VMware Workspace ONE Unified Endpoint Management Supplemental Administrative Guidance

Version 1.0
February 21, 2020

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Contents

1 Introduction

VMware Workspace ONE Unified Endpoint Management (UEM) is a mobile device management (MDM) solution that is used to enforce access, usage, and security configuration policies on registered mobile devices in order to mitigate the risk of theft, malicious software, or other misuse. The VMware Workspace ONE Unified Endpoint Management is comprised of the Unified Endpoint Management Server (UEM Server) and one or more VMware Intelligent Hub Agents (iOS Hub Agent and Android Hub Agent) installed on Apple and Android devices. The minimum configuration is one Unified Endpoint Management Server, and one VMware Intelligent Hub Agent installed on an Apple device and/or one VMware Intelligent Hub Agent installed on an Android device. Including additional VMware Intelligent Hub Agents installed on multiple Apple devices and additional VMware Intelligent Hub Agents installed on multiple Android devices as part of an operational configuration will not affect the validity of the functional claims made within this document and the Common Criteria certification

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating VMware Workspace ONE UEM. 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 also expected to be familiar with the general operation of the VMware Workspace ONE UEM product. This supplemental guidance includes references to VMware's standard documentation set for the product and does not explicitly reproduce materials located there. This guidance also includes information on configuration of the behavior of the iOS Hub Agent and Android Hub Agent as well as the communications between these Hub Agents and the UEM Server. However, these activities are still performed by administrators.

The reader is also expected to be familiar with the VMware Workspace ONE Unified Endpoint Management Version 1907 Security Target and the general CC terminology that is referenced in it. 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 VMware Workspace ONE UEM product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the evaluation are discussed here. Any functionality that is not described here or in the VMware Workspace ONE Unified Endpoint Management Version 1907 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 Unified Endpoint Management Version 1907 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.

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 the VMware Workspace ONE UEM that contain the security functions that were tested as part of the CC evaluation process.

4 References

The following security-relevant documents are included with the TOE. The System Administrator needs to verify that they are using the latest version of documents [1] through [6] by downloading the latest copy of the documents from docs.vmware.com. VMware frequently makes updates to Workspace ONE UEM documentation and having the latest versions ensures that the System Administrator is following the best practices and procedures. Documentation that is not related to the functionality tested as part of the CC evaluation is not listed here.

[1] Installing Workspace ONE UEM for on-premises and SaaS deployments VMware Workspace ONE UEM 1907

[2] Upgrade Guide for on-premises and SaaS deployments VMware Workspace ONE UEM 1907

[3] Console Basics VMware Workspace ONE UEM 1907

[4] Directory Service Integration VMware Workspace ONE UEM 1907

[5] Certificate Authority Integrations VMware Workspace ONE UEM 1907

[6] Integration with Apple Business Manager VMware Workspace ONE UEM 1907

The following documents were created is support of operating system and mobile device CC evaluations on which VMware Workspace ONE UEM components are installed:

[7] Operational and Administrative Guidance Microsoft Windows 10 and Windows Server (https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2019.1018)

[8] Apple iPad and iPhone Mobile Devices with iOS 12 Common Criteria Configuration Guide Version 1.7 (https://www.niap-ccevs.org/Product/Maint.cfm?AMID=1445&PID=10937)

[9] Samsung Android 9 on Galaxy Devices Version: 5.0 (https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10979)

The following document was created in support of the VMware Workspace ONE UEM CC evaluation:

[10] VMware Workspace ONE Unified Endpoint Management Version 1907 Security Target, Version 1.0

5 Evaluated Configuration

This section lists the components that have been included in the product'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

The TOE is the VMware Workspace ONE Unified Endpoint Management version 1907 that includes the TOE components described in the following table:

Table 1: Evaluated Components of the TOE

Component	Definition
Workspace ONE Unified Endpoint Management 1907 (UEM Server)	This satisfies the MDM Server Component of the TOE as it provides an enterprise-level management capability for a collection of mobile devices, including the administration of mobile device policies, reporting on device behavior, and sending commands to the iOS and Android Hub Agent(s). This MDM Server Component also provides a Mobile Application Store (MAS) Server that allows managed devices to download apps from a trusted repository.
Android Intelligent Hub Agent 19.08 (Android Hub Agent)	This satisfies the MDM Agent Component of the TOE as it is a VMware-developed application installed on mobile devices running the Samsung Android 9 operating system and uses the Android platform to establish a secure connection back to the UEM Server for the Android Hub Agent can provide status and policy information about the device.
iOS Intelligent Hub Agent 19.09 (iOS Hub Agent)	This satisfies the MDM Agent Component of the TOE as it is a VMware-developed application installed on mobile devices running the Apple iOS 12 operating system and uses the iOS platform to establish a secure connection back to the UEM Server for the iOS Hub Agent and iOS platform to provide status and policy information about the device.

The TOE boundary on the end user mobile devices includes only the iOS and Android Hub Agents itself; the actual devices have been evaluated against the Mobile Device Fundamentals Protection Profile under the Validation ID number identified in Table 2 below.

5.2 Supporting Environmental Components

The following table lists components and applications in the TOE's operational environment that must be present for the TOE to be operating in its evaluated configuration:

Table 2: Evaluated Components of the Operational Environment

Component	Definition
Active Directory / LDAP Server	Identity store that defines users for device enrollment and administrator accounts for access to the Admin Console. In the evaluated configuration, Windows Server 2016 (Version 1803) Active Directory/LDAP Server is used.
Apple iOS 12 Mobile Device (VID10937)	The MDM Agent Component of the TOE (Hub Agent) is an application that is installed on Apple mobile devices running iOS 12 operating systems so that the TOE can provide management functionality to the device.

Apple Push Notification Service (APNS) / Apple DEP	APNS is an iOS platform push notification service that enables the UEM Server to notify iOS Hub Agents and the iOS platform to connect directly to the UEM Server to retrieve data (e.g. policies). Apple DEP is an online service that automates the enrollment of iOS devices into the TOE in the evaluated configuration.
Certification Authority (CA) Server	The MDM Server Component and Android Hub Agent of the TOE connect to the CA Server during device enrollment so that the TOE can provide each device with a unique certificate generated by the CA Server. In the evaluated configuration, Windows Server 2016 (Version 1803) Active Directory Certificate Services is used.
Firebase Cloud Messaging Service (FCM)	FCM is an Android platform push notification service that enables the UEM Server to notify Android Hub Agents to connect directly to the UEM Server to retrieve data (e.g. policies).
Samsung Android 9 Mobile Device (VID 10979)	The MDM Agent Component of the TOE (Hub Agent) is an application that is installed on mobile devices running Android 9 operating systems so that the TOE can provide management functionality to the device.
SQL database	The TOE's RDBMS database used to store configuration settings and device data. In the evaluated configuration, Microsoft SQL Server 2012 Enterprise is used.
Syslog Server	The MDM Server Component of the TOE connects to the Syslog Server to persistently store audit data for the UEM Server's own operation as well as the audit data collected from the Hub Agent that it manages.
Windows Server 2016 (Version 1803)	This is the OS that the UEM Server is installed on.
Workstation	Any general-purpose computer that is used by an administrator to manage the TOE via the Admin Console and a user to manage their device via the Self-Service Portal. For the TOE to be accessed remotely, the workstation is required to have a browser to access the TOE's GUI based interfaces.

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:

- **Trusted components of the TOE:** The administrators need to perform assessments and define compliance policies to verify the availability of all TOE components and their audit functions to reduce the risk of an undetected attack on (or failure of) one or more TOE components
- **Availability of network connectivity:** VMware Workspace ONE UEM requires network connectivity in order to perform its functions, specifically its management of mobile devices. In cases where network connectivity is lost between TOE components, security on the mobile devices enrolled into the TOE's management is still enforced.
- **Trustworthiness of server platform:** The system on which the VMware server application is installed and the local network that it resides in is assumed to be configured securely and to have access to functionality, such as: reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services.
- **Trustworthiness of device platform:** The iOS and Android Hub Agents will be installed on mobile devices configured in accordance with their own Common Criteria evaluated configurations and will provide access to functionality, such as policy enforcement, cryptographic

services, data protection as well as trusted updates and software integrity verification of the Hub Agents.

- **Trusted administration:** Administrators are expected to be trusted individuals with relevant technical skills for administration of VMware Workspace ONE UEM and are expected to read and abide by its configuration instructions, including this supplemental guidance.
- **Proper users:** Users of mobile devices are expected to not be willfully negligent or hostile and will use the mobile device in a manner that complies with their organizational security policies.

6 Secure Acceptance, Installation, and Initial Configuration

6.1 Server Installation

The System Administrator will need to download the installation package files for VMware Workspace ONE UEM. The link to these files is provided as part of the deployment process by the Workspace ONE UEM consultant (VMware employee) assigned to the system administrator's organization.

In the evaluated configuration, VMware Workspace ONE UEM was deployed in an On-Premises configuration as described in [10]. This deployment consists of a single instance of the UEM Server application that resides in an internal network. VMware documentation may refer to the "Workspace ONE UEM Console Server" and "Workspace ONE UEM Device Services Server" which is the UEM Server performing specific functions for administrative management of the product and management of the devices, respectively. In the evaluated configuration, there is a single instance of the UEM Server that performs both of these functions and for this reason, these terms are referring to the same UEM Server instance.

The UEM Server also include the Mobile Application Store (MAS) Server functionality evaluated. This is installed automatically as part of the UEM Server software and is not a separate TOE component. However, since certain Common Criteria requirements explicitly reference MAS Server functionality separately from the remainder of the MDM capabilities, its configuration and use is discussed separately when necessary.

The following procedures describe the initial installation of the UEM Server and supporting operational environment components:

1. Install and/or configure the following supporting operational environment components as prerequisites to the installation of the UEM Server:
    a. Windows Server 2016 – Refer to [7] and Chapter 2 of [1] regarding software and hardware requirements as well as configuration instructions
    b. SQL database – Refer to Table 2 for software requirements and Chapter 2 of [1] for configuration instructions
    c. Active Directory / LDAP Server – Refer to Table 2 for software requirements
    d. Certification Authority (CA) Server – Refer to Table 2 for software requirements
    e. Syslog Server – Prepare organizational syslog server to receive audit data from UEM Server
2. Setup the database by completing the procedures in [1] Chapter 3 under "Run the Workspace ONE UEM Database Setup Utility" and "Verify Proper Database Installation"

3. Install VMware Workspace ONE UEM by following the procedures in [1] Chapter 4. Under "Run the Workspace ONE UEM Installer on Each Application Server (Console and Device Services)" perform the following specific selections:
    a. At Step 6 ("Select the Workspace ONE UEM features that you want to install on the specific server"), disable "AirWatch Cloud Messaging (AWCM) and "Default Redirect Site" when configuring the TOE features.
    b. At Step 12, choose "No" to opt-out of participating in the VMware User Experience Improvement Program.
4. Install post-installation patch by following the procedures in [2] Chapter 5 under "Perform a Patch Upgrade".
5. On the database server, execute the following database query to enable the required level of auditing for UEM Server:

```
UPDATE DBO.SystemCode
SET DefaultValue = 'True'
WHERE SystemCodeID = 5122
```

6. On the database server, execute the following database query to enable the mutual authentication capability between the UEM Server and Hub Agents (mobile devices):

```
UPDATE DBO.SystemCode
SET DefaultValue = 'True'
WHERE SystemCodeID = 5107
```

7. On the database server, execute the following database query to enable the ability to upload a policy signing certificate to the UEM Server:

```
UPDATE dbo.SystemCodeCategory
SET ResourceID = 7192
WHERE SystemCodeCategoryID = 370
```

8. On the database server, execute the following database query to configure the Device Scheduler execution periodicity to 30 seconds on the UEM Server:

```
UPDATE scheduler.QRTZ_SIMPLE_TRIGGERS
SET REPEAT_INTERVAL = 30000
WHERE TRIGGER_NAME LIKE 'b7719b0d-3941-40e4-9d0b-1ea99d55f3ad'
```

9. On the database server, execute the EventLogFilterFix.sql database query to enable the ability to view the maximum amount of audit events from within the UEM Server. The EventLogFilterFix.sql file can be requested from the Workspace ONE UEM consultant (VMware employee) assigned to the system administrator's organization.
10. Upload UEM Server's X.509v3 certificate by completing the following steps:
    a. Launch Certificate Manager as the Computer account.
    b. Import the X.509v3 certificate to be used by the UEM Server into the "Personal" certificate category.

11. Configure UEM Server for TLS mutual authentication with the mobile device by completing the following steps:
    a. Launch IIS Manager.
    b. Go to “Sites” > “Default Web Site” > “DeviceServices”.
    c. Click on “SSL Settings”.
    d. Check “Require SSL” and choose “Require” for Client certificates.
    e. Launch an elevated command prompt by entering “cmd.exe” at the Run box.
    f. Enter the following commands at the command prompt:
        1. netsh http show sslcert ipport=0.0.0.0:443
        2. netsh http delete sslcert ipport=0.0.0.0:443
        3. netsh http add sslcert ipport=0.0.0.0:443 certhash=[cert hash from above] appid={[GUID from above]} certstorename=MY verifyclientcertrevocation=enable VerifyRevocationWithCachedClientCertOnly=disable UsageCheck=Enable clientcertnegotiation=enable
        4. netsh http show sslcert
    g. Launch IIS Manager.
    h. Go to “Sites” > “Default Web Site”.
    i. Click on “Bindings…”.
    j. Click “Add…”.
    k. Choose “https” for the type, specify “All Unassigned” for IP address, specify “8443” for the port.
    l. Specify the X.509v3 certificate uploaded in Step 10 then click “OK”.
12. On the UEM Server, open the AirWatch/AirWatch 1907/Services/AW.ChangeEvent.QueueService.exe.config file in a text editor.
    a. Add the following string to the file in the <appSettings></appSettings> section:

        ```
        <!-- setting to enable TLS cert validation -->
        <add key="ValidateSyslogCert" value="true"/>
        ```

    b. On the UEM Server, launch services.msc
    c. Restart the “AirWatch Entity Change Queue Monitor” service.
13. On the UEM Server, open the AirWatch/AirWatch 1907/Websites/WanderingWiFi.AirWatch.Console.Web/Web.config file in a text editor.
    a. Add the following string to the file in the <appSettings></appSettings> section:

        ```
        <!-- setting to enable TLS cert validation -->
        <add key="ValidateSyslogCert" value="true"/>
        ```

    b. On the UEM server, restart IIS by executing the following commands:

        ```
        iisreset
        ```

14. On the UEM Server, open the AirWatch/AirWatch 1907/WebSites/WanderingWiFi.AirWatch.Console.Web/web.config, AirWatch/AirWatch 1907/Services/AW.ChangeEvent.QueueService.exe.config files in a text editor.
    a. Add the following string to the file in the <appSettings></appSettings> section:

        ```
        <add key=”OutboundTlsProtocols” value=”Tls12”/>
        ```

b. On the UEM Server, launch services.msc
c. Restart the "AirWatch Entity Change Queue Monitor" service.

15. On the UEM Server, limit the TLS ciphersuites such that only the claimed ciphers are enabled.
    a. Launch Start > Run > "gpedit.msc".
    b. Navigate to "Computer Configuration" > "Administrative Templates" > "Network" > "SSL Configuration Settings" > "SSL Cipher Suite Order".
    c. Enable "SSL Cipher Suite Order".
    d. Specify the following claimed SSL cipher suites in the text box.

        TLS_RSA_WITH_AES_128_CBC_SHA256
        TLS_RSA_WITH_AES_256_CBC_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

    e. Click "Apply" then "OK".
    f. Restart the system.
16. Ensure the following Windows Services are running on the UEM Server host machine:

    AirWatch API Workflow
    AirWatch Background Processor Service
    AirWatch Batch Processing Service
    AirWatch Compliance Service
    AirWatch Content Delivery
    AirWatch DataPlatform Service
    AirWatch Device Scheduler
    AirWatch Directory Sync Service
    AirWatch Entity Change Queue Monitor
    AirWatch Entity Reconcile Service
    AirWatch Eventlog Processor Service
    AirWatch GEM Inventory Service
    AirWatch Integration Service
    AirWatch Interrogator Queue Monitor
    AirWatch MEG Queue Service
    AirWatch Messaging Service
    AirWatch Outbound Queue Monitor Service
    AirWatch Policy Engine
    AirWatch Provisioning Package Service
    AirWatch Smart Group Service
    AirWatch SMS Service
    AirWatch Tunnel Service

17. After installation, use the following default credentials to authenticate to the UEM Server's Admin Console:

    Username: administrator
    Password: airwatch

18. Change the default password and then accept the license agreement.
19. Specify the password recovery questions and security PIN.
20. Configure the UEM Server to communicate with Apple Push Notification Service (APNS) by following the procedures in [3] Chapter 2 under "Generate a New APNs Certificate".
21. Configure the UEM Server to communicate with an external Active Directory / LDAP Server by following the procedures in [4].
22. Configure the UEM Server to communicate with the Certification Authority server by following the procedures in [5] Chapters 2 and 3.
23. Complete the mutual authentication configuration on the UEM Server:
    a. On the Admin Console, navigate to "Groups & Settings" > "All Settings" > "System" > "Advanced" > "Site URLs".
    b. Specify the "Device Management URL" to: https://[*UEM Server hostname*]:8443/DeviceManagement
    c. Specify the "MDM Enrollment URL" to: https://[*UEM Server hostname*]:8443/DeviceManagement/Enrollment
    d. Navigate to "Groups & Settings" > "All Settings" > "System" > "Security" > "Mutual TLS Authentication".
    e. For iOS, specify the Certificate Authority and Certificate Template for the Device Enrollment Profile and Hub Authentication Settings.
    f. For Android, specify the Certificate Authority and Certificate Template.
24. Configure the UEM Server to communicate with the external Syslog Server:
    a. On the Admin Console, navigate to "Groups & Settings" > "All Settings" > "System" > "Enterprise Integration" > "Syslog".
    b. Specify the "Hostname" of the Syslog Server, "Protocol" (SECURETCP), and "Port" (6514).
    c. Specify the Syslog Facility as "Kernel Messages".
    d. Click "Test Connection".
    e. Click "Save".
25. Configure the log level for auditing:
    a. On the Admin Console, verify "Organizational Group" is set to "Global".
    b. Navigate to "Groups & Settings" > "All Settings" > "Admin" > "Events" > "Event Settings"
    c. Set "Device" and "Console" to "Debug (7 and above)"
26. Configure the audit record format:
    a. On the Admin Console, navigate to "Groups & Settings > "All Settings" > "Devices & Users" > "General" > "Friendly Name".
    b. Specify the "Device Friendly Name Format" as follows:

       {EnrollmentUser} {DeviceModel} {DeviceOperatingSystem} {DeviceSerialNumber}

    c. Click "Save"
    d. Navigate to "Monitor" > "Reports and Analytics" > "Events" > "Syslog".
    e. Specify the "Message Content" as follows:

       AirWatch Syslog Details are as follows Event Type: {EventType}; Event: {Event}; User: {User}; Device Name: {DeviceFriendlyName}; EnrollmentUser: {EnrollmentUser}; Event Source: {EventSource}; Event Module: {EventModule}; Event Category: {EventCategory}; Event Data: {EventData}

    f. Click "Save"

27. Configure the UEM Server to communicate with Apple Device Enrollment Program (DEP) by following the procedures in [6] Chapter 2.
28. Configure the UEM Server for communication with an SMTP Server:
    a. On the Admin Console, navigate to "Groups & Settings" > "All Settings" > "Enterprise Integration" > "Email (SMTP)".
    b. Enter in the SMTP server and port.
    c. Click "Save".
29. Perform the following configuration settings to UEM Server:
    a. On the Admin Console, navigate to "Groups & Settings" > "All Settings" > "Installation" > "Performance Tuning".
    b. Ensure "Allow minutes as minimum compliance interval" is checked.
30. Upload the policy signing certificate to the UEM Server for use with the Android and iOS Hub Agents:
    a. On the Admin Console, navigate to "Groups & Settings" > "All Settings" > "System" > "Advanced" > "Policy Signing Certificate".
    b. Upload a valid X.509v3 policy signing certificate.
31. Upload the policy signing certificate to the UEM Server for use with the iOS platform:
    a. Navigate to "Groups & Settings" > "All Settings" > "Devices & Users" > "Apple" > "Profiles".
    b. Toggle "ENABLED" for "Sign Profiles (Requires Server SSL Certificate)".
    c. Click "UPLOAD" to upload a valid X.509v3 policy signing certificate and then click "SAVE".

6.2 Device Configuration, Agent Installation, and Enrollment

6.2.1 Configure Android Enrollment Restrictions

The UEM Server provides the ability to restrict Android devices from enrollment based upon the following restrictions and their associated procedures.

Limit enrollment to specific Android devices by IMEI:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to "Groups & Settings" > "All Settings" > "Devices & Users" > "General" > "Enrollment" > "Authentication".
3. Ensure "Devices Enrollment Mode" is set to "Registered Devices Only".
4. Navigate to "Devices" > "Lifecycle" > "Enrollment Status" > "ADD" > "Whitelist Devices".
5. Specify the whitelisted IMEIs.
6. Specify "IMEI" for device attribute.

Limit enrollment to specific Android devices by serial number:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to "Groups & Settings" > "All Settings" > "Devices & Users" > "General" > "Enrollment" > "Authentication".
3. Ensure "Devices Enrollment Mode" is set to "Registered Devices Only".
4. Navigate to "Devices" > "Lifecycle" > "Enrollment Status" > "ADD" > "Whitelist Devices".
5. Specify the whitelisted serial numbers.
6. Specify "Serial Number" for device attribute.

Limit enrollment of Android devices by specific device models:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Enrollment” > “Restrictions” > “ADD POLICY”.
3. Specify the Enrollment Policy Name, Organization Group, Policy Type.
4. Check “Allowed Device Types – Limit enrollment to specific platforms, models or operating systems”.
5. Specify “Only allow listed device types (Whitelist).”
6. Click “Add Device Restriction”.
7. Specify the Platform to Android, then choose the Manufacturer and Model.
8. Specify the Device Limit per User value and the operating system to “Any”.

Limit enrollment of Android devices by the number of devices:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Enrollment” > “Restrictions” > “ADD POLICY”.
3. Specify the Enrollment Policy Name, Organization Group, Policy Type.
4. Check “Device Limit per User”.
5. Specify “Maximum Devices Per User” value.

Limit enrollment of Android devices by manufacturer:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Enrollment” > “Restrictions” > “ADD POLICY”.
3. Specify the Enrollment Policy Name, Organization Group, Policy Type.
4. Check “Allowed Device Types – Limit enrollment to specific platforms, models or operating systems”.
5. Specify “Only allow listed device types (Whitelist).”
6. Click “Add Device Restriction”.
7. Specify the Platform to Android, choose a Manufacturer, and specify the Model to “Any”.
8. Specify the Device Limit per User value and the operating system to “Any”.

Limit enrollment of Android devices by operating system:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Enrollment” > “Restrictions” > “ADD POLICY”.
3. Specify the Enrollment Policy Name, Organization Group, Policy Type.
4. Check “Allowed Device Types – Limit enrollment to specific platforms, models or operating systems”.
5. Specify “Only allow listed device types (Whitelist).”
6. Click “Add Device Restriction”.
7. Specify the Platform to Android, specify the Manufacturer and then specify the Model to “Any”.
8. Specify the Device Limit per User value and the operating system.

6.2.2 Configure iOS Enrollment Restrictions

The UEM Server provides the ability to restrict iOS devices from enrollment based upon the following restrictions and their associated procedures.

Limit Enrollment to Specific Devices based on DEP identifier:

NOTE: This enrollment restriction configuration requires that the UEM Server is registered with the Apple Device Enrollment Program (DEP). Initial configuration with Apple DEP is described in Section 6.1. Once the procedures in Section 6.1 are performed, the UEM Server the UEM Server will acquire the list of registered devices through periodic synchronization with Apple DEP. For more information, refer to the procedures in [6] Chapter 2.

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Enrollment”.
3. Specify “Registered Devices Only” for “Devices Enrollment Mode”.

6.2.3 Prevent Android Device Unenrollment By User Configuration

In the evaluated configuration, the UEM Server is configured to prevent the unauthorized removal of the Android Hub Agent's software from the mobile device. When configured in this manner, the Android Hub Agent will perform the following actions to prevent unenrollment:

- Removes the unenrollment button;
- Disables the user from demoting the Android Hub Agent from a device Administrator (preventing uninstall); and
- Removes the ability to uninstall the Android Hub Agent through the Google Play Store.

