SQL Security with BI360

A Solver White Paper

Published: July 6, 2016
solverusa.com

Table of Contents

BI360 Security

Introduction

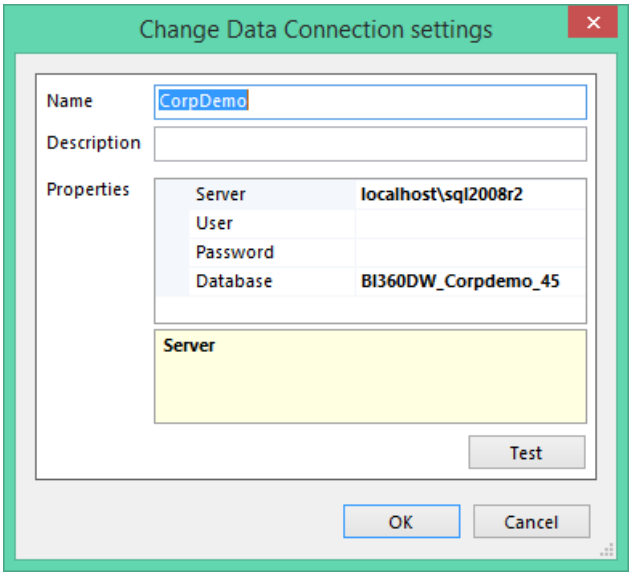
When implementing BI360 there are multiple areas of security to take into consideration. In particular, this document will focus on SQL and implementation security (user acceptance). Organizations should also be aware that there is application data security that must be configured. Full details on application data security can be found on the Solver Support Knowledgebase. Solver does not consult on SQL setup or maintenance but does provide information on the necessary permission so that the organization's users can use the BI360 software seamlessly. When using BI360 the following should be taken into consideration:

1. SQL Database Security
2. Application Database Upgrade Permissions

The next section will briefly describe the above mentioned security considerations. If you have additional questions about database security, please contact your IT.

SQL Database Security

The BI360 suite requires that users have access to the BI360 databases. The BI360 Suite allows the organization to use either Windows or SQL authentication to connect to these databases. The authentication method that will be used by the application is defined during install but can be changed at any time via the Administration Tool.



The above screenshot has been taken from the connections screen found within the **Administration Tool**->**System Settings**->**Setup**. The user and password have been left blank. When left blank, the application will use Windows Authentication to connect to the database. The next section will detail the permissions needed so that when connecting using Windows Authentication, the user connect without issue.

Organizations may choose to not leave this blank and use the credentials of a SQL user by typing in the information of a SQL user and the SQL user's password. When the application loads and connects to the

database(s), it will use this SQL user's permissions to access the data. Details of the permissions required for this user are described in the next section.

The application requires permissions to the following databases. If the Windows user or SQL user does not have these permission the user will get an error message saying "Login failed for users: <UserName>" and the application will not work.

1. The ERP database. For example, this could be GP, SL, AX etc.
    a. When dealing with an ERP with multiple databases, it is required that the user has access to all databases that the user will be connecting to. For example, when working with GP, there is a "Dynamics" database and the company database; "TWO" as it is referred to in the demo GP. The user will need read permissions on both of these databases in order to effectively use the application.
    b. There are two types of permissions that MAY be required. Please read carefully the following two bullet points that describe when the following permissions will be necessary.
        i. Db_DataReader: This is required for ALL BI360 users. It is required that a user be assigned as a db_DataReader on the ERP database because they are running reports that are pulling financial data from these systems.
        ii. Db_DataWriter: this permission is typically not required but is needed in the following two scenarios.
            1. The user is going to be using the Multi-Company Load (MCL) module to consolidate their companies. When running the MCL, the application will create multiple tables on the destination database where the consolidated data will be added. This requires write permissions on the database.
            2. The organization will be using Web Budgeting. When using Web Budgeting, the user can write data directly back to the ERP. This will require that the application pool user (created during the install or the Web Portal) have write permission on the ERP database.
2. OSR_Repository database. Created during the installation of the Reporting application, this small non-financial database contains application administrative information such as the license keys and the assigned users. ALL BI360 users, when using windows authentication, need both db_DataReader and db_DataWriter permissions on this database. This is necessary because the BI360 application authenticates the logged in user with the information stored in this database. Additionally, for caching purposes and to speed up reports, every time a report is opened, the application writes information into this repository database; this is where the write permissions on this database are required.

