

# 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** from 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.

Assessment Properties - CIS for SQL Server 2019 - Assessment1

Change the Assessment name or description.

General Security Checks Audited SQL Servers Internal Review Notes

Name: Assessment1

Description: Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2016, v1.0.0, August 17, 2017

Notes

OK Cancel Help

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.

Assessment Properties - CIS for SQL Server 2019 - Assessment1

Specify which security checks you want this Assessment to perform.

General Security Checks Audited SQL Servers Internal Review Notes

Security Checks (43 enabled)

Enabled	Name
<input type="checkbox"/>	Always Encrypted
<input type="checkbox"/>	Appropriate cryptographic modules have b...
<input checked="" type="checkbox"/>	Assembly host policy
<input type="checkbox"/>	Backup Encryption (Native)
<input type="checkbox"/>	Backup Encryption (Non-Native)
<input type="checkbox"/>	Certificate private keys were never exported
<input checked="" type="checkbox"/>	Contained database authentication type
<input checked="" type="checkbox"/>	DAC Remote Access
<input type="checkbox"/>	Dangerous Extended Stored Procedures (XS...
<input type="checkbox"/>	Database Master Key encrypted by Service...
<input type="checkbox"/>	Database Master Keys Encrypted by Passwo...
<input type="checkbox"/>	Database roles and members
<input type="checkbox"/>	Dynamic Data Masking
<input type="checkbox"/>	Encryption Methods
<input type="checkbox"/>	Files On Drives Not Using NTFS
<input type="checkbox"/>	Fixed Roles Assigned To public Or guest

Reset to Defaults Uncheck All Import Settings...

SQL Server Azure SQL Database Amazon RDS Database

Display Settings

Name Always Encrypted

Description Determine whether always encryption is configured for specified columns on SQL Server 2016 or later

Report Text Are specified columns using Always Encrypted to protect sensitive data on SQL 2016 or later?

External Cross Reference

Risk Level ☒ High ☐ Medium ☐ Low

Criteria

When enabled, this check will identify a risk if always encryption is not configured for specified columns on SQL Server 2016 or later. Please specify in [Server].[Database].[Schema].[Table].[Column] format.

Edit... Remove

OK Cancel Help

## 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.

Assessment Properties - CIS for SQL Server 2019 - Assessment1

Specify which security checks you want this Assessment to perform.

General Security Checks Audited SQL Servers Internal Review Notes

Security Checks (43 enabled)

Enabled	Name
<b>Access (40 checks)</b>	
<input type="checkbox"/>	Always Encrypted
<input type="checkbox"/>	Appropriate cryptographic modules have b...
<input checked="" type="checkbox"/>	Assembly host policy
<input type="checkbox"/>	Backup Encryption (Native)
<input type="checkbox"/>	Backup Encryption (Non-Native)
<input type="checkbox"/>	Certificate private keys were never exported
<input checked="" type="checkbox"/>	Contained database authentication type
<input checked="" type="checkbox"/>	DAC Remote Access
<input type="checkbox"/>	Dangerous Extended Stored Procedures (XS...
<input type="checkbox"/>	Database Master Key encrypted by Service...
<input type="checkbox"/>	Database Master Keys Encrypted by Passwo...
<input type="checkbox"/>	Database roles and members
<input type="checkbox"/>	Dynamic Data Masking
<input type="checkbox"/>	Encryption Methods
<input type="checkbox"/>	Files On Drives Not Using NTFS
<input type="checkbox"/>	Fixed Roles Assigned To public Or guest

Reset to Defaults Uncheck All Import Settings...

SQL Server Azure SQL Database Amazon RDS Database

Display Settings

Name Always Encrypted

Description Determine whether always encryption is configured for specified columns on SQL Server 2016 or later

Report Text Are specified columns using Always Encrypted to protect sensitive data on SQL 2016 or later?

External Cross Reference

Risk Level ☒ High ☐ Medium ☐ Low

Criteria

When enabled, this check will identify a risk if always encryption is not configured for specified columns on SQL Server 2016 or later. Please specify in [Server].[Database].[Schema].[Table].[Column] format.

Edit... Remove

OK Cancel Help

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.

Policy Properties - CIS for SQL Server 2019

Specify any additional information that should be included in the assessment report.

General Security Checks Audited SQL Servers Internal Review Notes

Text can be added to your security assessment report to enable manually gathering data and reporting it in one comprehensive place. Enter an optional title and additional text for your report here.

Title

CIS Interview Checks

Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2019, v1.0.0, August 17, 2017

1 Installation, Updates and Patches

1.1 Ensure Latest SQL Server Service Packs and Hotfixes are Installed (Not Scored)

1.2 Ensure Single-Function Member Servers are Used (Not Scored)

2 Surface Area Reduction

2.1 Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0' (Scored)

2.2 Ensure 'CLR Enabled' Server Configuration Option is set to '0' (Scored)

2.3 Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0' (Scored)

2.4 Ensure 'Database Mail XPs' Server Configuration Option is set to '0' (Scored)

2.5 Ensure 'OLE Automation Procedures' Server Configuration Option is set to '0' (Scored)

2.6 Ensure 'Remote Access' Server Configuration Option is set to '0' (Scored)

2.7 Ensure 'Remote Admin Connections' Server Configuration Option is set to '0' (Scored)

2.8 Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0' (Scored)

2.9 Ensure 'Trustworthy' Database Property is set to 'Off' (Scored)

2.10 Ensure Unnecessary SQL Server Protocols are set to 'Disabled' (Not Scored)

2.11 Ensure SQL Server is configured to use non-standard ports (Scored)

2.12 Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances (Scored)

2.13 Ensure 'sa' Login Account is set to 'Disabled' (Scored)

2.14 Ensure 'sa' Login Account has been renamed (Scored)

2.15 Ensure 'xp\_cmdshell' Server Configuration Option is set to '0' (Scored)

2.16 Ensure 'AUTO\_CLOSE OFF' is set on contained databases (Scored)

2.17 Ensure no login exists with the name 'sa' (Scored)

3 Authentication and Authorization

3.1 Ensure 'Server Authentication' Property is set to 'Windows Authentication Mode' (Scored)

Check Spelling

OK Cancel Help

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.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)