DEFENDABLE TECHNOLOGIES

Auralis™ Wave Optical Diode

Security Target

Version 1.6

October 2025

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Description
0.1	9 May 2025	Initial draft.
0.2	20 May 2025	Modified physical scope.
1.0	29 May 2025	Draft for evaluation.
1.1	2 June 2025	Addressed evaluator ORs.
1.2	3 July 2025	Addressed certifier ORs.
1.3	21 August 2025	Updated TOE guidance.
1.4	24 September 2025	Addressed CB ORs.
1.5	6 October 2025	Addressed CB ORs.
1.6	10 October 2025	Addressed CB ORs.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Defendable Technologies Auralis™ Wave Optical Diode Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is used to provide a one-way connection between two networks. It ensures that data can only be transmitted in one direction and that no data can be passed, either explicitly or covertly, in the reverse direction.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Defendable Technologies Auralis™ Wave Optical Diode SKU: AWH & AWV
Security Target	Defendable Technologies Auralis™ Wave Optical Diode Security Target, v1.6

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC:2022 Release 1

b) Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 2024-07-22

c) CC Part 2 extended

- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, November 2022, CC:2022, Revision 1, CCMB-2022-11-002

d) CC Part 3 conformant

- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, November 2022, CC:2022, Revision 1, CCMB-2022-11-003

e) CC Part 5 conformant

- Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1, CCMB-2022-11-005

f) Package Augmented

- Evaluation Assurance Level 2 (EAL2) – Structurally Tested
- Augmented with ALC_FLR.2 - Flaw Reporting Procedures

Note: All related CC documentation can be found on the Common Criteria Portal under CC:2022 Release 1 at the following location: https://www.commoncriteriaportal.org/cc/index.cfm.

1.4 Terminology

Table 2: Terminology

Term	Definition
CC	Common Criteria
CDS	Cross Domain Solution
EAL	Evaluation Assurance Level
PP	Protection Profile
SKU	Stock Keeping Unit
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

4 The TOE is a one-way data transfer subsystem.

2.2 Usage

5 The Auralis™ Wave is a standalone, tamper resistant optical diode specifically designed for unidirectional data transfer between two security domains (the sender and receiver networks depicted in Figure 1). It ensures secure one-way communication without data leakage back through the network. It interfaces with the sender side using a Lucent Connector (LC) while the receiver side uses a single Standard Connector (SC). No configuration is required for enforcement of unidirectional data transfer. The TOE is intended for deployment in a physically secure environment.

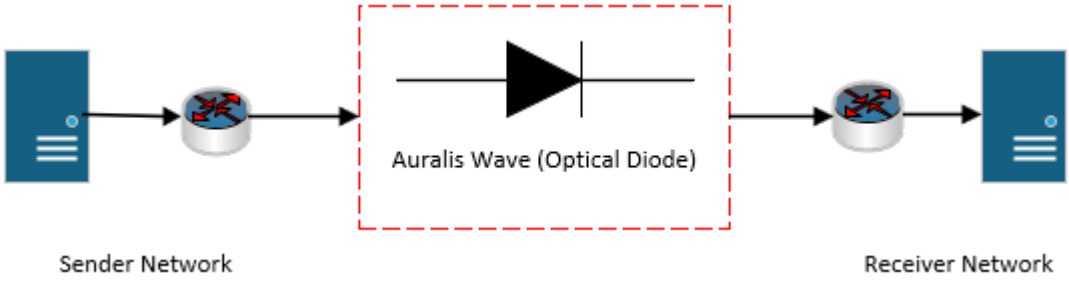

Figure 1: Example TOE deployment

2.3 Logical Scope

6 The TOE logical scope comprises the following security functions:

a) **Unidirectional Data Transfer.** The TOE ensures that data can only be transmitted in one direction and that no data can be passed, either explicitly or covertly, in the reverse direction.

b) **Failure with Preservation of Secure State.** The TOE will not allow data to be transmitted from receiver side to sender side in the event of hardware failures.

c) **Tamper Detection & Resistance.** The TOE will implement mechanisms to detect and resist physical tampering.

