

Configure TMS to Use Windows Authentication for External SQL Server



Document ID: 117817

Contributed by Shannon Beard, Cisco TAC Engineer.

Jul 09, 2014

Contents

Introduction

Requirements

Components Used

Configure Windows Authentication for TMS connection to the TMSNG (and TMSPE) databases

Configuration

Introduction

In order to configure the Telepresence Management Suite (TMS) to use Windows Authentication for External Structured Query Language (SQL) Server, you must change the IIS application user identity to a network service account. This document describes how to configure TMS to use Windows Authentication for the External SQL Server.

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Windows Server 2003, Windows Server 2008 R2 running Active Directory
- Windows Server running SQL Server 2005 or later.
- Windows Server 2003 (IIS 6) or Windows Server 2008 R2 (IIS 7) running TMS software.

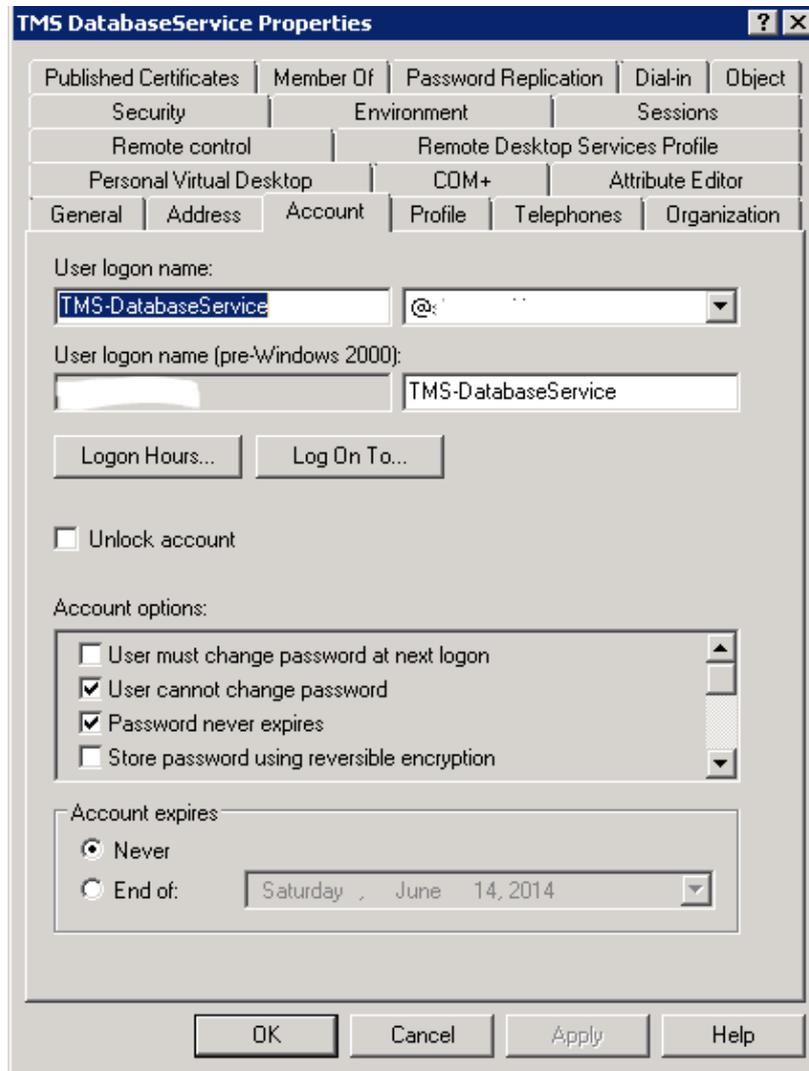
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure Windows Authentication for TMS connection to the TMSNG (and TMSPE) databases

If a customer would like to use Windows Authentication for TMS connection to the TMSNG and TMS Provisioning Extension (TMSPE) databases; you must change the IIS application user identity to a network service account to create a login in SQL.

