VMware Workspace ONE Boxer Email Client Version 21.05 Supplemental Administrative Guidance for Common Criteria

Version: 1.0
September 21, 2021

VMware
1155 Perimeter Center West
Suite 100
Atlanta, GA 30338

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Table of Contents

Table of Tables

Table of Figures

1 Introduction

The VMware Workspace ONE Boxer Email Client Version 21.05 (TOE) is an application software email client product that is installed on mobile devices. The Protection Profile for Application Software Version 1.3 (APP_PP) defines an application as "software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation." Additionally, the Application Software Extended Package for Email Clients Version 2.0 (EC_EP) defines an email client as "user applications that provide functionality to send, receive, access and manage email."

As a Common Criteria evaluated product, this guidance serves to define the 'evaluated configuration' in which the evaluation was performed and to summarize how to perform the security functions that were tested as part of the evaluation.

2 Intended Audience

This document is intended for VMware Workspace ONE Unified Endpoint Management (UEM) administrators and users responsible for deploying, configuring, and/or operating VMware Workspace ONE Boxer Email Client Version 21.05. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is expected to be familiar with the Security Target for VMware Workspace ONE Boxer Email Client Version 21.05 and the general CC terminology that is referenced in it. This supplemental guidance may include references to VMware Workspace ONE Boxer's standard documentation set for the product. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions on how to perform the security functions that are defined by these SFRs. The Boxer product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described here or in the VMware Workspace ONE Boxer Security Target was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the VMware Workspace ONE Boxer Security Target.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

UEM: stands for Unified Endpoint Management. UEM enables the user to configure, secure, monitor, and manage all types of mobile devices in the enterprise.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of VMware Workspace ONE Boxer that contain the security functions that were tested as part of the CC evaluation process.

UEM Console: stands for Unified Endpoint Management Console. The UEM Console is the means for an administrator to configure, monitor, and manage the mobile devices in the enterprise.

4 References

The following documents are part of the VMware Workspace ONE Boxer Email Client Version 21.05. This is the standard documentation set that is provided with the product.

[1] VMware Workspace ONE Boxer Admin Guide
[2] VMware Workspace ONE Boxer for Android User Guide
[3] VMware Workspace ONE Boxer for iOS User Guide

The following document was created in support of the Boxer evaluation:

[4] VMware Workspace ONE Boxer Email Client Version 21.05 Security Target – v1.5 (ST)

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims.

5.1 TOE Components

VMware Workspace ONE Boxer Email Client application (Boxer from this point forward) is an email client application software that is installed on mobile devices. All hardware that is present is part of the TOE's Operational Environment. In the evaluated configuration, the TOE is installed on a VID11036 certified iOS 13 device and VID11042 certified Android 10.0 device. For testing, this evaluation used an iPhone XS (iOS) and a Samsung Galaxy S10+ (Android).

The Boxer application runs on a mobile device running Apple iOS 13 OS as well as a mobile device running Android 10.0. The mobile devices will also have the VMware Workspace ONE UEM agent installed, as the devices are managed by the VMware Workspace ONE UEM Common Criteria certified mobile device management product.

The following table describes the TOE components in the evaluated configuration:

Component	Definition
VMware Workspace ONE Boxer Email Client Version 21.05 Application for Apple iOS 13*	VMware Email Client Application for iOS devices
VMware Workspace ONE Boxer Email Client Version 21.05 Application for Android 10.0*	VMware Email Client Application for Android devices

Table 5-1: TOE Components

*VID11036 certified iOS 13 and VID11042 certified Android 10.

5.2 Supporting Environment Components

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
OCSP Responder	A server deployed within the Operational Environment which confirms the validity and revocation status of certificates.
VMware Workspace ONE UEM Server	The VMware Workspace ONE UEM Server (UEM Server) is used to manage Boxer (the TOE) and its host mobile device. The UEM Server provides administrative access through its UEM Console.
VMware Workspace ONE UEM Hub Agent	The VMware Workspace ONE UEM Hub Agent (Hub Agent) is used to provide status and policy information about the device to the UEM Server. Additionally, the Hub Agent is responsible for retrieving configuration information for the managed TOE application installed on the device.
Microsoft Exchange Server 2019	Exchange server for sending and receiving emails to and from the Operational Environment configured to use ActiveSync to communicate.
Mobile Device	The hardware that runs the OS in which the application is installed. The TOE was installed on a VID11036 certified iOS 13 device and VID11042 certified Android 10 device. For testing, this evaluation used a Samsung Galaxy S10+ (Android) and an iPhone XS (iOS). **Note:** Devices will hereafter be written as “Samsung device” and “iPhone device.”

