Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Ad Noctem Connect 2.3

Version 1.0, 26 February 2026

Document reference: AISEP-CC-CR-2026-EFT-T053-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary **1**

Introduction **2**

Overview 2

Purpose 2

Identification 2

Target of Evaluation **4**

Overview 4

Description of the TOE 4

TOE Functionality 4

TOE Physical Boundary 4

Clarification of Scope 5

Security Policy 6

Secure Delivery 7

Version Verification 7

Documentation and Guidance 7

Secure Usage 7

Evaluation **9**

Overview 9

Evaluation Procedures 9

Functional Testing 9

Entropy Testing 9

Penetration Testing 9

Software Bill of Material (SBOM) assessment 9

Certification **11**

Overview 11

Assurance 11

Certification Result 11

Recommendations 11

Annex – References and Abbreviations 13

References 13

Abbreviations 14

Executive Summary

This report describes the findings of the IT security evaluation of Ad Noctem Connect 2.3 developed by Northrop Grumman Corporation against Common Criteria approved Protection Profiles (PPs).

The Target of Evaluation (TOE) is the Northrop Grumman Ad Noctem Connect. The TOE functions as a VPN client application designed to provide secure communications over untrusted networks. To achieve this, it implements the IKEv2/IPsec protocol suite. Configuration of the TOE is performed through a local, web-based management interface.

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

- *Protection Profile for Application Software, version 1.4, 07 October 2021 (PP_APP_V1.4)*
- *PP-Module for Virtual Private Network (VPN) Clients, version 2.4, 31 March 2022 (MOD_VPN_CLI_V2.4)*

Additionally, the above PPs can be grouped together using certified PP-Configurations. This evaluation used the following *PP-Configuration [4]:*

- *PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 (CFG_APP-VPNC_V1.3)*

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 04 February 2026.

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
- the system auditor should review the audit trail generated and exported by the TOE periodically.

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 [8]* 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 Profiles [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 the Ad Noctem Connect 2.3 by Northrop Grumman Corporation.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Ad Noctem Connect 2.3
Software version	2.3
Hardware platform	GB-100
Security Target	Security Target Ad Noctem Connect 2.3, Version 1.01, 25 February 2026
Evaluation Technical Report	Evaluation Technical Report 1.1, dated 26 February 2026 Document reference EFT-T053-ETR 1.1
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Extended, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	▪ Protection Profile for Application Software, version 1.4, 07 October 2021 (PP_APP_V1.4)

	▪ PP-Module for Virtual Private Network (VPN) Clients, version 2.4, 31 March 2022 (MOD_VPN_CLI_V2.4) ▪ PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 (CFG_APP-VPNC_V1.3)
Developer	Northrop Grumman Corporation 2980 Fairview Park Drive, Falls Church 22042, VA, USA
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 TOE is a secure VPN client appliance designed to establish trusted IPsec connections with a remote VPN Gateway located at the perimeter of a private network. The TOE operates as an IPsec peer using IKEv2 for cryptographic key exchange and relies on pre-configured, non-modifiable templates that define the IPsec and IKEv2 connection parameters. Users interact with the appliance only by physically connecting a laptop or PC and selecting a connection template, after which the TOE automatically establishes a secure communication channel over an untrusted network. This protected channel ensures confidentiality and integrity against eavesdroppers with access to the external network.

The TOE is delivered as a dedicated hardware appliance pre-provisioned with IPsec templates, pre-shared keys, and X.509v3 certificates. No administrative interfaces are available during operation, and any maintenance or configuration updates must be performed through the provisioning process. The TOE authenticates only the IPsec peers using either public-key cryptography validated by a trusted Certification Authority or pre-shared keys stored securely on the device. It does not perform human user authentication; this is handled by applications within the private network. The TOE's sole function is to provide a controlled, tamper-resistant mechanism for establishing secure VPN connectivity in remote or untrusted environments.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.4 of the *Security Target [8].*

