Azure MS SQL Server

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up Azure MS SQL Server authentication for compliance scans.

A few things to consider

Why should I use authentication?

With authentication we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? Yes, authentication is required for compliance scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

Authentication Technologies Matrix

What are the steps?

First, set up an Azure MS SQL Server Authentication account and privileges on target hosts (we'll help you with this below). Then, using Qualys Policy Compliance, complete these steps: 1) Add Azure MS SQL Server authentication records. 2) Launch a compliance scan. 3) Run the Authentication Report to view the authentication status (Passed or Failed) for each scanned host.

Azure MS SQL Server Setup

In order for the Qualys Compliance Scan to work properly on a SQL Server database, the following account and privileges must exist prior to running the compliance scan. Note – These scripts require a Server admin login account.

1) Create a SQL Server Authentication Login for the Scan Account

This script creates a database login for the user account to be used for scanning. Please provide a password before running the script. Tip – We recommend creating an account called QUALYS_SCAN.

Log in to **master** database and run the following:

CREATE LOGIN qualys_scan WITH PASSWORD=N'<password>';

2) Create a User Account

This script creates a user account, called QUALYS_SCAN, in the target database.

Log in to **master** database and run the following:

```
CREATE USER qualys_scan FOR LOGIN qualys_scan;
GRANT ALTER ANY USER TO qualys_scan;
```

Log in to **Azure SQL user** database and run the following:

```
CREATE USER qualys_scan FOR LOGIN qualys_scan;
GRANT VIEW DEFINITION TO qualys_scan;
GRANT VIEW DATABASE STATE TO qualys_scan;
```

3) Verify Privileges on the Scan Account

Verify that the QUALYS_SCAN account has all the privileges in the database in order to run a successful compliance scan. Log into the database using the "QUALYS_SCAN" account, then run the following queries to see if access is available to the account.

Query	Expected Results
select top 1 1 permission from sys.all_objects	1
select top 1 1 permission from sys.configurations	1
select top 1 1 permission from sys.databases	1
select top 1 1 permission from sys.database_permissions	1

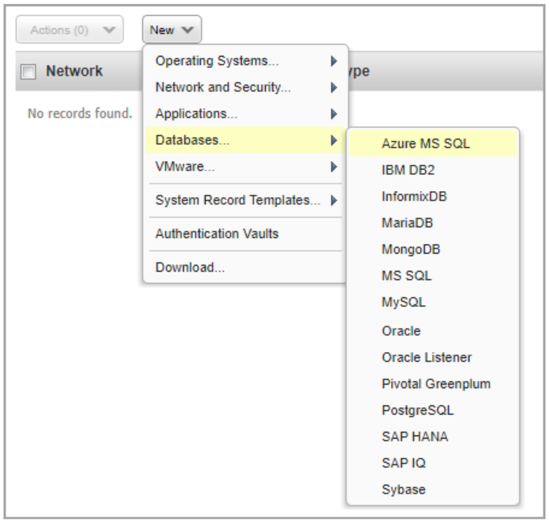
Did you get different results? Contact your SQL Server DBA to ensure that privileges are set up correctly.

Azure MS SQL Server Authentication Records

Each Azure MS SQL Server record identifies account login credentials, database information (unless you use auto discovery) and targets. This record type is only available in accounts with PC or SCA and is only supported for compliance scans.

How do I get started?

Go to **Scans** > **Authentication**, and then go to **New** > **Databases** > **Azure MS SQL**.



No records found.

