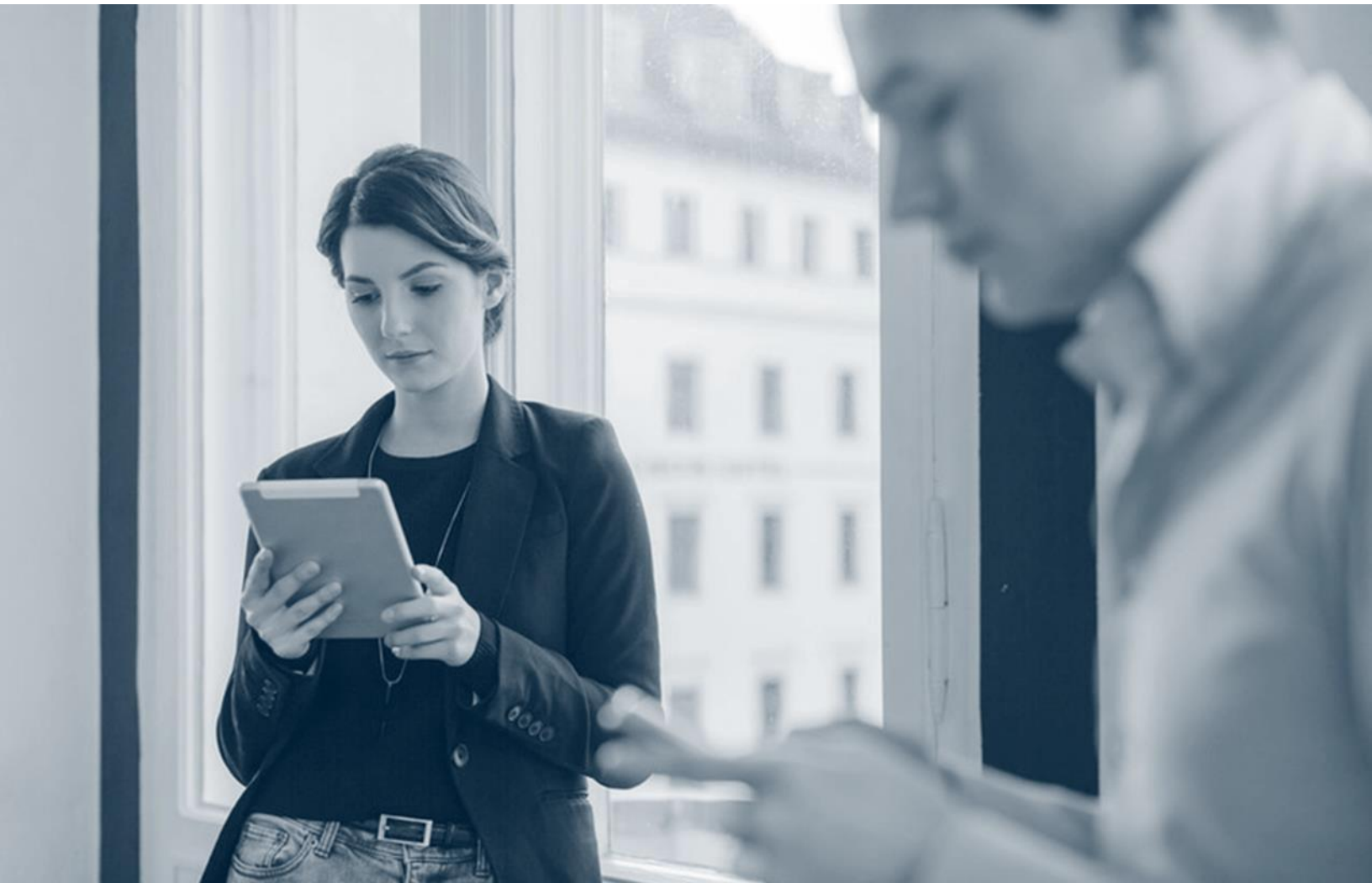




Commvault Compliance with CIS Level 1 Security Controls for the Database Deployed in a Windows Environment

CIS Microsoft SQL Server 2022 Benchmark v1.2.1

Friday, May 15, 2026



Commvault Compliance with the Level 1 Controls of CIS Microsoft SQL Server 2022 Benchmark v1.2.1 (Windows Environment)

The CIS Microsoft SQL Server 2022 Benchmark v1.2.1 provides prescriptive guidance for establishing a secure configuration posture to develop, deploy, assess, or secure solutions that incorporate Microsoft SQL Server 2022. The security controls in Level 1 provide a clear security benefit. The following table presents the compliance of the Commvault software with the Level 1 controls for Windows Environment.