TOE Physical Boundary

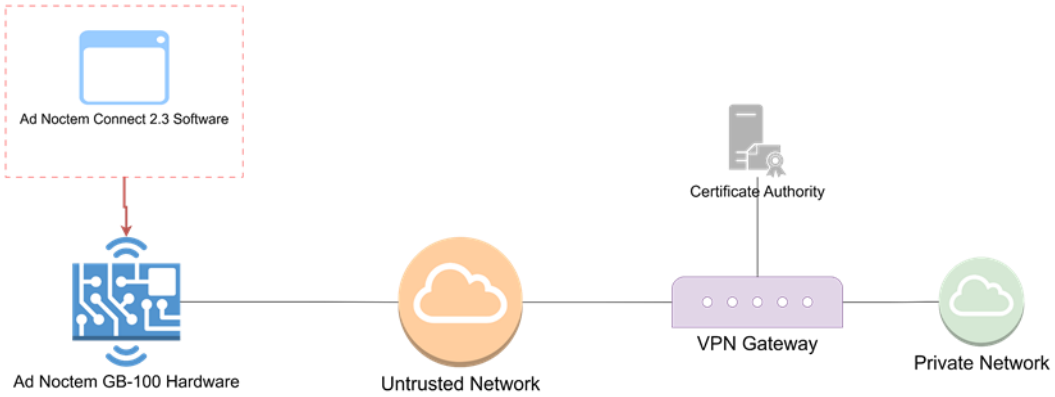
The physical boundary of the TOE consists solely of the Ad Noctem Connect 2.3 software, the IPsec connection templates, and the TOE Security Guidance, all of which reside on and are executed on a dedicated hardware platform, the GB-100 device. The TOE itself includes no hardware components; instead, it is installed on the appliance's storage and executed within the platform's program execution environment. Prior to execution, the platform verifies the integrity of the TOE's critical cryptographic and operating libraries, ensuring that the TOE is only loaded if all integrity checks succeed.

Alongside the TOE software, the physical boundary includes the three pre-configured IPsec templates:

- adnoctem-cert.template
- adnoctem-psk-roaming.template
- adnoctem-psk.template

Which define the VPN connection parameters executed by the TOE. It also includes the Common Criteria Security Guidance Supplement, provided in PDF format that can be downloaded from the developer's web site, which instructs administrators and users in the secure preparation and operation of the TOE.

The physical boundary for the Ad Noctem Connect 2.3 software 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 Profiles [4]* and *Supporting Documents [12]* 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 relies on the following external components to operate securely and as evaluated. These items are outside the TOE boundary and must be present and correctly configured in the operational environment.

Component	Description
Execution platform	The TOE is delivered pre-installed on the execution platform. The platform implements the physical connectivity to the TOE and the full software execution environment. The execution platform also implements the memories in which the TOE and the IPsec templates are stored. The TOE may only be stored and executed on the Northrop Grumman Corporation GB-100 execution platform. The execution platform is the physical appliance with the required network and user PC or laptop connectivity, memories, the entire program execution infrastructure, and the SUSE Enterprise Linux Micro OS 5.3 (Linux Kernel 5.14.21).
VPN Gateway	The TOE connects to a VPN gateway with IKEv2/IPsec support. The gateway should be operated by the operator of the Private network. It shall be configured to support the IPsec parameters required by the TOE.

Certificate Authority (CA)	The CA provides the TOE with X.509 certificates used for the authentication of the IPsec connection endpoints. The CA is operated by the operator of the VPN Gateway.
User PC or Laptop	The user of the TOE connects the PC or Laptop physically to the appliance on which the TOE resides and is executed. The TOE establishes a VPN connection between itself and the VPN Gateway and uses the VPN connection for securing the communication between the TOE and the VPN Gateway. The applications executed on the User PC or Laptop use the VPN connection for secure access to the resources of the Private Network.
User Connectivity	The User PC or Laptop must be connected physically to the appliance on which the TOE resides and is executed. Wireless connection must not be used. Physical connection must be done using a network cable. The network cable must be provided by the organization of the user. Unknown cables must not be used for connecting the User PC or Laptop to the TOE.
Provisioning Environment	The TOE is provisioned in a secure environment by the Organisational administrator. Once provisioned, the TOE is issued to the end user for use at remote sites. All administration of the TOE takes place in the provisioning environment by the Organisational administrator. The Organisational administrator uses the interfaces of the TOE platform to modify the TOE configuration files stored on the platform memories.
Private Network	The Private Network is a secure network operated by the organization of the user. In the Private Network the organization implements services to which the user connects over an insecure network using the User PC or Laptop. The user executes programs or accesses services in the Private Network over the VPN connection between the TOE and the VPN Gateway.

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.

Security Policy

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

The TOE is delivered pre-installed on the TOE Platform (GB-100) to the Organisational Administrator from the vendor (NGC). The end-user and the Organisational Administrator will be provided with a link to retrieve a copy of the *CC Evaluated guidance document [6]* and the TOE's *Security Target [8]* by the vendor.

