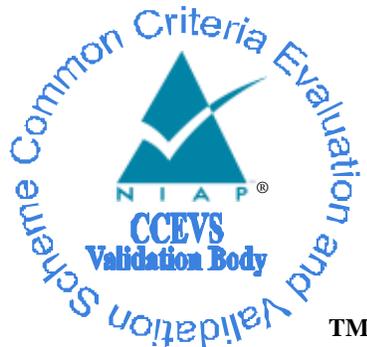


# National Information Assurance Partnership



## Common Criteria Evaluation and Validation Scheme Validation Report

### VMware Workspace ONE Unified Endpoint Management Version 2209

**Report Number: CCEVS-VR-VID11326-2023**  
**Version 1.0**  
**March 07, 2023**

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

Department of Defense  
ATTN: NIAP, SUITE: 6982  
9800 Savage Road  
Fort Meade, MD 20755-6982

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

**ACKNOWLEDGEMENTS**

**Validation Team**

Sheldon Durrant  
Lauren Hardy  
Lisa Mitchell  
Clare Parran

The MITRE Corporation

**Common Criteria Testing Laboratory**

Herbert Markle  
Chris Rakaczky

Booz Allen Hamilton (BAH)  
Laurel, Maryland

# Table of Contents

<b>1</b>	<b>EXECUTIVE SUMMARY</b> .....	<b>5</b>
<b>2</b>	<b>IDENTIFICATION</b> .....	<b>6</b>
<b>3</b>	<b>ASSUMPTIONS AND CLARIFICATION OF SCOPE</b> .....	<b>7</b>
3.1	ASSUMPTIONS .....	7
3.2	THREATS .....	7
3.3	CLARIFICATION OF SCOPE.....	8
<b>4</b>	<b>ARCHITECTURAL INFORMATION</b> .....	<b>9</b>
4.1	TOE INTRODUCTION .....	9
4.2	PHYSICAL BOUNDARY .....	9
<b>5</b>	<b>SECURITY POLICY</b> .....	<b>12</b>
5.1	SECURITY AUDIT .....	12
5.2	COMMUNICATION .....	12
5.3	CRYPTOGRAPHIC SUPPORT.....	12
5.4	IDENTIFICATION AND AUTHENTICATION .....	13
5.5	SECURITY MANAGEMENT .....	13
5.6	PROTECTION OF THE TSF .....	14
5.7	TOE ACCESS.....	14
5.8	TRUSTED PATH/CHANNELS .....	14
<b>6</b>	<b>DOCUMENTATION</b> .....	<b>15</b>
<b>7</b>	<b>EVALUATED CONFIGURATION</b> .....	<b>16</b>
<b>8</b>	<b>IT PRODUCT TESTING</b> .....	<b>17</b>
8.1	TEST CONFIGURATION .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.2	DEVELOPER TESTING .....	17
8.3	EVALUATION TEAM INDEPENDENT TESTING.....	17
8.4	EVALUATION TEAM VULNERABILITY TESTING.....	17
<b>9</b>	<b>RESULTS OF THE EVALUATION</b> .....	<b>19</b>
9.1	EVALUATION OF THE SECURITY TARGET (ASE) .....	19
9.2	EVALUATION OF THE DEVELOPMENT (ADV).....	19
9.3	EVALUATION OF THE GUIDANCE DOCUMENTS (AGD).....	19
9.4	EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC).....	20
9.5	EVALUATION OF THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE).....	20
9.6	VULNERABILITY ASSESSMENT ACTIVITY (VAN) .....	20
9.7	SUMMARY OF EVALUATION RESULTS .....	20
<b>10</b>	<b>VALIDATOR COMMENTS</b> .....	<b>21</b>
<b>11</b>	<b>ANNEXES</b> .....	<b>22</b>
<b>12</b>	<b>SECURITY TARGET</b> .....	<b>23</b>
<b>13</b>	<b>LIST OF ACRONYMS</b> .....	<b>24</b>
<b>14</b>	<b>TERMINOLOGY</b> .....	<b>25</b>
<b>15</b>	<b>BIBLIOGRAPHY</b> .....	<b>26</b>