Table 5-2: Supporting Environment Components

5.3 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profiles:

- **Platform:** The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

- **Proper administrator:** The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
- **Proper user:** The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

6 Secure Installation and Configuration

VMware Workspace ONE Unified Endpoint Management (UEM) administrators are responsible for deploying Boxer according to the procedures defined within this document. Note that this information is largely derived from [1] VMware Workspace ONE Boxer Admin Guide but summarized here to discuss only actions that are required as part of the 'evaluated configuration'. The administrator is encouraged to reference this document in full in order to have in-depth awareness of the security functionality of the Boxer, including functions that may be beyond the scope of this evaluation.

6.1 Configure Boxer Management by UEM Server

Before an administrator can configure settings for Boxer through the UEM Console, the administrator must add Workspace ONE Boxer as a public application to the UEM Console.

1. Authenticate to the UEM Console.
2. Navigate to "Apps & Books" > "Applications" > "Native" > "Public" > "List View".
3. Select "Add Application".
4. Configure the text boxes that display and select "Next".
    a. Managed By – View the organization group where the application is uploaded.
    b. Platform – Choose the appropriate platform.
    c. Source – Select to search for the Boxer application in the Google Play Store (Android) or the Apple App Store (iOS).
    d. Name – Enter "Workspace ONE Boxer".
5. Locate and select the Workspace ONE Boxer app in the Search results screen.
6. Review the information that automatically populates in the Details tab.
7. Under the "Deployment" tab, choose the app delivery mode either as On-Demand or Automatic.
    a. On Demand – Deploys application to the app catalog and lets the user to decide whether and when to install it. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic.
    b. Automatic – Deploys application to a device upon enrollment. If the device is enrolled, this option immediately prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and for mobile users.
    c. Under "Policies" settings, determine how your end users receive the app.
8. Assign Terms of Use, which displays when users first access the application from the App Catalog.
9. Select Save and Assign.

6.2 Cryptographic Configuration

[iOS] TLS communication and S/MIME cryptographic services for the Boxer application are provided by the underlying platform on an iPhone device running iOS 13. The specific cryptographic implementation for the iOS platform can be found in the Apple iOS 13 Security Target documentation (VID11036).

[Android] TLS communication cryptographic services for the Boxer application are provided by the underlying platform on a Samsung Galaxy mobile device running Android 10. The specific cryptographic implementation for the Android platform can be found in the Samsung Android 10 Security Target documentation (VID11042). Additionally, when Boxer is installed on a device running Android 10, the application includes the OpenSSL software library to perform the cryptographic services for S/MIME functionality.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

6.2.1 Asymmetric Key Generation and Key Establishment Configuration

The TOE requires no special configuration in order to generate asymmetric keys and to perform key establishment, as this functionality is provided by the TOE platform.

The TOE uses assigned certificates that are generated through the UEM Server (operational environment) communicating with a certificate authority server. The assigned certificates are used for user S/MIME functionality.

The TOE invokes the platform to support asymmetric key generation in support of TLS communications. The platform provided functionality support both RSA schemes using cryptographic key sizes of 2048-bit or greater that meet FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 and ECC schemes using “NIST curves” P-256, P-384 that meet FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4.

The TOE invokes the platform in support of two key establishment schemes for establishment of TLS communications.

- RSA key establishment conforming to “NIST SP 800-56B”.
- Elliptic curve-based key establishment conforming to NIST Special Publication 800-56A.

6.2.2 S/MIME Configuration

6.2.2.1 Encryption Algorithms

To enable the usage of the AES-128-CBC and AES-256-CBC encryption algorithms for S/MIME encryption and decryption, the following configurations must be made in the UEM Console:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to “Apps & Books” > “Native” > “Public”.
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click “Save & Assign”.

6. Click on the desired assignment name.
7. Click on “Email Settings” > “S/MIME” > “EDIT”.
8. Expand “Advanced”.
9. Specify “AES128” and “AES256” for the “Supported Encryption Algorithms”.
10. Specify either “AES256” or “AES128” for the “Default Encryption Algorithm”, depending on which algorithm is desired for encrypting outgoing messages sent from Boxer.
11. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.2.2.2 Message Digest Algorithms

To enable the usage of the id-sha256, id-sha384, id-sha512 message digest algorithms for S/MIME signing, the following configurations must be made in the UEM Console:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to “Apps & Books” > “Native” > “Public”.
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click “Save & Assign”.
6. Click on the desired assignment name.
7. Click on “Email Settings” > “S/MIME” > “EDIT”.
8. Expand “Advanced”.
9. Specify “SHA256”, “SHA384”, and “SHA512” for the “Supported Signing Algorithms”.
10. Specify either “SHA256”, “SHA384”, or “SHA512” for the “Default Signing Algorithm”, depending on which algorithm is desired for encrypting outgoing messages sent from Boxer.
11. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.2.2.3 Signature Algorithms

No configuration is needed for the signature algorithm, as sha256withRSAEncryption is the only enabled algorithm by default.

