Assurance Activity Report

Bastille Networks, Inc.
Bastille Enterprise Fusion Center Version 3.6

VID 11600

UL15574582-AAR
2026-01-12

Evaluated by

UL Verification Services Inc.
709 Fiero Lane, Suite 25
San Luis Obispo, CA 93401

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

TOE Evaluation Sponsor and Developer
Bastille Networks, Inc
499 Lake Ave,
Santa Cruz CA, 95062

ST Author
Dylan Lyman
UL Verification Services Inc.
709 Fiero Lane, Suite 25
San Luis Obispo, CA 93401

Evaluation Personnel
Oleg Andrianov
Meghana Achanta
Brad Mitchell
Michael Baron

Applicable Common Criteria Version
CC Version 3.1 R5, April 2017

Common Evaluation Methodology Version
CEM Version 3.1 R5, April 2017

Applicable Common Criteria Protection Profiles
Protection Profile for Application Software
Version 1.4, October 7, 2021

Table of Contents

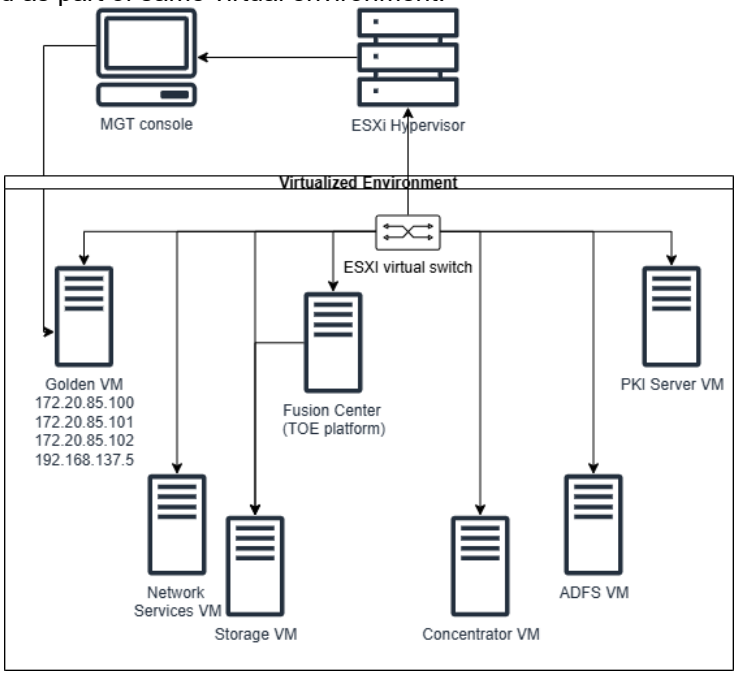
1 Overview

This document presents evaluation results of the Bastille Enterprise Fusion Center Version 3.6 against the Protection Profile for Application Software, Version 1.4, dated 2021-10-07 [PP]. This document contains a description of the assurance activities and associated results as performed by UL, an accredited Common Criteria Testing Laboratory. This Evaluation was conducted with the oversight and guidance provided by the National Information Assurance Partnership and its contributors.

1.1 Test Environment

The test environment used by the CCTL during the course of testing is briefly summarized below and conforms to the expected use-case of the TOE (Bastille Enterprise Fusion Center Version 3.6):

TOE is running on a platform in a Virtualized Environment on ESXi 8 hypervisor. Supporting Infrastructure has been implemented as part of same virtual environment.



1.2 Test Equivalency

The [ST] claims two platforms; therefore, testing occurred on both claimed platforms and no equivalency argument was necessary.

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the [ST] for a product claiming conformance to [PP].
The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in [PP]. The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in the Evaluation Technical Report. The evaluation team consisted of Oleg Andrianov, Meghana Achanta, Brad Mitchell, and Michael Baron from the CCTL. The test laboratory was configured by UL and physically located at the UL San Luis Obispo facility in an access-controlled environment.

