White Paper

Symantec™ Control Compliance Suite

Enforce Database Compliance and Eliminate Drift

Table of Contents

Data Breach Risk Persists

A cursory review of recent data breaches drives home the importance of vigilant data security practices. In 2019 alone more than 4,000 data breach incidents were recorded, and the count continues to increase with every passing year. Data breaches are among the top five common types of cybercrimes in the world. Mega-breaches grab headlines, but hundreds of less familiar data hacks can also increase the risk to an organization.

Data breaches have run at a record pace. Consider these statistics from the first half of 2019:

- **3,800:** The number of publicly disclosed breaches.
- **4.1 billion:** The number of records exposed.
- **+54%:** The increase in number of reported breaches versus the first six months of 2018.

Databases are one of the most critical assets of an organization's IT infrastructure and contain a treasure trove of valuable data—often highly sensitive personally identifiable information (PII). They also are an important area of emphasis for compliance programs. Non-compliance with the General Data Protection Regulation (GDPR), even in the absence of any data breach, can be very expensive. Fines for non-compliance can reach up to €20 million in case of an undertaking, and up to 4% of the total worldwide annual turnover of the preceding year, whichever is higher.

As the list of government and industry regulations grows, compliance pressure intensifies on the data stored in corporate databases. With increasing pressure to comply with these regulations, compliance is becoming a significant challenge for database administrators and security practitioners. Data professionals must be more vigilant in protecting company data, as well as monitoring and ensuring that sufficient protection is in place.

Most enterprise core database environments like Microsoft SQL Server and Oracle have the ability to be appropriately provisioned, hardened, secured, and locked down when conducting an initial installation. The challenge is understanding the important components that must be in place. It is not just the database itself; it is the server, the operating system, and the database that reside on it.

Security practitioners must ensure that the basic security practices listed on the following page are followed within an organization to secure databases from data breach and access by unauthorized individuals.

- Ensure the security configuration settings of assets comply with published security standards (Gold Standard) and industry best practices.
- Identify which network devices, servers, and databases are missing critical patch updates and have known default configuration settings and make the appropriate changes.

Data Breach Risk Persists (cont.)

- Ensure a continuous assessment to ensure compliance with your IT security policy and any drift to that policy is addressed on priority.
- Encrypt all sensitive, customer, and internal data with AES. Encrypt all communication links with SSLv3 or TLS.
- Ensure only authorized persons have access to the database and with appropriate access privileges.
- Segregation of duties – Ensure that the person in charge of monitoring or auditing the database is not the same whose actions are being monitored.
- Monitoring privileged users – Since these users have higher access privileges, special attention may be required on their actions (for database administrators, system administrators, and developers, as examples).

Symantec Control Compliance Suite

Symantec provides solutions that allow organizations to track the implementation of the practices listed above. Symantec Control Compliance Suite (CCS) is a modular, highly scalable solution to help identify security gaps and vulnerabilities and automate compliance assessments for over 100 regulations, mandates, and best-practice frameworks including GDPR, HIPAA, NIST, PCI, and SWIFT. Symantec CCS rapidly discovers and inventories all networks and assets including managed and unmanaged devices—allowing for assets to be profiled and ranked for risk potential. The solution also provides role-based, customizable web-based dashboards and reports to measure risk and provide a unified view of security and compliance. With CCS, organizations can improve their security posture, prioritize remediation, and reduce risk.

Symantec CCS Standards Manager delivers asset auto-discovery across network devices, servers, and databases and assesses the security configuration of these assets. Organizations employ Symantec CCS Standards Manager to discover and identify rogue and misconfigured assets, detect configuration drifts, and evaluate if systems are secured, configured, and patched according to customer security standards. These services help the customers achieve the following:

- Automatically discover network devices, servers, and databases across the physical and virtual data center.
- Leverage out-of-the-box templates to map policies, security frameworks, and standards to control statements.
- Automate the collection, aggregation, and normalization of technical security scans across a broad range of physical and virtual assets.
- Identify rogue and misconfigured assets.
- Identify which network devices, servers, and databases are missing critical patch updates and have known default configuration settings.
- Assess that the security configuration settings of assets comply with published security standards and best practices.
- Take advantage of robust asset management and exception management workflows to customize security scans in support of the organization's operational requirements and internal security frameworks.
- Use evidence data from technical, procedural, and third-party security controls assessments to deliver role-based, operational, and mandate-based reports.

Symantec CCS for Databases

Symantec CCS provides the most comprehensive coverage of database platforms for compliance scanning. It focuses on key security areas; regulatory compliance, pre-defined standards based on CIS Benchmarks, and a known set of configuration gotchas, including areas related to storage cost savings. The list below is a representation of controls that CCS supports, but by no means is it an exhaustive list of controls that CCS supports out of the box. In addition to the pre-built standards, one can also create custom controls or extend existing controls using the highly flexible framework provided by CCS out of the box.

- Entitlement (relevant for PCI, SOX):
  - Who has access to the grant/revoke/modify functions?
  - Who has direct access to the underlying data (versus using front-end application)?
- Security (CIS Benchmarks):
  - Is auditing/logging enabled and configured?
  - Is backup enabled and configured correctly? (Restore data after ransomware)
  - Are underlying database files adequately protected? (Oracle Configuration Files)
- Configuration:
  - Extraneous/unneeded services are disabled?
  - Are the communications limited and protected? (Database Denial of Service attacks)
- Potential storage cost savings:
  - Are database samples removed?
  - Are database files stored on the correct data volumes?

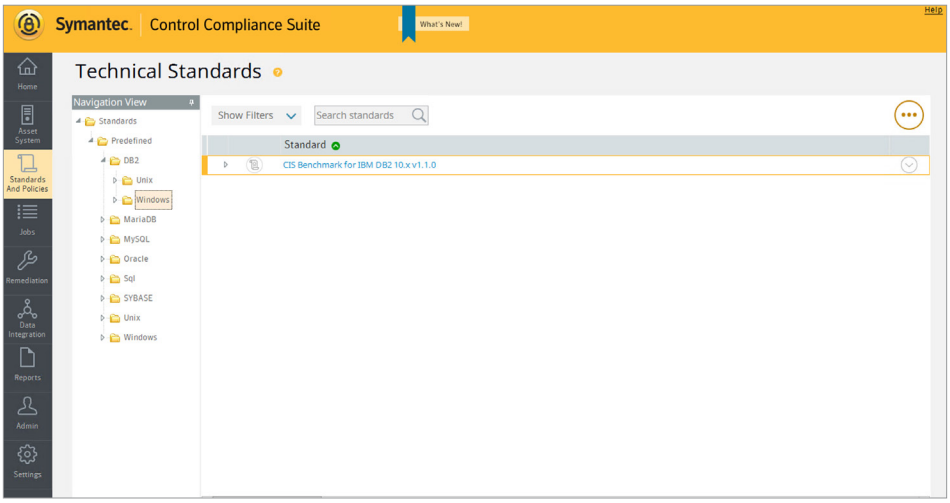
British Computer Society Top Ten: Database Attack Areas

The table below illustrates coverage of CCS controls across common risk areas.

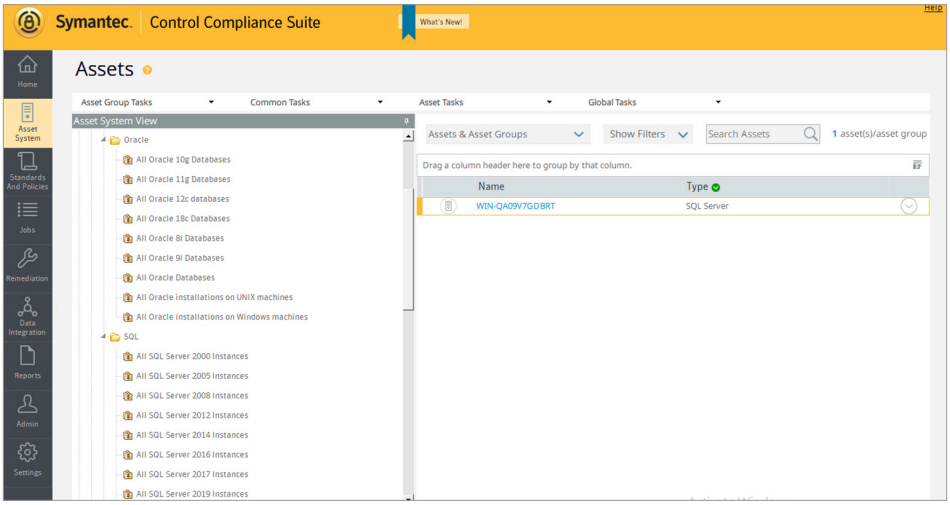
	CCS for DBs: Key Areas of Control		
Critical Areas	Regulatory	CIS Benchmarks	Configuration
1. Excessive Privileges	●	●	●
2. Unauthorized Privilege Elevation	●	●	
3. Platform Vulnerabilities			●
4. SQL Injections		●	●
5. Exploiting Unnecessary Services (and functionality)			●
6. Weak Audit		●	●
7. Denial of Service		●	●
8. Database Protocol Vulnerabilities			●
9. Weak Authentication (brute-force attacks)	●	●	●
10. Exposure of Backup Data		●	●

