SQL Server Security Benchmark [2.0.0.0]

CSDEMO-SQL-AG01

Company Confidential

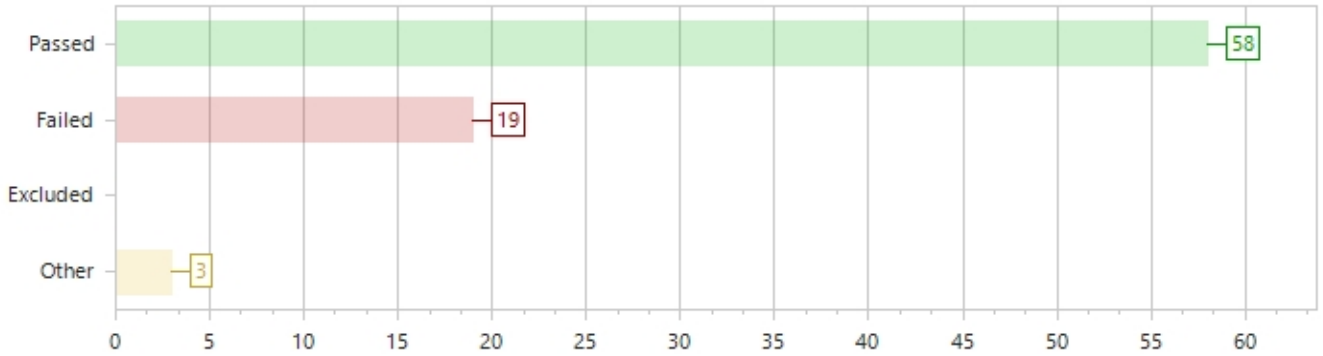
Document Properties

Author	CENTREL-WS01\XiaConfigurationDemo
Product	XIA Configuration Server [18.1.2.0]
Date	Wednesday, July 1, 2026 9:04:16 AM
Version	1.02

Table of Contents

SQL Server Security Benchmark [2.0.0.0]

The SQL Server Security Benchmark is a built-in compliance benchmark that evaluates and compares the security-related configuration of on-premises SQL Server instances and Azure SQL Managed Instances.



Section 1: Host Platform

The checks in this section verify that the host is running a supported server-grade operating system, is not performing conflicting roles.
These controls align with industry guidance such as Microsoft's security considerations for a SQL Server installation.

5 Benchmark Results

Ref.	Title	Configured Value
1.01	Ensure that the host is running a server operating system.	Microsoft Windows Server 2025 Datacenter
1.02	Ensure that the host is not a domain controller.	False
1.03	Ensure that the host operating system is at least "Windows Server 2019" (10.0.17763.0).	Microsoft Windows Server 2025 Datacenter
1.04	Ensure the host is used exclusively for SQL Server and is not running other server roles.	SQL Instance
1.05	Ensure the host has no pending reboots.	False

Section 2: SQL Server Service

The checks in this section verify that the SQL Server service is configured with an appropriate least-privilege service account, and that service-level logging and encryption settings are correctly applied.
These controls align with industry guidance such as Microsoft's SQL Server Security Best Practices.

14 Benchmark Results

Ref.	Title	Configured Value
2.01	Ensure that the SQL Server service is configured to use a Virtual Service or Managed Service Account.	User Account (CSDEMO\SqlServices)
2.02	Ensure that SQL Server Customer Feedback (CEIP) is disabled at the instance level.	Enabled
2.03	Ensure that the SQL Server "Error Reporting" setting is set to "Disabled".	Enabled
2.04	Ensure that the SQL Server "Dump Directory" is configured to a local drive path that is not located on the system drive.	C:\Program Files\Microsoft SQL Server\MSSQL17.MSSQLSERVER\MSSQL\LOG
2.05	Ensure that the SQL Server "Force Encryption" setting is set to "Yes".	No
2.06	Ensure that the SQL Server "Force Strict Encryption" setting is set to "Yes" on SQL Server 2022 and above.	No
2.07	Ensure that the SQL Server "Extended Protection" setting is set to "Required" on SQL Server 2008 R2 and above.	Off
2.08	Ensure that the SQL Server "Accepted NTLM SPNs" setting is set to correct values on SQL Server 2008 R2 and above.	
2.09	Ensure that the SQL Server is configured with a valid SSL/TLS certificate.	Certificate not specified
2.10	Ensure that the SQL Server Named Pipes protocol is "Disabled".	Disabled
2.11	Ensure that the SQL Server Shared Memory protocol is "Enabled".	Enabled
2.12	Ensure that the SQL Server TCP protocol is "Enabled".	Enabled
2.13	Ensure that the SQL Server TCP protocol is configured to use only static ports.	1433

⊗	2.14	Ensure that the SQL Server TCP protocol is configured to use a static port other than the default of "1433".	1433

Section 3: SQL Server Agent Service

The checks in this section verify that the SQL Server Agent service is configured with an appropriate least-privilege service account.

