Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2

Version 1.0, 1 July 2025

Document reference: AISEP-CC-CR-2025-EFT-T043-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary

This report describes the findings of the IT security evaluation of the EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2 appliances against a Common Criteria approved Protection Profile (PP).

The Target of Evaluation (TOE) is a suite of network appliances designed to capture an entire history of network traffic for offline analysis and investigation. It is a family of non-virtual and non-distributed network devices. Each device is a complete network appliance that includes all software, hardware, and security guidance constituting the TOE. The TOE also allows recording and storage of the entire access history of a network for detailed monitoring and forensic analysis.

This report concludes that the TOE has complied with the following PP [4]:

- *Collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23 March 2020. (CPP_ND_V2.2E)*

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs with the final Evaluation Technical Report (ETR) submitted on 19 June 2025.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends that administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- verify the hash of any downloaded software, as present on the Endace website
- the system auditor should review the audit trail generated and exported by the TOE periodically
- the administrator should update the device firmware and software in timely manners in response to the release of product updates due to known vulnerabilities.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria [1,2,3] and Protection Profile [4].
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [8], which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2
Software version	v7.2
Hardware platforms	EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5
Security Target	*Security Target EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2, Version 1.0, Dated 26 June 2025*
Evaluation Technical Report	*Evaluation Technical Report, EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2, Version 1.0, Dated 19 June 2025 (Document reference EFT-T043-ETR 1.0)*
Criteria	*Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5*
Methodology	*Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5*

Conformance	*Collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23 March 2020. (CPP_ND_V2.2E)*
Developer	Endace Measurement Systems Ltd Building C, Level 1 602 Great South Road, Ellerslie, Auckland 1051 New Zealand
Evaluation facility	Teron Labs Level 2, 14 Moore St, Canberra ACT 2601 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The Target of Evaluation (TOE) is the EndaceProbe EP Series running Endace OSm v7.2, a suite of non-virtual and non-distributed network appliances designed for 100% packet recording, storage and forensic analysis. These appliances provide visibility into network activity, enabling Security Operations (SecOps), Network Operations (NetOps), and IT teams to monitor, investigate, and respond to performance issues and security incidents with high confidence and precision.

The TOE encompasses only the networking and security management functions of the EndaceProbe platform. While the appliances also offer advanced packet capture, storage, and analysis capabilities, those features are outside the scope of this definition and are not considered part of the TOE. The evaluated functionality is limited to the secure operation, configuration, and communication aspects of the network device itself.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.3 of the Security Target [8].

TOE Physical Boundary

The TOE is the complete network appliance consisting of Endace OSm v7.2 software running on the EndaceProbe EP Series platforms. The TOE is physically bound by the hardware chassis of the following appliances: EP-92C8-G4, EP-94C8-G5, EP-2184-G5, and EP-2144-G5. Each of these appliances is a standalone, non-virtual, non-distributed system that includes all hardware, firmware, operating system components, and pre-installed software necessary to constitute the TOE.

The TOE software is deployed in an ISO package file and includes CentOS v7.9 Linux operating system with kernel version 5.14.0, integrated with Endace's proprietary packet capture and analysis software, as well as embedded cryptographic modules provided via Endace Crypto Firmware v2.1. All cryptographic operations are performed using CAVP-validated algorithms through wolfSSL v5.6.4 with WolfCrypt v5.2.1.

The TOE also integrates third-party components including:

- Apache Server 2.4.34
- OpenSSH 7.4
- wolfSSL 5.6.4 with WolfCrypt 5.2.1

The TOE software is delivered as an ISO image and deployed directly onto the physical hardware during provisioning. No components outside of the appliance chassis are considered part of the TOE boundary. External management stations, while used to interface with the TOE, are not included within the TOE boundary.