1.3 TD's Applied

TD Number	Title	Applied
0628	Addition of Container Image to Package Format	Yes
0650	Conformance Claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	Yes (Implicitly). No SFR, SAR, or Assurance Activity text was modified.
0664	Testing activity for FPT_TUD_EXT.2.2	Yes
0717	Format changes for PP_APP_V1.4	Yes
0719	ECD for PP APP V1.3 and 1.4	Yes (Implicitly)
0736	Number of elements for iterations of FCS_HTTPS_EXT.1	Yes
0743	FPT_DIT_EXT.1.1 Selection Exclusivity	Yes
0747	Configuration Storage Option for Android	Yes
0756	Update for platform-provided full disk encryption	Yes
0780	FIA_X509_EXT.1 Test 4 Clarification	Yes
0798	Static memory Mapping Exceptions	Yes
0815	Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	Yes
0822	Correction to windows manifest file for FDP_DEC_EXT.1	Yes
0823	Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3	Yes
0844	Addition of Assurance Package for Flaw Remediation v1.0	Yes (Implicitly)
0865	Consistency of Cryptographic Key Sizes	Yes
0914	Addition of PKG_TLS_V2.0 to Conformance claims	No, package not claimed.
0931	Clarification when CTR_DRBG is selected for FCS_RBG_EXT.2.2 in PP_APP_V1.4	Yes
0945	Adding FIPS 186-5 in PP_APP_V1.4	No, SFRs not applicable to the TOE.
0964	Clarifications to FMT_MEC_EXT.1 Windows Test	No, Change not applicable to the TOE platform

2 SFR Assurance Activities and Results

2.1 FCS_CKM.1 Cryptographic Key Generation Services

TSS

*The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the **generate no asymmetric cryptographic keys** selection is present in the ST. Otherwise, the evaluation activities shall be performed as stated in the selection-based requirements.*

[ST] Section 6.1.1.1 claims that the application does not generate asymmetric keys which has been verified in [ST] Section 7.1.1.

Guidance Documentation

None.

Tests

None.

2.2 FCS_RBG_EXT.1 Random Bit Generation Services

TSS

If "use no DRBG functionality" is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services.

If "implement DRBG functionality" is selected, the evaluator shall ensure that additional FCS_RBG_EXT.2 elements are included in the ST.

If "invoke platform-provided DRBG functionality" is selected, the evaluator performs the following activities. The evaluator shall examine the TSS to confirm that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The evaluator shall determine that for each of these functions, the TSS states which platform interface (API) is used to obtain the random numbers. The evaluator shall confirm that each of these interfaces corresponds to the acceptable interfaces listed for each platform below.

It should be noted that there is no expectation that the evaluators attempt to confirm that the APIs are being used correctly for the functions identified in the TSS; the activity is to list the used APIs and then do an existence check via decompilation.

[ST] Section 6.1.1.2 selects “Use no DRBG functionality”.

[ST] Section 7.1.2 states that the TOE does not directly use a DRBG and uses a platform cryptographic module.

Guidance Documentation

None.

Tests

If "invoke platform-provided DRBG functionality" is selected, the following tests shall be performed:

The evaluator shall decompile the application binary using a decompiler suitable for the application (TOE). The evaluator shall search the output of the decompiler to determine that, for each API listed in

the TSS, that API appears in the output. If the representation of the API does not correspond directly to the strings in the following list, the evaluator shall provide a mapping from the decompiled text to its corresponding API, with a description of why the API text does not directly correspond to the decompiled text and justification that the decompiled text corresponds to the associated API.

The following are the per-platform list of acceptable APIs:

Platforms:Android...

The evaluator shall verify that the application uses at least one of javax.crypto.KeyGenerator class or the java.security.SecureRandom class or /dev/random or /dev/urandom.

Platforms:Microsoft Windows...

