MS SQL Server 2005-2022

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 MS SQL Server authentication for MS SQL Server. For Windows, we support MS SQL Server 2005, 2008, 2012, 2014, 2016, 2017, 2019, and 2022. For Unix, we support MS SQL Server 2017, 2019, and 2022.

A few things to consider

Do I have to use authentication?

Yes, authentication is required for compliance scans. Choose the type of authentication you want to perform: Windows or Database (Unix or Windows). If you choose Windows, provide the name of the Windows domain where the account is stored. The domain name is required because the scanning engine must associate the operating system account with the MS SQL Server database account for authentication.

For Windows:

If you are using VM, then only Windows Authentication is required for MS SQL databases on Windows.

If you are using PC or SCA, then MS SQL Authentication is used. You can optionally use Windows authentication record for auto-discovery of Instance, Database, and Port.

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 a 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 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.

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 super-user account. For example, sa or an administrator domain account.

Please run the scripts provided below, in the order shown.
If creating a Windows authentication on the SQL Server, start with Step 1a.
If creating a SQL Server authentication on the SQL Server, start with Step 1b.

On-premise SQL Server Database

Interested in Amazon RDS or Google Cloud? Jump to a section below.

Amazon RDS for SQL Server

Cloud SQL for SQL Server

On-premise SQL Server Database

1a) Create a Windows Authentication Login for the Scan Account

This script creates a domain login for the user account to be used for scanning. Provide a domain name or local user account, and name of the target database before running the script. Tip – An admin needs to create the account on the host first. We recommend creating an account called QUALYS_SCAN.

```
USE [master]
GO
CREATE LOGIN [domain\QUALYS_SCAN] FROM WINDOWS WITH DEFAULT_DATABASE=[[name of database to scan]]
GO
```

1b) 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 and the name of the target database before running the script. Tip – We recommend creating an account called QUALYS_SCAN.

```
USE [master]
GO
CREATE LOGIN QUALYS_SCAN WITH PASSWORD=N'[password]', DEFAULT_DATABASE[name of database to scan], CHECK_EXPIRATION=ON, CHECK_POLICY=ON
GO
```

2) Create a User Account

This script creates a user account, called QUALYS_SCAN, in the master and/or target database. This must be executed on every database that needs to be a part of the assessment. When a new database is added to the SQL Server Instance and needs to be assessed, this user account also needs to be manually created in the new database.

```
USE [name of database to scan]
GO
CREATE USER [QUALYS_SCAN] FOR LOGIN [[username created in Step 1]]
GO
```

Tip: A script QG_MSSQLServer_scanuser_creation_helper_verx.x.sql is available in the zip file if you need to create a scan user in every online database in your SQL Server instance.

3) Grant Privileges to the Scan Account

Please run the scripts provided below to grant privileges to the scan account.
To grant the sysadmin role to the scan account, see Step 3a.
To grant restricted/read-only privileges to the scan account, see Step 3b.

3a) Grant Privileges to the Scan Account with Sysadmin Role

This script grants sysadmin role to the scan account for Windows authenticated login created in Step 1a.

```
EXEC master..sp_addsrvrolemember @loginame = N'domain\QUALYS_SCAN', @rolename =
N'sysadmin'
GO
```

This script grants sysadmin role to the scan account for local SQL Server login created in Step 1b.

```
EXEC master..sp_addsrvrolemember @loginame = N'QUALYS_SCAN', @rolename = N'sysadmin'
GO
```

3b) Grant Privileges to the Scan Account with Restricted/Read-only Privileges

Note: This section is required for master database only.