6.2.2.4 User S/MIME Certificates

To configure user certificates for S/MIME:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to “Groups & Settings” > “All Settings” > “System” > “Enterprise Integration” > “Certificate Authorities”.
4. On the “Certificate Authorities” tab, click “Add”.
    a. Specify the friendly name in the name field.
    b. Specify “Microsoft ADCS” for the authority type and “ADCS” for the protocol.
    c. Specify the CA CN of the issuing CA in the authority name field.
    d. Specify the AD server hostname authentication credentials.
    e. Click “Save”.
5. Click on the “Request Templates” tab, and then click “Add”.
    a. Specify the friendly name in the name field.
    b. Specify the certificate authority that was created on the previous tab.
    c. Specify “certificatetemplate:<template_name_from_Microsoft_CA_server>” in the issuing template field.

d. Specify “CN={EmailAddress}” for the subject name.
e. Specify “2048” for the private key length.
f. Ensure “Signing” and “Encryption” are enabled.
g. Specify the following SAN types:
    i. Email Address – {EmailAddress}
    ii. User Principal Name – {UserPrincipalName}
h. Ensure “Automatic Certificate Renewal” is enabled.
    i. Specify the auto renewal period.
i. Ensure “Enable Certificate Revocation” is enabled.
j. Specify “1.3.6.1.5.5.7.3.4” for EKU Attributes.
k. Click “Save”.

6. Navigate to “Apps & Books” > “Native” > “Public”.
7. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
8. Click “Save & Assign”.
9. Click on the desired assignment name.
10. Click on “Email Settings” > “S/MIME” > “EDIT”.
11. Choose “Required” for “S/MIME Status”.
12. Specify “Defined Certificate Authority” for “Certificate Source”.
13. Specify “YES” to “Use Same Signing and Encryption Certificate”.
14. Specify the “Certificate Authority” and “Certificate Template” that were created in Steps 4 and 5, respectively.
15. For iOS, specify “Device Trust Store Only” for “S/MIME Trust Store”.
16. For Android, specify “Device and Boxer Trust Store”.
17. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.2.3 Exchange Server Configuration on UEM Console

To configure the TOE to communicate with the Exchange server, the administrator will need to perform the following steps.

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to “Apps & Books” > “Native” > “Public”.
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click “Save & Assign”.
6. Click on the desired assignment name.
7. Click on “Email Settings”.
8. Specify the “Exchange ActiveSync Host” and “EWS URL” for the Exchange server, “{UserPrincipalName}” for user and “{EmailAddress}” for email address.
9. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.3 Certificate Configuration

6.3.1 S/MIME Certificate Revocation Check Frequency Behavior

Perform the following steps to configure how frequent the TOE must check the S/MIME certificate revocation status via OCSP:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.

3. Navigate to “Apps & Books” > “Native” > “Public”.
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click “Save & Assign”.
6. Click on the desired assignment name.
7. Click on “Email Settings”.
8. Click on “ADD” under “Custom Account Configuration”.
9. Define the “Configuration Key” for “PolicySMIMEEnableRevocationCheck” specify “1”.
10. If “at a frequency equal to the value received from OCSP responder” is desired:
    a. Configure “PolicySMIMERevocationTTL” to “1”.

       NOTE: If the OCSP Responder does not provide the nextUpdate value, the TOE rejects the certificate and will set the next validity check for revocation to 7 days.

11. Else if “an administratively set value which overrides the value from OCSP responder” is desired:
    a. For “PolicySMIMERevocationTTL” specify a numeric value for the number of days to retain revocation data.
12. Else if “automatically retrieve if no previous OCSP responder value or set value exists” is desired:
    a. No special configuration other than ensuring that “PolicySMIMEEnableRevocationCheck” is set to “1” is required.
13. iOS only: “Set PolicySMIMERevocationUseAIA” to “2”
14. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.3.2 S/MIME Certificate Revocation Status Checking Configuration

When the TOE cannot reach the OCSP responder, the application can be configured by a UEM administrator via UEM Console to either:

- Reject the certificate, or
- Accept the certificate if the last revocation status is valid. Reject the certificate if the last known revocation status is unknown or was revoked.

Complete the following steps:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to “Apps & Books” > “Native” > “Public”.
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click “Save & Assign”.
6. Click on the desired assignment name.
7. Click on “Email Settings”.
8. Click on “ADD” under “Custom Account Configuration”.
9. Define the “Configuration Key” for “PolicySMIMEEnableRevocationCheck” specify “1”.
10. The following values may be selected for “PolicySMIMERevocationStrictness”:
    a. “1” – Moderate – Accept the certificate if the last revocation status is valid. Reject the certificate if the last known revocation status is unknown or was revoked.
    b. “2” – Strict – Reject the certificate
11. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.3.3 Deploying CA Certificates

Root and Intermediate CA certificates need to be provided to the mobile devices on which the TOE is installed. The administrator will need to configure UEM Server to perform this operation.