    NOTE: when using SQL authentication (as defined during the installation), the application is hardcoded to a specific SQL user, "osruser", who is created during the installation process. This user has a hard coded password which cannot be changed. An organization may switch from SQL to Windows authentication or vice versa if desired. There is no need to setup SQL security for this user as it already has the necessary permissions to connect to the repository database.

3. BI360 Data Warehouse DB (BI360DW). This database is used by any organization that is using the *Data Warehouse Manager* and/or *Planning*. BI360 users need to have db_DataReader and db_DataWriter permissions on this database as they will be pulling financial information from this database. They need datawriter permissions on this database because they will be creating and maintaining the data within this database via the BI360 *Data Warehouse Manager* and *Planning*.
   Additionally, there are other necessary permissions required to use the BI360 Data Warehouse Manager completely. These permissions are all part of the database role "BI360_User" (formally referred to as "SODS_User"). These "Grant" permissions are:
   a. Update
   b. Select
   c. References
   d. Insert
   e. Execute
   f. Delete
   g. Create Table
   h. Create View
   i. Create Procedure

   To verify these permissions the use can run the following query in SQL.

```
--Declare Parameters
Declare @dbrolename varchar(50)

--Set Parameter
SET @dbrolename = 'BI360_User' --this could be
SODS_USER or BI360_USER

--Do Not Edit Below this Line
SELECT prin.[name] [User], sec.state_desc + ' ' +
sec.permission_name [Permission]
FROM [sys].[database_permissions] sec
JOIN [sys].[database_principals] prin ON
sec.[grantee_principal_id] = prin.[principal_id]
WHERE sec.class = 0 and prin.[name] =@dbrolename
ORDER BY [User], [Permission]
```

Windows vs SQL Authentication

The organization must choose between Windows or SQL authentication when connecting the application to the database(s). In BI360, it is not possible to assign both at the same time or to pass off one SQL authenticated user for one group or users and another SQL authenticated user for another set of users. Ultimately, the decision to use Windows or SQL authentication falls on the organization's system/IT/DBA admin who is controlling access to the various databases that are being accessed by the application. However, the following should be taken into consideration when using either windows or SQL authentication.

SQL Authentication

This type of authentication is stored on the SQL Server and consists of a user name and password. During the installation of the SQL Server, the user is prompted allow SQL authentication in conjunction with Windows authentication, called Mixed Mode. This can be changed after installation. In Mixed Mode, the SQL Server will enable a system administrator user with full rights/permissions, called 'sa'.

Disadvantages of SQL Server Authentication

- Less secure as a shared password may be released to unauthorized users, or for unauthorized access in other programs.
- If a user is a Windows domain user who has a login and password for Windows, he must still provide another (SQL Server) login and password to connect. Keeping track of multiple names and passwords is difficult for many users. Having to provide SQL Server credentials every time that one connects to the database can be annoying.
- SQL Server Authentication cannot use Kerberos security protocol.
- Windows offers additional password policies that are not available for SQL Server logins.

Advantages of SQL Server Authentication

- Allows SQL Server to support older applications and applications provided by third parties that require SQL Server Authentication.
- Allows SQL Server to support environments with mixed operating systems, where all users are not authenticated by a Windows domain.
- Allows users to connect from unknown or untrusted domains. For instance, an application where established customers connect with assigned SQL Server logins to receive the status of their orders.
- Allows software developers to distribute their applications by using a complex permission hierarchy based on known, preset SQL Server logins.
- A shared “application” user can be used so a password can be hidden from users and only a particular application will use it – easier maintenance.