Upon receipt of the TOE and its platform, the Organisational Administrator should be able to power-on the TOE Platform without any 'red' LEDs appearing on the GB-100 device. This indicates that integrity tests for the TOE Platform and the TOE have passed. It also indicates that the cryptographic self-tests have also been successful.

Before the TOE is deployed to the end-users, the Organisational Administrator must complete the provisioning process by configuring the following:

- TOE credentials
- VPN details and endpoint credentials

The TOE will be provided to the end-user in the evaluated configuration state along with a link to retrieve a copy of the *CC Evaluated Configuration Guide [6]* and the *Security Target [8].*

Installation of the TOE

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

Version Verification

The TOE Software is only executed on a dedicated execution platform. The execution platform boots up the TOE when the appliance is powered on. The users of the TOE platform can verify the installed version of both the TOE and the TOE platform from the Overview screen within the TOE platform management console. Any change in version will also be reflected in the Log view available on the TOE platform.

Documentation and Guidance

It is important that the TOE is 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 Ad Noctem Connect 2.3 is available for download from the developer's web site in PDF format. The title is:

- *Ad Noctem Connect Evaluated Configuration Guide Version 1.0, 03 February 2026*

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 application software 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 designed to provide Virtual Private Network (VPN) client functionality. It must not be used as a general-purpose computing platform, nor should it support activities such as executing compilers, running arbitrary user applications, or performing functions unrelated to its defined networking and security role. Restricting the TOE to its intended purpose ensures that its operational behaviour remains predictable and that its security controls cannot be undermined by unauthorised or non-security-related functionality.

The 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.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

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 unauthorized 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 Profiles [4]* 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 Documents [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 Profiles [4]* and *Supporting Documents [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]*.

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the *Protection Profile for Application Software [4.a]*:

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 18 December 2025 coinciding with the conclusion of the evaluation.

Software Bill of Material (SBOM) assessment

As part of the requirements outlined in the Application Software Protection Profile, the evaluator also submitted the TOE's Software Bill of Materials (SBOM). The SBOM provides a comprehensive inventory of all software components, third-party libraries, and dependencies included within the evaluated TOE. Submission of this information enables

rigorous supply-chain integrity verification, supports systematic vulnerability correlation across all embedded components, and ensures that no undeclared or untrusted software elements are present within the TOE. The SBOM serves as an essential artefact informing the vulnerability assessment activities and contributes materially to the assurance gained through the evaluation process.

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 Profiles that cover the technology area of application software with added security functionality including VPN Client functions. 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 Documents and Protection Profile Module activities, SBOM assessment, 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 Profiles (PPs) [4].* PPs provide assurance by providing a full *Security Target [8]*, and 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 Profiles *PP_APP_V1.4 [4.a], MOD_VPNC_V2.4 [4.b]* and *PP configuration for Application Software and Virtual Private Network (VPN) Clients [4.c]*.

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 Ad Noctem Connect 2.3 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 the Application Software and VPN Client *Protection Profiles [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
- 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 Profiles:
    a) *Protection Profile for Application Software: v1.4, 7 October 2021 (PP_APP_V1.4)*
    b) *Protection Profile Module for VPN Client: v2.4, 31 March, 2022 (MOD_VPNC_V2.4)*
    c) *PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 (CFG_APP-VPNC_V1.3)*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. *Ad Noctem Connect Evaluated Configuration Guide Version 1.0, 03 February 2026*
7. *Evaluation Technical Report, Ad Noctem Connect 2.3 Version 1.1, dated 26 February 2026* (Document reference EFT-T053-ETR 1.1)
8. *Security Target Ad Noctem Connect 2.3, Version 1.01, 25 February 2026.*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 02 July 2014*
10. *AISEP Policy Manual (APM):):* https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf
11. Entropy Documentation:
    a) *Entropy Report, Ad Noctem Connect 2.3 Version 1.0, Dated 21 January 2026 (Document reference T053-EAR 1.0)*
12. Protection Profile Supporting Documents
    a) *Supporting Document Mandatory Technical Document for PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022*
13. *CC and CEM Addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 2.0, 30 September 2021, CCDB-013-v2.0*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certificate Authority
CCRA	Common Criteria Recognition Arrangement
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange Version 2
IPsec	Internet Protocol Security
NGC	Northrop Grumman Corporation
PP	Protection Profile
SBOM	Software Bill of Materials
SSH	Secure Shell
TOE	Target of Evaluation
TLS	Transport Layer Security
VPN	Virtual Private Network

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.

Copyright

© Commonwealth of Australia 2026.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

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