# MS SQL Server 2000

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.

## A few things to consider

### Do I have to use authentication?

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.

### 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 2000 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. Please provide a domain name or a local user account and the name of the target database before running the script. Tip – An administrator needs to create the account on the host first. We recommend creating an account called QUALYS_SCAN.

```
USE [master]
GO
EXEC dbo.sp_grantlogin @loginame = N'domain \qualys_scan'
EXEC dbo.sp_defaultdb @loginame = N'domain \qualys_scan', @defdb = N'[name of database to scan]'
EXEC dbo.sp_defaultlanguage @loginame = N'domain \qualys_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
EXEC dbo.sp_addlogin @loginame = N'qualys_scan', @passwd = N'[password]', @defdb = N'[name
of database to scan]'
GO
EXEC master..sp_addsrvrolemember @loginame = N'qualys_scan', @rolename = N'sysadmin'
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]
GO
EXEC dbo.sp_grantdbaccess @loginame = N'qualys_scan', @name_in_db = N'[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 name permission from master.dbo.syslogins | SA |
| select top 1 1 permission from master.dbo.sysdatabases | 1 |
| select top 1 1 permission from master.dbo.sysconfigures | 1 |
| select top 1 1 permission from master.dbo.syspermissions | 1 |

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

Last updated: June 13, 2018