PP-Configuration for Enterprise Server Applications

Table of Contents

Acknowledgements

This PP-Configuration was developed by the iTC for Application Software international Technical Community (iTC) also known as AppSW-iTC with representatives from Industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

Revision History

Table 1. Revision history

Version	Date	Description
1.0	2022-04-06	Initial Release
1.0e	2024-02-15	Incorporated feedback received following initial release.

1. Introduction

1.1. PP-Configuration Overview

The purpose of a PP-Configuration is to combine Protection Profiles (PPs) and PP-Modules for various technology types into a single configuration that can be evaluated as a whole.

This PP-Configuration is for enterprise server applications.

1.2. PP-Configuration Reference

This PP-Configuration is identified as follows:

- PP-Configuration for Enterprise Server Applications, Version 1.0e, 2024-02-15
- As a shorthand reference, it can be identified as "CFG_APP-Server_V1.0e""

1.3. PP-Configuration Components

This PP-Configuration includes the following components:

Table 2. PP-Configuration Components

[base PP]	cPP_APP_SW_V1.0
[PP-Module 1]	MOD_Server_v1.0

2. Conformance Claims

2.1. CC Statement

To be conformant to this PP-Configuration, an ST must demonstrate Exact Conformance, as defined by the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs.

2.2. CC Conformance Claims

This PP-Configuration, and its components specified in section 1.3, are conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

3. SAR Statement

The set of SARs specified for this PP-Configuration are taken from, and identical to, those specified in the base PP.

3.1. Related Documents

Common Criteria[1]

Table 3. Common Criteria References

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.

[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017.
[addenda]	CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, May 2017.

[1] For details see http://www.commoncriteriaportal.org/