If you prefer to have a scan user without sysadmin role, follow these steps to grant privileges to the scan user created in Step 2:

```
USE [master]
GO
GRANT SELECT ON SYS.ALL_OBJECTS TO QUALYS_SCAN;
GRANT SELECT ON SYS.CONFIGURATIONS TO QUALYS_SCAN;
GRANT SELECT ON SYS.DATABASES TO QUALYS_SCAN;
GRANT SELECT ON SYS.DATABASE_PERMISSIONS TO QUALYS_SCAN;
GRANT SELECT ON SYS.SYSLOGINS TO QUALYS_SCAN;
GRANT SELECT ON SYS.TRACE_EVENTS TO QUALYS_SCAN;
GRANT SELECT ON SYS.TRACES TO QUALYS_SCAN;
GRANT SELECT ON SYS.SYSALTFILES TO QUALYS_SCAN;
GRANT SELECT ON SYS.SERVER_PRINCIPALS TO QUALYS_SCAN;
```

The following additional optional privileges are needed for certain controls in the master database.

Privileges Needed	Control ID
GRANT ALTER TRACE TO [scan login created in Step 1a or 1b];	2691, 3081, 3082, 3101, 3102, 3201, 4894, 4895, 4896, 4897, 4898, 4899, 4900, 4901, 4902, 4903, 4904, 4905, 4906, 4907, 4908, 4909, 4910, 4911, 4912, 4913, 4915, 4916, 4917, 4918, 4919, 4920, 4921, 4922, 4923, 4924, 4925, 4926, 4927, 4928, 4929, 4930, 4931, 7216, 7382, 10742, 10743, 10744, 10745, 10746, 10747, 10748,

	10749, 10750, 11303, 11304, 11365
GRANT VIEW SERVER STATE TO [scan login created in Step 1a or 1b];	10615
GRANT VIEW ANY DEFINITION TO [scan login created in Step 1a or 1b];	11488, 11489, 11490, 27014, 27015
GRANT EXECUTE ON xp_loginconfig TO [scan user created in Step 2];	3313, 9910
GRANT CONTROL SERVER TO [scan login created in Step 1a or 1b]; The CONTROL SERVER permission is a high-level privilege that is similar to sysadmin fixed server role. If you do not need to assess this control, then you do not need to grant this permission to the scan login. or For SQL Server 2022 and above: GRANT VIEW ANY CRYPTOGRAPHICALLY SECURED DEFINITION TO [scan login created in Step 1a or 1b];	3303

If you are intending to assess the msdb database, remember to create a scan user in msdb database and grant these privileges to assess the corresponding controls in msdb database.

Privileges Needed	Control ID
GRANT EXECUTE ON msdb..sp_enum_login_for_proxy TO [scan user created in Step 2 in msdb];	3304
GRANT EXECUTE ON msdb..sp_enum_proxy_for_subsystem TO [scan user created in Step 2 in msdb];	3314, 14791
GRANT SELECT ON msdb..sysproxies TO [scan user created in Step 2 in msdb];	10318
GRANT SELECT ON msdb..sysproxylogin TO [scan user created in Step 2 in msdb];	11491
GRANT VIEW DEFINITION TO [scan user created in Step 2 in msdb];	11491, 27899

Important notes:

Microsoft SQL Server behaves differently from other database platforms in that insufficient privileges for the scan account do not always generate explicit errors during assessment. Instead, the scan may complete successfully but return incomplete data, leading to potential false negatives/positives.

For example, a common issue occurs with control 11488. If the privilege "GRANT VIEW ANY DEFINITION TO <scan_login>" is not granted, the scan account cannot access the system tables that store the relevant data, resulting in an incorrect report of "Audit not configured". Similarly, without this same privilege, the scan account can only enumerate a limited set of server principals (typically itself and a few default principals) instead of all principals that exist on the SQL Server instance. This again can produce incomplete or misleading assessment results.

We highly recommend that customers review the list of required privileges documented in our MSSQL Authentication Guide. If any privilege appears overly permissive, we advise reviewing the associated control to determine whether its assessment is necessary. Customers can then make an informed decision on whether to grant or omit that privilege for the scan account.

4) Verify Privileges on the Scan Account

We provided a script in the zip archive to help you identify missing privileges from the user account to be used for scanning. The script is in the file QG_MSSQLServer_Auth_verx.x.sql. This script should be executed by an administrative user against the appropriate database to determine if all the appropriate privileges have been setup correctly. The script will generate an output listing the status of all the prerequisites.