The following procedures are performed to prevent unauthorized Android Device unenrollment:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “Android” > “Intelligent Hub Settings”.
3. Choose “ENABLED” for “Block User Unenrollment”.
4. Click “SAVE”.

6.2.4 Prevent iOS Device Unenrollment By User Configuration

Apple DEP provides the unenrollment protection mechanism for the UEM Server through the use of the Lock MDM Profile feature. The iOS Hub Agent leverages the functionality provided by the underlying device platform, which has been enrolled in Apple DEP, to prevent the unauthorized removal of the iOS Hub Agent software.

The following procedures are performed to prevent unauthorized iOS Device unenrollment:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “Apple” > “Device Enrollment Program”.
3. Edit the DEP profile configured in Section 6.1.
4. Choose “ENABLED” for “Lock MDM Profile”.

5. Click “SAVE”.

6.2.5 Mobile Device User Accounts

There are two methods of configuring user authentication for device enrollment:

- **Basic:** The account has a username/password defined by an Authorized Administrator on the UEM Server.
- **LDAP:** The UEM Server is connected to an Active Directory/LDAP Server that is used as a third-party identity store.

As part of the procedures in Section 6.1, the UEM Server was configured to communicate with an Active Directory/LDAP Server. This is all of the configuration necessary on the UEM Server for LDAP based user enrollment. To create a user account for the Basic method of user authentication, perform the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Accounts” > “Users” > “List View”.
3. From the main navigation menu, choose “Add” > “Add User”.
4. Populate the following fields in order to create a user account:

   Security Type
   Username
   Password
   Full Name
   Email Address
   Enrollment Organization Group
   User Role
   Notification Message Type

5. Click Save to create the user account.

6.2.6 Enrollment of Android Devices

In order to ensure that VMware Workspace ONE UEM is deployed in a manner that is consistent with the assumptions defined in Section 5.3 of this document, the underlying Android mobile device must be configured in a manner consistent with its Common Criteria evaluated configuration. Guidance for this can be found in the Common Criteria guidance at [9].

A user enrolls their Android mobile device through a series of steps. First, the user powers on the mobile device and follows the standard Android Setup Assistant instructions, including language, country/region, and Wi-Fi network. Once the device has been set up, the user will need to download the Android Hub Agent from the Google Play Store.

The device user will then enter the UEM Server’s IP address into the Android Hub Agent which will be used to establish the enrollment connection to the UEM Server. The user provides their credentials to authenticate to the UEM Server and then the enrollment process begins. The UEM Server will then provide the MDM profiles assigned to the device and initiate the SCEP process for the product to receive its unique X.509v3 certificate.

During enrollment the Android Hub Agent will record the UEM Server's DNS name and full URL with hostname as the reference identifier for the UEM Server. The presented identifier in the UEM Server's certificate is the same as the reference identifier of the UEM Server. To verify the reference identifier on an Android device, follow these procedures:

1. On the Android device, launch the Android Hub Agent.
2. Tap "This Device".
3. Tap "Enrollment".
4. Observe that the "Enrolled Server" is the reference identifier.

6.2.7 Enrollment of iOS Devices

In order to ensure that VMware Workspace ONE UEM is deployed in a manner that is consistent with the assumptions defined in Section 5.3 of this document, the underlying iOS mobile device must be configured in a manner consistent with its Common Criteria evaluated configuration. Guidance for this can be found in the Common Criteria guidance at [8].

A user enrolls their iOS mobile device through a series of steps. First, an Administrator will enroll the device in Apple DEP which is performed using the device's serial number. Then the user powers on the mobile device and follows the standard iOS Setup Assistant instructions, including language, country/region, and Wi-Fi network. Additionally, the iOS Setup Assistant will continue the enrollment process to the UEM Server through Apple DEP. Procedures for enrolling a device in Apple DEP are found in [6] Chapter 2 under "Apple Business Manager Device Enrollment".

As part of enrolling in Apple DEP, the iOS platform will receive the UEM Server's URL which will be used to establish the enrollment connection to the UEM Server. The user provides their credentials to authenticate to the UEM Server. Once authentication is successful, the iOS Hub Agent is then deployed as a managed app by the UEM Server to the iOS mobile device. The UEM Server will then provide the MDM profiles assigned to the device, which will include the device's unique X.509v3 certificate.

During enrollment the iOS platform and iOS Hub Agent will record the UEM Server's DNS name and full URL with hostname as the reference identifier for the UEM Server. The presented identifier in the UEM Server's certificate is the same as the reference identifier of the UEM Server. To verify the reference identifier on an iOS device, follow these procedures:

iOS Platform:

1. On the iOS device, tap "Settings" > "General" > "Device Management" > "Device Manager".
2. Tap "More Details".
3. Tap "MDM Settings".
4. Observe that the "Server URL" is the reference identifier.

iOS Hub Agent:

1. Launch the iOS Hub Agent on the mobile device.
2. Tap "This Device" > "Enrollment".
3. Observe that the "Server" is the reference identifier URL.

6.2.8 Force Android Device to Unenroll From Management

An Administrator is able to force an Android device to unenroll from management and prevent the device from enrolling again by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Devices” > “List View”.
3. Choose the specific mobile device to execute a Device Wipe under the “General Info” column.
4. Choose “More Actions” from the top right-hand menu then “Enterprise Wipe” under the Management heading.
5. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Enrollment” > “Authentication”.
6. Ensure “Devices Enrollment Mode” is set to “Registered Devices Only”.
7. Navigate to “Devices” > “Lifecycle” > “Enrollment Status” > “ADD” > “Whitelist Devices”.
8. Remove the whitelisted attributed (e.g. IMEI) corresponding to the device that was unenrolled.
9. Specify the whitelisted attributed (e.g. IMEI) for device attribute.

6.2.9 Force iOS Device to Unenroll From Management

An Administrator is able to force an iOS device to unenroll from management and prevent the device from enrolling again by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Devices” > “List View”.
3. Choose the specific mobile device to execute a Device Wipe under the “General Info” column.
4. Choose “More Actions” from the top right-hand menu then “Enterprise Wipe” under the Management heading.
5. Remove the device from Apple DEP by performing the procedures in [6] Chapter 2 under “Disassociate Devices From the Apple Business Manager”.

6.3 Cryptographic Engine Configuration

Cryptographic services for the UEM Server are provided by the underlying Windows server platform. The Windows Server 2016 platform uses Microsoft’s BCryptPrimitives.dll and CNG.sys to perform all cryptographic services.

Cryptographic services for the iOS and Android Hub Agents are mainly provided by the underlying mobile device platforms. The iOS Hub Agent uses Apple iOS platform’s CoreCrypto Module to perform all claimed cryptographic services. The Android Hub Agent uses the Android platform’s SCrypto and BoringSSL cryptographic modules to perform all claimed cryptographic services, except for the policy digital signature validation requirements. The Android Hub Agent implements OpenSSL for the specific purpose of performing the policy digital signature validation services.

Refer to the platform Security Targets at [7], [8], and [9] for more information about the cryptographic functionality provided by the Windows Server, iOS, and Android platforms and their corresponding cryptographic certificates.

Section 6.1 contains all steps necessary to configure the cryptographic modules used by VMware Workspace ONE UEM in the evaluated configuration. There are no specific steps that are required to

follow in order to configure key generation and establishment functionality; these functions are provided automatically by the underlying cryptographic modules and are specified by the specific protocols that require them.

This evaluation does not make any claims of cryptographic strength for any other cryptographic modules or configurations besides what is claimed in the VMware Workspace ONE Unified Endpoint Management Version 1907 Security Target, refer to [10].

6.4 Installing and Verifying Product Updates

6.4.1 Verifying UEM Server and Hub Agent Versions

The software versions of the UEM Server and Hub Agents can be verified by and Administrator. The UEM Server software can be checked by clicking on the "About" button on the UEM Server's Admin Console. Each iOS and Android Hub Agent's current software version can also be queried through the UEM Server's Admin Console through the following procedures:

Android Hub Agent:

1. Authenticate to the Admin Console.
2. Navigate to "Devices" > "List View".
3. Click on the enrolled mobile device details view.
4. Navigate to "More" > "Custom Attributes".
5. Verify the Android Hub Agent version value for Application "com.airwatch.androidagent.identity.xml", Attribute "identity.agentVersion".

iOS Hub Agent:

1. Authenticate to the Admin Console.
2. Navigate to "Devices" > "List View".
3. Click on the enrolled mobile device details view.
4. Click on "Apps" tab.
5. Verify the iOS Hub Agent version.

Additionally, mobile device users can query their Hub Agent version using the following procedures on their mobile device:

Android Hub Agent:

1. Launch the Android Hub Agent.
2. Tap "About".

iOS Hub Agent:

1. Launch the iOS Hub Agent.
2. Tap "About".

6.4.2 Update UEM Server Software

Updates for the UEM Server are downloaded as a zip package from the VMware support website. An Administrator can login to https://support.workspaceone.com/, then navigate to Software > Console, or at

https://resources.workspaceone.com/software/console. The Administrator installs a post-installation patch to update the software by following the procedures in [2] Chapter 5 under "Perform a Patch Upgrade". The UEM Server software updates are installed by the underlying platform directly onto the system; the platform does not have an automatic method of pulling down or installing the updates without the System Administrator (local authorized administrator of the platform) initiation via the platform. The updates are digitally signed using a Digicert X.509v3 certificate which is installed in the Windows trusted key store on the underlying platform which verifies the software updates.

Prior to installation, the following procedures will perform a software integrity check on the patch update:

1. Execute the following command:

   signtool.exe verify /a /pa /v <UEM-Server-Software-Update>

2. Verify that the signtool.exe application returns with "Successfully verified: <filename>".

6.4.3 Update Hub Agent Software

Updates to the Hub Agents' software are provided by the Google Play Store (Android), Apple Store (iOS), or the UEM Server store. The Hub Agents' software updates are signed using a public CA certificate during the software build and loaded onto the Google Play Store/Apple Store. The Google Play Store/Apple Store will then verify the signature and will sign the update with its own signature. The software update is downloaded onto the device by the mobile device user, the platform will verify the signature from the Google Play Store/Apple Store/UEM Server store.

Software updates to the Hub Agent software may be manually initiated by the user of the mobile device by accessing the Google Play Store, Apple Store or UEM Server store and installing an updated version of the Hub Agent app.

Alternatively, the Administrator can configure an update push to attempt to automatically update the Hub Agent software. For procedures on performing an update push to an existing application (i.e. Hub Agent), refer to Section 7.5.3.

7 Secure Management of the TOE

7.1 Authenticating to the UEM Server

7.1.1 Mobile Device Users to the Self-Service Portal

The UEM Server provides mobile device users access to the Self-Service Portal for the purposes of remote device registration and other self-service tasks. The Self-Service Portal can be accessed using the following procedures:

1. Navigate to the MDM Self-Service Portal in a web browser:

   https://[*UEM Server hostname*]/MyDevice

2. Authenticate with assigned credentials to the Self-Service Portal.

7.1.2 Administrators to the Admin Console

The UEM Server provides mobile device users access to the Admin Console for the purposes of remote administration of the UEM Server and management of the mobile devices. The Admin Console can be accessed using the following procedures:

1. Navigate to the MDM Self-Service Portal in a web browser:

   https://[*UEM Server hostname*]/AirWatch

2. Authenticate with assigned credentials to the Admin Console.

7.1.3 Administrator Login Session Timeout Configuration

The UEM Server provides the ability to configure the idle timeout for administrator sessions by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Admin” > “Console Security” > “Session Management”
3. Specify the time in minutes for “Idle Session Timeout” and click “Save”.