## List of Tables

Table 1: Evaluation Identifiers .....	6
Table 2: TOE Assumptions .....	7
Table 3: TOE Threats .....	8
Table 4: TOE Component Specifications .....	10

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

Table 5: IT Environment Components .....	11
Table 6: Cryptographic Algorithm Table for the Hub Agents .....	<b>Error! Bookmark not defined.</b>
Table 7: Cryptographic Algorithm Table for the Hub Agents .....	<b>Error! Bookmark not defined.</b>
Table 8: Acronym Definitions .....	24
Table 9: Term Definitions .....	25

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

## **1 Executive Summary**

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of VMware Workspace ONE Unified Endpoint Management Version 2209 provided by VMware, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in March 2023. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *Protection Profile for Mobile Device Management, version 4.0* [MDMPP] and *Protection Profile Module for Mobile Device Management Agents, version 1.0* [AGENTMOD].

The Target of Evaluation (TOE) is a Mobile Device Management product and is comprised of an MDM Server component (UEM Server) and one or more VMware Intelligent Hub Agent components (iOS Hub Agent and Android Hub Agent). In the evaluated configuration of the TOE, the UEM Server is deployed in an on-premises configuration. The UEM Server component provides a centralized enterprise level management capability for a collection of mobile devices running the iOS and Android Hub Agents. The UEM Server is also a Mobile Application Store (MAS) Server that allows managed devices to download apps from a trusted repository that resides within the organization managing the device. The management functionality includes management of Administrators and users, mobile device enrollment, mobile device status, mobile device compliance and policy management, and application management.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the MDMPP and the AGENTMOD. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The Validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the MDMPP and the AGENTMOD Assurance Activities. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *VMware Workspace ONE Unified Endpoint Management Version 2209 Security Target v1.0*, dated February 06, 2023 and analysis performed by the Validation team.

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

## 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product’s evaluation. Upon successful completion of the evaluation, the product is added to NIAP’s Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

<b>Item</b>	<b>Identifier</b>
<b>Evaluation Scheme</b>	United States NIAP Common Criteria Evaluation and Validation Scheme
<b>TOE</b>	VMware Workspace ONE Unified Endpoint Management Version 2209
<b>Protection Profile</b>	Protection Profile for Mobile Device Management, version 4.0 and Protection Profile Module for Mobile Device Management Agents, version 1.0, including all applicable NIAP Technical Decisions and Policy Letters
<b>Security Target</b>	VMware Workspace ONE Unified Endpoint Management Version 2209 Target v1.0, dated February 06, 2023
<b>Evaluation Technical Report</b>	Evaluation Technical Report for a Target of Evaluation “VMware Workspace ONE Unified Endpoint Management Version 2209” Evaluation Technical Report v1.0 dated February 10, 2023
<b>CC Version</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
<b>Conformance Result</b>	CC Part 2 extended, CC Part 3 conformant
<b>Sponsor</b>	VMware, Inc.
<b>Developer</b>	VMware, Inc.
<b>Common Criteria Testing Lab (CCTL)</b>	Booz Allen Hamilton, Laurel, Maryland
<b>CCEVS Validators</b>	Sheldon Durrant, Lauren Hardy, Lisa Mitchell, Clare Parran

**Table 1: Evaluation Identifiers**

### 3 Assumptions, Threats and Clarification of Scope

#### 3.1 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the [MDMPP] and [AGENTMOD].

Assumption	Assumption Definition
<b>A.COMPONENTS_RUNNING</b> (applies to distributed TOEs only)	[MDMPP] For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
<b>A.CONNECTIVITY</b>	The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
<b>A.MDM_SERVER_PLATFORM</b>	[MDMPP] The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities.  The MDM Server relies on this platform to provide a range of security-related services including 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 to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide MDM services, employing features such as a host-based firewall, which limits its network role to providing MDM functionality.
<b>A.MOBILE_DEVICE_PLATFORM</b>	[AGENTMOD] The MDM Agent relies upon mobile platform and hardware evaluated against the MDF PP and assured to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM Agent.
<b>A.PROPER_ADMIN</b>	One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
<b>A.PROPER_USER</b>	Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