Control		Support for the Control	Comments, if not supported
1	Installation, Updates and Patches		
1.1	Ensure Latest SQL Server Cumulative and Security Updates are Installed.	Yes	The latest version available for SQL server is installed during Commvault software installation.
1.2	Ensure Single-Function Member Servers are Used	Yes, requires manual configuration	The control is supported when required configurations are performed during the deployment of the Commvault software.
2	Surface Area Reduction		
2.1	Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'	Yes	
2.2	Ensure 'CLR Enabled' Server Configuration Option is set to '0'	Yes	The Commvault software allows only "safe CLR".
2.3	Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0'	Yes	
2.4	Ensure 'Database Mail XPs' Server Configuration	Yes	

Control	Support for the Control	Comments, if not supported
	Option is set to '0'	
2.5	Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0'	<p>Yes</p> <p>OLE automation procedures were used previously, but the procedures are not needed from Commvault software version FR 11.25 onwards as the procedures have CLR equivalents currently.</p>
2.6	Ensure 'Remote Access' Server Configuration Option is set to '0'	<p>Yes</p>
2.7	Ensure 'Remote Admin Connections' Server Configuration Option is set to '0'	<p>Yes</p>
2.8	Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0'	<p>Yes</p>
2.9	Ensure 'Trustworthy' Database Property is set to 'Off'	<p>Yes</p>
2.10	Ensure Unnecessary SQL Server Protocols are set to 'Disabled'	<p>Yes, requires manual configuration</p> <p>Communication with the Commvault SQL Server instance is done through TCP/IP protocol. You can disable all other protocols. For instructions, see Enable or Disable a Server Network Protocol.</p>

Control		Support for the Control	Comments, if not supported
2.11	Ensure SQL Server is configured to use non-standard ports	Yes	A default installation of SQL Server 2014 and later versions uses a dynamic port. For security reasons, you can configure a different port. For instructions, see Configure a Server to Listen on a Specific TCP Port .
2.12	Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances	Yes, requires manual configuration	To support this control, you must manually hide the SQL server instance. For instructions, see Hiding the SQL Server Instance .
2.13	Ensure the 'sa' Login Account is set to 'Disabled'	Yes	
2.14	Ensure the 'sa' Login Account has been renamed	Yes	
2.15	Ensure 'AUTO_CLOSE' is set to 'OFF' on contained databases	Yes	
2.16	Ensure no login exists with the name 'sa'	Yes	
2.17	Ensure 'clr strict security' Server Configuration Option is set to '1'	Yes	

Control		Support for the Control	Comments, if not supported
3	Authentication and Authorization		
3.1	Ensure 'Server Authentication' Property is set to 'Windows Authentication Mode'	Yes, requires manual configuration	To enable this control in your environment, follow the instructions in the troubleshooting article - Windows Authentication for Commvault SQL Server Connections .
3.2	Ensure CONNECT permissions on the 'guest' user is Revoked within all SQL Server databases.	Yes	
3.3	Ensure 'Orphaned Users' are Dropped From SQL Server Databases	Yes	
3.4	Ensure SQL Authentication is not used in contained databases	Yes	
3.5	Ensure the SQL Server's MSSQL Service Account is Not an Administrator	No	Primary interaction with the Commvault SQL Server instance is done using the sqladmin_cv account. The sqladmin_cv account has sysadmin role for the CommServe database and public role for all databases in the SQL instance. The sqlexec_cv user has public role for all databases. The Commvault software