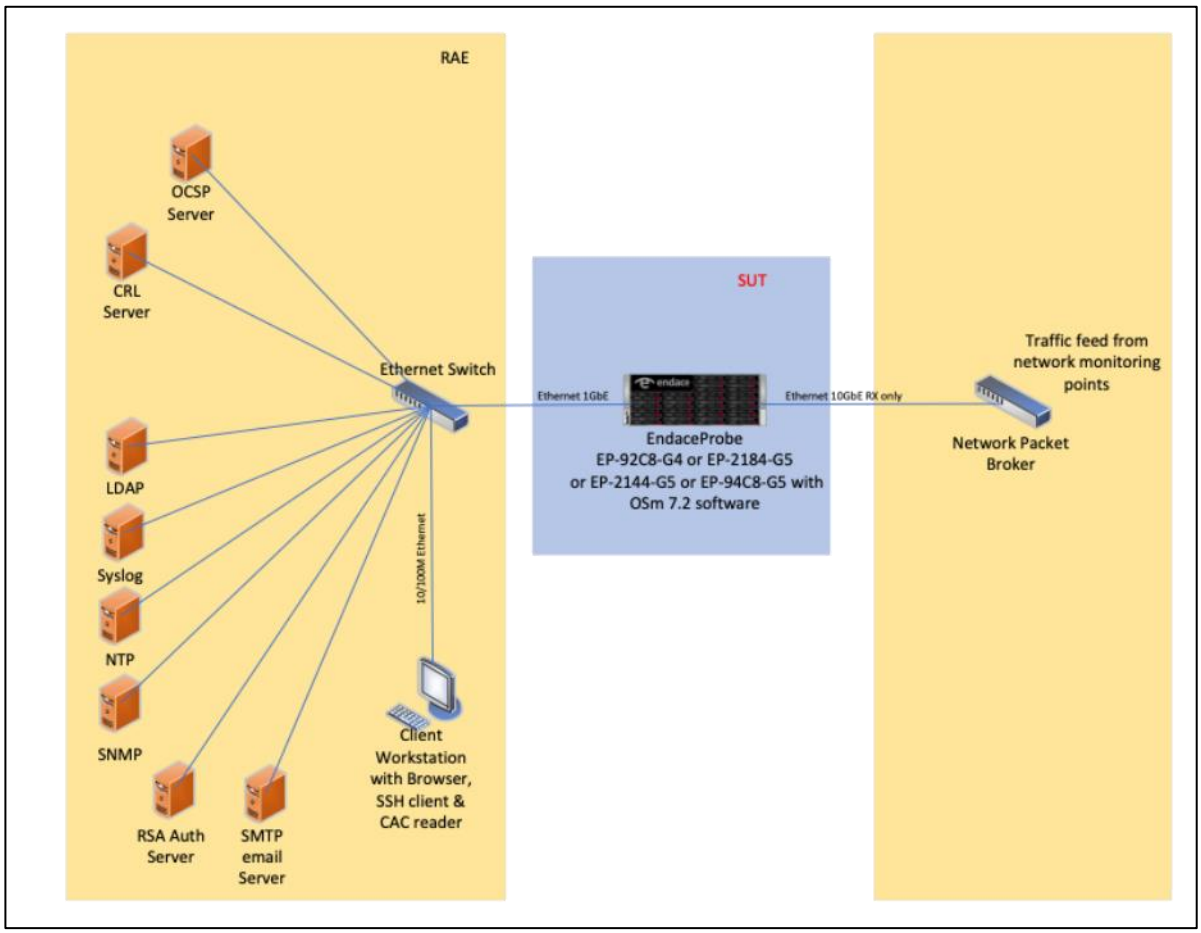
The TOE parts included in the physical boundary described as below:

Part of the TOE	Identification	Description
TOE Hardware	EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5	The hardware platform, the interfaces, and the casing of the TOE. Includes the processor, the memories, and the persistent storage.
TOE Software	Endace OSm v7.2	The software included in the TOE. The TOE software is distributed factory installed.
Security Guidance	*Common Criteria Guidance Supplement EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm 7.2.1 (EDM09-192) Version 1.8, Published February 2025*	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.

Architecture

The TOE is the EndaceProbe EP Series appliance models EP-92C8-G4, EP-94C8-G5, EP-2184-G5, and EP-2144-G5 running Endace OSm v7.2. Each appliance is a self-contained, non-virtualised hardware platform designed to provide lossless, high-precision packet capture and storage. The TOE is positioned between a network packet broker and a secure administrative environment. It receives mirrored traffic via a dedicated Ethernet interface from the packet broker, enabling comprehensive recording of network activity for retrospective analysis and investigation.

