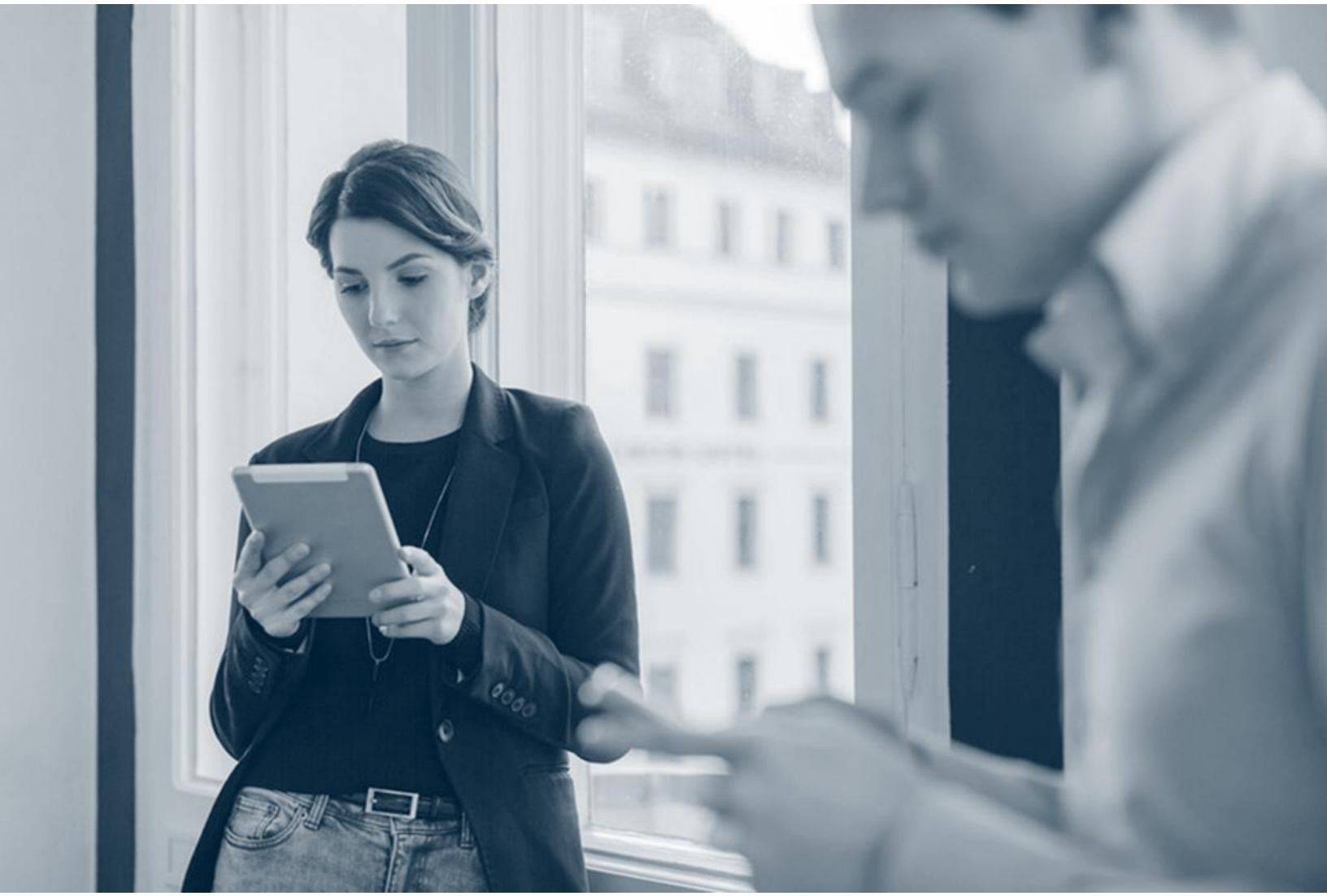




# Commvault Compliance with CIS Level 1 Security Controls

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
<b>1</b>	<b>Basic Configurations</b>		
1.1	Ensure web content is on non-system partition	<b>Yes, requires manual configuration</b>	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	<b>Yes, requires manual configuration</b>	<p>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 a system limitation.</p> <p>To support this control, complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Update the host header on the web server machine. For instructions, see <a href="#">Configure a</a></li> </ol>

Level 1 Control	Support for the Control	Comments, if not supported	
		<p><a href="#">Host Header for a Web Site (IIS 7)</a>.</p> <ol style="list-style-type: none"> <li>2. On the Web Console machine, add the additional setting <b>baseURL</b> to use virtual name instead of physical host name. For instructions, see <a href="#">Using a Virtual Name for a Web Service</a>.</li> <li>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.</li> <li>4. Verify that the Command Center and the compliance search are functional.</li> <li>5. Verify that the Analytics operations such as adding or removing a role are working fine as expected.</li> </ol>	
1.3	Ensure 'Directory browsing' is set to disabled	<b>Yes</b>	
1.4	Ensure 'application pool identity' is configured for all application pools	<b>Yes, requires manual configuration</b>	Refer to <a href="#">KB Article</a> .
1.5	Ensure 'unique application pools' is set	<b>Yes, requires manual</b>	Create a unique application pool and refer to <a href="#">KB Article</a> for more

Level 1 Control	Support for the Control	Comments, if not supported
	for sites	<p>configuration</p> <p>details.</p> <ol style="list-style-type: none"> <li>1. Login to IIS.</li> <li>2. From left panel, navigate to <b>Sites &gt; Consoles</b>.</li> <li>3. For each site, create an application pool and configure unique application pool for each site.</li> <li>4. Follow the <a href="#">Microsoft-Adding Application Pools</a> documentation and configure the application pool for an existing site.</li> </ol> <p><b>Note:</b> When performing this step, continue to retain below app to app-pool mapping:</p> <ul style="list-style-type: none"> <li>- SearchSvc – ConsolesAppPool</li> <li>- ProxySvc – WebSearchProxyApplication Pool</li> <li>- Indexgateway – ConsolesAppDotNetCore</li> </ul> <p>Create separate application pool for rest of the apps under Console site to isolate them as per hardening requirement.</p>
1.6	Ensure 'application pool identity' is configured for anonymous user identity	<p>Yes, requires manual configuration</p> <p>Refer to <a href="#">KB Article</a>.</p>

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.
<b>2</b>	<b>Configure Authentication and Authorization</b>		
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
<b>3</b>	<b>ASP.NET Configuration Recommendations</b>		
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 HttpOnly 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.
<b>4</b>	<b>Request Filtering and Other Restriction Modules</b>		
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.
<b>5</b>	<b>IIS Logging Recommendations</b>		
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 <a href="#">Configure Logging in IIS</a> .
5.2	Ensure Advanced IIS logging is enabled	Yes, requires manual configuration	To support this control, enable ETW logging. For instructions, see <a href="#">Logging to Event Tracing for Windows in IIS 8.5</a> .
5.3	Ensure 'ETW Logging' is enabled	Yes	
<b>6</b>	<b>FTP Requests</b>		
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	
<b>7</b>	<b>Transport Encryption</b>	
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

©1999–2020 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.



[COMMVULT.COM](https://www.commvault.com) | 888.746.3849 | [GET-INFO@COMMVULT.COM](mailto:GET-INFO@COMMVULT.COM)