2.4 Physical Scope

7 The physical boundary of the TOE is the Auralis™ Wave Optical Diode housed in a tamper resistant case. The TOE is provided in two form factors to support vertical and horizontal mounting. The internal components are the same. The form factor housing differs as follows:

- Physical size and shape
- Mount location and method
- Input/Output port location

8 For local distribution, the TOE is hand delivered by a Defendable Technologies Field Service Representative. For broader distribution, the TOE is delivered to customers via commercial carrier with a tracking system.

2.4.1 Guidance Documents

9 The TOE includes the following guidance document (PDF), delivered to customers upon request:

- Defendable Technologies Auralis™ Wave Optical Diode Common Criteria Guide, version 1.2, October 2025

2.4.2 Non-TOE Components

10 The TOE operates with the following components in the environment:

a) **Connecting Equipment.** The sender side and receiver side connected network equipment.

2.4.3 Exclusions

11 The TOE may be embedded within a rack mounted appliance provided by Defendable Technologies. The Auralis Core and Auralis Edge CDS appliances are not included in the evaluation.

3 Security Problem Definition

3.1 Threats

Table 3: Threats

Identifier	Description
T.TRANSFER	A user or process on the output network accidentally or deliberately transmits data through the TOE to the input network resulting in the unauthorized disclosure of information from the receiver side to the sender side.
T.TAMPER	An adversary tampers with the contents of the TOE during delivery, and/or after installation resulting in the unauthorized disclosure of information from the receiver side to the sender side.
T.FAILURE	A hardware failure may result in a violation of one-way data transmission causing the unauthorized disclosure of information.

3.2 Assumptions

Table 4: Assumptions

Identifier	Description
A.PHYSICAL	The TOE will be deployed in accordance with the physical security requirements of the receiver side.
A.CONNECT	The TOE is the only method of interconnecting the sender and receiver networks.
A.NO_EVIL	Authorised users of the TOE are non-hostile and follow all usage guidance to ensure that the TOE is configured and operated in a secure manner.

3.3 Organizational Security Policies

Table 5: Organizational Security Policies

Identifier	Description
P.PERSONNEL	The TOE shall be administered by authorized personnel who possess the necessary privileges to access the receiver network equipment.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 6: Security Objectives for the Operational Environment

Identifier	Description
OE.PHYSICAL	The TOE will be delivered and deployed in accordance with the physical security requirements of the receiver side.
OE.CONNECT	The TOE shall be the only method of interconnecting the sender side and receiver side.
OE.NO_EVIL	Authorised users of the TOE shall be non-hostile and follow all usage guidance to ensure that the TOE is configured and operated in a secure manner.
OE.PERSONNEL	The TOE shall be administered by authorized personnel who possess the necessary privileges to access the receiver network equipment.

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
O.ONE_WAY	The TOE shall ensure that data can only be transmitted from the sender side to the receiver side.
O.FAIL_SECURE	The TOE shall maintain a secure state in the event of a hardware failure ensuring that no data can be transferred from the receiver side to the sender side, even in the event of such failures.
O.ENCLOSURE	The TOE enclosure shall detect and resist physical tamper attempts.

5 Security Requirements

5.1 Conventions

12 This document uses the following font conventions to identify SFR operations:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

13 None defined.

5.3 Functional Requirements

Table 8: Summary of SFRs

Requirement	Title
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_IFF.5	No illicit information flows
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack

5.3.1 User Data Protection (FDP)

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [*Unidirectional Flow Policy*] on [

- *Subjects: Input Port, Output Port*
- *Information: All Data Transiting the TOE*]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute authorization

FDP_IFF.1.1 The TSF shall enforce the [*Unidirectional Flow Policy*] based on the following types of subject and information security attributes: [

- *Subjects: Input Port, Output Port*
- *Information: All Data Transiting the TOE*
- *Attributes: Inherent attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*data may flow from the Input Port to the Output Port*].

FDP_IFF.1.3 The TSF shall enforce the [*none*].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

FDP_IFF.5 No illicit information flows

Hierarchical to: FDP_IFF.4 Partial elimination of illicit information flows

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [*Unidirectional Flow Policy*].

5.3.2 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

- *Hardware failure*].

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that can compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist [*physical tampering of external fasteners and internal components*] to the [*AWH and AWV form factors*] by responding automatically such that the SFRs are always enforced.