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to "Groups & Settings" > "All Settings" > "Apps" > "Settings and Policies" > "Profiles".
4. Click "Add Profile" > "SDK Profile".
5. Specify either "Apple" or "Android".
6. Click on "Credentials".
7. Upload each of the CA certificates (click the "+" icon for each additional required CA file).
8. Click "SAVE".
9. Navigate to "Apps & Books" > "Native" > "Public".
10. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
11. Click on the "SDK" tab.
12. Specify the appropriate "SDK Profile" that was created in Step 4.
13. Click "Save & Assign".
14. Click "Save".
15. Click "Publish".

6.3.4 TLS Certificate Revocation Check Frequency Behavior

Perform the following steps to configure how frequent the TOE must check the TLS certificate revocation status via OCSP:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to "Apps & Books" > "Native" > "Public".
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click "Save & Assign".
6. Click on the desired assignment name.
7. Click on "Email Settings".
8. Click on "ADD" under "Custom Account Configuration".
9. Define the "Configuration Key" for "PolicyTLSEnableRevocationCheck" specify "1".
10. If "at a frequency equal to the value received from OCSP responder" is desired:
    a. Configure "PolicyTLSRevocationTTL" to "1".

       NOTE: If the OCSP Responder does not provide the nextUpdate value, the TOE rejects the certificate and will set the next validity check for revocation to 7 days.

11. Else if "an administratively set value which overrides the value from OCSP responder" is desired:
    a. For "PolicyTLSRevocationTTL" specify a numeric value for the number of days to retain revocation data.
12. Else if "automatically retrieve if no previous OCSP responder value or set value exists" is desired:
    a. No special configuration other than ensuring that "PolicyTLSEnableRevocationCheck" is set to "1" is required.
13. iOS only: "Set PolicyTLSRevocationUseAIA" to "2"

14. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.3.5 TLS Certificate Revocation Status Checking Configuration

When the TOE cannot reach the OCSP responder, the application can be configured by a UEM administrator via UEM Console to either:

- Reject the certificate, or
- Accept the certificate if the last revocation status is valid. Reject the certificate if the last known revocation status is unknown or was revoked.

Complete the following steps:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to “Apps & Books” > “Native” > “Public”.
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click “Save & Assign”.
6. Click on the desired assignment name.
7. Click on “Email Settings”.
8. Click on “ADD” under “Custom Account Configuration”.
9. Define the “Configuration Key” for “PolicyTLSEnableRevocationCheck” specify “1”.
10. The following values may be selected for “PolicyTLSRevocationStrictness”:
    a. “1” – Moderate – Accept the certificate if the last revocation status is valid. Reject the certificate if the last known revocation status is unknown or was revoked.
    b. “2” – Strict – Reject the certificate
11. Click “SAVE”, and then “SAVE” again, and then “PUBLISH”.

6.4 Boxer Installation

The TOE can be downloaded and installed by a mobile device user performing a search for the Boxer application on either the Google Play Store (Android) or the Apple App Store (iOS) and clicking the ‘Install’ button for Android or ‘GET’ button for iOS. The connection between the mobile device and its OS specific app store occurs over HTTPS/TLS.

Section 5.1 of this document lists the properties that are associated with the TOE. When downloading the TOE, this documentation should be checked as part of the acceptance procedures so that the correctness of the software application can be verified. This includes verifying that the user is operating the correct version of Boxer by accessing the application’s Settings → About to display the installed version of Boxer.

6.5 Exchange Server Configuration on TOE

After launching the Boxer application and supplying valid application authentication credentials the first time, the user will need to enter their Exchange mailbox password (i.e. Active Directory password), which is saved by the TOE for subsequent access attempts. Upon completion, each time the user launches and authenticates to Boxer, the TOE will synchronize the user’s mailbox with the Exchange server.

The connection between each Boxer application instance and Exchange server is secured with TLS. The TLS encryption on the Boxer side is handled by the TOE's platform. Therefore, the TOE requires no special configuration as conformant TLS is provided by the Common Criteria certified TOE platform.

7 Secure Management of VMware Workspace ONE Boxer

The following sections provide information on managing TOE functionality that is relevant to the claimed Protection Profiles. Note that this information is largely derived from [2] Workspace ONE Boxer for Android User Guide and [3] Workspace ONE Boxer for iOS User Guide but summarized here to discuss only actions that are required as part of the 'evaluated configuration'. The administrator is encouraged to reference these documents in full in order to have in-depth awareness of the security functionality of the Boxer, including functions that may be beyond the scope of this evaluation.

7.1 Authenticating to the TOE

After launching the Boxer app on their mobile device, users must authenticate to the TOE by entering their passcode in order to perform any management functions.

7.2 User Management

The UEM administrator acts remotely through a centralized management console (UEM Console) in the operating environment to configure the following Protection Profile (PP) defined functionality: enable/disable plaintext only mode globally, configure message sending/receiving to only use specified cryptographic algorithms, configure cryptographic functionality such as certificates, password length requirements, and OCSP retrieval frequency.

