SQL SECURITY AND REDHORSE CRM

This article will walk you through the best practices for setting up SQL logins and security for use with RedHorse CRM.

Authentication in SQL

When installing RedHorse CRM for the first time, you will be asked to enter login credentials for the SQL Server where the RedHorse database will be installed. There are two options available:

- **SQL Server Authentication** - SQL Server Authentication uses login names and passwords stored in SQL Server. You can select SQL Server Authentication only if SQL Server Authentication has been enabled on the server. When you select this option, you will be asked to enter a SQL Server login name and password. You may specify only one SQL Server login name that will be used by all users in RedHorse.
- **Windows Authentication** - Uses Windows Integrated Security for the login. Windows Authentication is more secure than SQL Server Authentication. Logins that use Windows Authentication are also easier to manage than SQL Server logins. When you select Windows Authentication, you do not need to enter a SQL Server login name. The login name used to log into Windows by any user of RedHorse will be used to log into SQL Server.

For a very simple or small installation, an installation where security in SQL Server is not a concern, or an installation where it is not necessary to track security for each user in RedHorse CRM, SQL Server Authentication is adequate.

For an installation where the administrator would like to control or monitor an individual user in SQL Server, Windows Authentication is recommended.

Using Windows Authentication

When using Windows Authentication in SQL Server, any user with Administrator rights will be able to run RedHorse CRM with no additional configuration steps required. Non Admin users will need additional setup in SQL Server to provide adequate security to access RedHorse CRM. User logins in SQL Server with db_owner rights to the RedHorse SQL database will be necessary. You can add these users individually to SQL Server or you can create a users group in your Windows Active Directory and then add your RedHorse CRM users Windows logins to this user group.

RedHorse Systems, Inc.
support@redhorsesystems.com
www.redhorsesystems.com

To set up Windows logins or groups in SQL Server, follow these steps:

1. If you will be using a group, create a users group in your Windows Active Directory and then add your Redhorse CRM users Windows logins to this user group.
2. In SQL server Management Studio add a new Login.
3. Enter the Windows login name or Active Directory Group name into the Login Name field.
4. Select Windows Authentication.
5. Go to the User Mapping page of the Login Properties dialog.
6. Check the Map checkbox next to the RedHorse CRM database.
7. Enter the name of the Windows login or group in the User field for the RedHorse CRM database in the format of domain\username.
8. Check db_owner in the Database Role Membership. Leave public also checked.
9. Save the new login.

Once the SQL login for the Windows Active Directory Group is created, any Windows user who is a member of the user group will be able to launch RedHorse CRM from their Windows session from any machine on the network.

Please contact support if you experience any issues during the setup of SQL security for RedHorse CRM.

RedHorse Systems, Inc.
support@redhorsesystems.com
www.redhorsesystems.com