5.4 Assurance Requirements

14 The TOE security assurance requirements (EAL2+) are summarized in Table 9. Augmented components are shown in bold text.

Table 9: Assurance Requirements

Assurance Class	Components	Description
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
ALC: Life-cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ASE: Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Unidirectional Data Transfer

15 As depicted in Figure 2, the Auralis™ Wave is composed of two main functional components working together to provide assurance of one-way data transfer; the Filter Coupler and the Isolator.

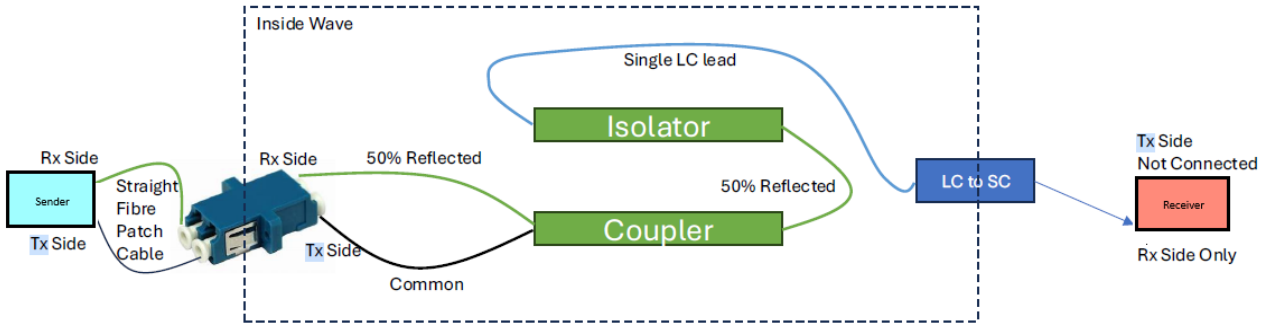

Figure 2: Auralis™ Wave Functional Components

16 The Filter Coupler functions as a specialized fibre optic junction. Its primary purpose is not only to divide but also to evenly distribute light across multiple fibres, allowing the signal to be transmitted to both the sender and receiver compute devices. A key consideration with this light junction is its function as a two-way conduit for light. If light is introduced into one of the outgoing fibres (i.e. connected incorrectly), it has the potential to travel back through the main incoming fibre and exit through the other outgoing fibres.

17 The Isolator acts as a critical component in maintaining unidirectional flow. It acts as a one-way gate within the fiber optic system, designed to permit light to pass freely from the sender side to the receiver side. If light attempts to travel in the opposite direction, the isolator prevents any reverse transmission complementing the splitter by acting as a directional control, ensuring that the light signal flows only in the desired direction.

18 The optical network interfaces have separate transmit and receive ports. This allows single strand optical cables to be used to connect with each optical interface (i.e., one for transmit and one for receive). In addition, there is no reverse path through the data diode itself.

19 The diode path is implemented using passive fibre optic components, specifically the optical coupler combined with the optical isolator. This arrangement ensures that no meaningful signal can propagate back from the receiver side to the sender side. The TOE supports the following fiber optic parameters:

- Wavelength: 1310nm
- Signal Strength: -9dBm to +5dBm

Note: Wavelengths and signal strengths outside of these specifications should not be used in the evaluated configuration. The TOE only supports single-mode fiber.

6.2 Fail Secure

20 The absence of a reverse signal path ensures that no data can be transferred from receiver side to sender side regardless of hardware failure. Security policy enforcement does not rely on power or active components.

6.2.1 Tamper Detection & Resistance

21 A tamper-evident seal provides clear signs of tampering by irreversibly breaking or changing when the wave is opened. The seal is placed over a screw and along the case seam. It must be torn, peeled, or visibly damaged to access the interior, indicating that the device has been opened or interfered with. Each seal is custom-made and serial-numbered, allowing verification against records. The absence of a correctly numbered seal is also considered evidence of tampering.

22 Drilled spanner heads achieve tamper resistance by using two small holes on the fastener head, requiring a matching spanner bit with protruding pins to engage and turn it. This design prevents common tools like flatheads or pliers from gripping or turning the fastener, making unauthorized removal more difficult without the proper tool.

