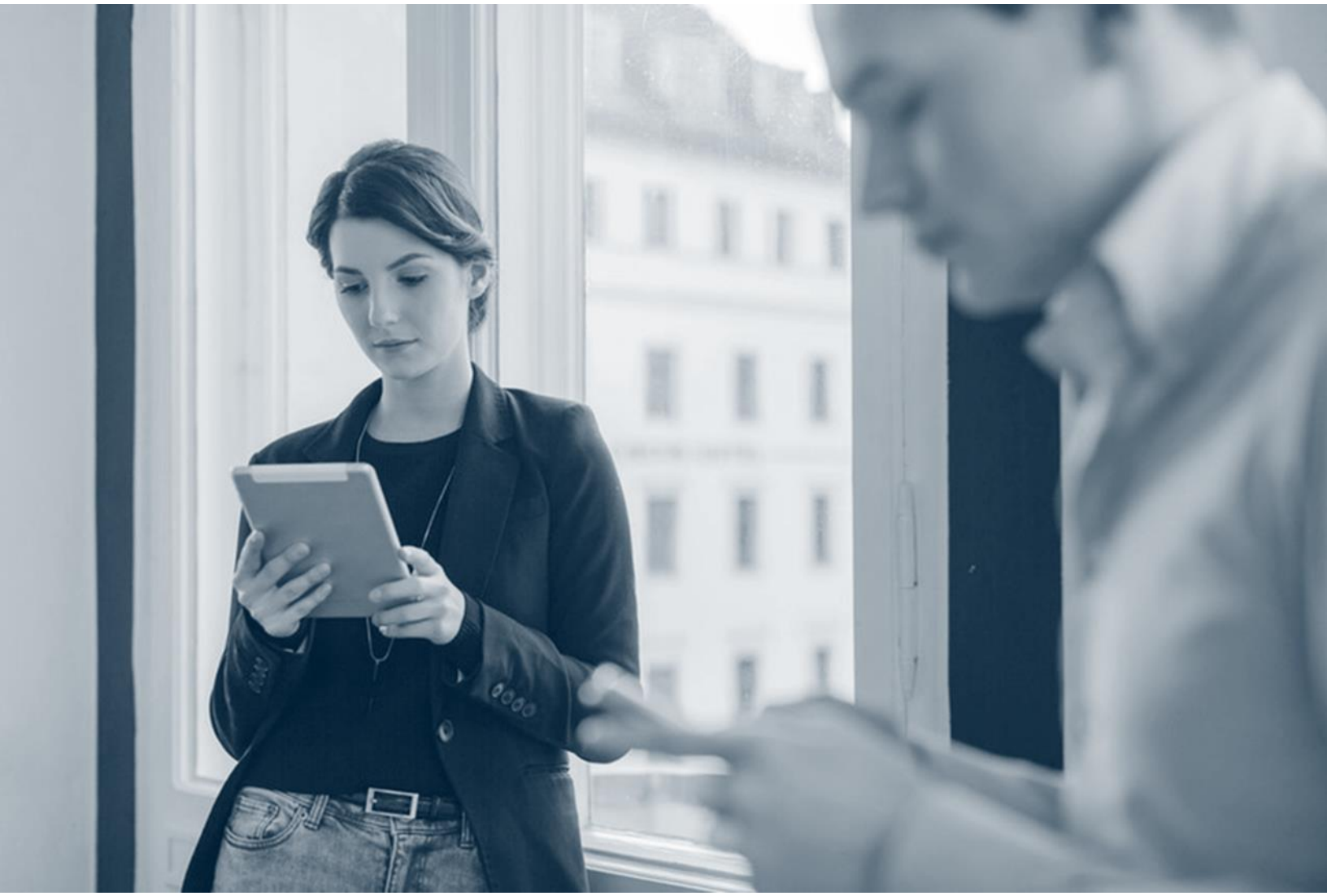




Commvault Compliance with CIS Level 1 Security Controls

CIS Microsoft IIS 10 Benchmark v1.1.1

Friday, July 9, 2021



Commvault Compliance with the Level 1 Controls of CIS Microsoft IIS 10 Benchmark v1.1.1

The **CIS Microsoft IIS 10 Benchmark** provides prescriptive guidance for establishing a secure configuration posture for Microsoft IIS 10 running on Microsoft Windows Server 2016. The benchmark includes several security controls with both Level 1 and Level 2 configuration profiles.

The security controls in Level 1 provide a clear security benefit. The controls in Level 2 extend the Level 1 and are intended for environments or use cases where security is paramount. The following table presents the compliance of the Commvault software with the Level 1 controls. We intend to extend our support for the Level 2 controls in the future versions of our software.