Common CCS Console Views and Details

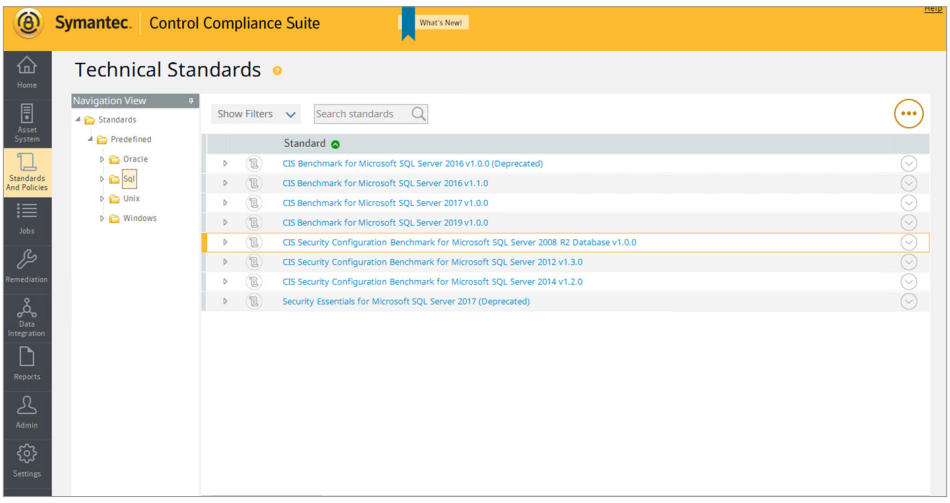
CCS Console View of Support for Different Databases: A snapshot of different database assets that can be scanned by CCS for compliance.



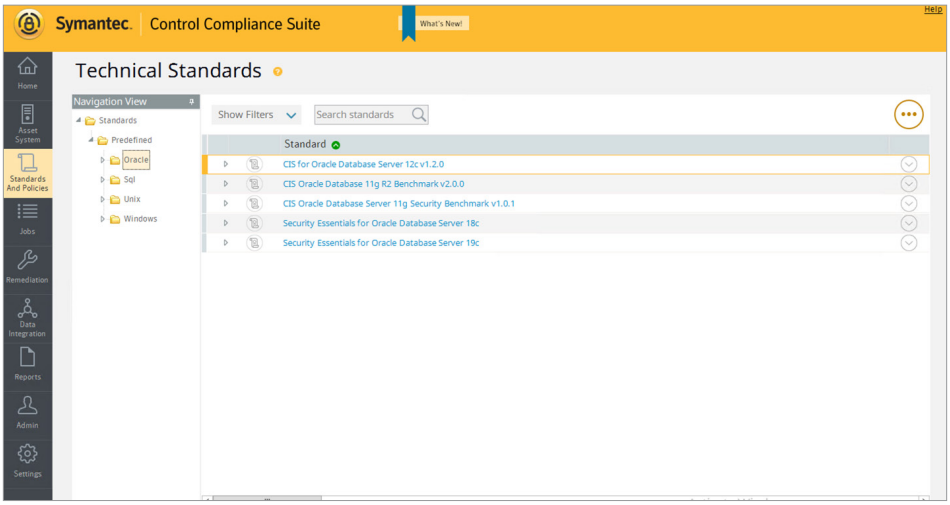
CCS Console View of Asset Groups: A snapshot of different versions of supported Oracle and SQL Server assets that can be scanned by CCS for compliance.