Control	Support for the Control	Comments, if not supported
		requires these permissions. So, this control cannot be supported.
3.6	Ensure the SQL Server's SQLAgent Service Account is Not an Administrator	No Primary interaction with the Commvault SQL Server instance is done using the sqladmin_cv account. The sqladmin_cv account has sysadmin role for the CommServe database and public role for all databases in the SQL instance. The sqlexec_cv user has public role for all databases. The Commvault software requires these permissions. So, this control cannot be supported.
3.7	Ensure the SQL Server's Full-Text Service Account is Not an Administrator	N/A The Commvault software does not contain Full-Text Service Account. So, this control is not applicable.
3.8	Ensure only the default permissions specified by Microsoft are granted to the public server role	Yes
3.9	Ensure Windows BUILTIN groups are not SQL Logins	Yes
3.10	Ensure Windows local groups are not SQL Logins	Yes
3.11	Ensure the public	Yes

Control		Support for the Control	Comments, if not supported
	role in the msdb database is not granted access to SQL Agent proxies		
3.12	Ensure the 'SYSADMIN' Role is Limited to Administrative or Built-in Accounts	Yes, requires manual configuration	Ensure only approved administrative or built-in accounts retain the SYSADMIN role. Remove any non-approved accounts using the query below, while preserving SYSADMIN access for Commvault (CV) accounts.
3.13	Ensure membership in admin roles in MSDB database is limited	Yes	
4	Password Policies		
4.1	Ensure 'MUST_CHANGE' Option is set to 'ON' for All SQL Authenticated Logins	N/A	The passwords are created by Commvault are stored in registry in encrypted format, and it cannot be changed because process is not interactive.
4.2	Ensure 'CHECK_EXPIRATION' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role	No	The passwords are created by Commvault are stored in registry in encrypted format, and it cannot be changed because process is not interactive.

Control	Support for the Control	Comments, if not supported
4.3 Ensure 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins	No	The passwords are created by Commvault are stored in registry in encrypted format, and it cannot be changed because process is not interactive.
5 Auditing and Logging		
5.1 Ensure 'Maximum number of error log files' is set to greater than or equal to '12'	Yes	
5.2 Ensure 'Default Trace Enabled' Server Configuration Option is set to '1'	Yes	
5.3 Ensure 'Login Auditing' is set to 'failed logins'	Yes	
5.4 Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins'	Yes	
6 Application Development		
6.1 Ensure Database and Application User Input is Sanitized	Yes	
6.2 Ensure 'CLR Assembly Permission Set' is	Yes	

	set to 'SAFE_ACCESS' for All CLR Assemblies		
7	Encryption		
7.1	Ensure 'Symmetric Key encryption algorithm' is set to 'AES_128' or higher in non-system databases	Yes	
7.2	Ensure Asymmetric Key Size is set to 'greater than or equal to 2048' in non-system databases	Yes	
8	Appendix: Additional Considerations		
8.1	Ensure 'SQL Server Browser Service' is configured correctly	Yes, requires manual configuration	<p>By default, the CommServe software uses the Microsoft SQL Server Browser service to enable clients and other Commvault applications to connect to the CommServe database through dynamic ports. If required, to prevent the CommServe database instance from being exposed by the SQL Server Browser service, you can configure the CommServe database to use a static port and turn off the SQL Server Browser service.</p> <p>If you use Workflow Engine and Web Services, you must manually configure static ports.</p>

©1999-2022 Commvault Systems, Inc. All rights reserved. Commvault, Commvault and logo, the "C hexagon" logo, Commvault Systems, Commvault HyperScale, ScaleProtect, Commvault OnePass, Unified Data Management, Quick Recovery, QR, CommNet, GridStor, Vault Tracker, InnerVault, Quick Snap, QSnap, IntelliSnap, Recovery Director, CommServe, CommCell, APSS, Commvault Edge, Commvault GO, Commvault Advantage, Commvault Complete, Commvault Activate, Commvault Orchestrate, Commvault Command Center, Hedvig, Universal Data Plane, the "Cube" logo, Metallic, the "M Wave" logo, and CommValue are trademarks or registered trademarks of Commvault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specification are subject to change without notice.

The development release and timing of future product releases remains at Commvault's sole discretion. Commvault is providing the following information in accordance with Commvault's standard product communication policies. Any resulting features, functionality, and enhancements or timing of release of such features, functionality, and enhancements are at the sole discretion of Commvault and may be modified without notice. All product roadmap or other similar information does not represent a commitment to deliver any material, code, or functionality, and should not be relied upon in making a purchasing decision.

Visit the [Commvault Documentation](#) website for complete documentation of Commvault products.

