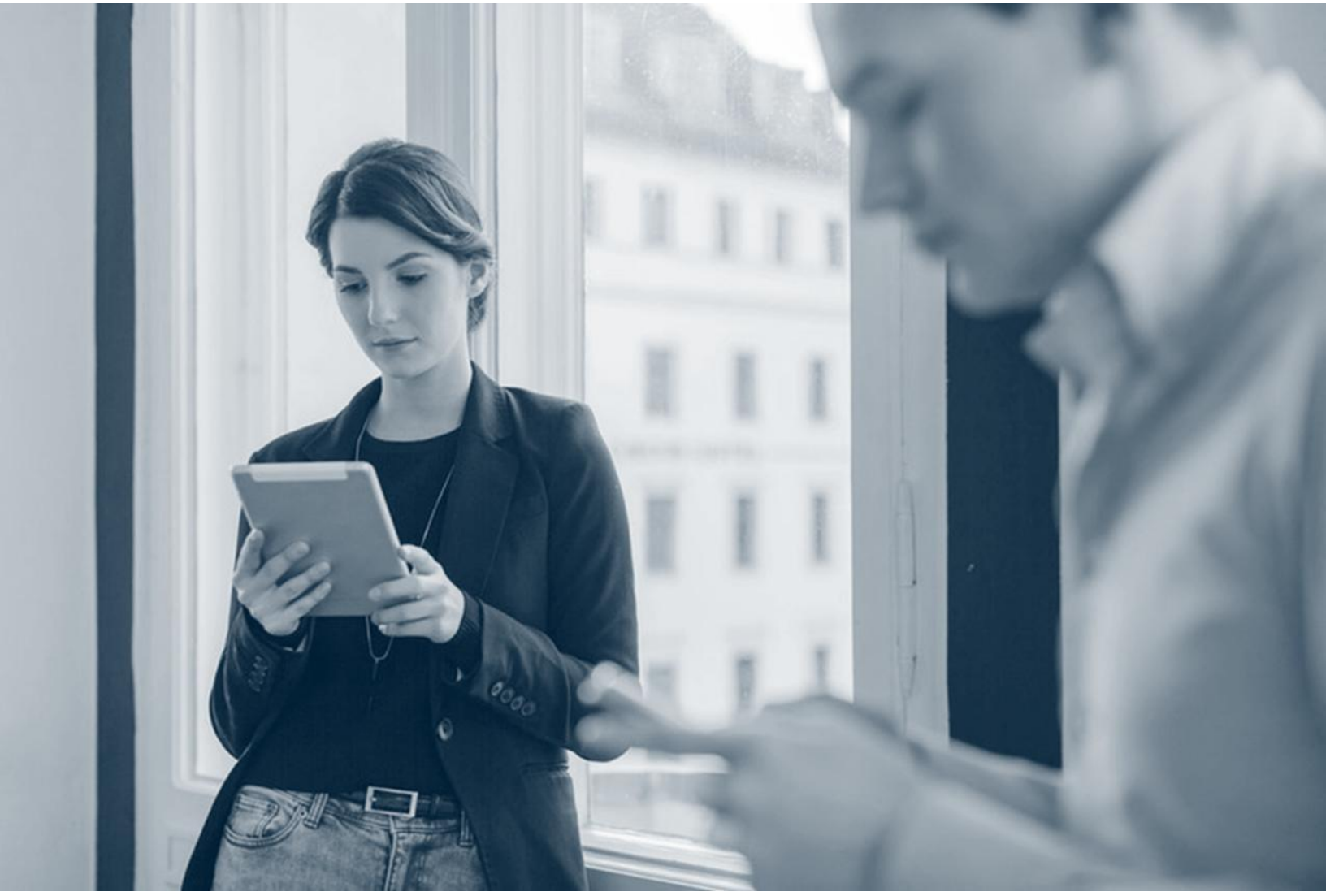
Commvault Compliance with CIS Level 1 Security Controls

CIS Microsoft IIS 10 Benchmark v1.2.1

Friday, Apr 22, 2025



Commvault Compliance with the Level 1 Controls of CIS Microsoft IIS 10 Benchmark v1.2.1

The **CIS Microsoft IIS Server 10** Benchmark provides prescriptive guidance for establishing a secure configuration posture to develop, deploy, assess, or secure solutions that incorporate IIS. 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.

Level 1 Control		Support for the Control	Comments, if not supported
1	**Basic Configurations**		
1.1	Ensure web content is on non-system partition	**Yes, requires manual configuration**	To support this configuration, you must perform a hardware refresh of the web server and then select a different installation path for the Commvault other than the system path (C Drive).
1.2	Ensure 'host headers' are on all sites	**Yes, requires manual configuration**	This control is supported from Feature Release 23 of the Commvault software with manual configuration. The OVA image could not support this configuration due to system limitation. To support this control, complete the following steps: 1. Update the host header on the web server machine. For instructions, see Configure a

Level 1 Control		Support for the Control	Comments, if not supported
			Host Header for a Web Site (IIS 7). 2. On the Web Console machine, add the additional setting **baseURL** to use virtual name instead of physical host name. For instructions, see Using a Virtual Name for a Web Service. 3. To ensure that the communication to the web server remains functional, add the virtual name in the DNS setting pointing to the IP address of the web server machine. 4. Verify that the Command Center and the compliance search are functional. 5. Verify that the Analytics operations such as adding or removing a role are working fine as expected.
1.3	Ensure 'Directory browsing' is set to disabled	**Yes**	
1.4	Ensure 'application pool identity' is configured for all application pools	**Yes, requires manual configuration**	Refer to KB Article.

Level 1 Control		Support for the Control	Comments, if not supported
1.5	Ensure 'unique application pools' is set for sites	**Yes, requires manual configuration**	Create a unique application pool and refer to KB Article for more details. 1. Login to IIS. 2. From left panel, navigate to **Sites > Consoles**. 3. For each site, create an application pool and configure unique application pool for each site. 4. Follow the Microsoft-Adding Application Pools documentation and configure the application pool for an existing site. **Note**: When performing this step, continue to retain below app to app-pool mapping: - SearchSvc – ConsolesAppPool - ProxySvc – WebSearchProxyApplication Pool - Indexgateway – ConsolesAppDotNetCore Create separate application pool for rest of the apps under Console site to isolate them as per hardening requirement.
1.6	Ensure 'application pool identity' is configured for anonymous user identity	**Yes, requires manual configuration**	Refer to KB Article.

Level 1 Control		Support for the Control	Comments, if not supported
1.7	Ensure WebDav feature is disabled	**Yes**	This control removes a Windows Feature, it is executed at the end to avoid destabilizing IIS during hardening. Reboot required after remediation.
2	**Configure Authentication and Authorization**		
2.1	Ensure 'global authorization rule' is set to restrict access	**N/A**	Commvault software does not support Windows integrated authentication.
2.2	Ensure access to sensitive site features is restricted to authenticated principals only	**N/A**	Commvault software uses custom API tokens. Disabling IIS Anonymous Authentication forces standard Windows credentials, rejecting these internal tokens and causing logins to fail.
2.3	Ensure 'forms authentication' require SSL	**Yes**	
2.5	Ensure 'cookie protection mode' is configured for forms authentication	**Yes**	
2.6	Ensure transport layer security for 'basic authentication' is configured	**Yes, requires manual configuration**	A valid SSL certificate must be installed in LocalMachine\My store and a DNS name must be resolvable before remediation. This will enforce SSL on the Consoles site and break HTTP access on port 82.
2.7	Ensure 'passwordFormat' is not set to clear	**Yes**	

Level 1 Control		Support for the Control	Comments, if not supported
3	**ASP.NET Configuration Recommendations**		
3.1	Ensure 'deployment method retail' is set	**Yes**	
3.4	Ensure IIS HTTP detailed errors are hidden from displaying remotely	**Yes**	
3.7	Ensure 'cookies' are set with HTTP Only attribute	**Yes**	
3.9	Ensure 'MachineKey validation method - .Net 4.5' is configured	**Yes**	
3.10	Ensure global .NET trust level is configured	**N/A**	The security control recommends maintaining medium or low global .NET trust level. However, with these trust levels, some of the Commvault processes does not function properly. So, we do not support this control currently.
4	**Request Filtering and Other Restriction Modules**		
4.5	Ensure Double-Encoded requests will be rejected	**N/A**	Commvault software uses double encoding.
4.6	Ensure 'HTTP Trace Method' is disabled	**Yes**	
4.7	Ensure Unlisted File Extensions are not allowed	**Yes**	Whitelists .svc and extensionless (.) before blocking unlisted extensions.

Level 1 Control		Support for the Control	Comments, if not supported
4.8	Ensure Handler is not granted Write and Script/Execute	**Yes**	
4.9	Ensure 'notListedIsapisAllowed' is set to false	**Yes**	
4.10	Ensure 'notListedCgisAllowed' is set to false	**Yes**	
4.11	Ensure 'Dynamic IP Address Restrictions' is enabled	**Yes, requires manual configuration**	Manual configuration needed to set exact maxConcurrentRequests and maxRequests thresholds.
5	**IIS Logging Recommendations**		
5.1	Ensure Default IIS web log location is moved	**Yes, requires manual configuration**	To support this control, configure a location different from the system drive (C Drive). For instructions, see Configure Logging in IIS.
5.2	Ensure Advanced IIS logging is enabled	**Yes, requires manual configuration**	To support this control, enable ETW logging. For instructions, see Logging to Event Tracing for Windows in IIS 8.5.
5.3	Ensure 'ETW Logging' is enabled	**Yes**	
6	**FTP Requests**		
6.1	Ensure FTP requests are encrypted	**Yes**	
6.2	Ensure FTP Logon attempt restrictions is	**Yes**	

Level 1 Control		Support for the Control	Comments, if not supported
	enabled		
7	**Transport Encryption**		
7.2	Ensure SSLv2 is Disabled	**Yes**	
7.3	Ensure SSLv3 is Disabled	**Yes**	
7.4	Ensure TLS 1.0 is Disabled	**Yes**	
7.5	Ensure TLS 1.1 is Disabled	**Yes**	
7.6	Ensure TLS 1.2 is Enabled	**Yes**	
7.7	Ensure NULL Cipher Suites is Disable	**Yes**	
7.8	Ensure DES Cipher Suites is Disabled	**Yes**	
7.9	Ensure RC4 Cipher Suites is Disabled	**Yes**	
7.10	Ensure AES 128/128 Cipher Suite is Disabled	**Yes**	
7.11	Ensure AES 256/256 Cipher Suite is Enabled	**Yes**	

Visit the Commvault Documentation website for complete documentation of Commvault products.