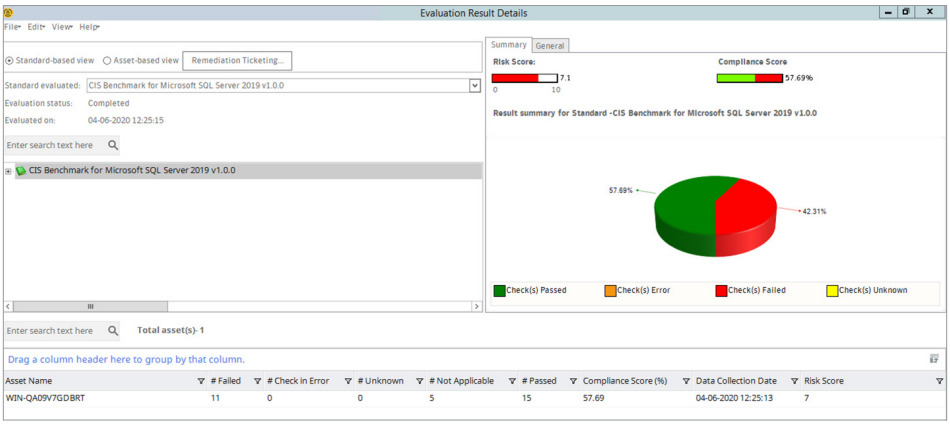
CCS Console View of Pre-Defined Microsoft SQL Database Standards: A snapshot of SQL Server CIS Benchmarks supported by CCS for compliance scanning.



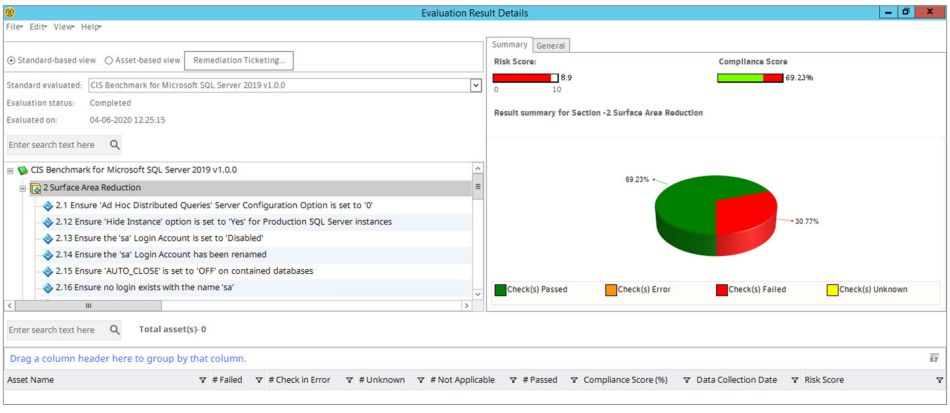
CCS Console View of Pre-Defined Microsoft Oracle Database Standards: A snapshot of Oracle database server CIS Benchmarks supported by CCS for compliance scanning.



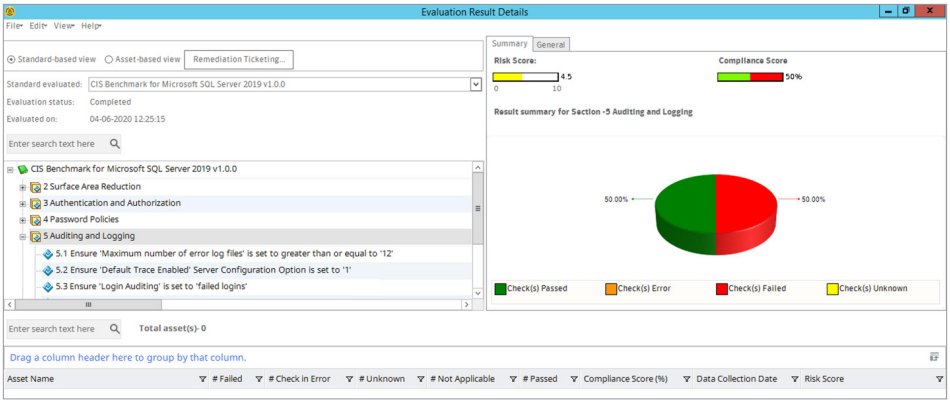
Evaluation Result Details (Overall Score): A summary of the overall risk score and compliance score along with Asset and other details against a CIS Benchmarks for SQL Server.



Evaluation Result Details (Surface Area Score): A drill-down into each section within the CIS benchmark for the overall risk score and compliance score along with Asset and other details.