To enable/disable plaintext-only mode globally, the following configurations must be made in the UEM Console:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to "Apps & Books" > "Native" > "Public".
4. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
5. Click "Save & Assign".
6. Click on the desired assignment name.
7. Click on "App Policies" > "Advanced".
8. Specify the "Plain Text Mode" as either "DISABLED" or "ENABLED".
9. Click "SAVE", and then "SAVE" again, and then "PUBLISH".

The TOE does not support key recovery.

At the TOE application, the User is considered the owner or user of the mobile device for which the TOE is installed. The TOE software provides one function that is considered administrative functionality to the end user: change password/passphrase authentication credential. The User of the mobile device may change their password/passphrase authentication credentials. For both Android and iOS, an administrator can force a password change by making the password complexity stricter (e.g. increase password length).

The user would be forced to change their password after having successfully authenticated with their old now non-compliant password.

7.2.1 Password Management

NOTE to the End User: Boxer will enforce the administratively defined minimum passcode length and the hardcoded maximum password length of 512 when a password is created. This passcode is used to derive cryptographic keys that are used to encrypt the Boxer database. Therefore, it is highly recommended to create a strong password of 8 or more characters that use all 4 character sets (uppercase, lowercase, numerals, special character).

TOE users are responsible for setting and changing their password/passphrase (passcode), using the following steps.

For Android:

1. Launch the TOE application.
2. Authenticate to the TOE.
3. Tap “Settings” > “Change shared passcode”.
4. Enter the current passcode.
5. Specify the new passcode.
6. Verify the new passcode.

For iOS:

1. Launch the TOE application.
2. Authenticate to the TOE.
3. Tap “Settings” > “Advanced” > “Passcode” > “Change Single Sign-On passcode”.
4. Enter the current passcode.
5. Specify the new passcode.
6. Verify the new passcode.

NOTE to the UEM Administrator: The passcode policy is used to control the passcodes used to derive the 256-bit cryptographic keys that are used to encrypt the Boxer database on the mobile device. Even though Boxer is designed to compensate for a poor passcode, by ensuring there is always enough entropy fed into the key derivation function to create a 256 bit key, it is highly recommended to create a strong passcode policy of 8 characters or more using characters from all 4 character sets (uppercase, lowercase, numerals, special character). The UEM provides additional passcode complexity and authentication failure handling settings that were not required to be tested as part of the Common Criteria Certification. See Apps / Settings and Policies / Security Policies (vmware.com) for additional information on these additional settings. The information below only covers those settings that were required for this evaluation.

Password composition requirements are configured via the UEM Console:

1. Authenticate to the UEM Console.
2. Specify the Organization Group (OG) for which to make the modifications.
3. Navigate to “Groups & Settings” > “All Settings” > “Apps” > “Settings and Policies” > “Profiles”.

4. Click on the desired Profile Name to modify.
5. Click on “Authentication”.
6. Ensure “Single Sign-On” is checked.
7. Click “SAVE”.
8. Navigate to “Apps & Books” > “Native” > “Public”.
9. Choose either the Android or iOS variant of Boxer and then click the pencil icon to edit.
10. Click “Save & Assign”.
11. Choose the assignment.
12. Under “App Policies” > “App Passcode”, choose “None”.
13. Verify “Single Sign-On” is set to “Enabled”.
14. Click “Save” and then “Save”.
15. Click “Publish”.
16. Go to “Groups and Settings”.
17. Click on “All Settings”.
18. Expand “Apps”.
19. Expand “Settings and Policies”.
20. Click on “Security Policies”.
21. Specify “Enabled” for “Single Sign-On”.
22. Choose “Passcode” for “Authentication Type”.
23. Choose “Alphanumeric” for “Passcode Mode”.
24. Set “Minimum Passcode Length” to a value between 4 and 10 characters.*
25. Click “Save”.

*NOTE: This setting only ensures that a user’s password must have the set minimum number of characters. Boxer will enforce the minimum passcode length set and the hardcoded maximum password length of 512.

7.2.2 Signing and Encrypting an Email

Full instructions are available in the “Compose Email” sections of [2] Workspace ONE Boxer for Android User Guide and [3] Workspace ONE Boxer for iOS User Guide.

Create a new email message by selecting the Compose icon. Tap the icons to perform actions or access additional functionality.

	The certificate icon allows the user to sign the email with their preloaded certificate.
	The lock icon encrypts the email sent from the device.

7.2.3 S/MIME Notifications

When the email content is viewed, the TOE shows a banner between the header and the body of the email. The banner notifies the user that the verification was successful by showing who the email was signed by and if the certificate is trusted. The banner uses color coding to help the user quickly identify

issues. The banner is black when the certificate is verified and trusted; the banner is orange when the certificate is untrusted; or the banner is red when there was a failure to decode/tampered email.

Examples of notifications are shown in Figures 7-1 through 7-12.