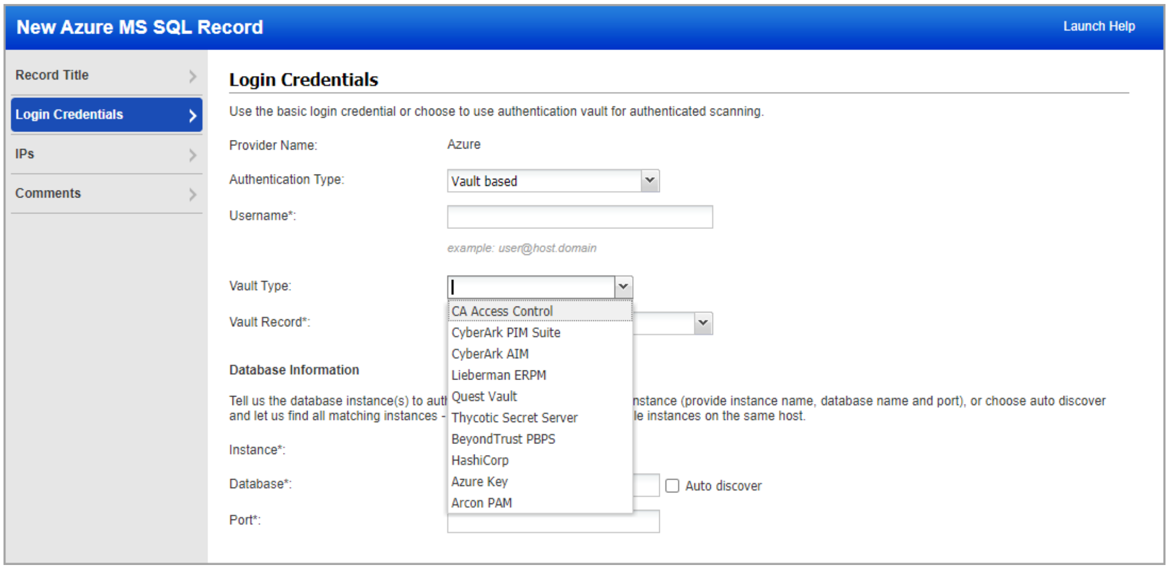
What login credentials are required?

It is recommended you define a dedicated user account for Azure MS SQL Server authentication. You'll need to tell us the user account to be used for authentication.

Can I access a password in a vault?

Yes. We support integration with multiple third party password vaults. Go to **Scans** > **Authentication** > **New** > **Authentication Vaults** and tell us about your vault system.

In the Azure MS SQL Server record, choose **Authentication Type: Vault based** on the **Login Credentials** tab and select your vault type and vault record. At scan time, we'll authenticate to hosts using the account name in your record and the password we find in your vault.



New Azure MS SQL Record

Login Credentials

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Provider Name: Azure

Authentication Type: Vault based

Username*:

example: user@host.domain

Vault Type:

Vault Record*:

Database Information

Tell us the database instance(s) to auth instance (provide instance name, database name and port), or choose auto discover and let us find all matching instances - le instances on the same host.

Instance*:

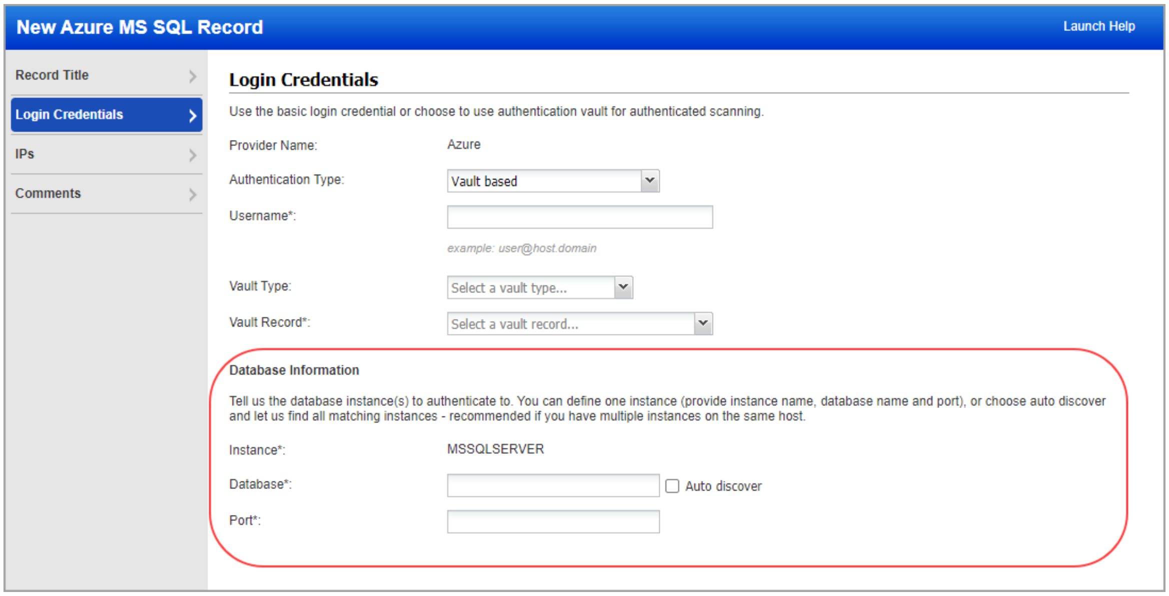
Database*: □ Auto discover

Port*:

Database information

Tell us the database instance(s) to authenticate to. You can define one instance (provide instance name, database name, and port). Currently, we support only MSSQLSERVER value for the database instance name and do not support named instances.

Use the **Auto discover** option and we'll automatically find database instances on your target hosts, so you don't have to provide database information in your record. This is recommended if you have multiple databases instances on the same host.



Login Credentials

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Provider Name: Azure

Authentication Type: Vault based

Username*:

example: user@host.domain

Vault Type: Select a vault type...

Vault Record*: Select a vault record...

Database Information

Tell us the database instance(s) to authenticate to. You can define one instance (provide instance name, database name and port), or choose auto discover and let us find all matching instances - recommended if you have multiple instances on the same host.

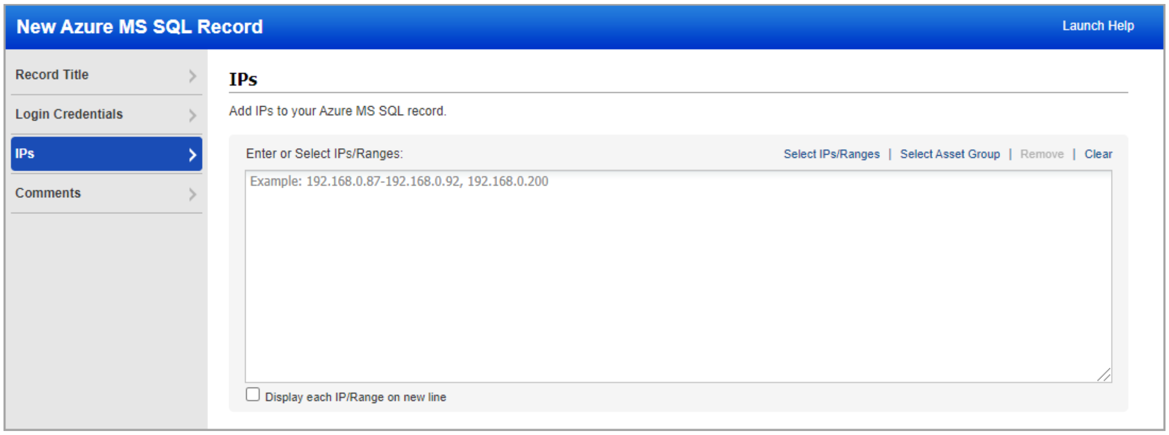
Instance*: MSSQLSERVER

Database*: ☐ Auto discover

Port*:

Which IPs should I add to my record?

Select the target compliance hosts (IPs) to authenticate to. Each IP may be included in one Azure MS SQL Server record.



IPs

Add IPs to your Azure MS SQL record.

Enter or Select IPs/Ranges:

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Display each IP/Range on new line

Last updated: May 27, 2022