# 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.

### 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; | 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; | 10615 |
| GRANT VIEW ANY DEFINITION TO; | 11488, 11489, 11490, 27014, 27015 |
| GRANT EXECUTE ON xp_loginconfig TO; | 3313, 9910 |
| GRANT CONTROL SERVER TO ;<br>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 | 3303 |

this permission to the scan login.

or

For SQL Server 2022 and above:
GRANT VIEW ANY CRYPTOGRAPHICALLY SECURED
DEFINITION TO;

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; | 3304 |
| GRANT EXECUTE ON msdb..sp_enum_proxy_for_subsystem TO; | 3314, 14791 |
| GRANT SELECT ON msdb..sysproxies TO; | 10318 |
| GRANT SELECT ON msdb..sysproxylogin TO; | 11491 |
| GRANT VIEW DEFINITION TO; | 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.

### 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 |

a) 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 |

b) 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 |