



# CONNECT SECURELY TO OBIEE WITH TABLEAU USING BI CONNECTOR

Whitepaper

## Abstract

Organizations have invested years and millions of dollars to build a robust security model to protect their strategic and important data in OBIEE. Read this whitepaper to learn how users can reuse OBIEE security model to connect from Tableau Desktop and Tableau Server to OBIEE data by using BI Connector.

## Introduction

Organizations depend on OBIEE's robust security model to protect their most strategic and important data assets. Often, years of effort and millions of dollars is invested by an organization to ensure that the right people have the right access to the right level of data stored in their OBIEE environments.

When Tableau, which provides modern visualization and analytics capability that is loved by users, is introduced in the organization, it is important to reuse the existing security model in OBIEE. This would allow organizations to maintain the highest levels of data security and efficiently integrate the new platform into their Business Intelligence fabric without reinventing or duplicating the security model.

BI Connector has been designed from the ground up to connect Tableau securely to OBIEE by reusing the existing security model in OBIEE. In this white paper, we will discuss the data security scenarios when connecting from Tableau Desktop and Tableau Server to OBIEE with live connection and data extraction options.

## Data Connection from Tableau to OBIEE

Tableau provides the capability to connect to a data source both in live and in extract mode. BI Connector supports both these options when connecting from Tableau to OBIEE.

### Connecting Securely from Tableau Desktop

When using BI Connector desktop version, the Tableau desktop user downloads the BI Connector and sets up an ODBC Data Source to OBIEE. Then the user opens Tableau and connects to OBIEE at which point she is required to enter her OBIEE username and password along with the OBIEE URL. You can use the Secure Socket Layer(SSL) enabled HTTPS URL for OBIEE or the HTTP URL. From OBIEE perspective, a user connecting from Tableau using BI Connector is similar to a user using web browser to connect to the OBIEE URL with their user name and password.

### Live Connection Method

The default method in Tableau is live connection. In this method the user's credentials are validated by OBIEE security layer. Once the user is authenticated the user is presented a list of subject areas from which they can do their analysis and visualization in Tableau.

All of OBIEE data level security rules are retained while the user is using Tableau to connect live to OBIEE. The user sees only the subject areas and the data that they have permission to access in OBIEE. You can login into OBIEE directly from a web browser and compare the visible subject areas to the Tableau view.

When the user saves the workbook, the user credentials are not saved for security reasons. When the user reopens the saved workbook that uses a live connection, the user is prompted to reenter the username and password for OBIEE.

