McAfee Advanced Threat Defense 4.12 Security Target

Version 0.4
12/02/2021

Prepared for:

McAfee, LLC.

6220 America Center Drive

Santa Clara, CA 95002

Prepared By:

Gossamer Laboratories

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is McAfee Advanced Threat Defense provided by McAfee Inc. The TOE is being evaluated as a network infrastructure device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – McAfee Advanced Threat Defense 4.12 Security Target

ST Version – Version 0.4

ST Date – 12/02/2021

1.2 TOE Reference

TOE Identification – McAfee Advanced Threat Defense 4.12

TOE Developer – McAfee, LLC.

Evaluation Sponsor – McAfee, LLC.

1.3 TOE Overview

The Target of Evaluation (TOE) is McAfee Advanced Threat Defense (ATD) running software version 4.12. ATD detects today's stealthy, zero-day malware with a layered approach. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic analysis (sandboxing) to analyze actual behavior.

1.4 TOE Description

The ATD hardware appliance implements dynamic and statistical analysis on data transmitted through a network to provide malware detection, assessment and classification.

The ATD processes the files through the down selectors for statistical analysis and provides a sandbox test environment which includes virtual machines running customer environments, anti-virus, anti-malware, local blacklist and whitelists. Files are executed within virtual machine environments that are monitored by the log file. The log file is then used to generate a security report of the potential malware.

For the purpose of evaluation, ATD will be treated as a network device offering CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records).

1.4.1 TOE Architecture

ATD is provided as a hardware network appliance. The product provides a web interface over TLS and a console connection.

There are 2 versions of the ATD product (ATD-3100 and ATD-6100). While there are different models in the TOE, they differ primarily in physical form factor, number and types of connections and slots, and relative performance but they each provide the same security characteristics as claimed in this security target.

1.4.1.1 Physical Boundaries

The ATD evaluated configuration includes software version 4.12 running on one of the following models:

- ATD-3100 with two E5-2609v4 (Broadwell)
- ATD-6100 with two E5-2695v4 (Broadwell)

Since the same software is installed on both platforms and all security functions provided by the TOE are implemented in software, the TOE security behavior is the same on both platforms for each of the SFRs defined by the NDcPP22e. Both platforms are running Linux 4.19 kernel and McAfee OpenSSL FIPS Object Module v1.0.2c which is why the exact same software (version 4.12) operates on both platforms. The differences are related to performance – number of CPUs and amount of memory and HD/SSD storage.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the audit log storage space on the evaluated appliances. The TOE can also sync its time with a NTP server. DNS is used to resolve names when performing certificate checking.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by McAfee Advanced Threat Defense:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management

- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log or export them to a syslog server using a TLS protected channel.

1.4.1.2.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its TLS and NTP implementations. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

1.4.1.2.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes. The TOE also provides X.509 certificate checking for its TLS connections.

1.4.1.2.4 Security management

The TOE provides a command line (CLI) management interface as well as a graphical user interface (GUI) accessed via the web. The web interface is protected with TLS. The management interface is limited to the authorized administrator (as defined by a role).

1.4.1.2.5 Protection of the TSF

The TOE provides a variety of means of protecting itself. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. It provides a hardware clock to ensure reliable timestamps and can also sync to an NTP server if configured. It protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an authorized administrator.

1.4.1.2.6 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

1.4.1.2.7 Trusted path/channels

The TOE provides a local console which is subject to physical protection. For remote access, the web GUI is protected by TLS thus ensuring protection against modification and disclosure.

The TOE also protects its audit records from modification and disclosure by using TLS to communicate with the syslog server.

1.4.2 TOE Documentation

McAfee provides a Common Criteria Guide as part of the evaluation. The following document was examined as part of the evaluation:

- Configuration Guide for Common Criteria Evaluation McAfee Advanced Threat Defense 4.12

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant
- Package Claims:
    - collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
- NIAP Technical Decisions

Technical Decision	Applied	Notes
TD0527	Yes	
TD0528	Yes	
TD0536	Yes	
TD0537	No	SFR not claimed
TD0538	Yes	
TD0546	No	SFR not claimed
TD0547	Yes	
TD0555	Yes	
TD0556	Yes	
TD0563	Yes	
TD0564	Yes	
TD0569	No	SFR not claimed
TD0570	Yes	
TD0571	Yes	
TD0572	Yes	
TD0580	Yes	
TD0581	Yes	
TD0591	Yes	
TD0592	Yes	

2.1 Conformance Rationale

The ST conforms to the NDcPP22e. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDcPP22e and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

In general, the NDcPP22e has defined Security Objectives appropriate for network devices and as such are applicable to the McAfee Advanced Threat Defense TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e. The NDcPP22e defines the following extended requirements and since they are not redefined in this ST the NDcPP22e should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
- NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication
- NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication
- NDcPP22e:FIA_PMG_EXT.1: Password Management
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
- NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps
- NDcPP22e:FPT_TST_EXT.1: TSF testing
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDcPP22e. The refinements and operations already performed in the NDcPP22e are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e and any residual operations have been completed herein. Of particular note, the NDcPP22e made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP22e which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the NDcPP22e that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The NDcPP22e should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by McAfee Advanced Threat Defense TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP22e:FAU_GEN.1: Audit Data Generation
	NDcPP22e:FAU_GEN.2: User identity association
	NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP22e:FCS_CKM.1: Cryptographic Key Generation
	NDcPP22e:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP22e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP22e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP22e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP22e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP22e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
	NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
	NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication
	NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication
FIA: Identification and authentication	NDcPP22e:FIA_AFL.1: Authentication Failure Management
	NDcPP22e:FIA_PMG_EXT.1: Password Management
	NDcPP22e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	NDcPP22e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP22e:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP22e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP22e:FMT_SMF.1: Specification of Management Functions
	NDcPP22e:FMT_SMR.2: Restrictions on Security Roles

FPT: Protection of the TSF	NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
	NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps
	NDcPP22e:FPT_TST_EXT.1: TSF testing
	NDcPP22e:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP22e:FTA_SSL.3: TSF-initiated Termination
	NDcPP22e:FTA_SSL.4: User-initiated Termination
	NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP22e:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel
	NDcPP22e:FTP_TRP.1/Admin: Trusted Path

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP22e:FAU_GEN.1)

NDcPP22e:FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***];

d) Specifically defined auditable events listed in Table 2.

Requirement	Auditable Events	Additional Content
NDcPP22e:FAU_GEN.1		
NDcPP22e:FAU_GEN.2		
NDcPP22e:FAU_STG_EXT.1		
NDcPP22e:FCS_CKM.1		
NDcPP22e:FCS_CKM.2		
NDcPP22e:FCS_CKM.4		
NDcPP22e:FCS_COP.1/DataEncryption		
NDcPP22e:FCS_COP.1/Hash		
NDcPP22e:FCS_COP.1/KeyedHash		
NDcPP22e:FCS_COP.1/SigGen		
NDcPP22e:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure
NDcPP22e:FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
NDcPP22e:FCS_RBG_EXT.1		

NDcPP22e:FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP22e:FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP22e:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_PMG_EXT.1		
NDcPP22e:FIA_UAU.7		
NDcPP22e:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
NDcPP22e:FIA_X509_EXT.2		
NDcPP22e:FIA_X509_EXT.3		
NDcPP22e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	
NDcPP22e:FMT_MTD.1/CoreData		
NDcPP22e:FMT_MTD.1/CryptoKeys		
NDcPP22e:FMT_SMF.1	All management activities of TSF data.	
NDcPP22e:FMT_SMR.2		
NDcPP22e:FPT_APW_EXT.1		
NDcPP22e:FPT_SKP_EXT.1		
NDcPP22e:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
NDcPP22e:FPT_TST_EXT.1		
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	
NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	
NDcPP22e:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	
NDcPP22e:FTA_TAB.1		
NDcPP22e:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel.	Identification of the initiator and target of failed trusted

	Failure of the trusted channel functions.	channels establishment attempt.
NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	

Table 2 Audit events

NDcPP22e:FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 2.

5.1.1.2 User identity association (NDcPP22e:FAU_GEN.2)

NDcPP22e:FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Protected Audit Event Storage (NDcPP22e:FAU_STG_EXT.1)

NDcPP22e:FAU_STG_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

NDcPP22e:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition, [***TOE shall consist of a single standalone component that stores audit data locally***]

NDcPP22e:FAU_STG_EXT.1.3

The TSF shall [***overwrite previous audit records according to the following rule: [events are written to a circular buffer and oldest events are overwritten first]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP22e:FCS_CKM.1)

NDcPP22e:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,

- ECC schemes using 'NIST curves' [P-256, P-384] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,

- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1,

].

5.1.2.2 Cryptographic Key Establishment (NDcPP22e:FCS_CKM.2)

NDcPP22e:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, 'Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' (TD0581 applied),
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 7919] (TD0580 applied),
].

5.1.2.3 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4)

NDcPP22e:FCS_CKM.4.1
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method
- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeroes]***];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [***o logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes]***]

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP22e:FCS_COP.1/DataEncryption)

NDcPP22e:FCS_COP.1.1/DataEncryption
The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, GCM as specified in ISO 19772***].

5.1.2.5 Cryptographic Operation (Hash Algorithm) (NDcPP22e:FCS_COP.1/Hash)

NDcPP22e:FCS_COP.1.1/Hash
The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384***] and message digest sizes [***160, 256, 384***] that meet the following: ISO/IEC 10118-3:2004.

5.1.2.6 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP22e:FCS_COP.1/KeyedHash)

NDcPP22e:FCS_COP.1.1/KeyedHash
The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384***] and cryptographic key sizes [***160, 256, 384 bits***] and message digest sizes [***160, 256, 384***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.7 Cryptographic Operation (Signature Generation and Verification) (NDcPP22e:FCS_COP.1/SigGen)

NDcPP22e:FCS_COP.1.1/SigGen
The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [***- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits]***]
that meet the following:
[***- For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3***].

5.1.2.8 HTTPS Protocol (NDcPP22e:FCS_HTTPS_EXT.1)

NDcPP22e:FCS_HTTPS_EXT.1.1
The TSF shall implement the HTTPS protocol that complies with RFC 2818.

NDcPP22e:FCS_HTTPS_EXT.1.2
The TSF shall implement HTTPS using TLS.

NDcPP22e:FCS_HTTPS_EXT.1.3
If a peer certificate is presented, the TSF shall [***not establish the connection***] if the peer certificate is deemed invalid.

5.1.2.9 NTP Protocol (NDcPP21:FCS_NTP_EXT.1)

NDcPP21:FCS_NTP_EXT.1.1
The TSF shall use only the following NTP version(s) [***NTP v4 (RFC 5905)***].

NDcPP21:FCS_NTP_EXT.1.2
The TSF shall update its system time using [***Authentication using [SHA1] as the message digest algorithm***].

NDcPP21:FCS_NTP_EXT.1.3
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses

NDcPP21:FCS_NTP_EXT.1.4
The TSF shall support configuration of at least three (3) NTP time sources

5.1.2.10 Random Bit Generation (NDcPP22e:FCS_RBG_EXT.1)

NDcPP22e:FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

NDcPP22e:FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[one] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.11 TLS Client Protocol Without Mutual Authentication (NDcPP22e:FCS_TLSC_EXT.1)

NDcPP22e:FCS_TLSC_EXT.1.1
The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[***TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,***
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289]
and no other ciphersuites.

NDcPP22e:FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [***the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN***].

NDcPP22e:FCS_TLSC_EXT.1.3
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [***Not implement any administrator override mechanism***].

NDcPP22e:FCS_TLSC_EXT.1.4
The TSF shall [***present the Supported Elliptic Curves/Supported Groups Extension with the***

following curves/groups: secp256r1, secp384r, ffdhe2048] and no other curves/groups] in the Client Hello.

5.1.2.12 TLS Server Protocol Without Mutual Authentication (NDcPP22e:FCS_TLSS_EXT.1)

NDcPP22e:FCS_TLSS_EXT.1.1
The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[***TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,***
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289]
and no other ciphersuites.

NDcPP22e:FCS_TLSS_EXT.1.2
The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [***TLS 1.1,***].

NDcPP22e:FCS_TLSS_EXT.1.3
The TSF shall perform key establishment for TLS using [***Diffie-Hellman groups [ffdhe2048], ECDHE curves secp384r1] and no other curves***].

NDcPP22e:FCS_TLSS_EXT.1.4
The TSF shall support [***session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)***].

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

NDcPP22e:FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within [***3-5***] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

NDcPP22e:FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed***].

5.1.3.2 Password Management (NDcPP22e:FIA_PMG_EXT.1)

NDcPP22e:FIA_PMG_EXT.1.1
The TSF shall provide the following password management capabilities for administrative passwords:
a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')'***];
b) Minimum password length shall be configurable to between [***5***] and [***15***] characters.

