Setup NTLM Access To Microsoft SQL Server From DigDash Enterprise With JTDS-SSO

This document explains how to access Microsoft SQL Server data sources using Windows authentication (with or without Single-Sign-On) from DigDash Enterprise.

I. SUPPORTED VERSIONS

- MS SQL Server 6.5
- MS SQL Server 7
- MS SQL Server 2000
- MS SQL Server 2005
- MS SQL Server 2008

II. WITHOUT JTDS-SSO ADD-ON

DigDash Enterprise natively supports access to Microsoft SQL Server without using this add-on.

You can also access a MS SQL Server data base using Windows authentication without this add-on by specifying the domain name, the user login and password on this domain.

The following condition must be fulfilled:

- In DigDash Enterprise Administrator, the URL should look like this: jdbc:jtds:sqlserver://[HOST]/[DATABASE];domain=[DOMAIN]
- The « User » and « Password » fields should be specified (no need for the domain in the user field).

III. WITH JTDS-SSO ADD-ON

The JTDS-SSO add-on is useful when you want to use the Windows integrated authentication without specifying a user name or password for the data base user.

The following conditions must be fulfilled:

- The DigDash Enterprise server is installed on a Windows computer currently connected to an NT domain
- The account used to launch tomcat (or the service account) must have access to the database, or you must specify a different account name and password when configuring the data source.

IV. SETTING UP THE JTDS-SSO ADD-ON

To allow DigDash Enterprise to access a MS SQL Server data base with Windows authentication, you must do the following:

1. Extract the folder <DigDash Enterprise install folder>/add-ons/jtds-ss/**jtds-sso.zip** to a folder of your choice on the hard drive. This archive contains a DLL **ntlmauth.dll** for each processor architecture.
2. Modify the environnment System variable **Path** by adding the path to the folder containing the **ntlmauth.dll** corresponding to your processor architecture.

Note on using the jTDS-SSO connector with Kerberos
In Active Directory, the service url HTTP/<computername>.<domainename> must be mapped (declared « SPN ») with the domain service account:
`Setspn.exe -S HTTP/<computer-name>.<domaine-name>:<port> <domain-user-account>`