The TOE Architecture is shown in the figure below.



Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [8].

Evaluated Functionality

Functional tests performed during the evaluation were taken from the Protection Profile [4] and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

Non-TOE Hardware/Software/Firmware

The TOE is the entire network appliance. Yet, it does require external IT devices to be properly operated. Specifically, the TOE requires the following items in the network environment:

- Syslog server supporting SSHv2 connections to send audit logs
- SSHv2 client for remote administration
- serial connection client for local administration

- The administrator may configure the TOE to acquire time from an NTP Server, but the NTP Server is not part of the TOE.
- The TOE may connect to an RSA SecurID, but the SecurID is not part of the TOE.
- The user of the TOE may deploy a set of analytics tools and there are no restrictions of which tools may be used. None of those tools are part of the TOE.
- Application Dock, InvestigationManager, EndaceCMS, and an external installation of Wireshark may be utilised at the user's discretion but are not part of the TOE.
- The TOE establishes secure connections to external Certificate Revocation Lists (CRL) Server and Online Certificate Status Protocol (OCSP) responder to verify the revocation status of the X.509 certificates. However, The CRL server and OCSP responder are not part of the TOE.

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [5] for policy relating to using an evaluated product in an unevaluated configuration.

The following components are considered outside of the scope of the TOE:

- use of telnet, since it violates the Trusted Path requirement set
- HTTP must not be used. It is not considered secure and violates the trusted path and trusted channel requirements.
- use of File Transfer Protocol and TFTP, since it violates the Trusted Path requirement set
- use of Simple Network Management Protocol, since it violates the Trusted Path requirement set
- RADIUS and TACACS+ are not considered secure and must not be used.
- IPMI/iDRAC Interface is not considered secure and must not be used.
- Web proxy function is not considered secure and must be disabled.
- The web interface, the web client, and the GUI must not be used for administrative functions on the TOE.

Security

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The Security Target [8] contains a summary of the functionality that is evaluated.

Secure Delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform:

- shipping label - Ensure that the shipping label correctly identifies the correct customer name and address as well as the device
- outside packaging - Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device
- inside packaging - Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, they should immediately contact the supplier providing the order number, tracking number and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Endace and not a different company masquerading as Endace. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:

- verify that the device was ordered using a purchase order. Endace devices are never shipped without a purchase order
- when a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken.
- Verify that this e-mail notification was received and contains the following information:
  - purchase order number
  - Endace order number used to track the shipment
  - carrier tracking number used to track the shipment
  - list of items shipped including serial numbers
  - address and contacts of both the supplier and the customer
- verify that the shipment was initiated by Vendor, performing the following tasks:
  - compare the carrier tracking number of the Endace order number listed in the Endace shipping notification with the tracking number on the package received
  - compare the carrier tracking number or the Endace order number listed in the Endace shipment notification with the tracking number on the package received.

Installation of the TOE

The Configuration Guides [6] contains all relevant information for the secure configuration of the TOE.

Version Verification

The verification of the TOE is largely automatic, as demonstrated in testing. The TOE cannot load a modified software image. Authentic software images can be downloaded from vendor's website. In addition to the automated verification, the site includes individual hashes for each image. The administrator should verify the hash of the software before installing it into the hardware platform.

Documentation and Guidance

It is important that the TOE be used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. The evaluated configuration guide document for the Endace OSm 7.2.1 for EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 is available on the vendor website. The title is:

- *Common Criteria Guidance Supplement EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2814-G5, EP-2144-G5 with Endace OSm v7.2.1* [6].

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [5].

Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

The network device is assumed to be physically secured within its operational environment, protected from physical attacks that could compromise its security or interfere with its physical connections and correct operation. This level of protection is expected to be sufficient to safeguard the device and the sensitive data it handles.

The TOE is expected to provide networking functionality as its primary purpose and should not offer any general-purpose computing capabilities, such as running compilers or user applications unrelated to its networking functions. This ensures that the device remains focused solely on its intended security and networking roles.

The network device's administrator(s) are assumed to be trustworthy, acting in the best interests of the organisation's security. This includes being well-trained, adhering to established policies, and following all guidance documentation. Administrators are responsible for ensuring that passwords and credentials used within the TOE are strong and secure. The TOE is not expected to protect against a malicious administrator who deliberately seeks to bypass or compromise its security features.

The TOE's firmware and software are assumed to be regularly updated by an administrator, particularly in response to newly discovered vulnerabilities. This ensures that the TOE remains protected against emerging threats.

The credentials (such as private keys) used by administrators to access the TOE must be securely protected on any platform where they are stored. Administrators must also ensure that sensitive residual information, including cryptographic keys, keying material, PINs, and passwords, is not accessible to unauthorised individuals when networking equipment is discarded or removed from service.

The TOE is assumed to be connected to distinct networks in a way that ensures its security policies are enforced on all relevant network traffic flowing between these networks.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant Protection Profile [4] with the applicable Technical Decisions and *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* [3] and relevant Supporting Document [12].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [10].

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9] and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs* [13] were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the Protection Profile [4] and Supporting Document [12]. The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report [11]. CAVP certificate references, organised by the applicable Security Functional Component, are given in the Security Target [8].

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the NDcPP Supporting Document [12] that follow a flaw hypothesis methodology. Accordingly, four types of flaw hypotheses have been considered:

- Type 1 - public vulnerabilities
- Type 2 - ND-iTC (Network international Technical Community) sourced
- Type 3 - evaluation team generated
- Type 4 - tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the **05 May 2025** coinciding with the conclusion of the evaluation. There were no identifiable Type 2 hypotheses for this evaluation.

During functional testing of the TOE, the Evaluation team did not observe any behaviour that would point to anomalous functionality or vulnerability. The evaluation team also conducted tool-generated vulnerability testing of the TOE as per the Supporting Document [12]

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification is focused on the evaluation of product compliance with Protection Profile that cover the technology area of network devices. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the PP Supporting Document, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profile (PP). PPs provide assurance by providing a full Security Target, an analysis of the Security Functional Requirements in that Security Target, guidance documentation and a basic description of the architecture of the TOE.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [8] and **has met** the requirements of the Protection Profile CPP_ND_V2.2E [4.a] and the applicable Technical Decisions.

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of the EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [8] have met the requirements of all relevant Protection Profile [4].

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [5].

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends that users and administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled

- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the hash of any downloaded software, as present on the https://www.endace.com/ website
- the system auditor should review the audit trail generated and exported by the TOE periodically.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. Protection Profile:
    a) *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (CPP_ND_V2.2E)*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. *Common Criteria Guidance Supplement EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm 7.2.1 (EDM09-192) Version 1.8, Published February 2025*
7. *Evaluation Technical Report, EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2, Version 1.0, Dated 19 June 2025* (Document reference EFT-T043-ETR 1.0)
8. *Security Target EndaceProbe EP-92C8-G4, EP-94C8-G5, EP-2184-G5 and EP-2144-G5 with Endace OSm v7.2, Version 1.0, Dated 26 June 2025*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf
11. Entropy Documentation:
    a) *Entropy Report: EndaceProbe EP-92C8-G4, EP-2184-G5, EP-2144-G5 and EP-94C8-G5, Version 1.0, Dated 7 December 2023*
12. Protection Profile Supporting Document
    a) *Supporting Document, Evaluation Activities for Network Device cPP, Version 2.2, December-2019*
13. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
ASE	Advanced Encryption Standard
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CCRA	Common Criteria Recognition Arrangement
CEM	Common Criteria Evaluation Methodology
CLI	Command Line Interface
CRL	Certificate Revocation List
cPP	Collaborative Protection Profile
Gbps	Gigabits per second
GPS	Global Positioning System
iDRAC	intelligent Dell Remote Access Controller
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPv4	Internet Protocol version 4
ISO	International Organisation for Standardisation
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
NTP	Network Time Protocol
PP	Protection Profile
RSA	Rivest-Shamir-Adleman
SSH	Secure Shell
ST	Security target
TACACS	Terminal Access Controller Access-Control System

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate