MS SQL Server 2005-2019

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 2005, 2008, 2012, 2014, 2016, 2017 and 2019.

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. 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.

- If you are using VM then only Windows Authentication is required.

- 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.

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.

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

Scan with Restricted/Read-only Account

Want to create a scan account without the sysadmin role? Follow these steps:

```
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;
```

Additional optional privileges are needed for certain controls, as shown below.

Privileges Needed	Control ID
GRANT ALTER TRACE TO qualys_scan;	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 EXECUTE on xp_loginconfig to qualys_scan;	3313, 9910

grant EXECUTE on msdb..sp_enum_login_for_proxy to qualys_scan;	3304
grant SELECT on msdb..sysproxies to qualys_scan;	10318
grant VIEW SERVER STATE to qualys_scan;	10615
grant SELECT on msdb..sysproxylogin to qualys_scan;	11491
grant VIEW ANY DEFINITION TO qualys_scan;	11488, 11489, 11490

2) Create a User Account

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

```
USE [name of database to scan]
GO
CREATE USER [qualys_scan] FOR LOGIN [[username created in Step 1]]
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 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
select top 1 1 permission from sys.syslogins	1
select top 1 1 permission from sys.trace_events	1
select top 1 convert(char(20),serverproperty('productversion')) permission	n.nn.nnnn.nn

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

Last updated: February 20, 2020