Assurance Activities Report for a Target of Evaluation

GovShield Version 1.60.05

Assurance Activities Report (AAR) Version 1.0

05/27/2026

Security Target (Version 1.0)

Evaluated by:

Booz | Allen | Hamilton

Booz Allen Hamilton Common Criteria Test Laboratory
NIAP Lab # 200423
1100 West St.
Laurel, MD 20707

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
General Dynamics Mission Systems
9500 Innovation Drive
Manassas, VA 20110

The Author of the Security Target:
Booz Allen Hamilton
1100 West St.
Laurel, 20707 USA

The TOE Evaluation was sponsored by:
Booz Allen Hamilton

Evaluation Personnel:
Herbert Markle

Applicable Common Criteria Version

Common Criteria for Information Technology Security Evaluation, April 2017 Version 3.1 Revision 5

Common Evaluation Methodology Version

Common Criteria for Information Technology Security Evaluation, Evaluation Methodology, April 2017 Version 3.1 Revision 5

Table of Contents

1 Purpose

The purpose of this document is to serve as a non-proprietary attestation that this evaluation has satisfied all the TSS, AGD, and ATE Assurance Activities required by the Protection Profiles/Extended Packages to which the TOE claims exact conformance. This will give system integrators valuable information about product configuration and testing, help to align Common Criteria evaluations with DISA Security Requirements Guides and Security Test Implementation Guides (SRGs/STIGs), and thereby streamline the process for U.S. Government procurement of validated products.

2 TOE Summary Specification Assurance Activities

The evaluation team completed the testing of the Security Target (ST) *GovShield Version 1.60.05 Security Target v1.0, February 6, 2026* and confirmed that the TOE Summary Specification (TSS) contains all Assurance Activities as specified by the *Protection Profile for Mobile Device Management Version 4.0, April 25, 2019 [MDMPP]* and *PP-Module for MDM Agent Version 1.0, April 25, 2019 [AGENTMOD]*. The evaluators were able to individually examine each SFR's TSS statements and determine that they comprised sufficient information to address each SFR claimed by the TOE as well as meet the expectations of the MDMPP and AGENTMOD Assurance Activities.

Through the evaluation of ASE_TSS.1-1, described in the ETR, the evaluators were able to determine that each SFR was described in enough detail to demonstrate that the TSF addresses the SFR. However, in some cases the Assurance Activities that are specified in the claimed source material instruct the evaluator to examine the TSS for a description of specific behavior to ensure that each SFR is described to an appropriate level of detail. The following is a list of each SFR, the TSS Assurance Activities specified for the SFR, and how the TSS meets the Assurance Activities. Additionally, each SFR is accompanied by the source material MDMPP and AGENTMOD that defines where the most up-to-date TSS Assurance Activity was defined.

[MDMPP] FAU_ALT_EXT.1 – *"The evaluator shall examine the TSS and verify that it describes how the alert system is implemented. The evaluator shall also verify that a description of each assigned event is provided in the TSS."*

Section 8.1.1 of the ST describes that alerts are generated based on information provided by the GovShield Client during a reachability event to the GovShield Server, and the alerts are viewable by administrators in the web GUI. The section also describes all five types of alert events that are claimed by the TOE.

[AGENTMOD] FAU_ALT_EXT.2 – *"The evaluator shall examine the TSS and verify that it describes how the alerts are implemented.*

The evaluator shall examine the TSS and verify that it describes how the candidate policy updates are obtained and the actions that take place for successful (policy update installed) and unsuccessful (policy update not installed) cases. The software components that are performing the processing must also be identified in the TSS and verified by the evaluator.

The evaluator also ensures that the TSS describes how reachability events are implemented, and if configurable are selected in FMT_SMF_EXT.4.2. The evaluator verifies that this description clearly indicates who (MDM Agent or MDM Server) initiates reachability events

The evaluator shall ensure that the TSS describes under what circumstances, if any, the alert may not be generated (e.g., the device is powered off or disconnected from the trusted channel), how alerts are queued, and the maximum amount of storage for queued messages."

Section 8.1.2 of the ST describes that alerts are generated based on information provided by the GovShield Client during a reachability event to the GovShield Server. Reachability events happen due to

enrollment/unenrollment or due to polling intervals being triggered on from the GovShield Client. GovShield Client initiates the reachability events but does so based upon its configuration which can be set by an administrator through the GovShield Server.

Section 8.5.5 of the ST describes that the GovShield Client obtains policy updates from the GovShield Server as part of reachability events, and that only properly signed policies will be applied by GovShield Client. The GovShield Client relies on its platform to verify the signature. The TSS is clear on which software component performs each part of the policy update process.

Section 8.1.2 of the ST describes that alerts are only created based upon a connection between the GovShield Client and GovShield Server. Thus, when a connection isn't established the GovShield Client will continue to collect data for alerts per its configured polling intervals, and will send this upon the next established connection to the GovShield Server. The maximum amount of storage is dependent on mobile device storage limits.

[MDMPP] FAU_GEN.1.1(1) – *"The evaluator shall check the TSS and ensure that it lists all of the auditable events. The evaluator shall check to make sure that every audit event type mandated by the PP is described in the TSS. The evaluator shall verify that for every audit event described in the TSS, the description indicates where the audit event is generated (TSF, TOE platform).*

If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

Section 8.1.3 of the ST lists in Table 16 all of the auditable events, including every audit event type mandated by the PP. It also describes for each audit event described, the component generating the record, and a note describing how it is invoked, if invoked by the platform.

[MDMPP] FAU_GEN.1.2(1) – *"The evaluator shall check the TSS and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field."*

Section 8.1.3 of the ST provides an example audit record to illustrate the standard format for TSF audit records. As shown in the example, each audit record contains Device ID (if applicable), Server Name, Event Type, Success/Failure, Date and Time, Subject Identity, and Additional Information.

[MDMPP] FAU_GEN.1.1(2) – "*The evaluator shall check the TSS and ensure that it provides a format for audit records."*

Section 8.1.4 of the ST provides an example audit record to illustrate the standard format for the MAS Server audit records. As shown in the example, each audit record contains Device ID (if applicable), Server Name, Event Type, Success/Failure, Date and Time, Subject Identity, and Additional Information.

[MDMPP] FAU_GEN.1.2(2) – *"The evaluator shall check the TSS and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field."*

Section 8.1.4 of the ST provides an example audit record to illustrate the standard format for the MAS Server audit records. As shown in the example, each audit record contains Device ID (if applicable), Server Name, Event Type, Success/Failure, Date and Time, Subject Identity, and Additional Information.

[AGENTMOD] FAU_GEN.1(2) – *"The evaluator shall check the TSS and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field.*

If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Agent; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

Section 8.1.5 of the ST provides an example audit record to illustrate the standard format for TSF audit records. As shown in the example, each audit record contains Date and Timestamp, identifies the Device ID as part of subject identity, Username as part of subject identity, Server Name to which device is assigned, Message which is the Event Type and Success/Failure.

Section 8.1.5 of the ST lists (in table 17) all of the auditable events, including every audit event type mandated by the PP. It also describes for each audit event described, the component generating the record, and a note describing how it is invoked, if invoked by the platform.

[MDMPP] FAU_NET_EXT.1 – *"The evaluator ensures that the TSS describes how reachability events are implemented, for each supported mobile platform. The evaluator verifies that this description clearly indicates who (MDM Agent or MDM Server) initiates reachability events."*

Sections 8.1.6 and 8.1.2 of the ST describe that reachability events happen due to enrollment/unenrollment or due to polling intervals being triggered on from the GovShield Client. GovShield Client initiates the reachability events but does so based upon its configuration which can be set by an administrator through the GovShield Server.

[MDMPP] FAU_SAR.1.1 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

The SFR selection is "implement functionality", therefore, this TSS Assurance Activity is not applicable.

[MDMPP] FAU_SAR.1.2 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

The SFR selection is "implement functionality", therefore, this TSS Assurance Activity is not applicable.

[AGENTMOD] FAU_SEL.1(2) – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS of the ST to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Agent; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

The SFR selection is "implement functionality", therefore, this TSS Assurance Activity is not applicable.

[MDMPP] FAU_STG_EXT.1 – *"The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided."*

Section 8.1.9 of the ST states that audit data will be transmitted in real time from the GovShield Server to a remote Oracle Database over a TLS v1.2. Section 8.8.2 of the ST states that the trusted channel is provided by the GovShield Server's underlying platform.

[MDMPP] FCO_CPC_EXT.1.1 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how the audit record*

protection functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).”

The SFR selection is “implement functionality”, therefore, this TSS Assurance Activity is not applicable.

[MDMPP] FCO_CPC_EXT.1.2 – *“If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how the audit record protection functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).”*

The “invoke platform-provided functionality” is selected as part of FCO_CPC_EXT.1.2; however, the audit record associated with FCO_CPC_EXT.1 is a management action that is performed on the GovShield Server which whitelists the mobile devices which can enroll into mobile device management. The selection for FCO_CPC_EXT.1.1 is “implement functionality” which aligns with the audit record purpose. Section 8.2.1 of the ST states that configuration of this enrollment restriction is the enablement step by the Authorized Administrator through the web GUI. Additionally, “Table 16: Auditable Events by Enforcing Component” in Section 8.1.3 of the ST confirms that the component which performs this audit record is the GovShield Server. Therefore, the evaluation team determined that "invoke platform-provided functionality" was properly selected due to FCO_CPC_EXT.1.2 discussing the handling of secure communications between a GovShield Client and the GovShield Server during enrollment which is handled by the TOE components' platforms. However, the audit record associated with this SFR is implemented by the TOE's GovShield Server component and would be considered “implement functionality”, which is selected under FCO_CPC_EXT.1.1. Since FCO_CPC_EXT.1.1 has selected “implement functionality”, the GovShield Server is invoking its own audit functionality to support the audit record related to this SFR.

[MDMPP] FCO_CPC_EXT.1.3 – *“If "invoke platform-provided functionality" is selected: The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the audit record protection functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).”*

The SFR selection is “implement functionality”, therefore, this TSS Assurance Activity is not applicable.

[MDMPP] FCS_CKM.1 – *If "invoke platform-provided functionality" is selected:*

“The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the key generation functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).”

If "implement functionality" is selected: The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.

The selection “invoke platform-provided functionality” has been included for this SFR. The selection “implement functionality” has not been included for this SFR; therefore, this portion of the TSS assurance activity does not apply.

Section 8.3.1 of the ST states that the GovShield Server invokes the underlying platform provided functionality for asymmetric key generation in support of HTTPS and TLS communications. The underlying platform provides functionality to support RSA schemes using cryptographic key sizes of 2048-bit or greater that meet FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.1 and ECC

schemes using “NIST curves” P-384 that meet FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Appendix B.4.

Section 8.3.1 of the ST states that the GovShield Client invokes the underlying platform for support of HTTPS communications. The underlying platform supports ECC schemes using “NIST curves” P-384 that meet FIPS_PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2

This adequately describes how the FCS_CKM.1.1 functionality is invoked.

[MDMPP] FCS_CKM.2 – *If "invoke platform-provided functionality" is selected:*

“The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the key establishment functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).”

If "implement functionality" is selected:

The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.

The evaluator shall ensure that the TSS describes how the TOE handles decryption errors. In accordance with NIST Special Publication 800-56B, the TOE must not reveal the particular error that occurred, either through the contents of any outputted or logged error message or through timing variations. If KTS-OAEP is supported, the evaluator shall create separate contrived ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.2.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each. If KTS-KEM-KWS is supported, the evaluator shall create separate contrived ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.3.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each.

If Diffie-Hellman group 14 is selected from FCS_CKM.2.1, the TSS shall describe how the implementation meets RFC 3526 Section 3.

The selection “invoke platform-provided functionality” has been included for this SFR. The selection “implement functionality” has not been included for this SFR; therefore, this portion of the TSS assurance activity does not apply.

Section 8.3.2 of the ST states that the GovShield Server invokes the underlying platform in support of two key establishment schemes for the establishment of HTTPS and TLS communications:

• RSA key establishment conforming to “RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017”, and
• Elliptic curve-based key establishment conforming to NIST Special Publication 800-56A.

Section 8.3.2 of the ST states that the GovShield Client invokes the underlying platform in support of the following key establishment scheme for the establishment of HTTPS communications:

• Elliptic curve-based key establishment conforming to NIST Special Publication 800-56A.

This adequately describes how the FCS_CKM.2.1 functionality is invoked.

[MDMPP] FCS_CKM_EXT.4.1 – *"If "invoking platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how the key destruction functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.3.3 of the ST states that the GovShield Server invokes the underlying platform's FIPS cryptographic module to destroy the keys and cryptographic security parameter data when no longer needed. The invoking of the destruction of keys stored in volatile memory occurs as a result of the GovShield Server making a cryptographic function call which requires a key and/or cryptographic security parameter data to be generated by the platform. The platform will destroy the reference to the key followed by a request for garbage collection when the generated cryptographic data is no longer needed. This occurs without requiring a separate function call to the platform by the GovShield Server. The invoking of the destruction of keys stored in non-volatile memory occurs as a result of the Authorized Administrator replacing the key within the Java KeyStore. The platform will destroy the key with a single direct overwrite with a new value of a key.

Section 8.3.3 of the ST states that the GovShield Client invokes the underlying mobile device platform to perform key destruction. The invoking of key destruction occurs as a result of the GovShield Client making a cryptographic function call which requires a key and/or cryptographic security parameter data to be generated by its platform. The platform will therefore perform key destruction when the generated cryptographic data is no longer needed, without requiring a separate function call for key destruction from the GovShield Client. Key data maintained by the GovShield Client platform in volatile memory are erased by a one-pass overwrite with zeroes. Key data maintained by the GovShield Client's platform in non-volatile memory is stored in flash memory and is erased by a one-pass overwrite with zeroes.

This adequately describes how the FCS_CKM_EXT.4.1 functionality is invoked.

[MDMPP] FCS_CKM_EXT.4.2 – *"The evaluator shall check to ensure the TSS lists each type of plaintext key material and CSP (authentication data, authorization data, secret/private symmetric keys, data used to derive keys, etc.) and its origin and storage location.*

The evaluator shall verify that the TSS describes when each type of key material and CSP is no longer needed.

If "invoke platform-provided functionality" is selected:

The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the key releasing functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

If "implement functionality" is selected:

The evaluator shall also verify that, for each type, the type of clearing procedure that is performed is listed. If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the clearing procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are cleared by overwriting once with zeros, while secret keys stored on the internal persistent storage device are cleared by overwriting one time with a random pattern that is changed before each write"). For block erases, the evaluator shall also ensure that the block erase command used is listed and shall verify that the command used also addresses any copies of the plaintext key material that may be created in order to optimize the use of flash memory."

The selection “invoke platform-provided functionality” has been included for this SFR. The selection “implement functionality” has not been included for this SFR; therefore, this portion of the TSS assurance activity does not apply.

Section 8.3.9 of the ST lists each secret in relation to the GovShield Server in Table 18. For each key, the purpose, the origin, and the storage location are described. All persistent keys are stored in the encrypted Java KeyStore, all non-persistent keys are stored in volatile memory, and all user credentials are stored in authentication repositories.

Section 8.3.3 of the ST states that the GovShield Server invokes the underlying platform’s FIPS cryptographic module to destroy the keys and cryptographic security parameter data when no longer needed. The invoking of the destruction of keys stored in volatile memory occurs as a result of the GovShield Server making a cryptographic function call which requires a key and/or cryptographic security parameter data to be generated by the platform. The platform will destroy the reference to the key followed by a request for garbage collection when the generated cryptographic data is no longer needed. This occurs without requiring a separate function call to the platform by the GovShield Server. The invoking of the destruction of keys stored in non-volatile memory occurs as a result of the Authorized Administrator replacing the key within the Java KeyStore. The platform will destroy the key with a single direct overwrite with a new value of a key.

Section 8.3.10 of the ST lists each secret in relation to the GovShield Client in Table 19. For each key, the purpose, the origin, and the storage location are described. All persistent keys are stored in the encrypted Android Keystore, and all non-persistent keys are stored in volatile memory.

Section 8.3.3 of the ST states that the GovShield Client invokes the underlying mobile device platform to perform key destruction. The invoking of key destruction occurs as a result of the GovShield Client making a cryptographic function call which requires a key and/or cryptographic security parameter data to be generated by its platform. The platform will therefore perform key destruction when the generated cryptographic data is no longer needed, without requiring a separate function call for key destruction from the GovShield Client. Key data maintained by the GovShield Client platform in volatile memory are erased by a one-pass overwrite with zeroes. Key data maintained by the GovShield Client’s platform in non-volatile memory is stored in flash memory and is erased by a one-pass overwrite with zeroes.

[MDMPP] FCS_COP.1(1) – *If "invoke platform-provided functionality" is selected:*

“The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the encryption/decryption functionality is invoked for each mode and key size selected in the MDM Server's ST (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).”

Section 8.3.4 of the ST states that the GovShield Server invokes the underlying platform to perform AES encryption/decryption services for HTTPS and TLS communications. Data in transit is protected using GCM mode and either 128-bit or 256-bit keys, which is conformant to NIST SP 800-38D.

Section 8.3.4 of the ST states that the GovShield Client invokes the underlying mobile device platform to perform AES encryption/decryption services for HTTPS communications. The platform uses GCM mode and 128-bit keys, which is conformant to NIST SP 800-38D.

This adequately describes how the FCS_COP.1.1(1) functionality is invoked.

[MDMPP] FCS_COP.1(2) – *If "invoke platform-provided functionality" is selected:*

“The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the hash functionality is invoked for each digest size selected in the MDM Server's ST (it should be noted that this

may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).

If "implement functionality" is selected:

The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS. The evaluator checks the AGD documents to determine that any configuration that is required to be done to configure the functionality for the required hash sizes is present. The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented testmacs."

Section 8.3.5 of the ST states that the GovShield Server invokes the platform to provide SHA-256 and SHA-384 cryptographic hashing services, conformant to FIPS PUB 180-4, with digest sizes of 256 and 384 bits, respectively. SHA-256 and SHA-384 are used by HMAC in message authentication in support of TLS and HTTPS communication. SHA-256 in support of ECDSA with P-256 curves used for digital signature services in support of HTTPS communication. SHA-256 is used for the digital signing of policies (ECDSA with P-256 curve).

Section 8.3.5 of the ST also states that the GovShield Client invokes the platform to provide SHA-256 cryptographic hashing services, conformant to FIPS PUB 180-4, with digest sizes of 256 bits. SHA-256 is used by HMAC in message authentication in support of HTTPS communication. SHA-256 in support of ECDSA with P-256 curves used for digital signature services in support of HTTPS communication. SHA-256 is used for the digital signing of policies (ECDSA with P-256 curve).

The SFR selection does not include "implement functionality", therefore, this part of the TSS Assurance Activity is not applicable.

[MDMPP] FCS_COP.1(3) – *If "invoke platform-provided functionality" is selected:*

"The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the digital signature functionality is invoked for each operation they are used for in the MDM Server (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

Section 8.3.6 of the ST states that the GovShield Server invokes underlying platform to provide all digital signature services in accordance with FIPS PUB 186-5. RSA with 2048-bit keys is used for policy signature generation, and digital signature services in support of HTTPS and TLS communication.

Section 8.3.6 of the ST also states that the GovShield Client invokes the underlying mobile device platform to provide digital signature services in accordance with FIPS PUB 186-5. RSA with 2048-bit keys is used for policy signature verification functionality, and digital signature services in support of HTTPS communication.

[MDMPP] FCS_COP.1(4) – *If "invoke platform-provided functionality" is selected:*

"The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the keyed-hash functionality is invoked for each mode and key size selected in the MDM Server's ST (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

If "implement functionality" is selected:

The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

Section 8.3.7 of the ST states that the GovShield Server invokes the platform to provide keyed-hash message authentication services conformant to FIPS PUBs 180-4 and 198-1. HMAC-SHA-256 and HMAC-SHA-384 are used to perform keyed-hash message authentication, with respective digest sizes of 256 and 384 bits in support of trusted communication.

Section 8.3.7 of the ST also states that the GovShield Client invokes the underlying mobile device platform to provide keyed-hash message authentication services conformant to FIPS PUBs 180-4 and 198-1. HMAC-SHA-256 is used to perform keyed-hash message authentication, with respective digest sizes of 256 bits in support of trusted communication.

The SFR selection does not include “implement functionality”, therefore, this part of the TSS Assurance Activity is not applicable.

[MDMPP] FCS_RBG_EXT.1.1 – *If "invoke platform-provided functionality" is selected:*

“The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the RBG functionality is invoked for each operation they are used for in the MDM Server (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).”

Section 8.3.8 of the ST states that the GovShield Server invokes the Java Runtime Environment Platform to provide random bit generation services. The underlying platform’s cryptographic module provides an AES counter DRBG (CTR_DRBG) that conforms to NIST SP 800-90A. In order to provide sufficient randomness to the keys generated by this DRBG (as specified in NIST SP 800-57), the DRBG is seeded with at least 256 bits of entropy which is gathered from a platform based RBG.

Section 8.3.8 of the ST states that the GovShield Client invokes the underlying mobile device platform to provide random bit generation services. The Android platform provides an AES counter DRBG (CTR_DRBG) that conforms to NIST SP 800-90A. In order to provide sufficient randomness to the keys generated by this DRBG (as specified in NIST SP 800-57), the DRBG is seeded with at least 256 bits of entropy from the platform’s hardware-based noise source.

Section 8.3.8 also states: “Note: The GovShield Server and GovShield Client software do not directly invoke their respective platforms’ deterministic random bit generator. Instead, the TOE’s software indirectly invokes their platforms’ deterministic random bit generator by directly invoking platform components, which in turn directly invoke the deterministic random bit generator.”

This adequately describes how the FCS_RBG_EXT.1.1 functionality is invoked.

[MDMPP] FCS_RBG_EXT.1.2 – *“Documentation shall be produced-and the evaluator shall perform the activities-in accordance with Appendix D: Entropy Documentation and Assessment and the "Clarification to the Entropy Documentation and Assessment Annex."*

In the future, specific statistical testing (in line with NIST SP 800-90B) will be required to verify the entropy estimates.”

Through TRRT (TQ1754), it was determined that the Assurance Activities for FCS_RBG_EXT.1.2 are conditional and only applicable when the TOE implements the DRBG functionality. The GovShield Server and GovShield Client invoke the platform-provided DRBG functionality and thus, this TSS Assurance Activity is satisfied due to not being required for this TOE.

[MDMPP] FCS_STG_EXT.1 – *"Regardless of whether this requirement is met by the TSF or the TOE platform, the evaluator will check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and how it is stored. The evaluator then performs the following actions.*

Persistent secrets and private keys manipulated by the TOE platform:

The evaluator shall examine the TSS to verify that it describes (for each supported platform) how the key storage functionality is invoked for each persistent secret and private key described in the TSS (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).

Persistent secrets and private keys manipulated by the TSF:

The evaluator reviews the TSS to determine that it makes a case that, for each item listed as being manipulated by the TOE, it is not written unencrypted to persistent memory, and that the item is stored by the platform."

Section 8.3.9 of the ST lists each persistent secret in relation to the GovShield Server in Table 18. For each key, the purpose, the origin, and the storage location are described. The TOE's Java Runtime Environment Platform is responsible for storing keys and relies on the BSafe cryptographic library to invoke the storage of persistent secrets and private keys which are produced through their operation. All persistent private keys are stored in the encrypted Java KeyStore/TrustStore and all user credentials are stored in authentication repositories. The X.509v3 certificate for policy signing is generated by the CA Server and loaded into the Java KeyStore after a request is made by the Authorized Administrator through the TOE. The X.509v3 certificates used for HTTPS and TLS are created by the CA Server, and loaded into the encrypted Java KeyStore/TrustStore by an Authorized Administrator through the underlying platform's interface.

There are no persistent secrets and private keys manipulated by the TSF as all persistent secrets and private keys are handled by the platform.

[AGENTMOD] FCS_STG_EXT.1(2) – *"The evaluator will verify that the TSS lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and, for each platform listed as supported in the ST, how it is stored. The evaluator shall verify that the Agent calls a platform-provided API to store persistent secrets and private keys."*

Section 8.3.10 of the ST lists each persistent secret in relation to the GovShield Client in Table 19. For each key, the purpose, the origin, and the storage location are described. All the GovShield Client's keys are stored in the encrypted Android Keystore/TrustStore of the device. The GovShield Client relies on its platform's BoringSSL to invoke the storage of persistent secrets and private keys which are produced through their operation. This cryptographic module is invoked by the platform APIs available to the GovShield Client when requesting an encryption function as assessed under FPT_API_EXT.1.

[MDMPP] FIA_ENR_EXT.1.1 – *"The evaluator shall examine the TSS and verify that it describes the process of enrollment for each MDM Agent/platform listed as supported in the ST. This description shall include the trusted path used for enrollment (FTP_TRP.1(2)), the method of user authentication (username/password, token, etc.), the method of authentication decision (local or remote authentication services), and the actions performed on the MDM Server upon successful authentication."*

Section 8.4.1 of the ST describes the process used by a MD user or Administrator to enroll a new GovShield Client. The description details the process that must be carried out for the GovShield Client to make initial contact with the GovShield Server, which results in the download of the GovShield Client

software onto the mobile device. The GovShield Client requires the MD user of Administrator to enter in username and password credentials. This initiates the HTTPS/TLS trusted path used for enrollment. The GovShield Server will validate the username and password against the user table in the non-TOE remote Oracle Database. The GovShield Server then requests the GovShield Client to provide the Android Mobile Device's Android Device ID to verify against the whitelist. If authentication and whitelisting are successful, enrollment continues with GovShield Server issuing an X.509v3 and the initial policy payload to the GovShield Client.