**Table 2: TOE Assumptions**

#### 3.2 Threats

Note: Unless otherwise stated Threats, Organizational Security Policies (OSPs), Assumptions and Security Objectives apply to both the Agent and Server.

This section identifies the threats against the TOE. These threats have been taken from the [MDMPP] and [AGENTMOD].

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

Threat	Threat Definition
<b>T.MALICIOUS_APPS</b>	[MDMPP] Malicious or flawed application threats exist because apps loaded onto a mobile device may include malicious or exploitable code. An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE, resulting in the compromise of TOE or TOE data.
<b>T.BACKUP</b>	[AGENTMOD] An attacker may try to target backups of data or credentials and exfiltrate data. Since the backup is stored on either a personal computer or end user's backup repository, it's not likely the enterprise would detect compromise.
<b>T.NETWORK_ATTACK</b>	[MDMPP] An attacker may masquerade as an MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands.
<b>T.NETWORK_EAVESDROP</b>	[MDMPP] An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the MDM Server and other endpoints.
<b>T.PHYSICAL_ACCESS</b>	[MDMPP] The mobile device may be lost or stolen, and an unauthorized individual may attempt to access user data. Although these attacks are primarily directed against the mobile device platform, the TOE configures features, which address these threats.

**Table 3: TOE Threats**

### 3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Mobile Device Management, version 4.0 [MDMPP] and Protection Profile Module for Mobile Device Management Agents, version 1.0 [AGENTMOD], including all relevant NIAP Technical Decisions. A subset of the “optional” and “selection-based” security requirements defined in the MDMPP and the AGENTMOD are claimed by the TOE and documented in the ST.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to security functionality not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by the product, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

## **4 Architectural Information**

Note: The following architectural description is based on the description presented in the Security Target.

### **4.1 TOE Introduction**

The TOE is a Mobile Device Management product and is comprised of an MDM Server component (UEM Server) and one or more agent components called VMware Intelligent Hubs (iOS Hub agent and Android Hub agent). In the evaluated configuration of the TOE, the UEM Server is deployed in an on-premises configuration. The UEM Server component provides a centralized enterprise level management capability for a collection of mobile devices running the iOS and Android Hub agents. The UEM Server is also a Mobile Application Store (MAS) Server that allows managed devices to download apps from a trusted repository that resides within the organization managing the device. The management functionality includes management of Administrators and users, mobile device enrollment, mobile device status, mobile device compliance and policy management, and application management. Administrators access the UEM Server through the Admin Console interface in order to manage users, policies, and devices. Users access the UEM Server through the Self-Service Portal, which allows them to perform administrative functions relating to their own devices.

The UEM Server runs on a Microsoft Windows Server 2019 operating system and authentication to the UEM Server is provided by the Active Directory/LDAP service. The UEM Server also provides local authentication for initial setup and to mitigate a denial of service in the event the Active Directory/LDAP service is unavailable. The UEM Server stores audit data remotely in a SQL database but can send audit records via a TLS encrypted trusted channel to a remote Syslog Server for remote storage.

In the evaluated configuration, the Hub agent runs on mobile devices with either Apple iOS 14, Apple iPadOS 14, and/or Android 11 operating systems. The communication channel between the Hub agent and the UEM Server is protected by TLS. Apple DEP is used to enroll the Apple devices with the UEM Server so that it can be managed by the UEM Server. The Hub agents provide status and policy information about the mobile device to the UEM Server. Figure 1 in the ST depicts the network configuration of the TOE.