7.1.4 Login Banner Configuration

The UEM Server supports the ability to display a configurable warning banner on the Admin Console and the Self-Service Portal login pages. The warning banner will be displayed to both Administrators and users prior to authenticating to the UEM Server on their respective interfaces. The warning banner can be configured by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings”.
3. Under the “System” heading choose “Branding”.
4. Select the “Override” value for the “Current Setting”.
5. Upload the Login Page and Self-Service Portal Login Page Background containing the warning message.
6. Click on “Custom CSS” and enter the following:

   #login { background-color: rgba(0, 0, 0, 0); } .login-bg-img

   { background-size: contain; }

7. Click “Save”.

7.2 Administrative Roles and Privileges

All administration of VMware Workspace ONE UEM is performed through the Admin Console. The Admin Console can have multiple administrator accounts, each with differing roles and levels of privilege. Administrators are viewed and managed under “Accounts” > “Administrators”. The “List

View" option shows all administrators defined by the Admin Console. New administrators are also defined here using the "Add" button. Administrative privileges are derived from two sources: Role, which determines the read/write permissions that the administrator has for various functions; and Organization Group, which defines the scope of control over which the authorized functions can be performed. Roles can be created, modified, and viewed under "Accounts" > "Administrators" > "Roles". The Create Role dialog lists all the various activities that can be assigned to a role and the ability to grant read and/or edit permissions for those activities. Note that an administrator who is creating a new Role cannot define privileges for it that the administrator's current Role does not already have.

Organization Groups are derived from the connected Active Directory server and are defined in the environment. However, data relating to these (such as child organizations) can be configured in the Admin Console under "Groups & Settings" > "Organization Groups" > "Organization Group Details".

For more information on the management of administrative accounts and role management, refer to [3] Chapter 3 under "Admin Accounts" and Chapter 4.

The DoD Annex for Mobile Device Management mandates administrative separation of duties through the use of several roles, each of which have a defined set of responsibilities. VMware Workspace ONE UEM accommodates the ability to meet this mandate through a combination of pre-defined administrative roles and the ability to create new roles with arbitrarily-defined privileges. The following table lists and describes the roles from the DoD Annex and how to configure the VMware Workspace ONE UEM to support them.

Table 3: Roles

Role	Description	Configured By
Server primary administrator	Responsible for server installation, initial configuration, and maintenance functions. Responsible for the setup and maintenance of security configuration administrator and auditor accounts.	Defined by default as "System Administrator" role.
Security configuration administrator	Responsible for security configuration of the server, setup and maintenance of mobile device profiles, definition of user groups, and setup and maintenance of the device user group administrator role, its members, and its permissions.	Defined by default as "AirWatch Administrator" role.
Device user group administrator	Responsible for maintenance of user accounts, including setup, change of account configurations, and account deletion.	Defined by default as "Device Manager" role.
Auditor	Responsible for review and maintenance of server and device audit logs.	Defined by default as "Report Viewer" role.

7.3 Connectivity Status And Periodicity Of Device Data

The connectivity status between the UEM Server and an enrolled device can be checked from both ends of the connection. An administrator on the UEM Console can check the connectivity status of a particular device by navigating to "Devices" > "List View", clicking the check box next to the entry for that device, and selecting "Query". The Last Seen column depicts the connection status of the device, and if the

device is not connected, the last time the connection was active. To check connectivity status from the Hub Agent side of the connection, launch the Hub Agent on the mobile device and select “My Device”. The connectivity status will be displayed.

The UEM Server will periodically check the status of enrolled devices for connectivity over an administrator-defined time interval and will collect data about the device, including:

- Connectivity status
- Current version of the MD firmware/software
- Current version of the hardware model of the device
- Current version of installed mobile applications

These values are configured globally for each device platform. The Android Hub Agent will connect to the UEM Server performing a network reachability test based upon the “Heartbeat Internal” which will update the Last Seen time of the device in the Admin Console. The collecting of information on the device by the Android Hub Agent occurs every ‘Data Sample Interval’. The Android Hub Agent then queues each sample interval of collected data, and will send up to the last 10 sample intervals of collected data to the UEM Server once the ‘Data Transmit Interval’ is reached. The following procedures are performed to collect this data from Android devices:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices and Users” > “Android” > “Intelligent Hub Settings”.
3. Specify values for the “Heartbeat Interval”, the “Data Transmit Interval”, and the “Data Sample Interval”.

The iOS Hub Agent also has the ability to configure the periodicity of reachability events by enforcing the sampling interval values that are configured on the UEM Server. When the UEM Server communicates with the iOS Hub Agent for policy/sample data, this is considered to be a reachability event since the outcome of this activity updates the Last Seen time of the device in the Admin Console. The following procedures are performed to collect this data from iOS devices:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices and Users” > “Apple” > “MDM Sample Schedule”.
3. Specify values for the configurable options on the “MDM Sample Schedule” page.

The UEM Server also allows an Administrator to limit the privacy-sensitive information that will and will not be collected on a managed device. The Administrator is able to configure this by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Privacy”
3. Toggle the selection for the different privacy-sensitive information categories (e.g. Personal Applications) between “Collect and Display”, “Collect Do Not Display” and “Do Not Collect”.
4. Click “SAVE” and then confirm by entering the Console Security PIN.

7.4 Device and Policy Configuration

The UEM Console provides the ability to issue commands remotely to managed devices. Devices can be viewed under “Devices” > “List View”. Selecting an individual device will open the “Details View” page

for that particular device. When issuing a command to the device, it may be handled on the device side of the connection by either the Hub Agent or the device's platform, but this is transparent to both the mobile device user and Administrator. The following table, taken from the VMware Workspace ONE Unified Endpoint Management Version 1907 Security Target [10], lists the commands and profiles (policies) used to manage and configure the mobile devices being managed. The table lists the management functions that can be performed by an Administrator, how those functions are initiated, as well as whether this behavior is enforced by the iOS and Android Hub Agent or by the underlying mobile device platform. Unless specified otherwise, the management function is initiated from the device "Details View" in the Admin Console.

Table 4: UEM Server Management Functions

iOS			Android		
Command	**Claimed in VID10937[1]**	**Implemented By**	**Command**	**Claimed in VID10979[2]**	**Implemented By**
1. transition to the locked state – "Lock" button.	Yes	Platform	**1. transition to the locked state** – "Lock" button.	Yes	Hub Agent
2. full wipe of protected data – "More" Actions" button > Device Wipe.	Yes	Platform	**2. full wipe of protected data –** "More Actions" button > Device Wipe.	Yes	Hub Agent
3. unenroll from management – "More" Actions" button > Device Wipe.	Yes	Platform	**3. unenroll from management** – "More Actions" button > Enterprise Wipe.	No	Hub Agent
4. install policies – assigned and applied to target devices at the creation or modification of a profile under Devices > Profiles & Resources > Profiles.	No	Platform	**4. install policies** – assigned and applied to target devices at the creation or modification of a profile under Devices > Profiles & Resources > Profiles.	No	Hub Agent
5. query connectivity status – "Query" button.	No	Platform	**5. query connectivity status** – "Query" button.	No	Hub Agent
6. query the current version of the MD firmware/software – "Query" button. Status shown in the main detail view page.	No	Platform	**6. query the current version of the MD firmware/software** – "Query" button. Status shown in the main detail view page.	No	Hub Agent
7. query the current version of the hardware model of the device – "Query" button. Status shown in the main detail view page.	No	Platform	**7. query the current version of the hardware model of the device** – "Query" button. Status shown in the main detail view page.	No	Hub Agent
8. query the current version of installed mobile applications – "Query" button. Status shown in the Apps tab under the main detail view page.	No	Platform	**8. query the current version of installed mobile applications** – "Query" button. Status shown in the Apps tab under the main detail view page.	No	Hub Agent

[1] TD0479
[2] TD0479

9. import X.509v3 certificates into the Trust Anchor Database – assigned and applied to devices as part of a policy under the "Credentials" tab when defining the policy.	Yes	Platform	**9. import X.509v3 certificates into the Trust Anchor Database** – assigned and applied to devices as part of a policy under the "Credentials" tab when defining the policy.	Yes	Hub Agent
10. install applications – Apps and Books tab, Details View. Admin will be prompted to define what devices an application is assigned to during definition or modification of the application. When the application is specified as automatic distribution, the installation is initiated by the TSF.	Yes	Platform	**10. install applications –** Apps and Books tab, Details View. Admin will be prompted to define what devices an application is assigned to during definition or modification of the application. When the application is specified as automatic distribution, the installation is initiated by the TSF.	Yes	Hub Agent
11. update system software – the UEM Server will send command to the iOS platform to update to the latest OS, then the iOS platform will reach out to Apple to get the latest OS.	Yes	Platform	**11. update system software –** the UEM Server will send command to Samsung's Enterprise Firmware Over the Air (E-FOTA) Server to update to the latest OS, then the E-FOTA Server will push the updated software to the devices.	Yes	Platform
12. remove applications – only Enterprise applications can be removed on iOS, refer to Function 13	Yes	Platform	**12. remove applications –** only Enterprise applications can be removed on Android, refer to Function 13	Yes	Hub Agent
13. remove Enterprise applications – specific application from a single device: Device details, Apps tab, Remove option ("X") button for the desired application.	Yes	Platform	**13. remove Enterprise applications –** specific application from a single device: Device details, Apps tab, Remove option button for the desired application.	Yes	Hub Agent
14. wipe Enterprise data – "More Actions" button > Enterprise Wipe.	Yes	Platform	**14. wipe Enterprise data –** "More Actions" button > Enterprise Wipe.	Yes	Hub Agent
15. remove imported X.509v3 certificates – "More" tab > "Certificates", Revoke option.	Yes	Platform	**15. remove imported X.509v3 certificates –** "Devices" > Profiles > choose the profile that pushed the certificate > "Devices" > "Remove Profile"	Yes	Hub Agent
16. alert the user – "Send" button. Note that this refers to alerting the user of the mobile device, not an Administrator on the UEM Server. This can be sent	No	Hub Agent (push notification), Platform (SMS)	**16. alert the user –** "Send" button. Note that this refers to alerting the user of the mobile device, not an Administrator on the UEM	No	Hub Agent (push notification), Platform (SMS)

as an email, SMS, or push notification.			Server. This can be sent as an email, SMS, or push notification.		
22. place applications into application process groups – Apps & Books > Applications > Applications Settings > App Groups.	No	Platform	**22. place applications into application process groups –** Apps & Books > Applications > Applications Settings > App Groups.	No	Hub Agent
23. revoke Biometric template – by deleting the passcode, this disables the biometric template for use.	No	Platform			
25. password policy – defined in the Passcode properties of a profile.	Yes	Platform	**25. password policy –** defined in the Passcode properties of a profile.	Yes	Hub Agent
26. session locking policy – Defined in the Passcode properties of a profile.	Yes	Platform	**26. session locking policy –** Defined in the Passcode properties of a profile.	Yes	Hub Agent
27. wireless networks (SSIDs) to which the MD may connect – Defined under the Wi-Fi properties of a profile.	No	Platform	**27. wireless networks (SSIDs) to which the MD may connect –** Defined under the Wi-Fi properties of a profile.	Yes	Hub Agent
28. security policy for each wireless network – defined in the Wi-Fi properties of a profile; the permitted CA(s) are defined by reference on the Wi-Fi properties to those defined under Credentials.	Yes	Platform	**28. security policy for each wireless network –** defined in the Wi-Fi properties of a profile; the permitted CA(s) are defined by reference on the Wi-Fi properties to those defined under Credentials.	Yes	Hub Agent
29. application installation policy – groups of required, whitelisted, and/or blacklisted apps can be defined in Apps & Books > Application Settings >App Groups. Note that iOS does not provide a mechanism to pre-emptively enforce application whitelisting/blacklisting but the TOE can take corrective action if a compliance policy is defined to detect the presence of a blacklisted or non-whitelisted app.	Yes	Platform	**29. application installation policy –** groups of required, whitelisted, and/or blacklisted apps can be defined in Apps & Books > Application Settings >App Groups.	Yes	Hub Agent
30. enable/disable policy for camera and screen capture across device – defined in the Restrictions properties of a profile.	Yes	Platform	**30. enable/disable policy for camera, microphone, and screen capture across device –** defined in the Restrictions properties of a profile.	Yes	Hub Agent
31. enable/disable policy for the VPN across MD and on a per-app basis – defined in the VPN properties of a profile or	Yes	Platform	**31. enable/disable policy for the VPN across MD –** defined in the VPN properties of a profile.	Yes	Hub Agent

in the "VPN Access" setting for an individual app assignment.					
			32. enable/disable policy for Wi-Fi, cellular, Bluetooth, and NFC – defined in the "Restrictions" tab of a profile.	Yes	Hub Agent
			33. enable/disable policy for data signaling – defined in the "Restrictions" tab of a profile.	No	Hub Agent
			34. enable/disable policy for Wi-Fi tethering, USB tethering, and Bluetooth tethering – defined in the "Restrictions" tab of a profile.	Yes	Hub Agent
			35. enable/disable policy for developer modes – defined in the "Restrictions" tab of a profile.	Yes	Hub Agent
36. enable policy for data-at-rest protection – For iOS devices, data-at-rest protection is automatically enabled if a passcode is set so this is configured under the Passcode properties of a profile.	Yes	Platform	**36. enable policy for data-at-rest protection –** "Require Storage Encryption" and "Require SD Card Encryption" options in the Passcode tab of a profile.	Yes	Hub Agent
			37. enable policy for removable media's data-at-rest protection – "Require SD Card Encryption" from the Passcode tab of a profile.	Yes	Hub Agent
40. enable/disable policy for display notification in the locked state – can enable/disable any notification on a per-app basis based upon the bundle ID.	Yes	Platform	**40. enable/disable policy for display notification in the locked state** – can enable/disable all notification through "Allow Notifications" defined in the "Restrictions" properties of a profile.	Yes	Hub Agent
47. the unlock banner policy – configured through the 'if lost return' function.	Yes	Platform	**47. the unlock banner policy** – "Lockscreen Overlay" under the Passcode tab in a profile.	Yes	Hub Agent
			49. enable/disable USB mass storage mode – defined in the "Restrictions" properties of a profile.	Yes	Hub Agent
50. enable/disable backup – defined in the "Restrictions" tab of a profile under the iCloud subcategory.	No	Platform	**50. enable/disable backup –** defined in the "Restrictions" tab of a profile.	No	Hub Agent
			52. enable/disable location services – defined in the	Yes	Hub Agent

