EMS Database Authentication Options

Dean Evans & Associates, Inc.

Event Management Systems
Schedule Clarity

Copyright

Dean Evans & Associates, Inc.
6465 Greenwood Plaza Blvd
Suite 600
Centennial, CO 80111

Information in this document is subject to change without notice.

Database Authentication Options

Introduction

EMS employs an application-level security model. All EMS end-user accounts are provisioned within the EMS application. Connectivity between the EMS database and all EMS components (e.g. EMS desktop client, Virtual EMS, EMS Web Client, etc.) is managed with one fixed EMS SQL Server user account (EMSUser) that is created during the EMS database installation process. This security model requires that the server authentication for the Microsoft SQL Server that your EMS database resides on must be set to a mixed mode (SQL Server and Windows Authentication mode).

This document outlines the steps to replace the EMSUser account with an Active Directory account/group that your organization can define and control. In addition, this option will allow you to exclusively use the Windows Authentication mode (instead of SQL Server and Windows Authentication mode) for your server authentication.

Customer Support

Unlimited toll-free customer support is available to EMS users who have a current Annual Service Agreement (ASA). If you are unable to resolve a problem or answer a question by reading the EMS documentation, contact us at:

Email:	**support@dea.com**
Web:	**www.dea.com**
Phone:	**(800) 288-4565**
Fax:	**(303) 796-7429**

Pre-Installation Requirements

- EMS and all of its components must be installed and functional.
- An EMS-specific Active Directory security group that contains all of your EMS desktop client users is required. This group will be granted explicit permissions to your EMS and EMS_Master databases.
- An EMS-specific Active Directory user account that is a member of the Active Directory security group outlined above is required. This account will be used to configure this database authentication option for EMS web based products (e.g. Virtual EMS, EMS Web Client, etc.)

EMS Database Configuration

1. Using *Microsoft SQL Server Management Studio*, add a login for the EMS Active Directory security group outlined above.
2. Under the **User Mapping** area, map the login to your EMS database. Add the *db_datareader* and *db_datawriter* roles.
3. Repeat Step 2 for the EMS_Master database.
4. Using *Microsoft SQL Server Management Studio*, execute the following statement against your EMS database:

   sp_addrolemember 'EMS_Role', '*securitygroup*'

   Note: Replace *securitygroup* with the name of your EMS Active Directory security group.

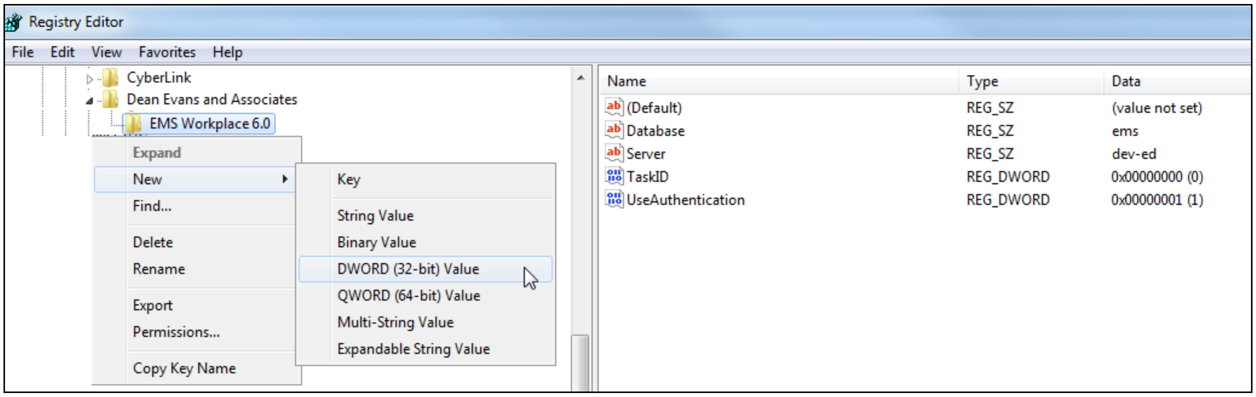
5. Repeat Step 4 for the EMS_Master database.

EMS Desktop Client Configuration

1. Go to an EMS desktop client user’s PC and open the *Registry Editor*.

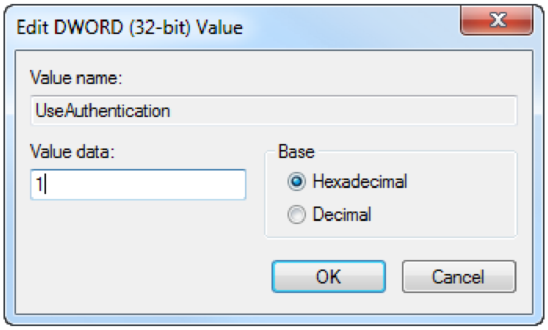
   WARNING: Registry changes can cause irreversible damage if done incorrectly.

2. Locate and expand **HKEY_CURRENT_USER**.
3. Locate and expand **Software**.
4. Locate and expand **Dean Evans and Associates**.
5. Highlight your EMS product folder (e.g. EMS Workplace 6.0).



Name	Type	Data
(Default)	REG_SZ	(value not set)
Database	REG_SZ	ems
Server	REG_SZ	dev-ed
TaskID	REG_DWORD	0x00000000 (0)
UseAuthentication	REG_DWORD	0x00000001 (1)

6. Right-click and add a **DWORD (32-bit) Value**.
7. Rename the **New Value #1** entry to ***UseAuthentication***.
8. Modify the **Value data** field to ***1***.



Value name: UseAuthentication

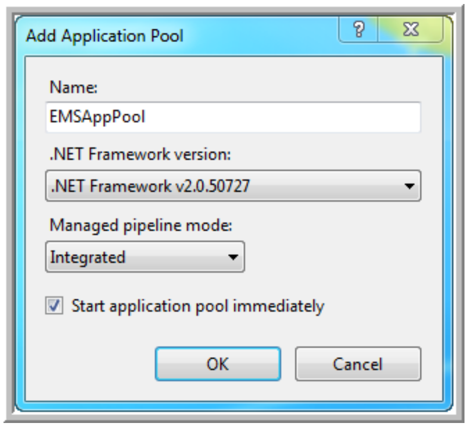
Value data: 1

Base
● Hexadecimal
○ Decimal

9. Launch your EMS desktop client application to verify connectivity.

EMS Web Based Application Configuration

1. Access *Internet Information Services (IIS) Manager* on your web server.
2. Create a new **Application Pool** that will be used by your EMS web based application(s) installed on this web server.



Add Application Pool

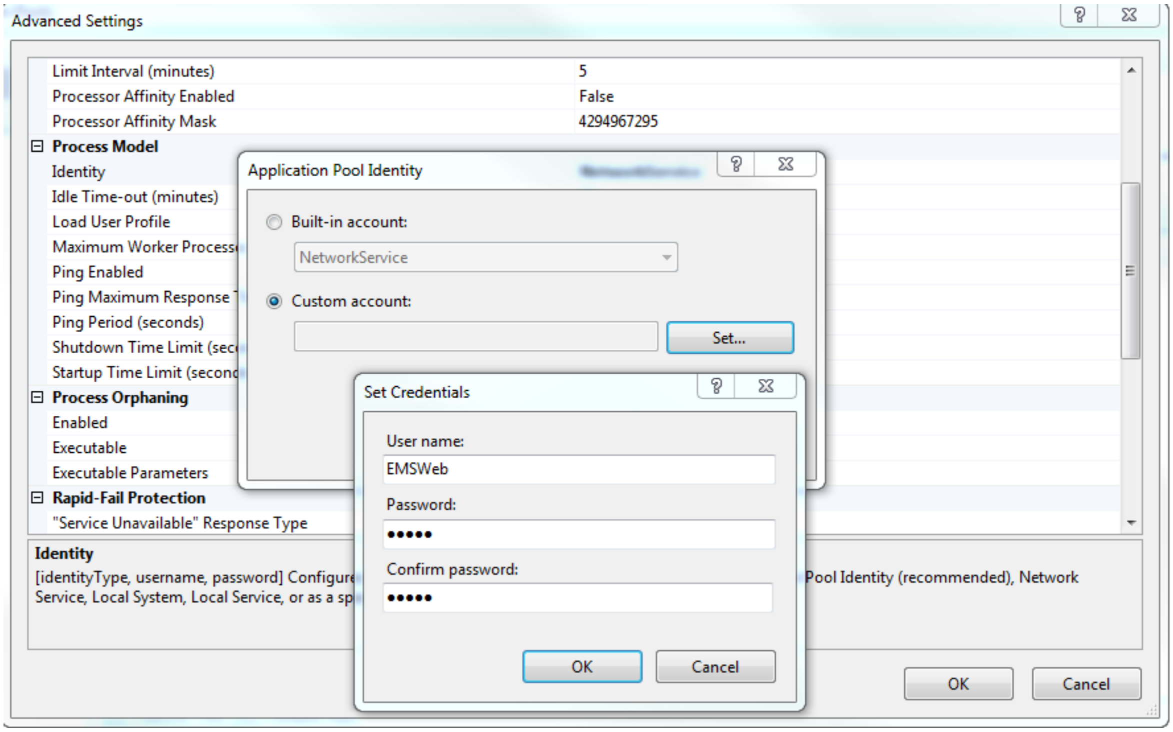
Name:
EMSAppPool

.NET Framework version:
.NET Framework v2.0.50727

Managed pipeline mode:
Integrated

☑ Start application pool immediately

3. Change the Application Pool **Identity** to run under a **Custom account**. Specify the EMS-specific Active Directory user account outlined in the Pre-Installation Requirements section.



Advanced Settings

Limit Interval (minutes) 5
Processor Affinity Enabled False
Processor Affinity Mask 4294967295
⊟ Process Model
Identity
Idle Time-out (minutes)
Load User Profile
Maximum Worker Process
Ping Enabled
Ping Maximum Response
Ping Period (seconds)
Shutdown Time Limit (sec
Startup Time Limit (second
⊟ Process Orphaning
Enabled
Executable
Executable Parameters
⊟ Rapid-Fail Protection
"Service Unavailable" Response Type

Identity
[identityType, username, password] Configure Pool Identity (recommended), Network Service, Local System, Local Service, or as a sp

Application Pool Identity

○ Built-in account:
NetworkService

● Custom account:

Set Credentials

User name:
EMSWeb

Password:
•••••

Confirm password:
•••••

4. Change the **Application Pool** in your EMS web based application to the pool defined above.
5. Open the **web.config** file for the EMS web based product and make the following changes:

```
<connectionStrings>
   <add name="deaConnection" providerName="System.Data.SqlClient" connectionString="server=MyServer;database=EMS;Trusted_Connection=yes" />
 </connectionStrings>
 <dataConfiguration>
   <databaseConnections>
     <add name="deaConnection" useEmsUser="false" useDetailedLogging="true" defaultCommandTimeout="20" />
   </databaseConnections>
 </dataConfiguration>
```

6. Launch your EMS web based product to verify connectivity.

Post Configuration

Once you have successfully verified EMS desktop client and EMS web based product connectivity to the EMS database, drop/disable your EMSUser account and re-verify connectivity once again.