National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Extended Package for Email Clients, Version 2.0, 18 June 2015

Report Number:	**CCEVS-VR-EP-0054**
Dated:	**13 September 2019**
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

Common Criteria Testing Laboratory

Base and Additional Requirements

Booz Allen Hamilton Cyber Assurance Testing Laboratory
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Application Software Extended Package for Email Clients, Version 2.0 (EP_EMAILCLIENT_V2.0), which is intended for use with the Protection Profile for Application Software (APP PP) Base-PP.

It presents a summary of the EP_EMAILCLIENT_V2.0 and the evaluation results.

Booz Allen Hamilton, located in Laurel, Maryland performed the evaluation of the EP_EMAILCLIENT_V2.0 concurrent with the first product evaluation against the Extended Package (EP) requirements. The evaluated product was VMware Workspace ONE Boxer Email Client 5.4.

This evaluation addressed the base and some of the optional and selection-based requirements of the EP_EMAILCLIENT_V2.0.

The Validation Report (VR) author independently performed an additional review of the Extended Package (EP) as part of the completion of this VR, to confirm it meets the claimed ACE requirements.

The evaluation determined the EP_EMAILCLIENT_V2.0 is both Common Criteria Part 2 extended and Part 3 conformant. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the EP identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 4). The Security Target (ST) includes material from both the APP PP and the EP_EMAILCLIENT_V2.0; completion of the ASE work units satisfied the ACE work units for this EP, but only for the materials defined in this EP.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

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 CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and EPs that have Assurance Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 work units specific to the technology described by the PP or EP.

In order to promote thoroughness and efficiency, the evaluation of the EP_EMAILCLIENT_V2.0 was performed concurrent with the first product evaluation against the EP's requirements. In this case, the Target of Evaluation (TOE) was VMware Workspace ONE Boxer Email Client 5.4, performed by Booz Allen Hamilton in Laurel, MD, United States of America.

The EP_EMAILCLIENT_V2.0 has a set of "base" requirements all conformant STs must include and "Optional" and "Selection-based" requirements. Optional requirements can be included in the ST, but are not required in order for an email client to claim conformance to EP_EMAILCLIENT_V2.0. Selection-based requirements must be included based on the selections made in the base requirements and the capabilities of the TOE. This evaluation claimed several of the optional and selection-based requirements.

A specific ST may not include all of these discretionary requirements, so the initial use of the EP addresses (in terms of the EP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units performed against the EP. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the EP_EMAILCLIENT_V2.0 were evaluated.

The following identifies the EP evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this EP and any subsequent evaluations that address additional optional, selection-based, or objective requirements (if applicable) in the EP.

Protection Profile/Extended Package	Application Software Extended Package for Email Clients, Version 2.0, 18 June 2015
ST (Base)	VMware Workspace ONE Boxer Email Client 5.4 Security Target, Version 1.0, June 13, 2019
Assurance Activity Report (Base)	VMware Workspace ONE Boxer Email Client 5.4 Assurance Activities Report (AAR) Version 1.0, 13 June 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Booz Allen Hamilton, Laurel, MD, USA

3 EP_EMAILCLIENT_V2.0 Description

The EP_EMAILCLIENT_V2.0 along with the Protection Profile for Application Software (APP PP) provide a baseline set of Security Functional Requirements (SFRs) for email clients running on any operating system regardless of the composition of the underlying platform. This EP also defines optional and selection-based requirements.

Email clients are user applications that provide functionality to send, receive, access, and manage email. The complexity of email content and email clients has grown over time. Modern email clients can render HTML as well as plaintext, and may include functionality to display common attachment formats, such as Adobe PDF and Microsoft Word documents. Some email clients allow their functionality to be modified by users through the addition of add-ons. Protocols have also been defined for communicating between email clients and servers. Some clients support multiple protocols for doing the same task, allowing them to be configured according to email server specifications.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections should exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions in the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
This EP does not define any assumptions.	

4.2 Threats

Table 2 shows applicable threats the EP extends, in addition to those defined in the Base-PPs.

Table 2: Threats

Threat Name	Threat Definition
T.FLAWED_ADDON	Email client functionality can be extended with integration of third-party utilities and tools. This expanded set of capabilities is made possible via the use of add-ons. The tight integration between the basic email client code and the new capabilities that add-ons provide increases the risk that malefactors could inject serious flaws into the email client application, either maliciously by an attacker, or accidentally by a developer. These flaws enable undesirable behaviors including, but not limited to, allowing unauthorized access to sensitive information in the email client, unauthorized access to the device's file system, or even privilege escalation that enables unauthorized access to other applications or the operating system.

4.3 Organizational Security Policies

Table 3 shows applicable organizational security policies the EP extends, in addition to those defined in the Base-PPs.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
This EP does not define any organizational security policies.	

4.4 Security Objectives

Table 4 shows security objectives for the TOE the EP extends, in addition to those defined in the Base-PPs.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.ADDON_INTEGRITY	To address issues associated with malicious or flawed plug-ins or extensions, conformant email clients implement mechanisms to ensure their integrity. This includes verification at installation time and update.

Table 5 shows security objectives for the Operational Environment, in addition to those defined in the Base-PP.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
This EP does not define any security objectives for the operational environment.	

5 Requirements

As indicated above, the EP_EMAILCLIENT_V2.0 requirements include "base" mandatory, optional, and selection-based requirements. Table 6 shows the mandatory requirements validated as part of the VMware evaluation activities referenced above.