			"Restrictions" tab of a profile.		
			53. enable/disable policy for user unenrollment – defined in the "Restrictions" tab of a profile.	No	Hub Agent
			54. enable/disable policy for the Always-On VPN protection across device – defined in the VPN properties of a profile.	Yes	Hub Agent
55. enable/disable policy for use of Biometric Authentication Factor – defined in the "Restrictions" tab of a profile.	Yes	Platform	**55. enable/disable policy for use of Biometric Authentication Factor** – defined in the Passcode properties of a profile.	Yes	Hub Agent
			58. enable/disable automatic updates of system software – defined on the Restrictions properties of a profile, "Allow OTA Upgrade"	No	Hub Agent
			59. enable/disable removable media – defined on the Restrictions properties of a profile, "Allow SD Card Access"	No	Hub Agent
60. application installation policy – groups of required, whitelisted, and/or blacklisted apps can be defined in Apps & Books > Application Settings >App Groups. Note that iOS does not provide a mechanism to pre-emptively enforce application whitelisting/blacklisting but the TOE can take corrective action if a compliance policy is defined to detect the presence of a blacklisted or non-whitelisted app. Note: Command #60 is an extension of Command #29 since allowed applications are only managed by name and not version.	Yes	Platform	**60. application installation policy –** groups of required, whitelisted, and/or blacklisted apps can be defined in Apps & Books > Application Settings >App Groups. Note: Command #60 is an extension of Command #29 since allowed applications are only managed by name and not version.	Yes	Hub Agent
61. iOS Hub Agent passcode authentication policy – specifying complexity requirements for authenticating to the Hub Agent can be defined in Settings > Apps >	No	Hub Agent			

Settings and Policies > Security Policies					

7.4.1 Profiles and Compliance Policies Configuration

Profiles (policies) for mobile devices are defined on the Admin Console under "Devices" > "Profiles & Resources" > "Profiles". Existing profiles will be listed here and the "Add" > "Add Profile" option allows for a new profile to be defined. Profiles are platform specific, so if an equivalent security configuration is required for both Android and iOS, a profile needs to be created under each platform. When defining a new profile, an assignment to an Organization, User Group, or Smart Group (refer to Section 7.5.1) is specified so that the profile is only applied to the relevant devices, users, and/or organizational members. AirWatch provides a large number of device settings and policies that can be defined within a profile, refer to Table 4 above for those included within the evaluation.

The Admin Console also provides Administrators the ability to create compliance policies. A compliance policy can be used to identify when a mobile device's configuration, apps and data is in conflict with the compliance policy. This is accomplished by having the Hub Agent periodically collect data regarding its mobile device and sending it to the UEM Server for analysis against the configured compliance policies. This is used to identify when a violation has occurred and the device is in a Not Compliant state (e.g. blacklisted apps). An Administrator can create a compliance policy using the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to "Devices" > "Compliance Policies" > select platform.
3. Choose "Add".
4. Select "Compliance Policy".
5. Choose applicable platform (Android or iOS) managed by the organization.
6. In drop-down, select to match "All" of the chosen policies, or "Any" of the chosen policies.
7. In first drop-down menu, select Rule to enforce, and in second drop-down, select particular caveats of chosen Rule as appropriate.
8. Click "Next".
9. In first drop-down, select particular action type, and in second drop-down, select particular caveats of Action to execute (Note: This action will automatically take place when device is found to be out of compliance with the "Rule" defined above).
10. Click "Next".
11. Click in "Assigned Groups" box, and select which Organization, User Group, or Smart Group to which the Compliance Policy will apply.
12. Click "Next".
13. Review Summary and click "Finish and Activate".

7.4.2 Administrator Alerts

The UEM Server provides Administrators with the ability to view information about enrolled mobile devices and to generate alerts when various events occur. Alerts are generated based on configurable compliance policies that can detect when a violation has occurred and to mark the affected device as Not Compliant in the device's overview in the Admin Console. The Administrator can configure UEM Server to send an alert upon detection of a violation of a compliance policy by selecting "Notify" > "Send Email to Administrator" and adding their email address during the definition of the compliance policy.

Administrators can view information about the status of managed devices through the UEM Admin Console. Two of the dashboards that are accessible from the Main Menu are "Monitor" and "Devices".

From the “Monitor” section of the Admin Console, Authorized Administrators can view the total number of enrolled and unenrolled devices, the total number of compliance violations, devices that failed to install policies (profiles) and which devices have blacklisted apps, devices without required apps, or devices with apps that are not whitelisted. The Administrator can also view the applications that are associated with particular devices, including application versions. From the “Devices” section of the Admin Console, the Administrator can view changes in the enrollment status of a device by viewing the enrollment status and enrollment history information. This also lists devices that are enrolled but do not have policies applied to them. The Administrator can also view the list of compromised (jailbroken/rooted) devices under this section of the Admin Console as well as detailed information about any specific device that the UEM Server knows about.

In addition to being able to review this information on demand, Authorized Administrators can configure the delivery of periodic (daily, weekly, monthly) alert emails from the “Monitor” section of the Admin Console for the following events when they are observed on a device:

- Presence of blacklisted apps
- Presence of non-whitelisted apps
- Absence of required apps
- Compromised (jailbroken or rooted) device
- Last time a device communicated with the UEM Server
- Unapproved model (iOS only)
- Unapproved device manufacturer (Android only)
- Unapproved operating system version (greater than, less than, equal to, not equal to specified version)

The process of rooting an Android device requires the device to be rebooted. During device reboot, the Android Hub Agent will detect the device has been rooted. If the device is connected to Wi-Fi, the Android Hub Agent will send an alert to the UEM Server and will wipe the device. If the device is not connected to Wi-Fi, an alert cannot be sent due to the lack of a connection and the Android Hub Agent will wipe the device. Since performing a device wipe will also remove the Android Hub Agent, this will prevent it from queuing the alert for a rooted device.

Administrators can also configure UEM Server to generate email alerts when devices enroll and unenroll in management by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Notifications”.
3. Choose “Override” for the Current Setting.
4. Under “Device Enrolled Successfully” choose “Send Email To: Administrator”.
5. Specify a valid administrator e-mail address and message template for successful device enrollment.
6. Under “Device Unenrolled” choose “Send Email To: Administrator”.
7. Specify a valid administrator e-mail address and message template for successful device enrollment.
8. Save the configuration.

7.5 MAS Server Configuration

VMware Workspace ONE UEM’s MAS Server capabilities are provided by the UEM Server.

7.5.1 Grouping Applications

Applications managed by the MAS Server are assigned to users via “smart groups”. A smart group consists of one or more organization groups, user groups, and device characteristics. Smart groups are listed under “Groups & Settings” > “Groups” > “Assignment Groups”. New smart groups can be created via the “Add Smart Group” button on this page. Once a smart group has been created, it can be assigned to an application. New applications are defined in the MAS Server under “Apps & Books” > “Applications” > “List View” using the “Add Application” button. When adding a new application, the “Assignment” tab is used to specify the initial smart group assignment. The “Save & Assign” button is used to commit this assignment after uploading the app. Existing applications are also listed here. To modify the group assignment for an existing application, select the application in the list view and select the “Assign” button, followed by “Update Assignment”. In both cases, the “Select Assignment Groups” text box allows the mapped group(s) to be specified.

The Administrator can perform the following functions by executing their associated procedures:

Create User Group:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “Groups” > “User Groups”
3. Select the “Add” dropdown -> “Add User Group”
4. Select “Custom” Type user group, provide details, and click “Save”.

Add User to New Group:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Accounts” > “Users” > “List View”
3. Select the check box next to the user to be added to the group.
4. Select the “More Actions” dropdown -> “Add to User Group”
5. Set the Group Name of the user group and click “Save”.

Create Assignment Group and Exclude User:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Groups & Settings” > “Groups” > “Assignment Groups”

3. Select “Add Smart Group”
4. Set the “User Group” selection to the User Group.
5. Add the user to be excluded in “Exclusions” -> “Excluded Users” and click “Add”.
6. Click “Save”.

Associate an Application with the Assignment Group:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Apps & Books” > “Applications” > “Native”
3. Select the radio button next to the app you would like to associate with the group and click “Assign”.
4. Select “Add Assignment”.
5. Provide the name of the assignment group created and click “Add”.
6. Click “Save and Publish”.

7.5.2 Application Installation Policies

Applications can also be grouped together when they share a common usage profile. The following types of groups can be defined:

- Whitelist: a device’s Hub Agent will notify the UEM Server if an app that is absent from the whitelist is present on the device.
- Blacklist: a device’s Hub Agent will notify the UEM Server if an app that is present on the blacklist is present on the device.
- Required: a device’s Hub Agent will notify the UEM Server if an app that is present on the required list is absent from the device.

These are defined through Compliance Policies (refer to Section 7.4.1). On the “Rules” tab or a Compliance Policy, application-related rules can be chosen using the “Application List” dropdown option. From here, the “Contains Non-Whitelisted App(s)”, “Contains Blacklisted App(s)”, and “Does Not Contain Required App(s)” options correspond to the violations listed above. Additional actions, such as sending an email alert to an Administrator or requiring a device check-in, can be specified in the “Actions” tab. The “Assignment” tab, like with the application assignments themselves, allow the applicable Organization, User Group, or Smart Group for this Compliance Policy to be assigned.

Note that a whitelist and blacklist policy can both be applied to the same device. In this case, the app whitelist acts as an exception to apps on the blacklist so they can be installed. This occurs when a device is part of multiple smart groups.

There are differences in how compliance policies for required apps, blacklisted apps, and whitelisted apps are enforced on Android and iOS devices based upon the functionality provided to an MDM through the operating system’s APIs:

- For Android devices, a blacklisted app cannot be installed after the policy with the blacklist is applied to the device. If the app is already installed when blacklist policy is applied, the Android Hub Agent will disable the app which makes it non-executable. The disable functionality is performed instead of removal of the app for BYOD purposes. If a single app is whitelisted, all other apps are considered blacklisted (except system apps).

- For iOS devices, iOS does not provide the ability to automatically push apps onto a device or the mandatory prohibition of blacklisted or non-whitelisted apps, so all enforcement of required/whitelisted/blacklisted apps is handled in a reactive manner. Additionally, if an iOS app is specified as automatically pushed to the device, the MD user will still be prompted to accept the app before it is downloaded and installed.

7.5.3 Application Download

For any applications that reside in the UEM Server's MAS Server functionality or public applications that are referenced through external links, the Administrator has the ability to assign one or more Smart Groups to the app to push it to a set of devices or make it available to be downloaded by them. This assignment can be used to determine if the app is automatically pushed to certain devices based on Smart Group membership or if it is available on demand.

