National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Endpoint Manager Mobile (EPMM) System 12

Report Number: CCEVS-VR-VID11566-2025

Dated: 10/15/2025

Version: 1.0

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

ACKNOWLEDGEMENTS

Validation Team

Lisa Mitchell

Sheldon Durrant

Linda Morrison

Clare Parran

Lori Sarem

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Elliot Keen

Eric Issac

Shaina Rae

Joan Marshall

Shyam Sundar Krishnamurthy

Intertek Acumen Security

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Ivanti Endpoint Manager Mobile (EPMM) System 12 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in October 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the •*PP-Configuration for Mobile Device Management (MDM) and MDM Agents*, Version 1.0, 27 January 2020 [CFG_MDM-MDM_AGENT_V1.0] which includes the *Protection Profile for Mobile Device Management*, Version 4.0, 25 April 2019 [PP_MDM_V4.0] and the *PP-Module for MDM Agents*, Version 1.0, 25 April 2019 [MOD_MDM_AGENT_V1.0] plus the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March, 2019 [PKG_TLS_V1.1] .

The TOE identified in this VR 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 Protection Profile (PP). This VR 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 ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Endpoint Manager Mobile (EPMM) System 12* Security Target, version 3.5 and analysis performed by the validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Ivanti Endpoint Manager Mobile (EPMM) System 12
Protection Profile	*PP-Configuration for Mobile Device Management (MDM) and MDM Agents*, Version 1.0, 27 January 2020 [CFG_MDM-MDM_AGENT_V1.0] which includes the *Protection Profile for Mobile Device Management*, Version 4.0, 25 April 2019 [PP_MDM_V4.0] and the *PP-Module for MDM Agents*, Version 1.0, 25 April 2019 [MOD_MDM_AGENT_V1.0] plus the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March, 2019 [PKG_TLS_V1.1]
Security Target	*Ivanti Endpoint Manager Mobile (EPMM) System 12* Security Target, version 3.5
Evaluation Technical Report	*Evaluation Technical Report for Ivanti Endpoint Manager Mobile (EPMM) System 12*, version 1.2
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor & Developer	Ivanti, Inc.
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security, 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Lisa Mitchell, Sheldon Durrant, Linda Morrison, Clare Parran, Lori Sarem, Chris

Item	Identifier
	Thorpe

3 Architectural Information

The Target of Evaluation (TOE) is the Ivanti Endpoint Mobile Manager (EPMM) 12 System (Version 12). The TOE (EPMM) is a distributed TOE and consists of two software components: the EPMM MDM Server and the EPMM MDM Agent (also referred to as MDM Server and MDM Agent).

The MDM Agent is installed on Android devices as an application that is supplied by Ivanti.

This Ivanti CC evaluation includes the Mobile Device Management (MDM) and the Mobile Application Management (MAM) functionality of the Ivanti EPMM. The Mobile Content Management (MCM) functionality of the EPMM is excluded from the CC evaluation. Additionally, the Target of Evaluation (TOE) includes Mobile Application Store (MAS) functionality that hosts applications, authenticates Agents, and securely transmits applications to enrolled mobile devices.

The MDM Server is a software application deployed on a virtual host. The MDM Server manages and monitors one or more instances of an MDM Agent. The MDM Agent is an application running on an Android device. This evaluation includes MDM Agent running on two different Android devices and operating system version:

- Galaxy S22 Ultra 5G running Android 13
- Galaxy S23 Ultra 5G running Android 14

3.1 TOE Type

The TOE is a distributed mobile device management system and includes both the server software and the client software.

3.2 Use Case

The TOE's use case is [USE CASE 1] "Enterprise-owned device for general purpose enterprise use" as defined in MOD_MDM_AGENT_V1.0. [USE CASE 1] An Enterprise-owned device for general-purpose business use is commonly called Corporately Owned, Personally Enabled (COPE). This use case entails a significant degree of Enterprise control over configuration and software inventory. Enterprise administrators use an MDM product to establish policies on themobile devices prior to user issuance. Users may use Internet connectivity to browse the web or access corporate mail or run Enterprise applications, but this connectivity may be under significant control of the Enterprise. The user may also be expected to store data and use applications for personal, non-enterprise use. The Enterprise administrator uses the MDM product to deploy security policies and query mobile device status.