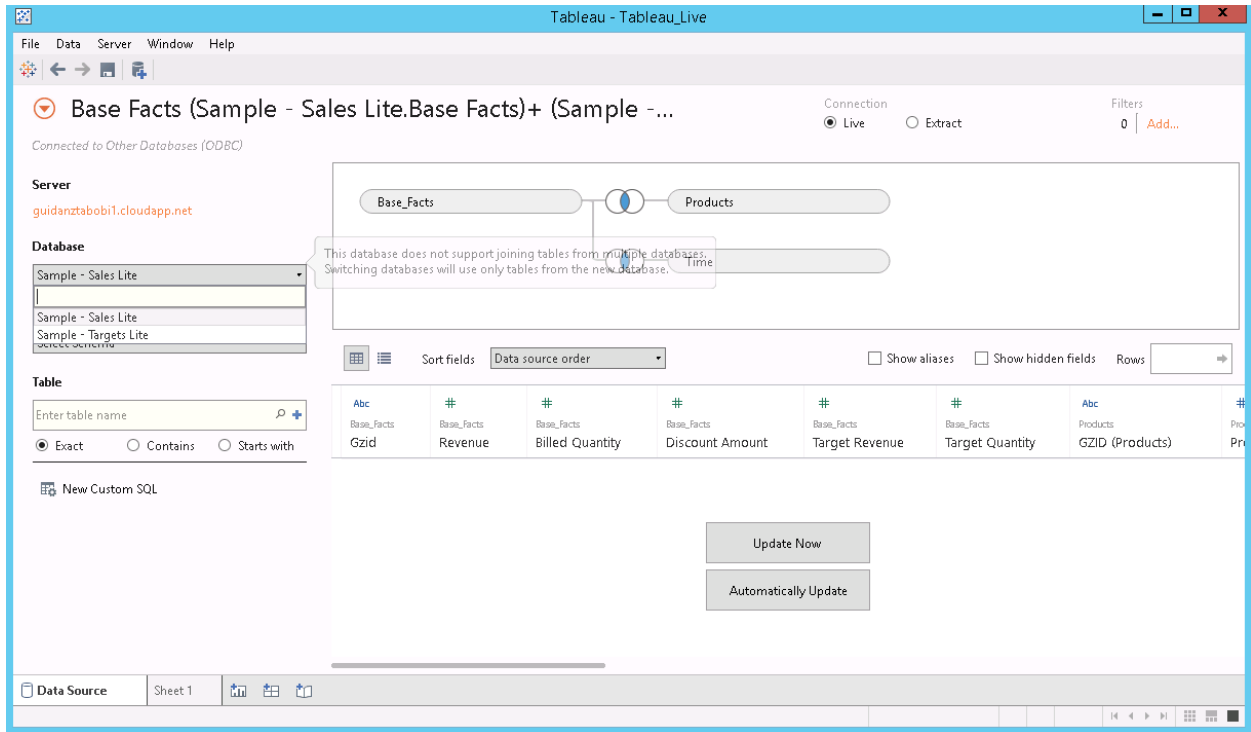


Figure 1 User sees only the subject areas they have permission to access when connecting to OBIEE