Mobile device users can download applications from the UEM Server's application store by performing the following procedures:

1. On the mobile device, launch the MDM Agent > "App Catalog".
2. Choose "Install" for the specified application to be installed on the mobile device.

Administrators can make an application accessible for download (ON DEMAND) by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Assign an application to a Smart Group by navigating to "Apps & Books" > "Internal" > "Add Application".
3. Specify the Organization Group ID and Application File then click "Continue" and "Save & Assign".
4. Click "Add Assignment" and specify the Smart Group.
5. Specify the App Delivery Method to "ON DEMAND" and then click "ADD".
6. Click "Save & Publish".
7. Click "PUBLISH".

Administrators can initiate an application download or update push (AUTO) to a device by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Assign application or an update to an existing application to a Smart Group by navigating to "Apps & Books" > "Internal" > "Add Application".
3. Specify the Organization Group ID and Application File then click "Continue" and "Save & Assign".
4. Click "Add Assignment" and specify the Smart Group.
5. Specify the App Delivery Method to "AUTO" and then click "ADD".
6. Click "Save & Publish".
7. Click "PUBLISH".

8 Auditable Events

8.1 Audit Data

8.1.1 UEM Server and Hub Agent Auditing

The UEM Server, iOS Hub Agent, and Android Hub Agent components of the TOE generate auditable events for their own behavior. Since the MAS Server is the same logical component as the UEM Server, all auditable events for both components will be treated identically. The TOE components also rely on their underlying platform to generate audit events.

The UEM Server stores all of the TOE's audit records within the SQL database. The UEM Server will also use syslog to transmit audit data to a remote Syslog Server as a permanent method of remote audit storage. The procedures for configuring the TOE's audit mechanisms and the connection to the Syslog Server are defined in Section 6.1. The only requirements of the Syslog Server are that it support the syslog and TLS 1.2 protocols. Audit data is also streamed simultaneously to the Syslog Server as it is generated. When data is transmitted to the Syslog server, it continues to be retained on the MDM Server. The MDM Server's copy of the audit data is retained indefinitely.

8.1.2 Review of Audit Data

Audit data generated by the TOE are always visible in the Admin Console under "Monitor" > "Reports & Analytics" > "Events". This is further broken down into "Device Events" for audit records of Hub Agent activity and "Console Events" for audit records of UEM Server activity. The only exception to this is Administrator login history, which can also be viewed under "Accounts" > "Administrators" > "System Activity" > "Login Activity". Audit records can also be reviewed via the Syslog Server.

TOE audit records are recorded with the following format:

> {Syslog Date and Time} {UEM Server IP Address} {Date and Time} {UEM Server Name} AirWatch Syslog Details are as follows Event Type: {EventType}; Event: {Event}; User: {User}; Device Name: {DeviceFriendlyName}; EnrollmentUser: {EnrollmentUser}; Event Source: {EventSource}; Event Module: {EventModule}; Event Category: {EventCategory}; Event Data: {EventData}

The audit records that are generated include at least the following information: date and time of the event {Date and Time}, event type {EventCategory}, subject identity {User}, and success or failure of the event {Event}. When identifying the mobile device this will be in the Device Name: {DeviceFriendlyName} field. Additional contents required by the audit records are usually found in the Event Data: {EventData} field.

8.1.3 Example Audit Records

The following Table lists the auditable events that are generated by the UEM Server, iOS Hub Agent, and Android Hub Agent TOE components as well as their underlying platforms in the course of executing the TOE's security functionality. The table includes the event and an example audit record for events generated by a TOE component. For events generated by the platform, refer to guidance documentation provided by the platforms at [7], [8], and [9].