1 Benchmark Results

Ref.	Title	Configured Value
3.01	Ensure that the SQL Server Agent service is configured to use a Virtual Service Account or Managed Service Account.	User Account (CSDEMO\SqlServices)

Section 4: SQL Server Full-Text Search Service

The checks in this section verify that the SQL Server Full-Text Search service is configured with an appropriate least-privilege service account.

1 Benchmark Results

Ref.	Title	Configured Value
4.01	Ensure that the SQL Server Full-Text Search service is configured to use a Virtual Service Account or Managed Service Account.	Not Installed

Section 5: SQL Server Browser Service

The checks in this section verify that the SQL Server Browser service is configured securely and only enabled when required. SQL Server Browser exposes instance and port information to clients, and therefore should remain disabled unless named instances or dynamic ports are in use. When enabled, it must run under a least-privilege identity.

3 Benchmark Results

Ref.	Title	Configured Value
5.01	Ensure that the SQL Server Browser service is disabled if not required or only the default instance is configured.	Disabled
5.02	Ensure that the SQL Server Browser service is configured to use the LocalService account or a Virtual Service Account.	Disabled
5.03	Ensure that "Hide Instance" is set to "True" for SQL Server instances.	Browser Service Disabled

Section 6: SQL Server Telemetry (CEIP) Service

The checks in this section verify that the SQL Server Telemetry (CEIP) service is disabled. This service collects diagnostic and usage data and sends it to Microsoft as part of the Customer Experience Improvement Program. It should be disabled in security-sensitive environments to minimize data exposure.

1 Benchmark Results

Ref.	Title	Configured Value
6.01	Ensure that the SQL Server Telemetry (CEIP) service is disabled or not installed.	Enabled

Section 7: SQL Server Platform

The checks in this section verify that the SQL Server version and edition are supported and appropriate for production use. Running an unsupported or deprecated SQL Server release introduces security, stability, and compliance risks, while unsupported editions such as Evaluation or Express may impose functional or licensing limitations. These controls ensure the platform meets minimum version requirements and aligns with Microsoft's support lifecycle and best-practice guidance.

4 Benchmark Results

Ref.	Title	Configured Value
7.01	Ensure the SQL Server instance is version "SQL Server 2019" (15.0.0.0) or newer.	Microsoft SQL Server 2025 (17.0.1115.1)
7.02	Ensure the SQL Server is not running an evaluation edition.	Enterprise Developer Edition (64-bit)
7.03	Ensure the SQL Server is not running Express edition.	Enterprise Developer Edition (64-bit)
7.04	Ensure the SQL Server is not running a developer edition.	Enterprise Developer Edition (64-bit)

Section 8: Surface Area Configuration

The checks in this section verify that high-risk features such as xp_cmdshell, OLE Automation, CLR integration, Ad Hoc Distributed Queries, and other optional components are disabled unless explicitly required. This follows Microsoft's guidance on minimizing SQL Server's attack surface, as documented in Surface Area Configuration.

9 Benchmark Results

Ref.	Title	Configured Value
8.01	Ensure ad hoc remote queries are disabled if not required.	Disabled
8.02	Ensure CLR integration is disabled if not required.	Disabled
8.03	Ensure database mail is disabled if not required.	Disabled
8.04	Ensure OLE automation is disabled if not required.	Disabled
8.05	Ensure remote DAC (Dedicated Admin Connection) is disabled if not required.	Disabled
8.06	Ensure the service broker endpoint is disabled if not required.	Disabled
8.07	Ensure SOAP endpoints are disabled if not required.	Disabled
8.08	Ensure SQL mail is disabled if not required.	Disabled
8.09	Ensure XP CMD Shell is disabled if not required.	Disabled

Section 9: Authentication & Access Control

The checks in this section verify that authentication settings, login configuration, and server-level permissions are securely defined and follow least-privilege principles. This includes enforcing secure authentication modes, protecting privileged accounts, preventing weak or unmanaged credentials, and ensuring that only trusted principals hold elevated permissions or access paths. Together, these controls help maintain a hardened and well-governed SQL Server security boundary. These controls align with industry guidance such as Microsoft's SQL Server Security Best Practices.

13 Benchmark Results

Ref.	Title	Configured Value
9.01	Ensure that the server authentication mode is set to "Windows Authentication Mode".	Windows Authentication Mode
9.02	Rename the "sa" account.	sa
9.03	Disable the "sa" account.	True
9.04	Ensure no logins have a blank password.	
9.05	Ensure SQL logins enforce password policy.	
9.06	Ensure SQL logins enforce password expiration.	##MS_PolicyEventProcessingLogin## ##MS_PolicyTsqlExecutionLogin## sa
9.07	Ensure that no orphaned users exist in any database.	
9.08	Ensure that the 'CONTROL SERVER' permission is not granted to any logins except "##MS_PolicySigningCertificate##".	
9.09	Ensure that the 'public' server role has only the default permissions assigned.	CSDEMO-SQL-AG01 | VIEW ANY DATABASE (Grant) TSQL Default TCP | CONNECT (Grant) TSQL Default VIA | CONNECT (Grant) TSQL Local Machine | CONNECT (Grant) TSQL Named Pipes | CONNECT (Grant)