The evaluator shall verify that rand_s, RtlGenRandom, BCryptGenRandom, or CryptGenRandom API is used for classic desktop applications. The evaluator shall verify the application uses the RNGCryptoServiceProvider class or derives a class from System.Security.Cryptography.RandomNumberGenerator API for Windows Universal Applications. It is only required that the API is called/invoked, there is no requirement that the API be used directly. In future versions of this document, CryptGenRandom may be removed as an option as it is no longer the preferred API per vendor documentation.

Platforms:Apple iOS...

The evaluator shall verify that the application invokes either SecRandomCopyBytes, CCRandomGenerateBytes, or CCRandomCopyBytes, or uses /dev/random directly to acquire random.

Platforms:Linux...

The evaluator shall verify that the application collects random from /dev/random or /dev/urandom.

Platforms:Oracle Solaris...

The evaluator shall verify that the application collects random from /dev/random.

Platforms:Apple macOS...

The evaluator shall verify that the application invokes either CCRandomGenerateBytes or CCRandomCopyBytes, or collects random from /dev/random.

If invocation of platform-provided functionality is achieved in another way, the evaluator shall ensure the TSS describes how this is carried out, and how it is equivalent to the methods listed here (e.g. higher-level API invokes identical low-level API).

Test Number	1
Test Objective	N/A
Test Steps Performed	[ST] doesn't claim "invoke platform-provided DRBG functionality", hence this test is not applicable.
Test Result	Pass

2.3 FCS_STO_EXT.1 Storage of Credentials

TSS

The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.

[ST] Section 7.1.3 states that the TOE stores the TLS Server private key using Linux Keyring and the external users are authenticated using the JSON Web tokens authorized by the Active Directory Services.

[ST] Section 7.1.3 states that no other credentials are stored in non-volatile memory and verification of credentials is out of the scope of the evaluation.

Guidance Documentation

None.

Tests

For all credentials for which the application implements functionality, the evaluator shall verify credentials are encrypted according to FCS_COP.1/SKC or conditioned according to FCS_CKM.1.1/AK and FCS_CKM.1/PBKDF. For all credentials for which the application invokes platform-provided functionality, the evaluator shall perform the following actions which vary per platform.

Platforms:Android...
The evaluator shall verify that the application uses the Android KeyStore or the Android KeyChain to store certificates.

Platforms:Microsoft Windows...
The evaluator shall verify that all certificates are stored in the Windows Certificate Store. The evaluator shall verify that other credentials, like passwords, are stored in the Windows Credential Manager or stored using the Data Protection API (DPAPI). For Windows Universal Applications, the evaluator shall verify that the application is using the ProtectData class and storing credentials in IsolatedStorage.

Platforms:Apple iOS...
The evaluator shall verify that all credentials are stored within a Keychain.

Platforms:Linux...
The evaluator shall verify that all keys are stored using Linux keyrings.

Platforms:Oracle Solaris...
The evaluator shall verify that all keys are stored using Solaris Key Management Framework (KMF).

Platforms:Apple macOS...
The evaluator shall verify that all credentials are stored within Keychain.

Test Number	1
Test Objective	Verify that the one private key that the TOE utilizes for the TOE's web GUI/API is stored using Linux Keyrings.
Test Steps Performed	The evaluator identified the configuration files of the TOE which contain references to cryptographic key files and verified that the referenced key files were symbolically linked to the single FIFO file named 'var/lib/bastille/nginx.key'. The evaluator verified that this key file (nginx.key) was Linux file mode 600 and root:root owned. The evaluator then verified that the Linux keyring service was active and running.
Test Result	Pass

2.4 FDP_DEC_EXT.1. Access to Platform Resources

FDP_DEC_EXT.1.1

TSS

None.

Guidance Documentation

The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required.

[ST] Section 6.1.2.1, FDP_DEC_EXT.1.1 selected “network connectivity.” TOE platform does not have sensitive repositories, and the TOE does not have access to those.

[AGD] Section 2.2 states that the TOE includes a Fusion Center, whereas the Elasticsearch cluster, Apache Kafka cluster and Microsoft Active Directory Federation Services (ADFS) and other systems that the customer can try to integrate such as Splunk, are part of the operation environment.