Table 5: Audit Record Examples

Auditable Event(s)	Audit Record Examples	Component Generating Record
Type of alert. [FAU_ALT_EXT.1]	**Change in enrollment status (enrolled Android)** Oct 2 10:59:05 172.16.72.29 October 02 14:58:16 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: Tester1Local Android Android 9.0 RF8M803LV4L; EnrollmentUser: Tester1Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 2, 2019 14:58:15 **Change in enrollment status (enrolled iOS)** Oct 25 09:22:40 172.16.72.29 October 25 13:23:25 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: Tester2Local iPhone Apple 12.4 F4GY207GKXKV; EnrollmentUser: Tester2Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 25, 2019 13:23:25 **Change in enrollment status (unenrolled)** Oct 23 12:56:15 172.16.72.29 October 23 16:56:22 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMConfirmed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Event Timestamp: October 23, 2019 16:56:22 **Failure to apply policies to a mobile device** Oct 24 11:29:29 172.16.72.29 October 24 15:29:31 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileFailed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Command; Event Data: Event Timestamp: October 24, 2019 15:29:28 **Presence of blacklisted apps**, **Presence of non-whitelisted apps**, and A**bsence of required apps** Oct 23 09:16:36 172.16.72.29 October 23 13:16:43 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Category: ComplianceStatus; Event Data: CompliancePolicy=Application List;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=doe_john@company.com;NotificationMessageTemplateName=Compliance Violation Admin Notification (HTML) Event Timestamp: October 23, 2019 13:16:43 **Compromised (jailbroken or rooted) device** Oct 24 14:17:12 172.16.72.29 October 24 18:17:03 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=Compromised Status;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=doe_john@company.com;NotificationMessageTemplateName=Compliance Violation Admin Notification (HTML) Event Timestamp: October 24, 2019 18:17:03 **Last time a device communicated with the MDM Server** Oct 21 15:30:44 172.16.72.29 October 21 19:30:51 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=Device Last Seen;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=doe_john@company.com;NotificationMessageTemplateName=Compliance Violation Admin Notification (HTML) Event Timestamp: October 21, 2019 19:30:51 **Unapproved model (iOS only)** Oct 23 08:37:14 172.16.72.29 October 23 12:37:21 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=Model;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=doe_john@company.com;NotificationMessageTemplateName=Compliance Violation Admin Notification (HTML) Event Timestamp: October 23, 2019 12:37:21 **Unapproved device manufacturer (Android only)**	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Oct 21 15:33:46 172.16.72.29 October 21 19:33:53 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=Device Manufacturer;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=doe_john@company.com;NotificationMessageTemplateName=Compliance Violation Admin Notification (HTML) Event Timestamp: October 21, 2019 19:33:53 **Unapproved operating system version** Oct 21 15:35:48 172.16.72.29 October 21 19:35:55 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=OS Version;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=doe_john@company.com;NotificationMessageTemplateName=Compliance Violation Admin Notification (HTML) Event Timestamp: October 21, 2019 19:35:55	
Start-up and shutdown of the MDM System [FAU_GEN.1.1(1)]	Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, and Android Platform
All administrative actions [FAU_GEN.1.1(1)]	Refer to audit records in the following rows of this table for types of administrative action audits: • "Enabling/Disabling communications between a pair of components" • "Issuance of command to perform function. Change of policy settings." • "Success or failure of function. (Android)" • "Success or failure of function. (iOS)" • "Change in banner setting."	UEM Server
Commands issued to the MDM Agent [FAU_GEN.1.1(1)]	Refer to audit records in row under "Issuance of command to perform function. Change of policy settings."	UEM Server
MDM Agent alerts [FAU_GEN.1.1(1)]	Refer to row under "Success/failure of sending alert. (Android)" and "Success/failure of sending alert. (iOS)"	Android Hub Agent, and iOS Platform
Enabling/Disabling communications	**Enabling communications between a pair of components (Android)**	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
between a pair of components. [FCO_CPC_EXT.1]	Feb 28 09:16:21 172.16.72.29 February 28 14:16:21 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToEnrollmentWhiteList; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=RF8M803LV4L;LocationGroup=Global Event Timestamp: February 28, 2020 14:16:21 **Enabling communications between a pair of components (iOS)** Feb 28 10:44:42 172.16.72.29 February 28 15:44:42 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToAppleDep; User: ; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=FFMX76VPKPHC;LocationGroup=Company Event Timestamp: February 28, 2020 15:44:42 **Disabling communications between a pair of components** Oct 23 13:35:29 172.16.72.29 October 23 17:35:36 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMRequested; User: Administrator; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: October 23, 2019 17:35:36	
Failure of key generation activity for authentication keys. [FCS_CKM.1]	Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, and Android Platform
Failure of the randomization process. [FCS_RBG_EXT.1]	Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, and Android Platform
Failure of MD user authentication. (Android) [FIA_ENR_EXT.1 /ANDROID]	Oct 2 10:33:24 172.16.72.29 October 02 14:32:39 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: UserEnrollmentAuthenticationFailure; User: sysadmin; Device Name: N/A; EnrollmentUser: N/A; Event Source: Device; Event Module: Enrollment; Event Category: Authentication; Event Data: UserEnrollmentName=Tester1;LocationGroup=570 Event Timestamp: October 2, 2019 14:32:39	UEM Server
Failure of MD user authentication. (iOS)	Oct 25 09:18:03 172.16.72.29 October 25 13:18:48 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event:	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
[FIA_ENR_EXT.1 /IOS]	UserEnrollmentAuthenticationFailure; User: sysadmin; Device Name: N/A; EnrollmentUser: N/A; Event Source: Device; Event Module: Enrollment; Event Category: Authentication; Event Data: EnrollmentType=DEP Enrollment;UserEnrollmentName=Tester2;LocationGroup=570 Event Timestamp: October 25, 2019 13:18:48	
Failure to validate X.509 certificate. [FIA_X509_EXT.1(1)]	**Android Hub Agent** Jan 14 13:58:58 172.16.72.29 January 14 18:59:22 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: PolicySigningFailed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: Failure Reason=Code: 64;Number of Times Occured=18 times Event Timestamp: January 14, 2020 18:58:58 Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, Android Hub Agent, and Android Platform
Failure to establish connection to determine revocation status. [FIA_X509_EXT.2]	**Android Hub Agent** Jan 17 09:08:36 172.16.72.29 January 17 14:09:00 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: PolicySigningFailed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: Failure Reason=Code: CERT_CHAIN_FAILED_REVOCATION_CHECK;Number of Times Occured=2 times Event Timestamp: January 17, 2020 14:08:39 Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, Android Hub Agent, and Android Platform
Issuance of command to perform function. Change of policy settings. [FMT_MOF.1(1)]	**Issuance of command to perform function (Android)** Oct 2 09:06:28 172.16.72.29 October 02 13:05:56 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: DeviceLockRequested; User: Administrator; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: October 2, 2019 13:05:56 Oct 23 12:56:14 172.16.72.29 October 23 16:56:21 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceWipeRequested; User: Administrator; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: FriendlyName=Tester1 Android Android 9.0.0 RF8M803LV4L;Admin=Administrator;OriginatingOrganizationGroup=Global;Notes=Test 056 - 002 Event Timestamp: October 23, 2019 16:56:21	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Oct 23 13:35:29 172.16.72.29 October 23 17:35:36 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMRequested; User: Administrator; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: October 23, 2019 17:35:36 Sep 12 10:44:27 172.16.72.29 September 12 14:44:25 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: DeviceInformationRequested; User: Administrator; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: September 12, 2019 14:44:25 **Issuance of command to perform function (iOS)** Sep 12 10:03:43 172.16.72.29 September 12 14:03:46 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceLockRequested; User: Administrator; Device Name: Tester3 iPhone iOS 12.4.0 F4GY207GKXKV; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: FriendlyName=Tester3 iPhone iOS 12.4.0 F4GY207GKXKV;Admin=Administrator;OriginatingOrganizationGroup=Global Event Timestamp: September 12, 2019 14:03:46 Oct 24 07:50:43 172.16.72.29 October 24 11:50:45 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceWipeRequested; User: Administrator; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: FriendlyName=Tester2 iPhone iOS 12.4.0 F4GY207GKXKV;Admin=Administrator;OriginatingOrganizationGroup=N/A;Notes= Event Timestamp: October 24, 2019 11:50:45 Oct 24 07:50:43 172.16.72.29 October 24 11:50:45 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMConfirmed; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Event Timestamp: October 24, 2019 11:50:45 Oct 24 08:06:35 172.16.72.29 October 24 12:06:36 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: DeviceInformationRequested; User: Administrator; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV;	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	EnrollmentUser: Tester2; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: October 24, 2019 12:06:36 **Change of policy settings (Android)** Sep 12 13:08:34 172.16.72.29 September 12 17:08:21 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ProfileCreated; User: Administrator; Device Name: N/A; Event Source: Server; Event Module: Profiles; Event Category: Profiles; Event Data: ProfileName=Function 25 - Camera Mic Screen Capture;SupportedPlatform=Android;Version=1;AssignmentType=Auto;AllowRemoval=Always;ManagedBy=Company;AssignedSmartGroups=Android 1 @ Company;ExcludedSmartGroups=N/A;EnableGeofencing=N/A;EnableScheduling=N/A;ProfileScope=Production Event Timestamp: September 12, 2019 17:08:21 Sep 12 13:08:35 172.16.72.29 September 12 17:08:21 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: RestrictionPayloadCreated; User: Administrator; Device Name: N/A; Event Source: Server; Event Module: Profiles; Event Category: Profiles; Event Data: ProfileName=Function 25 - Camera Mic Screen Capture;DeviceFunctionality=Allow Camera: False, Allow Microphone: False, Allow Factory Reset: True, Allow Airplane Mode: True;DeviceFunctionality=Allow screen capture: False, Allow Mock Locations: True, Allow Clipboard: True, Allow USB Media Player: True;DeviceFunctionality=Allow NFC: True, Allow Home Key: True, Allow Email Account Addition: True, Allow Google Account Addition: True;DeviceFunctionality=Allow POP/IMAP email: True, Allow Power Off: True, Allow Safe Mode: True, Allow Status Bar: True;DeviceFunctionality=Allow Notifications: True, Allow Wallpaper Change: True, Allow Audio Recording if Microphone is Allowed: True, Allow Video Recording if Camera is Allowed: True;DeviceFunctionality=Allow Ending Activity W Sep 12 13:08:35 172.16.72.29 September 12 17:08:21 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ProfilePublished; User: Administrator; Device Name: N/A; Event Source: Server; Event Module: Profiles; Event Category: Profiles; Event Data: LoginSessionID=z25ji4fibonv;Profile=Function 25 - Camera Mic Screen Capture Event Timestamp: September 12, 2019 17:08:21 **Change of policy settings (iOS)** Oct 1 10:33:55 172.16.72.29 October 01 14:33:44 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ProfileCreated; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server;	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Event Module: Profiles; Event Category: Profiles; Event Data: ProfileName=Function 33;SupportedPlatform=Apple iOS;Version=1;AssignmentType=Auto;AllowRemoval=Always;ManagedBy=Company;AssignedSmartGroups=iOS Testing SmartGroup @ Company;ExcludedSmartGroups=N/A;EnableGeofencing=N/A;EnableScheduling=N/A;DeploymentMode=Managed;RemovalDate=N/A Event Timestamp: October 1, 2019 14:33:44 Oct 1 10:33:55 172.16.72.29 October 01 14:33:44 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: RestrictionPayloadCreated; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Profiles; Event Category: Profiles; Event Data: ProfileName=Function 33;DeviceFunctionality=Allow use of camera: True, Allow FaceTime: True, Allow screen capture: True, Allow Biometric ID to unlock device: False;DeviceFunctionality=Allow use of iMessage: True, Allow installing public apps: True, Allow app removal: True, Allow in-app purchase: True;DeviceFunctionality=Allow documents from managed sources in unmanaged destinations: True, Allow documents from unmanaged sources in managed destinations: True, Force limited ad tracking: False, Allow Handoff: True;DeviceFunctionality=Allow automatic sync while roaming: True, Allow voice dialing: True, Allow internet results in Spotlight: True, Allow Siri: True;DeviceFunctionality=Allow Siri while device locked: True, Enable Siri Profanity Filter: Oct 1 10:33:55 172.16.72.29 October 01 14:33:45 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ProfilePublished; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Profiles; Event Category: Profiles; Event Data: LoginSessionID=uflmlv4a0cmf;Profile=Function 33 Event Timestamp: October 1, 2019 14:33:45	
Enrollment by a user. [FMT_MOF.1(2)]	Oct 2 10:59:05 172.16.72.29 October 02 14:58:16 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: Tester1Local Android Android 9.0 RF8M803LV4L; EnrollmentUser: Tester1Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 2, 2019 14:58:15	UEM Server
Success or failure of function. (Android) [FMT_SMF.1(2) /ANDROID]	**Choose X.509v3 certificates for MDM Server use** and **Configure Enterprise certificate to be used for signing policies** Oct 22 09:29:47 172.16.72.29 October 22 13:29:54 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: PolicySigningCertificateSettingChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=4vb5c3ubjbkq Event Timestamp: October 22, 2019 13:29:54	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Configure the devices specified by IMEI, serial number, specific device models, number of devices, manufacturer, and operating system allowed for enrollment Oct 21 16:22:08 172.16.72.29 October 21 20:22:15 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: EnrollmentRestrictionPolicyAdded; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Administration; Event Category: SystemSettings; Event Data: RestrictionsMode=Whitelist;DeviceRestriction=Android Device Limit per User: 10;PolicyName=Galaxy S10e Only Permitted;LocationGroup=Company;PolicyType=Organization Group Default;OwnershipType=C,E,S;EnrollmentType=MDM , Container;DeviceLimit=Unlimited;LimitEnrollment=Yes **Configure the TOE unlock banner** Sep 6 14:00:51 172.16.72.29 September 06 18:00:53 AirWatch AirWatch Syslog Details are as follows Event Type: ConsoleEvent: BrandingChangedUser: AdministratorEvent Source: ServerEvent Module: SettingsEvent Category: SystemSettingsEvent Data: LoginSessionID=bgczjbmqphin Event Timestamp: September 6, 2019 18:00:53 Sep 6 14:01:09 172.16.72.29 September 06 18:01:11 AirWatch AirWatch Syslog Details are as follows Event Type: ConsoleEvent: BrandingAdvancedChangedUser: AdministratorEvent Source: ServerEvent Module: SettingsEvent Category: SystemSettingsEvent Data: LoginSessionID=bgczjbmqphin Event Timestamp: September 6, 2019 18:01:11 **Configure periodicity of the following commands to the agent: (query connectivity status, query the current version of the MD firmware/software, query the current version of the hardware model of the device, query the current version of installed mobile applications)** and **Configure MDM Agent/platform to perform a network reachability test** Oct 22 15:24:03 172.16.72.29 October 22 19:24:10 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: AndroidHeartbeatIntervalSettingChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=k4i4lbg40y5i Event Timestamp: October 22, 2019 19:24:10	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Configure the privacy-sensitive information that will and will not be collected from particular mobile devices Feb 27 16:16:42 172.16.72.29 February 27 21:16:42 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DevicePrivacySettingsChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=d53qp3a2djzh;PersonalApplicationPrivacy=C:Do Not Collect E:Do Not Collect S:Do Not Collect U:Do Not Collect Event Timestamp: February 27, 2020 21:16:42 **Configure the interaction between TOE components** Feb 28 09:16:21 172.16.72.29 February 28 14:16:21 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToEnrollmentWhiteList; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=RF8M803LV4L;LocationGroup=Global Event Timestamp: February 28, 2020 14:16:21 **Configure the server administrator login session timeout** Nov 18 11:03:35 172.16.72.29 November 18 16:03:50 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ConsoleSessionTimeOutChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=n0fjx5ifgtju Event Timestamp: November 18, 2019 16:03:49 **Configure transfer of MDM server logs to another server for storage, analysis, and reporting** Oct 22 14:33:59 172.16.72.29 October 22 18:34:06 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: SyslogSettingChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Administration; Event Category: SystemSettings; Event Data: LoginSessionID=k4i4lbg40y5i Event Timestamp: October 22, 2019 18:34:06	
Success or failure of function. (iOS) [FMT_SMF.1(2) /IOS]	**Choose X.509v3 certificates for MDM Server use** and **Configure Enterprise certificate to be used for signing policies (iOS Hub Agent)** Oct 22 09:29:47 172.16.72.29 October 22 13:29:54 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: PolicySigningCertificateSettingChangedSuccess; User: Administrator; Device	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=4vb5c3ubjbkq Event Timestamp: October 22, 2019 13:29:54 **Choose X.509v3 certificates for MDM Server use** and **Configure Enterprise certificate to be used for signing policies (iOS Platform)** Nov 18 13:19:05 172.16.72.29 November 18 18:19:19 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: AppleProfileSigningCertificateChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=ihnezseuywf3 Event Timestamp: November 18, 2019 18:19:19 **Configure the devices specified by DEP identifier allowed for enrollment** Jan 13 14:32:19 172.16.72.29 January 13 19:32:44 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: EnrollmentAuthenticationSettingChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Administration; Event Category: SystemSettings; Event Data: DevicesEnrollmentMode=RegisteredDevicesOnly Event Timestamp: January 13, 2020 19:32:44 **Configure the TOE unlock banner** Sep 6 14:00:51 172.16.72.29 September 06 18:00:53 AirWatch AirWatch Syslog Details are as follows Event Type: ConsoleEvent: BrandingChangedUser: AdministratorEvent Source: ServerEvent Module: SettingsEvent Category: SystemSettingsEvent Data: LoginSessionID=bgczjbmqphin Event Timestamp: September 6, 2019 18:00:53 Sep 6 14:01:09 172.16.72.29 September 06 18:01:11 AirWatch AirWatch Syslog Details are as follows Event Type: ConsoleEvent: BrandingAdvancedChangedUser: AdministratorEvent Source: ServerEvent Module: SettingsEvent Category: SystemSettingsEvent Data: LoginSessionID=bgczjbmqphin Event Timestamp: September 6, 2019 18:01:11 **Configure periodicity of the following commands to the agent: (query connectivity status, query the current version of the MD firmware/software, query the current version of the hardware model of the device, query the current version of installed mobile applications)** and **Configure MDM Agent/platform to perform a network reachability test**	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Nov 19 10:44:54 172.16.72.29 November 19 15:45:08 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: AppleMdmSampleScheduleSettingChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Administration; Event Category: SystemSettings; Event Data: LoginSessionID=qs3jbhmsubr4 Event Timestamp: November 19, 2019 15:45:08 **Configure the privacy-sensitive information that will and will not be collected from particular mobile devices** Feb 27 16:16:42 172.16.72.29 February 27 21:16:42 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DevicePrivacySettingsChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=d53qp3a2djzh;PersonalApplicationPrivacy=C:Do Not Collect E:Do Not Collect S:Do Not Collect U:Do Not Collect Event Timestamp: February 27, 2020 21:16:42 **Configure the interaction between TOE components** Feb 28 10:44:42 172.16.72.29 February 28 15:44:42 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToAppleDep; User: ; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=FFMX76VPKPHC;LocationGroup=Company Event Timestamp: February 28, 2020 15:44:42 **Configure the server administrator login session timeout** Nov 18 11:03:35 172.16.72.29 November 18 16:03:50 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ConsoleSessionTimeOutChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=n0fjx5ifgtju Event Timestamp: November 18, 2019 16:03:49 **Configure transfer of MDM server logs to another server for storage, analysis, and reporting** Oct 22 14:33:59 172.16.72.29 October 22 18:34:06 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: SyslogSettingChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source:	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Server; Event Module: Administration; Event Category: SystemSettings; Event Data: LoginSessionID=k4i4lbg40y5i Event Timestamp: October 22, 2019 18:34:06	
Initiation and termination of the trusted channel. [FPT_ITT.1(2)]	Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, and Android Platform
Initiation of self-test. Failure of self-test. Detected integrity violation. [FPT_TST_EXT.1]	Refer to guidance documentation provided by the platform at [7].	Windows Platform
Success or failure of signature verification. [FPT_TUD_EXT.1]	Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, and Android Platform
Change in banner setting. [FTA_TAB.1]	Sep 6 14:00:51 172.16.72.29 September 06 18:00:53 AirWatch AirWatch Syslog Details are as follows Event Type: ConsoleEvent: BrandingChangedUser: AdministratorEvent Source: ServerEvent Module: SettingsEvent Category: SystemSettingsEvent Data: LoginSessionID=bgczjbmqphin Event Timestamp: September 6, 2019 18:00:53 Sep 6 14:01:09 172.16.72.29 September 06 18:01:11 AirWatch AirWatch Syslog Details are as follows Event Type: ConsoleEvent: BrandingAdvancedChangedUser: AdministratorEvent Source: ServerEvent Module: SettingsEvent Category: SystemSettingsEvent Data: LoginSessionID=bgczjbmqphin Event Timestamp: September 6, 2019 18:01:11	UEM Server
Initiation and termination of the trusted channel. [FTP_ITC.1(1)]	Refer to guidance documentation provided by the platform at [7].	Windows Platform
Initiation and termination of the trusted channel. [FTP_TRP.1(1)]	Refer to guidance documentation provided by the platform at [7].	Windows Platform