The TOE consists of a UEM Server and one or more instances of the iOS and Android Hub agents running on mobile devices. The expected deployment of the TOE is to have an on-premises deployment of the UEM Server running behind the firewall. The UEM Server hosts the Self-Service Portal so that enterprise users can enroll and manage their own devices from outside the firewall and the Admin Console resides behind the firewall. The connection between the iOS and Android Hub agent devices and the UEM Server is also protected by HTTPS. The connections between the UEM Server, and the Syslog Server and AD/LDAP Server are protected with TLS. The UEM Server connects to a SQL Database to store configuration information. The UEM Server is also connected to a CA Server in the internal network for the purposes of issuing unique certificates to the Hub agents.

### **4.2 Physical Boundary**

The TOE is comprised of software and includes the following components:

<b>Component</b>	<b>Definition</b>
------------------	-------------------

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

<b>Workspace ONE Unified Endpoint Management 2209 (UEM Server)</b>	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.
<b>Android Intelligent Hub 22.09 (Android Hub agent)</b>	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 to provide status and policy information about the device.
<b>iOS Intelligent Hub 22.11 (iOS Hub agent)</b>	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.

**Table 4: TOE Component Specifications**

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:

<b>Component</b>	<b>Definition</b>
<b>Active Directory / LDAP Server</b>	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.
<b>Apple iOS 14 Mobile Device (VID11146)</b>	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.
<b>Apple iPadOS 14 Mobile Device (VID11147)</b>	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.
<b>Apple Push Notification Service (APNS) / Apple DEP</b>	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.
<b>Certification Authority (CA) Server</b>	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.
<b>Firebase Cloud Messaging Service (FCM)</b>	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).
<b>Samsung Android 11 Mobile Device (VID 11160)</b>	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.
<b>SQL database</b>	The TOE’s RDBMS database used to store configuration settings and device data. In the evaluated configuration, Microsoft SQL Server 2019 is used.

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

<b>Syslog Server</b>	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.
<b>Windows Server 2019 (Version 1809)</b>	This is the OS that the UEM Server is installed on.
<b>Workstation</b>	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.

**Table 5: IT Environment Components**

## **5 Security Policy**

### **5.1 Security Audit**

The UEM Server component of the TOE creates audit records for auditable events related to administrative actions, configuration of the UEM Server itself, and server-initiated management activities that affect one or more managed mobile devices. The UEM Server's MAS Server functionality also generates audit records when it experiences a failure to push or update an application on a managed mobile device. The audit records are stored in an SQL database and are transferred to a remote Syslog Server over a TLS encrypted trusted channel. Audit records can be viewed on the Admin Console.

The UEM Server can issue 'compliance policies' to managed mobile devices. Compliance policies are used to compare the configuration, status, or characteristics of a mobile device against a certain baseline and can be used to generate an alert to an Administrator if an anomaly is detected. The Administrator can also request on-demand connectivity status updates through the use of push notifications.

iOS and Android Hub agents' audit records are created as long as the underlying mobile device is powered on. The iOS and Android Hub agents generate audit records for the activities it performs as a result of its interactions with the UEM Server or as a result of stored policy information. The iOS and Android Hub agents facilitate alerts by providing data to the UEM Server on a periodic basis. The UEM Server can then analyze this data (or the absence of data in the case of periodic reachability events) in order to determine if anomalous behavior is occurring.

### **5.2 Communication**

The iOS and Android Hub agents mobile devices are registered with the UEM Server so they can be enrolled into management by the UEM Server. This requires an Administrator to enable communications between these TOE components by including the mobile device's identifier in an allow list of devices that are allowed to enroll on the UEM Server. The enrollment process occurs over an HTTPS/TLS trusted channel that is handled by each TOE components' underlying platform. An Administrator can disable the communications between an iOS or Android Hub agent and the UEM Server by performing a wipe of the Hub agent's mobile device.

### **5.3 Cryptographic Support**

The UEM Server invokes the Windows Server 2019 platform for cryptographic services to establish TLS and HTTPS/TLS trusted channels and paths to ensure secure communications of data in transit. This includes the use of RSA and Elliptic Curve Cryptography (ECC) key establishment techniques. The MAS Server is integrated with the UEM Server, so it invokes the same cryptography services. The UEM Server also invokes the Windows Server 2019 platform to digitally sign policies sent to the Hub agents.

The iOS and Android Hub agents invoke their underlying mobile device platforms (Apple iOS 14, Apple iPadOS 14, and Android 11 respectively) for cryptographic services to also establish trusted communications. The iOS Hub agent invokes its underlying platform to verify the digital signatures of all policies received from the UEM Server. The Android Hub agent software contains an OpenSSL library for implementing the digital signature verification of all policies received from the UEM Server.

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

All cryptographic mechanisms use the TOE components' platform provided DRBG functionality to support their cryptographic operations. Cryptographic functionality includes encryption/decryption services, credential/key storage, key establishment, key destruction, hashing services, signature services, and hashed message authentication.

The following table contains the CAVP algorithm certificates corresponding to the Android Hub agent's digital signature verification cryptographic functionality which is implemented by its OpenSSL module.

	<b>Algorithm</b>	<b>CAVP Cert. # (Android 11)</b>
FCS_COP.1(2) – Hashing Algorithms	SHA-512	A3270
FCS_COP.1(3) – Signature Algorithms	ECDSA with P-521 NIST curve	A3270

**Table 6: Cryptographic Algorithm Table for the Hub Agents**

#### **5.4 Identification and Authentication**

The iOS and Android Hub agents register with the UEM Server so that their mobile device can be enrolled into management by the UEM Server. The mobile device user that is performing the enrollment must have a user account on the UEM Server to access the Self-Service Portal and authenticate to the TOE. During the enrollment process, the iOS and Android Hub agents record the UEM Server's DNS name and full URL with hostname. The iOS and Android Hub agents also receive a unique certificate during enrollment that is used to establish an HTTPS trusted channel with the UEM Server.

Administrators (through the Admin Console) and users (through the Self-Service Portal) cannot access the UEM Server without being authenticated. Administrators and users can view the configured pre-authentication warning banner and query the UEM Server's software version number prior to authentication.

The UEM Server interfaces with the underlying Windows Server 2019 platform to provide certificate validation services. Certificates are used for HTTPS/TLS authentication, code signing for software updates, code signing for integrity verification, and signing of MDM policies. The iOS and Android Hub agents rely on the underlying platform to perform all certificate validation services, except for policy signing on Android devices which is validated by the Android Hub agent's implementation of OpenSSL.

#### **5.5 Security Management**

The TSF provides separate administrative interfaces for Administrators and for mobile device users. Administrators use the Admin Console to manage users, policies, and devices, while MD users use the Self-Service Portal to perform actions related to their own devices. The mobile device user installs the TOE's iOS or Android Hub agent on the mobile device which will communicate with the UEM Server to enroll in management. Once enrolled, the TOE will prevent user-directed unenrollment from management.

The UEM Server can be used to transmit specific commands to a managed device such as forcibly locking the device, initiating a wipe operation, or sending a push notification. The UEM Server can also define policies (known as profiles) that specify the configuration settings for a device. These configuration settings can include functionality such as configuration of the password policy and what settings are applied to Wi-Fi connections. The UEM Server transmits iOS policies either to the iOS Hub agent or iOS/iPadOS platform directly, depending on the

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

functionality being configured. The UEM Server transmits Android policies to the Android Hub agent. The UEM Server invokes its underlying platform to sign all policy data using ECDSA with SHA-512. The underlying iOS/iPadOS mobile platform and Android Hub agent will validate the signed policies when they are received.

The UEM Server also includes the MAS Server functionality, which provides the ability to grant or deny access to specific applications stored on the MAS Server to devices or groups of devices. The MAS Server is accessed through the same Admin Console interface as the UEM Server, so the administrative roles defined for both components are the same.

### **5.6 Protection of the TSF**

The communications between the UEM Server and iOS and Android Hub agents are protected using HTTPS/TLS which is provided by the underlying platforms of the TOE components.

The UEM Server invokes its platform to verify the digital signatures of executables and .dlls using Microsoft's Authenticode making use of X.509v3 certificates. In addition, the UEM Server's platform uses FIPS validated cryptographic modules which perform their own integrity checks at startup.

The TOE components invoke their underlying platforms to update their software and the platforms will verify the digital signatures of the updates prior to installing them. The TOE components' software contains third party libraries. The TOE components use only documented APIs from their underlying platforms.

### **5.7 TOE Access**

The UEM Server displays a pre-authentication banner for the Admin Console and the Self-Service Portal. This can be customized by Administrators to fit the needs of the organization deploying the TOE.

### **5.8 Trusted Path/Channels**

The trusted communication channels between the UEM Server and the devices running the iOS and Android Hub agents, the Syslog Server, and the AD/LDAP Server make use of TLS or HTTPS/TLS, depending on the interface. The trusted communication channels are provided by the TOE components' underlying platforms.

The UEM Server platform uses HTTPS/TLS to provide a trusted path between itself and remote Administrators through the Admin Console and mobile device users through the Self-Service Portal as well as during the enrollment of a mobile device.

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

## **6 Documentation**

The vendor provided the following guidance documentation in support of the evaluation:

- VMware Workspace ONE Unified Endpoint Management Version 2209 Supplemental Administrative Guidance version 1.0
- Installing Workspace ONE UEM for on-premises and SaaS deployments VMware Workspace ONE UEM 2209
- Upgrade Guide VMware Workspace ONE UEM 2209
- Console Basics VMware Workspace ONE UEM 2209
- Directory Services VMware Workspace ONE UEM 2209
- Certificate Authority Integrations VMware Workspace ONE UEM 2209
- Integration with Apple Business Manager VMware Workspace ONE UEM 2209

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

## **7 Evaluated Configuration**

The evaluated configuration, as defined in the Security Target, is VMware Workspace ONE Unified Endpoint Management version 2209 comprising of the Unified Endpoint Management Server and one or more VMware Intelligent Hub Agents installed on Apple and Android devices. The minimum configuration for this evaluation 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. The Workspace ONE Unified Endpoint Management Server runs the software version 2209. The Android Intelligent Hub Agent runs software version 22.09. The iOS Intelligent Hub Agent runs software version 22.11. Section 4 describes the TOE's configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to directly communicate with the following environment components:

- Active Directory / LDAP Server for remote authentication
- Apple iOS 14 Mobile Device (VID11146) for installing iOS Hub Agent and to be managed by the TOE
- Apple iPadOS 14 Mobile Device (VID11147) for installing iOS Hub Agent and to be managed by the TOE
- Apple Push Notification Service (APNS) / Apple DEP for communicating with iOS devices and enrollment
- Certification Authority (CA) Server for issuing certificates
- Firebase Cloud Messaging Service (FCM) for communicating with Android devices
- Samsung Android 11 Mobile Device (VID11160) for installing Android Hub Agent and to be managed by the TOE
- SQL database for storing TOE data
- Syslog Server for recording of syslog data
- Windows Server 2019 (Version 1809) for installing UEM Server on
- Workstation for remote administration

To use the product in the evaluated configuration, the product must be configured as specified in the *VMware Workspace ONE Unified Endpoint Management Version 2209 Supplemental Administrative Guidance Version 1.0* document.

## **8 IT Product Testing**

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Evaluation Technical Report for a Target of Evaluation “VMware Workspace ONE Unified Endpoint Management Version 2209” Evaluation Technical Report v1.0 dated February 10, 2023*, as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation “VMware Workspace ONE Unified Endpoint Management Version 2209” Assurance Activities Report v1.0 dated February 10, 2023*.

### **8.1 Developer Testing**

No evidence of developer testing is required in the Evaluation Activities for this product.

### **8.2 Evaluation Team Independent Testing**

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the MDMPP and the AGENTMOD for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

### **8.3 Evaluation Team Vulnerability Testing**

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include the [rapid7.com/db/vulnerabilities](https://rapid7.com/db/vulnerabilities), [cvedetails.com/vulnerability-search](https://cvedetails.com/vulnerability-search), and the [nvd.nist.gov](https://nvd.nist.gov).

Upon the completion of the vulnerability analysis research and initially discovering no known vulnerabilities, the team identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications  
This test will attempt to intercept any TOE involved network traffic as evaluated in FPT\_ITT.1(2), FTP\_ITC.1(1), FTP\_TRP.1(1), and FTP\_TRP.1(2).
- Port Scanning  
This test will attempt to identify any way to subvert the security of the TOE by executing a side channel attack. A port scanner will be run against the TOE in an attempt to identify any open ports. Any port on a system that accepts external connections could potentially

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

- represent an attack vector. This test will identify any such ports and will attempt to enumerate them to determine their original purpose.
- **Web Interface Vulnerability Identification**  
This test looks for major vulnerabilities including cross-site scripting, SQL injection, directory traversal, unchecked file uploads, etc. as well as less critical vulnerabilities such as unnecessary information disclosure.

The TOE successfully prevented any attempts of subverting its security.

## **9 Results of the Evaluation**

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the MDMPP and the AGENTMOD.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

### **9.1 Evaluation of the Security Target (ASE)**

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the VMware Workspace ONE Unified Endpoint Management Version 2209 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the Evaluator performed an assessment of the Evaluation Activities specified in the MDMPP and the AGENTMOD Supporting Document in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

### **9.2 Evaluation of the Development (ADV)**

The evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the Evaluator performed the Evaluation Activities specified in the MDMPP and the AGENTMOD Supporting Document related to the examination of the information contained in the TOE Summary Specification.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

### **9.3 Evaluation of the Guidance Documents (AGD)**

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the Evaluator performed the

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

Evaluation Activities specified in the MDMPP and the AGENTMOD Supporting Document related to the examination of the information contained in the operational guidance documents.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

#### **9.4 Evaluation of the Life Cycle Support Activities (ALC)**

The Evaluation team applied each ALC CEM work units. The Evaluation team found that the TOE was identified.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

#### **9.5 Evaluation of the Test Documentation and the Test Activity (ATE)**

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the MDMPP and the AGENTMOD Supporting Document and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the MDMPP and the AGENTMOD Supporting Document, and that the conclusion reached by the Evaluation team was justified.

#### **9.6 Vulnerability Assessment Activity (VAN)**

The Evaluation team applied each AVA CEM work unit. The Evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The Evaluation team also ensured that the specific vulnerabilities defined in the MDMPP and the AGENTMOD Supporting Document were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the MDMPP and the AGENTMOD Supporting Document, and that the conclusion reached by the Evaluation team was justified.

#### **9.7 Summary of Evaluation Results**

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team performed the Evaluation Activities in the MDMPP and the AGENTMOD Supporting Document, and correctly verified that the product meets the claims in the ST.

## **10 Validator Comments**

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *VMware Workspace ONE Unified Endpoint Management Version 2209 Supplemental Administrative Guidance Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the routers and switches network infrastructure, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

## **11 Annexes**

Not applicable

## **12 Security Target**

The security target for this product's evaluation is *VMware Workspace ONE Unified Endpoint Management Version 2209 Security Target v1.0*, dated February 06, 2023.

## 13 List of Acronyms

<b>Acronym</b>	<b>Definition</b>
<b>APNS</b>	Apple Push Notification Service
<b>CA</b>	Certificate Authority
<b>CC</b>	Common Criteria
<b>CPU</b>	Central Processing Unit
<b>CSP</b>	Critical Security Parameter
<b>DEP</b>	[Apple] Device Enrollment Program
<b>FCM</b>	[Android] Firebase Cloud Messaging [Service]
<b>FQDN</b>	Fully Qualified Domain Name
<b>GUI</b>	Graphical User Interface
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure over a bidirectional TLS encrypted tunnel
<b>IMEI</b>	International Mobile Equipment Identity
<b>IP</b>	Internet Protocol
<b>IIS</b>	Internet Information Services
<b>IT</b>	Information Technology
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MAS</b>	Mobile Application Store
<b>MD</b>	Mobile Device
<b>MDM</b>	Mobile Device Management
<b>NFC</b>	Near-Field Communication
<b>NIAP</b>	National Information Assurance Partnership
<b>OS</b>	Operating System
<b>OSP</b>	Organizational Security Policy
<b>PP</b>	Protection Profile
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>SSL</b>	Secure Sockets Layer
<b>ST</b>	Security Target
<b>TCP</b>	Transmission Control Protocol
<b>TLS</b>	Transport Layer Security
<b>TOE</b>	Target of Evaluation
<b>TSF</b>	TOE Security Function
<b>UEM</b>	Unified Endpoint Management
<b>UI</b>	User Interface
<b>USB</b>	Universal Serial Bus
<b>VPN</b>	Virtual Private Network
<b>WLAN</b>	Wireless Local Area Network

**Table 7: Acronym Definitions**

## 14 Terminology

<b>Term</b>	<b>Definition</b>
<b>Administrator</b>	The claimed Protection Profile defines an Administrator as the person who is responsible for management activities, including setting the policy that is applied by the enterprise on the mobile device. This TOE defines separate user roles.
<b>Authorized Administrator</b>	Synonymous with Administrator.
<b>End User</b>	An individual who possesses a mobile device that is managed by VMware and who has limited authority to perform management functions using the Self-Service Portal
<b>MD User</b>	User with a mobile device (MD).
<b>Role</b>	The level of access given to Administrator accounts. The TOE comes with pre-defined roles but new roles with custom sets of privileges can be created.
<b>System Administrator</b>	The class of TOE Administrators that have complete access to a VMware environment, including the underlying Windows Server 2016 platform.
<b>Trusted Channel</b>	An encrypted connection between the TOE and a system in the Operational Environment.
<b>Trusted Path</b>	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
<b>User</b>	In a CC context, any individual who has the ability to manage TOE functions or data.

**Table 8: Term Definitions**

**VALIDATION REPORT**  
**VMware Workspace ONE Unified Endpoint Management Version 2209**

## **15 Bibliography**

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Mobile Device Management, version 4.0
6. Protection Profile Module for Mobile Device Management Agents, version 1.0
7. VMware Workspace ONE Unified Endpoint Management Version 2209 Security Target v1.0, dated February 06, 2023
8. VMware Workspace ONE Unified Endpoint Management Version 2209 Supplemental Administrative Guidance Version 1.0, dated February 06, 2023
9. Installing Workspace ONE UEM for on-premises and SaaS deployments VMware Workspace ONE UEM 2209
10. Upgrade Guide Workspace ONE UEM 2209
11. Console Basics VMware Workspace ONE UEM 2209
12. Directory Services VMware Workspace ONE UEM 2209
13. Certificate Authority Integrations VMware Workspace ONE UEM 2209
14. Integration with Apple Business Manager VMware Workspace ONE UEM 2209
15. Assurance Activities Report for a Target of Evaluation “VMware Workspace ONE Unified Endpoint Management Version 2209” Assurance Activities Report Version 1.0, dated February 10, 2023
16. Evaluation Technical Report for a Target of Evaluation “VMware Workspace ONE Unified Endpoint Management Version 2209” Evaluation Technical Report v1.0 dated February 10, 2023.