Windows Authentication

This type of authentication uses the Windows user account, and will not prompt for a password when creating a connection to the application. The user account is created on the domain in Active Directory. This is more secure than SQL Authentication as it uses Kerberos security protocol.

Disadvantages of Windows Authentication

- User must be logged on to the Windows session. Changing to another user name is not possible without a) logging off and back in as a different user, or b) running an application as another user.
- Additional maintenance will be required as each time a user is created, the user must be mapped to the database and SQL rights/roles must be applied.

Advantages of Windows Authentication

- Maintenance is easier, as an Active Directory group can be added to the SQL Server.
- This method is more secure due to Kerberos authentication, scheduled password changes, and passwords are not shared between users.
- Users added to a group can be given mapped to the database, given folder rights to a Terminal Server, and/or have data access filters in BI360 applied all at once.
- User accounts can expire or are disabled when the network administrator makes or enforces changes in Active Directory.

- Audits can be done on the database on a per user level.
- Security can be done per user or group, instead of all users sharing the same database security as given by a SQL authenticated user.

How does this play into the application?

When using BI360, depending on the implementation, users are able to connect to the database via other methods.

- With Windows authentication, since you are granting read permissions to a database, a user familiar with ODBC can use a third party tool to connect to the database and bypass application security. To avoid, this SQL authentication should be used.
- With SQL authentication, as a DBA you have no control of who has the password. If the password were to get compromised, you would have to change the password for all applications that are using it.

These are the two points to be aware of when implementing SQL security in BI360.

Solver's Recommendation

Before reading this section, please review the above sections. The below section is Solver's recommendation, but it is up to the organization to choose the authentication method(s) that best meet their business usage.

Solver's recommendation is to use windows authentication on the repository database and SQL authentication on the ERP/BI360 database. This will ensure the application works seamlessly while also ensuring that all potential security risks are covered.

Authentication to the Repository

When working with the repository specifically there are two types of users who will be accessing data found in this database

1. Administrators
2. End Users

Administrators are those who are making application wide changes, including

1. Adding/updating license keys
2. Adding/update integration packages
3. Adding/updating users
4. Adding/updating security

End users are defined as any user creating a report or running a report. It is possible that an end user is also an administrator.

Administrators need read and write permissions to the repository database. This is because when doing the actions listed above, write permissions are needed to the repository database to perform these actions.

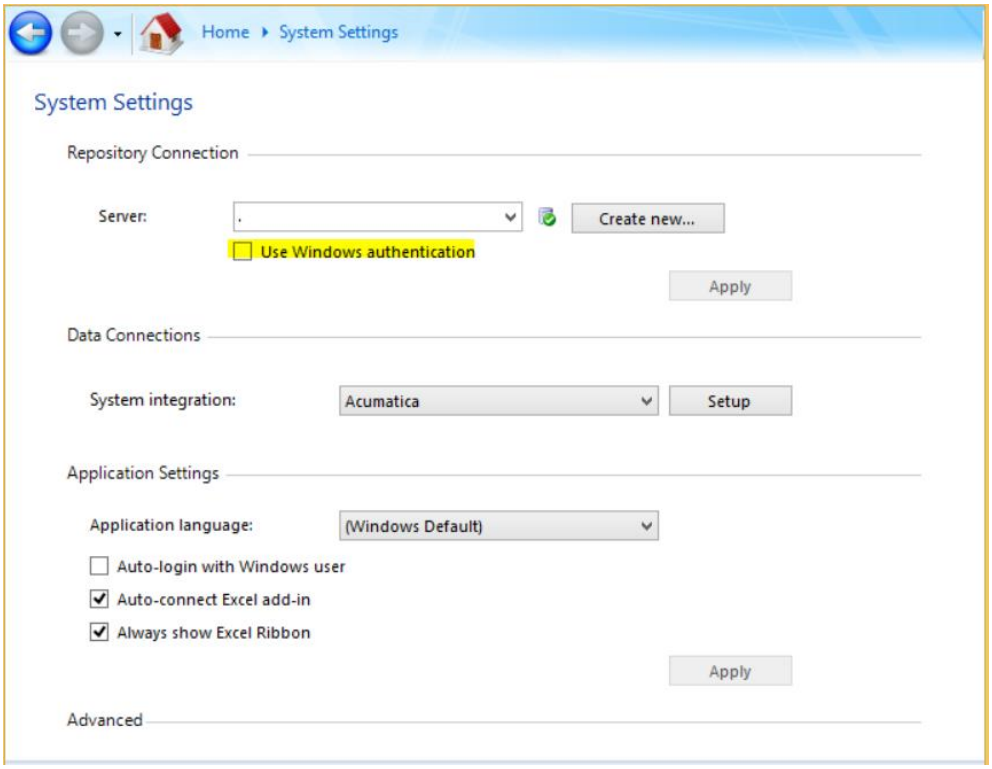
End users need read permissions to all tables, but only need write to a few tables. These tables are:

