

Security Configuration Checklists

For IT Products Program

Checklist Description

Version 2.1

Organization

IT Product & Version

Checklist Name & Version

Date

Please complete the following information and return this document to:

checklists@nist.gov.

| Field Name | Description | Example Data |
| --- | --- | --- |
| Checklist Name | The name of the checklist. |  |
| Checklist ID | Uniquely identifies the checklist in the NCP repository. This will be generated during the NCP submission process and assigned to the checklist. | *Will be populated by NIST.* |
| Version | The version or release number of the checklist. |  |
| Review Status | The status of the checklist within the internal NCP review process. A status of "Final" signifies that NCP has reviewed the checklist and has accepted it for publication within the program. Possible status options are: Candidate, Final, Archived, or Under Review. | *Will be populated by NIST.* |
| Entry Date | States the date when the checklist record was first listed in the NCP repository, in the format MM/DD/YYYY. | *Will be populated by NIST.* |
| Publication Date | States the date when the actual checklist document was published, in the format MM/DD/YYYY |  |
| Last Modified Date | States the date when the checklist record was last revised within the NCP repository, in the format MM/DD/YYYY. | *Will be populated by NIST.* |
| Product Category | The main product category of the IT product (e.g., firewall, IDS, operating system, web server). |  |
| Target  | The set of specific IT systems or applications that the checklist provides guidance for. |  |
| CPE Name | The CPE representation of a specific Target. |  |
| Checklist Role | The primary use or function of the IT product as described by the checklist (e.g., client desktop host, web server, bastion host, network border protection, intrusion detection). |  |
| Checklist Summary | Summarizes the purpose of the checklist and its settings. |  |
| Known Issues | Summarizes issues that may arise after application of the checklist to help users pinpoint any functional and operational problems caused by the checklist. |  |
| Audience | The intended audience that should be able to install, test, and use the checklist, including suggested minimum skills and knowledge required to correctly use the checklist. |  |
| Target Operational Environment | The IT product’s operational environment, such as Standalone, Managed, or Custom (with description, such as Specialized Security-Limited Functionality, Legacy, or United States Government). Generally only applicable for security compliance/vulnerability checklists. |  |
| Checklist Type | The type of checklist, such as Compliance, Vulnerability, and Specialized. |  |
| Checklist Installation Tools | Describes the functional tools required to use the checklist to configure the system, if they are not included with the checklist. |  |
| FIPS 140-2 Compliance | Whether the product can operate in a FIPS 140-2 validated mode (yes or no). |  |
| Regulatory Compliance | Whether the checklist is consistent with various regulations and standards (e.g., Health information Portability and Accountability Act [HIPAA], Gramm-Leach-Bliley Act [GLBA], FISMA [such as mappings to NIST SP 800-53 controls], ISO 27001, Sarbanes-Oxley, Department of Defense [DoD] 8500, Federal Risk and Authorization Management Program [FedRAMP], Committee on National Security Systems Instruction [CNSSI] 1253, Control Objectives for Information and Related Technologies [COBIT] 5, the NIST Cybersecurity Framework, the Center for Internet Security [CIS] Controls). |  |
| Authority  | The organization responsible for producing the original security configuration guidance represented by the checklist. Authorities are ranked according to their “Authority Type.” Within the NCP website, authorities are grouped with their authority types through the syntax of Authority Type: Authority. |  |
| Authority Type  | Type of organization that lends its authority to the checklist. The three types are Governmental Authority, Software Vendor, and Third Party (e.g., security organizations).  |  |
| Author  | The organization responsible for creating the checklist in its current format. In most cases an organization will represent both the author and authority of a checklist, but this is not always true. For example, if an organization produces validated SCAP content for a NIST publication, the organization that created the SCAP content will be listed as the Author, but NIST will remain the Authority |  |
| Rollback Capability | Whether the changes in product configuration made by applying the checklist can be rolled back and, if so, how to roll back the changes. |  |
| Testing Information | Platforms on which the checklist was tested. Can include any additional testing-related information such as summary of testing procedures used. Should specify any operational testing performed in production or mirrored production environments. |  |
| Comments, Warnings, Miscellaneous | Any additional information that the checklist developer wishes to convey to users. |  |
| Disclaimer | Legal notice pertaining to the checklist. |  |
| Product Support | Vendor will accept support calls from users who have applied this checklist on their IT product; warranty for the IT product has not been affected. Required for usage of NCP logo if the submitter is the product vendor. If the submitter is not the product vendor, the submitter should describe any agreement that they may have with the product vendor. |  |
| Point of Contact  | An email address where questions, comments, suggestions, and problem reports can be sent in reference to the checklist. The point of contact should be an email address that the checklist developer monitors for checklist problem reports.  |  |
| Sponsor  | States the name of the IT product manufacturer organization and individuals who sponsor the submitted checklist if it is submitted by a third-party entity. |  |
| Licensing  | States the license agreement (e.g., the checklist is copyrighted, open source, General Public License [GPL], free software, shareware). |  |
| SCAP Content  | A link to the machine-readable content representing the configuration guidance. This guidance is expressed using SCAP. |   |
| Supporting Resource  | A link to any supporting information, or content, relating to the guidance. This field can hold data ranging from an English prose representation of the actual guidance, to configuration scripts that apply guidance specific settings on a target. |  |
| Resource Description  | A prose description of the resource.  |  |
| Resource Type  | The format of the resource. Examples include SCAP content, prose, GPOs, security templates, etc.  |  |
| SHA-256  | The SHA-256 hash for the resource.  |  |
| Change History  | Running log detailing any changes made to the checklist since its inclusion in the repository. This field is updated with each version of the checklist.  |  |
| Dependency/ Requirement  | Indicate that another checklist or guide is required to properly use and implement the current checklist.  |  |
| References  | Any supporting references chosen by the developer that were used to produce the checklist or checklist documentation. |  |