Edit Assessments

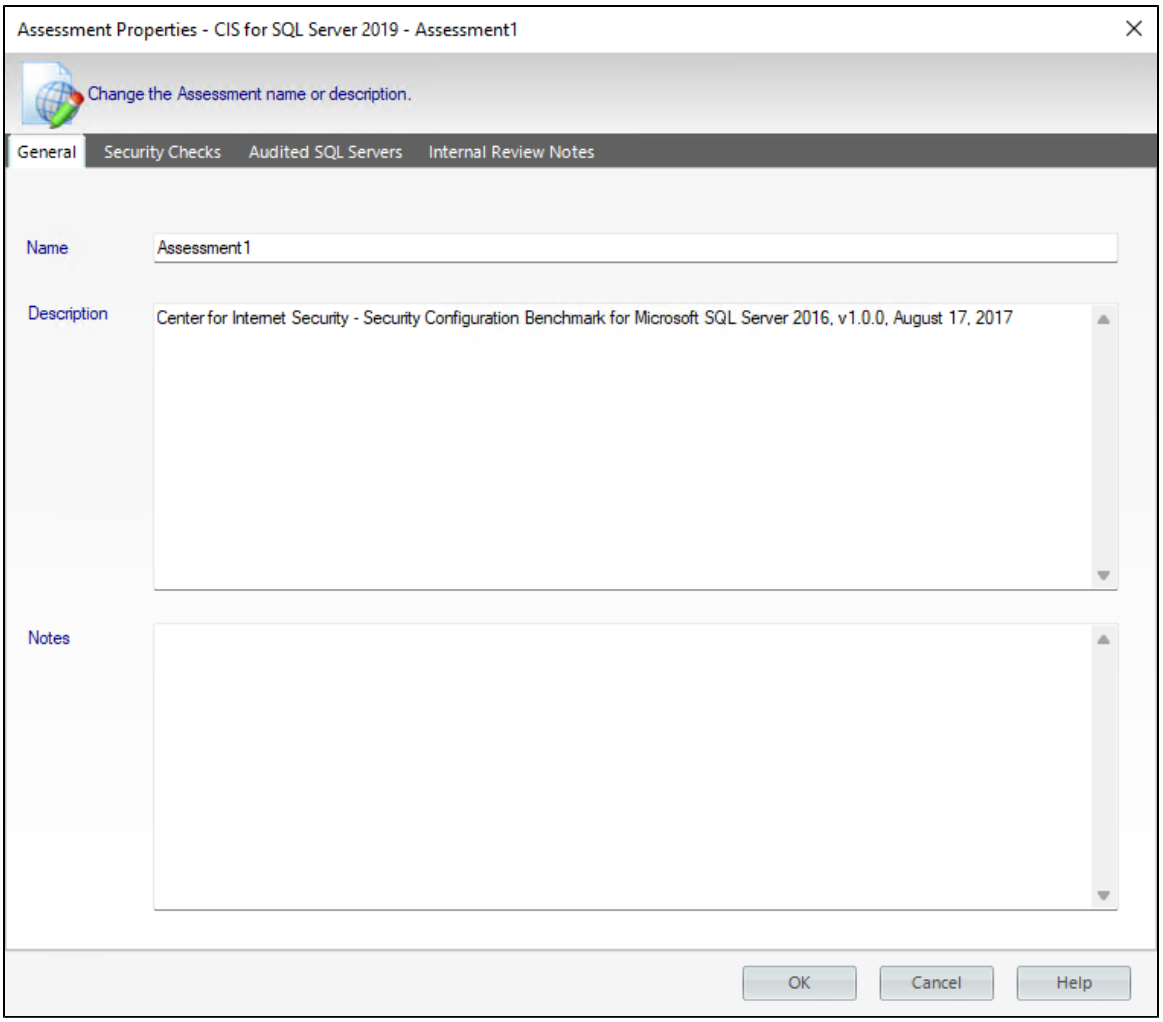
Edit the settings of your assessment by using the **Assessment Properties** window to change basic properties or how the assessment performs its security evaluation.

To access this window, click the respective assessment or policy on the Policies tree of the **Security Summary** view, then select **Edit Settings** fr om the ribbon options. You can also right-click the assessment and select **Properties** to access the same window.

