Using Windows Authentication with SQL Server and Smartcrypt

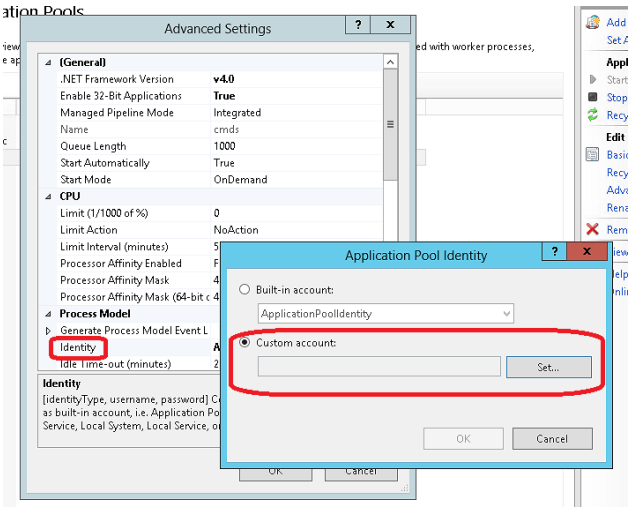
Windows Authentication

Summary of setup:

1. Create Windows Account (in AD or on local machine)
2. Create New Database in SQL Server
3. Set up ownership for Windows Authentication on new Database
4. Confirm you can log in with SQL Server Management Studio as Windows Credential

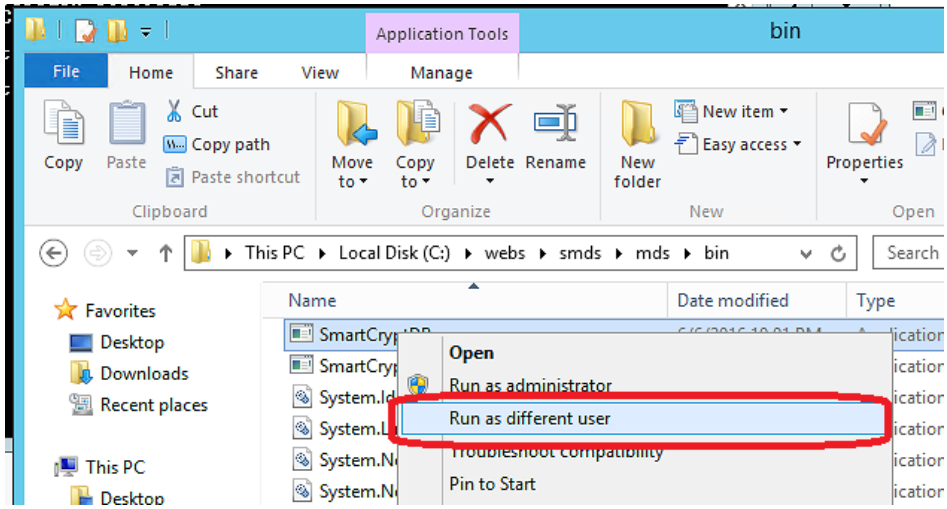
IIS Settings

The application pool need to authenticate and run as the user that has access to the database. This setting is available in the Advanced Settings of the Application pool in IIS.

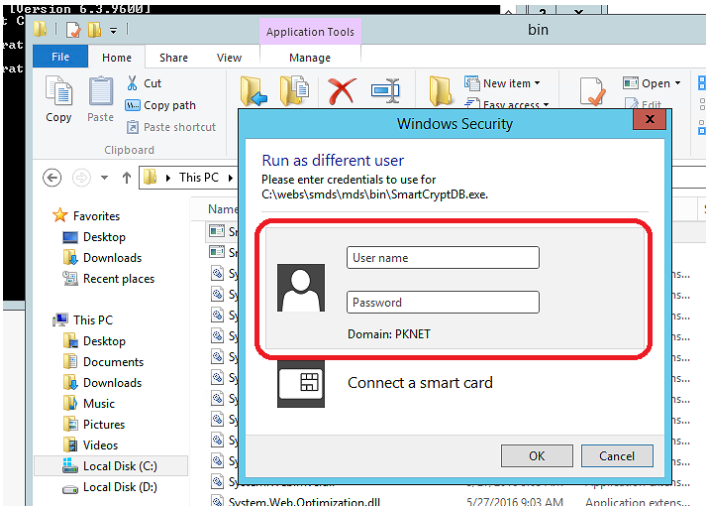


Loading Database Schema

The SmartcryptDB.exe utility needs to be executed by the account that has access to the database server. The SmartcryptDB.exe utility can be “Run As” any user by holding **<Shift> and Right Clicking** in Windows Explorer.



Then logging in as the actual Windows account defined in SQL Server to have access



Sample Connection String in Web.config

```
  <connectionStrings>
    <add name="SmartcryptEntities" providerName="System.Data.SqlClient" connectionString="Data source=
DBSERVER;initial catalog= DBNAME;Integrated Security=true;multipleactiveresultsets=True;App=EntityFramework" />
  </connectionStrings>
```

DBSERVER = Name of the database server – example: qadbserv.domain.com

DBNAME = Name of the Database created in the server - example: smartcrypt