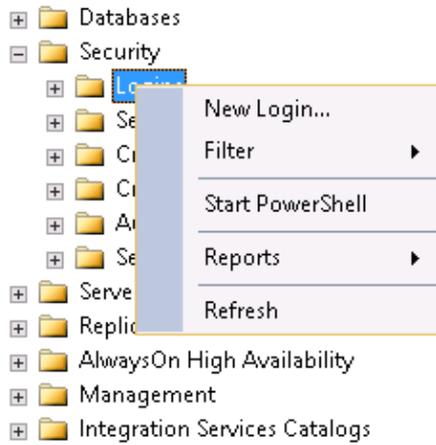
Configuration

1. Create a new Active Directory (AD) Service account, for example tms–databaseservice. If using Windows 2008 or later for AD, no special permissions are needed. If using Windows 2003, the user must be enabled to Log On as a Service.

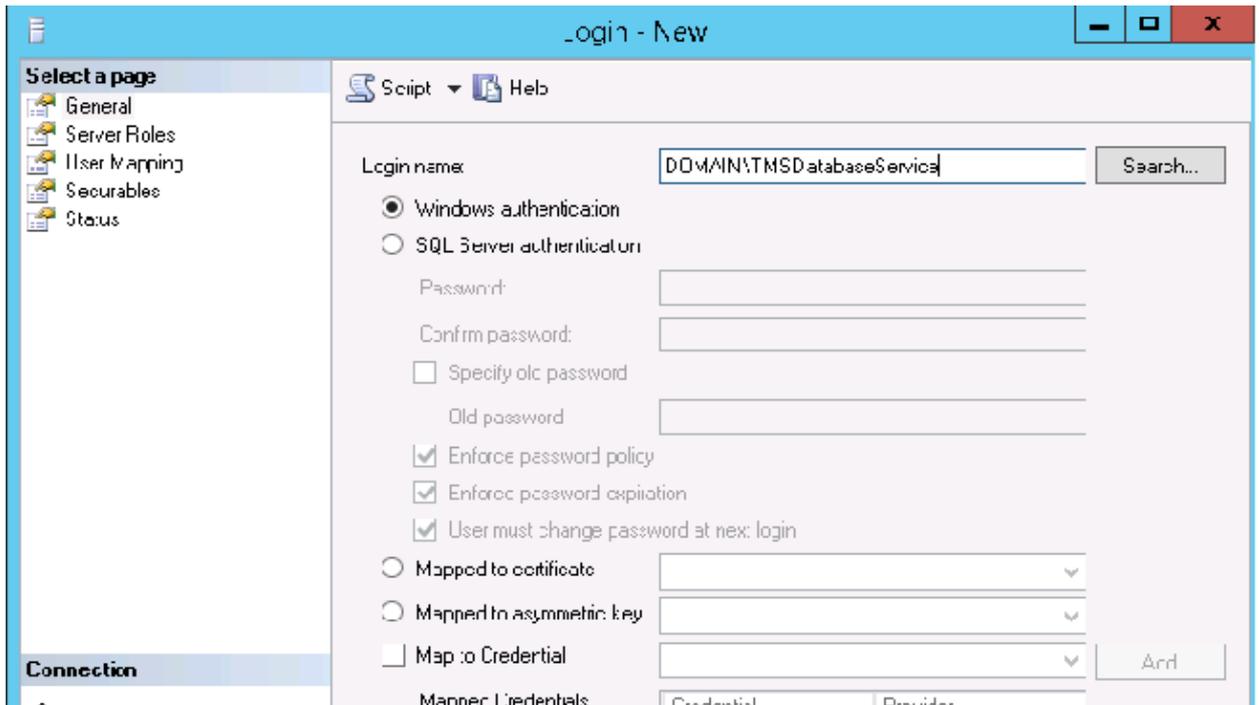


2. In the SQL Server, create a new log in; for example: tms–databaseservice; via SQL Management Studio:

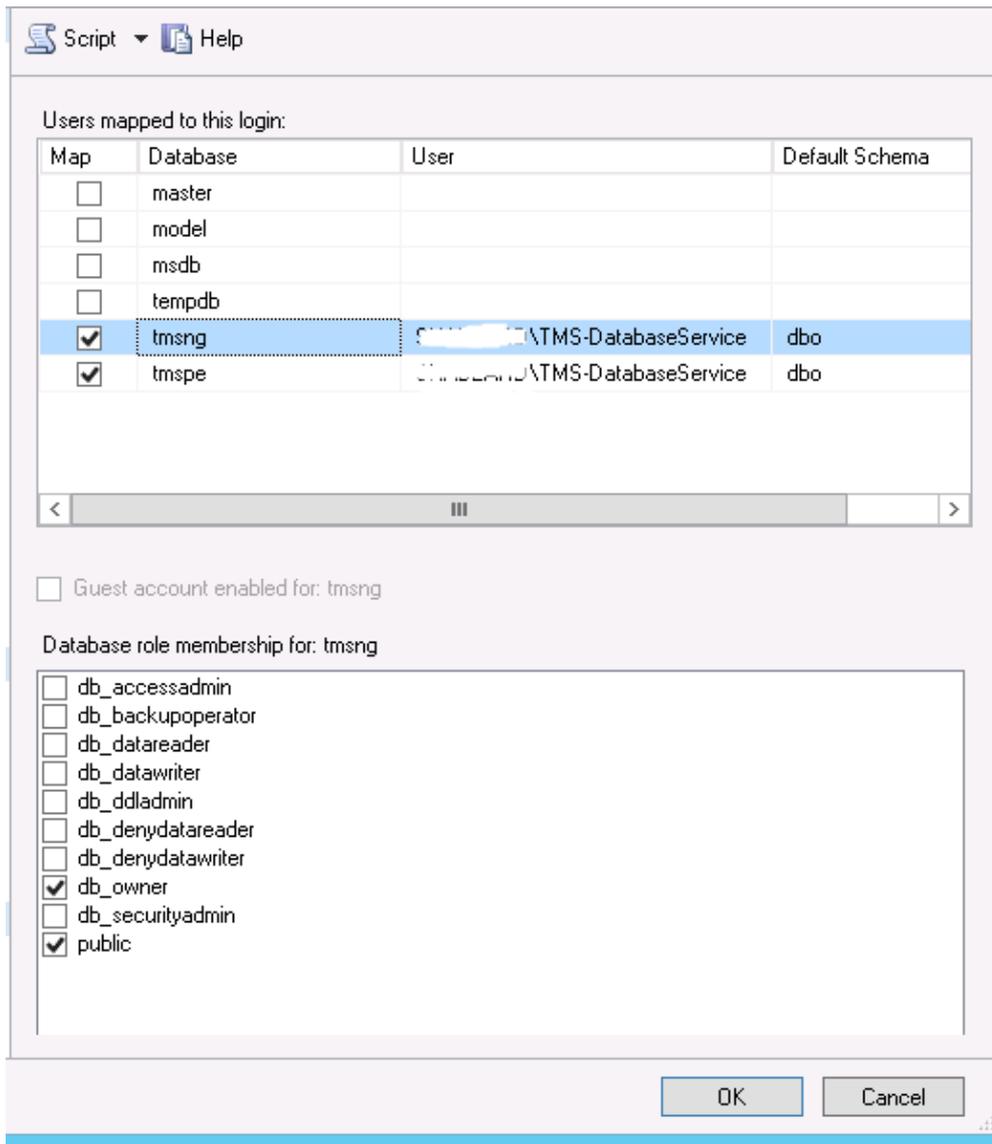
– Expand **Security** and right-click **Logins**. Select **New Login**.



– Under **General**, enter the domain account **DOMAIN\USERNAME** for the service user.



– Under **User Mapping**, select **tmsng** and **tmspe** if applicable. For **Default Schema**, select **dbo** and select **db_owner** for role membership.



