



HP Security Manager:

Using Microsoft® SQL Server with Network Service or with another account

Table of Contents

Overview	2
Introduction	2
SQL Permissions	3
Creating a SQL Database	3
Upgrading a SQL Database	4
Using a remote SQL Database	4
Less Elevated Privileges	5
Migrating the Security Manager Database	7
Running Security Manager service under (local) user account	8
Running HPSM application pool under (local) user	10
Sharing Same SQL with Web Jetadmin	13
Using a Different Database Name.....	13
Using a Different Port.....	14
Summary of Options for Remote Database	15
New Install, Remote Database, Rights to Create a Remote Database	15
New Install, Remote Database, No Rights to Create a Remote Database.....	15
Upgrade, Remote Database, Rights to Update a Remote Database	16
Upgrade, Remote Database, No Rights to Update a Remote Database	16
Troubleshooting Database and SQL issues.....	16
Database Encryption.....	23
SQL AlwaysOn.....	24

Failover	25
SQL Script	25
Appendix A.....	27
Links to other HP Security Manager Whitepapers	27

Overview

HP Security Manager requires a Microsoft SQL Server database in order to maintain a fleet of devices for security compliance. If desired, Security Manager can install and use a new MS SQL instance and database running under Microsoft SQL Express. However, it may be more convenient for Security Manager to use an existing full Microsoft SQL Server instance for performance benefits or to appease company policies. Fortunately, Security Manager can be configured to use SQL Server instead of SQL Express either on the same machine or a remote machine. This document describes the various SQL options and how to configure Security Manager to use a database other than the default SQL Express database that it offers to install.

While Security Manager only tests the two most recent SQL versions at the time of release, there should be no issues using older or newer SQL versions as Security Manager uses basic calls into the SQL database and isn't using SQL features that require later versions. Backward and forward compatibility should be present, there just isn't capacity to test the multitude of SQL versions offered over the years.

The same holds true for the multitude of special features offered by the various versions on SQL Server such as AlwaysOn and client/server encryption. There are entirely too many to test, but you'll likely find most will work fine with any client including Security Manager. One feature that has been minimally tested and found to work well is the AlwaysOn feature that provides high-availability failover and disaster recovery. See the chapter near the end of this document for more details.

Introduction

Whether using local or remote SQL Server, Express or Full, the rules are essentially the same. In every case, Security Manager needs access to a SQL server instance. It can either create a new database, upgrade an existing database, or attach to an existing database, depending upon the situation and the user rights. If Security Manager is instructed to install SQL Express on the local machine, a SQL instance and database for Security Manager will be created by the Security Manager installer. If Security Manager is pointed to a remote SQL server and instance during installation, proper rights must be present for the user running the installation to be able to create or update a SQL database wherever SQL server may reside or username and password have to be provided for the SQL database. Proper rights must also exist on the remote database itself for the user which the Security Manager service runs under to be able to read from and write to the database.

KEY POINT: Just to reiterate, for installing and upgrading Security Manager, the user who is logged into the machine and running the installer executable must have proper rights on the SQL server to either create a database or update an existing database. All the installer does is run SQL scripts to create or alter a database, and naturally any user running those commands needs to have proper SQL rights. In this case it is the Windows user who is running the installer. If this user does not have those rights, then the username and password of a different user can be provided during installation. For normal operation of

Security Manager after installation, the user running the Security Manager service (default as Network Service) needs to have permissions to at least read and write to the database (explained later).

Each Security Manager installation must point to its own unique database, multiple installations cannot share a database. Several techniques are available to allow Security Manager to install/use a SQL database in any location.

Both a named and default instance are supported when instructing Security Manager to use a remote SQL Server database.

SQL Permissions

There are three scenarios where Security Manager will interact with Microsoft SQL:

- Creating a database during installation of Security Manager.
- Upgrading a database during upgrading of Security Manager from one version to another.
- Running Security Manager to manage security features on a fleet of devices.

Each scenario requires a different set of SQL rights for potentially different users.