Table 6: Mandatory Requirements

Requirement Class	Requirement Component	Verified By
Mandatory		
FCS: Cryptographic Support	FCS_CKM_EXT.3 Protection of Key and Key Material	VMware Workspace ONE Boxer Email Client 5.4
	FCS_CKM_EXT.4 Cryptographic Key Destruction	VMware Workspace ONE Boxer Email Client 5.4
	FCS_IVG_EXT.1 Initialization Vector Generation	VMware Workspace ONE Boxer Email Client 5.4
	FCS_KYC_EXT.1 Key Chaining	VMware Workspace ONE Boxer Email Client 5.4
	FCS_SMIME_EXT.1 Secure/Multipurpose Internet Mail Extensions (S/MIME)	VMware Workspace ONE Boxer Email Client 5.4
FDP: User Data Protection	FDP_NOT_EXT.1 Notification of S/MIME Status	VMware Workspace ONE Boxer Email Client 5.4
	FDP_SMIME_EXT.1 S/MIME	VMware Workspace ONE Boxer Email Client 5.4
FIA: Identification and Authentication	FIA_X509_EXT.3 X509 Authentication and Encryption	VMware Workspace ONE Boxer Email Client 5.4
FMT: Security Management	FMT_MOF_EXT.1 Management of Functions Behavior	VMware Workspace ONE Boxer Email Client 5.4
FPT: Protection of the TSF	FPT_AON_EXT.1 Support for Only Trusted Add-ons	VMware Workspace ONE Boxer Email Client 5.4
FTP: Trusted Path/Channels	FTP_ITC_EXT.1 Inter-TSF Trusted Channel	VMware Workspace ONE Boxer Email Client 5.4

Table 7 shows the "**Optional**" requirements included in Appendix A of the EP_EMAILCLIENT_V2.0, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.5 Cryptographic Key Derivation (Password/Passphrase Conditioning)	VMware Workspace ONE Boxer Email Client 5.4
	FCS_NOG_EXT.1 Cryptographic Nonce Generation	PP evaluation
	FCS_SAG_EXT.1 Cryptographic Salt Generation	PP evaluation

Requirement Class	Requirement Component	Verified By
FDP: User Data Protection	FDP_NOT_EXT.2 Notification of URI	PP evaluation
	FDP_PST_EXT.1 Storage of Persistent Information	PP evaluation
	FDP_REN_EXT.1 Rendering of Message Content	PP evaluation

Table 8 shows the "**Selection-Based**" requirements included in Appendix B of the EP_EMAILCLIENT_V2.0, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors make associated selections in requirements levied on the TOE by the ST.

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_COP_EXT.2 Key Wrapping	VMware Workspace ONE Boxer Email Client 5.4
	FCS_SMC_EXT.1 Key Combining	PP evaluation
FIA: Authentication and Encryption	FIA_SASL_EXT.1 Simple Authentication and Security Layer (SASL)	PP evaluation
FPT: Protection of the TSF	FPT_AON_EXT.2 Trusted Installation and Update for Add-ons	PP evaluation

Table 9 shows the "**Objective**" requirements included in Appendix D of the EP_EMAILCLIENT_V2.0, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
This EP does not define any objective requirements.		

6 Assurance Requirements

Table 10 shows the assurance requirements applicable to the EP_EMAILCLIENT_V2.0.

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	VMware Workspace ONE Boxer Email Client 5.4
	ASE_ECD.1: Extended Components Definition	VMware Workspace ONE Boxer Email Client 5.4
	ASE_INT.1: ST Introduction	VMware Workspace ONE Boxer Email Client 5.4
	ASE_OBJ.1: Security Objectives for the Operational Environment	VMware Workspace ONE Boxer Email Client 5.4
	ASE_REQ.1: Stated Security Requirements	VMware Workspace ONE Boxer Email Client 5.4
	ASE_SPD.1: Security Problem Definition	VMware Workspace ONE Boxer Email Client 5.4
	ASE_TSS.1: TOE Summary Specification	VMware Workspace ONE Boxer Email Client 5.4
ADV: Development	ADV_FSP.1 Basic Functional Specification	VMware Workspace ONE Boxer Email Client 5.4
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	VMware Workspace ONE Boxer Email Client 5.4
	AGD_PRE.1: Preparative Procedures	VMware Workspace ONE Boxer Email Client 5.4
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	VMware Workspace ONE Boxer Email Client 5.4
	ALC_CMS.1: TOE CM Coverage	VMware Workspace ONE Boxer Email Client 5.4
	ALC_TSU_EXT.1 Timely Security Updates	VMware Workspace ONE Boxer Email Client 5.4
ATE: Tests	ATE_IND.1: Independent Testing – Conformance	VMware Workspace ONE Boxer Email Client 5.4
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	VMware Workspace ONE Boxer Email Client 5.4

7 Results of the Evaluation

Note that for ACE elements and work units identical to ASE elements and work units, the lab performed the ACE work units concurrent to the ASE work units.

Table 11: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	VMware Workspace ONE Boxer Email Client 5.4
ACE_CCL.1	Pass	VMware Workspace ONE Boxer Email Client 5.4
ACE_SPD.1	Pass	VMware Workspace ONE Boxer Email Client 5.4
ACE_OBJ.1	Pass	VMware Workspace ONE Boxer Email Client 5.4
ACE_ECD.1	Pass	VMware Workspace ONE Boxer Email Client 5.4
ACE_REQ.1	Pass	VMware Workspace ONE Boxer Email Client 5.4

8 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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the EP_EMAILCLIENT_V2.0 Assurance Activities to determine whether the claims made are justified.
- **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.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance 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.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 4, dated: September 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Application Software Extended Package for Email Clients, Version 2.0, 18 June 2015.

[7] Protection Profile for Application Software, Version 1.2, 22 April 2016

[8] VMware Workspace ONE Boxer Email Client 5.4 Security Target, Version 1.0, June 13, 2019

[9] VMware Workspace ONE Boxer Email Client 5.4, Assurance Activity Report (AAR) Version 1.0, June 13, 2019