Sample Output:

Server_servicename	DB_name	Username	Suser_name
SERVER1_MSSQLSERVER	master	dbo	SERVER1\Administrator

Prerequisites	Status
master	Current Database
SERVER1\Administrator	Current logged in user
14.0.1000.169	Current product version
qualysscanlogin	PASS - Database principal exists
XP_LOGINCONFIG	PASS - Execute privilege exists
ALTER TRACE	PASS - Privilege exists
VIEW ANY DEFINITION	PASS - Privilege exists
VIEW SERVER STATE	PASS - Privilege exists
ADSERVER\qualysscanlogin	PASS - Server principal exists

4a) If you intend to assess msdb database:

Prerequisites	Status
msdb	Current Database
SERVER1\Administrator	Current logged in user
qualysscanlogin	PASS - Database principal exists
SP_ENUM_LOGIN_FOR_PROXY	PASS - Execute privilege exists

SP_ENUM_PROXY_FOR_SUBSYSTEM	PASS - Execute privilege exists
SYSPROXIES	PASS - Select privilege exists
SYSPROXYLOGIN	PASS - Select privilege exists

4b) If you intend to assess a user database (HRDB for example):

Prerequisites	**Status**
HRDB	Current Database
SERVER1\Administrator	Current logged in user
qualysscanlogin	PASS - Database principal exists

Amazon RDS for SQL Server

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 and the name of the target database before running the script. Tip – We recommend creating an account called QUALYS_SCAN.

```
USE master
CREATE LOGIN QUALYS_SCAN WITH PASSWORD=N'[password]', DEFAULT_DATABASE=[name of database to scan], CHECK_EXPIRATION=ON, CHECK_POLICY=ON;

GRANT ALTER TRACE TO QUALYS_SCAN;
GRANT VIEW ANY DEFINITION TO QUALYS_SCAN;
GRANT VIEW SERVER STATE TO QUALYS_SCAN;

USE msdb
CREATE USER QUALYS_SCAN FOR LOGIN QUALYS_SCAN;
GRANT EXECUTE ON MSDB..SP_ENUM_PROXY_FOR_SUBSYSTEM TO QUALYS_SCAN;
GRANT EXECUTE ON MSDB..SP_ENUM_LOGIN_FOR_PROXY TO QUALYS_SCAN;
```

2) Create a User Account

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

```
use [name of database to scan]
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 from sys.all_objects;	1
select top 1 1 from sys.configurations;	1
select top 1 1 from sys.databases;	1
select top 1 1 from sys.database_permissions;	1
select top 1 1 from sys.syslogins;	1
select top 1 1 from sys.trace_events;	1
select top 1 convert(char(20),serverproperty('productversion')) permission;	n.nn.nnnn.nn
select top 1 convert(char(20),serverproperty('productversion')) permission;	n.nn.nnnn.nn

Cloud SQL for SQL Server

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 and the name of the target database before running the script. Tip – We recommend creating an account called QUALYS_SCAN.

```
USE master
CREATE LOGIN QUALYS_SCAN WITH PASSWORD=N'[password]', DEFAULT_DATABASE=[name of database to scan], CHECK_EXPIRATION=ON, CHECK_POLICY=ON
GO
```

2) Create a User Account

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

```
use [name of database to scan]
CREATE USER QUALYS_SCAN FOR LOGIN QUALYS_SCAN
GO
```

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 from sys.all_objects;	1
select top 1 1 from sys.configurations;	1
select top 1 1 from sys.databases;	1
select top 1 1 from sys.database_permissions;	1
select top 1 1 from sys.syslogins;	1
select top 1 1 from sys.trace_events;	1
select top 1 convert(char(20),serverproperty('productversion')) permission;	n.nn.nnnn.nn
select top 1 convert(char(20),serverproperty('productversion')) permission;	n.nn.nnnn.nn

Last updated: March 5, 2026