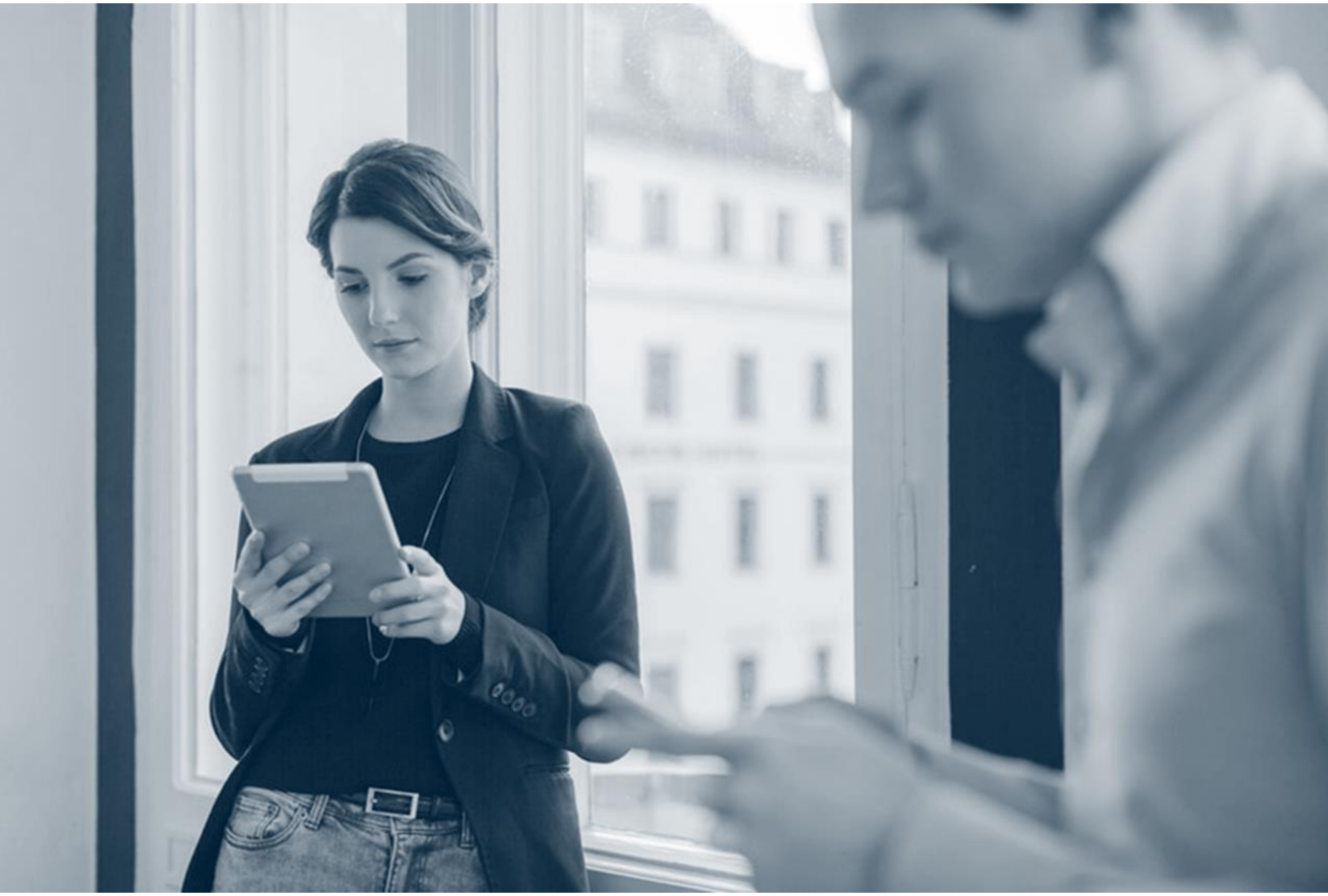
Commvault Compliance with CIS Level 1 Security Controls

CIS Microsoft SQL Server 2016 Benchmark v1.1.0

Friday, 9 July 2021



Commvault Compliance with the Level 1 Controls of CIS Microsoft SQL Server 2016 Benchmark v1.1.0

The **CIS Microsoft SQL Server 2016 Benchmark v1.1.0** provides prescriptive guidance for establishing a secure configuration posture to develop, deploy, assess, or secure solutions that incorporate Microsoft SQL Server 2016 on a Microsoft Windows platform.

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.