You can edit in the following tabs:

General

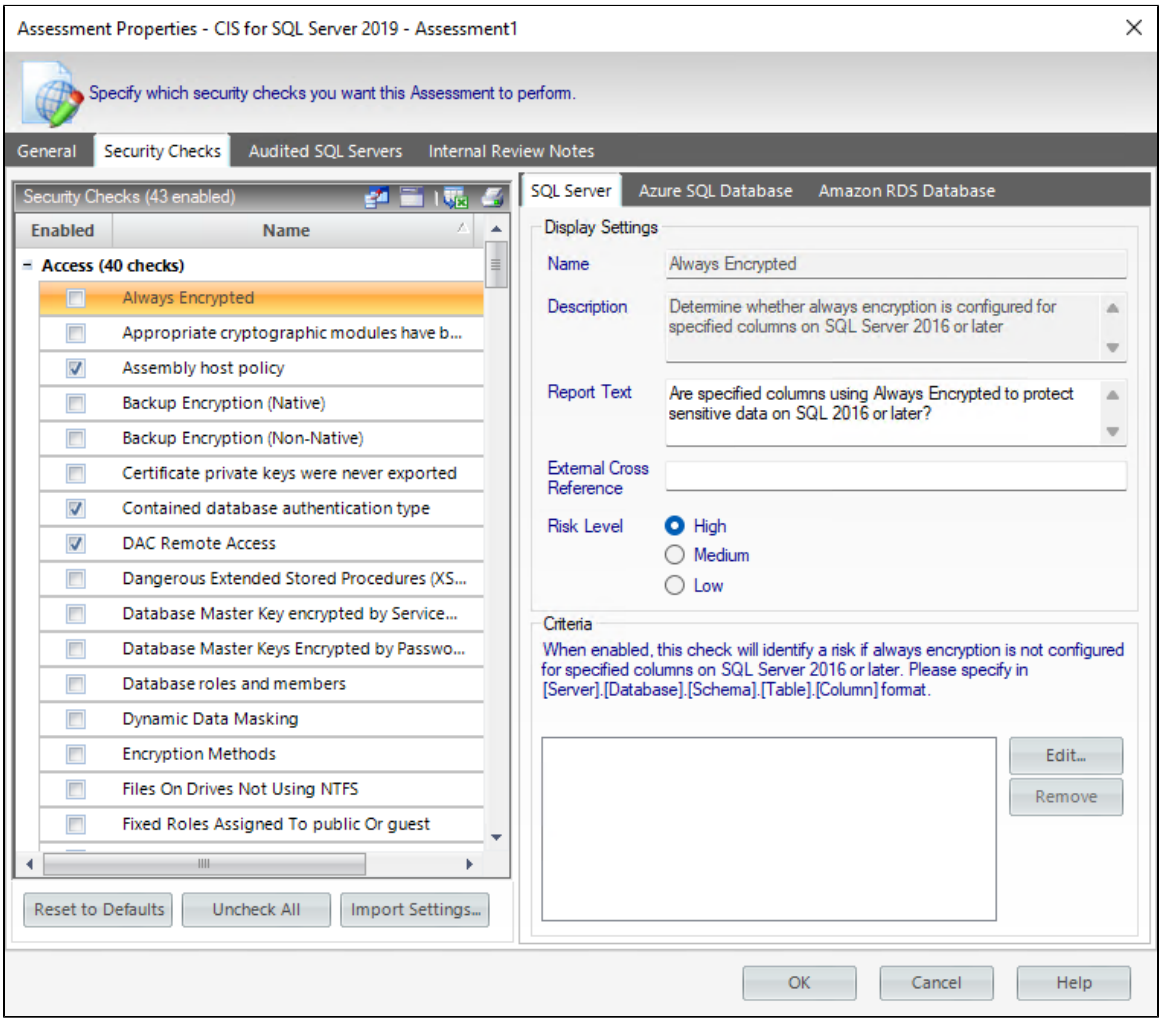
The **General** tab of the **Assessment Properties** window allows you to update the name and description of the selected assessment as well as any notes you want to provide.



The **Notes** field allows you to enter notes, questions, and other information about this assessment. Use these notes as a "cheat sheet" to remember details about your environment or security assessment from one audit to another. This approach ensures you gather all the data you need.

Security Checks

Security checks assess the vulnerability of specific Windows OS and SQL Server objects based on your criteria. The security checks performed by the selected assessment were copied from the policy associated with this assessment. You can modify the criteria of these checks to better fit your auditing needs for this assessment. Changes made to the assessment security checks will not affect the associated policy.



Available fields

You can update the following fields for SQL Server or Azure SQL Databases:

Report Text

The text entered in this field appears on your policy reports. For example, the Protocols security check includes the report text "Are unexpected Protocols enabled?". When unexpected protocols are enabled, the report displays the SQL Server instances where the risk is encountered.

External Cross Reference

Allows you to cross reference a security vulnerability included in your report to a number or label contained in an external policy, industry standard, or government regulation.

Risk Level

Allows you to set the severity of the risk posed by this finding. The risk level is important because it reflects how severe or risky a particular security finding is for your environment, allowing you to further customize security checks to meet your exact auditing needs. For example, finding an enabled Guest account on one instance may be a high risk, but on another instance it may be a low risk. The risk level also determines where the corresponding security finding appears on the policy or assessment Report Card and whether or not email notifications will be sent.