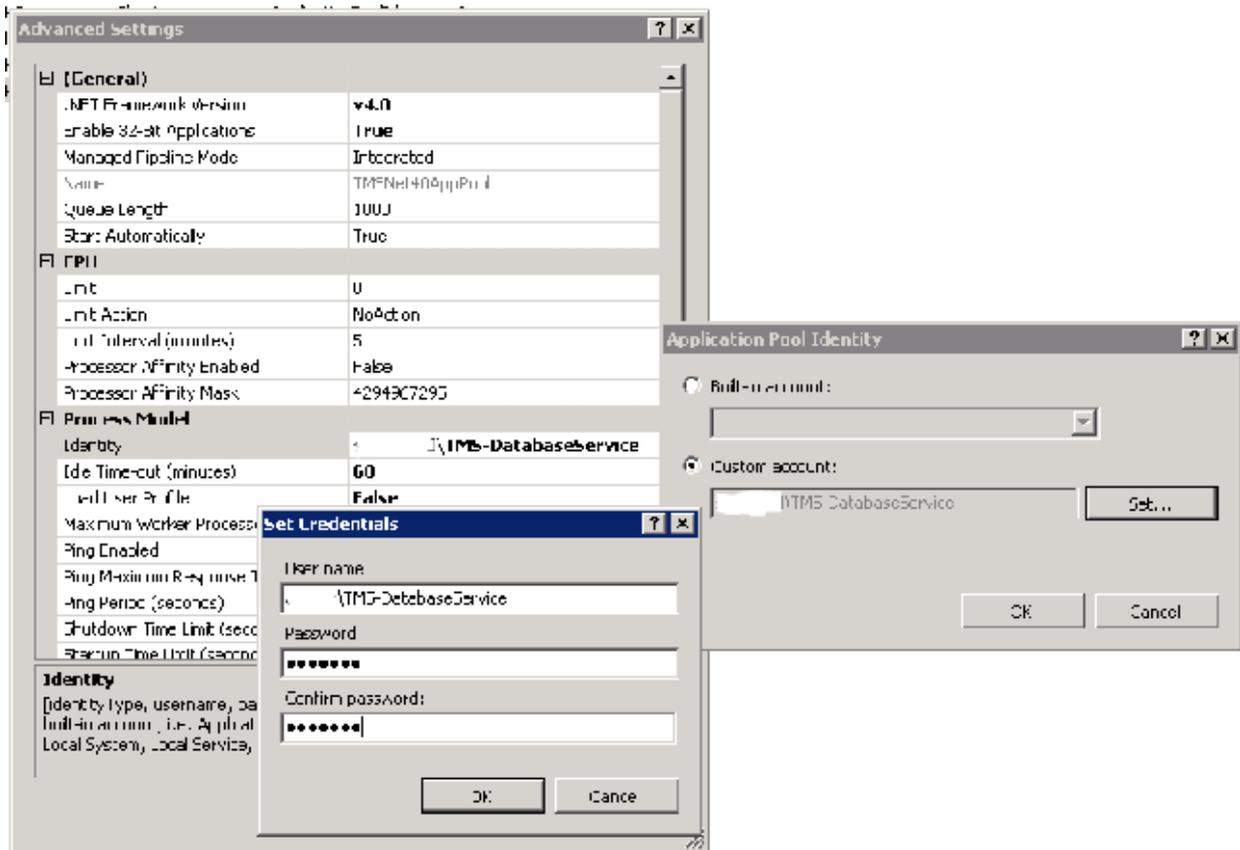
– Click **OK**.

Note: User should be automatically created when the login in step 2 is mapped to the tmsng database.