5.1.3.3 Protected Authentication Feedback (NDcPP22e:FIA_UAU.7)

NDcPP22e:FIA_UAU.7.1
The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.3.4 Password-based Authentication Mechanism (NDcPP22e:FIA_UAU_EXT.2)

NDcPP22e:FIA_UAU_EXT.2.1

The TSF shall provide a local [***password-based***] authentication mechanism to perform local administrative user authentication.

5.1.3.5 User Identification and Authentication (NDcPP22e:FIA_UIA_EXT.1)

NDcPP22e:FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:
- Display the warning banner in accordance with FTA_TAB.1;
- [***no other actions***].

NDcPP22e:FIA_UIA_EXT.1.2

The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.1.3.6 X.509 Certificate Validation (NDcPP22e:FIA_X509_EXT.1/Rev)

NDcPP22e:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:
- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [***the Online Certificate Status Protocol (OCSP) as specified in RFC 6960***]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

NDcPP22e:FIA_X509_EXT.1.2/Rev

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.1.3.7 X.509 Certificate Authentication (NDcPP22e:FIA_X509_EXT.2)

NDcPP22e:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***TLS***], and [***no additional uses***].

NDcPP22e:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***not accept the certificate***].

5.1.3.8 X.509 Certificate Requests (NDcPP22e:FIA_X509_EXT.3)

NDcPP22e:FIA_X509_EXT.3.1

The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization, Organizational Unit, Country***].

NDcPP22e:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (NDcPP22e:FMT_MOF.1/ManualUpdate)

NDcPP22e:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

5.1.4.2 Management of TSF Data (NDcPP22e:FMT_MTD.1/CoreData)

NDcPP22e:FMT_MTD.1.1/CoreData

The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.1.4.3 Management of TSF Data (NDcPP22e:FMT_MTD.1/CryptoKeys)

NDcPP22e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.4 Specification of Management Functions (NDcPP22e:FMT_SMF.1)

NDcPP22e:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***- Ability to set the time which is used for time-stamps,***
  - Ability to configure NTP,
  - Ability to configure the reference identifier for the peer,
  - Ability to manage the cryptographic keys,
  - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors
  - Ability to import X509v3 certificates to the TOE's trust store].

5.1.4.5 Restrictions on Security Roles (NDcPP22e:FMT_SMR.2)

NDcPP22e:FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

NDcPP22e:FMT_SMR.2.2

The TSF shall be able to associate users with roles.

NDcPP22e:FMT_SMR.2.3

The TSF shall ensure that the conditions
- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely are satisfied.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Protection of Administrator Passwords (NDcPP22e:FPT_APW_EXT.1)

NDcPP22e:FPT_APW_EXT.1.1

The TSF shall store administrative passwords in non-plaintext form.

NDcPP22e:FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext administrative passwords.

5.1.5.2 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP22e:FPT_SKP_EXT.1)

NDcPP22e:FPT_SKP_EXT.1.1
The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.5.3 Reliable Time Stamps (NDcPP22e:FPT_STM_EXT.1)

NDcPP22e:FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.
NDcPP22e:FPT_STM_EXT.1.2
The TSF shall [***allow the Security Administrator to set the time, synchronise time with an NTP server***].

5.1.5.4 TSF testing (NDcPP22e:FPT_TST_EXT.1)

NDcPP22e:FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [***during initial start-up (on power on), periodically during normal operation***] to demonstrate the correct operation of the TSF:

- ***Power-on Self-Tests:***
  - ***Firmware Integrity Test***
  - ***Known Answer Tests:***
    - ***HMAC KAT***
    - ***AES KAT***
    - ***AES CCM KAT***
    - ***AES GCM KAT***
    - ***XTS-AES KAT***
    - ***AES CMAC KAT***
    - ***Triple-DES KAT***
    - ***Triple-DES CMAC KAT***
    - ***RSA KAT***
    - ***DSA PCT***
    - ***DRBG KAT***
    - ***ECDSA PCT***
    - ***ECC CDH KAT***
- ***Conditional Self-Tests (run periodically during normal operation):***
  - ***DRBG Tested as required by [SP800-90] Section 11***
  - ***DRBG FIPS 140-2 continuous test for stuck fault***
  - ***NDRNG FIPS 140-2 continuous test for NDRNG***
  - ***DSA Pairwise consistency test on each generation of a key pair***
  - ***ECDSA Pairwise consistency test on each generation of a key pair***
  - ***RSA Pairwise consistency test on each generation of a key pair***

].

5.1.5.5 Trusted update (NDcPP22e:FPT_TUD_EXT.1)

NDcPP22e:FPT_TUD_EXT.1.1
The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].
NDcPP22e:FPT_TUD_EXT.1.2
The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

NDcPP22e:FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (NDcPP22e:FTA_SSL.3)

NDcPP22e:FTA_SSL.3.1

The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.6.2 User-initiated Termination (NDcPP22e:FTA_SSL.4)

NDcPP22e:FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.6.3 TSF-initiated Session Locking (NDcPP22e:FTA_SSL_EXT.1)

NDcPP22e:FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.6.4 Default TOE Access Banners (NDcPP22e:FTA_TAB.1)

NDcPP22e:FTA_TAB.1.1

Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Inter-TSF trusted channel (NDcPP22e:FTP_ITC.1)

NDcPP22e:FTP_ITC.1.1

The TSF shall be capable of using [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***no other capabilities***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

NDcPP22e:FTP_ITC.1.2

The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

NDcPP22e:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [***transmitting audit records to an audit server***].

5.1.7.2 Trusted Path (NDcPP22e:FTP_TRP.1/Admin)

NDcPP22e:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***TLS***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

NDcPP22e:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP22e:FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 3 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the useraccessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c
The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c
The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c
The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c
The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c
The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c
The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d
The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c
The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c
The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e
The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d
The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c
The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d
The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c
The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c
The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d
The developer shall provide the TOE for testing.

ATE_IND.1.1c
The TOE shall be suitable for testing.

ATE_IND.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e
The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d
The developer shall provide the TOE for testing.

AVA_VAN.1.1c
The TOE shall be suitable for testing.

AVA_VAN.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e
The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e
The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE generates audit events (see **Table 2 Audit events**) and has the capability to store them internally or export them to an audit log server. The TOE stores its internal audit events in a log that is protected with permission bits so that only the authorized administrator can read the audit events.

The internal audit log is written to a file which gets rolled over at 20MB. The authorized administrator is instructed to export audit events to a syslog server in real -time. The audit logs corresponding to the events are simultaneously sent to the external syslog server and local store. The TOE can be configured to use TLS to protect audit logs exported to the external server.

The Security audit function satisfies the following security functional requirements:

- NDcPP22e:FAU_GEN.1: The TOE can generate all the required auditable events as specified in **Table 2 Audit events**. Within each audit event is date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 2 Audit events**. For cryptographic keys, the act of importing, exporting or deleting a key is audited by name and the associated administrator account is identified.
- NDcPP22e:FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- NDcPP22e:FAU_STG_EXT.1: The TOE can be configured to export audit records to an external syslog server. This communication is protected using TLS.

6.2 Cryptographic support

The TOE contains the McAfee OpenSSL FIPS Object Module v1.0.2c that has been CAVP tested. In CC mode the TOE only uses CAVP tested algorithms and no further configuration is needed. The following functions have been CAVP tested to meet the associated SFRs.

Functions	Requirement	Certificates
Encryption/Decryption		
• AES GCM and CBC (128 or 256 bits)	FCS_COP.1/DataEncryption	A2063
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FCS_COP.1/SigGen	A2063
Cryptographic hashing		
• SHA-1, SHA-256, SHA-384 (digest sizes 160, 256, 384 bits)	FCS_COP.1/Hash	A2063
Keyed-hash message authentication		
• HMAC-SHA-1/256/384	FCS_COP.1/KeyedHash	A2063
Random bit generation		
• AES-256 CTR_DRBG with software based noise sources with a minimum of 256 bits of non-determinism	FCS_RBC_EXT.1	A2063

Key generation		
• RSA Key Generation (key size 2048)	FCS_CKM.1	A2063
• ECDSA Key Generation (P-256, P-384)	FCS_CKM.1	A2063
• DSA Key Generation (key size 2048)	FCS_CKM.1	A2063
Key Establishment		
• CVL KAS FFC	FCS_CKM.2	A2063
• CVL KAS ECC	FCS_CKM.2	A2063

Table 4 Cryptographic Functions

The TOE uses a software-based random bit generator that complies with Special Publication 800-90 using CTR_DRBG when operating in the FIPS mode. AES-256 is used in conjunction with a minimum of 256 bits of entropy.

In CC mode, the TOE provides TLS v1.2 for use by the web GUI and for protecting communications between the TOE and audit server. The TOE supports the following ciphersuites for syslog interfaces.

- TLS_RSA_WITH_AES_128_GCM_SHA256,
- TLS_RSA_WITH_AES_256_GCM_SHA384,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The TOE supports the following ciphersuites for its management interfaces

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

The following table presents the crypto security parameters (CSPs), secret keys, and private keys provided by the TOE. The table also identifies when each CSP or key is cleared.

CSP or Key:	Stored in	Zeroized upon:	Zeroized by:
TLS host RSA private key	On Disk	Admin Command to delete/change	Overwriting with zeros
TLS host RSA digital certificate	On Disk	Admin Command to delete/change	Overwriting with zeros
TLS pre-master secret	In Memory	Handshake done	Overwriting with pseudo random data
TLS session key	In Memory	Close of session	Overwriting with pseudo random data
Password hash	On Disk	Admin Command to delete/change	Overwriting once with zeros

The Cryptographic support function satisfies the following security functional requirements:

- NDcPP22e:FCS_CKM.1: The TOE supports asymmetric key generation using RSA, ECDSA and DSA for key establishment as part of TLS as described in the section above. The TOE acts as both a client and a server.

Scheme	Protocol	Service
RSA	TLS	Syslog (client)

ECDSA	TLS	Remote Administration (server), Syslog (client)
FFC	TLS	Remote Administration (server), Syslog (client)

Table 5 Service, Protocol and Key Establishment Scheme Mapping

- NDcPP22e:FCS_CKM.2: See FCS_CKM.1.
- NDcPP22e:FCS_CKM.4: All data is cleared as identified above.
- NDcPP22e:FCS_COP.1/DataEncryption: The TOE performs encryption and decryption using AES in either CBC or GCM mode, and key sizes of either 128 or 256.
- NDcPP22e:FCS_COP.1/Hash: The TOE supports cryptographic hashing services using SHA-1, SHA-256, and SHA-384, with digest sizes 160, 256, and 384. The hashing functions are used as part of TLS and signature verification for the image.
- NDcPP22e:FCS_COP.1/KeyedHash: The TOE supports keyed-hash message authentication using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384 using SHA-1/256/384 with 160/256/384-bit keys to produce a 160/256/384 output MAC. The SHA-1/256 and 384 algorithms have block sizes of 512 and 1024-bits respectively.
- NDcPP22e:FCS_COP.1/SigGen: The TOE supports the use of RSA with 2048 bit key sizes for cryptographic signatures. Digital signatures are used in TLS communications and on product updates.
- NDcPP22e:FCS_HTTPS_EXT.1: The TOE provides an HTTPS/TLS interface for GUI administration. The TOE implements the HTTPS protocol in accordance with RFC 2818.
- NDcPP22e:FCS_NTP_EXT.1: The TOE supports NTPv4 authenticating the NTP server that it synchronizes to using a sha1 message digest. The TOE allows one or more NTP servers to be configured. At least one is required for time synchronization to occur, but more than 3 NTP servers can be specified.
- NDcPP22e:FCS_RBG_EXT.1: The product uses an SP 800-90A AES-256 CTR_DRBG with software based noise sources with a minimum of 256 bits of non-determinism.
- NDcPP22e:FCS_TLSC_EXT.1: The TOE supports TLS v1.2 with the ciphersuites listed above for its syslog connection. The TOE supports the use of FQDN/hostname and IPv4 addresses as reference identifiers within a certificate's CommonName (CN) or Subject Alternate Name (SAN) extension. The TOE checks the SAN/CN when performing certificate validation as described in NDcPP22e:FIA_X509_EXT.1/Rev. Wildcards are allowed in certificates. The TOE does not support certificate pinning. IP addresses are converted to binary by parsing decimal delimited by periods. The conversion happens before any comparisons are made. Canonical format is enforced. Elliptical curves P-256 and P-384 are supported as well as DH 2048. These are not configurable.
- NDcPP22e:FCS_TLSS_EXT.1: The TOE supports TLS v1.2 with the ciphersuites listed above for the web management interface. The TOE will reject all SSL and older TLS versions (1.0, 1.1) for connection attempts. Elliptical curve P-384 is supported as well as DH 2048. The TOE performs session resumption based on session IDs according to RFC 5246.

6.3 Identification and authentication

The TOE provides a password mechanism for authenticating users. Users are associated with a username, password, and one or more roles. Users may authenticate locally or via the web interface. Passwords can be composed of any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1). Passwords are not echoed back when users logon to the TOE. Passwords can be between 1-64 characters.

The Authorized Administrator can set a lockout failure count for login attempts. If the count is exceeded, the targeted account is locked for an administrator-configurable time limit. The local console is always available even if the Web GUI is locked out.

The TOE requires identification and authentication before allowing access. Only the banner may be presented before authentication is complete.

The Identification and authentication function satisfies the following security functional requirements:

- NDcPP22e:FIA_AFL.1: An administrator account can be locked after failed authentication attempts. In order to re-establish the account, a settable time period must pass. Only the Web GUI account can be locked.
- NDcPP22e:FIA_PMG_EXT.1: The TOE offers a wide range of characters for passwords as described above.
- NDcPP22e:FIA_UAU.7: The TOE does not echo passwords as they are entered.
- NDcPP22e:FIA_UAU_EXT.2: The TOE provides a password mechanism for authentication.
- NDcPP22e:FIA_UIA_EXT.1: The only service offered by the TOE before authentication is complete is the displaying of the logon banner. The TOE provides a password mechanism for authenticating users via is console or Web GUI interfaces. Users are associated with a username, password, and one or more roles.
- NDcPP22e:FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate revocation. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE. The following fields are verified as appropriate:
  - Expiry date and time.
  - CA flag if not end certificate.
  - Certificate key size should be greater or equal to 2048
  - Certificate signature methods: sha256, sha384
  - Certificate presented identifier (hostname/IP) should match an entry in SAN or CN (if match not found in SAN)
  - Wildcard validation of SAN or CN field for presented identifier, it should be in the left-most domain level and there shouldn't be more than one wildcard in any of the entries
  - Certificate chain validation. Root CA must be trusted by MATD.
  - Certificate revocation check using OCSP. Authority information access (AIA) URL is must for checking revocation status, MATD accepts only HTTP URL in AIA.
  - X509v3 Extended Key Usage for purpose like server authentication, client authentication, certificate signing and OSCP signing
- NDcPP22e:FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted. If the OCSP server cannot be contacted for validity checks, then the connection is not established. Certificates are loaded in the trusted CA bundle for use when making validity checks. The TOE needs trusted root certificates in order to make validity checks.
- NDcPP22e:FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates.

6.4 Security management

The TOE provides an administrator role. User accounts that are associated with the administrator role are considered authorized administrators. An Authorized Administrator can access audit configuration data, user and administrator security attributes (including [re]setting passwords, but not viewing an existing password), warning banner configuration, and cryptographic support settings.

The TOE offers two administrative interfaces – command line and GUI. The TOE offers command line functions which are accessible via the CLI. The CLI is a text-based interface which can be accessed from a directly connected terminal. These command line functions can be used to manage basic settings such as IP address and recovery options. The functions that are specific to the CLI are unlocking user (accessible only by admin user), setting session timeout threshold for user inactivity, configuring interfaces, and options for debug and recovery.

The TOE also offers a web interface for management. The web interface offers access to the same functions as the CLI. The web interface is available using TLS v1.2. The web interface offers advanced management capabilities including setting CC mode, managing the audit trail, managing cryptographic keys, and certificate management.

The Security management function satisfies the following security functional requirements:

- NDcPP22e:FMT_MOF.1/ManualUpdate: Only the administrator can initiate product updates.
- NDcPP22e:FMT_MTD.1/CoreData: Only the administrator can configure TSF-related functions. The TOE will display a banner prior to login but the users do not have any way to manipulate the TOE without logging in. The trust store is accessed when administrators import/remove certificates as described in the Admin Guide. The trust store is protected by default and is restricted such that only administrators have access.
- NDcPP22e:FMT_MTD.1/CryptoKeys – Only the administrator can generate certificate requests and import certificates using the web GUI.
- NDcPP22e:FMT_SMF.1: The TOE includes the functions (both locally and remotely) necessary to manage certificates and the certificate store, configure the warning banner, manage user accounts, set the time, configuring the session inactivity time before session termination or locking, manage cryptographic keys, and to manage and verify updates of the TOE software and firmware.
- NDcPP22e:FMT_SMR.2: The TOE includes an administrator account that corresponds to the required 'Authorized Administrator' also referred to as 'Security Administrator' in some requirements or text.

6.5 Protection of the TSF

The TOE is an appliance and does not offer general purpose operating system interfaces to users. The does not provide access to locally stored passwords) and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE.

The TOE is a hardware appliance that includes a real-time clock. The TOE uses the clock to support several security functions including timestamps for audit records, timing elements of cryptographic functions, and inactivity timeouts. The TOE also has the ability to sync its time with an NTP server.

