

# 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 2000 - Assessment 1::CH-SP2010**

**Summary** | Change Log

View Settings | Refresh Audit Data | Save as New Assessment | Compare Assessments | Remove from Assessment | Configure Security Check | Edit Explanation Notes

**Server Status**

1 High Risk of 3  
0 Medium Risk of 3  
7 Low Risk of 27

**Audit Data Selection:**  
Use most current data as of 8/29/2018 9:33:38 AM

**Description:**  
Center for Internet Security - Benchmark for Microsoft SQL Server 2000, V 1.0, December, 2005

**SQL Server Info**

**Server Name:**  
CH-SP2010

**Audit Data Collected:**  
8/29/2018 6:47:23 AM

**Version:**  
SQL Server 2012 v11.0.5058.0

**Edition:**  
Enterprise Edition (64-bit)

**Windows OS:**  
Microsoft Windows Server 2012 R2 Datacenter

**Server Security Report Card**

33 Security Checks - 8 Risks (1 High and 7 Lows)

**Risk** | **Security Check** | **Findings**

Risk	Security Check	Findings
High	Public Database Role Has Permissions	1 High Risk
Low	Analysis Services Running	1 Low Risk
Low	Common TCP Port Used	1 Low Risk
Low	Dangerous Extended Stored Procedures (XSPs)	1 Low Risk
Low	Integration Services Running	1 Low Risk
Low	Remote Access	1 Low Risk
Low	SQL Server Version	1 Low Risk
Low	Stored Procedures Encrypted	1 Low Risk
OK	Agent Job Execution	OK
OK	Audit Data Is Stale	OK
OK	Blank Passwords	OK
OK	BUILTIN/Administrators Is sysadmin	OK
OK	Cross Database Ownership Chaining Enabled	OK
OK	Files On Drives Not Using NTFS	OK
OK	Fixed Roles Assigned To public Or guest	OK
OK	Guest User Enabled	OK
OK	Integration Services	OK

**Details** | Explanation Notes

**Security Check: Public Database Role Has Permissions**  
Determine whether the public database role has any permissions

**Risk Level:** High

Server is vulnerable if the public role has been granted any permissions or is a role member.

**Findings:**  
CH-SP2010 Public has permissions on 'master', 'model', 'msdb', 'ReportServer', 'ReportServerTempDB', 'SQLSecure', 'tempdb'

### 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.

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