23 Internally, each TOE device is filled with epoxy. The epoxy provides tamper resistance by physically encapsulating the fibers and eliminating access to internal connectors. The hardened epoxy makes it extremely difficult to remove or replace connectors without destroying components, effectively preventing unauthorized access or reconfiguration.

7 Rationale

7.1 Security Objectives Rationale

24 Table 10 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 10: Security Objectives Mapping

	T.TRANSFER	T.TAMPER	T.FAILURE	A.PHYSICAL	A.CONNECT	A.NO_EVIL	P.PERSONNEL
O.ONE_WAY	X						
O.FAIL_SECURE			X				
O.ENCLOSURE		X					
OE.PHYSICAL		X		X			
OE.CONNECT	X				X		
OE.NO_EVIL						X	
OE.PERSONNEL						X	X

25 Table 11 provides the justification to show that the security objectives are suitable to address the security problem.

Table 11: Suitability of Security Objectives

Element	Justification
T.TRANSFER	**O.ONE_WAY.** Enforcing one-way data transmission prevents the disclosure of information from the receiver side to the sender side. **OE.CONNECT.** The operational environment ensures that the TOE is the only interconnection point between the receiver side and the sender side.
T.TAMPER	**OE.PHYSICAL.** The operational environment ensures that delivery and operation occur in a secure manner, commensurate with the security requirements of the receiver side – thereby reducing the risk of tampering to acceptable levels. **O.ENCLOSURE.** The TOE enclosure is resistant to tampering due to its construction and incorporates tamper detection mechanisms.
T.FAILURE	**O.FAIL_SECURE.** Ensures that a failure of the TOE does not result in a violation of one-way data transmission.
A.PHYSICAL	**OE.PHYSICAL.** Upholds the assumption by restating it as an objective for the operational environment.
A.CONNECT	**OE.CONNECT.** Upholds the assumption by restating it as an objective for the operational environment.
A.NO_EVIL	**OE.NO_EVIL.** Upholds the assumption by restating it as an objective for the operational environment. **OE.PERSONNEL.** Also contributes to upholding this assumption as receiver side security requirements will likely include personnel vetting measures commensurate with the information being protected.
P.PERSONNEL	**OE.PERSONNEL.** Upholds the policy by restating it as an objective for the operational environment.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

26 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 12: Security Requirements Mapping

	O.ONE_WAY	O.FAIL_SECURE	O.ENCLOSURE
FDP_IFC.2	X		
FDP_IFF.1	X		
FDP_IFF.5	X		
FPT_FLS.1		X	
FPT_PHP.1			X
FPT_PHP.3			X

Table 13: Suitability of SFRs

Objectives	SFRs
O.ONE_WAY	**FDP_IFC.2.** Defines the scope of the Unidirectional Flow Policy (i.e. input, output, data). **FDP_IFF.1.** Defines the Unidirectional Flow Policy requiring that data only flow from input to output. **FDP_IFF.5.** Requires that there be no illicit information flows from output to input.
O.FAIL_SECURE	**FPT_FLS.1.** Requires the TOE to maintain a secure state in the event of a failure covering hardware components.

Objectives	SFRs
O.ENCLOSURE	**FPT_PHP.1.** Defines the implementation of tamper detection mechanisms. **FPT_PHP.3.** Defines the implementation of tamper resistance mechanisms.

Table 14: Dependency Analysis

SFR	Dependencies	Rationale
FDP_IFC.2	FDP_IFF.1	Met
FDP_IFF.1	FDP_IFC.1	Met
	FMT_MSA.3	Not met – the security attributes used to define the Unidirectional Flow SFP are inherent (i.e. they are not data objects) and therefore do not need to be initialized.
FDP_IFF.5	FDP_IFC.1	Met
FPT_FLS.1	None	n/a
FPT_PHP.1	None	n/a
FPT_PHP.3	None	n/a

7.3 TOE Summary Specification Rationale

27 Table 15 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 15: Map of SFRs to TSS Security Functions

	Unidirectional Data Transfer	Fail Secure	Tamper Detection & Resistance
FDP_IFC.2	X		
FDP_IFF.1	X		
FDP_IFF.5	X		
FPT_FLS.1		X	
FPT_PHP.1			X
FPT_PHP.3			X