

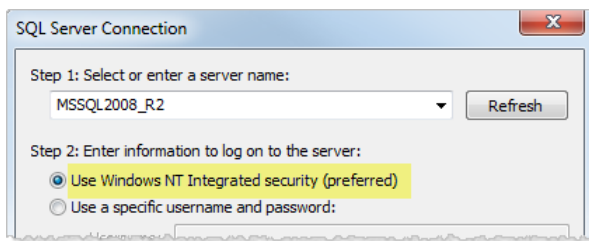
# SQL Server Impersonation

When you publish views to Tableau Server that connect to a SQL Server database, you can leverage the security rules set up in the database to filter the data each user sees. When a user accesses a view, Tableau Server connects to the database using an account that has the IMPERSONATE permission for that user's account. This account acts on behalf of the user's database account. As a result, without being prompted to log into the database, the user gets a view that shows only the data she has permission to see. There are two ways to set up impersonation:

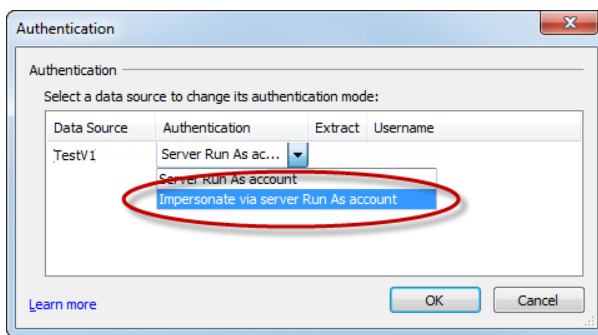
## A Use Tableau Server Run As

When you install Tableau Server, use an Active Directory Run As account for Tableau Server. In SQL Server, grant the Run As account the IMPERSONATE permission for the database users who'll be accessing views.

In Tableau Desktop, workbook authors connect to the database with **Use Window NT Integrated Security**:

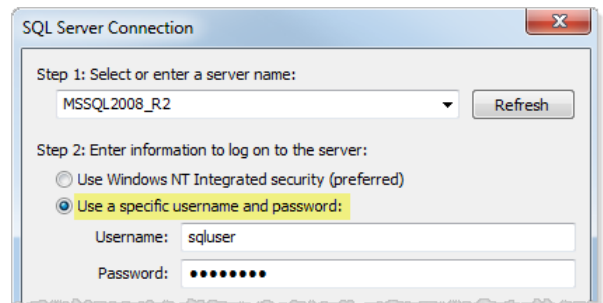


When authors publish workbooks, they select **Impersonate via server Run As account**:



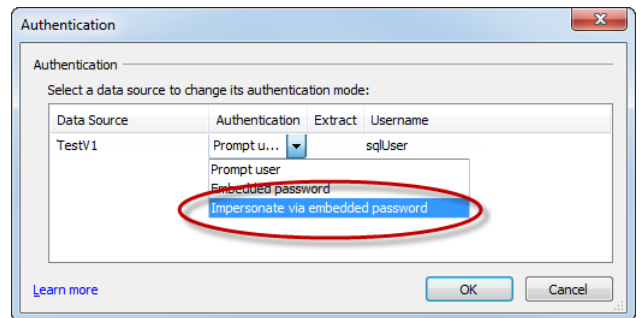
## B Embed SQL Server Credentials

Workbook authors connect to the database using a SQL Server account:



In SQL Server, this account has IMPERSONATE permission for the database users who'll be accessing views.

When they publish workbooks, authors select **Impersonate via embedded password**:



## Requirements

**Live SQL connections only:** Impersonation can only be used for views that have a live connection to a SQL Server database.

**Individual database accounts:** Each person who'll be accessing views on Tableau Server must have an individual account in the database. Membership as part of a group is insufficient.

**Matching credentials:** The credentials of each user's account on Tableau Server and in the database must match.

**SQL IMPERSONATE account:** You need a SQL Server database account that has IMPERSONATE permission for the above database user accounts.