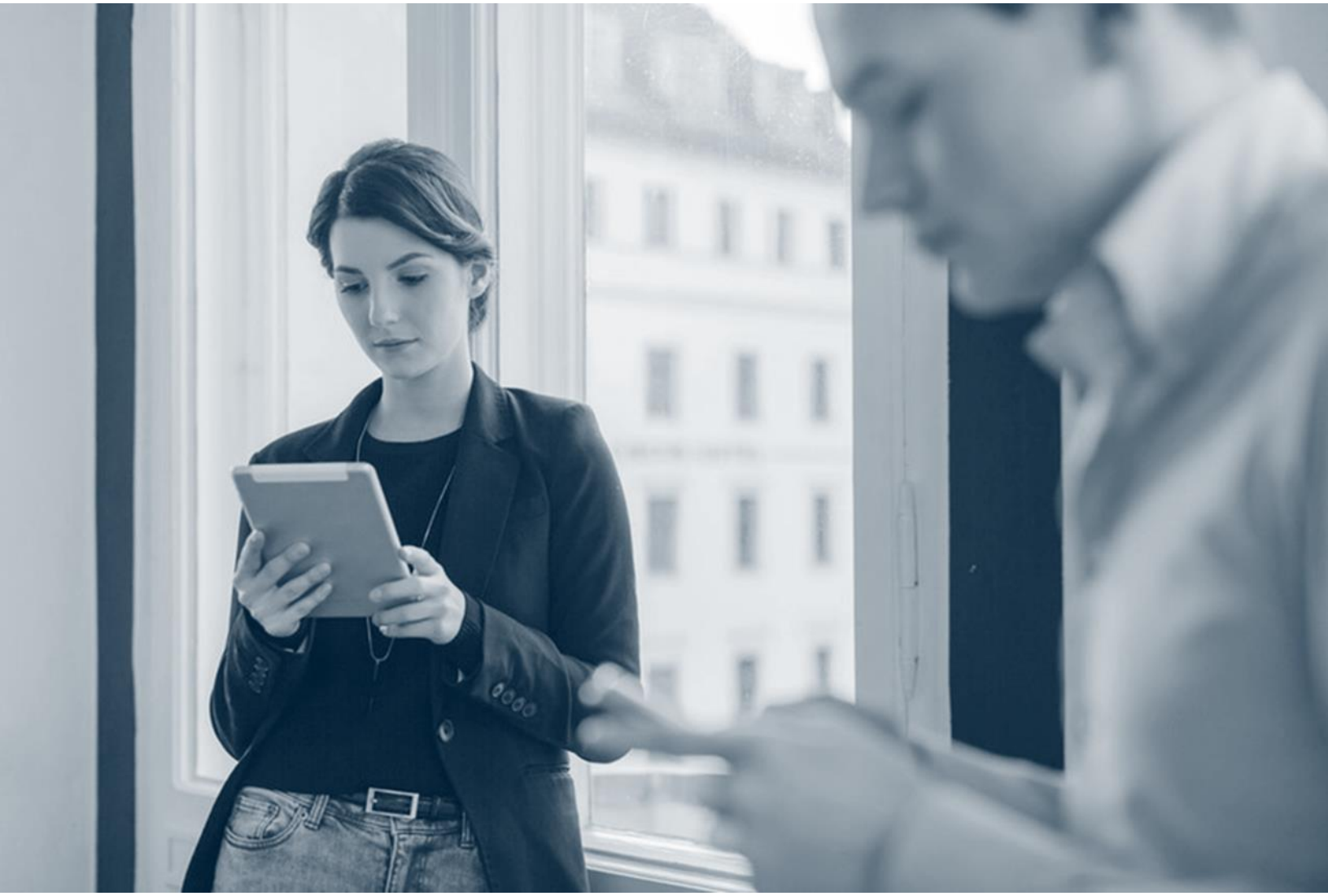
COMMVAULT

Commvault Compliance with CIS Level 1 Security Controls

Apache Tomcat 10 Benchmark v1.1.0

Wednesday, July 30, 2024



Commvault Compliance with the Level 1 Controls

The **Security Configuration Benchmark for Apache Tomcat 10** provides prescriptive guidance for establishing a secure configuration posture for Apache Tomcat versions 10 running on Linux. 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**
2	**Limit Server Platform Information Leaks**		
2.5	Disable client facing Stack Traces	**Yes**	This control is not applicable to the Commvault software. The error pages in our software are overridden using the web.xml file.
2.6	1.4.6 Turn off TRACE	**Yes**	