1. DatasourceSettings
2. IntegrationSettings

By doing windows authentication on this database, it prevents a more technical end user from figuring out a way to update the administrative tasks listed above. Solver recommends against SQL authentication to the repository because the SQL authentication is based upon a hardcoded users, osruser, with a hard coded password. Only our internal developers know this password, but some organizations may be against this.

To check if the organization is using windows or SQL authentication,

1. Open the Administration Tool -> System Settings.
2. Under Respository Connection -> Server there is a checkbox for Windows authentication
    a. If checked, this computer is connecting via windows authentication.
    b. If unchecked, this computer is connecting via SQL authentication.



NOTE: This is a per computer settings.

This section is intentionally left blank

Authentication to the ERP/BI360 database

Solver recommends SQL authentication on the ERP and/or BI360 database.

- On the ERP database, read permissions are needed unless the organization is using MCL. When using MCL, users also need permissions to update, delete, create table, drop table.
    - In particular, users need permission to update, delete and drop any table that begins with “OSR”. These are application tables that are created for MCL purposes, make sure that there are no other “OSR” tables that existed previously.
- On the BI360 database, users need read and write permission along with being assigned to the BI360_Users database role.

Although BI360 has its own level of application security, a technical user may know of other ways to get around this application security layer. Because of this, it is recommended to use SQL authentication. Unlike the repository, this SQL user is an account created and maintained within the organization and only your organization knows the password to this user. This password should only be given out to select individuals (consult your DBA) which will prevent the more technical users from bypassing BI360’s authentication layer.

This section is intentionally left blank

Application Database Upgrades

When upgrading the BI360 databases, there are only two databases that are upgraded during this process, the BI360 *Data Warehouse* database and the Repository database. **The BI360 upgrade does not upgrade, nor touch, the ERP database**. Before performing any upgrade, the aforementioned databases must be backed up. To run the BI360 upgrade, it is strongly recommended to be a sysadmin. When running the installers to upgrade the database, the user must either be logged in with a windows profile that has sysadmin permissions on the SQL server OR knows the password of a SQL user with sysadmin permissions. However, in organizations with tight security the following may be used.

1. OSR_Repository: The windows logged in user or SQL user must be a ddl_Admin on the OSR_Repository with DBO Schema
2. BI360 Data Warehouse database: the windows logged in user or SQL must be the db_Owner with DBO Schema. However, when creating the database or upgrading the database, the previously mentioned database role, “BI360_User”, will only be created by a user who is sysadmin.