9.10	Ensure that no logins use built-in Windows groups.	
9.11	Ensure that no logins use local Windows groups.	
9.12	Ensure that only trusted accounts can execute the "sp_invoke_external_rest_endpoint" stored procedure on SQL Server 2022 or above.	public (master)
9.13	Ensure that only trusted accounts are members of the sysadmin role. (Manual Validation)	CSDEMO\Administrator CSDEMO\SQL Administrators NT SERVICE\MSSQLSERVER NT SERVICE\SQLSERVERAGENT NT SERVICE\SQLWriter NT SERVICE\Winmgmt sa

Section 10: Advanced Engine Configuration

The checks in this section verify advanced SQL Server engine configuration options that influence security boundaries, cross-database behaviour, and startup execution paths. These controls align with Microsoft's guidance on hardening SQL Server engine behaviour and restricting legacy or high-risk features.

4 Benchmark Results

Ref.	Title	Configured Value
10.01	Ensure that the "CLR Strict Security" setting is enabled on SQL Server 2017 and above.	Enabled
10.02	Ensure that the "Cross database ownership chaining" setting is disabled.	Disabled
10.03	Ensure that the "Allow remote connections to this server" setting is disabled.	Enabled
10.04	Ensure that the "Scan for Startup Sprocs" setting is set to "False".	False

Section 11: Auditing and Logging

The checks in this section verify that SQL Server's auditing and logging features are configured to capture essential security-relevant events while avoiding deprecated or high-overhead mechanisms. Together, these settings provide reliable forensic visibility and support effective operational monitoring.

6 Benchmark Results

Ref.	Title	Configured Value
11.01	Ensure that the "Login Auditing" setting is set to "Failed logins only".	Failed Logins Only
11.02	Ensure that the "Enable C2 audit tracing" setting is disabled.	Disabled
11.03	Ensure that the "Default Trace Enabled" setting is set to "True".	True
11.04	Ensure that the "Common Criteria Compliance" setting is set to "Disabled".	Disabled
11.05	Ensure that the "Maximum number of error log files" setting is set to 12 or greater.	System Default
11.06	Ensure that the "Maximum error log file size" setting is set to a value between 102,400 KB and 1,048,576 KB.	Unlimited

Section 12: Databases

The checks in this section verify the configuration and security baseline of individual user and system databases against Microsoft best practices and industry-standard hardening benchmarks.

13 Benchmark Results

Ref.	Title	Configured Value
12.01	Ensure that no databases except MSDB are configured with "Trustworthy" set to "True".	
12.02	Ensure that no databases are configured with "Auto Close" set to "True".	
12.03	Ensure that no user databases are configured with the built-in 'sa' account as the owner.	
12.04	Ensure that no user databases are configured with "Cross-database Ownership Chaining Enabled" set to "True".	
12.05	Ensure that no databases are configured as contained databases unless required.	
12.06	Ensure that all user databases are configured with a recovery model of "Full" except databases that match '*staging*, *test*'.	
12.07	Ensure that all user databases are configured with a compatibility level of "SQL Server 2019 (150)" or above.	
12.08	Ensure that no user databases are configured with "Auto Shrink" set to "True".	
12.09	Ensure that no user databases are configured with "Auto Create Statistics" set to "False".	
12.10	Ensure that no user databases are configured with "Auto Update Statistics" set to "False".	
12.11	Ensure that all user databases are configured with "Page Verify" set to "CHECKSUM".	
12.12	Ensure that no user databases grant the "Connect" permission to the "guest" user.	
12.13	Ensure that all user CLR assemblies use SAFE_ACCESS, or are signed when using EXTERNAL_ACCESS under CLR Strict Security.	

Section 13: Encryption

The checks in this section verify that databases and backups are protected with strong, modern encryption standards. This includes enforcing Transparent Data Encryption (TDE) for data at rest, validating Database Encryption Keys, symmetric keys, and asymmetric keys. Together, these controls ensure that sensitive data remains protected against unauthorized access, theft, or compromise.

6 Benchmark Results

Ref.	Title	Configured Value
13.01	Ensure that all user databases are encrypted at rest with TDE.	CSDEMODB01 (Encryption Not Enabled) CSDEMODB02 (Encryption Not Enabled) LocalDatabase01 (Encryption Not Enabled)
13.02	Ensure that all encrypted user databases have a valid Database Encryption Key (DEK).	
13.03	Ensure that all encrypted user databases use AES-256 as the encryption algorithm.	
13.04	Ensure that all user databases use symmetric key encryption algorithms set to AES-128 or higher.	
13.05	Ensure that all user databases use asymmetric keys of 2048 bits or greater.	
13.06	Ensure that all database backups are encrypted.	CSDEMODB01 CSDEMODB02

About XIA Configuration

XIA Configuration is an IT infrastructure audit and documentation tool that automates the process of collecting and documenting network configurations.