Level 1 Control		Support for the Control	Comments, if not supported
1	Basic Configurations		
1.1	Ensure web content is on non-system partition (Scored)	No	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 (Scored)	Yes, requires manual configuration	<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>Update the host header. For instructions, see Configure a Host Header for a Web Site (IIS 7).</p> <p>After you update the host header, complete the following steps.</p> <ol style="list-style-type: none"> 1. On the web server machine, add the additional setting sIIInternalHostname with desired virtual name. 2. On the Web Console machine, add the additional setting baseURL to use virtual name instead of physical host name. 3. In the configuration.properties file located in the <code><InstallDirectory>\webclient\web-inf\classes</code> directory on the

Level 1 Control	Support for the Control	Comments, if not supported
		<p>corresponding compliance search machine, update the WebServiceUrl configuration to use the virtual name.</p> <ol style="list-style-type: none"> 4. 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. 5. Restart tomcat services on the web server machine. 6. Verify that the Command Center and the compliance search are functional. 7. In your CommCell environment, set the web server where you performed the configurations as the default web server. 8. 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 (Scored)	Yes
1.4	Ensure 'application pool identity' is configured for all application pools	No The Commvault software uses NetworkService account configuration. Disabling this configuration can affect the laptop related features in your

Level 1 Control		Support for the Control	Comments, if not supported
	(Scored)		CommCell environment.
1.5	Ensure 'unique application pools' is set for sites (Scored)	No	The ConsolesAppPool in the Commvault software is used by multiple Commvault applications. We do not support this control currently as this control can lead to significant regression issues.
1.6	Ensure 'application pool identity' is configured for anonymous user identity (Scored)	No	Commvault web services uses WCF module that cannot start unless you enable the anonymous authentication. Web service APIs of the Commvault are secured by Commvault's own authentication layer. These APIs that serve any user or secured content would not work unless you provide the Commvault authentication token to the web service. So, security is not a concern.
1.7	Ensure WebDav feature is disabled (Scored)	Yes	
2	Configure Authentication and Authorization		
2.1	Ensure 'global authorization rule' is set to restrict access (Not Scored)	N/A	Commvault software does not support Windows integrated authentication.
2.2	Ensure access to sensitive site features is restricted to authenticated principals only (Not	Yes	

Level 1 Control		Support for the Control	Comments, if not supported
	Scored)		
2.3	Ensure 'forms authentication' require SSL (Scored)	Yes	
2.5	Ensure 'cookie protection mode' is configured for forms authentication (Scored)	Yes	
2.6	Ensure transport layer security for 'basic authentication' is configured (Scored)	Yes	
2.7	Ensure 'passwordFormat' is not set to clear (Scored)	Yes	
3	ASP.NET Configuration Recommendations		
3.1	Ensure 'deployment method retail' is set (Scored)	Yes	
3.4	Ensure IIS HTTP detailed errors are hidden from displaying remotely (Scored)	Yes	
3.7	Ensure 'cookies' are set with HttpOnly attribute (Scored)	Yes	
3.9	Ensure 'MachineKey validation method -	Yes	

Level 1 Control	Support for the Control	Comments, if not supported
3.10	.Net 4.5' is configured (Scored)	
3.10	Ensure global .NET trust level is configured (Scored)	<p>No</p> <p>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.</p>
4	Request Filtering and Other Restriction Modules	
4.5	Ensure Double-Encoded requests will be rejected (Scored)	<p>No</p> <p>Commvault software uses double encoding.</p>
4.6	Ensure 'HTTP Trace Method' is disabled (Scored)	<p>Yes</p>
4.7	Ensure Unlisted File Extensions are not allowed (Scored)	<p>Yes, requires manual configuration</p> <p>Configure .svc and . as allowed file extensions. For instructions, see File Name Extensions.</p>
4.8	Ensure Handler is not granted Write and Script/Execute (Scored)	<p>Yes</p>
4.9	Ensure 'notListedIsapisAllowed' is set to false (Scored)	<p>Yes</p>
4.1	Ensure 'notListedCgisAllowed'	<p>Yes</p>

Level 1 Control		Support for the Control	Comments, if not supported
0	is set to false (Scored)		
4.11	Ensure 'Dynamic IP Address Restrictions' is enabled (Not Scored)	Yes	
5	IIS Logging Recommendations		
5.1	Ensure Default IIS web log location is moved (Scored)	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 (Scored)	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 (Not Scored)	Yes	
6	FTP Requests		
6.1	Ensure FTP requests are encrypted (Not Scored)	Yes	
6.2	Ensure FTP Logon attempt restrictions is enabled (Not Scored)	Yes	
7	Transport Encryption		
7.2	Ensure SSLv2 is Disabled (Scored)	Yes	
7.3	Ensure SSLv3 is Disabled (Scored)	Yes	

Level 1 Control		Support for the Control	Comments, if not supported
7.4	Ensure TLS 1.0 is Disabled (Scored)	Yes	
7.5	Ensure TLS 1.1 is Disabled (Scored)	Yes	
7.6	Ensure TLS 1.2 is Enabled (Scored)	Yes	
7.7	Ensure NULL Cipher Suites is Disabled (Scored)	Yes	
7.8	Ensure DES Cipher Suites is Disabled (Scored)	Yes	
7.9	Ensure RC4 Cipher Suites is Disabled (Scored)	Yes	
7.10	Ensure AES 128/128 Cipher Suite is Disabled (Scored)	Yes	
7.11	Ensure AES 256/256 Cipher Suite is Enabled (Scored)	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  | Be ready™

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