VMware Workspace ONE Unified Endpoint Management Version 2209 Supplemental Administrative Guidance

Version 1.0
February 6, 2023

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 2209 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 2209 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 2209 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 2209

[2] Upgrade Guide for on-premises and SaaS deployments VMware Workspace ONE UEM 2209

[3] Console Basics VMware Workspace ONE UEM 2209

[4] Directory Service Integration VMware Workspace ONE UEM 2209

[5] Certificate Authority Integrations VMware Workspace ONE UEM 2209

[6] Integration with Apple Business Manager VMware Workspace ONE UEM 2209

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] Microsoft Windows 10 and Windows Server 2019 (version 1809) Operational and Administrative Guidance v3.0 (request from Microsoft) (https://download.microsoft.com/download/Windows_10_version_1809_GP_OS_Administrative_Guide.pdf)

[8] Apple iOS 14: iPhones and Apple iPadOS 14: iPads Common Criteria Configuration Guide Version 1.0, 2021-05-25 (https://www.niap-ccevs.org/MMO/Product/st_vid11147-agd.pdf)

[9] Samsung Android 11 on Galaxy Devices Version: 7.0 (https://www.niap-ccevs.org/MMO/Product/st_vid11160-agd.pdf)

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

[10] VMware Workspace ONE Unified Endpoint Management Version 2209 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 2209 that includes the TOE components described in the following table:

Table 1: Evaluated Components of the TOE

Component	Definition
Workspace ONE Unified Endpoint Management 2209 (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 22.09 (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 11 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 22.11 (iOS Hub agent)	This satisfies the MDM Agent Component of the TOE as it is a VMware-developed application installed on mobile devices running either the Apple iOS 14 and/or Apple iPadOS 14 operating systems. The iOS Hub agent uses the iOS/iPadOS platforms to establish a secure connection back to the UEM Server for the iOS Hub agent and iOS/iPadOS 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 2019 (Version 1809) Active Directory/LDAP Server is used.

Apple iOS 14 Mobile Device (VID11146)	The MDM Agent Component of the TOE (Hub agent) is an application that is installed on Apple mobile devices running iOS 14 operating systems so that the TOE can provide management functionality to the device.
Apple iPadOS 14 Mobile Device (VID11147)	The MDM Agent Component of the TOE (Hub agent) is an application that is installed on Apple mobile devices running iPadOS 14 operating systems so that the TOE can provide management functionality to the device.
Apple Push Notification Service (APNS) / Apple DEP	APNS is an iOS/iPadOS platform push notification service that enables the UEM Server to notify iOS Hub agents and the iOS/iPadOS 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 2019 (Version 1809) 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 11 Mobile Device (VID 11160)	The MDM Agent Component of the TOE (Hub agent) is an application that is installed on mobile devices running Android 11 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 2019 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 2019 (Version 1809)	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 2019 (Version 1809) – 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. On the database server, execute the following database query to enable permissive configuration of the syslog server hostname:

```
DELETE from dbo.SystemCode where SystemCodeID = 1958
UPDATE dbo.SystemCode set DefaultValue = 'True' where SystemCodeID = 1958
```

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 OCSP checking between the UEM server / console and the AD/LDAP server:

```
DELETE from dbo.SystemCodeOverride where SystemCodeID = 5967
UPDATE dbo.SystemCode set DefaultValue = 'True' where SystemCodeID = 5967
```

7. 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
```

8. 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
```

9. On the database server, execute the eventlogfilterfix_2111.sql database query to enable the ability to view the maximum amount of audit events from within the UEM Server. The eventlogfilterfix_2111.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 IIS Manager.
    f. Go to "Sites" > "Default Web Site".
    g. Click on "Bindings…".
    h. Click "Add…".
    i. Choose "https" for the type, specify "All Unassigned" for IP address, specify "8443" for the port.
    j. Specify the X.509v3 certificate uploaded in Step 10 then click "OK".
    k. Launch an elevated command prompt by entering "cmd.exe" at the Run box.
    l. 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
12. On the UEM Server, open the \AirWatch\AirWatch 2209\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 2209\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"/>
    ```

14. On the UEM Server, open the \AirWatch\AirWatch 2209\Websites\WanderingWiFi.AirWatch.Console.Web\Web.config, \AirWatch\AirWatch 2209\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, open the \AirWatch\AirWatch 2209\Websites\AW.Console.Web.Mobile.DeviceManagement\Web.config file in a text editor.
    a. Delete the following lines from the file:

    ```
    <authentication mode="Forms">
            <forms name=".AIRWATCHSSP" loginUrl="~/Enrollment"
            protection="All" timeout="500000" slidingExpiration="true"/>
    </authentication>
    ```

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

    ```
    iisreset
    ```

17. In computer root trust store, remove:

    “AW Admin User Root”
    “AW Device Services Child Certificate”

    Also ensure there are only root CA certificates in the root trust store; and only intermediate CA certificates in the intermediate CA trust store.
18. 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_256_GCM_SHA384
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    ```

    e. Click “Apply” then “OK”.
    f. Restart the system.
19. 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 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

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

    Username: administrator
    Password: airwatch

21. Change the default password and then accept the license agreement.
22. Specify the password recovery questions and security PIN.
23. Configure the UEM Server to communicate with Apple Push Notification Service (APNS) by following the procedures in [3] Chapter 5 under "Generate a New APNs Certificate".
24. Configure the UEM Server to communicate with an external Active Directory / LDAP Server by following the procedures in [4].
25. Configure the UEM Server to communicate with the Certification Authority server by following the procedures in [5] Chapters 2 and 3.
26. 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/iPadOS, 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.
27. 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”.

28. 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)”
29. 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 RFC 5424 for Syslog format.
    f. Specify the “Message Tag” as follows:

       <UEM Server IP address>

       NOTE: UEM Server IP address is to be replaced with the literal IP address value.
    g. 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}

    h. Click “Save”
30. Configure the UEM Server to communicate with Apple Device Enrollment Program (DEP) by following the procedures in [6] Chapter 2.
31. 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”.
32. 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.
33. 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.
34. Upload the policy signing certificate to the UEM Server for use with the iOS/iPadOS 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”.

NOTE: If modifying these certificates (Steps 33 & 34) after the initial configuration, execute the database query below to clear the certificate data from the database, then perform Steps 33 & 34 to upload the new certificates, and then execute the command *iisreset* in the Windows command prompt on the UEM Server.

```
DELETE FROM dbo.SystemCodeOverride WHERE SystemCodeID = 130
```

35. Navigate to "Groups & Settings" > "All Settings" > "Devices & Users" > "Android" > "Android EMM Registration" > "Enrollment Settings".
    a. Ensure that the following settings are toggled:
        i. Management Mode for Corporate Devices: Work Managed
        ii. Google Account Generation for Corporate Devices: AOSP / Closed Network
    b. Click "Save".
36. Navigate to "Groups & Settings" > "All Settings" > "Apps" > "Setting and Policies" > "Security Policies".
    a. Toggle Single Sign-On to ENABLED.
    b. 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" > "Allow Devices".
5. Specify the allowed 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" > "Allow Devices".
5. Specify the allowed 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 (allowlist).”
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 (allowlist).”
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 (allowlist).”
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; and
- Removes the ability to uninstall the Android Hub agent through the Google Play Store.

Additionally, as a managed device the Android platform automatically prevents the user from demoting the Android Hub agent from a device Administrator (preventing uninstall).

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. Navigate to "Advanced" > "Staging" > "Enable Device Staging"
   a. Toggle Enable Device Staging Disabled.

   NOTE: This is to remove VMware Launcher for Android mobile devices which can cause usability issues with the mobile device.

6. 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 as well as downloading the Android Hub agent from the Google Play Store. The process used for downloading and installing the Android Hub agent in the evaluated configuration was the QR Code method. The following links provide procedures to perform a QR code installation and enrollment.

1. https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2209/Android_Platform/GUID-AndroidEnrollmentEnrollWithQRCode.html

2. https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/closednetworkandroid/GUID-closednetworkQR.html

The device user will then enter the UEM Server's URL 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/iPadOS 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/iPadOS 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/iPadOS 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 “Delete Device” 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”.
8. Choose “MORE ACTIONS” > “Delete”.
9. Click “SAVE”.

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 “Delete Device” 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 2019 (Version 1809) platform. The Windows Server 2019 (Version 1809) platform uses Microsoft’s SymCrypt 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/iPadOS platforms’ 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 related to [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 2209 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 an Administrator. The UEM Server software can be checked by clicking on the “About VMware AirWatch” 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 7 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 either the MD user (local authorized administrator of the device) directly, the Hub agent after receiving a command from the UEM Server to update the Hub agent software, or the Hub agent based upon a configured policy which requires the Hub agent software to install updates as soon as they are available. Once the update is downloaded onto the device, the platform will verify the signature from the Google Play Store/Apple App Store/UEM Server app 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 Authorized Administrators 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 16 under “Admin Accounts” and Chapter 13.

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 configure the periodicity of the collection of 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 is also configured by the UEM Server to generate periodic reachability events based upon a configured 'sample interval'. When the 'sample interval' is reached, the iOS Hub agent will initiate a connection to the UEM Server and the UEM Server communicates with the iOS Hub agent to collect policy/sample data from the device. 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 configure the periodicity of the collection of 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 2209 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 VID11146[1] VID11147[2]**	**Implemented By**	**Command**	**Claimed in VID11160[3]**	**Implemented By**
1. transition to the locked state – "Lock" button.	Yes to both	Platform	**1. transition to the locked state** – "Lock" button.	Yes	Hub Agent
2. full wipe of protected data – "More Actions" button > "Device Wipe".	Yes to both	Platform	**2. full wipe of protected data –** "More Actions" button > "Device Wipe".	Yes	Hub Agent
3. unenroll from management – "More Actions" button > "Device Wipe".	No to both	Platform	**3. unenroll from management** – "More Actions" button > "Device Wipe".	No	Hub Agent
4. install policies – assigned and applied to target devices at the creation or modification of a profile under "Devices" >	No to both	Platform	**4. install policies** – assigned and applied to target devices at the creation or modification of a profile under "Devices" >	No	Hub Agent

[1] TD0479

[2] TD0479

[3] TD0479

“Profiles & Resources” > “Profiles”.			“Profiles & Resources” > “Profiles”. Note: The Server sends the "public app update policy" to Google Play Store which sends the policy to the device for processing.		
5. query connectivity status – “Query” button.	No to both	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 to both	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 to both	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 to both	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
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 to both	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 & Books” > “Applications” > “Native”. 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 to both	Platform	**10. install applications –** “Apps & Books” > “Applications” > “Native”. 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. Note: This is for internal apps hosted by the TOE. Apps hosted by Google Play Store can also be managed with the "public app update policy". The Server sends this policy to Google Play Store which sends the policy to the device for processing.	Yes	Hub Agent
11. update system software – the UEM Server will send command to the iOS/iPadOS platform to update to the	Yes to both	Platform	**11. update system software –** the UEM Server will send command to the Enterprise Firmware Over the Air	Yes	Platform

identified OS version, then the iOS/iPadOS platform will reach out to Apple to get the OS version.			(EFOTA) ONE Server to update to the latest OS, then the EFOTA ONE Server will push the updated software to the devices.		
12. remove applications – specific managed app from a single device: “Device details” view, “Apps” tab, Remove option (“X”) button for the desired managed app. Note: Managed apps are those from the Apple App Store that are installed on the device due to TOE policies.	Yes to both	Platform	**12. remove applications –** specific managed app from a single device: “Device details” view, “Apps” tab, Remove option (“X”) button for the desired managed app. Note: Managed apps are those from the Google Play Store that are installed on the device due to TOE policies.	Yes	Hub Agent
13. remove Enterprise applications – specific internal app from a single device: “Device details” view, “Apps” tab, Remove option (“X”) button for the desired internal app. Note: Internal apps are those from the UEM Server (MAS Server).	Yes to both	Platform	**13. remove Enterprise applications –** specific internal app from a single device: “Device details” view, “Apps” tab, Remove option (“X”) button for the desired internal app. Note: Internal apps are those from the UEM Server (MAS Server).	Yes	Hub Agent
14. wipe Enterprise data – “More Actions” button > “Enterprise Wipe”.	Yes to both	Platform	**14. wipe Enterprise data –** “More Actions” button > “Device Wipe”.	Yes	Hub Agent
15. remove imported X.509v3 certificates – “Devices” > “Profiles & Resources” > “Profiles” > choose the profile that pushed the certificate > “Devices” > “Remove Profile”	Yes to both	Platform	**15. remove imported X.509v3 certificates –** “Devices” > “Profiles & Resources” > “Profiles” > choose the profile that pushed the certificate > “Devices” > “Remove Profile”	Yes	Hub Agent
16. alert the user – “Send” button. Note: This refers to alerting the user of the mobile device, not an Administrator on the UEM Server. This can be sent as an email, SMS, or push notification.	No to both	Hub Agent (push notification), Platform (SMS)	**16. alert the user –** “Send” button. Note: This refers to alerting the user of the mobile device, not an Administrator on the UEM Server. This can be sent as an email, SMS, or push notification.	No	Hub Agent (push notification), Platform (SMS)
			20. retrieve MD-software integrity verification values – “Groups & Settings” > “All Settings” > “Apps” > “Settings & Policies” > “Settings” > “Custom Settings”. Paste and save the following in the Custom Settings field: *{ "SafetyNetEnabled":true }* Verify SafetyNet from the Summary tab in the “Device details” view.	No	Hub Agent

			The TOE uses the SafetyNet Attestation API which provides a cryptographically-signed attestation, assessing the device's integrity.		
23. revoke Biometric template – by deleting the passcode, this disables the biometric template for use.	No to both	Platform			
25. password policy – defined in the Passcode properties of a profile.	Yes to both	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 to both	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.	Yes to both	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 to both	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, allowed, and/or denied apps can be defined in “Apps & Books” > “Application Settings” > “App Groups”.	Yes to both	Platform	**29. application installation policy –** groups of required, allowed, and/or denied 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 to both	Platform	**30. enable/disable policy for camera 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 – defined in the VPN properties of a profile. **on a per-app basis –** defined in the “Tunnel & Other Attributes” setting for an individual app assignment.	Yes to both	Platform	**31. enable/disable policy for the VPN across MD or on a per-app basis –** defined in the VPN properties of a profile.	Yes	Hub Agent
			32. enable/disable policy for Bluetooth – defined in the “Restrictions” tab of a profile.	Yes	Hub Agent
			34. enable/disable policy for Wi-Fi tethering, USB tethering, and/or Bluetooth tethering – defined in the “Restrictions” tab of a profile.	No	Hub Agent
36. enable policy for data-at-rest protection – For iOS	No to both	Platform			

devices, data-at-rest protection is automatically enabled if a passcode is set so this is configured under the Passcode properties of a profile.					
38. enable/disable policy for local authentication bypass – Deletes the user’s passcode, allowing the user to access the device: “Device” > “Details View” > “More Actions” > “Clear Passcode Device”.	No to both	Platform	**38. enable/disable policy for local authentication bypass –** Deletes the user’s passcode, allowing the user to access the device: “Device” > “Details View” > “More Actions” > “Change Device Passcode”.	Yes	Hub Agent
39. configure the Bluetooth trusted channel policy – Can enable/disable discoverable mode and change the name of the entire device which will change the Bluetooth device name; defined in the “Restrictions” tab of a profile.	No to both	Platform			
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 to both	Platform	**40. enable/disable policy for display notification in the locked state** – can enable/disable all notification through "Allow Keyguard Notifications" defined in the “Restrictions” properties of a profile.	No	Hub Agent
47. the unlock banner policy – configured through the ‘if lost return’ function under “Lock Screen Message” tab of a profile.	Yes to both	Platform	**47. the unlock banner policy** – “Set a Lockscreen Message” under the “Custom Messages” properties of a profile.	Yes	Hub Agent
49. enable/disable USB mass storage mode and/or USB data transfer without user-authentication – defined in the “Restrictions” tab of a profile.	No to both	Platform	**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 to both	Platform	**50. enable/disable backup –** defined in the “Restrictions” tab of a profile.	No	Hub Agent
			51. enable/disable Hotspot and/or USB tethering – select “Allow All Tethering”, defined in the “Restrictions” tab of a profile	Yes	Hub Agent
			52. enable/disable location services across device – defined in the “Restrictions” tab of a profile.	Yes	Hub Agent
			53. enable/disable policy for user unenrollment – defined in the “Intelligent Hub Settings”.	No	Hub Agent

			54. enable/disable policy for the Always-On VPN protection across device – defined in the VPN properties of a profile. Note: The TOE must configure the VPN to enforce this policy. If the MD user sets the VPN settings this policy will not be enforced.	Yes	Hub Agent
55. enable/disable policy for use of Biometric Authentication Factor – defined in the "Restrictions" tab of a profile.	Yes to both	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 – managed under "Add Profile" > "Android Profile" > "System Updates".	No	Hub Agent
60. application installation policy – groups of required, allowed, and/or denied 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.	No for both	Platform	**60. application installation policy –** groups of required, allowed, and/or denied 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" > "Settings and Policies" > "Security Policies".	No for both	Hub Agent			

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. The TOE 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. apps on a deny list). 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.

Authorized 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 apps on a deny list, devices without required apps, or devices with apps that are not on an allow list. The Authorized Administrator can also view the applications that are associated with particular devices, including application versions. From the "Devices" section of the Admin Console, the Authorized 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 Authorized Administrator can also view detailed information about any specific device that the UEM Server knows about under this section of the Admin Console.

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 apps on a deny list
- Presence of apps not on an allow list
- Absence of required apps
- 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 UEM Server also provides Authorized Administrators with the ability to view an audit processing failure alert on the Admin Console for when a connection between the UEM Server and Syslog Server cannot be established. Configure the generation of this alert by performing the following procedures:

1. Authenticate to the Admin Console as an Administrator.
2. Navigate to “Administrator” > “Manage Account Settings” > “Notifications”.
3. Toggle “Console and Email” for Logging Server Failure.

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

4. Authenticate to the Admin Console as an Administrator.
5. Navigate to “Groups & Settings” > “All Settings” > “Devices & Users” > “General” > “Notifications”.
6. Choose “Override” for the Current Setting.
7. Under “Device Enrolled Successfully” choose “Send Email To: Administrator”.
8. Specify a valid administrator e-mail address and message template for successful device enrollment.
9. Under “Device Unenrolled” choose “Send Email To: Administrator”.
10. Specify a valid administrator e-mail address and message template for successful device enrollment.
11. 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 categorization of apps can be made both for apps under the control of the UEM Server (i.e. internal apps) as well as publicly-available apps on the Google Play Store/Apple App Store (i.e. managed apps). The following types of groups can be defined:

- Allow list: If an app is not on the list, it is not permitted on managed devices. When used with a compliance policy, the device’s Hub agent will notify the UEM Server if an app that is absent from the allow list is present on the device.
- Deny list: If an app is on this list, it is not allowed on managed devices. When used with a compliance policy, the device’s Hub agent will notify the UEM Server if an app that is present on the deny list is present on the device.

- Required: If an app is on this list, it is required MD users install it on managed devices. When used with a compliance policy, the device's Hub agent will notify the UEM Server if an app that is present on the required list is absent from the device.

Additionally, if the Android Hub agent detects an app on a deny list upon the compliance policy being applied to the device (i.e. the app's installation predates the policy), the alerting process immediately remediates the non-compliance by disabling the app. Otherwise, for both the Android Hub agent or the iOS/iPadOS platform, if the deny list compliance policy is applied prior to the installation of the app, the installation of the app is prevented.

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

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-Allowed App(s)", "Contains Denied 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 (iOS only), 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.

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 or Fully Qualified Domain Name} {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 {EventType}, subject identity {User}, success or failure of the event {Event}, and where (i.e. Device or Server) the event occurred {EventSource}. 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] Section 7, [8] Section 6.1, and [9] Section 5.4.

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)** Dec 16 08:52:42 uem.cctl.company.com 2022-12-16T13:52:29.931107Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: CCTest1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTest1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Event Timestamp: 2022-12-16T08:51:13.327000 **Change in enrollment status (enrolled - iOS)** Dec 14 10:04:17 uem.cctl.company.com 2022-12-14T15:02:22.805762Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=uem2021srv.uem2021.catl Event Timestamp: 2022-12-14T15:02:20.620000 **Change in enrollment status (unenrolled)** Dec 14 10:07:19 uem.cctl.company.com 2022-12-14T15:05:24.810023Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMConfirmed; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: N/A; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Event Timestamp: 2022-12-14T15:05:24.237000 **Failure to apply policies to a mobile device**	UEM Server

Auditable Event(s)	**Audit Record Examples**	**Component Generating Record**
	Dec 14 10:21:35 uem.cctl.company.com 2022-12-14T15:19:40.358754Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileFailed; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Devices; Event Category: Command; Event Data: ErrorCode=4001 Profile Installation Failed;ErrorCode=4001 Profile Failed to Install;ErrorCode=1009 The profile “Test Case 002I 002P/V_1” could not be installed.;ErrorCode=15000 The VPN service “VPN (VPN Configuration)” could not be installed.;Profile=Test Case 002I 002P Event Timestamp: 2022-12-14T15:19:39.800000 **Presence of apps on a deny list**, **Presence of apps not on an allow list**, and A**bsence of required apps** Dec 14 10:58:34 uem.cctl.company.com 2022-12-14T15:56:39.335118Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=Application List;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=incoming@uem-postfix.uem2021.catl;NotificationMessageTemplateName=Compliance Violation Admin Notification Event Timestamp: 2022-12-14T15:56:38.723000 **Last time a device communicated with the MDM Server** Dec 6 14:40:59 uem.cctl.company.com 2022-12-06T19:40:00.752399Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=Device Last Seen;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=incoming@uem-postfix.uem2021.catl;NotificationMessageTemplateName=Compliance Violation Admin Notification Event Timestamp: 2022-12-06T19:39:59.377000 **Unapproved model (iOS only)** Dec 14 11:09:45 uem.cctl.company.com 2022-12-14T16:07:50.330285Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data:	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	CompliancePolicy=Model;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=incoming@uem-postfix.uem2021.catl;NotificationMessageTemplateName=Compliance Violation Admin Notification Event Timestamp: 2022-12-14T16:07:49.743000 **Unapproved device manufacturer (Android only)** Feb 3 07:04:33 uem.cctl.company.com 2023-02-03T12:04:23.453094Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=Device Manufacturer;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=incoming@uem-postfix.uem2021.catl;NotificationMessageTemplateName=Compliance Violation Admin Notification Event Timestamp: 2023-02-03T12:04:22.887000 **Unapproved operating system version** Dec 14 11:12:10 uem.cctl.company.com 2022-12-14T16:10:15.619500Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceNotificationSent; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: CompliancePolicy=OS Version;CompliancePolicyNotification=SendEmailToAdmin;NotificationSentTo=incoming@uem-postfix.uem2021.catl;NotificationMessageTemplateName=Compliance Violation Admin Notification Event Timestamp: 2022-12-14T16:10:15.030000	
Start-up and shutdown of the MDM System [FAU_GEN.1.1(1)]	Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4.	Windows Platform, iOS/iPadOS 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

Auditable Event(s)	Audit Record Examples	Component Generating Record
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/iPadOS platform
Enabling/Disabling communications between a pair of components. [FCO_CPC_EXT.1]	**Enabling communications between a pair of components (Android)** Dec 10 10:04:17 uem.cctl.company.com 2022-12-10T15:02:22.805762Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToEnrollmentWhiteList; User: ; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=RFCR71C47ZN;LocationGroup=Company Event Timestamp: 2022-12-10T15:02:20.993000 **Enabling communications between a pair of components (iOS)** Dec 13 14:41:51 uem.cctl.company.com 2022-12-13T19:39:55.716528Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToAppleDep; User: sysadmin; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=F17G80KL0D81;LocationGroup=Company Event Timestamp: 2022-12-13T19:39:55.123000 **Disabling communications between a pair of components (iOS)** Jan 23 12:53:39 uem.cctl.company.com 2023-01-23T17:53:26.156484Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMRequested; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.7.1 GG7GJ02TQ19D; EnrollmentUser: N/A; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: 2023-01-23T17:53:25.250000 **Disabling communications between a pair of components (Android)** Jan 27 11:48:29 uem.cctl.company.com 2023-01-27T16:48:16.673987Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: UserEnrollmentTokenDeleted; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Administration; Event Category: UserManagement; Event Data: LoginSessionID=jxrzovcdle4k;User=0;Token=V6R7RB Event Timestamp: 2023-01-27T16:48:16.063000	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
Failure of key generation activity for authentication keys. [FCS_CKM.1]	Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4	Windows Platform, iOS/iPadOS platform, and Android Platform
Failure of the randomization process. [FCS_RBG_EXT.1]	Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4.	Windows Platform, iOS/iPadOS platform, and Android Platform
Failure of MD user authentication. (Android) [FIA_ENR_EXT.1 /ANDROID]	Jan 11 12:39:49 uem.cctl.company.com 2023-01-11T17:39:34.984687Z 10.137.2.36 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=cctest1;LocationGroup=570 Event Timestamp: 2023-01-11T17:39:34.390000	UEM Server
Failure of MD user authentication. (iOS) [FIA_ENR_EXT.1 /IOS]	Dec 14 09:34:15 uem.cctl.company.com 2022-12-14T14:32:20.608436Z 10.137.2.36 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: EnrollmentType=DEP Enrollment;UserEnrollmentName=cctest1;LocationGroup=570 Event Timestamp: 2022-12-14T14:32:19.967000	UEM Server
Failure to validate X.509 certificate. [FIA_X509_EXT.1(1)]	**Android Hub Agent** Dec 8 07:26:27 uem.cctl.company.com 2022-12-08T12:25:29.087986Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: PolicySigningFailed; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: Failure Reason=Code: EXPIRED_CERTIFICATE Event Timestamp: 2022-12-08T12:25:02.000000 Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4.	Windows Platform, iOS/iPadOS platform, Android Hub Agent, and Android Platform
Failure to establish connection to determine revocation status.	**Android Hub Agent** Dec 9 07:59:19 uem.cctl.company.com 2022-12-09T12:58:22.306137Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: PolicySigningFailed; User: sysadmin; Device Name: CCTestAD1 Android	Windows Platform, iOS/iPadOS platform,

Auditable Event(s)	Audit Record Examples	Component Generating Record
[FIA_X509_EXT.2]	Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: Failure Reason=Code: CERT_CHAIN_FAILED_REVOCATION_CHECK Event Timestamp: 2022-12-09T12:57:41.000000 Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4.	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 ('transition to lock state' example)** Jan 17 10:32:29 uem.cctl.company.com 2023-01-17T15:32:15.077948Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: DeviceLockRequested; User: Administrator; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: 2023-01-17T15:32:14.530000 **Issuance of command to perform function ('full wipe of protected data' example)** Dec 16 05:28:23 uem.cctl.company.com 2022-12-16T10:26:29.477829Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceWipeRequested; User: Administrator; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: FriendlyName=CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M;Admin=Administrator;OriginatingOrganizationGroup=Company;Notes=Test Case 058 - Subtest 02 Event Timestamp: 2022-12-16T10:26:28.503000 **Issuance of command to perform function ('query connectivity status' example)** Dec 15 08:21:59 uem.cctl.company.com 2022-12-15T13:20:04.625949Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: DeviceInformationRequested; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: Event Timestamp: 2022-12-15T13:19:59.273000 **Change of policy settings** Dec 14 11:24:08 uem.cctl.company.com 2022-12-14T16:22:13.748418Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: ProfileCreated; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Profiles; Event Category: Profiles; Event Data: ProfileName=Test Case 008 - Initial Policy;SupportedPlatform=Apple	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	iOS;Version=1;AssignmentType=Auto;AllowRemoval=Always;ManagedBy=Company;AssignedSmartGroups=Company @ Company;ExcludedSmartGroups=N/A;EnableGeofencing=N/A;EnableScheduling=N/A;DeploymentMode=Managed;RemovalDate=N/A Event Timestamp: 2022-12-14T16:22:13.053000 Dec 14 11:24:08 uem.cctl.company.com 2022-12-14T16:22:13.748418Z 10.137.2.36 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=Test Case 008 - Initial Policy;DeviceFunctionality=Allow use of camera: False, Allow FaceTime: False, Allow screen capture: True, Allow Biometric ID to unlock device: True;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, Dec 14 11:24:08 uem.cctl.company.com 2022-12-14T16:22:13.749413Z 10.137.2.36 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=vodnjar50kw0;Profile=Test Case 008 - Initial Policy Event Timestamp: 2022-12-14T16:22:13.167000	
Enrollment by a user. [FMT_MOF.1(2)]	Dec 16 08:52:42 uem.cctl.company.com 2022-12-16T13:52:29.931107Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: CCTest1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTest1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Event Timestamp: 2022-12-16T08:51:13.327000	UEM Server
Success or failure of function. (Android) [FMT_SMF.1(2) /ANDROID]	**Choose X.509v3 certificates for MDM Server use (HTTPS/TLS trusted connections)** Refer to guidance documentation provided by the platform at [7] Section 7. **Choose X.509v3 certificates for MDM Server use** and **Configure Enterprise certificate to be used for signing policies** Nov 10 11:32:02 uem.cctl.company.com 2022-11-10T16:31:47.652331Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: PolicySigningCertificateSettingChangedSuccess; User: Administrator; Device	Windows Server, 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=vbqtnzl5grs0 Event Timestamp: 2022-11-10T16:31:47.103000 **Configure the devices specified by IMEI, serial number, specific device models, number of devices, manufacturer, and operating system allowed for enrollment** Jan 17 16:00:07 uem.cctl.company.com 2023-01-17T20:59:52.634806Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: EnrollmentRestrictionPolicyModified; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Administration; Event Category: SystemSettings; Event Data: RestrictionsMode=Allowlist;DeviceRestriction=Android<br/>Device Limit per User: 10;PolicyName=Device Manufacturer Restriction;LocationGroup=Company;PolicyType=Organization Group Default;OwnershipType=C,E,S;EnrollmentType=MDM , Container;DeviceLimit=Unlimited;LimitEnrollment=Yes Event Timestamp: 2023-01-17T20:59:52.087000 **Configure the TOE unlock banner** Feb 8 10:35:42 uem.cctl.company.com 2023-02-08T15:35:32.163755Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: BrandingChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=uhkjqvsvlu02 Event Timestamp: 2023-02-08T15:35:28.087000 Feb 8 10:35:42 uem.cctl.company.com 2023-02-08T15:35:32.163755Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: BrandingAdvancedChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=uhkjqvsvlu02 Event Timestamp: 2023-02-08T15:35:28.087000 **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** Jan 10 11:32:02 uem.cctl.company.com 2023-01-10T16:31:47.652331Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: AndroidHeartbeatIntervalSettingChangedSuccess; User: Administrator; Device	

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=rkdfmacy41w3 Event Timestamp: 2023-01-10T16:31:47.103000 **Configure the privacy-sensitive information that will and will not be collected from particular mobile devices** Feb 1 11:35:36 uem.cctl.company.com 2023-02-01T16:35:26.152186Z 10.137.2.36 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=vbqtnzl5grs0;PersonalApplicationPrivacy=C:Do Not Collect<br/>E:Do Not Collect<br/>S:Do Not Collect<br/>U:Do Not Collect<br/>;UnmanagedProfilesPrivacy=C:Collect and Display<br/>E:Do Not Collect<br/>S:Collect and Display<br/>U:Do Not Collect<br/> Event Timestamp: 2023-02-01T16:35:23.013000 **Configure the interaction between TOE components** Dec 10 10:04:17 uem.cctl.company.com 2022-12-10T15:02:22.805762Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToEnrollmentWhiteList; User: ; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=RFCR71C47ZN;LocationGroup=Company Event Timestamp: 2022-12-10T15:02:20.993000 **Configure the server administrator login session timeout** Nov 21 13:43:15 uem.cctl.company.com 2022-11-21T18:43:01.219071Z 10.137.2.36 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=atdcvkpwgz1l Event Timestamp: 2022-11-21T18:43:00.673000 **Configure transfer of MDM server logs to another server for storage, analysis, and reporting** Dec 5 07:52:19 uem.cctl.company.com 2022-12-05T12:51:19.636253Z 10.137.2.36 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=egwka2bsgbtd Event Timestamp: 2022-12-05T12:51:19.060000	

Auditable Event(s)	Audit Record Examples	Component Generating Record
Success or failure of function. (iOS) [FMT_SMF.1(2) /IOS]	**Choose X.509v3 certificates for MDM Server use (HTTPS/TLS trusted connections)** Refer to guidance documentation provided by the platform at [7] Section 7. **Choose X.509v3 certificates for MDM Server use** and **Configure Enterprise certificate to be used for signing policies (iOS Hub Agent)** Nov 10 11:32:02 uem.cctl.company.com 2022-11-10T16:31:47.652331Z 10.137.2.36 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=vbqtnzl5grs0 Event Timestamp: 2022-11-10T16:31:47.103000 **Choose X.509v3 certificates for MDM Server use** and **Configure Enterprise certificate to be used for signing policies (iOS/iPadOS platform)** Nov 10 11:39:49 uem.cctl.company.com 2022-11-10T16:39:34.984687Z 10.137.2.36 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=vbqtnzl5grs0 Event Timestamp: 2022-11-10T16:39:34.390000 **Configure the devices specified by DEP identifier allowed for enrollment** Dec 14 08:34:15 uem.cctl.company.com 2022-12-14T13:32:20.608436Z 10.137.2.36 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: 2022-12-13T14:32:19.967000 **Configure the TOE unlock banner** Feb 8 10:35:42 uem.cctl.company.com 2023-02-08T15:35:32.163755Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: BrandingChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=uhkjqvsvlu02 Event Timestamp: 2023-02-08T15:35:28.087000	Windows Platform, UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Feb 8 10:35:42 uem.cctl.company.com 2023-02-08T15:35:32.163755Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: BrandingAdvancedChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=uhkjqvsvlu02 Event Timestamp: 2023-02-08T15:35:28.087000 **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** Feb 8 10:40:49 uem.cctl.company.com 2023-02-08T15:40:39.108603Z 10.137.2.36 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=wzbsq2eqqro2 Event Timestamp: 2023-02-08T15:40:38.537000 **Configure the privacy-sensitive information that will and will not be collected from particular mobile devices** Feb 1 11:35:36 uem.cctl.company.com 2023-02-01T16:35:26.152186Z 10.137.2.36 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=vbqtnzl5grs0;PersonalApplicationPrivacy=C:Do Not Collect<br/>E:Do Not Collect<br/>S:Do Not Collect<br/>U:Do Not Collect<br/>;UnmanagedProfilesPrivacy=C:Collect and Display<br/>E:Do Not Collect<br/>S:Collect and Display<br/>U:Do Not Collect<br/> Event Timestamp: 2023-02-01T16:35:23.013000 **Configure the interaction between TOE components** Dec 13 14:41:51 uem.cctl.company.com 2022-12-13T19:39:55.716528Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: DeviceAddedToAppleDep; User: sysadmin; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Devices; Event Category: Device; Event Data: Device=F17G80KL0D81;LocationGroup=Company Event Timestamp: 2022-12-13T19:39:55.123000 **Configure the server administrator login session timeout**	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Nov 21 13:43:15 uem.cctl.company.com 2022-11-21T18:43:01.219071Z 10.137.2.36 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=atdcvkpwgz1l Event Timestamp: 2022-11-21T18:43:00.673000 **Configure transfer of MDM server logs to another server for storage, analysis, and reporting** Dec 5 07:52:19 uem.cctl.company.com 2022-12-05T12:51:19.636253Z 10.137.2.36 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=egwka2bsgbtd Event Timestamp: 2022-12-05T12:51:19.060000	
Initiation and termination of the trusted channel. [FPT_ITT.1(2)]	Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4.	Windows Platform, iOS/iPadOS 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] Section 7.	Windows Platform
Success or failure of signature verification. [FPT_TUD_EXT.1]	Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4.	Windows Platform, iOS/iPadOS platform, and Android Platform
Change in banner setting. [FTA_TAB.1]	Feb 8 10:35:42 uem.cctl.company.com 2023-02-08T15:35:32.163755Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: BrandingChanged; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=uhkjqvsvlu02 Event Timestamp: 2023-02-08T15:35:28.087000 Feb 8 10:35:42 uem.cctl.company.com 2023-02-08T15:35:32.163755Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: BrandingAdvancedChanged; User: Administrator; Device Name: N/A;	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	EnrollmentUser: N/A; Event Source: Server; Event Module: Settings; Event Category: SystemSettings; Event Data: LoginSessionID=uhkjqvsvlu02 Event Timestamp: 2023-02-08T15:35:28.087000	
Initiation and termination of the trusted channel. [FTP_ITC.1(1)]	Refer to guidance documentation provided by the platform at [7] Section 7.	Windows Platform
Initiation and termination of the trusted channel. [FTP_TRP.1(1)]	Refer to guidance documentation provided by the platform at [7] Section 7.	Windows Platform
Initiation and termination of the trusted channel. [FTP_TRP.1(2)]	Refer to guidance documentation provided by the platforms at [7] Section 7, [8] Section 6.1, and [9] Section 5.4.	Windows Platform, iOS/iPadOS platform, and Android Platform
Failure to push a new application on a managed mobile device [FAU_GEN.1.1(2)]	**Failure to push a new application on a managed mobile device (Android)** Dec 19 10:57:56 uem.cctl.company.com 2022-12-19T15:56:01.275814Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Command; Event Data: Event Timestamp: 2022-12-19T15:56:00.713000 **Failure to push a new application on a managed mobile device (iOS)** Dec 19 09:20:15 uem.cctl.company.com 2022-12-19T14:18:23.194397Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ApplicationReasonChange; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Apps; Event Category: ApplicationSample; Event Data: ApplicationBundleId=com.air-watch.boxer;DeviceReportedReason=Failed;TimeReceived=12/19/2022 2:18:22 PM Event Timestamp: 2022-12-19T14:18:22.410000	UEM Server
Failure to update an existing application on a managed mobile device [FAU_GEN.1.1(2)]	Jan 6 08:42:03 uem.cctl.company.com 2023-01-06T13:41:48.316378Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Devices; Event Category: Command; Event Data: ApplicationType=Internal;Application=NIAPTestCase33;ErrorCode=2604 Could	UEM Server

Auditable Event(s)	Audit Record Examples	Component Generating Record
	not validate manifest.;ApplicationVersion=1.1;ApplicationUUID=17c12dfd-5d6a-48bc-97a3-516905b8ffb4 Event Timestamp: 2023-01-06T13:41:47.677000	
Startup and shutdown of the MDM Agent [FAU_GEN.1.1(2)]	Refer to guidance documentation provided by the platforms at [8] Section 6.1, and [9] Section 5.4.	iOS/iPadOS platform and Android Platform
MDM policy updated, any modification commanded by the MDM Server [FAU_GEN.1.1(2)]	**MDM policy updated** Dec 16 06:00:03 uem.cctl.company.com 2022-12-16T10:58:09.136123Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileConfirmed; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Profile=Test Case 058 - Subtest 04 Event Timestamp: 2022-12-16T10:58:08.207000 **Any modification commanded by the MDM Server** Dec 15 08:41:41 uem.cctl.company.com 2022-12-15T13:39:46.952370Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: RemoveApplicationRequested; User: Administrator; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Dashboard; Event Category: Command; Event Data: BytesReceived=17 Event Timestamp: 2022-12-15T13:39:46.370000	iOS Hub Agent, iOS/iPadOS platform, and Android Hub Agent
Success/failure of sending alert. (Android) [FAU_ALT_EXT.2 /ANDROID]	**Successful application of policies to a mobile device** Dec 19 10:43:03 uem.cctl.company.com 2022-12-19T15:41:08.103976Z AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileConfirmed; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Profile=Test 004 Event Timestamp: 2022-12-19T15:41:07.557000 **Generating periodic reachability events** Dec 19 10:47:00 uem.cctl.company.com 2022-12-19T15:45:05.226784Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: CheckIn; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Devices; Event Category: Delivery; Event Data: Application=;ApplicationVersion=;BytesReceived=82 Event Timestamp: 2022-12-19T15:45:04.523000 **Change in enrollment state (enrolled)**	Android Hub Agent

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Dec 16 08:52:42 uem.cctl.company.com 2022-12-16T13:52:29.931107Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: CCTest1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTest1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Event Timestamp: 2022-12-16T08:51:13.327000 **Change in enrollment state (unenrolled)** Jan 27 11:47:25 uem.cctl.company.com 2023-01-27T16:47:12.553787Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMConfirmed; User: sysadmin; Device Name: Deleting - Deleting - CCTestAD1 Android Android 11.0 RF8M6451QJJ; EnrollmentUser: N/A; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Event Timestamp: 2023-01-27T16:47:12.023000 **Failure to install an application from the MAS Server**, and **Failure to update an application from the MAS Server** Dec 19 10:57:56 uem.cctl.company.com 2022-12-19T15:56:01.275814Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Command; Event Data: Event Timestamp: 2022-12-19T15:56:00.713000 **Detection of apps on a deny list**, **Detection of apps not on an allow list**, and **Required apps missing** Dec 19 11:01:26 uem.cctl.company.com 2022-12-19T15:59:31.056869Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=Application List Event Timestamp: 2022-12-19T15:59:30.460000 **Unapproved device manufacturer** Dec 19 11:59:41 uem.cctl.company.com 2022-12-19T16:57:46.558148Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	Data: ComplianceStatus=NonCompliant;CompliancePolicy=Device Manufacturer Event Timestamp: 2022-12-19T16:57:45.980000 **Unapproved operating system version** Dec 19 11:09:34 uem.cctl.company.com 2022-12-19T16:07:39.439864Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=OS Version Event Timestamp: 2022-12-19T16:07:38.870000	
Success/failure of sending alert. (iOS) [FAU_ALT_EXT.2 /IOS]	**Successful application of policies to a mobile device** Dec 14 11:28:28 uem.cctl.company.com 2022-12-14T16:26:33.019655Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: InstallProfileConfirmed; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Profile=Test Case 008 - Policy Update Event Timestamp: 2022-12-14T16:26:32.467000 **Generating periodic reachability events** Dec 14 13:08:15 uem.cctl.company.com 2022-12-14T18:06:20.875432Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: CheckIn; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Devices; Event Category: Delivery; Event Data: Application=;ApplicationVersion=;BytesReceived=82 Event Timestamp: 2022-12-14T18:06:19.953000 **Change in enrollment state (enrolled)** Dec 14 10:04:17 uem.cctl.company.com 2022-12-14T15:02:22.805762Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=uem2021srv.uem2021.catl Event Timestamp: 2022-12-14T15:02:20.620000 **Change in enrollment state (unenrolled)** Jan 23 12:43:52 uem.cctl.company.com 2023-01-23T17:43:38.967342Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: BreakMDMConfirmed; User: sysadmin; Device Name: CCTestAD1 iPhone iOS	iOS/iPadOS platform

Auditable Event(s)	Audit Record Examples	Component Generating Record
	14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Devices; Event Category: Command; Event Data: Event Timestamp: 2023-01-23T17:43:38.403000 **Failure to install an application from the MAS Server**, Dec 19 09:20:15 uem.cctl.company.com 2022-12-19T14:18:23.194397Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ApplicationReasonChange; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: Apps; Event Category: ApplicationSample; Event Data: ApplicationBundleId=com.air-watch.boxer;DeviceReportedReason=Failed;TimeReceived=12/19/2022 2:18:22 PM Event Timestamp: 2022-12-19T14:18:22.410000 **Failure to update an application from the MAS Server** Jan 6 08:42:03 uem.cctl.company.com 2023-01-06T13:41:48.316378Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: InstallApplicationFailed; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Devices; Event Category: Command; Event Data: ApplicationType=Internal;Application=NIAPTestCase33;ErrorCode=2604 Could not validate manifest.;ApplicationVersion=1.1;ApplicationUUID=17c12dfd-5d6a-48bc-97a3-516905b8ffb4 Event Timestamp: 2023-01-06T13:41:47.677000 **Detection of apps on a deny list**, **Detection of apps not on an allow list**, and **Required apps missing** Dec 14 10:47:00 uem.cctl.company.com 2022-12-14T15:45:05.226784Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=Application List Event Timestamp: 2022-12-14T15:45:04.523000 **Unapproved model** Dec 14 11:15:45 uem.cctl.company.com 2022-12-14T16:13:50.157303Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: CCTestAD1 iPad iOS 14.6.0 GG7G5FWZQ16M; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data:	

Auditable Event(s)	Audit Record Examples	Component Generating Record
	ComplianceStatus=NonCompliant;CompliancePolicy=Model Event Timestamp: 2022-12-14T16:13:49.587000 **Unapproved operating system version** Dec 14 11:12:17 uem.cctl.company.com 2022-12-14T16:10:22.218183Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: ComplianceStatusChanged; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Compliance; Event Category: ComplianceStatus; Event Data: ComplianceStatus=NonCompliant;CompliancePolicy=OS Version Event Timestamp: 2022-12-14T16:10:21.643000	
All modifications to the audit configuration that occur while the audit collection functions are operating. [FAU_SEL.1]	Dec 19 13:16:42 uem.cctl.company.com 2022-12-19T18:14:47.664934Z 10.137.2.36 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=c5pxvson5loe;ApplicationGroup=Android Denylist Event Timestamp: Nov 2022-12-19T18:14:47.070000	iOS Hub Agent, iOS/iPadOS platform, and Android Hub Agent
Enrollment in management. [FIA_ENR_EXT.2]	**Enrollment in management (Android)** Dec 16 08:52:42 uem.cctl.company.com 2022-12-16T13:52:29.931107Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: CCTest1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTest1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Event Timestamp: 2022-12-16T08:51:13.327000 **Enrollment in management (iOS)** Dec 14 10:04:17 uem.cctl.company.com 2022-12-14T15:02:22.805762Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=uem2021srv.uem2021.catl Event Timestamp: 2022-12-14T15:02:20.620000	iOS/iPadOS platform, and Android Hub Agent
Failure of policy validation. [FMT_POL_EXT.2]	**Failure of policy validation (Android)** Jan 31 11:56:57 uem.cctl.company.com 2023-01-31T16:56:44.564385Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: PolicySigningFailed; User: sysadmin; Device Name: CCTestAD1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: Failure Reason=Code:	iOS Hub Agent, iOS/iPadOS platform, and Android Hub Agent

Auditable Event(s)	Audit Record Examples	Component Generating Record
	POLICY_SIGNING_SIGNATURE_VALIDATION_FAILED Event Timestamp: 2023-01-31T16:56:34.000000 **Failure of policy validation (iOS)** Jan 25 15:54:38 uem.cctl.company.com 2023-01-25T20:54:25.666406Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: Policy Validation signature missing from the respo; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Device; Event Module: CustomDeviceEvents; Event Category: Custom; Event Data: = Event Timestamp: 2023-01-25T15:52:36.377000	
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] Section 6.1, and [9] Section 5.4 **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)** Dec 16 08:52:42 uem.cctl.company.com 2022-12-16T13:52:29.931107Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: EnrollmentComplete; User: sysadmin; Device Name: CCTest1 Android Android 11.0 RFCR71C47ZN; EnrollmentUser: CCTest1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Event Timestamp: 2022-12-16T08:51:13.327000 **Enroll in management (iOS)** Dec 14 10:04:17 uem.cctl.company.com 2022-12-14T15:02:22.805762Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Device; Event: MDMEnrollmentComplete; User: sysadmin; Device Name: CCTestAD1 iPhone iOS 14.7.1 F17G80KL0D81; EnrollmentUser: CCTestAD1; Event Source: Server; Event Module: Enrollment; Event Category: Enrollment; Event Data: Url=uem2021srv.uem2021.catl Event Timestamp: 2022-12-14T15:02:20.620000 **Configure whether users can unenroll from management (Android)** Feb 13 09:24:32 uem.cctl.company.com 2023-02-13T14:24:24.002418Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: AndroidHeartbeatIntervalSettingChangedSuccess; User: Administrator; Device	iOS Hub Agent, iOS/iPadOS platform, Android Hub Agent, and Android Platform

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=l0wz5pzcx2cx Event Timestamp: 2023-02-13T14:24:23.433000 **Configure whether users can unenroll from management (iOS)** Jan 9 08:58:47 uem.cctl.company.com 2023-01-09T13:58:33.112246Z 10.137.2.36 AirWatch Syslog Details are as follows Event Type: Console; Event: AuthorizedSecurityPin; User: Administrator; Device Name: N/A; EnrollmentUser: N/A; Event Source: Server; Event Module: Administration; Event Category: SecurityPin; Event Data: LoginSessionID=1ng1vwbwrgyw;SecurityPinInputAttemptNumber=1;ActionAttempted=Delete DEP;User=Administrator Event Timestamp: 2023-01-09T13:58:32.560000 **Configure periodicity of reachability events (Android)** Jan 10 11:32:02 uem.cctl.company.com 2023-01-10T16:31:47.652331Z 10.137.2.36 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=rkdfmacy41w3 Event Timestamp: 2023-01-10T16:31:47.103000 **Configure periodicity of reachability events (iOS)** Feb 8 10:40:49 uem.cctl.company.com 2023-02-08T15:40:39.108603Z 10.137.2.36 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=wzbsq2eqqro2 Event Timestamp: 2023-02-08T15:40:38.537000	

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.