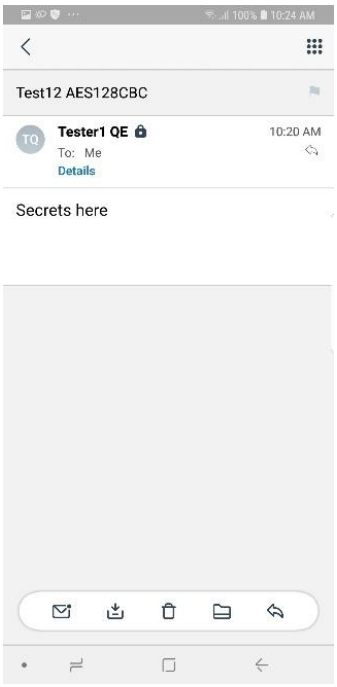

Figure 7-1: Android - Encryption Verified

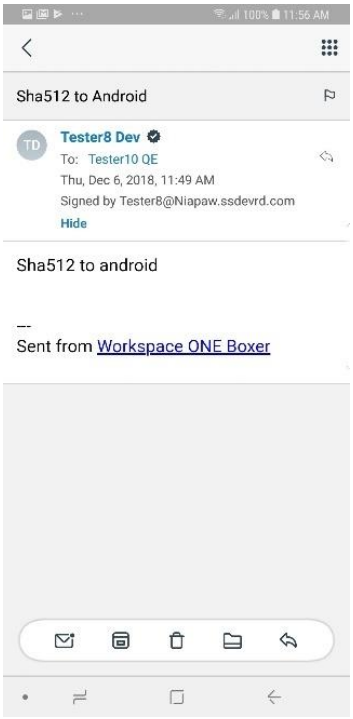

Figure 7-2: Android - Validated Signature

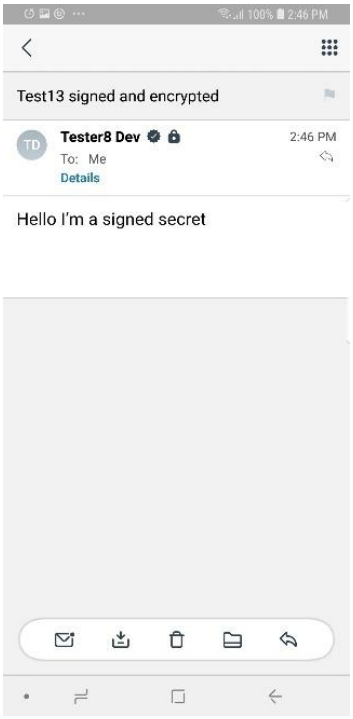

Figure 7-3: Android - Encryption Verified and Validated Signature

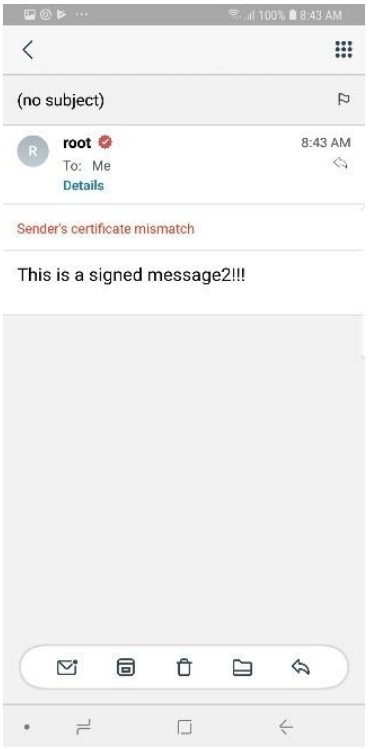

Figure 7-4: Android - Unverified and Unvalidated Signature 1

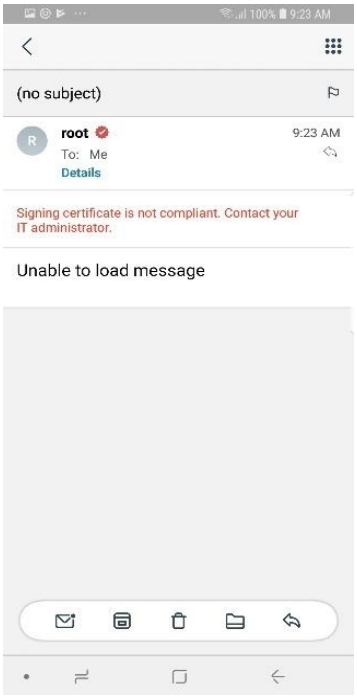

Figure 7-5: Android - Unverified and Unvalidated Signature 2

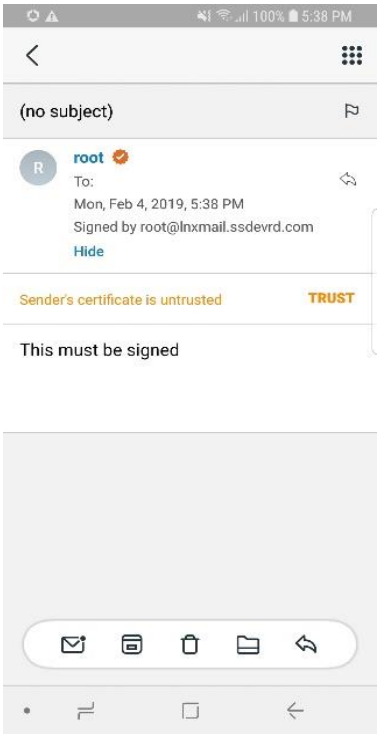

Figure 7-6: Android - Unvalidated and Unverified Signature 3

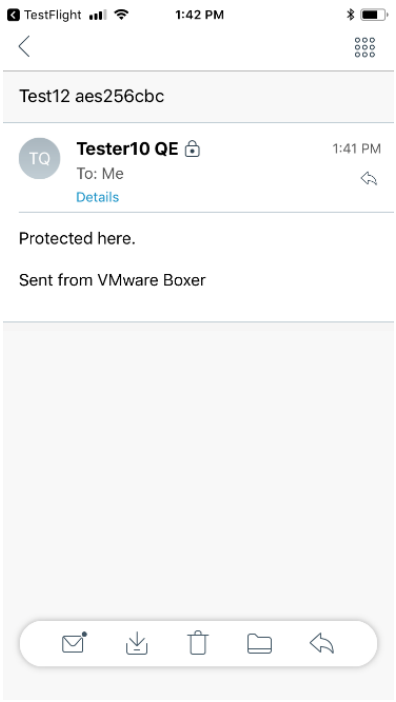

Figure 7-7: iOS - Encryption Verified

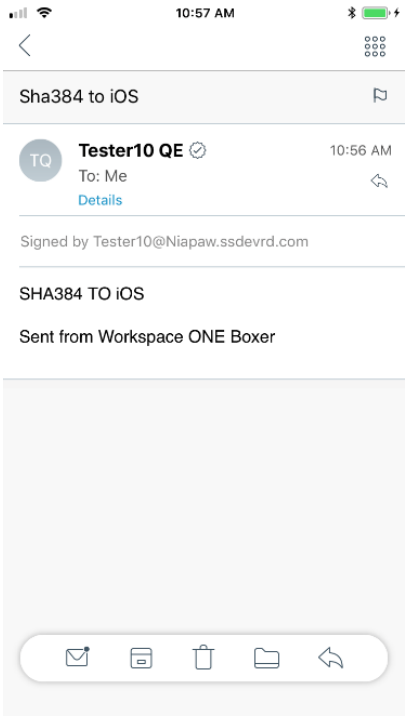

Figure 7-8: iOS -Validated Signature

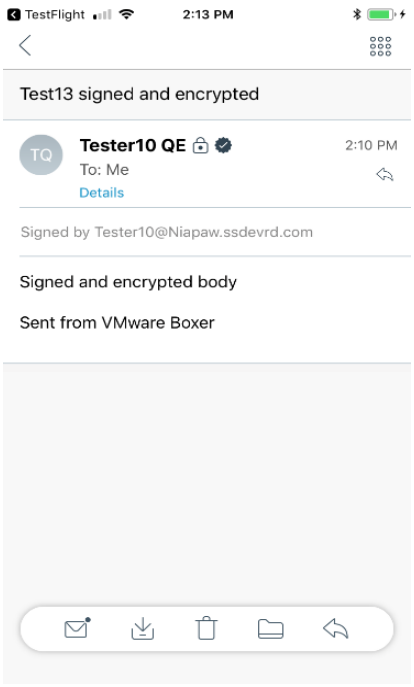

Figure 7-9: iOS - Encryption Verified and Validated Signature

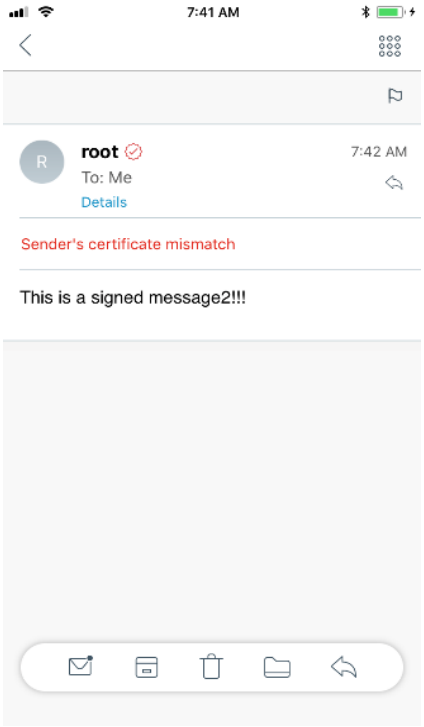

Figure 7-10: iOS - Unverified and Unvalidated Signature 1

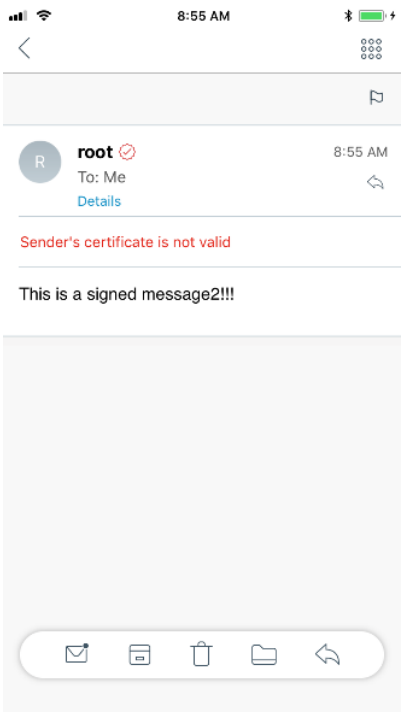

Figure 7-11: iOS - Unverified and Unvalidated Signature 2

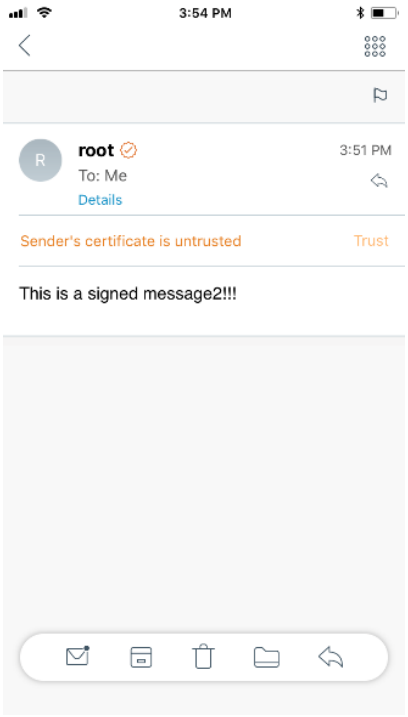

Figure 7-12: iOS - Unverified and Unvalidated Signature 3

7.2.4 TOE Add-Ons

The TOE does not support the installation of trusted or untrusted add-ons.

7.3 Secure Updates

The TOE provides a user with the ability to check the version of the TOE that is currently running on the mobile device.

> [Android] Within the application, the TOE will display the version by navigating: Settings → About. The Android OS also provides the versioning information by using the App manager.
>
> [iOS] Within the application, the TOE will display the version by navigating: Settings → About.