The TOE contains a cryptomodule (McAfee OpenSSL FIPS Object Module v1.0.2c) based on the OpenSSL 1.0.2v module. All MATD processing (sample acceptance, analysis and reporting) is coordinated by Advance Malware Analysis System (AMAS). When this core component starts up, it checks the sanity of the openssl library, using the fipscheck binary on /lib64/libcrypto.so.10. The module performs the set of FIPS power-on tests specified in Section 5.1.5.4. Upon failing any of its FIPS mode power-on self-tests, the TOE's AMAS service will abort.

The TOE supports loading updates by the administrator using CLI commands. To determine the current version, the administrator logs on to the CLI and verifies the software version using "show" command. The administrator obtains the update, and the TOE automatically verifies its digital signature using a pre-loaded private key. An unverified update cannot be installed.

The Protection of the TSF function satisfies the following security functional requirements:

- NDcPP22e:FPT_APW_EXT.1: The TOE does not offer any interfaces that will disclose a plaintext password to any user. Additionally, passwords are not stored in plaintext on the TOE.
- NDcPP22e:FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose a stored cryptographic key to any users.
- NDcPP22e:FPT_STM_EXT.1: The TOE provides a hardware clock and the ability to sync time using an NTP Server.

NDcPP22e:FPT_TST_EXT.1: The TOE performs the following self-tests:

- Power-on Self-Tests:
  - Firmware Integrity Test
  - Known Answer Tests:

        - HMAC KAT
        - AES KAT
        - AES CCM KAT
        - AES GCM KAT
        - XTS-AES KAT
        - AES CMAC KAT
        - Triple-DES KAT
        - Triple-DES CMAC KAT
        - RSA KAT
        - DSA PCT
        - DRBG KAT
        - ECDSA PCT
        - ECC CDH KAT
    - Conditional Self-Tests (run periodically during normal operation):
        - DRBG Tested as required by [SP800-90] Section 11
        - DRBG FIPS 140-2 continuous test for stuck fault
        - NDRNG FIPS 140-2 continuous test for NDRNG
        - DSA Pairwise consistency test on each generation of a key pair
        - ECDSA Pairwise consistency test on each generation of a key pair
        - RSA Pairwise consistency test on each generation of a key pair.
- NDcPP22e:FPT_TUD_EXT.1: The TOE provides a means for obtaining an installing digitally signed updates.

6.6 TOE access

The TOE provides an inactivity timeout for console and web sessions. The authorized administrator can set the inactivity timeout. When an inactivity period is exceeded, the session is terminated. The user will be required to login in after any session has been terminated due to inactivity or after voluntary termination.

The TOE also provides the ability to set a login banner. The banner is displayed before a user session is established. The banner will be displayed when accessing the TOE via the console or TLS interfaces.

The TOE access function satisfies the following security functional requirements:

- NDcPP22e:FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- NDcPP22e:FTA_SSL.4: The TOE allows a user to logout (or terminate) both local and remote sessions.
- NDcPP22e:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- NDcPP22e:FTA_TAB.1: The TOE can be configured to display a login banner when administrators successfully establish interactive sessions with the TOE, allowing users to terminate their session prior to performing any functions.

6.7 Trusted path/channels

The TOE provides a trusted path for its remote administrative users accessing the TOE via a web GUI using TLS. Note that local administrator access via the serial port is also allowed for command line access. However, this access is protected by physical protection of the serial interface along with the TOE itself.

When an administrator attempts to connect to the TOE remotely, the TOE attempts to negotiate a session. If the session cannot be negotiated, the connection is dropped. When negotiating a TLS, the TOE and the client application (web browser) used by the administrator will negotiate the most secure algorithms available at both ends to protect that session. The available algorithms are identified in section 6.2 above.

Remote connections to third-party syslog servers are supported for exporting audit records to an external audit server. Communication with those external servers is protected using TLS. The TOE is acting as a client in this instance and receives a certificate from the audit server for identification.

In all cases, TLS ensures traffic is not modified or disclosed.

The Trusted path/channels function satisfies the following security functional requirements:

- NDcPP22e:FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that any exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification.
- NDcPP22e:FTP_TRP.1/Admin: The TOE provides TLS based on its cryptomodule to ensure secure remote administration. The administrator can initiate the remote session, the remote session is secured (disclosure and modification) using CAVP tested cryptographic operations.