FORTINET

Endpoint Posture Check

FortiOS 7.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 13, 2022
FortiOS 7.2 Endpoint Posture Check
01-720-792162-20220713

TABLE OF CONTENTS

Endpoint posture check

The following are different context-based posture checks that FortiClient EMS supports as part of the Zero Trust solution:

Recommended posture checks

For vulnerable devices, checking for devices with high-risk vulnerabilities and above is recommended.

Rule type	Posture check	Supported operating systems
Vulnerable devices	Critical	Windows, macOS, Linux
	High or higher	Windows, macOS, Linux
	Medium or higher	Windows, macOS, Linux
	Low or higher	Windows, macOS, Linux
Antivirus (AV) software	AV software is installed and running. For Windows, this feature supports third party AV applications. For macOS and Linux, this feature can only check if FortiClient AV protection is enabled and does not recognize third party AV applications.	Windows, macOS, Linux
	AV signature is up-to-date	Windows, macOS, Linux
Windows security	Windows Defender is enabled	Windows
	Bitlocker Disk Encryption is enabled	Windows
	Exploit Guard is enabled	Windows
	Application Guard is enabled	Windows
	Windows Firewall is enabled	Windows
Security	FileVault Disk Encryption is enabled	macOS
EMS management	FortiClient installed and Telemetry is connected to EMS	Windows, macOS, Linux, iOS, Android
Common vulnerabilities and exposures (CVE)	Presence of [CVE]	Windows, macOS, Linux, iOS, Android
Firewall threat	Presence of [Firewall threat ID]	Windows, macOS, Linux, iOS, Android

Other posture checks

Rule type	Posture check	Supported operating systems
Active Directory (AD) group	Member of [AD Group]	Windows, macOS
Certificate	Certificate contains [Subject CN] and [Issuer CN]	Windows, macOS, Linux
File	Presence of [File]	Windows, macOS, Linux
IP range	Device in the [IP Range]	Windows, macOS, Linux, IOS, Android
Logged in domain	Member of [Domain]	Windows, macOS
On-Fabric status	On-Fabric	Windows, macOS, Linux, IOS, Android

Rule type	Posture check	Supported operating systems
OS version	Windows Server 2022	Windows
	Windows Server 2019	Windows
	Windows Server 2016	Windows
	Windows Server 2012 R2	Windows
	Windows Server 2012	Windows
	Windows Server 2008 R2	Windows
	Windows 11	Windows
	Windows 10	Windows
	Windows 8.1	Windows
	Windows 8	Windows
	Windows 7	Windows
	Mojave	macOS
	High Sierra	macOS
	Sierra	macOS
	Catalina	macOS
	Big Sur	macOS
	Monterey	macOS
	CentOS 7.5	Linux
	CentOS 7.4	Linux
	CentOS 8	Linux
	Red Hat 7.6	Linux
	Red Hat 7.5	Linux
	Red Hat 7.4	Linux
	Red Hat 8	Linux
	Red Hat 8.1	Linux
	Ubuntu 18.04	Linux
	iOS 9, 10, 11, 12, 13, 14	iOS
	Android 5, 6, 7, 8, 9, 10, 11	Android
Registry key	[Registry Key]	Windows

Rule type	Posture check	Supported operating systems
Running process	Presence of [Running Process]	Windows, macOS, Linux
Sandbox detection	Sandbox detected malware in last 7 days	Windows, macOS
User identity	User-specified	Windows, macOS, Linux, iOS, Android
	Social network login	Windows, macOS, Linux, iOS, Android
	Verified user	Windows, macOS, Linux, iOS, Android

Change log

Date	Change Description
2022-03-31	Initial release.
2022-04-27	Updated for FortiClient EMS 7.0.4.
2022-07-13	Updated for FortiClient EMS 7.0.6.

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.