The TOE automatically checks to see if an update is available. If there is an update available, the user is notified that the product has an update available and directs the user to go to the appropriate app store to download. Additionally, the user can leverage the platform features to independently check for updates by navigating to the Google Play Store (Android) or the Apple App Store (iOS). The TOE does not automatically update its own binaries or executable files. The binary code is only modified or replaced if the user manually initiates the update via the platform provided update mechanism.

The application for Android is packaged in .apk format and for iOS it is packaged in .ipa format.

Updates to the TOE are provided by the Google Play Store (Android) or Apple App Store (iOS) over HTTPS/TLS. Once the update has been completed by the developer, it is then digitally signed by the developer and sent to the Google Play Store/Apple App Store. The TOE software is digitally signed using a Verisign X.509v3 certificate. The Google Play Store/Apple App Store will then verify the signature and will sign the update with its own signature. When the update gets sent to the mobile device, the mobile device will verify the signature from the Google Play Store/Apple App Store. Secure communication between the mobile device and its app store is handled by the underlying platform. This secure channel is considered part of the operating environment and is out of the scope of the evaluation.

Once an update is performed, users should verify the application's current version (Settings → About) to ensure that the update was successfully installed.

7.4 Application Access Permissions

Workspace One Boxer was designed to give users a single app with integrated mail, calendar and contacts. Therefore, the application requires the following access permissions to perform the following functionality:

- Network Connectivity
  - full network access to send/receive emails and attachments
  - receive data from Internet
  - sync email with Exchange server
- Camera
  - take pictures and videos and send as attachments
- Device Storage

    - read the contents of USB storage (internal)
    - modify or delete the contents of USB storage (internal)
    - save email attachments
    - attach files to email
- Phone
    - read phone status and identity
    - allow a phone ID to be created to assist in diagnostics and troubleshooting
- Touch/Face ID (iOS only)
    - unlock Boxer using Face ID or Touch ID
- Near Field Communications (Android only)
    - Support printing emails using NFC.
- Fingerprint (Android only)
    - unlock Boxer using fingerprint
- Vibrator (Android only)
    - Physical notifications
- Contacts (address book)
    - read user's contacts
    - modify user's contacts
    - find accounts on the device
- Calendar
    - add or modify calendar events and send email to guests
    - read calendar events
- Accounts (Android only)
    - access to multiple accounts on the system to integrate into one app access
- Profile (Android only)
    - access user profile for sharing across multiple VMware Workspace One products

8 Modes of Operation

The TOE does not support different modes. It is installed in its operational mode.

9 Obtaining Technical Assistance

VMware Workspace ONE Boxer offers technical assistance through their website at http://support.getboxer.com/ and submitting a message under "Contact support".