3.3 TOE Description

The TOE is an MDM solution where the claimed security functions are implemented in a central MDM Server and distributed MDM Agents. The EPMM MDM Server integrates with backend enterprise IT systems and enables IT to define security and management policies for mobile apps.

The MDM Server is a software application that runs on an Intel x64 architecture server platform as a virtual system with Oracle Linux as the operating system (OS).

The MDM Server provides two administrative interfaces, each used for specific administrative actions. The Admin Portal provides capabilities for administrators to manage users, devices, policies and mobile device configurations. The System Manager provides administrative functions to control and configure the operation of the MDM Server including basic system configuration information (e.g., network addresses, date/time, hostname, e-mail settings), TOE updates, certificate management, TLS configuration, and export of various operational logs.

The MDM Agent, an application running on Galaxy S22 and S23 running Android 13 and 14 respectively, is an Android application. The MDM Agents work with the MDM Server to configure corporate email, Wi-Fi, VPN, and X.509 security certificates and to create a clear separation between personal and business information. Once installed, the MDM Agent creates a secure EPMM container that protects enterprise data and applications. This allows an MDM Server Administrator to selectively wipe only the enterprise data on the device if the user leaves or if the device falls out of compliance or is lost.

4 Security Policy

The TOE provides the security functions required by the:

- *Protection Profile for Mobile Device Management*, Version 4.0, hereafter referred to as PP_MDM_V4.0.
- *PP-Module for MDM Agent*, Version 1.0, hereafter referred to as MOD_MDM_AGENT_V1.0.
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, hereafter referred to as PKG_TLS_V1.1.

4.1.1.1 Security Audit

The MDM Server has the capability to create and retain audit logs for significant security incidents in real-time. These logs are securely stored by the MDM Server and can be accessed for review by authorized administrators. Additionally, the MDM Server exports these audit logs to a syslog server.

The MDM Agent possesses the capability to produce audit logs for events pertaining to security and can signal when it has been registered and when policies are effectively implemented onto it.

4.1.1.2 Cryptographic Support

Both the MDM Server and MDM Agent incorporate cryptographic modules equipped with certified algorithms to perform cryptographic operations. These operations encompass asymmetric key generation and exchange, encryption/decryption, cryptographic hashing, and keyed-hash message authentication. To support these functions adequate mechanisms for random bit generation, the destruction of keys and protected data are provided.

The cryptographic functionality is used to implement security communication protocols: TLS and HTTPS used for communication between the MDM Server and the MDM Agent, the syslog server, as well as between the MDM Server and a trusted, remote administrator.

4.1.1.3 Identification and Authentication

The MDM Server requires that users, whether administrators or mobile device users (MD users), to be authenticated before any security related functionality is allowed. MD Users are required to enroll their device with the MDM Server using an MDM Agent.

Both the MDM Server and the MDM Agent are required to utilize X.509 certificates which includes the validation check of the certificate in relation with the TLS connection in order to create a secure connection with the MDM Server and MDM Agent. This will also occur with connections between the MDM Server and administrators that have remote access via the web interface and the syslog server.

4.1.1.4 Security Management

The MDM Server allows for two distinct roles: that of the Administrator and the mobile device user (MD User). The Administrator interacts with the MDM Server and MD User interacts with a

device that hosts the MDM Agent. The MDM Server also supports user access to management functions by defining their role and the capabilities each role is allowed.

The MDM Server presents all functionality needed to manage its own security functions as well as to manage the mobile device policies that are transmitted to MDM Agents. This ensures that security management functions are only allowed use by authorized administrators. MD Users are only allowed necessary functions such as their enrolling in the MDM Server.

The MDM Agent holds functionality needed to create a secure connection with and enrollment in the MDM Server, implement any policies received from an appropriately enrolled MDM Server, and be able to account the results of applying such policies.

4.1.1.5 Protection of the TSF

The MDM Server and Agent act together in order to ensure all security related interactions between their components are protected from modification and disclosure and any undesirable entities.

The MDM Server contains the ability to perform self-tests to make sure that appropriate functionality is taking place and is maintained. The MDM Server is able to verify cryptographically during start-up that its executable image has not been tampered with or corrupted.

The MDM Server and MDM Agents utilize digital signatures to verify trusted updates which mitigates the risk of malicious changes to the TOE.

4.1.1.6 TOE Access

The MDM Server supports two GUI administrator interfaces that support two Administrator interfaces.

4.1.1.7 Trusted Path/Channels

The MDM Server uses TLS/HTTPS to create a secure communication channel between itself and remote administrators. It uses TLS to communicate with a syslog server. The MDM Server also uses TLS to connect with MD Users over a protected channel via their MDM Agent on their mobile device.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *Protection Profile for Mobile Device Management*, Version 4.0, 25 April 2019 [PP_MDM_V4.0]
- *PP-Module for MDM Agents*, Version 1.0, 25 April 2019 [MOD_MDM_AGENT_V1.0]
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March, 2019 [PKG_TLS_V1.1]

That information has not been reproduced here and the PP_MDM_V4.0/ MOD_MDM_AGENT_V1.0/PKG_TLS_V1.1 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/PKG_TLS_V1.1 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/ PKG_TLS_V1.1.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and applicable Technical Decisions. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- *Endpoint Manager Mobile (EPMM) System 12 Common Criteria Administrative Guidance*, version 1.3

Any additional customer documentation provided with the product or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 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 *Test Plan for Ivanti Endpoint Manager Mobile (EPMM) System 12*, version 1.2; *Test Plan for Ivanti Endpoint Manager Mobile (EPMM) Agent on Galaxy S22 Ultra Running Android 13*, version 1.1; and the *Test Plan for Ivanti Endpoint Manager Mobile (EPMM) Agent on Galaxy S23 Ultra Running Android 14*, version 1.1. The Assurance Activity Report (AAR) provides an overview of testing and the prescribed assurance activities.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the *Protection Profile for Mobile Device Management*, Version 4.0, 25 April 2019 [PP_MDM_V4.0], *PP-Module for MDM Agents*, Version 1.0, 25 April 2019 [MOD_MDM_AGENT_V1.0] and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March, 2019 [PKG_TLS_V1.1].

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is an MDM solution where the claimed security functions are implemented in a central MDM Server and distributed MDM Agents. The EPMM MDM Server integrates with backend enterprise IT systems and enables IT to define security and management policies for mobile apps.

The MDM Server is a software application that runs on an Intel x64 architecture server platform as a virtual system with Oracle Linux as the operating system (OS).

The MDM Server provides two administrative interfaces, each used for specific administrative actions. The Admin Portal provides capabilities for administrators to manage users, devices, policies and mobile device configurations. The System Manager provides administrative functions to control and configure the operation of the MDM Server including basic system configuration information (e.g., network addresses, date/time, hostname, e-mail settings), TOE updates, certificate management, TLS configuration, and export of various operational logs.

The MDM Agent, an application running on Galaxy S22 and S23 running Android 13 and 14 respectively, is an Android application. The MDM Agents work with the MDM Server to configure corporate email, Wi-Fi, VPN, and X.509 security certificates and to create a clear separation between personal and business information. Once installed, the MDM Agent creates a secure EPMM container that protects enterprise data and applications. This allows an MDM Server Administrator to selectively wipe only the enterprise data on the device if the user leaves or if the device falls out of compliance or is lost.

8.1.1 Physical Boundary

8.1.1.1 Physical Boundary and the Operational Environment

The TOE is a distributed TOE that includes two software builds, EPMM MDM Server and EPMM MDM Agent (MDMPP Client). The builds include software libraries that include the cryptographic libraries; the HTTP Server library that provides the Graphical User Interface (GUI) as well as other off-the-shelf (OTS) libraries. Each TOE component runs on an operating system provided by the Operational Environment (OE) and accesses the OE libraries by the well known APIs.

The MDM Server software build includes two cryptographic libraries: Ivanti MDM OpenSSL Component and Ivanti MDM Bouncy Castle. Both libraries are CAVP certified and described in detail in Section **Error! Reference source not found.** of the ST. As depicted in the figures below, the Ivanti MDM OpenSSL Component cryptographic library is used to support the two administrator interfaces, Admin Portal and System Manager; communicate with the Audit Server; and provides the communication channels to the MDM Agents. The MDM Bouncy Castle cryptographic library is used as an initial connection to the Audit Server and supports data at rest, encrypting X.509 certificates stored in flat files.

The MDM Client software build includes one cryptographic library Ivanti MDM Android Client OpenSSL Component that is CAVP certified and described in detail in Section **Error! Reference**

source not found. of the ST. Ivanti MDM Android Client OpenSSL Component provides the cryptographic function used for the communication channels to the MDM Server. The TOE relies on the Android device's Operational Environment's cryptographic library, Samsung BoringSSL Android 1.7 and Samsung BoringSSL Android 1.8 for Android 13 and Android 14 respectively, to encrypt data stored in Android's Truststore, provided by the OE.

The following two figures depict the two TOE components in their operational environment. They provide a rough diagram of the software TOE and identify the security enforcing software modules. The TOE is depicted in turquoise (hash and solid). The figures include a capital letter identifying each of the communication paths.

Figure 1: The TOE and the MDM Server's Operational Environment

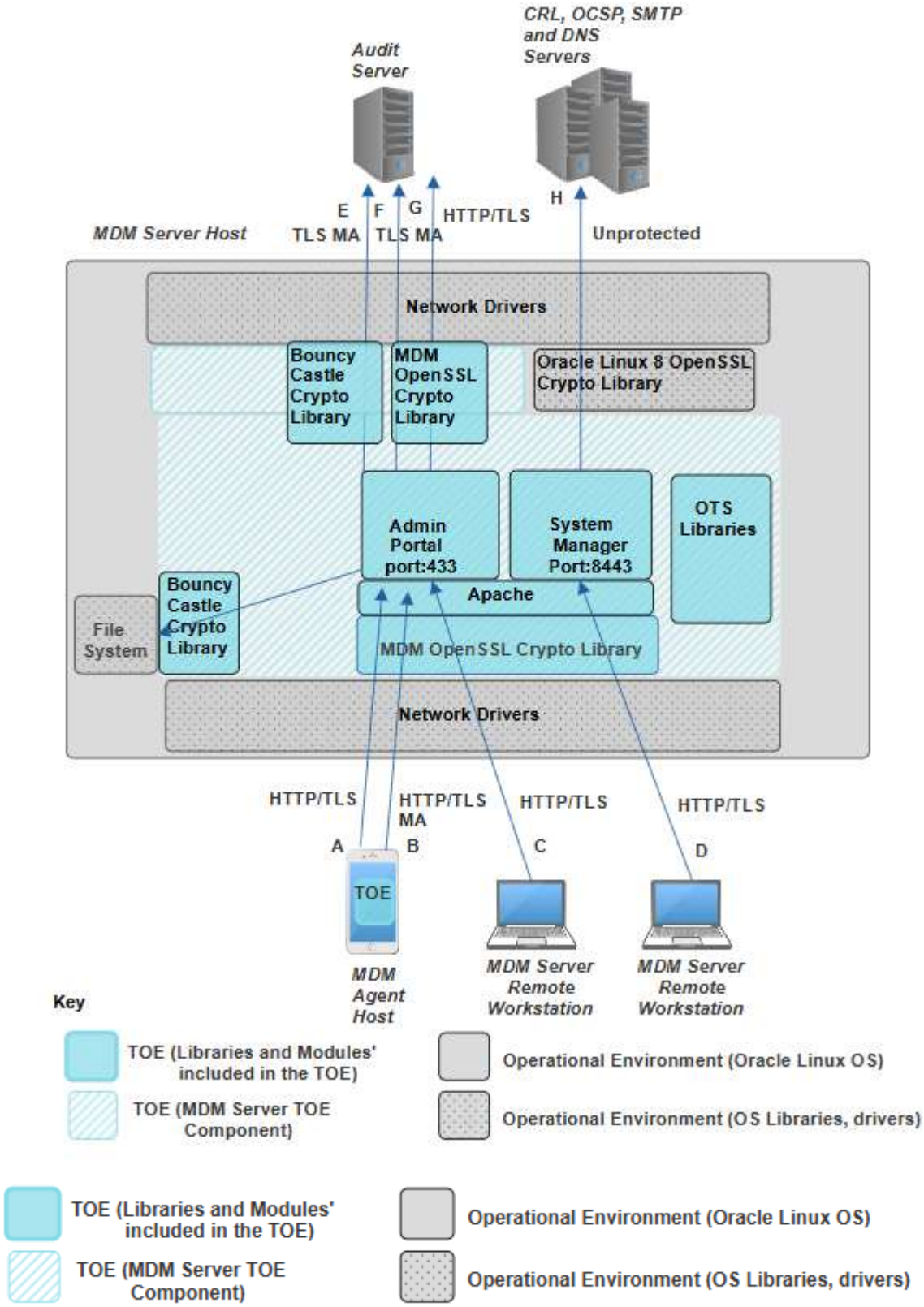
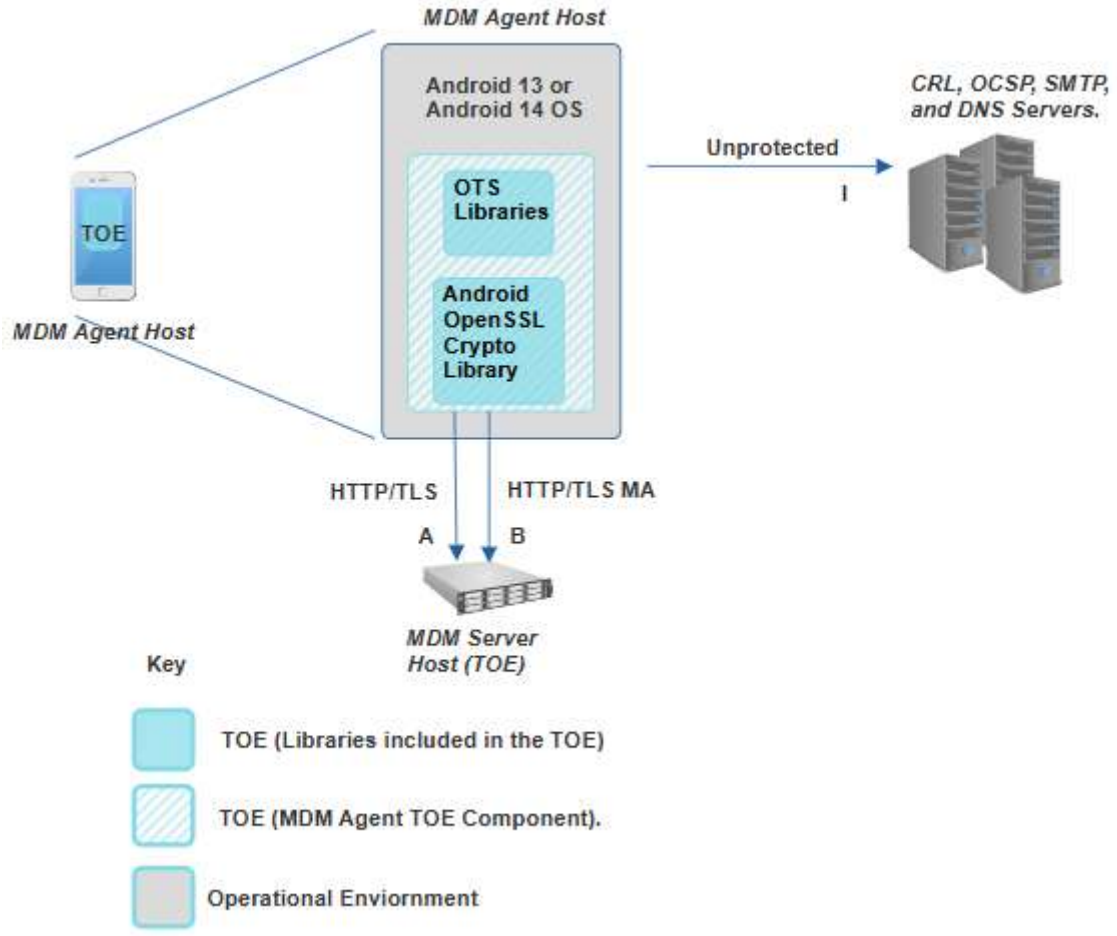


Figure 2: The TOE and the MDM Agent's Operational Environment



The following table identifies the servers, workstations, and hardware required for the EPMM MDM Server and MDM Agent components of the TOE.

Table 1: The Ivanti EPMM Device/Host/Server Operational Environment

Components	Mandatory /Optional	TOE Components	Description
CRL Servers	Mandatory	Both	A Certificate Revocation List (CRL) Server used to validate X.509 certificates. Communication is via an unprotected channel.
DNS Server(s)	Mandatory	Both	A Domain Name System (DNS) Server used to resolve Fully Qualified Domain Names (FQDNs) to IP addresses for certificate validation. A DNS Server is required in both

Components	Mandatory /Optional	TOE Components	Description
			TOE environments. The TOE components communicate with DNS Servers on an unprotected path.
MDM Agent Host	Mandatory	MDM Agent	The device hosting the MDM Agent component of the TOE. The host is a Galaxy S22 Ultra 5G device running Android 13 OS or a Galaxy S23 Ultra 5G device running Android 14 OS. The MDM Agent software component of the TOE must be installed on the host and configured in the CC evaluated configuration. Refer to Section 8.1.1.3 for specific details of the MDM Agent Host.
MDM Server Host	Mandatory	MDM Server	The device hosting the MDM Server software component of the TOE. The host is a Dell PowerEdge R640 Server with hypervisor VMware ESXi 7.02 running Oracle Linux 8.9 Operating System. The MDM Server software component of the TOE must be installed on the host and configured in the CC evaluated configuration. Refer to Section 8.1.1.2 for specific details of the MDM Server Host.
MDM Server Remote Workstation(s)	Mandatory	MDM Server	The MDM Server component of the TOE supports two GUI interfaces that enable Administrators to manage and monitor the TOE. Administrators access these interfaces via remote workstations using HTTP over TLS (HTTPS). The OE requires one or more remote workstations connecting to the MDM Server's Admin Portal administrator interface and the MDM Server's System Manager administrator interface.
OCSP Servers	Mandatory	Both	An Online Certificate Status Protocol (OCSP) Server used to validate X.509 certificates. Communication is via an unprotected channel.
SMTP Server	Mandatory	Both	The MDM Server supports sending Alerts if a specific event occurs. One type of Alerts is an email message. Therefore, both TOE components must have access to a Simple Mail Transfer Protocol Server (SMTP). Communication is via an unprotected channel.

Components	Mandatory /Optional	TOE Components	Description
Audit Server	Mandatory	MDM Server	An Audit Server is required by the MDM Server to enable the MDM Server to transfer audit Events. Communication is via mutual authenticated TLS. The Audit Server must support Syslog and HTTPS.

8.1.1.2 The MDM Server Details

The MDM Server runs on a virtual system and is described in the following tables.

Table 2: MDM Server Hardware Detail (Operational Environment)

Model	Processor	GHz	Hypervisor
Dell PowerEdge R640 Server	Intel(R) Xeon(R) Gold 5215 CPU (Cascade Lake)	2.10Ghz	VMware ESXi 7.02

Table 3: MDM Server Software Detail (Operational Environment)

Item	Software
Operating System	Oracle Linux 8.9
Runtime Environment	Java SE Run Java SE Runtime Environment v8 (1.8) on Oracle Linux 8.9
Hypervisor	VMWare ESXi 7.02
Kernel	Red Hat Compatible Kernel (RHCK) kernel package kernel-4.18.0-80.el8

The MDM Server, Ivanti Endpoint Manager Mobile (Core), can be downloaded by customers from https://forums.ivanti.com/s/contactsupport?language=en_US and installed on compliant hardware listed above. Licenses are provided by Ivanti Secure via email. When a customer request is received, Ivanti will provide an authcode via email. Customers must register in https://forums.ivanti.com/s/contactsupport?language=en_US portal and generate the license string by providing Hardware id with earlier provided authcode. These auth codes are not reusable.

Table 4: The MDM Server TOE Component Build

Build Name	Cryptographic Libraries included in the Build	CAVP #	Other Libraries included in the Build
EPMM 12.3.1.0 Build 84	Ivanti MDM Bouncy Castle 1.0.2.4	#A6073	Apache 2.4
	Ivanti MDM OpenSSL Component 1.1.1g	#A6074	OTS Libraries identified in Appendex B

Refer to Section **Error! Reference source not found.** in the ST for complete information about the CAVP certified cryptographic libraries included in the TOE.

8.1.1.3 The MDM Agent Details

The MDM Agent consists of a software application deployed on one of two Android mobile devices.

Galaxy S22 Ultra 5G Android 13

Samsung Electronics Co., Ltd.

Galaxy S23 Ultra 5G Android 14

Samsung Electronics Co., Ltd.

The following tables include the Android device details.

Table 5: MDM Agent Host Hardware Detail (Operational Environment)

Manufacturer	Device Name	Models	Chipset Vendor	SoC	Microarchitecture
Samsung	Galaxy S22 Ultra 5G	SM-S908B, SM-S908B/DS, SM-S908U, SM-S908U1, SM-S908W, SM-S908N, SM-S9080, SM-S908E, SM-S908E/DS	Samsung	Exynos 2200 (AMD RDNA™ 3)	ARMv8
Samsung	Galaxy S23 Ultra 5G	SM-S918B, SM-S918B/DS, SM-S918U, SM-S918U1, SM-S918W, SM-S918N, SM-S9180, SM-S918E, SM-S918E/DS	Qualcomm	Snapdragon 8 Gen 2 Mobile Platform	ARMv8

The MDM Agent is obtained from Ivanti personnel and is referred to as the Federal Build (vs. the commercial build).

Table 6: The MDM Agent TOE Component Build

Build Name	Cryptographic Library included in the Build	CAVP #	Other Libraries included in the Build
MDMPP-MIClient-12.5.1.0.s	Ivanti MDM Android Client OpenSSL Component 2.2.1	#6402	Apache
			OTS Libraries identified in **Error! Reference source not found.**

Refer to Section **Error! Reference source not found.** of the ST for complete information about the CAVP certified cryptographic libraries included in the TOE.

8.2 Excluded Functionality

- Ivanti Sentry is not included in the evaluation.
- The evaluated configuration does not include the CLI interface referred to as the Ivanti Self-Service User Portal user interface.
- The EPMM evaluation does not include the Non-admin and Guest roles supported by Android devices.
- The EPMM evaluated configuration does not support connecting to the MDM Server using the SSH network protocol. SSH, also known as Secure Shell or Secure Socket Shell, provides a CLI.
- The EPMM Agent that was evaluated is the Federal Build and is acquired through Ivanti personnel. It is not the Ivanti commercial EPMM Agent, also known as mobile@work, available via Google Play and the Ivanti website.
- The Trusted Front End (TFE) functionality is not included in the evaluated configuration.
- SAML is not enabled in the CC evaluated configuration.
- ActiveSync is not enabled in the evaluated configuration.