[AGD] Section 8.0 provides the steps on how to configure network-parameters for ‘webhooks’ which allow the TOE to relay event data to other web applications such as Splunk and Elastic Logstash.

[ST] Section 6.1.2.1, FDP_DEC_EXT.1.2 selected “no sensitive information repositories.”

Tests[1]

Platforms:Android...
The evaluator shall verify that each uses-permission entry in the AndroidManifest.xml file for access to a hardware resource is reflected in the selection.

Platforms:Microsoft Windows...
For Windows Universal Applications the evaluator shall check the AppxManifest.xml file for a list of required hardware capabilities. The evaluator shall verify that the user is made aware of the required hardware capabilities when the application is first installed. This includes permissions such as ID_CAP_ISV_CAMERA, ID_CAP_LOCATION, ID_CAP_NETWORKING, ID_CAP_MICROPHONE, ID_CAP_PROXIMITY and so on. A complete list of Windows App permissions can be found at: http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx

For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of the required hardware resources.

Platforms:Apple iOS...
The evaluator shall verify that either the application or the documentation provides a list of the hardware resources it accesses.

Platforms:Linux...
The evaluator shall verify that either the application software or its documentation provides a list of the hardware resources it accesses.

Platforms:Oracle Solaris...
The evaluator shall verify that either the application software or its documentation provides a list of the hardware resources it accesses.

Platforms:Apple macOS...

[1] Modified by TD0822

The evaluator shall verify that either the application software or its documentation provides a list of the hardware resources it accesses.

Test Number	1
Test Objective	Verify that the [ST], and/or [AGD], provides a list of the hardware resources that the TOE accesses, and that the list is consistent with the selection in FDP_DEC_EXT.1.1.
Test Steps Performed	[ST] section 6.1.2.1 selects only “network connectivity” and “no sensitive information repositories.” [ST] Section 7.2.2 identifies the “network” as the hardware resource that the TOE accesses to perform its functions. [AGD] Section 3.0 states “The Bastille Enterprise Fusion Center requires only general computing hardware and network adapters”. The evaluator determined that the TOE accesses only the listed network hardware resources, which is consistent with the selection in FDP_DEC_EXT.1.1.
Test Result	Pass

FDP_DEC_EXT.1.2

TSS

None.

Guidance

The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to sensitive information repositories. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each sensitive information repository which it accesses, identify the justification as to why access is required.

[ST] Section 6.1.2.1, FDP_DEC_EXT.1.1 selected “network connectivity.” TOE platform does not have sensitive repositories, and the TOE does not have access to those.

[AGD] Section 2.2 states that the TOE includes a Fusion Center, whereas the Elasticsearch cluster, Apache Kafka cluster and Microsoft Active Directory Federation Services (ADFS) and other systems that the customer can try to integrate such as Splunk, are part of the operation environment.

[AGD] Section 8.0 provides the steps on how to configure network-parameters for ‘webhooks’ which allow the TOE to relay event data to other web applications such as Splunk and Elastic Logstash.

[ST] Section 6.1.2.1, FDP_DEC_EXT.1.2 selected “no sensitive information repositories.”

Tests[2]

Platforms:Android...

The evaluator shall verify that each uses-permission entry in the AndroidManifest.xml file for access to a sensitive information repository is reflected in the selection.

Platforms:Microsoft Windows...

For Windows Universal Applications the evaluator shall check the AppxManifest.xml file for a list of required capabilities. The evaluator shall identify the required information repositories when the application is first installed. This includes permissions such as

[2] Modified by TD0822

ID_CAP_CONTACTS,ID_CAP_APPOINTMENTS,ID_CAP_MEDIALIB and so on. A complete list of Windows App permissions can be found at:

http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx

For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of sensitive information repositories it accesses.

Platforms:Apple iOS...

The evaluator shall verify that either the application software or its documentation provides a list of the sensitive information repositories it accesses.

Platforms:Linux...

The evaluator shall verify that either the application software or its documentation provides a list of sensitive information repositories it accesses.