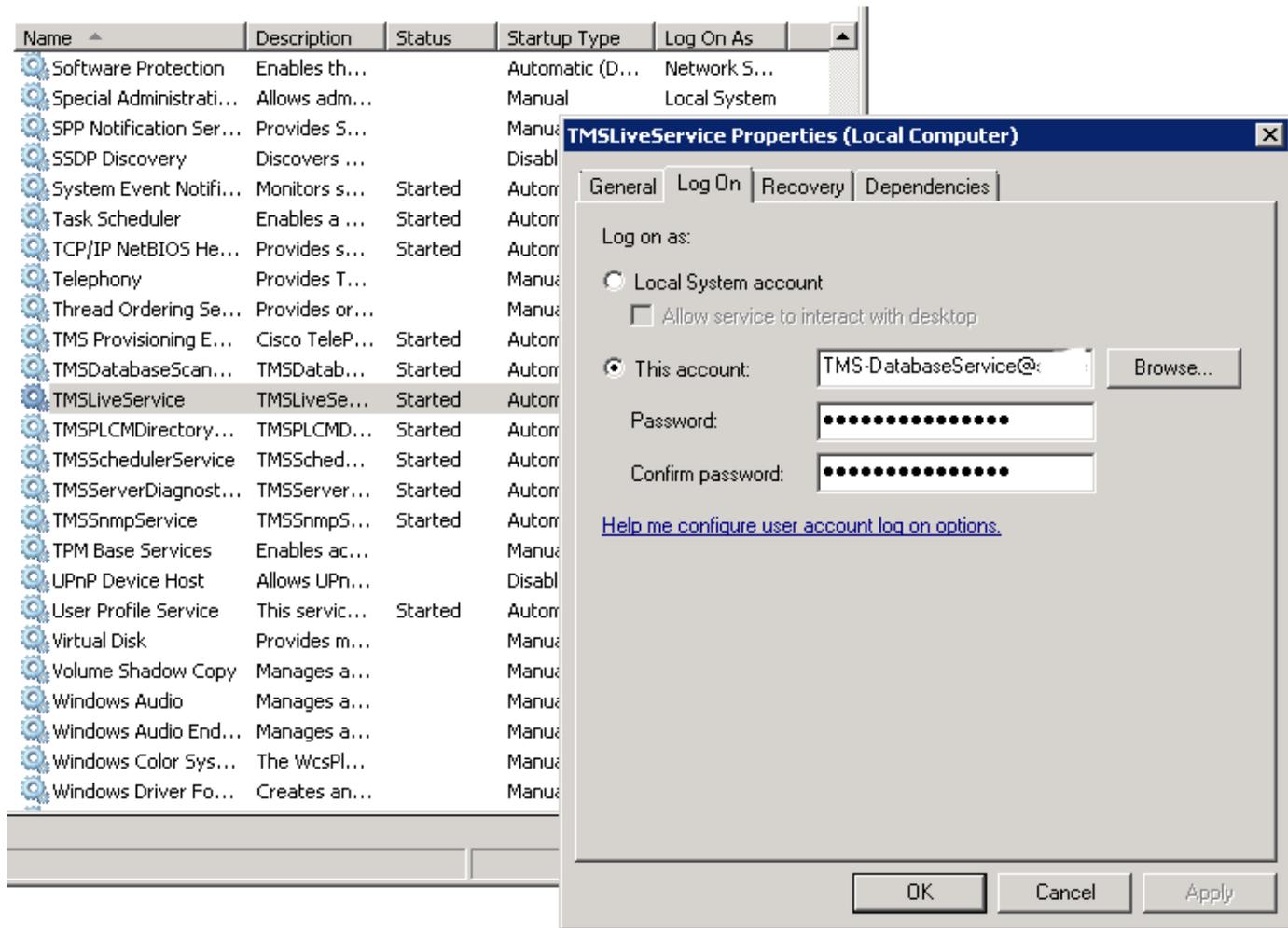
- In SQL Server, create a new login for the user account that runs TMS' IIS App pool. The default account for Windows 2003 (IIS 6) is **NT AUTHORITY\NETWORK SERVICE**; the default account for Windows 2008 (IIS 7) is IIS **APPPool\TMSNet40AppPool**.

Note: Since this is a local account, you cannot create a login for this user if using an external SQL Server.

If you use an external SQL Server; the **IIS APPPOOL\TMSNet40AppPool** user identity in IIS must be changed to a domain user (it can be the same user created in Step 1— ex: tms–databaseservice) via **IIS > Application Pools > right-click TMSNet40AppPool** and choose **Advanced Settings > Process Model > Identity**. Choose **Custom Account** and enter the service account (**DOMAIN\USERNAME**) and click **OK**.



Open *Services* and right-click each TMS Service, then go to '*Properties*' > *Log On ...* Choose *This account* and enter the service account *DOMAIN\USERNAME* and password. Open *TMS Tools* and go to *Database Connection Settings*. Enable Windows Authentication for both TMSNG and TMSPE databases.



Restart all TMS Services and the World Wide Web Publishing Service or restart the server.