- Create Database – A Windows user running the installer executable needs at a minimum Create Database rights (sysadmin preferred).
- Upgrade Database – A Windows user running the installer executable to upgrade versions needs DBO rights to perform potential commands on the database such as insert, update, alter, create table.
- Run Security Manager – The Windows account that runs the Security Manager service (default of Network Service) needs DBO rights to perform operations such as reading and writing.

NOTE: Below is an explanation of how to run with less rights or a different account, if desired.

Creating a SQL Database

If Security Manager is instructed to create a database during installation, SQL commands are performed to create the database and its necessary tables. In order for the Security Manager installer to be able to create a SQL database, the credentials of the user running the Security Manager installer need to have at least Database Create rights on the SQL instance (sysadmin preferred). If a local database is desired, since the user running the Security Manager installer likely is a member of the Admin group of the local machine, proper rights will be present to create a SQL database. However, if a remote database is desired, such as on a remote SQL Server farm, it is unlikely that the SQL database administrator (DBA) will provide sysadmin or even Create Database rights for the user running the Security Manager installer. If this is the case, options to create the database include:

- SQL DBA runs the Security Manager installer on the remote SQL server and instructs it to create database only which will create a database and all necessary tables.
- SQL DBA uses the batch script from the InstallSqlScripts.zip (which is installed in the root directory of security manager) and runs it to create the database and all necessary tables.
- SQL DBA logs into the Security Manager machine, performs the install, and instructs the installer to create the database and all necessary tables on the remote server\instance.
- SQL DBA provides temporary sysadmin rights to the Windows user running the installer until it completes creating the database and necessary tables.

Upgrading a SQL Database

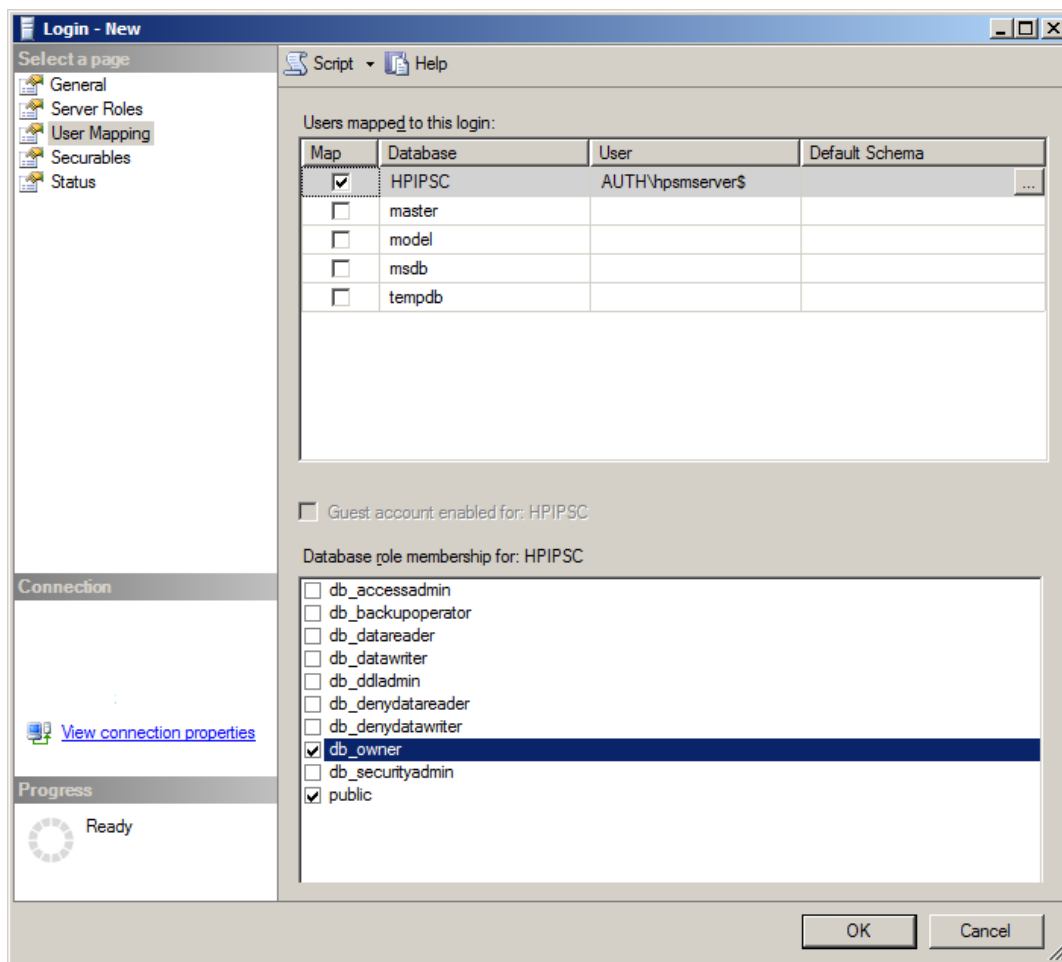
When attempting to upgrade Security Manager from one version to another, it is very likely that new columns have been added to tables or new tables have been created to represent new features. SQL commands such as insert, update, alter, create table may be used to upgrade the database, and these commands require elevated rights on the Security Manager database for the Windows user running the installer and issuing the commands. DBO rights for the Windows user running the upgrade will suffice to allow for these commands to be performed. If a local database is desired, since the user running the Security Manager installer likely is a member of the Admin group of the local machine, proper rights will be present to upgrade the SQL database. However, if a remote database is desired, DBO rights will be necessary for the Windows user running the upgrade. If allowing such rights on a permanent basis is an issue, options to upgrade the database include:

- SQL DBA provides temporary DBO rights on the Security Manager database for the Windows user running the upgrade until it completes.
- SQL DBA logs into the Security Manager machine and performs the upgrade, allowing it to upgrade the database.
- SQL DBA obtains a SQL script and runs it to upgrade the database and all necessary tables.

Using a remote SQL Database

When the database has been created and Security Manager is trying to use it, the credentials of the user running the Security Manager service will need DBO rights on the database. By default, Security Manager runs under Network Service, but the Security Manager service identifies itself as a network service only locally. Remotely, Security Manager identifies itself as Domain\Machine\$ when Windows Authentication (Integrated Security) is used. In this case, use SQL Management Studio to create a new login under Security, Logins and make sure the Domain\Machine\$ account (where Machine\$ is the name of the Security Manager machine followed by a dollar sign) has DBO rights on the Security Manager database under User Mapping.

NOTE If it is desired to use a Windows User account instead of a Windows Machine account, the properties of the Security Manager service and IIS need to be changed from Network Service to the Windows User account. When performed, Security Manager identifies itself to the remote SQL Server as the Windows User account. Therefore, make sure the Windows User account has DBO rights on the database. Directories on the Security Manager machine where Security Manager files reside must have Full Control rights for that user account as well.



SQL Server 2012 by default may not include **Network Service** as a default login. To rectify the situation, use Microsoft SQL Server Management Studio to add the service name to the logins for this database instance. You can then ensure the login for **Network Service** has DBO rights on the HP Security Manager database.

Less Elevated Privileges

DBO rights merely provide complete control over a single database. Providing DBO rights on the Security Manager database does not provide access to any other databases nor does it allow any administrative tasks on the SQL instance. It just allows Security Manager to perform tasks on the one database it uses.

That being said, there still may be cases where it is against company policy to assign elevated rights such as DBO rights on ANY database that is contained on the company SQL farm. It is possible to run HP Security Manager on just read/write rights on the database after making a configuration file change. Navigate to the following folder location on the Security Manager server:

Program Files (x86)\HP JetAdvantage Security Manager\HPSM_Service.exe.config

Open the **HPSM_Service.exe.config** file in a text editor and locate the following entry:

```
<add key="shrinkDB" value="true" />
```

Change the **"true"** value to **"false"** so that it looks like this:

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/195104311344011303>