

**National Information Assurance Partnership**  
**Common Criteria Evaluation and Validation Scheme**



**Validation Report**

**Aruba, a Hewlett Packard Enterprise Company**  
**2930F, 2930M, 3810M, and 5400R Switch Series**  
**running ArubaOS version 16.08**

**Report Number: CCEVS-VR-11099-2021**  
**Dated: January 8, 2021**  
**Version: 1.0**

**National Institute of Standards and Technology**  
**Information Technology Laboratory**  
**100 Bureau Drive**  
**Gaithersburg, MD 20899**

**National Security Agency**  
**Information Assurance Directorate**  
**9800 Savage Road STE 6940**  
**Fort George G. Meade, MD 20755-6940**

## **ACKNOWLEDGEMENTS**

### **Validation Team**

Paul Bicknell  
Jenn Dotson  
Randy Heimann  
Patrick Mallett  
Lisa Mitchell  
Clare Olin  
Jean Petty  
*The MITRE Corporation*

Farid Ahmed  
Peter Kruus  
*Johns Hopkins University Applied Physics Laboratory*

### **Common Criteria Testing Laboratory**

Tammy Compton  
Wasif Sikder  
*Gossamer Security Solutions, Inc.*  
*Catonsville, MD*

## Table of Contents

1	Executive Summary .....	1
2	Identification .....	1
3	Architectural Information .....	3
3.1	TOE Evaluated Platforms .....	3
3.2	TOE Architecture .....	4
3.3	Physical Boundaries .....	4
4	Security Policy .....	4
4.1	Security audit .....	5
4.2	Cryptographic support .....	5
4.3	Identification and authentication .....	5
4.4	Security management .....	5
4.5	Protection of the TSF .....	5
4.6	TOE access .....	6
4.7	Trusted path/channels .....	6
5	Assumptions .....	6
6	Clarification of Scope .....	6
7	Documentation .....	7
8	IT Product Testing .....	7
8.1	Developer Testing .....	7
8.2	Evaluation Team Independent Testing .....	7
9	Evaluated Configuration .....	7
10	Results of the Evaluation .....	8
10.1	Evaluation of the Security Target (ASE) .....	8
10.2	Evaluation of the Development (ADV) .....	8
10.3	Evaluation of the Guidance Documents (AGD) .....	8
10.4	Evaluation of the Life Cycle Support Activities (ALC) .....	9
10.5	Evaluation of the Test Documentation and the Test Activity (ATE) .....	9
10.6	Vulnerability Assessment Activity (VAN) .....	9
10.7	Summary of Evaluation Results .....	10
11	Validator Comments/Recommendations .....	10
12	Annexes .....	10
13	Security Target .....	10
14	Glossary .....	10
15	Bibliography .....	11

## 1 Executive Summary

This report documents the assessment by the National Information Assurance Partnership (NIAP) Validation team of the evaluation of the Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 solution provided by Hewlett Packard Enterprise Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in January 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018.

The TOE is the Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08. The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 (NDcPP21) Security Target, Version 0.5, 01/07/2021 and analysis performed by the Validation team.

## 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing

laboratories CCTLs using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product’s evaluation. Upon successful completion of the evaluation, the product is added to NIAP’s Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

<b>Item</b>	<b>Identifier</b>
<b>Evaluation Scheme</b>	United States NIAP Common Criteria Evaluation and Validation Scheme
<b>TOE</b>	Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 (Specific models identified in Section 3.1)
<b>Protection Profile</b>	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
<b>ST</b>	Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 (NDcPP21) Security Target, Version 0.5, 01/07/2021
<b>Evaluation Technical Report</b>	Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08, Version 0.3, January 7, 2021
<b>CC Version</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
<b>Conformance Result</b>	CC Part 2 extended, CC Part 3 conformant
<b>Sponsor</b>	Aruba, a Hewlett Packard Enterprise Company
<b>Developer</b>	Aruba, a Hewlett Packard Enterprise Company
<b>Common Criteria Testing Lab (CCTL)</b>	Gossamer Security Solutions, Inc.
<b>CCEVS Validators</b>	Farid Ahmed, Paul Bicknell, Jenn Dotson, Randy Heimann, Peter Kruus, Patrick Mallett, Lisa Mitchell, Clare Olin, Jean Petty

### 3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is the Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08. The TOE is a family of switches designed to support scalability, security and high performance for campus networks. The TOE is a network device offering CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records).

#### 3.1 TOE Evaluated Platforms

The TOE evaluated configuration consists of the following models:

Series	Hardware Models	Processor
Aruba 2930F Switch Series	2930F 24G 4SFP+ Switch (JL253A) 2930F 48G 4SFP+ Switch (JL254A) 2930F 24G PoE+ 4SFP+ Switch (JL255A) 2930F 48G PoE+ 4SFP+ Switch (JL256A) 2930F 8G PoE+ 2SFP+ Switch (JL258A) 2930F 24G 4SFP Switch (JL259A) 2930F 48G 4SFP Switch (JL260A) 2930F 24G PoE+ 4SFP Switch (JL261A) 2930F 48G PoE+ 4SFP Switch (JL262A) 2930F 24G PoE+ 4SFP+ Switch (JL263A) 2930F 48G PoE+ 4SFP+ Switch (JL264A) 2930F 48G PoE+ 4SFP 740W Switch (JL557A)	Dual Core ARM Coretex A9 (ARMv7-A Architecture)
Aruba 2930M Switch Series	2930M 24G 1-slot Switch (JL319A) 2930M 24G PoE+ 1-slot Switch (JL320A) 2930M 48G 1-slot Switch (JL321A) 2930M 48G PoE+ 1-slot Switch (JL322A) 2930M 40 Port 1G + 8 Port SmartRate PoE+ (JL323A) 2930M 24 Port SmartRate PoE+ (JL324A) 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch (R0M67A) 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch (R0M68A)	Dual Core ARM Coretex A9 (ARMv7-A Architecture)
Aruba 3810M Switch Series	3810M 24G 1-slot Switch (JL071A) 3810M 48G 1-slot Switch (JL072A) 3810M 24G PoE+ 1-slot Switch (JL073A) 3810M 48G PoE+ 1-slot Switch (JL074A) 3810M 16SFP+ 2-slot Switch (JL075A) 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch (JL076A)	Freescale P2020 Dual Core (e500 Architecture)
Aruba 5400R Switch Series	5406R z12 Switch (J9821A) 5412R z12 Switch (J9822A) 5406R/5412R-24-port 10/100/1000Base-T PoE+ MACsec (No PSU) v3 z12 Card (J9986A) 5406R/5412R-24p 1000BASE-T (No PSU) v3 z12 Card (J9987A) 5406R/5412R-24p SFP (No PSU) v3 z12 Card (J9988A) 5406R/5412R-12p PoE+ / 12p 1GbE SFP (No PSU) v3 z12	Freescale P2020 Dual Core (e500 Architecture)

Series	Hardware Models	Processor
	Card (J9989A) 5406R/5412R-20p PoE+ / 4p SFP+ (No PSU) v3 z12 Card (J9990A) 5406R/5412R-20p PoE+ / 4p 1/25/5/XGT PoE+ (No PSU) v3 z12 Card (J9991A) 5406R/5412R-20p PoE+ / 1p 40GbE QSPF+ (No PSU) v3 z12 Card (J9992A) 5406R/5412R-8p 1G/10GbE SFP+ v3 (No PSU) v3 z12 Card (J9993A) 5406R/5412R-2-port 40GbE QSFP+ (No PSU) v3 z12 Card (J9996A)	

### 3.2 TOE Architecture

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory and processor, and software that implements switching functions, configuration information and drivers. While the hardware varies between different appliance models, the software code is shared across all platforms. It is in the software code that all the security functions claimed in the ST are enforced.

### 3.3 Physical Boundaries

Each TOE appliance runs a version of the Aruba software and has physical network connections to its environment to facilitate the switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external SYSLOG server in the network environment. The evaluation required an audit server, management workstation, and certificate authority in the IT environment. The scope of the evaluation was limited to the requirements in the ST – all other functionality was outside the scope of the evaluation.

## 4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF

6. TOE access
7. Trusted path/channels

## **4.1 Security audit**

The TOE can generate logs for a wide range of security relevant events. It can be configured to store the logs locally so they can be accessed by an administrator and to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

## **4.2 Cryptographic support**

The TOE provides CAVP certified cryptography in support of its SSHv2 and TLS protocol implementations. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature, and secure hashing.

## **4.3 Identification and authentication**

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except for passing network traffic in accordance with its configured switching rules and reading the login banner. It provides the ability to both assign attributes (usernames, passwords, and roles) and to authenticate users against these attributes. The TOE also provides X.509 certificate checking for its TLS connections.