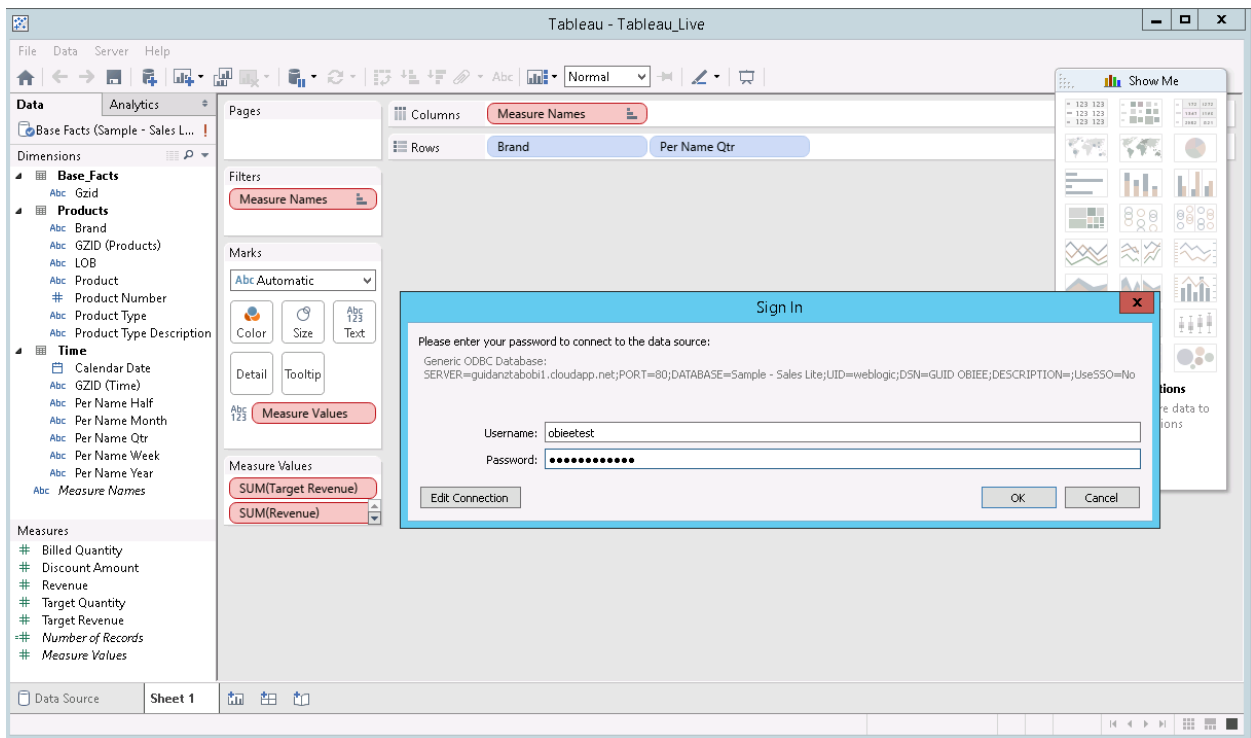


Figure 2 User is prompted for credentials every time she opens the worksheet

## Extract Scenario

Using BI Connector, the Tableau user can extract the data from OBIEE as a one time or on periodic basis using the Extract method in the Tableau data source. In this case as well the user is prompted for username and password when connecting to the data source to initiate the extract. Once the user selects the tables she wants to analyze, sets the extract filter and moves to the worksheet to analyze, the Tableau data extract (.tde) gets created. Once the extract completes the user can now analyze the data embedded in the .tde file. The data in the .tde extract has only the data that her OBIEE security allows. The user then saves the workbook.

When the user reopens the saved .tde file, the user is not required to reenter the OBIEE username and password since the data is already downloaded into .tde file. The user does not require any password to access the worksheet that uses the .tde file. However, if the user needs to change the extract criteria, then Tableau/BI connector now asks for her OBIEE credentials again before proceeding to create a new extract or modifying an extract. This prevents any unintended update of the Tableau worksheet that was created.

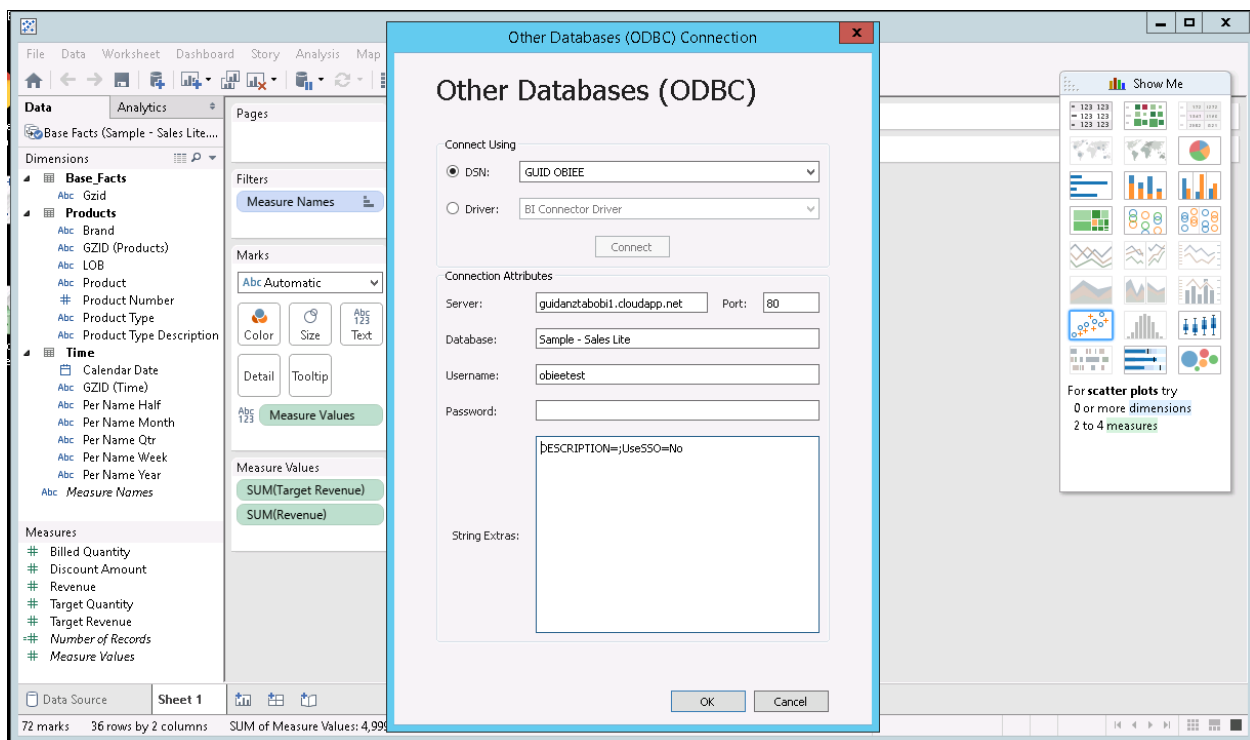


Figure 3 If the user needs to change the extract conditions, the user is prompted for credentials

## Tableau Server

The first step to using Tableau server is to create a data source in Tableau Desktop where the user connects to OBIEE using BI Connector and then publish the data source to Tableau server as seen in the below screenshot.

