#) 

### Failed to save server Auditing settings

Failed to save Auditing settings for server: ofrdemosql. Storage account 'ofrdemostorage2' is not in the list of allowed FQDNs on the Azure SQL Server. Please add the target to the list of allowed FQDNs on server 'ofrdemosql' and retry the operation.


## Vulnerability Assessment

[Dashboard](#) > [AdventureWorks \(ofrdemosql/AdventureWorks\)](#) >

### Server settings ...

ofrdemosql

 Save  Discard  Feedback

 Saving Azure Defender for SQL for server ofrdemosql...

#### AZURE DEFENDER FOR SQL

☒ ON ☐ OFF



Azure Defender for SQL costs 15 USD/server/month. It includes Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.

#### VULNERABILITY ASSESSMENT SETTINGS

##### Subscription

[Select Subscription](#)



##### Storage account

ofrdemostorage2

[Select Storage account](#)

## Error Configuring

*Failed to save Azure Defender for SQL settings The storage account 'ofrdemostorage2' defined in the vulnerability assessment configuration is not in the list of allowed FQDNs on the server. Please add this storage account to the list of allowed FQDNs on your 'ofrdemosql' server and retry the operation or update the vulnerability assessment configuration with a valid storage account.*

 Failed to save Azure Defender for SQL settings 

The storage account 'ofrdemostorage2' defined in the vulnerability assessment configuration is not in the list of allowed FQDNs on the server. Please add this storage account to the list of allowed FQDNs on your 'ofrdemosql' server and retry the operation or update the vulnerability assessment configuration with a valid storage account.

a few seconds ago

## I/E Service

Dashboard > ofrdemosql > AdventureWorks (ofrdemosql/AdventureWorks) >

### Export database ...

AdventureWorks

File name \*

Subscription \*

Storage (Premium not supported) \*  

ofrdemostorage2

backups


Select storage



Authentication type

Server admin login \*

\*Password

## Database export error

*Failed to export the database: AdventureWorks. ErrorCode: 400 ErrorMessage: The operation was not allowed because of the outbound firewall rule configuration for '[ofrdemostorage2.blob.core.windows.net](#)'. .*

 Database export error 

Failed to export the database: AdventureWorks.  
ErrorCode: 400  
ErrorMessage: The operation was not allowed because of the outbound firewall rule configuration for 'ofrdemostorage2.blob.core.windows.net'.

a few seconds ago

## Kusto Query

### 1. Find operation in MonManagementResourceProvider

```
Execute: [Web] [Desktop] [Web (Lens)] [Desktop (SAW)] https://sqlazureeus22.kustomfa.windows.net/sqlazure1
MonManagementResourceProvider
| where controller_name == 'OutboundFirewallRules'
| where request_url contains "<serverName>" and request_url contains "<outboundFqdn>"
| project originalEventTimestamp, request_id, http_verb, response_code, request_url
```

### 2. Use timestamps and request\_id from (1) to find full traces in MonManagement

```
Execute: [Web] [Desktop] [Web (Lens)] [Desktop (SAW)] https://sqlazureeus22.kustomfa.windows.net/sqlazure1
MonManagement
| where originalEventTimestamp >= datetime(<beginTime>)
| where originalEventTimestamp <= datetime(<endTime>)
| where request_id =~ "<requestId>"
```

3. At this point, the only error we are aware of is due to reaching the max limit of OFRs (200). For other cases, you will need to employ generic MonManagement debugging abilities. Please escalate to Connectivity queue if unable to determine the problem or if you believe there is a bug.

## Common Errors and Cause

Error	Severity	Owner	Description	Cause
46842	EX_USER	<USERACCT>	Logical server %ls defined in the elastic query configuration is not in the list of Outbound Firewall Rules on the server. Please add this logical server name to the list of Outbound Firewall Rules on your %ls server and retry the operation.	Data exfiltration prevention is enabled, but the target server not in the allowed FQDN list.
16539	EX_USER	USERACCT	Operation failed since the external data source '%ls' has underlying storage account that is not in the list of Outbound Firewall Rules on the server. Please add this storage account to the list of Outbound Firewall Rules on your server and retry the operation	Data exfiltration is blocked and the destination is not in allowed list. ErrorCorrectiveAction: Add destination to allowed list for data exfiltration.
45530	EX_USER	USERACCT	The operation was not allowed because of the outbound firewall rule configuration for '%ls'.	The outbound firewall rules blocked the request.

**How good have you found this content?**



-