## **4.4 Security management**

The TOE provides Command Line Interface (CLI) commands and a web GUI to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled using roles that can be assigned to TOE users. The TOE supports the following roles: Manager, Operator. The Manager role can make changes to the TOE configuration while the Operator role is a read-only role.

## **4.5 Protection of the TSF**

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects stored passwords and cryptographic keys, so they are not directly accessible in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment. The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operation environment. The TOE performs self-tests to detect failure and protect itself from malicious updates.



## 4.6 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

## 4.7 Trusted path/channels

The TOE protects interactive communication with administrators using SSH for CLI and TLS for the web GUI to ensure both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs.

## 5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

That information has not been reproduced here and the NDcPP21 should be consulted if there is interest in that material.

This evaluation was limited to the functionality and assurances covered in the NDcPP21 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

## 6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the assurance activities specified in the NDcPP21 and performed by the evaluation team.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP21 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

## **7 Documentation**

The following documents were available with the TOE for evaluation:

- Common Criteria Configuration Guidance Network Device Collaboration Protection Profile, Target of Evaluation: Aruba 2930F, 2930M, 3810M and 5400R Switch Series, version 1.7, September 11, 2020.

## **8 IT Product Testing**

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in the Assurance Activity Report (NDcPP21) for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08, Version 0.3, 01/07/2021 (AAR) and the proprietary Detailed Test Report (NDcPP21) for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08, Version 0.3, 01/07/2021 (DTR). The DTR shows the test configuration, provides the tested platforms, and lists the test tools.

### **8.1 Developer Testing**

No evidence of developer testing is required in the assurance activities for this product.

### **8.2 Evaluation Team Independent Testing**

The Evaluation team verified the product according the Common Criteria Certification document and ran the tests specified in the NDcPP21 including the tests associated with optional requirements.

## **9 Evaluated Configuration**

The evaluated configuration consists of the models as defined in Section 3.1 of this Validation Report.

To use the product in the evaluated configuration, the product must be installed, configured, and managed as specified in the documentation referenced in Section 7 of this Validation Report.

## **10 Results of the Evaluation**

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5.

### **10.1 Evaluation of the Security Target (ASE)**

The Evaluation team applied each ASE CEM work unit and ensured the ST contained a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

### **10.2 Evaluation of the Development (ADV)**

The Evaluation team applied each ADV CEM work unit, assessed the design documentation, and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP21 related to the examination of the information contained in the TSS.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

### **10.3 Evaluation of the Guidance Documents (AGD)**

The Evaluation team applied each AGD CEM work unit and ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the

evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

#### **10.4 Evaluation of the Life Cycle Support Activities (ALC)**

The Evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

#### **10.5 Evaluation of the Test Documentation and the Test Activity (ATE)**

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP21 and recorded the results in the DTR, summarized in the AAR.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

#### **10.6 Vulnerability Assessment Activity (VAN)**

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is provided in the DTR prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched, on 12/30/2020, the National Vulnerability Database (<https://web.nvd.nist.gov/vuln/search>), Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>), Rapid7 Vulnerability Database (<https://www.rapid7.com/db/vulnerabilities>), Tipping Point Zero Day Initiative (<http://www.zerodayinitiative.com/advisories>), Exploit / Vulnerability Search Engine (<http://www.exploitsearch.net>), SecurITeam Exploit Search (<http://www.securiteam.com>), Tenable Network Security (<http://nessus.org/plugins/index.php?view=search>), Offensive Security Exploit Database (<https://www.exploit-db.com/>) with the following search terms: "HPE Aruba", "2930F", "2930M", "3810M", "5400R", "TLS", "SSH", "TCP".

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 10.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

## 11 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. No versions of the TOE and software, either earlier or later were evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, should be assessed separately and no further conclusions can be drawn about their effectiveness.

## 12 Annexes

Not applicable

## 13 Security Target

The Security Target is identified as: *Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 (NDcPP21) Security Target, Version 0.5, 01/07/2021.*

## 14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common

Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

## 15 Bibliography

The Validation team used the following documents to produce this Validation Report:

- [1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
- [4] collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018.
- [5] Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 (NDcPP21) Security Target, Version 0.5, 01/07/2021 (ST).
- [6] Assurance Activity Report (NDcPP21) for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08, Version 0.3, 01/07/2021 (AAR).
- [7] Detailed Test Report (NDcPP21) for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08, Version 0.3, 01/07/2021 (DTR).
- [8] Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08, Version 0.3, 01/07/2021 (ETR)