### Live Connection Scenario

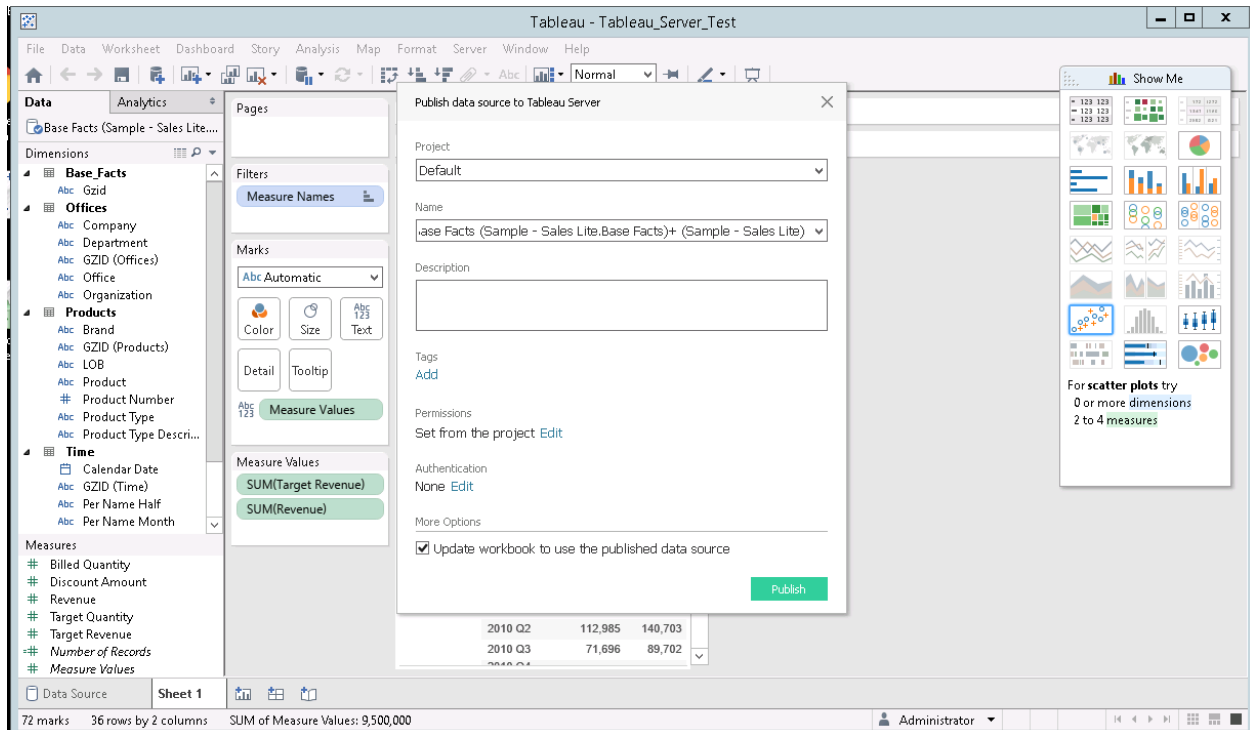


Figure 4 Publish OBIEE data source from Tableau Desktop to Tableau Server

Once the data source is published, go to Tableau server and test the connection. You will notice in the password section there are 2 options –

1. Prompt user for password, if needed
2. Embedded password in connection

With option 1, any worksheet created with this data source on the server or desktop will always ask for OBIEE username and password for the user using the report. This will ensure that the OBIEE security is maintained in Tableau.

