National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Axway API Gateway version 7.4.1 with SP2

Report Number: CCEVS-VR-VID10778-2017

Dated: January 13, 2017

Version: 1.0

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

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

Kenneth Stutterheim

Marybeth Panock

The Aerospace Corporation

Evaluation Team

Eve Pierre

Brittany Conti

Computer Sciences Corporation

Table of Contents

List of Tables

List of Figures

1. Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Axway API Gateway version 7.4.1, the Target of Evaluation (TOE), performed by Computer Sciences Corporation. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed in January 2017. The information in this report is largely derived from the ST, and the evaluation sensitive documents: the Evaluation Technical Report (ETR) and the functional testing report, which are summarized in the Assurance Activity Report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, September 2012.

The Axway API Gateway is an enterprise security management solution that provides management in a centralized location for access control over web services and related resources.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Axway API Gateway version 7.4.1 with SP2 Security Target version 1.1
Sponsor and Developer	Axway Inc. 26 rue des Pavillions Puteaux Cedex, France 92807
CCTL	Computer Sciences Corporation 7459A Candlewood Road Hanover, Maryland 21076
Completion Date	January 17, 2017
Interpretations	There were no applicable interpretations used for this evaluation.

Item	Identifier
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	[PP_ESM_PM] Standard Protection Profile for Enterprise Security Management Policy Management v2.1, dated October 24, 2013. [PP_ESM_AC] Standard Protection Profile for Enterprise Security Management Access Control v2.1, dated October 24, 2013.
Disclaimer	This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.
Evaluation Personnel	Brittany Conti Eve Pierre Computer Sciences Corporation
Validation Personnel	Daniel P. Faigin Kenneth Stutterheim Marybeth S. Panock The Aerospace Corporation

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 called Common Criteria Testing Laboratories (CCTLs) 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 IT 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 Product Compliant List (PCL).

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST), describing the security features, claims, and assurances of the product

Table 2: Evaluation Identifiers

Item	Identifier
ST Title and Version	Axway API Gateway version 7.4.1 with SP2 Security Target version 1.1
Publication Date	January 13, 2017
Vendor	Axway
ST Author	Computer Sciences Corporation; Brittany Conti, Eve Pierre
Target of Evaluation Reference	Axway API Gateway version 7.4.1 with SP2
TOE Software Version	Axway API Gateway version 7.4.1 with SP2
Keywords	Enterprise Security Management, Policy Management, Access Control, Securing Web APIs, SOA-based systems

3. Security Policy

The core functionality of the Axway API Gateway is the ability to define and enforce policies to protect APIs and web services.

4. Security Problem Definition

4.1. Assumptions

The ST identified the following security assumptions contained in Table 3:

Table 3: Secure Usage Assumptions

Assumption	Definition
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data
A.ROBUST	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment
A.USERID	The TOE will receive identity data from the Operational Environment.
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data
A.POLICY	The TOE will receive policy data from the Operational Environment.
A.ROBUST	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication

Assumption	Definition
A.SYSTIME	The TOE will receive a reliable time data from the Operational Environment
A.USERID	The TOE will receive identity data from the Operational environment.
A.INSTALL	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.

4.2. Threats

The ST identified the following threats addressed by the TOE:

Table 4: Threats

Identifier	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONDTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FORGE	A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.
T.WEAKPOL	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
T.DISABLE	A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.

T.FALSIFY	A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
T.FORGE	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.MASK	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.
T.NOROUTE	A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
T.OFLOWS	A malicious user may attempt to provide incorrect Policy Management data to the TOE in order to alter its access control policy enforcement behavior.
T.UNAUTH	A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.

4.3. Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

Table 5: Organizational Security Policies

OSP	Definition
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

5. Architectural Information

5.1. Physical Scope and Boundary

The TOE is a comprehensive platform for managing, delivering, and securing APIs allowing for centralized enterprise security management solution. The TOE controls how APIs and web services are exposed to and accessed by external client applications.

The TOE comprises the Axway API Gateway v7.4.1 software. The TOE is deployed as a software component comprised of three main components for policy definition and policy consumption as follows:

a) **Policy Studio.** A GUI application that provides the user with the primary administrative interface to the Gateway. Policy Studio is used to construct policies and administer the TOE.

b) **API Gateway.** One or more instances of the API Gateway software that enforce policies to control web services. Basic configuration is performed using the Policy Studio to virtualize APIs and develop policies (for example, to enforce security, compliance, and operational requirements). A simple TOE deployment is depicted in figure 1 below.

c) **API Gateway Manager**. A web-based interface for monitoring Gateway traffic in real-time and for configuring global password policy, audit events, audit offload and other configurable items.,