[MDMPP] FIA_ENR_EXT.1.2 – *"The evaluator shall examine the TSS and verify that it implements a policy to limit the user's enrollment of devices."*

Section 8.4.1 of the ST describes that the only devices with a whitelisted Android Device ID are allowed to enroll with the GovShield Server. When devices with a non-whitelisted Android Device ID attempt to enroll, the enrollment process is automatically stopped.

[AGENTMOD] FIA_ENR_EXT.2 – *"The evaluator shall examine the TSS to verify that it describes which types of reference identifiers are acceptable and how the identifier is specified (e.g. preconfigured in the MDM Agent, by the user, by the MDM server, in a policy)."*

Section 8.4.2 of the ST describes how the URL for the GovShield Server serves as the reference identifier for all subsequent communications between the GovShield Client and GovShield Server. The GovShield Server URL is embedded into the QR code used for the enrollment process and is recorded as the GovShield Server's reference identifier once successful enrollment occurs.

[MDMPP] FIA_UAU.1.1 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

The SFR selection is "implement functionality", therefore, this TSS Assurance Activity is not applicable.

[MDMPP] FIA_UAU.1.2 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

The SFR selection is "implement functionality", therefore, this TSS Assurance Activity is not applicable.

[MDMPP] FIA_X509_EXT.1.1(1) – TD0641*"If invoke platform-provided functionality is selected:*

The evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity.)

The TSS must describe when revocation checking is performed. It is expected that revocation checking is performed when a certificate is used in an authentication step. It is not sufficient to verify the status of an X.509 certificate only when it is loaded onto the device.

If implement functionality is selected:

The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place. The evaluator ensures the TSS also provides a description of the certificate path validation algorithm.

The TSS must describe when revocation checking is performed. It is expected that revocation checking is performed when a certificate is used in an authentication step. It is not sufficient to verify the status of an X.509 certificate only when it is loaded onto the device.

The SFR selection is "invoke platform-provided functionality", therefore, this portion of the TSS Assurance Activity is applicable. The SFR selection is "implement functionality" was not claimed, therefore, this portion of the TSS Assurance Activity is not applicable.

Section 8.4.4 of the ST states that the underlying platform is invoked by the GovShield Server to provide X.509v3 certificate services for signing policies that are sent to the GovShield Clients and for TLS and HTTPS/TLS session establishment when operating as both a client and server for the respective protocol. Additionally, the GovShield Client invokes its underlying platform to provide X.509v3 certificate services for signature verification for signed policies sent from the GovShield Server, and in support of HTTPS/TLS connections from the GovShield Client to the GovShield Server. For both the GovShield Client and GovShield Server, revocation checking is performed every time a certificate is presented for a validation check.

[MDMPP] FIA_X509_EXT.1.2(1) – *"The evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

For both the GovShield Server and GovShield Client, Section 8.4.4 of the ST states revocation checking is performed every time a certificate is presented for a validation check. Validation checks occur during signature verification for signed policies and in support of TLS and HTTPS/TLS connections. During the validation checks, the underlying platform is invoked in order to check if the basicConstraint extension is present and the CA flag is set to TRUE.

[MDMPP] FIA_X509_EXT.2.1 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

The SFR selection is "invoke platform-provided functionality", therefore, this TSS Assurance Activity is applicable.

Section 8.4.4 of the ST states that the underlying platform is invoked by the GovShield Server to provide X.509v3 certificate services for signing policies that are sent to the GovShield Clients and for TLS and HTTPS/TLS session establishment when operating as both a client and server for the respective protocol. Additionally, the GovShield Client invokes its underlying platform to provide X.509v3 certificate services for signature verification for signed policies sent from the GovShield Server, and in support of HTTPS/TLS connections from the GovShield Client to the GovShield Server.

[MDMPP] FIA_X509_EXT.2.2 – *"The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates.*

If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).

If "implement functionality" is selected, the evaluator shall examine the TSS to confirm that it describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used

in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described."

The SFR selection is "invoke platform-provided functionality", therefore, this portion of the TSS Assurance Activity is applicable. The SFR selection is "implement functionality" was not claimed, therefore, this portion of the TSS Assurance Activity is not applicable.

Section 8.4.4 of the ST states the GovShield Server's platform uses the certificate it creates for policy signing based upon the certificate being generated by the platform based upon an Authorized Administrator's request in the web GUI. The GovShield Server also relies on its platform to provide its X.509v3 certificate as part of TLS and HTTPS/TLS session establishment in all cases where the GovShield Server is the server component in the session (e.g., connections to GovShield Clients) as well as upon the server component's request where the GovShield Server is the client component and mutual authentication has been configured. The GovShield Server's platform knows the certificate to use for its HTTPS/TLS session establishment based upon its loading into the Java Keystore. The GovShield Server's platform uses the OCSP as specified in RFC 6960 to verify revocation status. Revocation checking occurs each time a certificate is presented for a validation check. If the GovShield Server's platform cannot establish a connection to determine the validity of a certificate, then the certificate is not accepted. Sections 2 and 3 of the GovShield Installation Guide v1.0 contain instructions for configuring the operating environment so that the TOE can use the certificates. The instructions include prerequisites for the entire TOE's underlying platform, configuration of Java and JBoss, and specifications of the certificates files.

Section 8.4.4 of the ST states the GovShield Client's platform uses the certificate provided during enrollment to support the HTTPS/TLS connections from the GovShield Client to the GovShield Server and uses the public key used for verification of the signed policies also received through the GovShield Client from the GovShield Server. The underlying platform is able to determine which certificate to use for the validity check based upon the presented certificate's data. The GovShield Client's platform uses CRL as specified in RFC 5280 Section 6.3 to verify revocation status. Revocation checking occurs each time a certificate is presented for a validation check. If the GovShield Client's platform cannot establish a connection to determine the validity of a certificate, then the certificate is not accepted.

[MDMPP] FIA_CLI_EXT.1 – TD0754 – *"The evaluator shall ensure that the TSS describes how the client is uniquely identified."*

Section 8.4.5 of the ST states that each Android Mobile Device receives its unique X.509v3 certificate within the initial payload sent to it during enrollment by the GovShield Server; which is subsequently used by the GovShield Client to uniquely identify itself during HTTPS/TLS connections to the GovShield Server.

[MDMPP] FMT_MOF.1(1) – *"The evaluator shall examine the TSS and user documents to ensure that they describe what security management functions are restricted to the administrator and what actions can be taken for each management function. The evaluator shall verify that the security management functions are restricted to authorized administrators and the administrator is only able to take the actions as described in the user documents."*

Section 8.5.1 of the ST states that only Authorized Administrators have the ability to manage the TOE through the web GUI and thus, all functions related to FMT_SMF.1(1), FMT_SMF.1(2), and FMT_SMF.1(3) are restricted to the Administrator. Section 8.5.9 also states that the only user roles are the Administrator and the MD User, and thus, the Administrator is the only Authorized Administrator.

[MDMPP] FMT_MOF.1(2) – *"The evaluator shall examine the TSS and verify that it describes how unauthorized users are prevented from enrolling in the MDM services."*

Section 8.5.2 of the ST states that a MD user or an Administrator with physical custody of the mobile device can initiate the enrollment process. The MD user or Administrator must enter valid credentials

through the GovShield Client interface for the enrollment process to continue. If the MD user or Administrator passes authentication, they are authorized to perform the enrollment process. Failure of the authentication process would prevent enrolling the mobile device into the MDM services.

[MDMPP] FMT_MOF.1(3) – *"The evaluator shall examine the TSS to determine that all methods of initiating an application download or update push are specified."*

Section 8.5.3 of the ST discusses the methods by which an application download or update push is initiated. The MAS Server component of the GovShield Server provides the ability to configure 'application access groups' in the web GUI. Applications can be added to the MAS Server as an individual file that is uploaded to the GovShield Server and stored in the Oracle Database. During the application's initial upload or after the upload has been completed, the application is assigned to one or more policies. Android Mobile devices are assigned to an 'application access group' that ties that group of devices to an application management policy. The Android Mobile Devices assigned to an 'application access group' will have their GovShield Client download the applications that have been added to the corresponding application policy in the MAS Server upon their next reachability event related to application management.

[MDMPP] FMT_POL_EXT.1 – TD0754 – *"The evaluator shall verify that the ST describes how policies are signed, to include whether the private key used for signing is associated with an X509 certificate or public key, the method for distributing the policy verification material (a certificate or provisioned public key) to the agent, and the method for distinguishing whether a policy is appropriate for an agent. If tokens are claimed in FMT_POL_EXT.1.3, the evaluator shall verify the ST describes how tokens are established and distributed to the agent."*

Section 8.5.4 of the ST states the GovShield Server invokes its platform to digitally sign the policies with a trusted X.509v3 certificate using RSA 2048 with SHA-256. The TOE's method for distributing the policy verification material is that the GovShield Server provides the GovShield Client the public key used to verify the signature of policies as part of an initial payload during enrollment of an Android Mobile Device. The method for distinguishing whether a policy is appropriate for an agent based upon the policy being assigned to the Android Mobile Device, and each policy's signature being validated by the GovShield Client's platform before the GovShield Client applies the policy to its Android Mobile Device.

[AGENTMOD] FMT_POL_EXT.2 – *"The evaluator ensures that the TSS describes how the candidate policies are obtained by the MDM Agent, the processing associated with verifying the digital signature of the policy updates, and the actions that take place for successful (signature was verified) and unsuccessful (signature could not be verified) cases. The software components that are performing the processing must also be identified in the TSS and verified by the evaluators."*

Section 8.5.5 of the ST describes that policies are sent to a device's GovShield Client by the GovShield Server when they are assigned to that Android Mobile Device and the GovShield Client performs a reachability event to determine an updated or new policy has been assigned. Every policy is signed with a trusted X.509v3 certificate using RSA 2048 with SHA-256 by the GovShield Server's platform. The GovShield Client requests its underlying platform to verify each policy before the GovShield Client will apply the policy to the Android Mobile Device.

[MDMPP] FMT_SMF.1(1) – TD0479 – *"The evaluator shall examine the TSS to ensure that it describes each management function claimed. The evaluator shall examine the TSS to ensure that it identifies the management functions implemented for each supported MDM Agent/platform, which are likely to be subsets of all of the management functions available to the administrator on the MDM Server. The evaluator shall examine the TSS to verify that any differences between management functions and policies for each supported MDM Agent/platform are clearly indicated.*

The evaluator shall determine if the Mobile Device has been evaluated. If so, the evaluator shall examine the TSS to verify that it clearly identifies which management functions match the selections and assignments of the evaluated Mobile Device and which management functions were not evaluated."

Section 8.5.6 of the ST provides a list describing all security management functions claimed by the TOE. Table 20 lists the management functions that can be performed by the GovShield Server as defined FMT_SMF.1.1(1), and whether this behavior is enforced by the GovShield Client or by the underlying mobile device platform. There is only a single MDM Agent/platform claimed, GovShield Client and Android respectively, and thus, Table 20 covers all management functions for this MDM Agent/platform pair and there is no possibility of any differences as there is only a single pair. The mobile device has been evaluated under VID11593 and Table 20 contains a column that identifies which management functions were and were not claimed as part of the mobile device evaluation.

[MDMPP] FMT_SMF.1(2) – *"The evaluator shall examine the TSS to ensure that it describes each management function listed. For function c.4, the evaluator shall examine the TSS to ensure that it describes the privacy-sensitive information that the TOE has the capability to collect from enrolled mobile devices."*

Section 8.5.7 of the ST describes each of the claimed management functions listed in the SFR. Function c.4 is selectable and is not claimed within this evaluation and thus, there is no claim for privacy-sensitive information that the TOE has the capability to collect from enrolled mobile devices.

[MDMPP] FMT_SMF.1(3) – *"The evaluator shall examine the TSS to ensure that it describes each management function listed.*

The evaluator shall examine the TSS to determine if the MAS Server creates its own groups or relies on the groups specified by the MDM Server."

Section 8.5.3 of the ST discusses the methods by which an application download or update push is initiated. The MAS Server component of the GovShield Server provides the ability to configure 'application access groups' in the web GUI. Applications can be added to the MAS Server as an individual file that is uploaded to the GovShield Server and stored in the Oracle Database. During the application's initial upload or after the upload has been completed, the application is assigned to one or more policies. Android Mobile devices are assigned to an 'application access group' that ties that group of devices to an application management policy. The Android Mobile Devices assigned to an 'application access group' will have their GovShield Client download the applications that have been added to the corresponding application policy in the MAS Server upon their next reachability event related to application management.

[AGENTMOD] FMT_SMF_EXT.4 – *"The evaluator shall verify that the any assigned functions are described in the TSS and that these functions are documented as supported by the platform. The evaluator shall examine the TSS to verify that any differences between management functions and policies for each supported mobile device are listed.*

The evaluator shall verify that the TSS describes the methods in which the MDM Agent can be enrolled.

The TSS description shall make clear if the MDM Agent supports multiple interfaces for enrollment and configuration (for example, both remote configuration and local configuration)."

Section 8.5.8 of the ST describes how certificates used for authentication of the GovShield Client communications are imported during enrollment into management, how administrator-provided device management functions defined in FMT_SMF.1(1) are received and processed by the GovShield Clients (including the TOE unlock banner), whether users can configure the interaction between TOE components by allowing unenroll from management, and the configuration of the periodicity of reachability events.

Section 8.5.6 of the ST provides a listing of all security management functions claimed by the TOE. Table 20 lists the management functions that can be performed by the GovShield Server as defined FMT_SMF.1.1(1), and whether this behavior is enforced by the GovShield Client or by the underlying mobile device platform. There is only a single MDM Agent/platform claimed, GovShield Client and

Android respectively, and thus, Table 20 covers all management functions for this MDM Agent/platform pair and there is no possibility of any differences as there is only a single pair. The mobile device has been evaluated under VID11593 and Table 20 contains a column that identifies which management functions were and were not claimed as part of the mobile device evaluation.

Section 8.4.1 of the ST describe how the GovShield Clients are used to enroll the mobile devices into management. These sections fully describe the enrollment process which only describes a single interface for enrollment by the MD user/Authorized Administrator as well as between the GovShield Client and the GovShield Server. The section also describes performing user authentication and restricting enrollment of devices.

[MDMPP] FMT_SMR.1.1(1) – This SFR does not contain any MDMPP TSS Assurance Activities.

[MDMPP] FMT_SMR.1.2(1) – *"The evaluator shall examine the TSS to verify that it describes the administrator role and the powers granted to and limitations of the role."*

Section 8.5.9 of the ST describes the two administrative roles, Administrator and MD User, as well as the privileges and limitations for each role. Administrators can manage the TOE through the web GUI and every Administrator has access to all functions through this interface. Administrators also have the ability to interact with the TOE through the GovShield Client interface. MD Users can only interact with the TOE through the GovShield Client interface.

[MDMPP] FMT_SMR.1.1(2) – This SFR does not contain any MDMPP TSS Assurance Activities.

[MDMPP] FMT_SMR.1.2(2) – *"The evaluator shall examine the TSS to verify that it describes the administrator role and the powers granted to and limitations of the role."*

Section 8.5.10 of the ST states that since the MAS Server is not accessed separately from the remainder of the GovShield Server capabilities, the user roles and their ability to interact with the MAS Server functionality is defined in the same manner as for FMT_SMR.1(1).

Section 8.5.9 of the ST describes the two administrative roles, Administrator and MD User, as well as the privileges and limitations for each role. Administrators can manage the TOE through the web GUI and every Administrator has access to all functions through this interface. Administrators also have the ability to interact with the TOE through the GovShield Client interface. MD Users can only interact with the TOE through the GovShield Client interface.

[AGENTMOD] FMT_UNR_EXT.1 – *"The evaluator shall ensure that the TSS describes the mechanism used to prevent users from unenrolling or the remediation actions applied when unenrolled."*

Section 8.5.11 of the ST states that in the evaluated configuration, only the Administrator will have the ability to unenroll GovShield Clients from the deployment. This is enforced through a default policy that is installed on all GovShield Clients upon enrollment. When configured in this manner, the GovShield Client will configure the Android Mobile Device's Samsung Knox functionality to prevent the MD user from removing the 'device owner role' being assigned to the GovShield Client on the device.

[MDMPP] FPT_API_EXT.1 – *"The evaluator shall verify that the TSS lists the platform APIs used by the MDM software. The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported."*

Section 8.6.1 of the ST lists the platform APIs used by the GovShield Server and GovShield Client.

The list of supported APIs and their corresponding public documentation are as follows:

[SERVER] The GovShield Server uses only the supported Windows Server platform APIs listed below in order to function.

- Apache Commons - https://commons.apache.org/
- Apache Logging - https://logging.apache.org/index.html
- BSafe Crypto - https://www.dell.com/support/product-details/en-us/product/bsafe-crypto-j/resources/manuals
- FasterXML - https://github.com/fasterxml/jackson
- Hibernate - https://docs.spring.io/spring-framework/reference/data-access/orm/hibernate.html
- java.security - https://docs.oracle.com/javase/8/docs/api/java/security/package-summary.html
- javax.security - https://docs.oracle.com/javase/8/docs/technotes/guides/security/
- javax.servlet - https://docs.oracle.com/cd/E17802_01/products/products/servlet/2.5/docs/servlet-2_5-mr2/javax/servlet/package-summary.html
- JBoss EJB - https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/7.4/html-single/developing_jakarta_enterprise_beans_applications/index
- Spring Framework - https://docs.spring.io/spring-framework/docs/4.3.x/spring-framework-reference/html/
- Spring Security - https://docs.spring.io/spring-security/site/docs/4.1.2.RELEASE/reference/html/
- Wildfly Elytron - https://github.com/wildfly-security/wildfly-elytron

[AGENT] The GovShield Client uses only the supported Android platform APIs listed below in order to function.

- android.security - https://developer.android.com/reference/android/security/package-summary
- BSafe Crypto - https://www.dell.com/support/product-details/en-us/product/bsafe-crypto-j/resources/manuals
- java.security - https://developer.android.com/reference/java/security/package-summary
- javax.crypto - https://developer.android.com/reference/javax/crypto/package-summary
- javax.net.ssl - https://developer.android.com/reference/javax/net/ssl/package-summary
- Samsung Knox - https://docs.samsungknox.com/dev/
- SQL Cipher - https://www.zetetic.net/sqlcipher/sqlcipher-api/

[MDMPP] FPT_ITT.1(2) – *"The evaluator shall examine the TSS to determine that the methods and protocols used to protect distributed TOE components are described. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.*

If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

Section 8.6.2 of the ST states that HTTPS/TLS is used for the secure transfer of communications between the GovShield Server and the GovShield Client. This claim is consistent with the selections made for the FPT_ITT.1.1(2) requirement as well as throughout the remainder of the ST.

Section 8.6.2 of the ST states that the GovShield Client invokes its platform based upon a reachability event. The GovShield Server's platform is invoked by the GovShield Client's platform making a HTTPS/TLS connection request. During TLS session establishment, the GovShield Server's platform will also validate the identity of the presented X.509v3 certificate from the GovShield Client's platform. The

GovShield Client relies on its underlying platform to provide the HTTPS/TLS communication path and to validate the GovShield Server's X.509v3 certificate.

[MDMPP] FPT_LIB_EXT.1 – TD0895 – *"The evaluator shall verify that the TSS lists the libraries used by the MDM software or the public libraries used by the cloud MDM services. The evaluator shall verify that libraries found to be packaged with or employed by the MDM software are limited to those in the assignment.*

Library Document

(conditional: The TOE is a cloud MDM service) The evaluator shall verify that the non-public Library Document lists the libraries used by the MDM service."

Section 8.6.3 of the ST lists the libraries used by the GovShield Server in Table 21. Section 8.6.3 of the ST lists the libraries used by the GovShield Client in Table 22. The evaluation team reviewed the list of third-party libraries with the developer and documented the third-party libraries found during the review. The libraries documented in Tables 21 and Table 22 match the list created by the evaluation team. This is not a cloud MDM service.

[MDMPP] FPT_TST_EXT.1.1 – This SFR does not contain any MDMPP TSS Assurance Activities.

[MDMPP] FPT_TST_EXT.1.2 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).*

If "implement functionality" is selected, the evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

The evaluator shall examine the TSS to ensure that it describes how to verify the integrity of stored TSF executable code when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code has not been compromised. The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful e.g., hash not verified) cases."

The SFR selection "invoke platform-provided functionality" was claimed, therefore, this portion of the TSS Assurance Activity is applicable. The SFR selection "implement functionality" was not claimed, therefore, this portion of the TSS Assurance Activity is not applicable.

Section 8.6.4 of the ST states that the Java Runtime Environment Platform is responsible for executing GovShield Server's software integrity check during the start or the restart of the GovShield Server's software. Each time the JBoss EAP is started, whether at boot or restarted manually, the TOE validates all of the .jar files that are contained in the GovShield Server's software file. JBoss performs a SHA-256 checksum on each of the .jar files within the deployed GovShield Server's software file, and compares the calculated checksum to the checksum defined in the manifest listing. The manifest listing is created at build time and provided within the GovShield Server's software file. The manifest can be trusted as the GovShield Server's software file is digitally signed at build time, and is verified by the platform as part of the installation process. If any checksum comparison does not match the GovShield Server software will not be started, and the failure is audited along with identifying which .jar file(s) failed.

Section 4 of the GovShield Installation Guide v1.0 contains the procedures for starting the GovShield Server's software. This information matches what is described within the ST and contains additional detail for validating the successful and failed integrity checks which occur during its startup.

Section 8.6.4 of the ST also includes an argument that these tests are sufficient to validate the correct operation of the TSF because the platform does an integrity check of the GovShield Server's software, and the GovShield Server will not be started if the integrity check fails.

[MDMPP] FPT_TUD_EXT.1.1 – This SFR does not contain any MDMPP TSS Assurance Activities.

[MDMPP] FPT_TUD_EXT.1.2 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.6.5 of the ST states the GovShield Server's platform is invoked based upon an Authorized Administrator starting the platform's JBoss EAP service as part of the update process, which will result in the platform verifying the digital signature of the GovShield Server software update. Note that the Authorized Administrators the ability to initiate updates to GovShield Client are implemented by the TOE through the GovShield Server's MAS Server functionality.

[MDMPP] FPT_TUD_EXT.1.3 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).*

If "implement functionality" is selected, the evaluator shall examine the TSS and verify that it describes the standards by which the updates are digitally signed and how the signature verification process is implemented."

The SFR selection "invoke platform-provided functionality" was claimed, therefore, this portion of the TSS Assurance Activity is applicable. The SFR selection "implement functionality" was not claimed, therefore, this portion of the TSS Assurance Activity is not applicable.

Section 8.6.5 of the ST states the GovShield Server's platform is invoked based upon an Authorized Administrator starting the platform's JBoss EAP service as part of the update process, which will result in the platform verifying the digital signature of the GovShield Server software update. The GovShield Client's platform is invoked by the GovShield Client once the update is downloaded onto the Android Mobile Device and will invoke the platform's application installation process which will verify the software update's digital signature before installing the GovShield Client software update.

[MDMPP] FTA_TAB.1 – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity).*

If "implement functionality" is selected, the TSS shall describe when the banner is displayed."

The SFR selection "invoke platform-provided functionality" was not claimed, therefore, this portion of the TSS Assurance Activity is not applicable. The SFR selection "implement functionality" was claimed, therefore, this portion of the TSS Assurance Activity is applicable.

Section 8.7.1 of the ST states that the GovShield Server displays a configurable consent warning banner on the web GUI. The warning banner must be acknowledged by clicking the 'ACCEPT' button before an

administrator can access the login page. Additionally, the GovShield Client displays a configurable consent warning banner on its login page.

[MDMPP] FTP_ITC_EXT.1 – *"The evaluator shall ensure that the TSS contains whether the MDM Server communication channel is internal or external to the TOE."*

Section 8.8.1 of the ST describes an GovShield Server communication channel to the GovShield Client that is internal to the TOE. This internal communication channel is established after a successful Android Mobile Device enrollment and is logically distinct form other communication channels.

[MDMPP] FTP_ITC.1.1(1) – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.8.2 of the ST states that in the evaluated configuration, the GovShield Server connects with the Oracle Database, which also operates as the audit server, using TLS v1.2 to protect the audit data, authentication data, and TOE configuration data that traverses the channel. The GovShield Server invokes the TLSv1.2 connection used to protect the aforementioned data while in transit to/from the Operational Environment's Oracle Database. The MAS Server functionality is logically integrated with the GovShield Server and as a result requires the same remote communication mechanisms to operate.

[MDMPP] FTP_ITC.1.2(1) – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.8.2 of the ST states that in the evaluated configuration, the GovShield Server connects with the Oracle Database, which also operates as the audit server, using TLS v1.2 to protect the audit data, authentication data, and TOE configuration data that traverses the channel. The GovShield Server invokes the TLSv1.2 connection used to protect the aforementioned data while in transit to/from the Operational Environment's Oracle Database. The MAS Server functionality is logically integrated with the GovShield Server and as a result requires the same remote communication mechanisms to operate.

[MDMPP] FTP_ITC.1.3(1) – *"The evaluator shall examine the TSS to determine that the methods of communication with authorized IT entities are indicated, along with how those communications are protected.*

If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

Section 8.8.2 of the ST states that in the evaluated configuration, the GovShield Server connects with the Oracle Database, which also operates as the audit server, using TLS v1.2 to protect the audit data, authentication data, and TOE configuration data that traverses the channel. The GovShield Server invokes the TLSv1.2 connection used to protect the aforementioned data while in transit to/from the Operational Environment's Oracle Database. The MAS Server functionality is logically integrated with the GovShield Server and as a result requires the same remote communication mechanisms to operate.

[MDMPP] FTP_TRP.1.1(1) – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.8.3 of the ST states that the GovShield Server's platform's HTTPS/TLS server function is invoked based upon Administrators attempting to connect (i.e., invoking the platform) to the web GUI for the purposes of remote administration.

[MDMPP] FTP_TRP.1.2(1) – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.8.3 of the ST states that the GovShield Server's platform's HTTPS/TLS server function is invoked based upon Administrators attempting to connect (i.e., invoking the platform) to the web GUI for the purposes of remote administration.

[MDMPP] FTP_TRP.1.3(1) – *"The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.*

If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

Section 8.8.3 of the ST states that the GovShield Server's platform's HTTPS/TLS server function is invoked based upon Administrators attempting to connect (i.e., invoking the platform) to the web GUI for the purposes of remote administration. This claim is consistent with the selections made for the FTP_TRP.1(1) requirement as well as throughout the remainder of the ST.

[MDMPP] FTP_TRP.1.1(2) – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.8.4 of the ST states that the HTTPS/TLS (TLS v1.2) communication path is used by the GovShield Client for the purposes of enrolling an Android Mobile Device after an MD user or an Authorized Administrator begins the enrollment process through the GovShield Client. The TOE components rely on their underlying platforms to provide the HTTPS/TLS communication path, and to validate the other TOE components' X.509v3 certificate. This claim is consistent with the selections made for the FTP_TRP.1(2) requirement as well as throughout the remainder of the ST. Thus, the GovShield Client and platform are invoked by the MD user or Authorized Administrator and the GovShield Server and platform are invoked in response to a connection request from the GovShield Client.

[MDMPP] FTP_TRP.1.2(2) – *"If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."*

Section 8.8.4 of the ST states that the HTTPS/TLS (TLS v1.2) communication path is used by the GovShield Client for the purposes of enrolling an Android Mobile Device after an MD user or an Authorized Administrator begins the enrollment process through the GovShield Client. The TOE components rely on their underlying platforms to provide the HTTPS/TLS communication path, and to validate the other TOE components' X.509v3 certificate. This claim is consistent with the selections made for the FTP_TRP.1(2) requirement as well as throughout the remainder of the ST. Thus, the GovShield Client and platform are invoked by the MD user or Authorized Administrator and the GovShield Server and platform are invoked in response to a connection request from the GovShield Client.

[MDMPP] FTP_TRP.1.3(2) – *"The evaluator shall examine the TSS to determine that the methods of remote enrollment are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of enrollment are consistent with those specified in the requirement, and are included in the requirements in the ST.*

If "invoke platform-provided functionality" is selected, the evaluator shall examine the TSS to verify that it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the MDM Server; nonetheless, that mechanism will be identified in the TSS as part of this evaluation activity)."

Section 8.8.4 of the ST states that the HTTPS/TLS (TLS v1.2) communication path is used by the GovShield Client for the purposes of enrolling an Android Mobile Device after an MD user or an Authorized Administrator begins the enrollment process through the GovShield Client. The TOE components rely on their underlying platforms to provide the HTTPS/TLS communication path, and to validate the other TOE components' X.509v3 certificate. This claim is consistent with the selections made for the FTP_TRP.1(2) requirement as well as throughout the remainder of the ST. Thus, the GovShield Client and platform are invoked by the MD user or Authorized Administrator and the GovShield Server and platform are invoked in response to a connection request from the GovShield Client.

3 Operational Guidance Assurance Activities

The evaluation team completed the testing of the Operational Guidance, and confirmed that the Operational Guidance contains all Assurance Activities as specified by the *Protection Profile for Mobile Device Management Version 4.0, April 25, 2019 [MDMPP]* and *PP-Module for MDM Agent Version 1.0, April 25, 2019 [AGENTMOD]*. The evaluators reviewed the MDMPP and AGENTMOD to identify the security functionality that must be discussed for the operational guidance. This is prescribed by the Assurance Activities for each SFR and the Guidance SARs. The evaluators have listed below each of the SFRs defined in the MDMPP and AGENTMOD that have been claimed by the TOE (some SFRs are conditional or optional) as well as the Guidance SAR, along with a discussion of where in the operational guidance the associated Assurance Activities material can be found. The following references are used in this section of the document:

(1) *GovShield Version 1.60.05 Security Target v1.0, February 6, 2026* [ST]
(2) *GovShield Installation Guide v1.0, February 6, 2026* [Install Guide]
(3) *GovShield User Guide v1.0, February 6, 2026* [User Guide]

[MDMPP] FAU_ALT_EXT.1 – *"The evaluator shall examine the guidance document and verify that it describes how the alerts can be configured, if configurable."*

The evaluation team has determined that the alerts themselves are not individually configurable but occur due to actions occurring on the mobile device due to the device's configured policy or an action by a user or an Administrator. The following policy settings or actions result in alerts:

- Section 9.2 of the User Guide describes enrollment which will generate an alert for change in enrollment state.
- Sections 2.5.1 and 2.5.2 of the User Guide describe actions which will result in unenrollment which will generate an alert for change in enrollment state.
- Section 9.2 of the User Guide describes enrollment which will generate an alert for failure and successful application of policies to a mobile device.
- Section 4.1.1 of the User Guide describes creating a policy which has Polling Interval as a variable which will generate an alert for failure and successful application of policies to a mobile device.
- Section 4.1.1 of the User Guide describes creating a policy which has Polling Interval, App Polling Interval, and Audit Log Publishing Rate as variables which will generate an alert for periodic reachability events.

- Section 4.1.1 of the User Guide describes creating a policy which has App Polling Interval as a variable which will generate an alert for failure to install an application from the MAS Server
- Section 4.1.1 of the User Guide describes creating a policy which has App Polling Interval as a variable which will generate an alert for failure to update an application from the MAS Server

[AGENTMOD] FAU_ALT_EXT.2 – There are no AGD assurance activities for this SFR.

[MDMPP] FAU_GEN.1.1(1) – *"The evaluator shall check the administrative guide and ensure that it lists all of the auditable events. The evaluator shall check to make sure that every audit event type mandated by the PP is described.*

The evaluator shall also make a determination of the administrative actions that are relevant in the context of this PP including those listed in the Management section. The evaluator shall examine the administrative guide and make a determination of which administrative commands are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security relevant with respect to this PP. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements."

Sections 7.2, 8.2 and 8.3 of the User Guide include sample tables of all the auditable events and required event types mandated by the PP. Within the sample table of auditable events, there are sample audit records for the success and/or failure of functions that originate from the GovShield Client and GovShield Server (including the MAS Server component).

The Install Guide and User Guide were developed with the intent of providing specific guidance for managing TOE functionality as described by the statement in Section 1 for both documents.

"This document is intended for administrators responsible for installing, configuring, and/or operating GovShield. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is also expected to be familiar with the general operation of the GovShield product. This guidance also includes information on configuration of the behavior of the platforms upon which GovShield operates.

The reader is also expected to be familiar with the GovShield Version 1.60.05 Security Target and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions on how to perform the security functions that are defined by these SFRs. The GovShield Version 1.60.05 product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the evaluation were assessed. Any functionality that is not described in the GovShield Version 1.60.05 Security Target was not evaluated and should be exercised at the user's risk."

Based upon this statement, the PP author stated that the Install Guide and User Guide were developed specifically for the scope of the Common Criteria evaluation. Through the assessment of the SFR Guidance Assurance Activities, the evaluation team confirmed that these documents contained all management actions needed to install, configure, and operate the TOE as it relates to the SFRs. The directions in the Install Guide are primarily installation and configuration actions which occur as part of the setup of the TOE but are necessary for all TOE functions to operate. The User Guide contains the administrative commands related to the SFRs during the operation of the TOE.

[MDMPP] FAU_GEN.1.2(1) – *"The evaluator shall check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief*

description of each field. The evaluator shall check to make sure that the description of the fields contains the information required in FAU_GEN.1.2(1).”

Section 8.1 of the User Guide provides an example audit record to illustrate the standard format for TSF audit records. As shown in the example, each audit record contains Device ID (if applicable), Server Name, Event Type, Success/Failure, Date and Time, Subject Identity, and Additional Information. The description of the fields contains the information required by the SFR.

[MDMPP] FAU_GEN.1.1(2) – *“The evaluator shall check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field.”*

Section 8.3 of the User Guide provides an example audit record to illustrate the standard format for the MAS Server audit records. As shown in the example, each audit record contains Device ID (if applicable), Server Name, Event Type, Success/Failure, Date and Time, Subject Identity, and Additional Information. The description of the fields contains the information required by the SFR.

[MDMPP] FAU_GEN.1.2(2) – *“The evaluator shall check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that the description of the fields contains the information required in FAU_GEN.1.2(2).”*

Section 7.1 of the User Guide provides an example audit record to illustrate the standard format for TSF audit records. As shown in the example, each audit record contains Date and Timestamp, identifies the Device ID as part of subject identity, Username as part of subject identity, Server Name to which device is assigned, Message which is the Event Type and Success/Failure. The description of the fields contains the information required by the SFR.

[AGENTMOD] FAU_GEN.1(2) – There are no AGD assurance activities for this SFR.

[MDMPP] FAU_NET_EXT.1 – *“The evaluator shall verify that the guidance instructs administrators on the method of determining the network connectivity status of an enrolled agent.”*

Section 2.6 of the User Guide describes that Administrators have two methods for checking the network connectivity status of an enrolled device, through the ‘Device Management’ dashboard and the ‘Device Alerts’ dashboard.

[MDMPP] FAU_SAR.1.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FAU_SAR.1.2 – *“The evaluator shall check the AGD guidance and ensure that it describes how the administrator accesses the audit data and describes the format of the audit record.”*

Sections 6, 7, and 8 of the User Guide describe the ability to check audit logs through the Device Alerts, Audit Log, and Server Audit Log tabs of the administrative interface. Respectively, these tabs have audit logs for events and changes performed on the device, log messages from devices being managed by the MDM server, and GovShield server activity events

[AGENTMOD] FAU_SEL.1(2) – *“The evaluator shall examine the operational guidance to determine that it contains instructions on how to define the set of auditable events as well as explains the syntax for multi-value selection (if applicable). The evaluator shall also verify that the operational guidance shall identify those audit records that are always recorded, regardless of the selection criteria currently being enforced.”*

The ‘multi-value selection’ is not selected, and as such, this portion of the AGD Assurance Activity is not applicable.

Section 7.2 of the User Guide states under this SFR that there is no specific configuration to turn on and off auditing on the TOE, thus the GovShield Client and its underlying platform will always perform auditing. However, an Authorized Administrator creates policies on the GovShield Server and will assign them to one or more Android Mobile Devices. These policies include requirements for the GovShield Client to generate audit records for the functionality configured in the policies. Once the GovShield Client receives and applies a policy requiring auditing, the GovShield Client will always generate the necessary audit records. The evaluation determined that based upon this, only functions that are controlled by a policy would not always be audited, and the decision on whether an audit is generated or not would be based upon the GovShield Client having consumed a policy related to that event. For this reason, the selection of auditable events is configurable through policy.

[MDMPP] FAU_STG_EXT.1 – *"The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.*

The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server."

Section 2 of the Install Guide describes how audit data is logged remotely to the Oracle Database. The 'no other method' was selected in FAU_STG_EXT.1.1 and thus, there is no local audit data and no relationship between local audit data and the audit data logged in the Oracle Database.

Section 2 of the Install Guide states that an Oracle SQL Server of at least version 19c configured to accept TLS v1.2 requests are the requirements on the audit server. Sections 2 and 3 of the Install Guide contain instructions for configuring the operating environment so that the TOE can use Java, JBoss, and the BSafe cryptographic library to perform all cryptographic services. The instructions include prerequisites for the entire TOE's underlying platform, configuration of Java and JBoss, and specifications of the certificates files.

[MDMPP] FCO_CPC_EXT.1.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FCO_CPC_EXT.1.2 – There are no AGD assurance activities for this SFR.

[MDMPP] FCO_CPC_EXT.1.3 – *"The evaluator shall examine the guidance documentation to confirm that it contains instructions for enabling and disabling communications with any individual component of a distributed TOE. The evaluator shall confirm that the method of disabling is such that all other components can be prevented from communicating with the component that is being removed from the TOE (preventing the remaining components from either attempting to initiate communications to the disabled component, or from responding to communications from the disabled component)."*

Section 9.2 of the User Guide describes enrollment which enables communications between the GovShield Client and GovShield Server.

Sections 2.5.1 and 2.5.2 of the User Guide describe actions which will result in unenrollment which disables communications between the GovShield Client and GovShield Server. Both Sections also state that this action disallows the device from accessing the GovShield Server. The method of disabling communications results in the unenrollment of the device which will prevent all communication between TOE components because the GovShield Client has been removed from the device through this action.

[MDMPP] FCS_CKM.1 – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_CKM.2 – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_CKM_EXT.4 – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_COP.1(1) – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_COP.1(2) – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_COP.1(3) – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_COP.1(4) – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_RBG_EXT.1 – When the TOE invokes this functionality, there are no AGD assurance activities for this SFR.

[MDMPP] FCS_STG_EXT.1 – There are no AGD assurance activities for this SFR.

[AGENTMOD] FCS_STG_EXT.1(2) – There are no AGD assurance activities for this SFR.

[MDMPP] FIA_ENR_EXT.1.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FIA_ENR_EXT.1.2 – *"The evaluator shall ensure that the administrative guidance describes the method(s) of restricting user enrollment and that it instructs the administrator how to configure the restrictions."*

Section 2.1 of the User Guide describes whitelisting a device by defining the allowed Android Device IDs which can enroll into the TOE.

[AGENTMOD] FIA_ENR_EXT.2 – *"The evaluator shall examine the operational guidance to verify that it describes how to configure reference identifier of the MDM Server's certificate and, if different than the reference identifier, the Domain Name or IP address (for connectivity) of the MDM Server."*

Section 9.2 of the User Guide describes enrollment which includes the actions the Administrator needs to take within the web GUI as well as the user or the Administrator need to take on the GovShield Client. These actions include the generation and subsequent scanning of a QR code. Within the QR code is an embedded URL for the GovShield Server. The GovShield Client will record the URL of the GovShield Server during a successful enrollment of the Android Mobile Device. The URL will then be used as the GovShield Server's reference identifier for subsequent communications between the GovShield Client and GovShield Server.

[MDMPP] FIA_UAU.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FIA_X509_EXT.1.1(1) – TD0641 – "*If "internal lookup of TOE-managed certificate status" is selected, then the evaluator shall ensure the AGD documentation describes how issued certificates are reported as invalid.*"

The "internal lookup of TOE-managed certificate status" is not selected, as such, this AGD Assurance Activity is not applicable.

[MDMPP] FIA_X509_EXT.1.2(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FIA_X509_EXT.2.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FIA_X509_EXT.2.2 – *"If the requirement that the administrator is able to specify the default action is selected, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed."*

The "allow the administrator to choose whether to accept the certificate in these cases" is not selected, as such, this AGD Assurance Activity is not applicable.

[MDMPP] FIA_CLI_EXT.1 – TD0754 – There are no AGD assurance activities for this SFR.

[MDMPP] FMT_MOF.1(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FMT_MOF.1(2) – There are no AGD assurance activities for this SFR.

[MDMPP] FMT_MOF.1(3) – *"The evaluator shall confirm that the operational guidance contains how to initiate an application download or update push."*

Section 5 of the User Guide describes the ability to manage applications, including the ability to assign an application to a policy and select whether or not to install the application on the device. Section 5 also includes directions to change the APK file which covers an update to the application.

[MDMPP] FMT_POL_EXT.1 – *"If applicable, the evaluator shall verify that the AGD guidance instructs administrators on configuring the Enterprise certificate to be used for signing policies or signing the policies before applying them."*

Section 9.1 of the User Guide describes the ability to generate a certificate through the System Configuration page by clicking the 'Generate' button.

[AGENTMOD] FMT_POL_EXT.2 – There are no AGD assurance activities for this SFR.

[MDMPP] FMT_SMF.1(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FMT_SMF.1(2) – *"The evaluator shall verify the AGD guidance includes detailed instructions of what options are available and how to configure each management functional capability listed."*

Section 2.1 of the User Guide describes whitelisting a device by defining the allowed Android Device IDs which can enroll into the TOE. This satisfies how to 'configure the devices specified by Android Device ID allowed for enrollment'.

Section 9.1 of the User Guide describes the ability to generate a certificate through the System Configuration page by clicking the 'Generate' button. Sections 2 and 3 of the Install Guide contain instructions for configuring the operating environment so that the TOE can use the certificates. The instructions include prerequisites for the entire TOE's underlying platform, configuration of Java and JBoss, and specifications of the certificates files. Together these satisfy how to 'choose X.509v3 certificates for MDM Server use'.

Section 9.1.2 of the User Guide describes the web GUI's consent banner being configured through the System Configuration page. Section 4.2.1.1 of the User Guide describes the MDM Configuration options

for a policy which includes the 'App Use Consent Message' which will display a message on the login page of the GovShield Client. Together these satisfy how to 'configure the TOE unlock banner'.

Section 4.1.1 of the User Guide describes creating a policy which has Polling Interval, App Polling Interval, and Audit Log Publishing Rate as variables. Section 4.2.1.1 of the User Guide further describes the MDM Configuration options for a policy. This satisfies how to 'configure periodicity of the following commands to the agent: Polling Interval, App Polling Interval, Audit Log Publishing Rate'.

Section 9.2 of the User Guide describes enrollment which enables communications between the GovShield Client and GovShield Server. Sections 2.5.1 and 2.5.2 of the User Guide describe actions which will result in unenrollment which disables communications between the GovShield Client and GovShield Server. Together these satisfy how to 'configure the interaction between TOE components'.

[MDMPP] FMT_SMF.1(3) – *"The evaluator shall confirm that the operational guidance contains how to create and define user groups and how to specify which applications are accessible by which group.*

The evaluator shall verify the AGD guidance includes detailed instructions of what options are available and how to configure each management functional capability listed."

Section 4.1 of the User Guide describes that each device is assigned a single policy upon the device's enrollment and that a device can only have one policy assigned. Section 2.2 of the User Guide describes the ability to manage the policy to which the device is assigned. Section 5 of the User Guide describes the ability to manage applications, including the ability to assign an application to a policy and select whether or not to install the application on the device. Section 5 also includes directions to change the APK file which covers an update to the application. Together these actions create an application access group for each policy. An application access group is the set of Android Mobile Devices which have been assigned to a policy and the applications available to those devices is determined by the applications that are also assigned to the same policy.

[AGENTMOD] FMT_SMF_EXT.4 – *"The evaluator shall verify the AGD guidance includes detailed instructions for configuring each function in this requirement.*

If the MDM Agent is a component of the MDM system (i.e. MDM Server is the Base-PP), the evaluator shall verify, by consulting documentation for the claimed mobile device platforms, that the configurable functions listed for this Agent are supported by the platforms.

If the MDM Agent supports multiple interfaces for configuration (for example, both remote configuration and local configuration), the AGD guidance makes clear whether some functions are restricted to certain interfaces."

Section 9.2 of the User Guide describes enrollment which includes the actions the Administrator needs to take within the web GUI, the user or the Administrator need to take on the GovShield Client, and provides information on the enrollment process to include providing a certificate to the GovShield Client for secure communications with GovShield Server. This satisfies 'Import the certificates to be used for authentication of MDM Agent communications' and 'Enroll in management' functions in this requirement.

Section 4.2.2.1 of the User Guide describes configuring the Restrictions section of a device policy, including having 'Admin Removal' unchecked which will prevent unenrollment. The evaluated configuration of the TOE does not allow users to unenroll the Agent from management. This satisfies 'Configure whether users can unenroll from management' function in this requirement.

Section 1 of the User Guide contains a table which lists all of the administrator-provided device management functions that may or may not be claimed by the underlying mobile device platform evaluation (VID11593). For each function listed in the table, it specifies under the "Claimed in VID11593" column "Yes" if claimed and "No" if not claimed by the underlying mobile device platform evaluation. For

functions where the value is "Yes", the fact that it was evaluated as part of the mobile device platform evaluation means that it is supported by the platform. The evaluation team confirmed all Yes statements by reviewing the mobile device's Security Target. For functions where the value is "No", mobile device documentation which covers the function or a justification explaining why it would not be covered in the mobile device documentation is listed below:

- 5. query connectivity status - https://developer.android.com/reference/android/net/ConnectivityManager
- 6. query the current version of the MD firmware/software - https://developer.android.com/reference/android/os/Build
- 7. query the current version of the hardware model of the device - https://developer.android.com/reference/android/os/Build
- 8. query the current version of installed mobile applications – https://developer.android.com/reference/android/content/pm/PackageManager
- 16. alert the user – https://developer.android.com/reference/android/app/NotificationManager#notify(int,%20android.app.Notification)
- 33. enable/disable policy for data signaling over USB and/or removable storage card (SD card) - https://developer.android.com/reference/android/os/UserManager#DISALLOW_USB_FILE_TRANSFER
- 34. enable/disable policy for Wi-Fi tethering – https://docs.samsungknox.com/devref/knox-sdk/reference/com/samsung/android/knox/restriction/RestrictionPolicy.html#setTethering(boolean)
- 51. enable/disable Hotspot functionality authenticated by passcode - https://developer.android.com/reference/android/os/UserManager#DISALLOW_CONFIG_TETHERING
- 58. enable/disable automatic updates of system software - https://docs.samsungknox.com/devref/knox-sdk/reference/com/samsung/android/knox/restriction/RestrictionPolicy.html#allowOTAUpgrade(boolean)

Section 1 of the User Guide states that all administration of GovShield is performed through the web GUI. As such, the MDM Agent is only configurable via the web GUI. There are no other interfaces over which the MDM Agent is configurable.

[MDMPP] FMT_SMR.1.1(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FMT_SMR.1.2(1) – *"The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE and which interfaces are supported."*

Section 1 of the User Guide provides instructions for administering the TOE via the web GUI which is the only supported administrative interface. Section 3 of the User Guide describes creating a user with the Admin role, which is the only role which can administer the TOE.

[MDMPP] FMT_SMR.1.1(2) – There are no AGD assurance activities for this SFR.

[MDMPP] FMT_SMR.1.2(2) – *"The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE and which interfaces are supported."*

Section 1 of the User Guide provides instructions for administering the TOE via the web GUI which is the only supported administrative interface. Section 3 of the User Guide describes creating a user with the Admin role, which is the only role which can administer the TOE.

[AGENTMOD] FMT_UNR_EXT.1 – *"The evaluator shall ensure that the administrative guidance instructs administrators in configuring the unenrollment prevention in each available configuration*

interface. If any configuration allows users to unenroll, the guidance also describes the actions that unenroll the Agent."

Section 4.2.2.1 of the User Guide describes configuring the Restrictions section of a device policy, including having 'Admin Removal' unchecked which will prevent unenrollment. The evaluated configuration of the TOE does not allow users to unenroll the Agent from management.

[MDMPP] FPT_API_EXT.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FPT_ITT.1(2) – "*The evaluator shall confirm that the operational guidance contains instructions for establishing the communication paths for each supported method*."

Sections 2 and 3 of the Install Guide contain instructions for configuring the operating environment so that the TOE can use Java, JBoss, and the BSafe cryptographic library to perform all cryptographic services. The instructions include prerequisites for the entire TOE's underlying platform, configuration of Java and JBoss, and specifications of the certificates files.

[MDMPP] FPT_LIB_EXT.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FPT_TST_EXT.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FPT_TUD_EXT.1.1 – *"The evaluator shall ensure that the administrator guidance includes instructions for determining the current version of the TOE."*

Section 9.3 of the User Guide describes checking the current version of the TOE within the web GUI's System Settings menu, and specifically for a GovShield Client within its About popup. Section 2.2 of the User Guide describes checking the current version of the installed applications on a device through the web GUI, which would include the TOE's GovShield Client.

[MDMPP] FPT_TUD_EXT.1.2 – There are no AGD assurance activities for this SFR.

[MDMPP] FPT_TUD_EXT.1.3 – *"The evaluator shall examine the AGD guidance to verify that it describes how to query the current version of the TSF software, how to initiate updates and how to check the integrity of updates prior to installation."*

Section 9.3 of the User Guide describes checking the current version of the TOE within the web GUI's System Settings menu, and specifically for a GovShield Client within its About popup. Section 2.2 of the User Guide describes checking the current version of the installed applications on a device through the web GUI, which would include the TOE's GovShield Client. Section 4 of the Install Guide describes the process for initiating an update to the MDM.ear software file which is the GovShield Server and the process of Java verifying the digital signature of the GovShield Server software update.

Section 5 of the User Guide describes the use of the TOE's application management functionality to update the GovShield Client on mobile devices. This process includes the ability of the administrator to initiate the update by selecting to install the application on the device and describes that the integrity of the app is checked via digital signature by the mobile device prior to installation.

[MDMPP] FTA_TAB.1 – *"The evaluator follows the operational guidance to configure a notice and consent warning message."*

Section 9.1.2 of the User Guide describes the web GUI's consent banner being configured through the System Configuration page. Section 4.2.1.1 of the User Guide describes the MDM Configuration options for a policy which includes the 'App Use Consent Message' which will display a message on the login page of the GovShield Client.

[MDMPP] FTP_ITC_EXT.1 – There are no AGD assurance activities for this SFR.

[MDMPP] FTP_ITC.1.1(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FTP_ITC.1.2(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FTP_ITC.1.3(1) – *"The evaluator shall confirm that the operational guidance contains instructions for configuring the communication channel between the MDM Server and authorized IT entities for each supported method."*

Sections 2 and 3 of the Install Guide contain instructions for configuring the operating environment so that the TOE can use Java, JBoss, and the BSafe cryptographic library to perform all cryptographic services. The instructions include prerequisites for the entire TOE's underlying platform, configuration of Java and JBoss, and specifications of the certificates files.

[MDMPP] FTP_TRP.1.1(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FTP_TRP.1.2(1) – There are no AGD assurance activities for this SFR.

[MDMPP] FTP_TRP.1.3(1) – *"The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method."*

Section 1 of the User Guide describes using a web browser and entering the GovShield Server's URL to establish the remote administrative session. Section 1 of the User Guide also states that this is the only method of administering GovShield.

[MDMPP] FTP_TRP.1.1(2) – There are no AGD assurance activities for this SFR.

[MDMPP] FTP_TRP.1.2(2) – There are no AGD assurance activities for this SFR.

[MDMPP] FTP_TRP.1.3(2) – *"The evaluator shall confirm that the operational guidance contains instructions for establishing the enrollment sessions for each supported method."*

Section 9.2 of the User Guide describes enrollment which includes the actions the Administrator needs to take within the web GUI as well as the user or the Administrator need to take on the GovShield Client. These actions include the generation and subsequent scanning of a QR code. Within the QR code is an embedded URL for the GovShield Server. The GovShield Client will record the URL of the GovShield Server during a successful enrollment of the Android Mobile Device. The URL will then be used as the GovShield Server's reference identifier for subsequent communications between the GovShield Client and GovShield Server.

4 Test Assurance Activities (Test Report)

The following sections demonstrate that all ATE Assurance Activities for the TOE have been met. This evidence has been presented in a manner that is consistent with the "Reporting for Evaluations Against NIAP-Approved Protection Profiles" guidance that has been provided by NIAP. Specific test steps and associated detailed results are not included in this report in order for it to remain non-proprietary. The test report is a summarized version of the test activities that were performed as part of creating the Evaluation Technical Report (ETR).

The evaluation team conducted testing activities between January 2024 and April 2026. Testing was conducted at the Booz Allen CCTL in Laurel, MD on an isolated network.

4.1 Platforms Tested and Composition

Evaluator-conducted manual testing was completed in April 2026. The evaluation team set up a test environment for the independent functional testing that allowed them to perform all test assurance activities against the GovShield Version 1.60.05 over the SFR relevant interfaces.

All required test assurance activities were performed against the TOE for the two components GovShield (GovShield Server) and GovShield Client (Android 15 mobile device) that were claimed in the Security Target. Multiple GovShield Clients were used during testing to ensure that the addition of Android mobile devices did not introduce any changes of behavior or security claims made in the Security Target.

The evaluation team performed testing of the TSF functionality across the claimed components as well as the GovShieldWeb MDM Server administrative interface. The full set of tests were developed to stimulate each applicable TSF relevant interface; which would fully test all combinations of the claimed platforms and their TSF relevant interfaces. The testing is consistent with the use of the interfaces defined within the ST. Thus, the testing of the interfaces was based upon testing SFR functionality related to user actions over each interface.

4.1.1 Test Configuration

The evaluation team conducted testing at the Booz Allen CCTL in Laurel, MD on an isolated network. The evaluation team configured the TOE for testing according to the *GovShield Installation Guide, Version 1.0 and GovShield User Guide, Version 1.0* (AGD) documents. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces.

ESXi 8.0.3 host server

The GovShield Server platform operating environment:

- ESXi 8.0.3
- Microsoft Windows 2022
- OpenJDK 11
- JBoss Enterprise Application Platform 7.4

The GovShield Server was configured to communicate with the following environment components:

- Oracle Database 19 (GovShieldDB) using TLS
- CA Servers (GovShieldRootCA, GovShieldRootIntermediateCA, GovShieldCA)
- Administrator Workstation to access GovShieldWeb administrative interface (HTTPS/TLS)
- Samsung Android Mobile Devices

The GovShield Client platform operating environment:

- Samsung Android Mobile Devices
    - Galaxy Tab Active5
    - Android 15

The GovShield Client was configured to communicate with the following environment components:

- Samsung Knox Licensing Server
- Samsung Knox Enterprise Firmware-over-the-air (E-FOTA) Server
- CA Servers (GovShieldRootCA, GovShieldRootIntermediateCA, GovShieldCA)

Operational Components:

- Function: Switch
    - Model: Cisco Catalyst WS-C Switch, WS-C3560X-24P

  - OS: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 12.2(55)SE3
  - Protocols: N/A

- Function WAP
  - Model: UniFi PRO Wireless Access Point (WAP)
  - Firmware: 4.0.27.10067

- Function: GovShieldRootCA, GovShieldIntermediateCA, GovShieldCA
  - ESXi server 8.0.3
  - OS: Red Hat Enterprise Linux 8.4 (Ootpa)

- Function Oracle Database Server
  - ESXi 8.0.3
  - Microsoft Windows Server 2022 Standard 10.0.20348 Build 20349
  - Oracle SQL*Plus: Release 19.0.0.0.0 - Production on Sun Feb 22 17:18:22 2026 Version 19.3.0.0.0
- Administrator Workstation
  - ESXi 8.0.3
  - Microsoft Windows 2022
  - OpenJDK 11
  - JBoss Enterprise Application Platform 7.4

The following test tools were installed in the operational environment on multiple test workstations and servers for testing purposes:

- OpenSSL 1.1.1n 15 Mar 2022 (Library: OpenSSL 1.1.1k 25 Mar 2021)
- Wireshark 4.6.4
- Oracle SQL*Plus: Release 19.0.0.0.0 - Production on Sun Feb 22 17:18:22 2026 Version 19.3.0.0.0
- ZenMap 7.90
- tcpdump 4.99.0 and 4.9.3

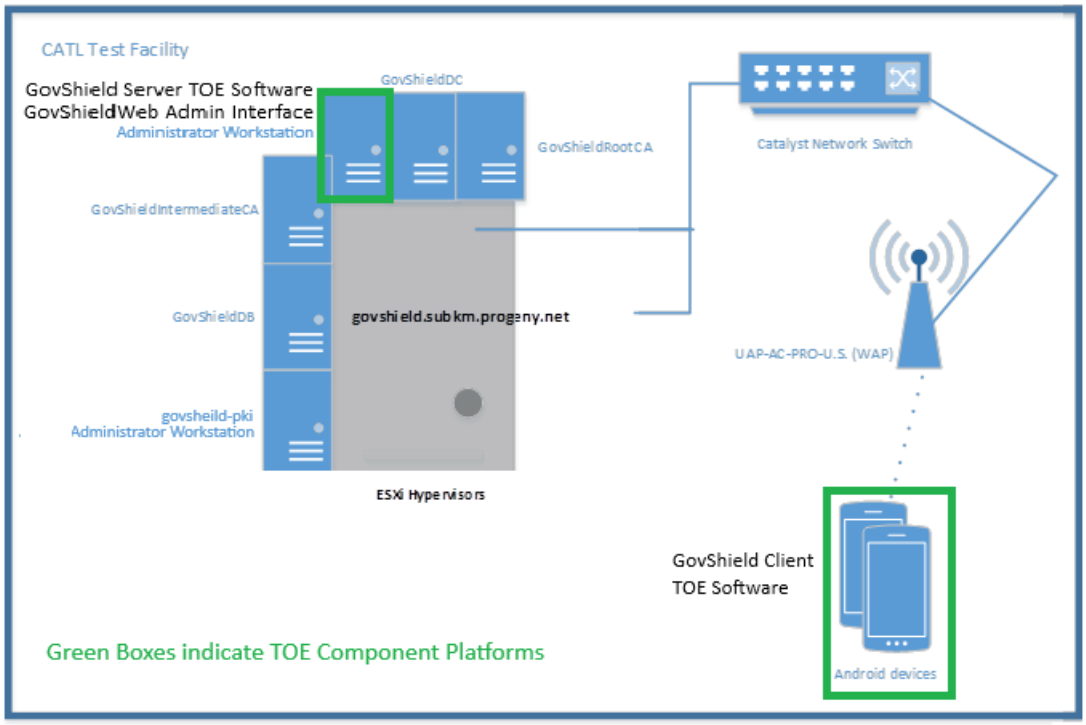

Figure 1 - Test Configuration

4.2 Omission Justification

There were no testing omissions because there was no sampling of testing, as all required test assurance activities were performed against the TOE as claimed in the Security Target.

4.3 Test Cases

The evaluation team conducted a set of testing that includes all ATE Assurance Activities as specified by the *Protection Profile for Mobile Device Management Version 4.0, April 25, 2019 [MDMPP] and PP-Module for MDM Agent Version 1.0, April 25, 2019 [AGENTMOD].* The evaluators reviewed the MDMPP and AGENTMOD to identify the security functionality that must be verified through functional testing. This is prescribed by the Assurance Activities for each SFR.

If an SFR is not listed, one of the following conditions applies:

- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a test Assurance Activity for a different SFR.
- The Assurance Activity for the SFR does not specify any actions related to ATE activities (e.g. FCS_RBG_EXT.1).

Note that some SFRs do not have Assurance Activities associated with them at the element level (e.g. FMT_SMR.1.1(1)). In such cases, testing for the SFR is considered to be satisfied by completion of all Assurance Activities at the component level.

The following lists for each ATE Assurance Activity, the test objective, test instructions, test steps, and test results. Note that unless otherwise specified, the test configuration is to be in the evaluated configuration as defined by the AGD. For example, some tests require the TOE to be brought out of the evaluated

configuration to temporarily disable cryptography to prove that the context of transmitted data is accurate. As part of the cleanup for each test, the TOE is returned to the evaluated configuration.

4.3.1 Security Audit

Test Case Number	001
SFR	[MDMPP]FAU_ALT_EXT.1.1 – Server Alerts – Test 1
Test Objective	For each MDM Agent/platform listed as supported in the ST: Test 1: The evaluator shall enroll a device and ensure that the MDM server alerts the administrator of the change in enrollment status. The evaluator shall unenroll (retire) a device and ensure that the MDM server alerts the administrator of the change in enrollment status.
Test Instructions	Execute this test per the test steps.
Test Steps	***Enrollment:*** 1. Enroll the mobile device to the MDM system by following the procedures in [MDMPP]FIA_ENR_EXT.1.1 – Test Case 024. 2. Verify that the MDM server alerts the administrator of the device enrollment. ***Unenrollment:*** 3. Unenroll the mobile device from the MDM system. a. Navigate to “Device Management”. b. Choose the specific Device to unenroll from management under the “Device ID” column. c. On the bottom toolbar, choose “Actions” > “Wipe Device”. d. Confirm the unenroll request. e. Verify that the device has been unenrolled from management. 4. Verify that the MDM server alerts the administrator of the device unenrollment.
Test Results	Enrollment: The evaluator confirmed that when a mobile device is successfully enrolled, the MDM agent generated an alert message about the change of status. The alert message was received by the MDM server and the receipt of the alert was audited by the MDM server. The successful enrollment was indicated in the Device Management page with a line displaying the information about the mobile device. Unenrollment: The evaluator confirmed that when a mobile device was successfully unenrolled (equivalent to wiping the device), the MDM agent generated an alert message about the change of status. The successful unenrollment of the device was indicated in the Device Management page by the removal of the device from the display. Verdict: Pass
Execution Method	Manual

Test Case Number	002
SFR	[MDMPP]FAU_ALT_EXT.1.1 – Server Alerts – Test 2
Test Objective	For each MDM Agent/platform listed as supported in the ST: Test 2: The evaluator shall configure policies, which the MDM agent should not be able to apply. These policies shall include: • a setting which is configurable on the MDM Server interface but not supported by the platform on which the MDM Agent runs, if any such settings exist • a valid configuration setting with an invalid parameter, which may require manual modification of the policy prior to transmission to the device The evaluator shall deploy such policies and verify that the MDM server alerts the administrator about the failed application of the policy.
Test Instructions	Execute this test per the test steps.
Test Steps	***A setting which is configurable on the MDM Server interface but not supported by the platform on which the MDM Agent runs:*** **This portion of this assurance activity is not applicable because no such setting exists. All Android devices claimed by this evaluation can process all policy settings claimed by this evaluation which are configured on the MDM Server.** ***A valid configuration setting with an invalid parameter, which may also require manual modification of the policy prior to transmission to the device:*** 1. Authenticate to the MDM Server Web UI as the Administrator. a. Navigate to "Policies". b. Add a new Bluetooth Profile (FAKE). 2. Wait for the MDM agent to check in with the MDM server. 3. Verify that the policy failed to apply due to a valid configuration setting with an invalid parameter.
Test Results	The evaluator confirmed that there are no setting which are configurable on the MDM Server interface that are not supported by the platform on which the MDM Agent run. The evaluator confirmed that when a policy with an invalid parameter set was sent to the mobile device, the MDM agent did not implement the policy. The MDM agent generated and sent an alert message indicating the failure to apply the policy. The alert message was received by the MDM server. Verdict: Pass
Execution Method	Manual

Test Case Number	003
SFR	[MDMPP]FAU_ALT_EXT.1.1 – Server Alerts – Test 3
Test Objective	For each MDM Agent/platform listed as supported in the ST: Test 3: (Conditional) The evaluator shall trigger each of the events listed and ensure that the MDM Server alerts the administrator.
Test Instructions	Execute this test per the test steps.
Test Steps	***Last time a device performed a policy reachability event with the MDM Server:***

	1. Wait the configured interval for an enrolled device to perform a policy reachability check with the MDM server. 2. Verify that the MDM administrator is alerted when a device performs a policy reachability check. 3. Verify that the audit record(s) for the device performing a policy reachability check is generated. ***Failure to install an application from the MAS Server:*** 1. Authenticate to the MDM Server Web UI as the administrator. 2. Navigate to "APK Management" → "New". 3. Upload the unsigned MDM APK file. 4. Specify the Policy Bundle. 5. Specify "Device" to Install On. 6. Click "Add". 7. Observe that the application failed to install on the mobile device. 8. Verify that the MDM administrator is alerted of the failure to install the application. 9. Verify that the audit record for the application installation failure is generated. ***Failure to update an application from the MAS Server:*** 1. Authenticate to the MDM Server Web UI as the administrator. 2. Navigate to "APK Management" → "New". 3. Upload the signed MDM APK file. 4. Specify the Policy Bundle. 5. Specify "Device" to Install On. 6. Click "Add". 7. Observe that the application successfully installed on the mobile device. 8. Navigate to "APK Management" → "New". 9. Select and edit the APK that was uploaded in Step 3. 10. Check "Update APK". 11. Upload the unsigned update to the APK that was uploaded from Step 3. 12. Click "Update". 13. Observe that the application failed to install on the mobile device. 14. Verify that the MDM administrator is alerted of the failure to install the update to the application. Verify that the audit record for the failure to install the update to the application is generated.
Test Results	The evaluator confirmed that the MDM agent generated and sent alert messages for a network reachability event, the failure to install an application, and failure to update an application. These alerts were received by the MDM server. Verdict: Pass
Execution Method	Manual

Test Case Number	004
SFR	[AGENTMOD]FAU_ALT_EXT.2 – Agent Alerts – Test 1
Test Objective	Test 1: The evaluator shall perform a policy update from the test environment MDM server. The evaluator shall verify the MDM Agent accepts the update, makes the configured changes, and reports the success of the policy update back to the MDM Server.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the MDM Server Web UI. 2. Create a policy that disables the Camera: *a.* Navigate to "Policies". *b.* On the bottom toolbar, choose "New" > "Create". c. Specify the required fields on the "MDM Settings" tab and click "Device Policy". d. Ensure "Camera" is unchecked. e. Click "Save". 3. Verify via audit records that the mobile device reports that the policy update is successfully received and applied. 4. Verify policy was applied by attempting to use the Camera
Test Results	The evaluator confirmed that the MDM agent implemented the policy sent from the MDM server that disabled the camera permissions settings and allowed the camera application to remain. The evaluator confirmed that the camera usage was not allowed. The evaluator confirmed that the MDM agent generated and sent an alert message to the MDM server for the successful update and application of the policy. Verdict: Pass
Execution Method	Manual

Test Case Number	005
SFR	[AGENTMOD]FAU_ALT_EXT.2 – Agent Alerts – Test 2
Test Objective	Test 2: The evaluator shall perform each of the actions listed in FAU_ALT_EXT.2.1 and verify that the alert does in fact reach the MDM Server.
Test Instructions	Execute this test per the test steps.
Test Steps	***Successful application of policies to a mobile device:*** This is tested in [AGENTMOD]FAU_ALT_EXT.2 – Test Case 004. ***Generating periodic reachability events:*** This is tested in [AGENTMOD]FAU_ALT_EXT.2 – Test Case 006. ***Change in enrollment state:*** This is tested in [MDMPP]FAU_ALT_EXT.1.1 – Test Case 001. ***Failure to install an application from the MAS Server:*** This is tested in [MDMPP]FAU_ALT_EXT.1.1 – Test Case 003.

	Failure to update an application from the MAS Server: This is tested in [MDMPP]FAU_ALT_EXT.1.1 – Test Case 003.
Test Results	Each of the actions defined in FAU_ALT_EXT.2.1 are met by testing performed in other test cases. The evaluation confirmed that all of the referenced test cases were assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	006
SFR	[AGENTMOD]FAU_ALT_EXT.2 – Agent Alerts – Test 3
Test Objective	Test 3: The evaluator shall configure the MDM Agent to perform a network reachability test, both with and without such connectivity and ensure that results reflect each.
Test Instructions	Execute this test per the test steps.
Test Steps	***With Connectivity:*** 1. Ensure the mobile device is connected to the network. 2. Wait the configured time interval for the enrolled mobile device to perform a network reachability operation. 3. Verify that the time difference between "Reachability Events" reflects the value configured for the applied policy. ***Without Connectivity:*** 1. Place the mobile device into Airplane Mode. 2. Wait the configured time interval for the enrolled mobile device to perform a network reachability operation. 3. Verify that the "Last Contacted" timestamp is not updated from the timestamp that was recorded when connectivity was available. 4. Disable Airplane Mode on the mobile device. 5. Verify that audit records are generated for the failure of the MDM agent sending the reachability alert to the MDM server.
Test Results	The evaluator confirmed that the MDM Agent generated and sent a network reachability event alert message to the MDM Server for a Successful check in (when a connection was already established) and a failed check in (when a network connection was not established) after the connection was restored. Verdict: Pass
Execution Method	Manual

Test Case Number	007
SFR	[AGENTMOD]FAU_ALT_EXT.2 – Agent Alerts
Test Objective	Test 4: The evaluator shall remove network connectivity from the MDM Agent and generate an alert/event as defined in FAU_ALT_EXT.2.1. The evaluator shall restore network connectivity to the MDM Agent and verify that the alert generated

	while the TOE was disconnected is sent by the MDM Agent upon re-establishment of the connectivity.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Place the mobile device into Airplane Mode. 2. Wait the configured time interval for the enrolled mobile device to perform a network reachability operation. 3. Disable Airplane Mode on the mobile device. 4. Verify that audit records are generated for the failure of the MDM agent sending the reachability alert to the MDM server.
Test Results	The evaluator confirmed that the MDM Agent generated and sent a network reachability event alert message to the MDM Server for a Successful check in (when a connection was already established) and a failed check in (when a network connection was not established) after the connection was restored. Verdict: Pass
Execution Method	Manual

Test Case Number	008
SFR	[MDMPP]FAU_GEN.1.1(1) – Audit Data Generation
Test Objective	The evaluator shall test the TOEs ability to correctly generate audit records by having the TOE generate audit records for the events listed in the provided table and administrative actions. This should include all instances of an event. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. For administrative actions, the evaluator shall test that each action determined by the evaluator above to be security relevant in the context of this PP is auditable. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.
Test Instructions	Execute this test per the test steps.
Test Steps	The TOE's ability to generate audit records for each of the events listed in Table 13 from the Security Target, including all administrative actions is tested in conjunction with the testing of the security mechanism directly.
Test Results	The evaluator confirmed that all required audit records were generated by the MDM Server. The evaluator also confirmed that the audit records contained all required information as specified in the Security Target, including the Device ID (if applicable), Server Name (MDM server), Event Type, Success/Failure, Date and Time, Subject Identity, and the defined additional information. Verdict: Pass
Execution Method	Manual

Test Case Number	009
SFR	[MDMPP]FAU_GEN.1.2(1) – Audit Data Generation
Test Objective	When verifying the test results from FAU_GEN.1.1(1), the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

	Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected. The Auditable Events table includes optional, selection-based and objective requirements. The auditing of these requirements are only required if the requirement is included in the ST. (Refer to Table 13 in the Security Target for the Server Auditable Events table)
Test Instructions	Execute this test per the test steps.
Test Steps	The TOE's ability to generate audit records, in the format specified per the AGD (with each field having the proper entries), for each of the events listed in Table 13 from the Security Target, including all administrative actions is tested in conjunction with the testing of the security mechanism directly.
Test Results	The valuator confirmed that all required audit records were generated by the MDM Server. The evaluator also confirmed that the audit records contained all required information as specified in the Security Target, including the Device ID (if applicable), Server Name (MDM server), Event Type, Success/Failure, Date and Time, Subject Identity, and the defined additional information. Verdict: Pass
Execution Method	Manual

Test Case Number	010
SFR	[MDMPP]FAU_GEN.1.1(2) – Audit Generation (MAS Server)
Test Objective	The evaluator shall verify that when an application or update push fails, that the audit records generated match the format specified in the guidance and that the fields in each audit record have the proper entries.
Test Instructions	Execute this test per the test steps.
Test Steps	This test was run in conjunction with [AGENTMOD]FAU_ALT_EXT.2 - Test Case 005
Test Results	The evaluator confirmed that all required audit records were generated by the MAS Server (one in the same device as the MDM Server). The evaluator also confirmed that the audit records contained all required information as specified in the Security Target, including the Device ID (if applicable), Server Name (MAS server), Event Type, Success/Failure, Date and Time, Subject Identity, and the defined additional information. Verdict: Pass
Execution Method	Manual

Test Case Number	011
SFR	[MDMPP]FAU_GEN.1.2(2) – Audit Generation (MAS Server)
Test Objective	When verifying the test results from FAU_GEN.1.1(2), the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the

	security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.
Test Instructions	Execute this test per the test steps.
Test Steps	The TOE's ability to generate audit records, in the format specified per the AGD (with each field having the proper entries), for each of the events listed from [MDMPP] FAU_GEN.1.1(2), is tested in conjunction with the testing of the security mechanism directly.
Test Results	The evaluator confirmed that all required audit records were generated by the MAS Server (one in the same device as the MDM Server). The evaluator also confirmed that the audit records contained all required information as specified in the Security Target, including the Device ID (if applicable), Server Name (MAS server), Event Type, Success/Failure, Date and Time, Subject Identity, and the defined additional information. Verdict: Pass
Execution Method	Manual

Test Case Number	012
SFR	[AGENTMOD]FAU_GEN.1(2) – Audit Data Generation
Test Objective	The evaluator shall use the TOE to perform the auditable events defined in the Auditable Events table in FAU_GEN.1.1(2) and observe that accurate audit records are generated with contents and formatting consistent with those described in the TSS. Note that this testing can be accomplished in conjunction with the testing of the security mechanisms directly.
Test Instructions	Execute this test per the test steps.
Test Steps	The TOE's ability to generate audit records, in the format specified per the AGD (with each field having the proper entries), for each of the events listed from [AGENTMOD] FAU_GEN.1.1(2), is tested in conjunction with the testing of the security mechanism directly.
Test Results	The evaluator confirmed that all required audit records were generated by the Host agent. The evaluator also confirmed that the audit records contained all required information as specified in the Security Target, including the Device ID (if applicable), Server Name (MDM server), Event Type, Success/Failure, Date and Time, Subject Identity, and the defined additional information. Verdict: Pass
Execution Method	Manual

Test Case Number	013
SFR	[MDMPP]FAU_NET_EXT.1.1 – Network Reachability Review
Test Objective	For each MDM Agent/platform listed as supported in the ST: The evaluator shall configure the MDM Agent/platform to perform a network reachability test, both with and without such connectivity and shall ensure that by following the guidance, the evaluator can determine results that reflect both.
Test Instructions	Execute this test per the test steps.
Test Steps	***With Connectivity:***

	1. Ensure the mobile device is connected to the network. 2. Wait the configured time interval for the enrolled mobile device to perform a network reachability operation. 3. Verify that the "Last Contacted" timestamp is updated to the expected value on the Device Management tab on the MDM Server Web UI. ***Without Connectivity:*** 1. Place the mobile device into Airplane Mode. 2. Wait the configured time interval for the enrolled mobile device to perform a network reachability operation. 3. Verify that the "Last Contacted" timestamp is not updated from the timestamp that was recorded when connectivity was available.
Test Results	The evaluator confirmed that when the mobile device was active on the network the TOE performed it's check in with the MDM Server. When the connection was disrupted in a manner where the mobile device could not check in to the MDM server, the MDM server did not updated its last contacted listing. Once the connection was re-established the mobile device performed a check-in with the MDM server and the MDM server updated the Last Contacted date and time. Verdict: Pass
Execution Method	Manual

Test Case Number	014
SFR	[MDMPP]FAU_SAR.1.2 – Audit Review
Test Objective	The evaluator shall attempt to view the audit record as the authorized administrator and verify that the action succeeds. The evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Navigate to the MDM Server Web Console. 2. Authenticate as the administrator. 3. Attempt to view a sampling of audit records on the "Server Audit Log" page. 4. Verify that the audit records match the format specified in the administrative guide.
Test Results	The evaluator confirmed that each audit record had the following attributes: • date and time of the event [Date and Time] • type of event : [Event Type: Audit Log Received Display Device Log Data] • subject identity [compinstaller admin user or GovShield MDM Agent along with a Device ID] • (if relevant) the outcome (success or failure) of the event [Success: true] • additional information section [Additional Info:] Verdict: Pass
Execution Method	Manual

Test Case Number	015

SFR	[AGENTMOD]FAU_SEL.1(2) – Security Audit Event Selection
Test Objective	Test 1: For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.
Test Instructions	Execute this test per the test steps.
Test Steps	There is no specific configuration to turn on and off auditing on the TOE, thus the GovShield Client and its underlying platform will always perform auditing. However, an Authorized Administrator creates policies on the GovShield Server and will assign them to one or more Android Mobile Devices. These policies include requirements for the GovShield Client to generate audit records for the functionality configured in the policies. Once the GovShield Client receives and applies a policy requiring auditing, the GovShield Client will always generate the necessary audit records. Refer to FMT_SMF.1.1(1)_050_subtest12&13 for installing and removing apps for an example.
Test Results	There is no specific configuration to turn on and off auditing on the TOE, thus the GovShield Client and its underlying platform will always perform auditing. However, an Authorized Administrator creates policies on the GovShield Server and will assign them to one or more Android Mobile Devices. These policies include requirements for the GovShield Client to generate audit records for the functionality configured in the policies. Once the GovShield Client receives and applies a policy requiring auditing, the GovShield Client will always generate the necessary audit records. The evaluator was able to confirm the ability of an authorized administrator to view the audit logs from the GovShieldWeb interface's Server Audit Log, Device Alerts, and Audit Log pages. Verdict: Pass
Execution Method	Manual

Test Case Number	016
SFR	[AGENTMOD]FAU_SEL.1(2) – Security Audit Event Selection
Test Objective	Test 2: [conditional]: If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.
Test Instructions	Execute this test per the test steps.
Test Steps	N/A – The ST does not claim other attributes for this SFR.
Test Results	Pass
Execution Method	Manual

Test Case Number	017
SFR	[MDMPP]FAU_STG_EXT.1.1 – External Trail Storage
Test Objective	Testing of the trusted channel mechanism will be performed as specified in the associated evaluation activities for the particular trusted channel mechanism.

	The evaluator shall perform the following test for this requirement: Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Begin capturing packets with Wireshark between the MDM Server and the remote audit server. 2. Perform some activity on the TOE that causes audit records to be transmitted to the remote audit server. 3. Stop capturing packets with Wireshark. 4. Examine the packet capture and verify that the communications are not transmitted in plaintext. 5. On the remote audit server, verify the records generated during Step 2 are received successfully. 6. Record the name and version of the software used on the audit server.
Test Results	The evaluator confirmed the connection between the TOE and the remote audit server and found the communication channel was protected using TLS 1.2. The evaluator stimulated different events that would cause audit to be transferred including a login event. The credential "Password1!" used for the login event was searched within the .pcapng and was not found. At no time was there any data sent in the clear between the TOE and the remote audit server (Oracle Database). Audit server name / version: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production Version 19.3.0.0.0 Verdict: Pass
Execution Method	Manual

4.3.2 Communications

Test Case Number	018
SFR	[MDMPP]FCO_CPC_EXT.1.3 Component Registration Channel Definition – Test 1
Test Objective	Test 1: The evaluator shall confirm that an IT entity that is not currently a member of the distributed TOE cannot communicate with any component of the TOE until the non-member entity is enabled by an administrator for each of the non-equivalent TOE components that it is required to communicate with (non-equivalent TOE components are as defined in the minimum configuration for the distributed TOE)
Test Instructions	Execute this test per the test steps.
Test Steps	Refer to FIA_ENR_EXT.1.2 – Test Case 025: “Limit enrollment to specific devices by Android Device ID”. Test Case 025 verifies that an Android Agent that has not been enrolled cannot communicate with the MDM Server.
Test Results	The evaluator confirmed that the referenced test case was assigned a passing

	verdict. Verdict: Pass
Execution Method	Manual

Test Case Number	019
SFR	[MDMPP]FCO_CPC_EXT.1.3 – Component Registration Channel Definition – TD0594 – Test 2
Test Objective	The evaluator shall confirm that after enablement, an IT entity can communicate only with the components that it has been enabled for. This includes testing that the enabled communication is successful for the enabled component pair, and that communication remains unsuccessful with any other component for which communication is possible but has not been explicitly enabled. Some TOEs may set up the registration channel before the enablement step is carried out, but in such a case the channel must not allow communications until after the enablement step has been completed.
Test Instructions	Execute this test per the test steps.
Test Steps	Refer to FIA_ENR_EXT.1.1 – Test Case 024. Test Case 024 verifies that once the device is enrolled the MDM Server and the Android Agent can communicate.
Test Results	The evaluator confirmed that the referenced test case was assigned a passing verdict. Verdict: Pass
Execution Method	Manual

Test Case Number	020
SFR	[MDMPP]FCO_CPC_EXT.1.3 – Component Registration Channel Definition – TD0594 – Test 3
Test Objective	The evaluator shall separately disable each TOE component in turn and ensure that the other TOE components cannot then communicate with the disabled component, whether by attempting to initiate communications with the disabled component or by responding to communication attempts from the disabled component. In situations where one component acts as the "Gatekeeper" for all other components, the test would involve disabling the components in turn on the Gatekeeper and ensuring that the TOE no longer communicates with disabled components.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Unenroll and prevent the mobile device from reenrolling (disable re-enrollment) into MDM. a. Authenticate to the MDM Server Web UI as the Administrator. b. Command the specified mobile device to unenroll from management: i. Navigate to “Device Management”. ii. Select the device. iii. Select “Actions” > “Unenroll Device”. iv. Confirm the action. c. Navigate to “Device Management”. Ensure the Device ID of the unenrolled device is not present in the list of devices on the Device Management page.
Test Results	The evaluator confirmed that the Device with id "14525a35cafe49a3" was shown as "enrolled" because it is present in the "Device Management" page with

	characteristics that define the OS, OS Version, Model, Firmware, and Last Contacted information (top half of screen capture). Additionally, the evaluator observed that the absence of the device from the "Device Management" page demonstrated that the device had been unenrolled from management when the evaluator issued the wipe command. This unenrollment action disabled the MDM agent from communicating with the MDM server. Verdict: Pass
Execution Method	Manual

4.3.3 Cryptographic Support

All cryptographic services for the GovShield Version (1.60.05) are provided by the underlying platforms for the TOE components.

> [SERVER] Cryptographic services for the GovShield Server are provided by the underlying Java Runtime Environment Platform. The Java Runtime Environment Platform uses the BSafe cryptographic library to perform all cryptographic services.
>
> [AGENT] Cryptographic services for the GovShield Client is provided by the underlying Android mobile device platform. The GovShield Client uses the Android platform's BoringSSL cryptographic module to perform all claimed cryptographic services.

Only test cases for FCS_CKM_EXT.4 are included as these were conditional tests that required addressing.

Test Case Number	021
SFR	[MDMPP]FCS_CKM_EXT.4.2 – Cryptographic Key Destruction
Test Objective	For each software and firmware key clearing situation the evaluator shall repeat the following tests. Note that at this time hardware-bound keys are explicitly excluded from testing. Test 1: The evaluator shall utilize appropriate combinations of specialized operational environment and development tools (debuggers, simulators, etc.) for the TOE and instrumented TOE builds to test that keys are cleared correctly, including all intermediate copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key. Cryptographic TOE implementations in software shall be loaded and exercised under a debugger to perform such tests. The evaluator shall perform the following test for each key subject to clearing, including intermediate copies of keys that are persisted encrypted by the TOE: 1. Load the instrumented TOE build in a debugger. 2. Record the value of the key in the TOE subject to clearing. 3. Cause the TOE to perform a normal cryptographic processing with the key from #1. 4. Cause the TOE to clear the key. 5. Cause the TOE to stop the execution but not exit. 6. Cause the TOE to dump the entire memory footprint of the TOE into a binary file. 7. Search the content of the binary file created in #4 for instances of the known key value from #1.

	The test succeeds if no copies of the key from #1 are found in step #7 above and fails otherwise. The evaluator shall perform this test on all keys, including those persisted in encrypted form, to ensure intermediate copies are cleared.
Test Instructions	Execute this test per the test steps.
Test Steps	N/A – No ATE testing activities as "invoke platform-provided functionality" is selected in the Security Target.
Test Results	Pass
Execution Method	Manual

Test Case Number	022
SFR	[MDMPP]FCS_CKM_EXT.4.2 – Cryptographic Key Destruction
Test Objective	For each software and firmware key clearing situation the evaluator shall repeat the following tests. Note that at this time hardware-bound keys are explicitly excluded from testing. Test 2: In cases where the TOE is implemented in firmware and operates in a limited operating environment that does not allow the use of debuggers, the evaluator shall utilize a simulator for the TOE on a general purpose operating system. The evaluator shall provide a rationale explaining the instrumentation of the simulated test environment and justifying the obtained test results.
Test Instructions	Execute this test per the test steps.
Test Steps	N/A – No ATE testing activities as "invoke platform-provided functionality" is selected in the Security Target.
Test Results	Pass
Execution Method	Manual

4.3.4 Identification and Authentication

Test Case Number	023
SFR	[MDMPP]FIA_ENR_EXT.1.1 – Enrollment of Mobile Device into Management – Test 1
Test Objective	Test 1: The evaluator shall attempt to enroll a device without providing correct credentials. The evaluator shall verify that the device is not enrolled and that the described enrollment actions are not taken.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Power on the Android mobile device. 2. Join the mobile device to the test network. 3. Attempt to enroll the device using invalid credentials: a. Install the Android Agent onto the mobile device via QR code enrollment method. 4. Enter the Username created in the Setup and an invalid password. 5. On the MDM Server, authenticate and navigate to the "Device Management". 6. Verify that the device is not listed as "Enrolled" (i.e., "Policy Name, Policy Version, OS, OS Version, Model, Firmware, and Last Contacted" information is unknown or undefined).
Test Results	The evaluator confirmed that the mobile device did not successfully enroll into the MDM Swerver when incorrect credentials were supplied.

	Verdict: Pass
Execution Method	Manual

Test Case Number	024
SFR	[MDMPP]FIA_ENR_EXT.1.1 – Enrollment of Mobile Device into Management – Test 2
Test Objective	Test 2: The evaluator shall attempt to enroll the device providing correct credentials. The evaluator shall verify that the device is enrolled and that the described enrollment actions are taken
Test Instructions	Execute this test per the test steps.
Test Steps	1. Power on the Android mobile device. 2. Join the mobile device to the test network. 3. Attempt to enroll the device into MDM using valid credentials: a. Install the Android Agent onto the mobile device via QR code enrollment method. 4. Enter the Username and Password created in the Setup. 5. Verify enrollment to the MDM Server. 6. On the MDM Server, authenticate and navigate to “Device Management”. 7. Verify that the enrolled device is listed as “Enrolled” (i.e., “Policy Name, Policy Version, OS, OS Version, Model, Firmware, and Last Contacted” information is defined with the expected values).
Test Results	The evaluator confirmed the mobile device correctly enrolled to the MDM Server when correct credentials and the device ID was correct. The evaluator was able to observe the enrollment steps via the server audit and the device management page where the device was shown to have communicated with the MDM server showing the correct policy and version. Verdict: Pass
Execution Method	Manual

Test Case Number	025
SFR	[MDMPP]FIA_ENR_EXT.1.2 – Enrollment of Mobile Device into Management – Test 1
Test Objective	For each type of policy selected, the evaluator shall perform the following: Test 1: The evaluator shall attempt to configure the MDM Server according to the administrative guidance in order to prevent enrollment. The evaluator shall verify that the user cannot enroll a device outside of the configured limitation. (For example, the evaluator may try to enroll a disallowed device, or may try to enroll additional devices beyond the number allowed.)
Test Instructions	Execute this test per the test steps.
Test Steps	***Limit enrollment to specific devices by Android Device ID:*** 1. Authenticate to the MDM Server Web UI as the Administrator. 2. Navigate to “Device Management”. 3. Click “New”. 4. Specify the permitted Android Device ID. 5. Attempt to enroll a mobile device with a non-permitted Android Device ID.

	6. Verify that enrollment of the prohibited device is unsuccessful. 7. Remove enrollment restrictions that were created specifically for each subtest of this test.
Test Results	The evaluator confirmed that the mobile device did not successfully enroll into the MDM Swerver when incorrect device ID was provided (not correctly whitelisted). Verdict: Pass
Execution Method	Manual

Test Case Number	026
SFR	[AGENTMOD]FIA_ENR_EXT.2 – Agent Enrollment of Mobile Device into Management
Test Objective	The evaluator shall follow the operational guidance to establish the reference identifier of the MDM server on the MDM Agent and in conjunction with other evaluation activities verify that the MDM Agent can connect to the MDM Server and validate the MDM Server's certificate.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Enroll an Android mobile device into MDM. 2. Note the fully qualified domain name (FQDN) of the MDM Server. 3. On the Android device, launch the MDM Agent. 4. Navigate to "Configuration" from the hamburger menu. 5. Observe that the "MDM Web Service URL" is the reference identifier.
Test Results	The evaluator confirmed that the Host agent identifies the MDM server name as a URL within the Host agent's configuration page and is also included in the Alert messages. The evaluator also confirmed that the MDM server certificate used the same FQDN as was configured. The Host Agent successfully validated the MDM Server as indicated by the successful connection and successful enrollment. Verdict: Pass
Execution Method	Manual

Test Case Number	027
SFR	[MDMPP]FIA_UAU.1.2 – Timing of Authentication – Test 1
Test Objective	The evaluator shall perform the following tests: Test 1: The evaluator shall attempt to perform the prohibited actions before authentication. The evaluator shall verify the actions cannot be performed.
Test Instructions	Execute this test per the test steps.
Test Steps	MDM Server Web UI: 1. Attempt to navigate to a protected web resource within the MDM Server Web UI prior to authentication: Using a fresh instance Chrome/Explore web browser copy the below into the web browser address bar: https://govshieldweb.govshield.demo:8543/mdm/#?page=mdmSetting 2. Verify that the login screen is displayed vs the settings page.

	3. Press the ACCEPT button but do not provide credentials 4. Paste the above URL in address bar and hit return 5. Verify no advancement to the settings page occurs and the ACCEPTED button is still checked. 6. Press LOGIN button (with no credentials added) 7. Verify User is unauthorized alert displays and login page is still presented.
Test Results	The evaluator confirmed that an attempt to gain access to the GovShieldWeb interface by a user providing no credentials was prohibited. This attempt include trying to access the page directly without using the login page and via the login page after accepting the banner and providing no credentials. Verdict: Pass
Execution Method	Manual

Test Case Number	028
SFR	[MDMPP]FIA_UAU.1.2 – Timing of Authentication – Test 2
Test Objective	The evaluator shall perform the following tests: Test 2: The evaluator shall attempt to perform the prohibited actions after authentication. The evaluator shall verify the actions can be performed.
Test Instructions	Execute this test per the test steps.
Test Steps	***MDM Server Web UI:*** 1. Attempt to navigate to a protected web resource within the MDM Server Web UI prior to authentication: Using a fresh instance Chrome/Explore web browser copy the below into the web browser address bar: https://govshieldweb.govshield.demo:8543/mdm/#?page=mdmSetting 2. Verify that the login screen is displayed vs the settings page. 3. Press the ACCEPT button and then provide correct credentials 4. Press LOGIN button (with no credentials added) 5. Verify that the settings page is displayed
Test Results	The evaluation confirmed access to the GovShieldWeb interface was granted only after the evaluator supplied correct credentials was the MDM server settings page displayed. Only users with Admin roles are allowed access to the GovShieldWeb interface. Therefore, there are no prohibited actions to be able to perform. Verdict: Pass
Execution Method	Manual

Test Case Number	029
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 1 – TD0641
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in

	conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 1: The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing, for each of the following reasons, in turn: • by establishing a certificate path in which one of the issuing certificates is not a CA certificate, • by omitting the basicConstraints field in one of the issuing certificates, • by setting the basicConstraints field in an issuing certificate to have CA=False, • by omitting the CA signing bit of the key usage field in an issuing certificate, and • by setting the path length field of a valid CA field to a value strictly less than the certificate path. The evaluator shall then establish a valid certificate path consisting of valid CA certificates, and demonstrate that the function succeeds. The evaluator shall then remove trust in one of the CA certificates, and show that the function fails.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	030
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 2 – TD0641
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	031
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 3 – TD0641

Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 3: The evaluator shall test that the TOE can properly handle revoked certificates--conditional on whether CRL, OCSP, OCSP stapling, or certificate status lookup is selected; if multiple methods are selected, then a test shall be performed for each method. The evaluator shall test revocation of the node certificate and revocation of the intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA). If OCSP stapling per RFC 6066 is the only supported revocation method, testing revocation of the intermediate CA certificate is omitted. For FIA_X509_EXT.1.1(2) if included, if "no revocation method" is selected, this test is omitted. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails, if "internal lookup of TOE-managed certificate status" is selected, then the evaluator shall follow AGD guidance to report the certificate as invalid.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as “invoke platform-provided functionality” is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	032
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 4 – TD0641
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 4: [conditional] If OCSP option is selected, the evaluator shall send the TOE an OCSP response signed by a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall cause a CA to sign a CRL with a certificate that has a key usage extension but does not have the cRLsign key usage bit set, and verify that validation of the CRL fails. If certificate status lookup is selected, this test is omitted. For FIA_X509_EXT.1.1(2) if included, if "no revocation method" is selected, this test is omitted.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as “invoke platform-provided functionality” is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.

Test Results	Pass
Execution Method	Manual

Test Case Number	033
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 5 – TD0641
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 5: The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	034
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 6 – TD0641
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 6: The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	035
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 7 – TD0641
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in

	FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	036
SFR	[MDMPP]FIA_X509_EXT.1.1(1) – X.509 Certificate Validation – Test 8 – TD0641
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including each of the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least three certificates: the node certificate to be tested, an Intermediate CA, and the self-signed Root CA. Test 8a: (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall establish a valid, trusted certificate chain consisting of an EC leaf certificate, an EC Intermediate CA certificate not designated as a trust anchor, and an EC certificate designated as a trusted anchor, where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain. Test 8b: (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall replace the intermediate certificate in the certificate chain for Test 8a with a modified certificate, where the modified intermediate CA has a public key information field where the EC parameters uses an explicit format version of the Elliptic Curve parameters in the public key information field of the intermediate CA certificate from Test 8a, and the modified Intermediate CA certificate is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	037
SFR	[MDMPP]FIA_X509_EXT.1.2(1) – X.509 Certificate Validation – Test 1
Test Objective	The tests described must be performed in conjunction with the other certificate

	services evaluation activities, including the functions in FIA_X509_EXT.2.1. The evaluator shall create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. Test 1: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOEs certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	038
SFR	[MDMPP]FIA_X509_EXT.1.2(1) – X.509 Certificate Validation – Test 2
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The evaluator shall create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. Test 2: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOEs certificate has the cA flag in the basicConstraints extension not set. The validation of the certificate path fails.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	039
SFR	[MDMPP]FIA_X509_EXT.1.2(1) – X.509 Certificate Validation – Test 3
Test Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The evaluator shall create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. Test 3: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOEs certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.
Test Instructions	Execute this test per the test steps.
Test Steps	This test assurance activity is met by the underlying platform as "invoke platform-provided functionality" is specified for the MDM Server component in the Security Target. Therefore, this test assurance activity does not apply for this TOE component.
Test Results	Pass
Execution Method	Manual

Test Case Number	040
SFR	[MDMPP]FIA_X509_EXT.2.2 – X.509 Certificate Validation – Test 1
Test Objective	The evaluator shall perform the following test for each trusted channel: Test 1: The evaluator shall demonstrate use of a valid certificate requiring certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.
Test Instructions	Execute this test per the test steps.
Test Steps	**MDM Server to Environmental Entity (e.g. audit server/database) (TLS):** 1. Begin capturing packets from the MDM server. 2. Perform an action that causes the MDM server to initiate a TLS connection to the environmental entity. 3. Verify the connection from the MDM server to the environmental entity is successful. 4. Stop capturing packets from the OCSP responder server. 5. Stop capturing packets from the MDM server. 6. Disconnect the connection between the MDM Server and the OCSP responder. 7. Begin capturing packets from the MDM server. 8. Perform an action that causes the MDM server to initiate a TLS connection to the environmental entity. 9. Verify the connection from the MDM server to the environmental entity is unsuccessful. 10. Stop capturing packets. **MDM Agent to MDM Server (TLS):** 1. Begin capturing packets between the mobile device, CRL distribution point, and MDM server hosts. 2. Perform an action that causes the MDM Agent to initiate a TLS connection to the MDM Server. 3. Verify the connection from the MDM Agent to the MDM Server is successful. 4. Stop capturing packets. 5. Disconnect the connection between the MDM Agent and the CRL distribution point. 6. Begin capturing packets from the CRL distribution point. 7. Begin capturing packets from the MDM server.

	8. Perform an action that causes the MDM Agent to initiate a TLS connection to the MDM Server.
	9. Verify the connection from the MDM Agent to the MDM Server is unsuccessful.
	10. Stop capturing packets.
	
	MDM Agent to MDM Server (Unable to verify Policy Signing):
	
	1. Disconnect the connection between the MDM Agent and the CRL distribution point.
	`iptables -A INPUT -i ens160 -s 10.137.2.10 -j DROP`
	`iptables -L -v -n --line-numbers`
	`iptables -D INPUT 1`
	2. Begin capturing packets from the CRL distribution point.
	3. From the MDM Server, configure a policy and transmit it to the mobile device.
	4. Verify the mobile device accepted the configured policy.
	5. After a few seconds, stop capturing packets from the CRL distribution point.
	6. Verify Device was unable to contact CRL distribution point.
	7. Verify Device created audit record showing unable to contact CRL distribution point.

Test Results	The evaluator confirmed that when the environment was configured so that the OCSP server was available the connection to the DB was successful. The evaluator then confirmed that when the environment was configured so that the OCSP server was not available, the connection to the DB was unsuccessful due to an unknown certificate. This is consistent with the ST claim that if the TOE cannot perform revocation checking the certificate is rejected and the TOE will terminate the session. Verdict: Pass
Execution Method	Manual

FIA_X509_EXT.5 is removed per TD0754. Therefore, Tests 41 and 42 are removed.

4.3.5 Security Management

Test Case Number	043
SFR	[MDMPP]FMT_MOF.1.1(1) – Management of Functions Behavior – Test 1
Test Objective	Test 1: The evaluator shall attempt to access the functions and policies in FMT_SMF.1(1) as an unauthorized user and verify that the attempt fails.
Test Instructions	Execute this test per the test steps.
Test Steps	Refer to [MDMPP]FIA_UAU.1.2 - Test 27 which proves that unauthorized users cannot access the mdmSettings page. MDM Server Web UI: 1. As a admin user login and go to the USERS page to display users and

	roles. 2. Verify that "user1" does not have admin rights. 3. Logout 4. Attempt to login as "user1" 5. Verify login attempts fails with a forbidden notice. 6. Using a fresh instance of Chrome/Explorer web browser, copy the ling into the address: https://govshieldweb.govshield.demo:8543/mdm/#?page=mdmSetting 7. Verify that the login screen is displayed vs the default mdmSettings page. If access is not granted: Stop and mark test as a Pass. If access is granted: Continue with below tests: 8. From within the Mobile Device Management Console: 9. Attempt to lock the device: See "Command the mobile device to transition to the locked state" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. 10. Attempt to perform a full wipe of protected data: See "Command the mobile device to perform a full wipe of protected data" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. 11. Attempt to unenroll the device from management: See "Command the device to unenroll from management" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. 12. Attempt to install new policies: See "Command the MDM Server to install new policies" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. 13. Attempt to query information from a device: See "Query the connectivity status of a device" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. 14. Attempt to wipe enterprise data: See "Wipe Enterprise data" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. 15. Attempt to define/create/install a device policy: See "Define a password length/complexity/lifetime" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. 16. Configure application access groups: See "Command the MDM Server to install new policies" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050 and [MDMPP]FMT_SMF.1.1(3) – Test Case 054. 17. Download applications: See "Install applications" in [MDMPP]FMT_SMF.1.1(1) – Test Case 050. Verify all attempts to execute the above 2-8 test steps fail.
Test Results	The evaluator confirmed that access was not granted to the GovShieldWeb interface to unauthorized users. No management functions were able to be

	accessed. Verdict: Pass
Execution Method	Manual

Test Case Number	044
SFR	[MDMPP]FMT_MOF.1.1(1) – Management of Functions Behavior – Test 2
Test Objective	Test 2: [conditional] The evaluator shall attempt to access the functions and policies in FMT_SMF.1(3) as an unauthorized user and verify that the attempt fails.
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in [MDMPP] FMT_MOF.1.1(1) – Test Case 043.
Test Results	The evaluator confirmed that access was not granted to the GovShieldWeb interface to unauthorized users. No management functions were able to be accessed. Verdict: Pass
Execution Method	Manual

Test Case Number	045
SFR	[MDMPP]FMT_MOF.1.1(2) – Management of Functions Behavior (Enrollment)
Test Objective	The test of this function is performed in conjunction with FIA_ENR_EXT.1.
Test Instructions	Execute this test per the test steps.
Test Steps	Refer to FIA_ENR_EXT.1.1 - Test Cases 023, 024, 025.
Test Results	Per the test assurance activity, management of enrollment behavior (valid / invalid authentication handling, limit enrollment to specific devices by Android device ID) is met by testing performed in FIA_ENR_EXT.1. The evaluator confirmed that the referenced test cases were assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	046
SFR	[MDMPP]FMT_MOF.1.1(3) – Management of Functions in (MAS Server Downloads)
Test Objective	The evaluator shall ensure that the MAS Server verifies that the mobile device is enrolled in the MDM Server and is in a compliant state. The evaluator shall verify that an application cannot be downloaded from the MAS Server prior to enrolling the device with the MDM. The evaluator shall partially enroll the mobile device, so the device is connected to the MDM Server, but is not compliant and verify that applications cannot be downloaded.
Test Instructions	Execute this test per the test steps.
Test Steps	**According to FMT_SMR.1(2) from the Security Target TSS, "The MAS Server is logically integrated with the GovShield Server." Therefore, when a device is not enrolled into the MDM Server, it is not possible to access or download applications from the MAS Server.**

	There is no concept of partial enrollment during the enrollment process. Therefore, the MDM Server has to believe the device state is being wiped while the device itself doesn't realize it has been issued a wipe command. This can be accomplished by delaying the time between the device check-in interval to a longer time period giving opportunity to issue the wipe command at the MDM Server had have the device recognize the command roughly 30 minute later. **Partially enrolled mobile device, not belonging to appropriate application access group** 1. Authenticate to the MDM Server Web UI as the administrator. 2. Create a policy which will extend the time period for the unenrollment execution by the device by increasing the "Server Communication interval" setting to 30 minutes. 3. Wait until mobile device implements the policy **Update/Install an application** 4. Go to the APK Management page and update an application assigned to policy 2. 5. Verify action by checking the Server Audit Log for the audit record with an event of New App Uploaded showing the name of the application installed/updated in step 4. **Unenroll mobile device** 6. Go to the Device Management page and select the correct device and issue the "Wipe" command. 7. Go to the Server Audit Log page and verify the Certificate Revoked audit record is present **On the mobile device** 8. Verify that the GovShield app is still installed **With Device having the GovShield app still installed and the MDM Server believes the Device is unenrolled, the Device is considered in a partially enrolled but non-compliant state** 9. Launch the GovShield app and attempt to login to force an update that would normally cause the application to be installed. 10. Verify that the application in Step 7 is not downloaded.
Test Results	The evaluator confirmed that an application was not downloaded to a mobile device from the MAS server prior to the mobile device being completely enrolled into the MDM Server. Verdict: Pass

Execution Method	Manual

Test Case Number	047
SFR	[MDMPP]FMT_POL_EXT.1.1 – Trusted Policy Update
Test Objective	The evaluator shall perform a policy update in accordance with FMT_SMF.1(1). The evaluator shall examine the policy either at the MDM Server, in transmission, or at the MDM agent, and verify the TSF signs the update and provides it to the MDM Agent..
Test Instructions	Execute this test per the test steps.
Test Steps	**Send a signed policy:** 1. Under the system configuration (gear) verify that the Disable Policy Signing is checked (meaning enabled) 2. Save 3. Create a policy test2 v2 and save the policy 4. Wait for the polling time (5 minutes) 5. Verify the device sends the Alert text notifying the administrator that the policy has been updated. **Send a unsigned policy:** 6. Under the system configuration (gear) verify that the Disable Policy Signing is checked (meaning disabled) 7. Save 8. Update policy test2 v2 and save the policy 9. Wait for the polling time (5 minutes) 10. Verify the device sends the Alert text notifying the administrator that the policy failed to update due to some form of a verification failure of digital signature. **Send a policy with a Fake signature:** 11. Under the system configuration (gear) verify that the Disable Policy Signing is unchecked (meaning enabled) and the Use Fake Private Key is selected (meaning the policy will be signed using a Fake signature) 12. Save 13. Update policy test2 v3 and save the policy 14. Wait for the polling time (5 minutes) 15. Verify the device sends the Alert text notifying the administrator that the policy failed to update due to some form of verification failure of digital signature.
Test Results	The evaluator confirmed that the MDM Server digitally signed the policy prior to providing the policy to the Host agent. Verdict: Pass
Execution Method	Manual

Test Case Number	048
SFR	[AGENTMOD]FMT_POL_EXT.2 – Agent Trusted Policy Update – Test 1
Test Objective	This evaluation activity is performed in conjunction with the evaluation activity for FIA_X509_EXT.1 and FIA_X509_EXT.2 as defined in the Base-PPs.

	Test 1: The evaluator shall perform a policy update from an available configuration interface (such as through a test MDM Server). The evaluator shall verify the update is signed and is provided to the MDM Agent. The evaluator shall verify the MDM Agent accepts the digitally signed policy
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in [MDMPP]FMT_POL_EXT.1.1 – Test Case 047.
Test Results	The evaluator confirmed that the Host agent validated the digital signature prior to implementing the policy. Verdict: Pass
Execution Method	Manual

Test Case Number	049
SFR	[AGENTMOD]FMT_POL_EXT.2 – Agent Trusted Policy Update – Test 2
Test Objective	This evaluation activity is performed in conjunction with the evaluation activity for FIA_X509_EXT.1 and FIA_X509_EXT.2 as defined in the Base-PPs. Test 2: The evaluator shall perform a policy update from an available configuration interface (such as through a test MDM Server). The evaluator shall provide an unsigned and an incorrectly signed policy to the MDM Agent. The evaluator shall verify the MDM Agent does not accept the digitally signed policy.
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in [MDMPP]FMT_POL_EXT.1.1 – Test Case 047.
Test Results	The evaluator confirmed that if the digital signature was deemed invalid or was missing, the MDM agent did not implement the policy and generated an Alert message and sent the alert message to the MDM Server. Verdict: Pass
Execution Method	Manual

Test Case Number	050
SFR	[MDMPP]FMT_SMF.1.1(1) – Specification of Management Functions (Server configuration of Agent)
Test Objective	For each MDM Agent/platform listed as supported in the ST: Test 1: The evaluator shall verify the ability to command each MDM Agent functional capability and configure each MDM Agent policy listed above.
Test Instructions	Execute this test per the test steps.
Test Steps	**1.** ***Command the mobile device to transition to the locked state:*** a. Ensure that the device is currently in an unlocked state. b. Navigate to “Device Management”. c. Choose the specific Device to transition to the locked state under the “Device ID” column. d. On the bottom toolbar, choose “Actions” > “Device Lock”. e. Confirm the device lock request. f. Verify that the device transitioned to the locked state.

	2. ***Command the mobile device to perform a full wipe of protected data:*** a. Refer to FAU_ALT_EXT.1.1 - Test Case 001 unenroll section. **3.** ***Command the device to unenroll from management:*** a. Refer to FAU_ALT_EXT.1.1 - Test Case 001 unenroll section. **4.** ***Command the MDM Server to install new policies:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab. d. Specify the desired configuration on the “Device Management” tab. e. Click “Save”. **5.** ***Query the connectivity status of a device:*** a. Navigate to “Device Management”. b. Select the device. c. Click “Update”. **6.** ***Query the current version of the device firmware/software:*** a. Navigate to “Device Management”. b. Select the device. c. Click “Update”. **7.** ***Query the current version of the device hardware model:*** a. Navigate to “Device Management”. b. Select the device. c. Click “Update”. **8.** ***Query the current version of the installed applications:*** a. Navigate to “Device Management”. b. Select the device. c. Click “Update”. d. Select the device and click “Edit”. e. Review the list of applications in the Installed Applications table. **9.** ***Import X.509v3 certificates into the Trust Anchor Database:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”. d. Click “New” under “Approved Certificate Listing”. e. Upload the certificate by specifying the Certificate File. f. Click “Save” and then click “Save”. g. On the mobile device validate the new certificate has been imported into certificate store.

	10. ***Install applications:*** a. Navigate to “APK Management”. b. On the bottom toolbar, choose “New”. c. Upload the application by specifying the MDM APK File. d. Specify the Policy Bundles. e. Specify the “Install On” and/or Notes fields. f. Click “Add”. g. Have mobile device login and then wait for polling time. h. On mobile device validate that the application has been installed. **11.** ***Update system software:*** 1. Authenticate to the MDM Server Web UI. 2. Create a policy that enables the ability to update OS software: a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”. d. Ensure “Firmware Updates Over the Air (FOTA)” is checked. e. Click “Save”. 3. Verify via audit records that the mobile device reports that the policy update is successfully received and applied. 4. From the Device Management page identify the device, firmware, and OS Version. 5. From the Device initiate an update via FOTA 6. After installation completion, verify version has been updated on device Wait until next polling cycle and then verify the new version is being reported on the Device Management page. **12.** ***Remove applications:*** a. Navigate to APK Management b. Click on application package name wanting to remove c. Click edit d. Ensure the correct policy for the device is listed e. Uncheck the Device box f. Click update to save changes g. Have device login and then wait for polling time. h. On mobile device validate that the application has been removed. **13.** ***Remove Enterprise applications:*** a. **See subtest 12.**. **14.** ***Wipe Enterprise data:*** a. Refer to FAU_ALT_EXT.1.1 - Test Case 001 unenroll section.

	15. ***N/A – Omit*** **16.** ***Alert the user:*** a. Navigate to "Device Management". b. Select the device. c. Click "Create Alert". d. Click "Alert to Selected". e. Specify the message to send in the alert. f. Click "Save". **17.** ***N/A - OMIT*** **18.** ***N/A - OMIT*** **19.** ***N/A - OMIT*** **20.** ***N/A - OMIT*** **21.** ***N/A - OMIT*** **22.** ***N/A - OMIT*** **23.** ***N/A - OMIT*** **24.** ***N/A – OMIT*** **25.** ***Define a password length/complexity/lifetime*****:** a. Navigate to "Policies". b. On the bottom toolbar, choose "New" > "Create". c. Specify the required fields on the "MDM Settings" tab and click "Device Policy". d. Specify the Password Restriction: i. Minimum Password Complexity: Complex ii. Min Password Length: 8 iii. Min Numbers: 3 iv. Max Password Lifetime: 60 e. Click "Save". f. On mobile device validate that the current lock type is the high **26.** ***Define the session locking policy (screen-lock enabled/disabled, screen lock timeout, number of authentication failures):*** a. Navigate to "Policies". b. On the bottom toolbar, choose "New" > "Create". c. Specify the required fields on the "MDM Settings" tab and click "Device Policy". d. Specify the Password Restriction: i. Max Auto-Lock Time: 10 ii. Max Failed Attempts: 5 e. Click "Save". f. Fail login attempts 5 times and verify phone disables (shuts down) g. On mobile device validate that the Screen timeout is 10 minutes and that the mobile device shuts down after 5 failed login attempts. **27.** ***Define the wireless networks (SSIDs) to which the MD may connect:***

a. Navigate to “Policies”.
b. On the bottom toolbar, choose “New” > “Create”.
c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”.
d. Click “New” to Specify the Wireless SSID Whitelist.
    i. Specify the SSID Name
    ii. Specify the Security Type
    iii. Specify the Credentials Type.
e. Click “Submit” and then “Save”.
f. On the mobile device attempt to connect to the authorized network and confirms that it succeeds.
g. On the mobile device attempt to connect to an unauthorized network listed and confirm failure.
h. On the mobile device attempt to manually configure a connection to a non-authorized network and confirm failure.

28. ***Define the security policy for each wireless network, including the CA(s) from which the MD will accept WLAN authentication server certificate(s), the security type, the authentication protocol, and the client credentials to be used for authentication:***

a. On mobile device attempt to connect to unauthorized network verify connection attempt fails.
b. Navigate to “Policies”.
c. On the bottom toolbar, choose “New” > “Create”.
d. Specify the required fields on the “MDM Settings” tab and click “Device Policy”.
e. Click “New” to Specify the Wireless SSID Whitelist.
    i. Specify the SSID Name (use the SSID of network that failed in step a.)
    ii. Specify the Security Type
    iii. Specify the Accepted Cert Authority
    iv. Specify the Credentials Type
    v. Specify the Client Credential
f. Click “Submit” and then “Save”.
g. On mobile device attempt to connect to the same network as in step a. and verify it now is successful.

29. ***Define the application installation policy by specifying authorized application repository(s) and denying application installation:***

a. Navigate to “Policies”.
b. On the bottom toolbar, choose “New” > “Create”.
c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”.
d. Click “New” under “Application Restrictions”.
e. Specify the application Package Name.
f. Specify authorized application repositories by disabling the Google Play Store app.
g. Click “New” under “Blacklisted Applications”.

	h. Specify the application Package Name. i. Ensure that Applications from Unknown Sources is disabled. j. Click “Submit” and then click “Save”. k. On the mobile device attempt to install an application from the store that has been blacklisted and confirm that it is not allowed. **30.** ***Enable/disable policy for camera and microphone across device:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”. d. Ensure “Camera” is unchecked. e. Ensure “Microphone” is unchecked. f. Click “Save”. g. On the mobile device, attempt to use the camera h. On the mobile device verify in Settings that the Camera and Microphone are DISABLED. **31.** ***N/A – OMIT*** **32.** ***Enable/disable policy for cellular and NFC:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”. d. Ensure “Cellular Signal” is unchecked. e. Ensure “NFC” is unchecked. f. Click “Save”. g. On the mobile device verify in Settings that the NFC is disabled (greyed out so user cannot reenable. h. On the mobile device verify that the mobile data is disabled and is greyed. Message stating Security policy prevents use of Mobile Data should be displayed. **33.** ***Enable/disable policy for data signaling over USB, removable storage card (SD card):*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”. d. Ensure “SD Card” is unchecked. e. Ensure “USB Debugging”, “USB File Transfer”, “USB Host Storage”, and “USB Mass Storage” is unchecked. f. Ensure the USB Host Mode Whitelist is empty. g. Click “Save”. h. On the mobile device verify in Settings that the USB entries are

	DISABLED. Attempt to access the SD card and verify this fails. **34.** ***Enable/disable policy for Wi-Fi tethering, USB tethering:*** a. Navigate to "Policies". b. On the bottom toolbar, choose "New" > "Create". c. Specify the required fields on the "MDM Settings" tab and click "Device Policy". d. Ensure "WiFi Tethering" is unchecked. e. Ensure the USB Host Mode Whitelist is empty. f. Click "Save". g. On the mobile device verify that the Ethernet and USB tethering are disabled and are not allowed to be enabled. **35.** ***Enable/disable policy for developer modes:*** a. Navigate to "Policies". b. On the bottom toolbar, choose "New" > "Create". c. Specify the required fields on the "MDM Settings" tab and click "Device Policy". d. Ensure "Developer Mode" is unchecked. e. Click "Save". f. On mobile device verify that the Settings show that the Developer Mode is DISABLED and that the selections under the Settings main tab do not show Developer selection. **36.** ***Enable policy for data-at-rest protection:*** a. Navigate to "Policies". b. On the bottom toolbar, choose "New" > "Create". c. Specify the required fields on the "MDM Settings" tab and click "Device Policy". d. Ensure "Device Encryption" is selected. e. Click "Save". f. On the mobile devise verify in settings that the Device Encryption is ENABLED **37.** ***Enable policy for removable media's data-at-rest protection:*** a. Navigate to "Policies". b. On the bottom toolbar, choose "New" > "Create". c. Specify the required fields on the "MDM Settings" tab and click "Device Policy". d. Ensure "External Storage Encryption" is selected. e. Click "Save". f. On the mobile devise verify in settings that the SD Card (Removable Device) Encryption is ENABLED **38.** ***Enable/disable policy for local authentication bypass:*** a. Navigate to "Device Management". b. Select the device. c. Select "Reset Password".

	d. Specify the new password. e. Click “Update”. f. On the mobile device enter the new password (which is obfuscated) and verify successful authentication. **39.** ***N/A – OMIT*** **40.** ***N/A – OMIT*** **41.** ***N/A – OMIT*** **42.** ***N/A – OMIT*** **43.** ***N/A – OMIT*** **44.** ***N/A – OMIT*** **45.** ***N/A – OMIT*** **46.** ***N/A – OMIT*** **47.** ***Define the unlock banner policy:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab. d. Specify the unlock banner text in the “Device Lock Screen Message” textbox. e. Click “Save”. f. On the mobile device verify the warning banner is displayed on the lock screen. **48.** ***N/A – OMIT*** **49.** ***Enable/disable USB mass storage mode:*** a. This is tested in conjunction with the testing activities in subtest 33. **50.** ***N/A – OMIT*** **51.** ***Enable/disable hotspot functionality authenticated by pre-shared key, authenticated by passcode:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”. d. Ensure “Unsecured Hotspot” is unchecked. e. Click “Save”. **52.** ***N/A – OMIT*** **53.** ***N/A – OMIT*** **54.** ***N/A – OMIT*** **55.** ***Enable/disable policy for use of Biometric Authentication Factor:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”.

	d. Ensure “Fingerprint Login” is unchecked. e. Click “Save”. f. On the mobile device verify in Settings that Face Login and Fingerprint Login are DISABLED and not available to enable. **56.** ***N/A – OMIT*** **57.** ***N/A – OMIT*** **58.** ***Enable/disable automatic updates of system software:*** a. Navigate to “Policies”. b. On the bottom toolbar, choose “New” > “Create”. c. Specify the required fields on the “MDM Settings” tab and click “Device Policy”. d. Ensure “Firmware Updates Over the Air(FOTA)” is not selected. e. Click “Save”. f. On the mobile device verify that options under Software Updates are now disabled.
Test Results	The evaluator confirmed all functionality claimed in the ST, worked as expected and generated the expected audit records: Subtest 01 – The mobile device displays its lock screen after having received the command from the MDM server to transition to the locked state. The series of server audit records are displayed ranging from "Lock Device" (server audit record) command to "Lock Device Command Received" (device audit record). For all subtests (02, 03, 14) where a device wipe operation, unenrollment, and wipe of Enterprise data is performed against an already enrolled device, refer to FAU_ALT_EXT.1.1 - Test Case 001. Subtest 04 – The configured policy (policy3, version 2) is applied to the mobile device with device ID fd62a940039bec3e. NOTE: This was an update to a new policy (version 1). Subtest 05, 06, 07 – The querying of the connectivity status (last contacted), current version of the device firmware/software (firmware), and the device hardware model (model) is collected as part of the configured (5 minutes) periodic device check-ins as shown in subtest 04 where there is a "Reachability Event". The status information collected is displayed on the "Device Management" page in each respective column. Subtest 08 – The querying of the current version of installed applications is displayed in the detailed view of a selected device from the Device Management page. Newly installed applications appeared in the list after selecting "Update". A review of the list of Installed Applications confirmed that it was consistent with the list of installed applications and versions reported by the device OS app manager. Subtest 09 – The import of a X.509v3 certificate was configured per the defined policy. MDM server audit records list the policy and version which confirm the configuration. The configured X.509v3 certificate is present in the mobile device platform trust anchor and shown in the second screen capture in the "View security certificates". Subtest 10 – The "net.progeny.boozeenterprise_1.0-release.apk" application is imported into the Application Management (MAS server), linked to a policy, and specified to install to the device. The configured application is then observed as installed on the mobile device and an alert from the mobile device confirms the successful installation of the application. Finally, the MDM server reports in a server audit entry the successful installation of the application on the mobile device. Subtest 11 – refer to Test FPT_TUD_EXT.1_069

	Subtest 12 – The alert messages received by the MDM server show that the policy was implemented by the Host agent and the Host agent successfully removed the application. Subtest 13 – See subtest 12. Behavior is the same whether an application or Enterprise application. Subtest 14 – refer to FAU_ALT_EXT1.1 – Test Case 001 unenroll section. Subtest 15 – N/A Subtest 16 – The alert message "This is an alert per subtest 16 within Test Case 050" is transmitted to the selected device and then displayed as an application notification on the device. Corresponding MDM server audit log entries for the alert are generated with Event Types "Device Alert Created", "Device Alert Check", and "Device Alert Received". Subtest 17 through 24 – N/A Subtest 25 – A configured policy specifying mobile device password, complexity, and lifetime was defined as a complex password consisting of minimum length of 8 characters, 3 numbers, and validity period of 60 days as part of "policy2, version 7". The successful application of this policy was confirmed by an audit record reported back to the MDM server in the form of an MDM agent alert. The evaluator also confirmed, as shown in the screen capture from the mobile device that a device lock enforcement with a complex password as defined from the applied policy was required. Subtest 26 – A configured policy (policy2, version 8) specifying the session locking policy (enablement of the screen lock, a maximum timeout value of 10 minutes, and a maximum number of authentication failures of 5 attempts) was defined, transmitted to the device, and shown as configured on the mobile device. The successful application of this policy was also confirmed by an audit record reported back to the MDM server in the form of an MDM agent alert. The evaluator also confirmed, as shown in the series of screen captures from the mobile device, that only 10 minutes was the maximum value for the screen timeout, and that after the evaluator attempted more than 4 successive authentication failures at the device lock screen, that the device disabled its functionality and reported the message "Device turned off. Contact IT administrator. (net.progeny.nosis.nast.mdm)". Subtest 27 – A configured policy (policy2, version 9) specifying the wireless SSIDs (cattle) to which the MD may connect was defined, transmitted to the device, and shown as configured on the mobile device. The successful application of this policy was also confirmed by an audit record reported back to the MDM server in the form of an MDM agent alert. Enforcement of the policy was confirmed by the evaluator induced attempts to connect to other broadcasted networks apart from "cattle", and the manual configuration of additional networks. These attempts were unsuccessful as shown in the series of screen captures from the mobile device Wi-Fi settings UI. Subtest 28 – A configuration policy2 version 48 specifying the allowed wi-fi network settings was generated and the Host agent implemented this policy. The evaluator validated the allowed network by successfully connecting to the network with the mobile device with the Host agent software installed. Subtest 29 – A configured policy (policy2, version 11) specifying the allowed set of application sources and permitted applications was defined to limit the scope of permitted applications to those from known sources (MAS server) by enforcing the disablement of the "Google Play Store" repository and denying access to it in the form of a Blacklisted Application in the applied policy. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. The evaluator confirmed the enforcement of this policy by verifying that the Google Play Store was inaccessible from the device launcher and set of available applications in the settings UI app manager. Installation of applications from other unknown sources was also confirmed as disabled per the policy.

	Subtest 30 – A configured policy (policy2, version 13) specifying the disablement of the device camera and microphone was defined. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. Enforcement of this policy was confirmed by verifying the Camera application did not launch. The MDM agent itself also reported that the Camera and Microphone was set to "DISABLED". Subtest 31 – N/A Subtest 32 – A configuration policy3 version 6 specifying the Cellular Signal and NFC settings are disabled was generated and the Host agent implemented this policy. The evaluator confirmed that the Host agent implemented the policy by verifying the mobile device settings of Cellular Singal and NFC were indeed disabled. Subtest 33 – A configured policy (policy2, version 15) specifying the disablement of data signaling over USB (USB debugging, USB file transfer, USB host storage, and USB mass storage, and no permitted USB host modes), and access to a removable storage card (SD card) was defined. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. This is shown in the MDM agent's Settings panel of enabled/disabled restrictions. The evaluator also confirmed that external USB connections to the device was disabled and verified that an externally inserted SD card was inaccessible. Subtest 34 – A configured policy (policy2, version 19) specifying the disablement of Wi-Fi tethering and USB tethering was defined. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. The evaluator verified that Mobile Hotspot and Tethering was unable to be activated (enabled) via the device setting UI. Subtest 35 – A configured policy (policy2, version 21) specifying the disablement of developer modes ("Developer Mode") was defined. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. The evaluator verified that "Developer options" was not available from within the device settings UI after having previously verified it was accessible prior to the application of the policy (which was activated by tapping the device Build number a sufficient number of successive times to display the hidden UI element). Subtest 36 – A configuration policy2 version 22, specifying the enablement of the Device Encryption and SD Card encryption settings, was generated and the Host agent implemented this policy. The evaluator validated the implementation of the policy by verifying the device settings for Device Encryption and SD Card encryption were enabled. Subtest 37 – A configured policy (policy2, version 22) specifying the device policy for removable media (SD card) data-at-rest protection (External Storage Encryption) was defined. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. The evaluator confirmed that in order to use an externally inserted formatted SD card, it had to be encrypted before first use. Subtest 38 – Local authentication bypass (password reset) action was transmitted to the mobile device. An evaluator defined password value was specified, replacing the previously configured password value on the specified device. The evaluator confirmed that after the MDM agent reported a periodic "Password Reset Check" event to the MDM server that the specified device was successfully unlocked from a locked state after having supplied the evaluator defined password value as part of the password reset action from the MDM server. Subtest 39-46 – N/A Subtest 47 – The device unlock banner (Device Lock Screen) policy (policy2, version 25) was defined. The banner message was displayed on the mobile device

	after having confirmed its successful application to the mobile device in the form of device alerts received as a server audit log entry for the same policy. Subtest 48 – N/A Subtest 49 – A configured policy (policy2, version 15) specifying the device policy for USB and Mass storage was defined. The evaluator validated the implementation of the policy by verifying the device settings for USB and USB Mass storage were all disabled. Subtest 50 – N/A Subtest 51 – A configured policy (policy3, version 7) specifying the device policy for disabling the use of mobile device as a hotspot. The evaluator validated the implementation of the policy by verifying the device settings for Unsecured Hotspot was disabled. Subtest 52-54 – N/A Subtest 55 – A biometric authentication factor (policy2, version 27) policy was defined disabling fingerprint based authentication to the mobile device. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. Enforcement of this policy was confirmed by the evaluator's attempts to enable Fingerprint based authentication from within the device Screen lock type settings UI element. Subtest 56, 57 – N/A Subtest 58 – A policy (policy2, version 29) defining the disablement of the automatic updates of system software (device/platform OS/firmware OTA updates) was configured. Application of this policy was confirmed by the MDM agent itself and in the form of a device alert received by the MDM server. Enforcement of this policy was confirmed by evaluator attempts to select any options from the device Software update settings UI element. The evaluator confirmed that all referenced test cases were assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	051
SFR	[MDMPP]FMT_SMF.1.1(2) – Specification of Management Functions (Server Configuration of Server) – Test 1
Test Objective	The tests of functions b, c.1, c.2, and c.5 are performed in conjunction with the use of the function. Test 3 also covers function c.4. The evaluator shall perform the following test: Test 1: The evaluator shall configure the TSF authentication certificate(s) and verify that the correct certificate is used in established trusted connections (FPT_ITT.1(1), FPT_ITT.1(2), FTP_ITC.1(1), and FTP_TRP.1(2)).
Test Instructions	Execute this test per the test steps.
Test Steps	1. From the MDM Server platform, launch C:\jboss-eap-7.4\conf\. 2. Import the certificate to be used by the MDM Server into the Java keystore “mdmserverkeystore.jks” certificate repository. The use of the configured TSF authentication certificate is performed in conjunction with testing performed in FPT_ITT.1(2), FTP_ITC.1(1), and FTP_TRP.1(2).
Test Results	The evaluator confirmed that when a Host agent authentication certificate was

	generated following the AGD, the Host Agent successfully used this certificate to establish a TLSv2.1 trusted channel with the MDM Server. - In FPT_ITT.1(2) - Test Case 064, the certificate presented by the MDM server to the MDM agent is present in the server Certificate message, which corresponds to the same certificate configured for use by the MDM server via the "mdmserverkeystore.jks" certificate repository. - In FTP_ITC.1(1) - Test Case 073, the certificate presented by the MDM server to the database/audit server is present in the server Certificate message, which corresponds to the same certificate configured for use by the MDM server via the "mdmserverkeystore.jks" certificate repository. - In FTP_TRP.1(2) - Test Case 079, the certificate presented by the MDM server to the is present in the server Certificate message, which corresponds to the same certificate configured for use by the MDM server via the "mdmserverkeystore.jks" certificate repository. The evaluator confirmed that all referenced test cases were assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	052
SFR	[MDMPP]FMT_SMF.1.1(2) – Specification of Management Functions (Server Configuration of Server) – Test 2
Test Objective	The tests of functions b, c.1, c.2, and c.5 are performed in conjunction with the use of the function. Test 3 also covers function c.4. The evaluator shall perform the following test: Test 2: (conditional) The evaluator shall configure the periodicity for the assigned list of commands to the agent for several configured time periods and shall verify that the MDM Server performs the commands schedule.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the MDM Server Web UI as the administrator. 2. In order to configure the periodicity of the following tasks: Query connectivity status Query the current version of the MD firmware/software Query the current version of the hardware model of the device Query the current version of installed mobile applications 3. Navigate to “MDM Settings” > “New” > “Create” > “App to Server Communication Settings”. 4. Specify the “Server Communication Interval(min)” value to 5 minutes. 5. Verify that audit records are generated for the successful configuration of this function. 6. Wait at least for two Check-Ins to occur to establish that the interval between Check-In is 5 minutes. 7. Repeat Steps 3 – 5, except in Step 4, configure the value to 10 minutes. 8. Wait at least for two Check-Ins to occur to establish that the interval between Check-Ins is 10 minutes.

Test Results	The evaluator confirmed that an admin has the ability to set a time frame for the periodic check in. When policies of different times were deployed, the Host Agent implemented the policy and followed the new timeframes for each new policy. Verdict: Pass
Execution Method	Manual

Test Case Number	053
SFR	[MDMPP]FMT_SMF.1.1(2)– Specification of Management Functions (Server Configuration of Server) – Test 3
Test Objective	The tests of functions b, c.1, c.2, and c.5 are performed in conjunction with the use of the function. Test 3 also covers function c.4. The evaluator shall perform the following test: Test 3: (conditional) The evaluator shall design and perform tests to demonstrate that the assigned function may be configured and that the intended behavior of the function is enacted by the MDM Server.
Test Instructions	Execute this test per the test steps.
Test Steps	**Configure the interaction between TOE components** 1. Authenticate to the Admin Console as an Administrator. 2. Navigate to “Device Management”. 3. Click “New”. 4. Specify the permitted Android Device IDs. 5. Commit the selection. **Configure the TOE unlock banner** Refer to [MDMPP]FTA_TAB.1.1 – Test Case 071.
Test Results	The evaluator confirmed the ability to perform Server configuration items such as whitelisting a device to allow for the enrollment of the device, configuring the consent banner (Test 071), Configuring the X.509 certificates (Test 50 subtest 9), updating policy parameters such as polling intervals (Test 052) and the Host agent. The MDM Server generated correct audit records for the policy update/creation. The evaluator confirmed that all referenced test cases and subtests were assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	054
SFR	[MDMPP]FMT_SMF.1.1(3) – Specification of Management Functions (MAS Server)
Test Objective	The evaluator shall ensure that the MAS client can only access the applications specified for the group they are enrolled in. The evaluator shall create a user group, making sure that the MAS client user is excluded from the group. Verify that an application accessible to that group cannot be accessed. The evaluator shall include the MAS client user in the group and assure that the application can be accessed.
Test Instructions	Execute this test per the test steps.

Test Steps	1. Assign the device to only Policy2 2. Wait for policy to be activated on device 3. Verify that the application has been removed from the device. 4. Assign the same device to only Policy3 5. Wait for policy to be activated on device 6. Verify that the application has been installed on the device.
Test Results	The evaluator confirmed that a Host agent successfully downloaded an application that was permitted within the implemented policy on the particular Host agent. The evaluator also confirmed that a Host agent was unable to download an application that was not permitted within the implemented policy on the particular Host agent. Verdict: Pass
Execution Method	Manual

Test Case Number	055
SFR	[AGENTMOD]FMT_SMF_EXT.4 – Specification of Management Functions – Test 1
Test Objective	Test 1: In conjunction with the evaluation activities in the Base-PP, the evaluator shall attempt to configure each administrator-provided management function and shall verify that the mobile device executes the commands and enforces the policies.
Test Instructions	Execute this test per the test steps.
Test Steps	This Assurance Activity is satisfied by testing performed in [MDMPP]FMT_SMF.1.1(1) Test 1 (Test Case 050).
Test Results	The evaluator confirmed that all referenced test case was assigned a verdict of pass.
Execution Method	Manual

Test Case Number	056
SFR	[AGENTMOD]FMT_SMF_EXT.4 – Specification of Management Functions – Test 2 – TD0491
Test Objective	Test 2: The evaluator shall configure the MDM Agent authentication certificate in accordance with the configuration guidance. The evaluator shall verify that the MDM Agent uses this certificate in performing the tests for FPT_ITT.1(2) (MDM as Base-PP) or FTP_ITC_EXT.1(2) (MDF as Base-PP).
Test Instructions	Execute this test per the test steps.
Test Steps	1. Perform the test steps in [MDMPP]FPT_ITT.1.1(2) – Test Case 064. 2. Inspect the packet capture and review it to ensure the mobile device (TLS client) client certificate Common Name (CN) identifier corresponds to the device identifier assigned to the mobile device.
Test Results	The evaluator confirmed that when a Host agent authentication certificate was generated following the AGD, the Host Agent successfully used this certificate for TLS communications with the MDM Server. Verdict: Pass
Execution Method	Manual

Test Case Number	057
SFR	[AGENTMOD]FMT_SMF_EXT.4 – Specification of Management Functions – Test 3

Test Objective	Test 3: In conjunction with other evaluation activities, the evaluator shall attempt to enroll the MDM Agent in management with each interface identified in the TSS, and verify that the MDM Agent can manage the device and communicate with the MDM Server.
Test Instructions	Execute this test per the test steps.
Test Steps	This Assurance Activity is satisfied by testing performed in [MDMPP]FIA_ENR_EXT.1 (Test Cases 023, 024 & 025).
Test Results	This test was conducted with other evaluation activities. During the entirety of IND testing, the evaluator observed that the Agent, once enrolled (FIA_ENR_EXT.1 and FIA_ENR_EXT.2), manages the host device per the digitally signed policy set at the MDM Server (FMT_POL_EXT.1, FMT_POL_EXT.2, and FMT_SMF.1), rejects unsigned policies, controls applications that can be installed/deleted/forbidden, and uses TLS v1.2 protocol (FTP_ITC.1) for all communications. Verdict: Pass
Execution Method	Manual

Test Case Number	058
SFR	[AGENTMOD]FMT_SMF_EXT.4 – Specification of Management Functions – Test 4
Test Objective	Test 4: [conditional] In conjunction with the evaluation activity for FAU_ALT_EXT.2.1, the evaluator shall configure the periodicity for reachability events for several configured time periods and shall verify that the MDM Server receives alerts on that schedule.
Test Instructions	Execute this test per the test steps.
Test Steps	Periodicity of reachability events is performed in [MDMPP] FMT_SMF.1.1(2) – Test Case 052.
Test Results	The evaluator confirmed that all referenced test was assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	059
SFR	[AGENTMOD]FMT_SMF_EXT.4 – Specification of Management Functions – Test 5
Test Objective	Test 5: [conditional] The evaluator shall design and perform tests to demonstrate that the assigned function may be configured and that the intended behavior of the function is enacted by the mobile device.
Test Instructions	Execute this test per the test steps.
Test Steps	N/A – The Security Target does not specify an assigned function for this SFR
Test Results	Pass
Execution Method	Manual

Test Case Number	060
SFR	[MDMPP]FMT_SMR.1.2(1) – Security Management Roles
Test Objective	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure,

	however, that each supported method of administering the TOE that conforms to the requirements of this PP be tested; for instance, if the TOE can be administered through a local hardware interface or HTTPS then both methods of administration must be exercised during the evaluation team's test activities.
Test Instructions	Execute this test per the test steps.
Test Steps	In order to manage the administrative functions, the TOE is administered through a TLS/HTTPS web interface for the administrator (MDM Server Web UI). All testing activities that involve configuration, such as MDM policies, are performed throughout the evaluation using the TOE TLS/HTTPS web interface (e.g. [MDMPP]FMT_SMF.1.1(1) – Test Case 050.
Test Results	The evaluator confirmed that the TOE is administered through a TLS/HTTPS web interface for the administrator (MDM Server Web UI). All testing activities that involve configuration, such as MDM policies, are performed throughout the evaluation using the TOE TLS/HTTPS web interface (e.g. [MDMPP]FMT_SMF.1.1(1) – Test Case 050. The evaluator confirmed that all referenced test case was assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	061
SFR	[MDMPP]FMT_SMR.1.2(2) – Security Management Roles (MAS Server)
Test Objective	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this PP be tested; for instance, if the TOE can be administered through a local hardware interface or HTTPS then both methods of administration must be exercised during the evaluation team's test activities.
Test Instructions	Execute this test per the test steps.
Test Steps	According to the Security Target for [MDMPP]FMT_SMR.1(2): "[SERVER] The MAS Server is logically integrated with the GovShield Server. It is accessed by Administrators using the APK Management dashboard in the web GUI. Since this is not accessed separately from the remainder of the GovShield Server capabilities, the user roles and their ability to interact with the MAS Server functionality is defined in the same manner as for FMT_SMR.1(1) above. The GovShield Server also maintains the roles of enrolled mobile devices and application access groups for MAS Server functionality." In order to manage the administrative functions, the TOE is administered through a TLS/HTTPS web interface for the administrator (MDM Server Web UI). All testing activities that involve configuration, such as MDM policies, are performed throughout the evaluation using the TOE TLS/HTTPS web interface (e.g. [MDMPP]FMT_SMF.1.1(1) – Test Case 050.
Test Results	According to the Security Target for [MDMPP]FMT_SMR.1(2): "[SERVER] The MAS Server is logically integrated with the GovShield Server. It

	is accessed by Administrators using the APK Management dashboard in the web GUI. Since this is not accessed separately from the remainder of the GovShield Server capabilities, the user roles and their ability to interact with the MAS Server functionality is defined in the same manner as for FMT_SMR.1(1) above. The GovShield Server also maintains the roles of enrolled mobile devices and application access groups for MAS Server functionality." The evaluator confirmed that the TOE is administered through a TLS/HTTPS web interface for the administrator (MDM Server Web UI). All testing activities that involve configuration, such as MDM policies, are performed throughout the evaluation using the TOE TLS/HTTPS web interface (e.g. [MDMPP]FMT_SMF.1.1(1) – Test Case 050. The evaluator confirmed that all referenced test case was assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	062
SFR	[AGENTMOD]FMT_UNR_EXT.1 – User Unenrollment Prevention – Test 1
Test Objective	Test 1: If 'prevent the unenrollment from occurring' is selected: The evaluator shall configure the Agent according to the administrative guidance for each available configuration interface, shall attempt to unenroll the device, and shall verify that the attempt fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. On the Android mobile device, navigate to 2. Tap "Deactivate". 3. Observe that "Deactivate" is not possible to tap or is unavailable. 4. On the Android mobile device, launch the 5. Verify that the "Unenroll Device" button is absent from the interface. 6. Attempt to uninstall the MDM Agent app from the mobile device. 7. Verify that the uninstall is unsuccessful. 8. Observe that there is no unenrollment option.
Test Results	The evaluator confirmed that after the MDM server deployed a policy preventing users from unenrolling the Host agent, the Host agent correctly enforced the policy by denying the user's unenrollment request. Verdict: Pass
Execution Method	Manual

Test Case Number	063
SFR	[AGENTMOD]FMT_UNR_EXT.1 – User Unenrollment Prevention – Test 2
Test Objective	Test 2: If 'apply remediation actions' is selected: If any configuration allows the user to unenroll, the evaluator shall configure the Agent to allow user unenrollment, attempt to unenroll, and verify that the remediation actions are applied.
Test Instructions	Execute this test per the test steps.
Test Steps	The ST does not select "apply remediation actions"; therefore, this test assurance activity does not apply.
Test Results	Pass

Execution Method	Manual

4.3.6 Protection of the TSF

Test Case Number	064
SFR	[MDMPP]FPT_ITT.1.1(2) – Internal TOE TSF Data Transfer (MDM Agent) – Test 1
Test Objective	Test 1: The evaluator shall ensure that communications using each specified (in the operational guidance) communication method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Launch Wireshark on the MDM Server and begin capturing packets between the MDM Server and MDM Agent. 2. Initiate communication between the MDM Server and the MDM Agent device. 3. Stop capturing packets from the MDM Server. 4. Communication between the MDM Server and the MDM Agent device is successful. 5. Inspect the packet capture and review it to ensure the data is encrypted using TLS v1.2.
Test Results	The evaluator confirmed, through analyzing a packet capture, that all communication between the MDM server and the Host agent was encrypted using TLSv1.2. Upon further examination of the packet capture, it was confirmed that plaintext data was not sent over this secure channel. Verdict: Pass
Execution Method	Manual

Test Case Number	065
SFR	[MDMPP]FPT_ITT.1.1(2) – Internal TOE TSF Data Transfer (MDM Agent) – Test 2
Test Objective	Test 2: The evaluator shall ensure, for each method of communication, the channel data is not sent in plaintext. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in [MDMPP]FPT_ITT.1.1(2) – Test Case 064.
Test Results	Pass
Execution Method	Manual

Test Case Number	066
SFR	[MDMPP]FPT_TST_EXT.1.2 – Functionality Testing – Test 1
Test Objective	The evaluator shall perform the following tests: Test 1: The evaluator performs the integrity check on a known good TSF

	executable and verifies that the check is successful.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Turn JBoss off 2. Place a good .ear file into the deployment directory (C:\jboss-eap-7.4\standalone\deployments). 3. Watch for the MDM-NIAP-<ear file name>.ear.isdeploying file to appear almost immediately. 4. Open .isdeploying file to verify the correct .ear file name. 5. Check audit log (C:\jboss-eap-7.4\standalone\log\server.log) for successful records. (search for Phase 1 of 2)
Test Results	The evaluator confirmed that the TOE performed a successful integrity check of the TSF executables as expected. Additionally, the evaluator confirmed that the integrity check caught an evaluator introduced modification of an executable and correctly reported the failure. Verdict: Pass
Execution Method	Manual

Test Case Number	067
SFR	[MDMPP]FPT_TST_EXT.1.2 – Functionality Testing – Test 2
Test Objective	The evaluator shall perform the following tests: Test 2: The evaluator modifies the TSF executable, performs the integrity check on the modified TSF executable and verifies that the check fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Turn JBoss off 2. Open .ear file in a hex editor and modify a hex number in the middle of the file using ‘aa’. 3. Replace the current .ear file with the modified version of the .ear. 4. Watch for the MDM-NIAP-<ear file name>.ear.failed file to appear almost immediately. 5. Open .failed file to verify reason is “SHA-256 digest error for….” 6. Check audit log (C:\jboss-eap-7.4\standalone\log\server.log) for failure records (search for Phase 1 of 2) and look for “SHA-256 digest error for….”.
Test Results	Pass
Execution Method	Manual

Test Case Number	068
SFR	[MDMPP]FPT_TUD_EXT.1.1 – Trusted Update
Test Objective	The evaluator shall query the TSF for the current version of the software according to the AGD guidance and shall verify that the current version matches that of the documented and installed version.
Test Instructions	Execute this test per the test steps.
Test Steps	**MDM Server:** 1. Navigate to the MDM Server Web UI: `https://` 2. Click on the Gear symbol and then select the “About” to access the

	version information. 3. Verify the TOE version with that of the one in the guidance documentation. **MDM Agent (Android):** 1. On the Mobile device, open the GovShield app 2. Press the gear symbol and then select the "About" to access the version information. 3. Verify the TOE version with that of the one in the guidance documentation.
Test Results	The evaluator verified the ability to query both the MDM Server and Host Agent versions. The evaluator then confirmed that properly signed updates for each component were successfully installed, and that both the MDM Server and Host Agent reported the correct post-update versions. Verdict: Pass
Execution Method	Manual

Test Case Number	069
SFR	[MDMPP]FPT_TUD_EXT.1.3 – Trusted Update – Test 1
Test Objective	The evaluator shall perform the following tests: Test 1: The evaluator shall attempt to initiate an update digitally signed by the vendor and verify that the update is successfully installed.
Test Instructions	Execute this test per the test steps.
Test Steps	**MDM Server:** 1. Record the current version of the MDM Server: a. Navigate to the MDM Server Web UI: `https://` b. Click on "About" to access the version information. 2. Attempt to install an update that is digitally signed by GovShield a. Copy signed ear into C:\jboss-eap-7.4\standalone\deployments b. Remove old ear and ear.deployed c. Make a blank file name of file with .ear.deploy as the suffix d. Start jboss 3. Watch C:\jboss-eap-7.4\standalone\deployments directory for the file indicating installation attempt (suffix .isdeploying) 4. Watch C:\jboss-eap-7.4\standalone\deployments directory for the file indicating installation (suffix .deployed) 5. Verify that the update installation did succeeded due to the package being signed by reading contents of the .deployed file which should have the name of the .ear deployed. 6. Verify that the version number stayed the same: a. Navigate to the MDM Server Web UI: `https://` b. Click on "About" to access the version information. c. Verify the version number increased.

	MDM Agent (Android): 1. Authenticate to the MDM Server Web UI as the administrator. 2. Navigate to "APK Management" → "New". 3. Upload the signed MDM APK file. 4. Specify the Policy Bundle. 5. Specify "Device" to Install On. 6. Click "Add". 7. Wait for polling and observe that the application installed on the mobile device. Verify that the MDM administrator is alerted of the successful installation of the application. (reported version on device)
Test Results	The evaluator verified the ability to query both the MDM Server and Host Agent versions. The evaluator then confirmed that properly signed updates for each component were successfully installed, and that both the MDM Server and Host Agent reported the correct post-update versions. Verdict: Pass
Execution Method	Manual

Test Case Number	070
SFR	[MDMPP]FPT_TUD_EXT.1.3 – Trusted Update – Test 2
Test Objective	The evaluator shall perform the following tests: Test 2: The evaluator shall attempt to install an update not digitally signed by the vendor and verify that either the signature can be checked (allowing the update to be aborted) or the update is not installed.
Test Instructions	Execute this test per the test steps.
Test Steps	**MDM Server:** 1. Record the current version of the MDM Server: a. Navigate to the MDM Server Web UI: `https://` b. Click on "About" to access the version information. 2. Attempt to install an update that is NOT digitally signed by GovShield 3. Copy unsigned ear into C:\jboss-eap-7.4\standalone\deployments 4. Remove old ear and ear.deployed 5. Make a blank file name of file with .ear.deploy as the suffix 6. Start jboss 7. Watch C:\jboss-eap-7.4\standalone\deployments directory for the file indicating installation attempt (suffix .isdeploying) 8. Watch C:\jboss-eap-7.4\standalone\deployments directory for the file indicating installation failure (suffix .failed) 9. Verify that the update installation did NOT succeeded due to the package not being signed by reading contents of the .failed file. 10. Verify audit records were produced for installation failure. 11. Verify that the version number stayed the same: a. Navigate to the MDM Server Web UI: `https://`

	b. Click on "About" to access the version information. c. Verify the version number stayed the same. **MDM Agent (Android):** 1. Authenticate to the MDM Server Web UI as the administrator. 2. Navigate to "APK Management" → "New". 3. Upload the unsigned MDM APK file. 4. Specify the Policy Bundle. 5. Specify "Device" to Install On. 6. Click "Add". 7. Wait and observe that the application failed to install on the mobile device. 8. Verify that the MDM administrator is alerted of the failure to install the application. 9. Verify that the audit record for the application installation failure is generated.
Test Results	The evaluator verified the ability to query both the MDM Server and Host Agent versions. The evaluator then confirmed that an improperly signed update for each component was successfully blocked from being installed, and that both the MDM Server and Host Agent reported the correct post update versions showing no change. Verdict: Pass
Execution Method	Manual

4.3.7 TOE Access

Test Case Number	071
SFR	[MDMPP]FTA_TAB.1.1 – Default TOE Access Banners
Test Objective	The evaluator shall also perform the following test: The evaluator shall start up or unlock the TSF. The evaluator shall verify that the notice and consent warning message is displayed in each instance described in the TSS.
Test Instructions	Execute this test per the test steps.

Test Steps	***MDM Server Web UI:***
	
	1. Authenticate to the MDM Server Web UI:
	a. Click on the gear icon in the top right area of the header on the main page.
	b. Choose "System Configuration".
	c. Specify the following text into the text field for "Consent Banner":
	
	`NIAP START - You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.`
	`By using this IS (which includes any device attached to this IS), you consent to the following conditions:`

	-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. NIAP END d. Choose “Save”. 2. Log out of the MDM Server Web UI. 3. Navigate to the MDM Server Web UI via the following URL: https://govshieldweb.govshield.demo:8543 4. Verify that the notice and consent warning message configured in Step 1c is displayed.
Test Results	The evaluator confirmed the ability to configure the default MDM Server consent banner. The evaluator observed that the newly configured consent banner was correctly displayed, by the MDM Server, during the next login. The evaluator also noted that the consent banner requires the user to accept the terms of use prior to being allowed to enter credentials. Verdict: Pass
Execution Method	Manual

4.3.8 Trusted Path/Channels

Test Case Number	072
SFR	[MDMPP]FTP_ITC_EXT.1.1 – Trusted Channel – Test 1
Test Objective	This testing can be completed in conjunction with the testing for FPT_ITT.1(1)/FPT_ITT.1(2), FTP_ITC.1(2) or FTP_ITC.1(3).
Test Instructions	Execute this test per the test steps.
Test Steps	N/A
Test Results	This is tested in conjunction with the testing activities in FPT_ITT1(2) Tests 064 and 065 The evaluator confirmed that the referenced test cases were assigned a verdict of

	pass. Verdict: Pass
Execution Method	Manual

Test Case Number	073
SFR	[MDMPP]FTP_ITC.1.3(1) – Inter-TSF Trusted Channel (Authorized IT Entities) – Test 1
Test Objective	Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) communication method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	***MDM Server – Database Server (which additionally acts as the audit storage):*** 1. Using Wireshark, begin capturing packets between the MDM Server and the database server. 2. Perform some action that causes a TLS connection to be established between the MDM Server and the database server. 3. Stop capturing packets between the MDM Server and the database server. 4. Inspect the packet capture and ensure that the communications are successful and encrypted with TLS v1.2.
Test Results	The evaluator reviewed the AGD and found only instructions to configure and use the secure TLS connection to establish a connection to the database server. The evaluator confirmed, through analyzing a packet capture, that all communication between the MDM server and the database server (which also acts as the audit server) was encrypted using TLSv1.2. Upon further examination of the packet capture, it was confirmed that plaintext data was not sent over this secure channel. This is consistent with the Security Target claim of using only TLSv1.2. Verdict: Pass
Execution Method	Manual

Test Case Number	074
SFR	[MDMPP]FTP_ITC.1.3(1) – Inter-TSF Trusted Channel (Authorized IT Entities) – Test 2
Test Objective	Test 2: The evaluator shall ensure, for each method of communication, the channel data is not sent in plaintext. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in [MDMPP]FTP_ITC.1.3(1) – Test Case 073.
Test Results	The evaluator confirmed that the referenced test case was assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	075
SFR	[MDMPP]FTP_ITC.1.3(1) – Inter-TSF Trusted Channel (Authorized IT Entities) – Test 3
Test Objective	Test 3: The evaluator shall ensure, for each communication channel with the MDM Server, that a protocol analyzer identifies the traffic as the protocol under testing. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in [MDMPP]FTP_ITC.1.3(1) – Test Case 033.
Test Results	The evaluator confirmed that the referenced test case was assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	076
SFR	[MDMPP]FTP_TRP.1.3(1) – Trusted Path (for Remote Administration) – Test 1
Test Objective	The evaluator shall also perform the following tests: Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Using Wireshark, begin capturing packets between the test machine web browser and the MDM Server. 2. Using the web browser, navigate to the MDM web administration console URL: `https://10.137.2.122:8543/mdm` 3. Authenticate to the MDM Web Administration Console. 4. Stop capturing packets between the web browser and the MDM Server. 5. Inspect the packet capture and ensure that the communication is successful, and that the data are encrypted.
Test Results	The evaluator confirmed, through analyzing a packet capture, that all communication between the management workstation and the database server and the GovShieldWeb administrator interface, was encrypted using HTTPS/TLSv1.2. Upon further examination of the packet capture, it was confirmed that plaintext data was not sent over this secure channel. This is consistent with the Security Target claim of using only HTTPS/TLSv1.2. Verdict: Pass
Execution Method	Manual

Test Case Number	077
SFR	[MDMPP]FTP_TRP.1.3(1) – Trusted Path (for Remote Administration) – Test 2
Test Objective	The evaluator shall also perform the following tests: Test 2: For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish remote administrative sessions without invoking the trusted path. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Inspect the operational guidance and determine and determine the methods of initiating a remote administrative session. 2. Compare the methods to the ST and determine if the ST is consistent 3. Compare the methods used in testing to ensure all methods have been tested.
Test Results	The evaluator reviewed the AGD and found only instructions to configure and use the secure HTTPS connection to establish a remote administrative session. The evaluator found no other interface described to initiate a remote administrative session. Therefore, the GovShieldWeb interface is the only interface available for remote administration. Verdict: Pass
Execution Method	Manual

Test Case Number	078
SFR	[MDMPP]FTP_TRP.1.3(1) – Trusted Path (for Remote Administration) – Test 3
Test Objective	The evaluator shall also perform the following tests: Test 3: The evaluator shall ensure, for each method of remote administration, the channel data is not sent in plaintext. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in [MDMPP]FTP_TRP.1.3(1) – Test Case 076.
Test Results	The evaluator confirmed that the referenced test case was assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	079
SFR	[MDMPP]FTP_TRP.1.3(2) – Trusted Path (for Enrollment) – Test 1
Test Objective	For each MDM Agent/platform listed as supported in the ST: Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) enrollment method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

	Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	***MDM Agent (Android) to MDM Server:*** 1. Using Wireshark, begin capturing packets between the MDM Server and MDM Agent. 2. Enroll a mobile device into MDM. 3. Stop capturing packets between the MDM Server and the MDM Agent. 4. Inspect the packet capture and ensure that the communication data are successful and encrypted.
Test Results	The evaluator reviewed the AGD and found only instructions to configure and use the secure HTTPS/TLSv1.2 connection to establish a connection to the Host agent. The evaluator confirmed, through analyzing a packet capture, that all communication between the MDM server and the Host agent was encrypted using TLSv1.2. Upon further examination of the packet capture, it was confirmed that plaintext data was not sent over this secure channel. This is consistent with the Security Target claim of using only HTTPS/TLSv1.2. Verdict: Pass
Execution Method	Manual

Test Case Number	080
SFR	[MDMPP]FTP_TRP.1.3(2) – Trusted Path (for Enrollment) – Test 2
Test Objective	For each MDM Agent/platform listed as supported in the ST: Test 2: For each method of enrollment supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish enrollment sessions without invoking the trusted path. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	Refer to [MDMPP]FIA_ENR_EXT.1.1 – Test Case 023, 024, and 025 which tests the MDM Server's ability to enroll Android mobile devices.
Test Results	The evaluator confirmed that the referenced test cases were assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

Test Case Number	081
SFR	[MDMPP]FTP_TRP.1.3(2) – Trusted Path (for Enrollment) – Test 3
Test Objective	For each MDM Agent/platform listed as supported in the ST: Test 3: The evaluator shall ensure, for each method enrollment, the channel data is not sent in plaintext. Further evaluation activities are associated with the specific protocols.
Test Instructions	Execute this test per the test steps.
Test Steps	This is tested in conjunction with the testing activities in "[MDMPP] FTP_TRP.1.3(2) – Test Case 079".

Test Results	The evaluator confirmed that the referenced test case was assigned a verdict of pass. Verdict: Pass
Execution Method	Manual

5 Evaluation Activities for SARs

This section addresses assurance activities that are defined in the *Protection Profile for Mobile Device Management Version 4.0, April 25, 2019* [MDMPP] that correspond with Security Assurance Requirements. The *PP-Module for MDM Agent Version 1.0, April 25, 2019 [AGENTMOD]* does not define any SARs beyond those defined within the base-PP to which it must claim conformance.

ADV_FSP.1 – "*There are no specific evaluation activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in Section 5 and the relevant appendices, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other evaluation activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided."*

The evaluator has confirmed that the interface information has been provided with the ADV_FSP documentation (Security Target).

The evaluation team reviewed the FSP and found that it describes the following external interfaces:

- E1: Administrator Workstation to GovShieldWeb Admin Console – This interface is used when an administrator is performing configuration changes to the Mobile Device Management services, such as deploying a device profile or policy. This interface is protected using TLS/HTTPS.
- E2: GovShield Server to SQL Database – This interface is used for the transfer of audit log data to a remote audit log server from the GovShield MDM Server and for storage of configuration data. This interface is protected using TLS.
- E3: GovShield Server to Certification Authority Server – This interface is used for the transmission of Certification Authority related data, such as revocation status of the Android mobile device client certificates used for mutual authentication and Oracle Database's server certificate.
- E4: GovShield Client (Android) to GovShield MDM Server – This interface is used to transfer policy data between the Host Agent and MDM Server. This interface is protected using HTTPS.
- E5: GovShield Client (Android) to Certification Authority Server – This interface is used for the transmission of Certification Authority related data, such as revocation status of GovShield MDM Server certificate.
- E6: E-FOTA - Samsung Knox Enterprise Firmware-over-the-air (E-FOTA) Server allows the TOE Administrators to push firmware updates to one or more enrolled Android Mobile Devices. The GovShield Client Platform is invoked by a request for the mobile device's software to be updated through the E-FOTA Server.
- E7: Samsung Know Licensing Server - The TOE communicates with the Samsung Knox Licensing Server to verify the Knox licensing key provides to the GovShield Client on an Android Mobile Device. Once the key is verified by the Samsung Knox Licensing Server, it will activate the Android Mobile Device's Knox platform which provides the TOE access to enterprise functions of the Android Mobile Device.

AGD_OPE.1 – "*Some of the contents of the operational guidance will be verified by the evaluation activities in Sections 4.2, 4.3, and 4.4 and evaluation of the TOE according to the CEM. The following additional information is also required.*

If cryptographic functions are provided by the TOE, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

The documentation must describe the process for verifying updates to the TOE by verifying a digital signature - this may be done by the TOE or the underlying platform. The evaluator shall verify that this process includes the following steps:

Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).

Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature.

The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities."

Section 2, item 3, third bullet of the AGD: Installation Guide states that cryptographic services for GovShield are provided by BSafe cryptographic libraries and the use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. Additionally, this section states that the evaluation does not make any claims of cryptographic strength for any other cryptographic modules or configurations besides what is claimed in the GovShield Version 1.60.05 Security Target.

Section 1 of the GovShield User Guide states that the Android Mobile Device platform's BoringSSL cryptographic module for cryptographic services and the use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. Additionally, the evaluation does not make any claims of cryptographic strength for any other cryptographic modules or configurations besides what is claimed in the GovShield Version 1.60.05 Security Target.

Section 3.2 of the AGD: GovShield Installation Guide contains all steps necessary to configure the cryptographic modules used by GovShield Server in the evaluated configuration.

Section 5.0 of the AGD: GovShield User Guide describes the process for verifying GovShield Client updates to the TOE. This description includes when the digital signature is accomplished, how to obtain the update, where to place the update, how to update the mobile device using APK Management, when the digital signature is validate by the Android device, and validating whether the installation was successful or unsuccessful.

> "The GovShield Client software updates are digitally signed during the software build process. The signed software updates must be obtained from General Dynamics Mission Systems and placed in the filesystem of the GovShield server. Once the update is downloaded onto the Android Mobile Device, following the below procedures, the GovShield Client will invoke the platform's application installation process which will verify the software update's digital signature before installing the GovShield Client software update. Only a successful verification of the digital signature will result in the installation of the update to the GovShield Client software, and a failed verification will result in the update process being stopped. Upon successful completion of the installation, the GovShield Client will send an alert message to the GovShield Server. The updated GovShield Client version can be verified by clicking the cog on the home screen and then selecting the *About*. This displays the version of the GovShield Client."

The "following the below procedures" refer to the instructions on using the APK Management page on the GovShield administrative interface. The following is stated about the APK Management page:

> "The APK Management page allows administrators to upload Android application package files, from the filesystem, that can be assigned to specific security policies. These applications are typically custom applications that cannot be found on the Google Play Store. Through this application management mechanism is also where the GovShield Client's software updates would be managed."

Additionally, Both AGD documents state in section 1 that any functionality that is not described in the AGD or in the GovShield Version 1.60.05 Security Target was not evaluated and should be exercised at the user's risk.

> "The GovShield Version 1.60.05 product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the evaluation were assessed. Any functionality that is not described in the GovShield Version 1.60.05 Security Target was not evaluated and should be exercised at the user's risk."

NOTE: There are no steps required to configure the Android's BoringSSL cryptographic module for use as it is automatically part of the Samsung Device Android implementation.

Section 4 of the AGD: GovShield Installation Guide describes the process for installing an update for the GovShield server. Additionally this paragraph describes that Java is responsible for executing GovShield Server's software integrity check during the start or the restart of the GovShield Server's software.

AGD_PRE.1 – "*As indicated in the introduction above, there are significant expectations with respect to the documentation, especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST."*

The AGD: GovShield Installation Guide as a whole adequately addresses the GovShield server platform which is made up of the Microsoft Windows 2022 platform with Java SE Runtime Environment and JBoss Enterprise Application Platform application server. The AGD:GovShield User Guide adequately addresses the GovShield Client platform which is identified as Samsung Android 15 mobile devices. The TOE components in the AGD match the TOE components defined in the ST.

ALC_CMC.1 – *"The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a website advertising the TOE, the evaluator shall examine the information on the website to ensure that the information in the ST is sufficient to distinguish the product.."*

The evaluation team verified that the Security Target (ST), TOE, and Supplemental Administrative Guidance (AGD) were labeled consistently to correctly identify the operational environment and TOE software versions in the CC evaluation.

Specifically, Section 1.2 of the ST states in the TOE Reference that the TOE is the GovShield Version 1.60.05

The title page of the AGD documents state that the TOE is the GovShield Version 1.60.05. TOE components described in AGD are:

- GovShield Installation Guide describes installation procedures for establishing the GovShield Server
- GovShield User Guide describes the GovShield Client and the use of the GovShield Server administrative interface to manage the GovShield Clients.
- All version references in both documents refer to 1.60.05

The above 1.60.05 references matches the TOE components listed in section 1.2 of the ST.

There is currently no public web page advertising the TOE.

All of this information as stated above provides sufficient context to accurately identify the TOE as such in the ST and AGD.

ALC_CMS.1 – *"The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the evaluation activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.*

Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in-depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation.

The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.."

The evaluation team confirmed the TOE had a unique identifier under ALC_CMC.1 which is GovShield Version 1.60.05. The evaluation team reviewed the following documentation and confirmed that this identifier was consistently used to reference the TOE:

(1) *GovShield Version 1.60.05 Security Target v1.0, February 6, 2026* [ST]
(2) *GovShield Installation Guide v1.0, February 6, 2026* [Install Guide]
(3) *GovShield User Guide v1.0, February 6, 2026* [User Guide]

ATE_IND.1 – *"The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Evaluation Activities. While it is not necessary to have one test case per test listed in an evaluation activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered.*

The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result"

The evaluation team created a Detailed Test Report (DTR) to address all aspects of this requirement. The DTR is made up of the proprietary GovShield Version 1.60.05 Test Plan (Proprietary_BoozAllen_GovShield_MDMv4_Server+Agent_Test_Plan.docx) and the Proprietary_BoozAllen_GovShield_MDMv4_Server+Agent_ATE_TestMatrix_Results.xlsx. The DTR discusses the test facility, environment, configuration, test tools, equivalency argument, test cases, test procedures, expected results, identification of evidence collected, and analysis of test results. The evaluator's test environment diagram is located in section entitled Test Environment of the GovShield Version 1.60.05 Test Plan document. Section 4 of this document presents a public releasable summary of the testing activity per SFR accomplished during testing. Therefore, this assurance activity is considered satisfied.

AVA_VAN.1 – *"As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in network infrastructure devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated."*

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the MDMPP and AGENTMOD requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	**Description**
Progeny	This is a generic term for searching for known vulnerabilities for the specific product (Former name)
GovShield	This is a generic term for searching for known vulnerabilities for the specific product. Use version 1.60.05 only if necessary
General Dynamics Mission Systems	The vendor.
JBoss EAP 7.4	TOE is installed on JBoss enterprise application platform.
Generic Terminology	
Mobile Device Manager	Generic term
Mobile Device Agent	Generic term
Host Agent	Generic term
Third-Party Libraries	
Third-Party Libraries for GovShield Server	List is defined in the ST
Third-Party Libraries for GovShield Client app	List is defined in the ST

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (May 27, 2026). The following public vulnerability sources were searched:

a) Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
https://www.cvedetails.com/vulnerability-search.php

b) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories

c) Offensive Security Exploit Database: https://www.exploit-db.com/

d) National Vulnerability Database: https://nvd.nist.gov/vuln/search#/nvd/home

e) CISA KEV databases: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Upon the completion of the vulnerability analysis research, the team had 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:

* Network Exploitation and Network Interception : Any TOE communication over the network could be prone to eavesdropping and interception by a malicious party. The TOE should provide appropriate encryption and authentication mechanisms to secure all data in transit to mitigate eavesdropping, man-in-the-middle attack, and arp-poisoning.

* Bypass MDM / smart-phone Gatekeeper:

- Malicious MDM/EMM Enrollment : Installing a malicious management profile (via phishing links, SMS, or QR codes). Once the device is enrolled in an attacker-controlled EMM (Enterprise Mobility Management) system, the attacker has administrative control, including the ability to install, update, or remove apps.

- Silent App Installation : On Android devices, especially those with Samsung Knox or specific managed profiles, an MDM can push apps without user interaction. A malicious MDM can abuse this to silently install spyware or banking Trojans.

- Bypassing Security Controls : Just as SideStepper bypassed trust prompts in iOS, attackers can use malicious profiles to bypass Android's "Unknown Sources" restriction or "Restricted Settings" (introduced in Android 13).

- Man in the middle on MDM commands : Attackers can intercept the communication between the Android device and the MDM server, allowing them to hijack commands and force the device to install malicious apps signed with a rogue certificate.

* Malicious Code : There is a possibility of a software product being infected with a virus or malicious code even when coming directly from a vendor.

Conclusion:

During the course of the evaluation, the GovShield product had 8 third-party libraries that needed to be updated to mitigate medium through critical vulnerabilities before the completion of testing. The continuation of IND testing showed that the patches did not have an effect on the operations of the TOE. A final public search was performed May 27, 2026, using the keywords and list of libraries and versions defined in the ST, resulted in 0 vulnerability findings.

Based on the results of the above penetration testing, the evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

The evaluation team determined that the TOE was not vulnerable to any of the defined attacks or had unsatisfied publicly known vulnerabilities. There were no vulnerability issues discovered with the final version of the TOE, that could affect the security posture of a deployed system.

6 Evaluating Additional Components for a Distributed TOE

This section addresses assurance activities that are defined in the *Protection Profile for Mobile Device Management Version 4.0, April 25, 2019* [MDMPP] that correspond with distributed TOE Requirements.

Evaluator Actions for Assessing the ST – *"The evaluator shall examine the TSS to identify any extra instances of TOE components allowed in the ST and shall examine the description of how the additional components maintain the SFRs to confirm that it is consistent with the role that the component plays in the evaluated configuration. For example: the secure channels used by the extra component for intra-TOE communications (FPT_ITT) and external communications (FTP_ITC) must be consistent, the audit information generated by the extra component must be maintained, and the management of the extra component must be consistent with that used for the original instance of the component in the minimum configuration."*

Section 8.1 of the ST describes the minimum configuration…

The evaluation team reviewed all of Section 8 of the ST and determined that there are no instances where functionality is being described for these TOE components that would result in different SFR claims for adding one or more additional instances of these components. Therefore, the evaluation team has determined that adding additional instances of these TOE components would not impact the SFR claims made by the minimum configuration and the additional instances have consistent SFR claims to their minimum configuration equivalents.

Evaluator Actions for Assessing the Guidance Documentation – *"The evaluator shall examine the description of the extra instances of TOE components in the guidance documentation to confirm that they are consistent with those identified as allowed in the ST. This includes confirmation that the result of applying the guidance documentation to configure the extra component will leave the TOE in a state such that the claims for SFR support in each component are as described in the ST and therefore that all SFRs continue to be met when the extra components are present.*

The evaluator shall examine the secure communications described for the extra components to confirm that they are the same as described for the components in the minimum configuration (additional connections between allowed extra components and the components in the minimum configuration are allowed of course)."

Section 1 of the AGD: GovShield User Guide describes the minimum configuration as…

GovShield consists of a MDM Server (i.e., GovShield Server) and a client agent application (i.e., GovShield Client) installed on each managed Samsung Android device**.**

This is consistent with Sections 1.2 and 8.0 of the ST.

> "The minimum configuration for this evaluation is one GovShield Server, and one GovShield Client installed on an Android Mobile Device. Including additional GovShield Clients installed on multiple Android Mobile 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 minimum configuration for this evaluation is one Server and one Client installed on an Android device. Including additional Clients installed on multiple Android devices as part of an operational configuration will not affect the validity of the functional claims made within the TSS. All TSS descriptions regarding the role, operation, and management of a Client would be consistent with every additional Client and Android device added to the minimum evaluated configuration. Therefore, all TSS descriptions regarding the Client can be read with the

understanding that the descriptions would apply to one or more of these TOE components and the method in which the additional TOE components met the SFRs would be the same as their minimum configuration equivalent."

The evaluation team has concluded that if there was one or many GovShield Clients the SFRs will continue to be met.

Based upon the ST and AGD descriptions, communication between TOE components is based on HTTPS/TLS. The entirety of the AGD: Installation Guide configures the GovShield server and its underlying platform for secure communications with the GovShield Clients. All steps must be completed before being able to enroll a device. Sections 9.2 QR Code Device Provisioning of the AGD: GovShield User Guide describes the ability to enroll an Android device into the GovShield MDM Server for management. During enrollment, the GovShield Client is installed on the devices, which establishes a secure connection between the GovShield and the GovShield Client. Section 10 Device Setup in the AGD: GovShield User Guide provides the instructions to load the required X.509 certificate for communication with the GovShield MDM Server.

These sections describe the process in a manner that the procedures can be used for multiple devices and their respective GovShield Clients. The evaluation team has determined that since the procedures for configuring a single Android GovShield Client is the same as multiple instances of these TOE components, the secure communications between Android GovShield Clients and the GovShield are consistent.

Evaluator Actions for Testing the TOE – *"The evaluator tests the TOE in the minimum configuration as defined in the ST (and the guidance documentation).*

If the description of the use of extra components in the ST and guidance documentation identifies any difference in the SFRs allocated to a component, or the scope of the SFRs involved (e.g. if different selections apply to different instances of the component) then the evaluator tests these additional SFR cases that were not included in the minimum configuration.

In addition, the evaluator tests the following aspects for each extra component that is identified as allowed in the distributed TOE:

- *Communications: the evaluator follows the guidance documentation to confirm, by testing, that any additional connections introduced with the extra component and not present in the minimum configuration are consistent with the requirements stated in the ST (e.g. with regard to protocols and ciphersuites used). An example of such an additional connection would be if a single instance of the component is present in the minimum configuration and adding a duplicate component then introduces an extra communication between the two instances. Another example might be if the use of the additional components necessitated the use of a connection to an external authentication server instead of using locally stored credentials.*

- *Audit: the evaluator confirms that the audit records from different instances of a component can be distinguished so that it is clear which instance generated the record.*

- *Management: if the extra component manages other components in the distributed TOE then the evaluator shall follow the guidance documentation to confirm that management via the extra component uses the same roles and role holders for administrators as for the component in the minimum configuration."*

The evaluation team's review of ST and AGD determined that the description of the use of extra TOE components did not describe any difference in the SFRs allocated to the TOE components or increase the scope of the SFRs included within the evaluation. Therefore, the evaluation team determined that the

claims for the additional TOE component instances were consistent with their equivalent components in the minimum configuration.

The following functionality, defined in the test cases, were run multiple times throughout the course of testing. Multiple Android devices with the GovShield Client software were enrolled with the management server during these tests.

Communication:

- FCO_CPC_EXT.1 – Repeated these tests on 2nd Android device
- FPT_ITT.1(2) – Repeated these tests on 2nd Android device
- FTP_TRP.1(2) – Repeated these tests on 2nd Android device
- FIA_ENR_EXT.2 – This was tested in conjunction with FTP_TRP.1(2) activities since that SFR covers agent enrollment
- FIA_ENR_EXT.1 – This was tested in conjunction with FTP_TRP.1(2) activities since that SFR covers agent enrollment

The evaluation team found that when testing additional instances of the Android GovShield Client TOE components that no additional connections were introduced above those defined in the minimum configuration. The evaluation team determined that all connections between the different Android GovShield Clients to the GovShield MDM Server were identical with regards to the SFR claims.

Audit:

- FAU_GEN.1(2):
  - FIA_ENR_EXT.2
  - FAU_ALT_EXT.2

In conjunction with performing the communication tests, the required level of audit was generated for the above SFRs. The evaluation team verified that the audit records corresponding to another Android GovShield Client were distinguishable from their minimum configuration TOE component equivalents. Each audit record contained the unique Device ID of the Android GovShield Client device sending the records.

Management:

The set of Management SFRs from AGENTMOD are: FMT_POL_EXT.2, FMT_UNR_EXT.1, and FMT_SMF_EXT.4

According to section E.3 of the MDMPP:

> "Management: if the extra component manages other components in the distributed TOE then the evaluator shall follow the guidance documentation to confirm that management via the extra component uses the same roles and role holders for administrators as for the component in the minimum configuration."

Additional management testing beyond the minimum configuration would only apply in the case where any of the TOE GovShield Client components managed other TOE components. In FMT_POL_EXT.2, FMT_UNR_EXT.1, and FMT_SMF_EXT.4 the GovShield Client is responsible only for management of its own TOE component functions. Therefore, additional management testing beyond the minimum configuration is not required.

The evaluation team determined through testing that adding additional Android GovShield Clients to the minimum configuration did not impact the SFR claims for this evaluation, and that SFR functions being addressed by the additional TOE components were able to be distinguished from their minimum configuration counterparts.

7 Conclusions

The TOE was evaluated against the ST and has been found by this evaluation team to be conformant with the ST. The overall verdict for this evaluation is: Pass.

8 Glossary of Terms

Acronym	Definition
AGD	Administrative Guidance Documents
CA	Certificate Authority
CC	Common Criteria
CPU	Central Processing Unit
CSP	Critical Security Parameter
EAP	Enterprise Application Platform
E-FOTA	Samsung Knox Enterprise Firmware-over-the-air
ESXi	Elastic Sky X Integrated
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure over a bidirectional TLS encrypted tunnel
IP	Internet Protocol
IT	Information Technology
Java SE	Java Standard Edition
MAS	Mobile Application Store
MD	Mobile Device
MDM	Mobile Device Management
NFC	Near-Field Communication
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
USB	Universal Serial Bus
WAP	Wireless Access Point
WLAN	Wireless Local Area Network

Table 7-1: Acronyms

Term	Definition
End User	An individual who possesses a mobile device that is managed by GovShield and who has limited authority to perform management functions using the Self-Service Portal
Role	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.
System Administrator	The class of TOE Administrators that have complete access to a GovShield environment, including the underlying Windows Server 2022 platform.

Administrator	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.
Authorized Administrator	Synonymous with Administrator.
MD User	User with a mobile device (MD).
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

Table 7-2: Terminology