With option 2, the username and password are embedded in the data source and it uses the credentials that are supplied in the data connection for all users. This needs to be carefully evaluated if this is the right approach for your data security needs. If you need to provide data access to your senior executives and they don't want the hassle of entering their OBIEE username or password every time, you can create a Tableau Site or User group with select users and provide restricted access to the embedded password OBIEE data source.

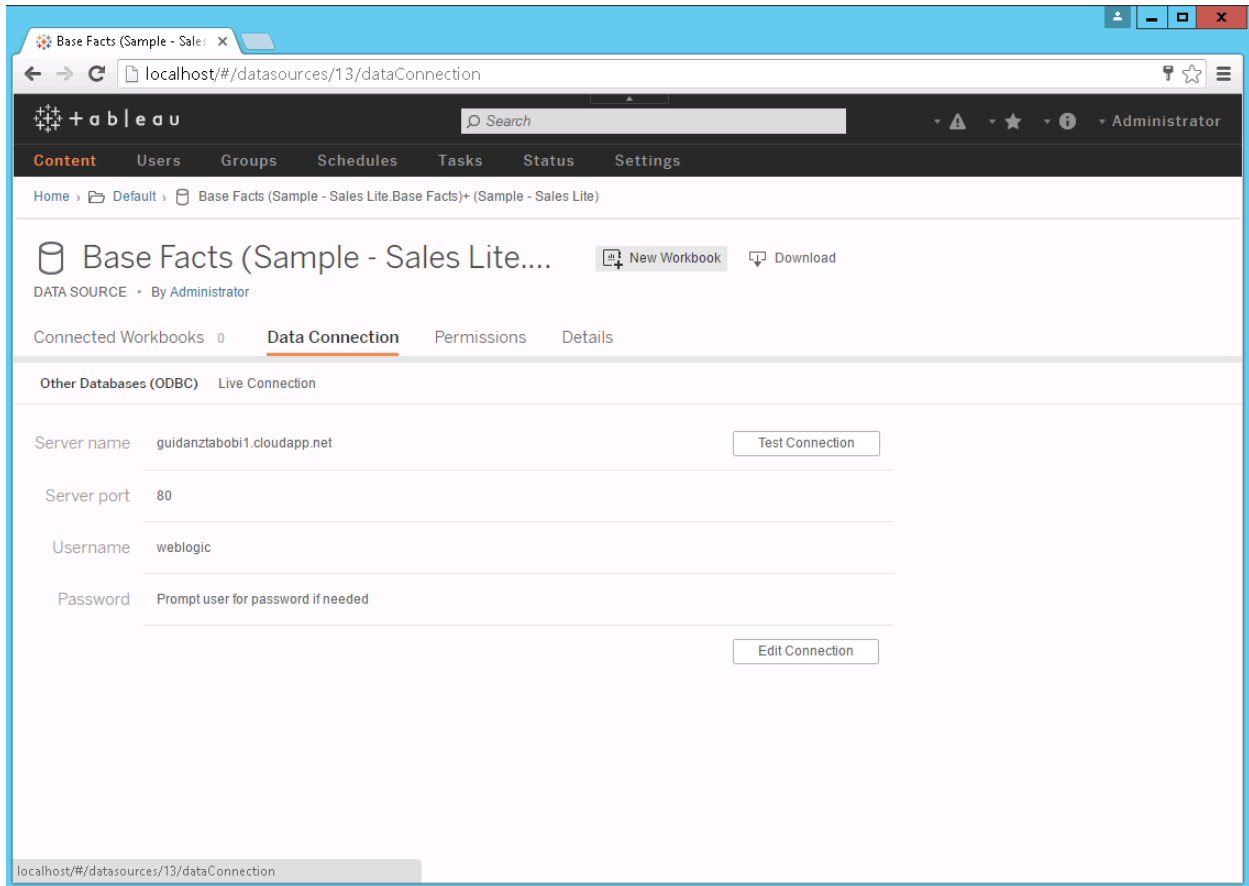


Figure 5 Notice the Prompt user for password option in the published data connection

When another user connects to a worksheet with this data source it will always ask their OBIEE username and password. The user will only see the data that she is authorized to view.