This section is intentionally left blank

Web Portal

When installing the web portal, the application will create a user, (referred to as an Application Pool User) on the SQL Server where the repository database is created called “Domain\MachineName$”. For example, if the web server machine where the Portal is being installed is called “WebServer01” and your domain is called “MyDomain”; during the Portal install, the application pool user MyDomain\WebServer01$ will be created on SQL. This user needs to be mapped with the following permissions:

1. Read/write to the OSR_Repository
2. Read on all databases that will be connected to in the Portal.
    a. This user is ONLY created on the SQL server where the Repository is created. If the company ERP databases are located on separate SQL servers, this Application Pool User must be added to each one of those SQL servers. When creating this user on another SQL Server, use windows authentication and grant read permissions to the necessary ERP databases.

    NOTE: this application pool user is NOT a domain account and DOES NOT need to be created on the domain controller.

This section is intentionally left blank

User Acceptance Phase

During or near the end of an implementation it is important to have a user acceptance test (UAT) phase. This phase comes after the software has been installed, the data has been pulled into a report and now the users are using the form in a user acceptance phase to make sure that the forms are working as desired, including that SQL security is being inherited properly. As a BI360 Administrator, this is a great time to test the security of the forms and the data that users are seeing and/or adding.

Some general best practices when distributing the forms are:

1. Place the reports in a central shared drive location. This is a great time to use Planning's Assignment feature.
    a. Store files in a location with read only permissions. You don't want users to be able to save any changes to the "production" reports.
    b. If an organization has purchased Report Publisher, then there should be a separate set of reports strictly for Report Publisher. This is strongly recommended because if a report used by Publisher is left open in Excel, then the report cannot be accessed by Publisher and the Publisher subscription will not be delivered.
        i. Keep in mind that if implementing a separate Publisher folder with BI360 reports, that any changes made to a report need to be brought over to the Publisher folder.
2. Protect the form using Excel's protect worksheet feature. This will prevent users from making any undesired changes. Changes that are needed can be reviewed by a report designer and not by the end users.
3. Assign users as player users. When distributing the forms out to the end users, they should be Player Users who can only run reports and not drag in fields.
4. Color coordinate cells where possible so that users know which cells to type into.

Dev vs Production Environments

It is strongly recommended to have a dev and production environment. An organization can test upgrades and new features in the dev environment while leaving the working production environment in place for the end users. If a change is made in dev that results in the application no longer working, it will have no impact on the production users. The issue in dev can be resolved in a controlled manner without becoming "production emergency". An ideal dev and production environment is two completely separate systems. In BI360, you need a separate SQL Server and Application machine for each environment; this is not required but recommended. Although they are separate machines, it is recommended that they be configured exactly the same (unless you are testing a new operating system or Microsoft Office compatibility with BI360), so that the environment can be ruled out as an issue.

Besides have a dev and production environment, an organization should also have dev and production BI360 reports. When "production" reports have been created and have been confirmed, they should be placed into the central location as mentioned in #1 of the User Acceptance Phase. However, if you want to make a change to this report to add more data, you should create a copy of the report and store it in a dev location where only a select number of "report designers" have access to it.

Additional Information

Solver Support Center

The Solver Support Center (support.solverusa.com) is the centralized location for users to learn more about the BI360 Suite. From opening and managing your support tickets to reading knowledgebase articles about the product, the Solver Support Center has everything a user will need.

Users may contact Solver Support if they have questions about the BI360 Suite. One of our technical support consultants will gladly assist you.

Users can access the Solver Knowledgebase for more information about the entire BI360 Suite. From user guides, white papers, training manuals and much more, the Solver Support Center has everything a user will need to get started with the application.

Solver Forum

The Solver Forum (solverusa.com/forum) is a great resource for users to ask questions about the software. Other users or one of the many Solver employees frequently check the boards and can quickly answer your questions.

Solver Feedback

Solver invites customers to participate in providing feature requests for future versions of BI360 on a site just for user feedback, feedback.solverusa.com. On the Solver Feedback site, users may suggest features for updates and upgrades to BI360 – and/or vote on existing feature submissions from fellow customers to really push for feature(s) that would make BI360 even more powerful, dynamic, and intuitive.