Criteria

Some security checks allow you to enter criteria the policy will check for, such as specific user accounts, stored procedures, or the login audit level. Text entered into these fields must be the exact spelling of the object or user being checked.

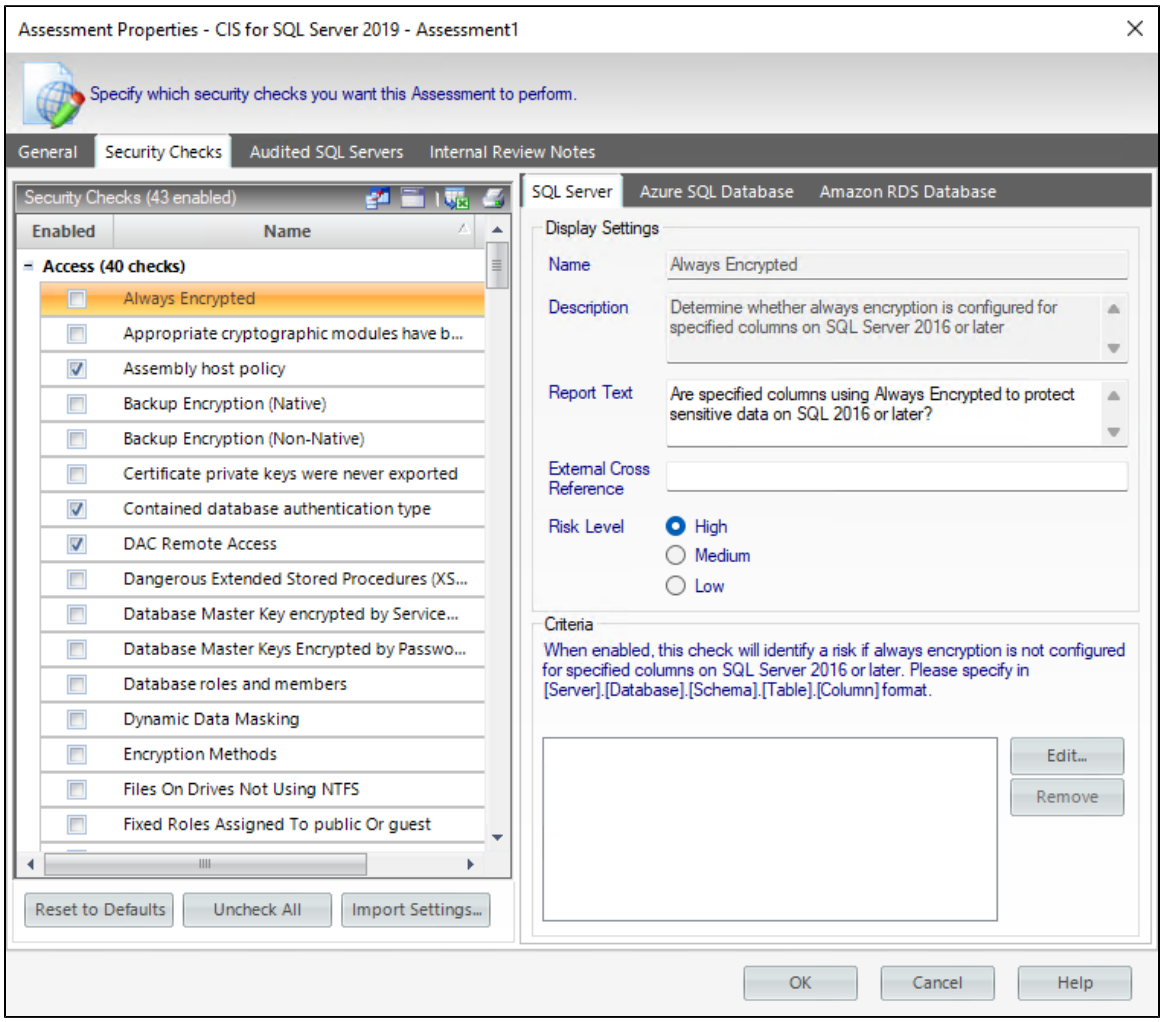
If the criteria for any given security check is entered incorrectly, the risk will appear in the Security Report Card. Select the risk and you can see the correct criteria names in the Details section. Open the Policy details window and enter the correct name on the Security Checks tab.

Some security check criteria support using the percent wildcard character (%) to specify objects whose names apply a naming convention. For example, to specify all users whose logon starts with sql, enter the following syntax: `domain\sql%`.

Any criteria you introduce, you can changed it with the option **Edit**, or delete it by using **Remove**.