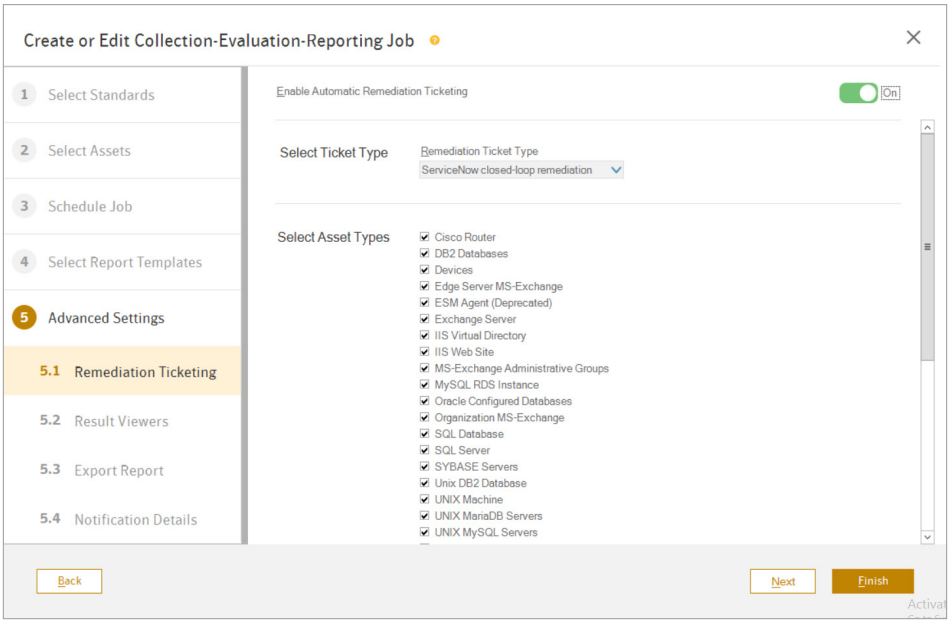


Evaluation Result Details (Auditing and Logging Score): A drill-down into each section within the CIS benchmark for an overall risk score and compliance score along with Asset and other details.

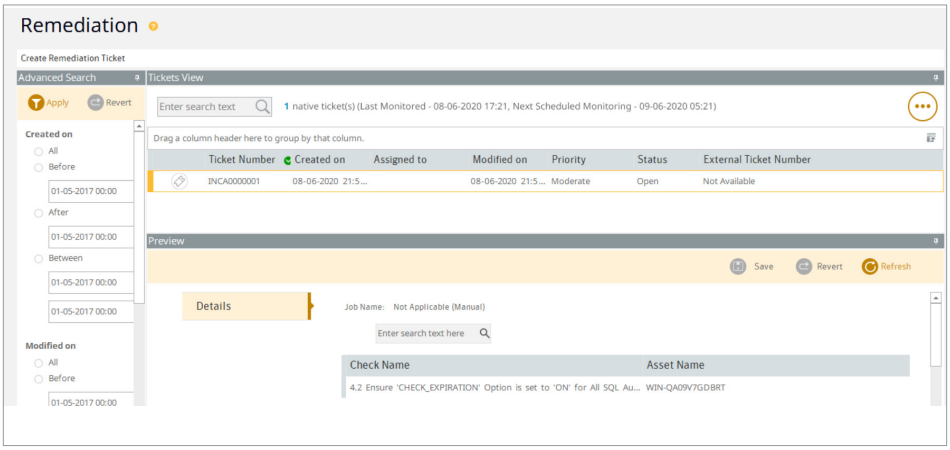


Integrated Remediation Tracking Through Third-Party Ticketing System: An automated ticket based on the assessment results can also be created using CCS in a third-party ticketing system and tracked in the CCS console. A workflow is provided to configure the integration with a third-party ticketing system.

CCS Console View for Configuring Automated Ticket Creation: A view of the steps and workflow for integration with third-party ticketing systems.



CCS Console View for Tracking the Ticket Status: A view of the CCS console that is used to track the status of the automated tickets created by CCS.



Synopsis

Symantec CCS offers the leading market solution for database security and compliance. It covers the entire lifecycle: from scanning the database for potential misconfiguration and drift from well-defined policies and CIS benchmarks to closing the loop with tracking the progress of remediation through integration with third-party systems. CCS offers comprehensive coverage of various database platforms that is continuously updated with the latest security controls from CIS and, combined with other security solutions from Symantec, ensures that critical data is protected from unauthorized access by malicious actors. Learn more.

SED-DCCCS-WP100 July 15, 2020