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 documents: the Detailed Test Reports (DTRs) and the ETR. The reader of this document can assume that all 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 team determined the TOE Name to be Part 2 extended, and meets the SARs contained in the claimed PPs. Additionally, the evaluator performed the Assurance Activities specified in the claimed PPs.

9.1 Evaluation of Security Target

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 Ivanti Endpoint Manager Mobile (EPMM) System 12 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/ PKG_TLS_V1.1.

The validation team 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 Development Documentation

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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/PKG_TLS_V1.1 related to the examination of the information contained in the TOE Summary Specification.

The validation team 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.

9.3 Evaluation of Guidance Documents

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 Assurance Activities specified PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/PKG_TLS_V1.1 related to the examination of the information contained in the operational guidance documents.

The validation team 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.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team 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 Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/ PKG_TLS_V1.1 and recorded the results in a Test Report, summarized in the ETR and AAR.

The validation team 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 PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/PKG_TLS_V1.1 and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Vulnerability Assessment document prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluation team searched the National Vulnerability Database (https://nvd.nist.gov/vuln/search#/nvd/home?resultType=records), the Ivanti website (https://www.ivanti.com/), and the CVE site (https://www.cve.org/) on 10/13/2025 with the following search terms:

- Ivanti Endpoint Manager Mobile (EPMM) 12
- Ivanti, Inc.
- Oracle Linux 8.9

- Mobile Device Management
- Mobile Management Software
- MDM Server
- MDM Agent
- Galaxy S22 Ultra 5G Android 13
- Galaxy S22 Ultra 5G Android 14
- Mobile@Work
- EPMM 12.3.1.0
- Ivanti MDM OpenSSL Component 1.1.1g
- Ivanti MDM Bouncy Castle v1.0.2.4
- Ivanti Apache 2.4
- TLS/SSL MDM
- Remote Wipe MDM
- MDM enrollment vulnerability
- MDM privilege escalation

The validation team 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.

9.7 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 followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Endpoint Manager Mobile (EPMM) System 12 Common Criteria Administrative Guidance*, version 1.3. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the PP_MDM_V4.0/MOD_MDM_AGENT_V1.0/ PKG_TLS_V1.1 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: *Ivanti Endpoint Manager Mobile (EPMM) System 12 Security Target*, version 3.5.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

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, 25 April 2019 [PP_MDM_V4.0]
6. *PP-Module for MDM Agents*, Version 1.0, 25 April 2019 [MOD_MDM_AGENT_V1.0]
7. *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March, 2019 [PKG_TLS_V1.1].
8. *Ivanti Endpoint Manager Mobile (EPMM) System 12 Security Target*, version 3.5.
9. *Endpoint Manager Mobile (EPMM) System 12 Common Criteria Administrative Guidance*, version 1.5.
10. *Evaluation Technical Report for Ivanti Endpoint Manager Mobile (EPMM) System 12*, version 1.2.
11. *Test Plan for Endpoint Manager Mobile (EPMM) System 12*, version 1.2.
12. *Test Plan for Ivanti Endpoint Manager Mobile (EPMM) Agent on Galaxy S22 Ultra Running Android 13*, version 1.1.
13. *Test Plan for Ivanti Endpoint Manager Mobile (EPMM) Agent on Galaxy S23 Ultra Running Android 14*, version 1.1.
14. *Assurance Activity Report for Ivanti Endpoint Manager Mobile (EPMM) System 12*, version 0.4.
15. *Vulnerability Assessment for Ivanti Endpoint Manager Mobile (EPMM) 12*, version 1.1.