SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-128 – Guide for Security-Focused Configuration Management of Information Systems

NIST SP 800-128 is NIST's guide to security-focused configuration management (SecCM): planning, secure baselines, configuration change control, and monitoring for systems.

What it is

NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, explains how to manage the configuration of systems so that they reach and keep a secure state. It introduces the term security-focused configuration management (SecCM) to distinguish the security aspects of configuration management from its broader engineering and operational uses, and it organizes SecCM into four phases: planning, identifying and implementing configurations, controlling configuration changes, and monitoring.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Original edition with errata update of October 10, 2019
EFFECTIVE August 2011	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: https://csrc.nist.gov/pubs/sp/800/128/upd1/final

Why it matters

- **Establish secure baselines** Each system has an approved baseline configuration that represents the most secure state consistent with its operational requirements.
- **Control change before it happens** Changes are identified, proposed, reviewed, analyzed for security impact, tested, and approved before implementation, so drift is prevented rather than discovered.
- **Support NIST SP 800-53 and the RMF** The guide provides the process behind the CM controls and feeds the monitoring step of the Risk Management Framework.
- **Automate assessment** Guidance on SCAP-validated tools lets organizations check configurations against baselines and checklists at scale.

How SmartSuite supports NIST SP 800-128

SecCM Control Library

Hold the four phases, the NIST SP 800-53 CM controls, and each system's SecCM plan as structured records with implementation status.

Ownership, Cadence, and Accountability

Assign system owners, security officers, and Configuration Control Board members, and schedule baseline reviews and monitoring cycles.

Evidence Collection and Audit Trail

Record change requests, security impact analyses, approvals, test results, and baseline versions with timestamps and reviewers.

Baseline Testing and Verification

Log SCAP and manual assessment results against approved baselines and track deviations to closure.

Risk and Vendor Alignment

Connect configuration items and changes to the risks, vendors, and systems they affect for security impact analysis.

Configuration Compliance Reporting

Generate status views of baseline compliance, open changes, and unauthorized change findings for leadership and auditors.

Common framework mappings

NIST 800-53 Rev.5 | NIST 800-53B Rev. 5 | NIST 800-37 Rev.2 | NIST CSF 2.0 | NIST 800-171 Rev. 3 | CIS Controls v8.1 | ISO 27002:2022 | ITIL 4 | COBIT 2019

Official resources

NIST SP 800-128 publication page

The NIST Computer Security Resource Center record for the guide and its October 2019 update, with status, abstract, keywords, and authors.

csrc.nist.gov/pubs/sp/800/128/upd1/final

NIST SP 800-128 (PDF, includes updates as of October 10, 2019)

The full text of the guide, including the errata table, the four SecCM phases, and the plan, change request, CCB charter, and impact analysis templates in the appendices.

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

NIST SP 800-53 Rev. 5 publication page

The control catalog whose Configuration Management (CM) family NIST SP 800-128 supports.

csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST National Checklist Program

The NIST program that publishes common secure configuration checklists referenced by the guide as the basis for baseline configurations.

nist.gov/programs-projects/national-checklist-program

Frequently asked questions

What is NIST SP 800-128?

NIST SP 800-128 is the Guide for Security-Focused Configuration Management of Information Systems, published by NIST in August 2011 and updated with errata in October 2019. It describes how to plan configuration management, establish secure baseline configurations, control changes to them, and monitor systems so that they stay in a secure state.

What does security-focused configuration management (SecCM) mean?

SecCM is the term NIST uses for the information security aspects of configuration management. General configuration management tracks and controls all changes to a system; SecCM concentrates on the settings, software, patches, and architecture that determine the system's security state and on analyzing the security impact of every change.

What are the four phases of SecCM in NIST SP 800-128?

Planning, which produces the SecCM policy, plan, roles, and tools; identifying and implementing configurations, which establishes the approved secure baseline; controlling configuration changes, which runs each change through request, security impact analysis, testing, and approval; and monitoring, which assesses systems against their baselines and reports unauthorized change.

How does NIST SP 800-128 relate to NIST SP 800-53?

It is the implementation guide for the Configuration Management (CM) control family in NIST SP 800-53. Controls such as CM-2 baseline configuration, CM-3 configuration change control, CM-4 impact analyses, and CM-6 configuration settings describe what is required; NIST SP 800-128 describes how to do it and supplies templates.

Is NIST SP 800-128 mandatory?

NIST guidelines are expected practice for U.S. federal agencies meeting FISMA requirements, and contractors handling controlled unclassified information meet related configuration management requirements in NIST SP 800-171. For other organizations it is voluntary and is often adopted because it aligns with CIS Controls, ISO/IEC 27002, and ITIL configuration practices.

What changed in the October 2019 update to NIST SP 800-128?

The 2019 errata update added an abstract and keywords, replaced the term information system with system throughout, updated the FISMA citation to the Federal Information Security Modernization Act of 2014, aligned role acronyms with current NIST terminology, and made other editorial corrections. The four-phase process and the appendices were unchanged.

What is SCAP and why does NIST SP 800-128 cover it?

The Security Content Automation Protocol is a set of specifications that let tools express and check configuration settings, vulnerabilities, and patches in a standard way. Chapter 3 explains how SCAP-validated tools can automate the assessment of systems against baselines and checklists, which makes SecCM monitoring practical at scale.

License included / downloadable: Yes NIST SP 800-128 is a U.S. government publication available free of charge from NIST, and its SecCM phases and templates are included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-128-security-focused-configuration-management-of-information-systems