3	**Protect the Shutdown Port**		
3.1	Set a nondeterministic Shutdown command value	**Yes**	Commvault software always set the shutdown port to -1 in server.xml which disables the shutdown port. So, this control is not applicable. But for compliance reason shutdown can set to "NONDETERMINISTICVALUE" which will not have any effect.
4	**Protect Tomcat Configurations**		
4.1	Restrict access to $CATALINA_HOME	**Yes**	
4.2	Restrict access to $CATALINA_BASE	**Yes**	
4.3	Restrict access to Tomcat configuration directory	**Yes**	
4.4	Restrict access to Tomcat logs directory	**Yes**	
4.5	Restrict access to Tomcat temp directory	**Yes**	
4.6	Restrict access to Tomcat binaries directory	**Yes**	
4.7	Restrict access to Tomcat web	**Yes**	

	application directory		
4.8	Restrict access to Tomcat catalina.policy	Yes	
4.9	Restrict access to Tomcat catalina.properties	Yes	
4.10	Restrict access to Tomcat context.xml	Yes	
4.11	Restrict access to Tomcat logging.properties	Yes	
4.12	Restrict access to Tomcat server.xml	Yes	
4.13	Restrict access to Tomcat tomcat-users.xml	Yes	
4.14	Restrict access to Tomcat web.xml	Yes	
6	**Connector Security**		
6.2	Ensure SSLEnabled is set to True for Sensitive Connectors	Yes	
6.3	Ensure scheme is set accurately	Yes	
6.4	Ensure secure is set to true only for SSL-enabled Connectors	Yes	
6.5	Ensure SSL Protocol is set to TLS for Secure Connectors	Yes	By default, a new installation will be set to use TLS 1.2 and 1.3. Customers are free to change that to 1.3 only, or anything else that tomcat

			itself supports.
7	**Establish and Protect Logging Facilities**		
7.2	Specify file handler in logging.properties files	**Yes**	This control is not applicable to the Commvault software. Our software uses logback feature
7.4	Ensure directory in context.xml is a secure location	**Yes**	Default tomcat log location is /var/log/commvault/Log_files/web. These tomcat log files are default secured by protected with O-RWX permissions
7.5	Ensure pattern in context.xml is correct	**Yes**	Yes, Commvault meet this requirement. We configure the access log value to log client IP, timestamp, requested resource, plus some timing information.

7.6	Ensure directory in logging.properties is a secure location	Yes	

8	**Configure Catalina Policy**		
8.1	Restrict runtime access to sensitive packages	Yes	
9	**Application Deployment**		
9.1	Starting Tomcat with SecurityManager	No	Implementing this effectively may require a custom SecurityManager and could introduce significant regression risk
10	**Miscellaneous ConfigurationSettings**		
10.1	Ensure Web content directory is on a separate partition from the Tomcat system files	No	We do not support installing tomcat on a separate partition from the web content files. Commvault binary locations are tied to the installer and are fixed relative to the commvault install point.
10.2	Restrict access to the web administration application	Yes	This item is referring to the manager application. We completely disable the manager

			application, so this rule is not applicable.
10.4	Force SSL when accessing the manager application	**Yes**	This item is referring to the manager application. We completely disable the manager application, so this rule is not applicable.
10.7	Turn off session façade recycling	**Yes**	
10.12	Do not allow symbolic linking	**Yes**	
10.13	Do not run applications as privileged	**Yes**	
10.14	Do not allow cross context requests	**Yes**	
10.16	Enable memory leak listener	**Yes**	
10.17	Setting Security Lifecycle Listener	**Yes**	
10.18	Use the logEffectiveWebXml and metadata-complete settings for deploying applications in production	**Yes**	
10.19	Ensure Manager Application Passwords are Encrypted	**Yes**	This item is referring to the manager application. We completely disable the manager application, so this rule is not applicable.

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