Audited SQL Servers

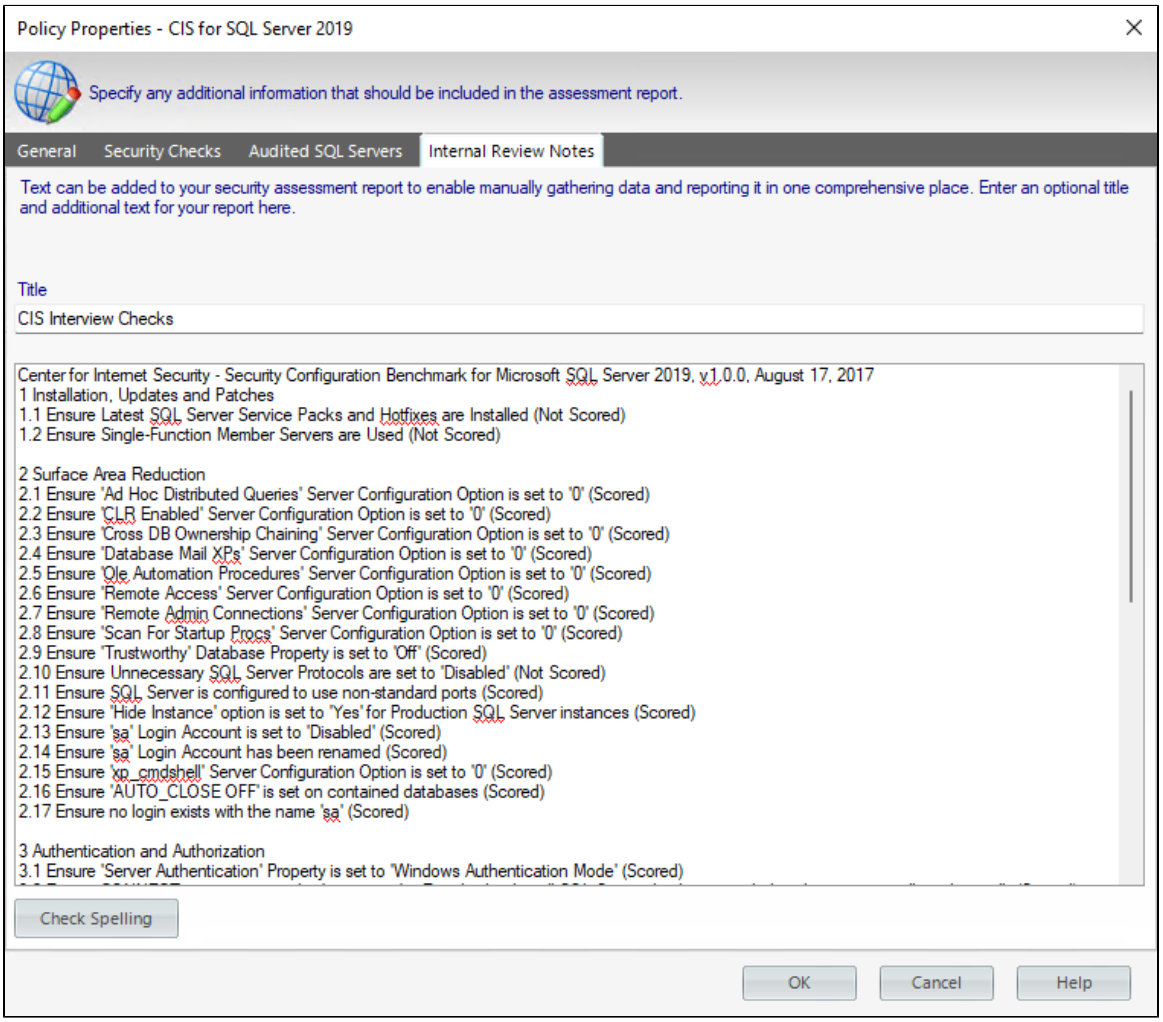
The **Audited SQL Servers** tab allows you to change which registered SQL Server instances are assigned to this assessment within IDERA SQL Secure. You can add or remove instances from this assessment to better match your current auditing needs. Each registered SQL Server instance can belong to multiple assessments.



Edit the instance list, and then click **OK**. SQL Secure automatically re-runs the assessment based on this new scope.

Internal Review Notes

The **Internal Review Notes** tab allows you to edit the manually-collected data applied to your assessment. Manually-collected data is security information that cannot be gathered and assessed through IDERA SQL Secure.



SQL Secure adds your **Internal Review Notes** to the Risk Assessment report, providing a fuller picture of your assessment status. These notes can also serve as a questionnaire to be used for manually gathering additional data that may be required in your assessment.

To edit these notes, click inside the provided text box and enter your changes.