# Commercial Solutions for Classified (CSfC) Selections for General Purpose Operating System

## Overview

Transport Layer Security (TLS) Protected Server products (as defined in the Mobile Access (MA) Capability Package (CP) and Campus WLAN CP) used in Commercial Solutions for Classified (CSfC) solutions shall be validated by National Information Assurance Partnership (NIAP)/Common Criteria Evaluation and Validation Scheme (CCEVS) or Common Criteria Recognition Arrangement (CCRA) partnering schemes as complying with the current requirements of NIAP Protection Profile for General Purpose Operating System Version 4.2 and this validated compliance shall include the selectable requirements contained in this document.

Please provide questions, comments on usability, applicability, and/or shortcomings to the CSfC Program (csfc@nsa.gov).

## Notes

## Document Conventions

The conventions used in descriptions of the document are as follows:

- Assignment completed within a selection in the PP: the completed assignment text is indicated with *italicized and underlined text* (i.e., CSfC mandatory completed assignments/selections unless otherwise indicated by the text "at least one of the following underlined selections")
- Assignment partially completed in the PP: indicated with *italicized text*
- Refinement text is indicated with ~~strikethroughs~~
- Additional clarifying text or CSfC specific language is indicated with `light blue Courier New Text`
- Links to sources, additional information, and email addresses are indicated with blue underlined text.

## Protection Profile for General Purpose Compute Platform Selections

**Use Case**
Use Case 1 End User Devices

**FMT_SMF_EXT.1.1**

| Management Function | Administrator | User |
|---|---|---|

| | | |
|---|---|---|
| Enable/disable [selection: *screen lock*, *session timeout*] | X | ~~O~~ X |
| Configure [selection: *screen lock*, *session*] inactivity timeout | X | ~~O~~ X |
| Configure local audit storage capacity | ~~O~~ X | ~~O~~ X |
| Configure minimum password length | ~~O~~ X | ~~O~~ X |
| Configure minimum number of special characters in password | ~~O~~ X | ~~O~~ X |
| Configure minimum number of numeric characters in password | ~~O~~ X | ~~O~~ X |
| Configure minimum number of uppercase characters in password | ~~O~~ X | ~~O~~ X |
| Configure minimum number of lowercase characters in password | ~~O~~ X | ~~O~~ X |
| Configure lockout policy for unsuccessful authentication attempts through [selection: *timeouts between attempts*, *limiting number of attempts during a time period*] | ~~O~~ X | ~~O~~ X |
| Configure host-based firewall | ~~O~~ X | ~~O~~ X |
| Configure name/address of directory server with which to bind | O | O |
| Configure name/address of remote management server from which to receive management settings | O | O |
| Configure name/address of audit/logging server to which to send audit/logging records | ~~O~~ X | ~~O~~ X |
| Configure audit rules | ~~O~~ X | ~~O~~ X |
| Configure name/address of network time server | O | O |
| Enable/disable automatic software update | O | O |
| Configure WiFi interface | ~~O~~ X | ~~O~~ X |
| Enable/disable Bluetooth interface | ~~O~~ X | ~~O~~ X |

| | | |
|---|---|---|
| Enable/disable [assignment: *list of other external interfaces*] | O | O |
| [assignment: *list of other management functions to be provided by the TSF*] | O | O |

**FAU_GEN.1.1**

a. Start-up and shut-down of the audit functions;

b. All auditable events for the **not specified** level of audit; and

c.

- Authentication events (Success/Failure);
- Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes);
- Privilege or role escalation events (Success/Failure);
- [selection:
  - *File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions),*
  - *User and Group management events (Successful and unsuccessful add, delete, modify, disable, enable, and credential change),*
  - *Audit and log data access events (Success/Failure),*
  - *Cryptographic verification of software (Success/Failure),*
  - *Attempted application invocation with arguments (Success/Failure e.g. due to software restriction policy),*
  - System reboot, restart, and shutdown events (Success/Failure),
  - *Kernel module loading and unloading events (Success/Failure),*
  - *Administrator or root-level access events (Success/Failure),*
  - [assignment: other specifically defined auditable events].

  ]