# **Configuration Annex** to the

# Protection Profile for General Purpose Operating Systems

Annex Release 1
For Protection Profile Version 4.2

**22 May 2018**

# 1. Purpose

This Configuration Annex to the Protection Profile (PP) for General Purpose Operating Systems provides configuration requirements for operating systems. This Annex is consistent with [CNSSI-1253], which requires US National Security Systems to adhere to certain configuration parameters. Accordingly, configuration guidance produced according to the requirements of this Annex is suitable for use in US National Security Systems.
These configuration requirements serve the following audiences:

| Audience | Purpose |
|---|---|
| IT Product Vendors | Use these guidelines to structure the creation of product-specific configuration guidance produced as part of a Common Criteria evaluation. The creation of administrative guidance is required by NIAP-approved Protection Profiles. The items specified in this document, as well as any best practices, should be provided as part of the administrative guidance. For each configuration item, the guidance must include the steps necessary to configure the setting of the product. |
| Test Labs | Use these guidelines to configure and test systems undergoing evaluation against a NIAP-approved Protection Profile. Using this guidance during evaluation provides assurance that the guidance is correct and implementable. |
| Network Owners and Assessors | Use these guidelines to assess the configuration of operational systems when product-specific guidance does not exist. |

## 1.1 Relationship to NIST Risk Management Framework

In order to implement security controls from the NIST Risk Management Framework, each component of the information system must possess the necessary security functionality and also be properly configured to leverage that functionality.

NIAP Protection Profiles express requirements for security functionality for individual IT products within the overall information system. This includes management functions which indicate where an enterprise or end user is expected to be able to operationally configure the product. However, the Protection Profile does not indicate specific values for each configuration setting. This Annex specifies those specific requirements for operational configuration of a product type. It also provides a mapping to each NIST control which the operational setting helps the overall system implement. This complements the control mapping provided with each Protection Profile, which is focused on security functionality. Together, these documents support the creation of system security plans, as well as the Select, Implement, Assess, and Monitor steps of the Risk Management Framework (RMF).

# 2. Configuration Requirements

The table below describes configuration requirements for operating systems.

Each configuration requirement is associated with a security functionality requirement (SFR) from the associated Protection Profile or Module. Each configuration requirement is also associated with a NIST 800-53 security control and CNSSI 1253 configuration value where applicable. See Wireless EP/Module for wireless-specific configuration requirements.

| Configuration Action | NIST Control | CNSSI 1253 Value or DoD-specific Value | NIAP PP Reference |
|---|---|---|---|
| Configure Minimum Password Length to 12 Characters | IA-5 (1)(a) | 12 characters | FMT_MOF_EXT.1 |
| Require at Least 1 Special Character in Password | IA-5 (1)(a) | at least one | FMT_MOF_EXT.1 |
| Require at Least 1 Numeric Character in Password | IA-5 (1)(a) | at least one | FMT_MOF_EXT.1 |
| Require at Least 1 Uppercase Character in Password | IA-5 (1)(a) | at least one | FMT_MOF_EXT.1 |
| Require at Least 1 Lowercase Character in Password | IA-5 (1)(a) | at least one | FMT_MOF_EXT.1 |
| Enable Screen Lock | AC-11a. |  | FMT_MOF_EXT.1 |
| Set Screen Lock Timeout Period to 30 Minutes or Less | AC-11a. | 30 minutes | FMT_MOF_EXT.1 |
| Disable Unauthenticated Login (such as Guest Accounts) |  |  | FIA_AFL.1 |
| Set Maximum Number of Authentication Failures to 3 Within 15 Minutes | AC-7a. | 3<br>15 minutes | FMT_MOF_EXT.1 |
| Enable Host-Based Firewall | SC-7 (12) |  | FMT_MOF_EXT.1 |
| Configure Name/Address of Remote Management Server From Which to Receive Config Settings | CM-3(3) |  | FMT_MOF_EXT.1 |
| Configure the System to Offload Audit Records to a Log Server | AU-4(1) |  | FAU_GEN.1.1.c |
| Set Logon Warning Banner | AC-8a. | *see text below* | FMT_MOF_EXT.1 |
| Audit All Logons (Success/Failure) and Logoffs (Successful) | AU-2a. | Authentication events:<br>(1) Logons (Success/Failure)<br>(2) Logoffs (Success) | FAU_GEN.1.1.c |
| Audit File and Object Events (Unsuccessful) | AU-2a. | File and Objects events:<br>(1) Create (Success/Failure)<br>(2) Access (Success/Failure)<br>(3) Delete (Success/Failure)<br>(4) Modify (Success/Failure)<br>(5) Permission Modification (Success/Failure)<br>(6) Ownership Modification (Success/Failure) | FAU_GEN.1.1.c |
| Audit User and Group Management Events (Success/Failure) | AU-2a. | User and Group Management events:<br>(1) User add, delete, modify, disable, enable (Success/Failure)<br>(2) Group/Role add, delete, modify (Success/Failure) | FAU_GEN.1.1.c |

|  |  |  |  |
|---|---|---|---|
| Audit Privilege or Role Escalation Events (Success/Failure) | AU-2a. | Privilege/Role escalation (Success/Failure) | FAU_GEN.1.1.c |
| Audit All Audit and Log Data Accesses (Success/Failure) | AU-2a. | Audit and log data access (Success/Failure) | FAU_GEN.1.1.c |
| Audit Cryptographic Verification of Software (Success/Failure) | AU-2a. |  | FAU_GEN.1.1.c |
| Audit Program Initiations (Success/Failure) | AU-2a. | Application (e.g., Firefox, Internet Explorer, MS Office Suite, etc.) initialization (Success/Failure) | FAU_GEN.1.1.c |
| Audit System Reboot, Restart, and Shutdown Events (Success/Failure) | AU-2a. | System reboot, restart and shutdown (Success/Failure) | FAU_GEN.1.1.c |
| Audit Kernel Module Loading and Unloading Events (Success/Failure) | AU-2a. |  | FAU_GEN.1.1.c |
| Enable Automatic Software Update | SI-2 |  | FMT_MOF_EXT.1 |

## Logon Banner Text

**For DoD Systems:**
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

**For non-DoD NSS:**
*organization-defined system use notification message or banner*

# 3. References

| Identifier | Title |
|---|---|
| [CC] | Common Criteria for Information Technology Security Evaluation -<br>• Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.<br>• Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.<br>• Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017. |
| [CNSSI-1253] | Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, 27 March 2014. |