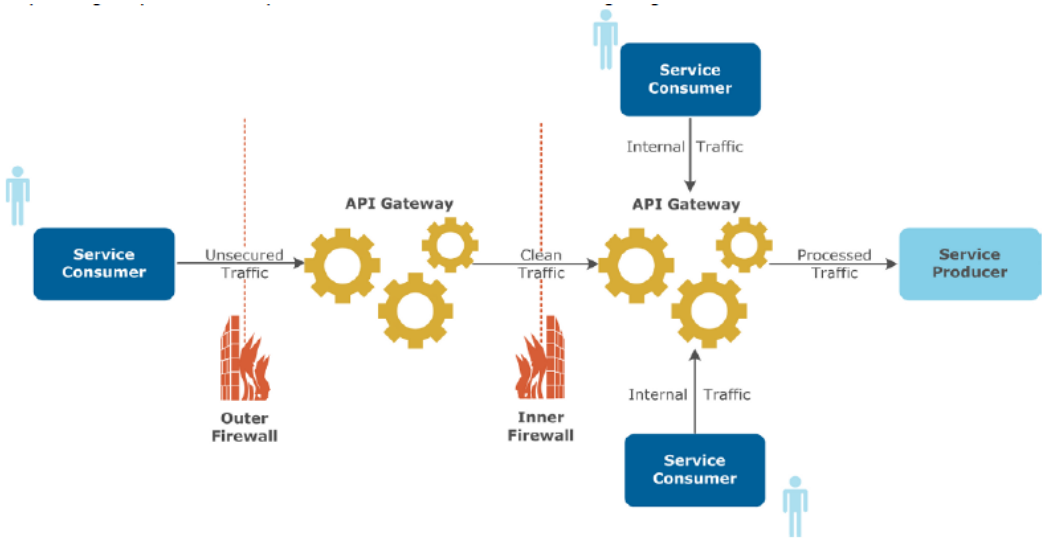

Figure 1: Secure Usage Scenario

5.2. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

a. **OpenSSL.** Cryptography of the TLS is provided by OpenSSL FIPS Object Module Version 2.0.10 within OpenSSL v1.0.1j package (CAVP Certificate AES: #4127; RSA: #2237; ECDSA: #945; SHA: #3396; DRBG: #1247; HMAC: #2700; Component Test: #936). A FIPS mode license is required in the evaluated configuration.

b. **Entrust Authority Security Toolkit for Java**

c. **DHCP Server.** The TOE can utilize a Dynamic Host Configuration Protocol (DHCP) server to acquire automatically assign an IP address.

d. **Web Browser.** The remote administrator can use a web browser to access the Web GUI interface (API Gateway Manager). See below for supported browsers.

e. **LDAP Server –** Used for external Identification and Authentication for administrators and client service users.

f. **Audit Server –** Used for external audit storage.

6. Logical Scope of the TOE

The TOE enforces the following security policies as described in the ST.

6.1. Access Control Policy Definition

The TOE includes the Policy Studio tool which is used to define and configure security policies that are enforced by the API Gateway server. The TOE only consumes policies that are defined by its policy definition component. Policies are transmitted from Policy Studio to the API Gateway server using a TLS trusted channel to protect the TSF data.

6.2. Access Control Policy Enforcement

The core functionality of the TOE is the ability to define and enforce policies to protect APIs and web services. The TOE enforces policies via message filters wherein each filter processes message request in a certain way. The ST identifies the message filters that are included in the evaluated configuration. In the evaluated configuration, the Gateway may only consume policies that are created and deployed from the Axway Policy Studio.

6.3. Security Audit

The TOE generates audit events associated with use of the administrative functions, creation of and changes to the access control policy, authentication and authorization

failures, and for use of its management functions. The TOE may store logs locally on the file system or configured to store logs on an external audit server. Communication with the external audit server is secured using TLS

6.4. Robust Administrative Access

Access to the TOE can be achieved via the Policy Studio application and the web-based API Gateway Manager interface. Users must authenticate prior to being granted access. Users may access TOE protected functions and data based upon their user roles. Users may authenticate via username and password.

6.5. Continuity of Enforcement

The Gateway continues policy enforcement in the event of a loss of connectivity with Policy Studio by enforcing the last policy received. Continuous connectivity with the Policy Studio is neither expected nor required.

6.6. Protected Communication

The TOE uses TLS to provide trusted channels for communication between its separate components; between itself and an external LDAP server and between itself and an external HTTP-based audit server. It provides a trusted path via HTTPS for remote administrators to access the TOE external interfaces.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- API Gateway v7.4.1 Administrator's Guide, 14 March 2016
- API Gateway v7.4.1 Concepts Guide, 14 March 2016
- API Gateway v7.4.1 Policy Developer Guide, 14 March 2016
- API Gateway v7.4.1 Installation Guide, 14 March 2016
- API Gateway v7.4.1 Common Criteria Guide, 16 November 2016

All documentation delivered with the product is relevant to and within the scope of the TOE.

