

Working with approved assessments

Approved assessments accurately represent your security status at a specific point in time. An approved assessment represents the final step, or stage, in your audit process. Approved assessments typically contain your accepted and official security status in response to an audit. When you approve an assessment, it is automatically locked and set to approved mode.

Use the approved mode to safely archive the assessment, preserving your findings and explanation notes.

To approve assessments:

- The assessment must be published. Go to [Working with published assessments](#) for more information.
- Select your published assessment from the Policies tree of the **Security Summary** view and click **Approve** in the ribbon menu options of the **Summary** tab of your published assessment.



You can perform the following actions in the approve mode:

- Manually add or remove notes about an approved assessment by editing the **Notes** field on the assessment **Properties** window.
- Continue to use the **Change Log** tab to review activity that previously occurred on this assessment. However, no other changes are allowed.

Actions and Tasks for Approved Assessments

The following options are available in the **Summary** tab of a selected approved assessment:

CIS for SQL Server 2019 - Assessment11::WINDEV2204EVAL

Summary

Assessment Actions: Edit Settings, Refresh Audit Data, Publish, Save as New Assessment, Compare Assessments, Remove from Assessment

Security Check Actions: Configure Security Check, Edit Explanation Notes

Server Actions: Take a Snapshot

Server Status: 0 High Risk of 5, 2 Medium Risk of 8, 6 Low Risk of 30

Audit Data Selection: Use most current data as of 6/16/2022 11:18:40 AM

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

SQL Server Info: Server Name: WINDEV2204EVAL, Audit Data Collected: 6/15/2022 6:13:57 PM

Server Security Report Card: 43 Security Checks - 8 Risks (2 Mediums and 6 Lows)

Risk	Security Check	Findings
Medium Risk	SQL Server Service Login Account Not Acceptable	1 Medium Risk
Medium Risk	SQL Server Version	1 Medium Risk
Low Risk	Common TCP Port Used	1 Low Risk
Low Risk	Hide Instance Option is set	1 Low Risk
Low Risk	Maximum number of error log files	1 Low Risk
Low Risk	Remote Access	1 Low Risk
Low Risk	SQL Logins Not Using Password Expiration	1 Low Risk
Low Risk	SQL Server Agent Login Account Not Acceptable	1 Low Risk

Details: Explanation Notes

Security Check: SQL Server Audit is Configured for Logins (CIS 5.4)
SQL Server Audit is configured to record both failed and successful logins. This check is only valid for Enterprise Edition SQL Server 2008 R2 and above.

Risk Level: Medium

Findings: WINDEV2204EVAL (Explained) Does not have audit turned on to capture failed or successful logins.

View Assessment Settings

Allows you to view the configuration settings for an approved assessment, such as the security checks performed by the assessment.

Save as New Assessment

Allows you to create a new assessment that uses the same settings and audit data as the selected assessment. When you save a new assessment, SQL Secure lists the assessment in the **Draft Assessment** folder under the associated policy in the Policies tree.

Compare Assessments

Allows you to compare the findings and settings of an approved assessment against another saved assessment or the original policy. You can compare different types of assessments (draft, published, or approved). When you compare this assessment against the original policy from which it was saved, you can identify changes that have occurred since the assessment had been saved.