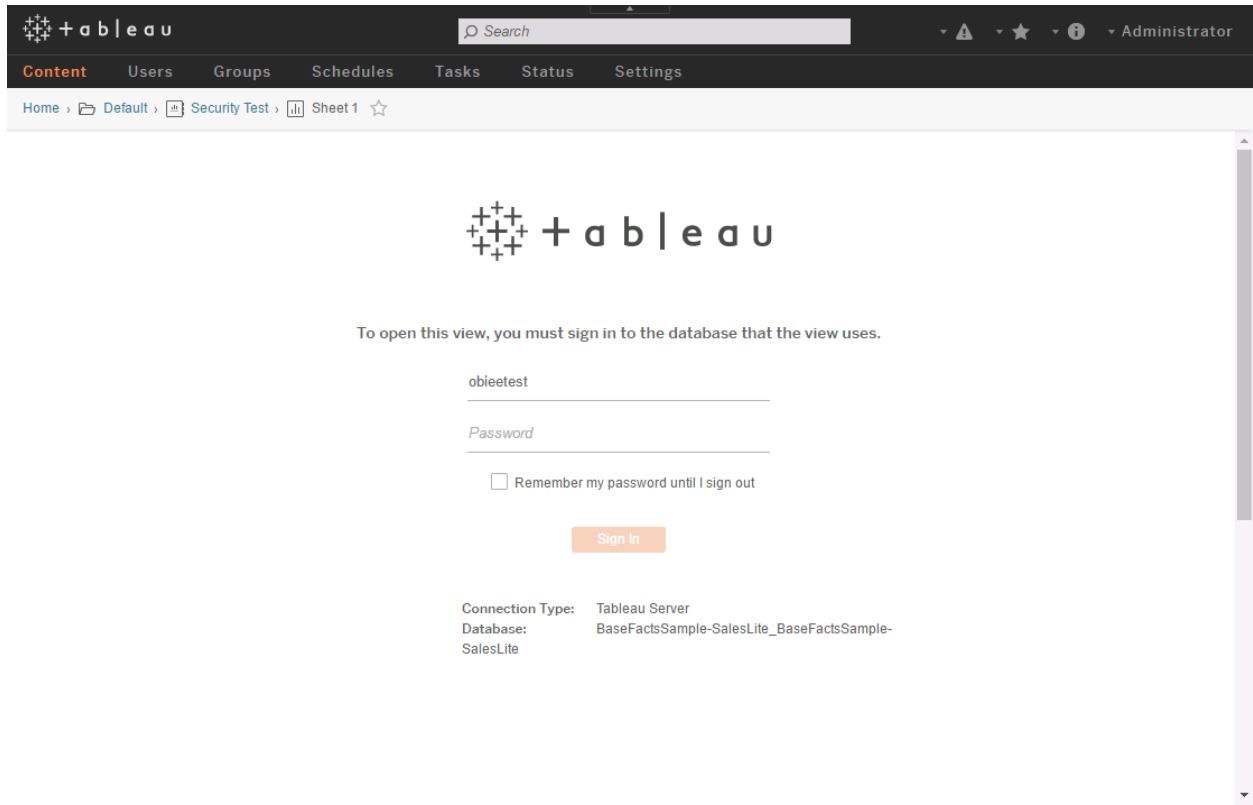


Figure 6 OBIEE username and password is requested when user connects to worksheet on Tableau server

## Extract Scenario

If you need the data source to be regularly extracted and refreshed incrementally from OBIEE then the OBIEE username and password needs to be embedded in the server data connection.

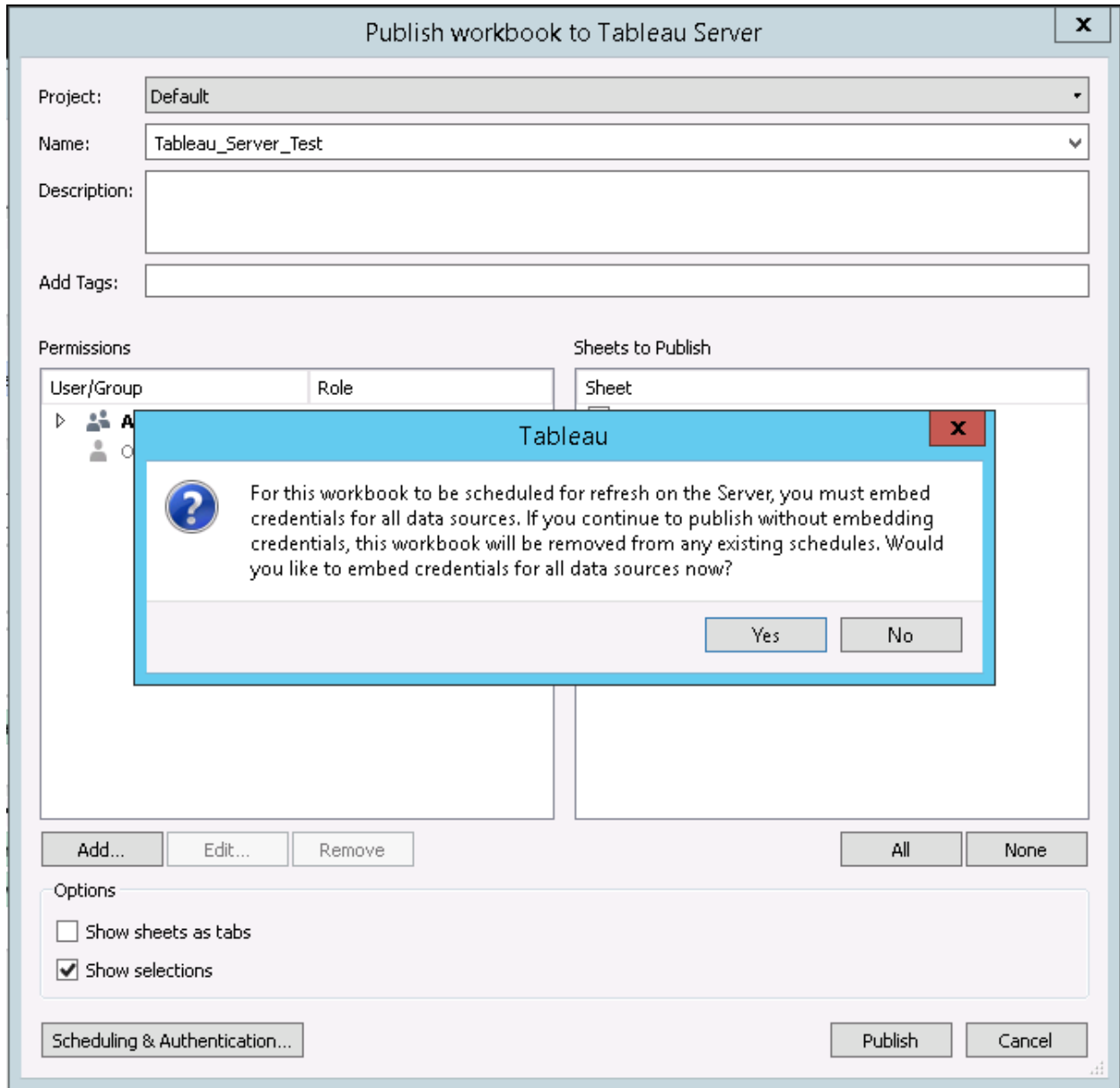


Figure 7 For automated data refresh from OBIEE, password needs to be embedded in the data connection

## Conclusion

In this whitepaper we reviewed the data security considerations while connecting from Tableau Desktop and Tableau Server to OBIEE data sources using the live connection and data extract options. BI Connector ensures that OBIEE data security rules are strictly followed when a user connects from Tableau to OBIEE. By using BI Connector, organizations can now get a jump start in meeting the business demand for modern visualization and self-service capability for OBIEE data while reusing their investment in OBIEE based enterprise data security model.



## Recommended Next Steps

If you haven't tried BI Connector yet, [download a free trial](#).

## Resources to learn more

1. [BI Connector Website](#)
2. [BI Connector – How it works](#)
3. [14 Day Free Trial of BI Connector](#)
4. [Read the BI Connector blog](#) for the latest update on BI Connector
5. [Contact us](#) with your questions and feedback.