8. IT Product Testing

This section describes the testing efforts of the evaluation team.

8.1. Evaluation team independent testing

The evaluation team conducted independent testing at the Axway facilities in Dublin, Ireland. The evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profiles and the evaluation team verified that each test passed.

8.2. Evaluated Configuration

The evaluated configuration includes the Axway API Gateway v7.4.1 with SP2 running on Windows 2012 and on Red Hat Enterprise Linux 6.6. All components of the TOE run on the same OS platforms. The Policy Studio component requires xWindows environment and GTK+2. The TOE also requires the following be included in its operational environment:

- OpenSSL (Secure Sockets Layer) FIPS Object Module version 2.010 for cryptography used by the TOE
- Entrust Authority Security Toolkit for Java
- DHCP Server
- Internet Explorer 8, 9, 10,11 or Chrome 19 or higher – Used to access the API Gateway Manager interface
- LDAP Server – Used for external Identification and Authentication
- Audit Server – Used for external audit storage

8.3. Vulnerability Analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

9. Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

Computer Sciences Corporation (CSC) has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Standard Protection Profile for Enterprise Security Management Policy Management v2.1, dated October 24, 2013 and the Standard Protection Profile for Enterprise Security Management Access Control v2.1, dated October 24, 2013. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on January 13, 2017.

10. Validator Comments

- The validation team's observations support the evaluation team's conclusion that the Axway API Gateway version 7.4.1 meets the claims stated in the Security Target.
- The validation team notes that the vulnerability analysis conducted was limited to search terms associated with the product and vendor names against the National Vulnerabilities Database. This should not be considered as a comprehensive search.
- The validation team observed that the ST specifies that the API Gateway TOE component operates on the Windows Server 2012 R2 and the Redhat Enterprise Linux 6.6 operating systems. The detailed information in Operational Environment portion of the CAVP certificates supports these operating systems but also provides the hardware and the architecture as well. Namely, the Operational Environment of all the relevant Axway OpenSSL CAVPs specify "Intel Xeon w/ RHEL 6.6 on VMWare ESX 5.5; Intel Xeon w/ RHEL 6.6; Intel Xeon w/ Windows 2012R2 64bit on VMWare ESX 5.5; and Intel Xeon w/ Windows 2012R2 64bit." This is not an issue because the API Gateway TOE components interface with these two supported operating systems, not with the underlying hardware or architecture. The evaluation testing was with the identified operating systems, Windows Server 2012 R2 and Redhat Enterprise Linux 6.6, and was successful.
- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance via the invocation of the assurance activities specified in the relevant ESM Policy Management and Access Control Protection Profiles.
- This evaluation covers only the software as identified in this document, no earlier or later versions.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the pertinent Protection Profiles; any additional security related functionality outside that specified was not covered by this evaluation.
- Any documentation in addition to the listing in section 7 above or available via download was not included in the evaluation and therefore should not be relied upon when configuring or using the product in its evaluated configuration.

11. Annexes

None

12. Security Target

Axway API Gateway version 7.4.1 with SP2 Security Target version 1.1 January 2017

13. Glossary

- **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.
- **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.
- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

AIS	Automated Information System
API	Application Programing Interface
CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
CSC	Computer Sciences Corporation
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GIMP	GNU Image Manipulation Program
GTK+2	GIMP Toolkit Release 2
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List

RHEL	Red Hat Enterprise Linux
SOA	Service Oriented Architecture
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. Computer Sciences Corporation (CSC), January 2017, Axway API Gateway version 7.4.1 with SP2 Security Target, Version 1.1
6. Computer Sciences Corporation (CSC), December 2016. Axway API Gateway version 7.4.1 Assurance Activity Report, v0.4
7. Computer Sciences Corporation (CSC), December 9, 2016. Axway Evaluation Technical Report for Axway API Gateway version 7.4.1 with SP2 Security Target. Version 0.3 (Evaluation Sensitive)
8. Computer Sciences Corporation (CSC), December 9, 2016. Axway API Version 7.4.1 With SP2 Evaluation Team Test Report. Version 0.4 (Evaluation Sensitive)
9. Axway, 14 March 2016. Administrator Guide Axway API Gateway Version 7.4.1
10. Axway, 16 November 2016. Common Criteria Guide Axway API Gateway Version 7.4.1
11. Axway, 14 March 2016. Concepts Guide Axway API Gateway Version 7.4.1
12. Axway, 14 March 2016. Installation Guide Axway API Gateway Version 7.4.1
13. Axway, 14 March 2016. Policy Developer Guide Axway API Gateway Version 7.4.1