Auditable Event(s)	Audit Record Examples	Component Generating Record
Initiation and termination of the trusted channel. [FTP_TRP.1(2)]	Refer to guidance documentation provided by the platforms at [7], [8], and [9].	Windows Platform, iOS Platform, and Android Platform
Failure to push a new application on a managed mobile device [FAU_GEN.1.1(2)]	Nov 20 10:09:46 172.16.72.29 November 20 15:10:00 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Command; Event Data: Event Timestamp: November 20, 2019 15:09:46	UEM Server
Failure to update an existing application on a managed mobile device [FAU_GEN.1.1(2)]	Nov 20 10:09:46 172.16.72.29 November 20 15:10:00 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Command; Event Data: Event Timestamp: November 20, 2019 15:09:46	UEM Server
Success/failure of sending alert. (Android) [FAU_ALT_EXT.2 /ANDROID]	**Successful application of policies to a mobile device** Sep 13 11:29:43 172.16.72.29 September 13 15:29:37 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileConfirmed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Profile=Test Case 004 - Initial Policy Event Timestamp: September 13, 2019 15:29:37 **Generating periodic reachability events** Nov 19 07:45:55 172.16.72.29 November 19 12:46:09 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: CheckIn; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: Devices; Event Category: Delivery; Event Data: Application=;ApplicationVersion=;BytesReceived=82 Event Timestamp: November 19, 2019 12:46:09 **Change in enrollment state (enrolled)** Oct 2 10:59:05 172.16.72.29 October 02 14:58:16 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: Tester1Local Android Android 9.0 RF8M803LV4L; EnrollmentUser: Tester1Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 2, 2019 14:58:15 **Change in enrollment state (unenrolled)**	Android Hub Agent

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Oct 23 13:35:30 172.16.72.29 October 23 17:35:37 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMConfirmed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Event Timestamp: October 23, 2019 17:35:37 **Failure to install an application from the MAS Server**, and **Failure to update an application from the MAS Server** Nov 20 10:09:46 172.16.72.29 November 20 15:10:00 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Command; Event Data: Event Timestamp: November 20, 2019 15:09:46 **Detection of blacklisted apps**, **Detection of non-whitelisted apps**, and **Required apps missing** Oct 21 15:00:47 172.16.72.29 October 21 19:00:55 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=Application List Event Timestamp: October 21, 2019 19:00:55 **Rooted device** Oct 24 14:15:09 172.16.72.29 October 24 18:15:00 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: CompromisedStatusReported; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: Devices; Event Category: CompromisedStatus; Event Data: CompromisedStatus=Compromised;ApplicationVersion=SDK V19.8.0 Event Timestamp: October 24, 2019 18:15:00 Oct 24 14:15:09 172.16.72.29 October 24 18:15:00 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: CompromisedStatusChanged; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: Devices; Event Category: CompromisedStatus; Event Data: CompromisedStatus=Compromised;ApplicationVersion=Compromised flag changed from False to True. Event Timestamp: October 24, 2019 18:15:00	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Unapproved device manufacturer Oct 21 15:33:46 172.16.72.29 October 21 19:33:53 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=Device Manufacturer Event Timestamp: October 21, 2019 19:33:53 **Unapproved operating system version** Oct 21 15:35:48 172.16.72.29 October 21 19:35:55 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=OS Version Event Timestamp: October 21, 2019 19:35:55	
Success/failure of sending alert. (iOS) [FAU_ALT_EXT.2 /IOS]	**Successful application of policies to a mobile device** Oct 3 08:26:58 172.16.72.29 October 03 12:26:32 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileConfirmed; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Profile=Test Case 008 Event Timestamp: October 3, 2019 12:26:32 **Receiving periodic reachability events** Jan 14 17:59:16 172.16.72.29 January 14 22:59:41 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: CheckIn; User: sysadmin; Device Name: Tester4 iPhone iOS 12.4.0 FFMX76VPKPHC; EnrollmentUser: Tester4; Event Source: Device; Event Module: Devices; Event Category: Delivery; Event Data: Application=;ApplicationVersion=;BytesReceived=82 Event Timestamp: January 14, 2020 22:59:41 **Change in enrollment state (enrolled)** Oct 25 09:22:40 172.16.72.29 October 25 13:23:25 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: Tester2Local iPhone Apple 12.4 F4GY207GKXKV; EnrollmentUser: Tester2Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 25, 2019 13:23:25	iOS Platform

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Change in enrollment state (unenrolled) Oct 23 15:42:19 172.16.72.29 October 23 19:42:27 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMConfirmed; User: sysadmin; Device Name: Tester3 iPhone iOS 12.4.0 FFMX76VPKPHC; EnrollmentUser: Tester3; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Event Timestamp: October 23, 2019 19:42:27 **Failure to install an application from the MAS Server**, and **Failure to update an application from the MAS Server** Feb 4 12:48:32 172.16.72.29 February 04 17:48:32 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: Tester3 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester3; Event Source: Server; Event Module: Devices; Event Category: Command; Event Data: ApplicationType=Internal;Application=SITH SDK App;ErrorCode=2604 Could not validate manifest.;ApplicationVersion=20.1.0;ApplicationUUID=e8a25bed-c8da-4710-8119-6b3792767d64 Event Timestamp: February 4, 2020 17:48:32 **Detection of blacklisted apps**, **Detection of non-whitelisted apps**, and **Required apps missing** Oct 22 16:46:48 172.16.72.29 October 22 20:46:55 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=Application List Event Timestamp: October 22, 2019 20:46:55 **Jailbroken device** Nov 21 15:01:31 172.16.72.29 November 21 20:01:45 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: CompromisedStatusReported; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Device; Event Module: Devices; Event Category: CompromisedStatus; Event Data: CompromisedStatus=Compromised;ApplicationVersion=SDK V19.9.1 Event Timestamp: November 21, 2019 20:01:45 Nov 21 15:01:31 172.16.72.29 November 21 20:01:45 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: CompromisedStatusChanged; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Device; Event Module: Devices; Event	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Category: CompromisedStatus; Event Data: CompromisedStatus=Compromised;ApplicationVersion=Compromised flag changed from False to True. Event Timestamp: November 21, 2019 20:01:45 **Unapproved model** Oct 23 08:37:14 172.16.72.29 October 23 12:37:21 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=Model Event Timestamp: October 23, 2019 12:37:21 **Unapproved operating system version** Oct 23 08:49:48 172.16.72.29 October 23 12:49:55 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: Tester2 iPhone iOS 12.4.0 F4GY207GKXKV; EnrollmentUser: Tester2; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=OS Version Event Timestamp: October 23, 2019 12:49:55	
All modifications to the audit configuration that occur while the audit collection functions are operating. [FAU_SEL.1]	Jan 15 08:32:12 172.16.72.29 January 15 13:32:36 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ApplicationGroupCreated; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Apps; Event Category: Applications; Event Data: LoginSessionID=xkxvxrk3r33g;ApplicationGroup=Android Whitelist Event Timestamp: January 15, 2020 13:32:36 Jan 15 08:32:49 172.16.72.29 January 15 13:33:14 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: ApplicationGroupAssignmentModified; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Apps; Event Category: Applications; Event Data: LoginSessionID=xkxvxrk3r33g;ApplicationGroup=Android Whitelist Event Timestamp: January 15, 2020 13:33:14	iOS Hub Agent, iOS Platform, and Android Hub Agent
Enrollment in management. [FIA_ENR_EXT.2]	**Android Hub Agent** Oct 2 10:59:05 172.16.72.29 October 02 14:58:16 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: Tester1Local Android Android 9.0 RF8M803LV4L; EnrollmentUser: Tester1Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 2, 2019 14:58:15	iOS Platform, and Android Hub Agent

Auditable Event(s)	Audit Record Examples	Component Generating Record
	iOS Platform Oct 25 09:22:40 172.16.72.29 October 25 13:23:25 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: Tester2Local iPhone Apple 12.4 F4GY207GKXKV; EnrollmentUser: Tester2Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 25, 2019 13:23:25	
Failure of policy validation. [FMT_POL_EXT.2]	**Android Hub Agent** Jan 16 10:56:24 172.16.72.29 January 16 15:56:49 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: PolicySigningFailed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: Failure Reason=Code: POLICY_SIGNING_SIGNATURE_VALIDATION_FAILED;Number of Times Occured=0 times Event Timestamp: January 16, 2020 15:56:24 **iOS Hub Agent** Jan 15 19:48:57 172.16.72.29 January 16 00:49:21 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: Policy Signature Validation Failed; User: sysadmin; Device Name: Tester4 iPhone iOS 12.4.0 FFMX76VPKPHC; EnrollmentUser: Tester4; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: = Event Timestamp: January 16, 2020 00:43:57 Refer to guidance documentation provided by the platform at [8].	iOS Hub Agent, iOS Platform, and Android Hub Agent
Outcome (Success/failure) of function. [FMT_SMF_EXT.4]	**Import the certificates to be used for authentication of MDM Agent communications** Refer to guidance documentation provided by the platforms at [8] and [9]. **Administrator-provided device management functions in MDM PP** Refer to audit records in row under "Issuance of command to perform function. Change of policy settings." **Enroll in management (Android)** Oct 2 10:59:05 172.16.72.29 October 02 14:58:16 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: Tester1Local Android Android 9.0 RF8M803LV4L; EnrollmentUser: Tester1Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com	iOS Hub Agent, iOS Platform, Android Hub Agent, and Android Platform

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Event Timestamp: October 2, 2019 14:58:15 **Enroll in management (iOS)** Oct 25 09:22:40 172.16.72.29 October 25 13:23:25 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: Tester2Local iPhone Apple 12.4 F4GY207GKXKV; EnrollmentUser: Tester2Local; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=niap-uem.ssdevrd.com Event Timestamp: October 25, 2019 13:23:25 **Configure whether users can unenroll from management (Android)** Oct 1 15:36:05 172.16.72.29 October 01 19:36:03 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: UnenrollSetting; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M803LV4L; EnrollmentUser: Tester1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Device; Event Data: Event Timestamp: October 1, 2019 19:36:04 **Configure whether users can unenroll from management (iOS)** Nov 4 15:23:19 172.16.72.18 November 04 19:23:20 AirWatch NIAP AirWatch Syslog Details are as follows Event Type: ConsoleEvent: AuthorizedSecurityPinUser: AdministratorEvent Source: ServerEvent Module: AdministrationEvent Category: SecurityPinEvent Data: ActionAttempted=Delete DEP;SecurityPinInputAttemptNumber=1;User=Administrator;LoginSessionID=hporbbjlcmr2Device Friendly Name: N/AEnrollment User: N/A **Configure periodicity of reachability events (Android)** Nov 19 10:52:59 172.16.72.29 November 19 15:53:14 AirWatch AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileConfirmed; User: sysadmin; Device Name: Tester1 Android Android 9.0.0 RF8M31B724F; EnrollmentUser: Tester1; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Profile=AndroidAgentSettings Event Timestamp: November 19, 2019 15:53:14 **Configure periodicity of reachability events (iOS)** Nov 19 10:44:54 172.16.72.29 November 19 15:45:08 AirWatch AirWatch Syslog Details are as follows Event Type: Console; Event: AppleMdmSampleScheduleSettingChangedSuccess; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module:	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Administration; Event Category: SystemSettings; Event Data: LoginSessionID=qs3jbhmsubr4 Event Timestamp: November 19, 2019 15:45:08	

9 Operational Modes

VMware does not have distinct operational modes. Adherence to this guidance is necessary to ensure that it has been deployed in a Common Criteria compliant manner.

10 Additional Support

While reading this documentation you may encounter references to documents that are not included here. You can access this documentation through the VMware's website (docs.vmware.com).

VMware frequently makes updates to Workspace ONE UEM documentation to incorporate the latest bug fixes and feature enhancements. Therefore, it is recommended to always pull the documents from VMware's website each time they need to be referenced because having the latest versions ensures that an Administrator is following the best practices and procedures.