Control		Support for the Control	Comments, if not supported
1	**Installation, Updates and Patches**		
1.1	Ensure Latest SQL Server Service Packs and Hotfixes are Installed (Not Scored)	Yes	The workflow engine that is built-in with the Commvault software performs automatic updates of the SQL server.
1.2	Ensure Single-Function Member Servers are Used (Not Scored)	Yes	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' (Scored)	Yes	
2.2	Ensure 'CLR Enabled' Server Configuration Option is set to '0' (Scored)	No	The Commvault software uses the CLR functionality and the functionality cannot be disabled. So, the software does not support this control.
2.3	Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0' (Scored)	Yes	
2.4	Ensure 'Database Mail XPs' Server Configuration	Yes	

Control		**Support for the Control**	**Comments, if not supported**
	Option is set to '0' (Scored)		
2.5	Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0' (Scored)	**No**	Commvault software uses OLE. If OLE is disabled, few software functionalities do not work.
2.6	Ensure 'Remote Access' Server Configuration Option is set to '0' (Scored)	**Yes**	
2.7	Ensure 'Remote Admin Connections' Server Configuration Option is set to '0' (Scored)	**Yes**	
2.8	Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0' (Scored)	**Yes**	
2.9	Ensure 'Trustworthy' Database Property is set to 'Off' (Scored)	**Yes**	
2.10	Ensure Unnecessary SQL Server Protocols are set to 'Disabled' (Not Scored)	**Yes, requires manual configuration**	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.

Control		Support for the Control	Comments, if not supported
2.11	Ensure SQL Server is configured to use non-standard ports (Not Scored)	**Yes, requires manual configuration**	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 (Scored)	**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' (Scored)	**Yes**	
2.14	Ensure the 'sa' Login Account has been renamed (Scored)	**Yes**	
2.15	Ensure 'xp_cmdshell' Server Configuration Option is set to '0' (Scored)	**Yes**	
2.16	Ensure 'AUTO_CLOSE' is set to 'OFF' on contained databases (Scored)	**Yes**	
2.17	Ensure no login exists with the name 'sa' (Scored)	**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' (Scored)	**No**	When the 'Server Authentication' property is set to 'Windows Authentication Mode', the SQL access becomes less secure for the Commvault software. If the control is an absolute requirement in your environment, you can enable the control by following the instructions in the knowledgebase article at the following link: http://kb.commvault.com/article/DOC0551
3.2	Ensure CONNECT permissions on the 'guest' user is Revoked within all SQL Server databases excluding the master, msdb and tempdb (Scored)	**Yes**	
3.3	Ensure 'Orphaned Users' are Dropped From SQL Server Databases (Scored)	**Yes**	
3.4	Ensure SQL Authentication is not used in contained databases (Scored)	**Yes**	
3.5	Ensure the SQL	**No**	Primary interaction with the Commvault

Control		Support for the Control	Comments, if not supported
	Server's MSSQL Service Account is Not an Administrator (Not Scored)		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.
3.6	Ensure the SQL Server's SQLAgent Service Account is Not an Administrator (Not Scored)	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 (Not Scored)	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 (Scored)	Yes	
3.9	Ensure Windows BUILTIN groups are	Yes	

Control		Support for the Control	Comments, if not supported
	not SQL Logins (Scored)		
3.10	Ensure Windows local groups are not SQL Logins (Scored)	Yes	
3.11	Ensure the public role in the msdb database is not granted access to SQL Agent proxies (Scored)	Yes	
4	**Password Policies**		
4.1	Ensure 'MUST_CHANGE' Option is set to 'ON' for All SQL Authenticated Logins (Not Scored)	N/A	The Commvault software creates sqladmin_cv and sqlexec_cv users that are used only by Commvault software to access the CommServe database. So, this control is not applicable.
4.2	Ensure 'CHECK_EXPIRATION ' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role (Scored)	No	
4.3	Ensure 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins (Scored)	No	Windows policy is designed based on the organization requirements. So, without an understanding of the organization Windows policy, this control cannot be supported.

Control		**Support for the Control**	**Comments, if not supported**
5	**Auditing and Logging**		
5.1	Ensure 'Maximum number of error log files' is set to greater than or equal to '12' (Scored)	**Yes**	
5.2	Ensure 'Default Trace Enabled' Server Configuration Option is set to '1' (Scored)	**Yes**	
5.3	Ensure 'Login Auditing' is set to 'failed logins' (Scored)	**Yes**	
5.4	Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins' (Scored)	**Yes**	
6	**Application Development**		
6.1	Ensure Database and Application User Input is Sanitized (Not Scored)	**Yes**	
6.2	Ensure 'CLR Assembly Permission Set' is	**No**	The Commvault software uses the CLR functionality and the functionality cannot be disabled. So, the software does not

Control		Support for the Control	Comments, if not supported
	set to 'SAFE_ACCESS' for All CLR Assemblies (Scored)		support this control.
7	**Encryption**		
7.1	Ensure 'Symmetric Key encryption algorithm' is set to 'AES_128' or higher in non-system databases (Scored)	**Yes**	
7.2	Ensure Asymmetric Key Size is set to 'greater than or equal to 2048' in non-system databases (Scored)	**Yes**	
8	**Appendix: Additional Considerations**		
8.1	Ensure 'SQL Server Browser Service' is configured correctly (Not Scored)	**Yes, requires manual configuration**	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.

Control		Support for the Control	Comments, if not supported
			If you use Workflow Engine and Web Services, you must manually configure static ports.

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.

COMMVAULT® | Be ready™

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM