Platforms supported by CIS, USGCB, and FDCC checks

Whether you work for a United States government agency, a company that does business with the federal government, or a company with strict security rules, you may need to verify that your assets meet a specific set of configuration standards. For example, your company may require that all of your workstations lock out users after a given number of incorrect logon attempts.

Like vulnerability scans, configuration assessment scans are useful for gauging your security posture. They help to verify that your IT department is following secure configuration practices. Using Nexpose, you can scan your assets as part of a configuration assessment audit. A license-enabled feature called Policy Manager provides checks for compliance with several configuration standards. The following table lists and describes available types of Policy Manager checks and the platforms that you can scan with each type.

Some things to keep in mind:

- The types of Policy Manager checks available in your specific Nexpose installation depend on your license.

  For more information, see the topic ***Viewing, activating, renewing, or changing your license*** in the *Administer* section of Nexpose Help.
- Nexpose updates vulnerability and policy checks with every content update release, so the list of supported platforms is constantly expanding. We'll update this page every time we add new platforms.

  For more information, see the topic ***Managing online updates*** in the *Administer* section of Nexpose Help.

Where can you get more information about Policy Manager checks?

See the topic ***Performing configuration assessment*** in Nexpose Help.

Types of checks	Description	Platforms that you can scan
USGCB 2.0 policies	The United States Government Configuration Baseline (USGCB) is an initiative to create security configuration baselines for information technology products deployed across U.S. government agencies. USGCB 2.0 evolved from FDCC (see below), which it replaces as the configuration security mandate in the U.S. government. Companies that do business with the federal	• Windows Vista • Windows XP • Windows Vista Firewall • Windows XP Firewall • Internet Explorer 7

	government or have computers that connect to U.S. government networks must conform to USGCB 2.0 standards. For more information, go to usgcb.nist.gov.	
USGCB 1.0 policies	USGCB 2.0 is not an update of 1.0. The two versions are considered separate entities. For that reason, the application includes USGCB 1.0 checks in addition to those of the later version. For more information, go to usgcb.nist.gov.	• Windows 7 • Windows 7 Firewall • Internet Explorer 8
FDCC policies	The Federal Desktop Core Configuration (FDCC) preceded USGCB as the U.S. government-mandated set of configuration standards. For more information, go tohttp://fdcc.nist.gov/fdcc.nist.gov.	• Windows Vista • Windows XP • Windows Vista Firewall • Windows XP Firewall • Internet Explorer 7
CIS benchmarks	These benchmarks are consensus-based, best-practice security configuration guidelines developed by the not-for-profit Center for Internet Security (CIS), with input and approval from the U.S. government, private-sector businesses, the security industry, and academia. The benchmarks include technical control rules and values for hardening network devices, operating systems, and middleware and software applications. They are widely held to be the configuration security standard for commercial businesses. For more information, go tohttp://fdcc.nist.gov/www.cisecurity.org.	• Red Hat Enterprise Linux 4 • Red Hat Enterprise Linux 5 • Red Hat Enterprise Linux 6 CIS Windows 2008 v1.2.0.9 • CIS Windows 2008 Enterprise Domain Controller • CIS Windows 2008 Enterprise Member Server • CIS Windows 2008 Specialized Security (Limited Functionality) Domain Controller • CIS Windows 2008 Specialized Security (Limited Functionality) Member Server CIS Windows 7 v1.2.0.2 • CIS Windows 7 Enterprise Disktop • CIS Windows 7 Enterprise Laptop • CIS Windows 7 Specialized Security (Limited Functionality) Desktop • CIS Windows 7 Specialized Security (Limited Functionality) Laptop CIS Windows XP v2.0.1.14 • CIS Windows XP Enterprise Desktop (Domain)

		• CIS Windows XP Enterprise Desktop (Standalone) • CIS Windows XP Enterprise Mobile (Domain) • CIS Windows XP Enterprise Mobile (Standalone) • CIS Windows XP Legacy (Domain) • CIS Windows XP Legacy (Standalone) • CIS Windows XP NIST Enterprise • CIS Windows XP NIST Legacy • CIS Windows XP NIST Specialized • CIS Windows XP Specialized Security (Domain) • CIS Windows XP Specialized Security (Standalone) CIS Windows 2003 v2.0.0.7 • CIS Windows 2003 Enterprise (Domain Controller) • CIS Windows 2003 Enterprise (Member Server) • CIS Windows 2003 Legacy (Domain Controller) • CIS Windows 2003 Legacy (Member Server) • CIS Windows 2003 Special (Domain Controller) • CIS Windows 2003 Special (Member Server)