Platforms:Oracle Solaris...

The evaluator shall verify that either the application software or its documentation provides a list of sensitive information repositories it accesses.

Platforms:Apple macOS...

The evaluator shall verify that either the application software or its documentation provides a list of sensitive information repositories it accesses.

Test Number	1
Test Objective	Verify that either the application software or its documentation provides a list of sensitive information repositories the TOE application accesses.
Test Steps Performed	[ST] Section 6.1.2.1 selected “no sensitive information repositories.” [ST] section 7 does not describe or discuss sensitive information repositories accessed by the TOE. [AGD] does not instruct the administrator on how to access any sensitive repositories.
Test Result	Pass

2.5 FDP_NET_EXT.1 Network Communications

TSS

None.

Guidance Documentation

None.

Tests

The evaluator shall perform the following tests:
Test 1: The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user-initiated.

Test 2: The evaluator shall run the application. After the application initializes, the evaluator shall run network port scans to verify that any ports opened by the application have been captured in the ST for the

third selection and its assignment. This includes connection-based protocols (e.g. TCP, DCCP) as well as connectionless protocols (e.g. UDP).

Platforms:Android...
If "no network communication" is selected, the evaluator shall ensure that the application's AndroidManifest.xml file does not contain a uses-permission or uses-permission-sdk-23 tag containing android:name="android.permission.INTERNET". In this case, it is not necessary to perform the above Tests 1 and 2, as the platform will not allow the application to perform any network communication.

Test Number	1
Test Objective	Verify that any network communications witnessed are documented in the TSS or are user-initiated.
Test Steps Performed	The evaluator isolated each process of the TOE which interreacts with the network stack of the host platform. The evaluator stopped all TOE processes and started each TOE process individually while running a packet capture. The evaluator verified, using the packet capture, that the expected network connections (as defined in the TSS of [ST]) were consistent with what was observed in the packet captures. The evaluator repeated this process for all processes of the TOE, which included the following communication categories: • User-initiated • TOE response based on external entities • TOE/Application initiated.
Test Result	Pass

Test Number	2
Test Objective	Run network port scans to verify that any ports opened by the application have been captured in the [ST] for the third selection and its assignment.
Test Steps Performed	The evaluator started all TOE processes and verified that they were running. The evaluator ran a TCP port scan on all 65,535 TCP ports and expected to only see TCP ports 22, 80 and 443 open. The evaluator verified from the port scan that only TCP ports 22, 80 and 443 were open. The evaluator ran a UDP port scan on all 65,535 UDP ports and expected to see no UDP ports open. The evaluator verified in the port scan that no UDP ports were open.
Test Result	Pass

2.6 FDP_DAR_EXT.1 Encryption of Sensitive Application Data

TSS

The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the following activities cover all of the sensitive data identified in the TSS.
If "not store any sensitive data" is selected, the evaluator shall inspect the TSS to ensure that it describes how sensitive data cannot be written to non-volatile memory. The evaluator shall also ensure that this is consistent with the filesystem test below.

[ST] Section 7.2.1 states that only the TLS Server private key is stored in the non-volatile memory and no other sensitive data is retained.

Guidance Documentation

None.

Tests[3]

Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1.

If "implement functionality to encrypt sensitive data as defined in the PP-Module for File Encryption" or "protect sensitive data in accordance with FCS_STO_EXT.1" is selected, the evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted.

If "leverage platform-provided functionality" is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis.

Platforms:Android...
The evaluator shall inspect the TSS and verify that it describes how files containing sensitive data are stored with the MODE_PRIVATE flag set.

Platforms:Microsoft Windows...
The Windows platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption, such as BitLocker or Encrypting File System (EFS), clear to the end user.

Platforms:Apple iOS...
The evaluator shall inspect the TSS and ensure that it describes how the application uses the Complete Protection, Protected Unless Open, or Protected Until First User Authentication Data Protection Class for each data file stored locally.

Platforms:Linux...
The Linux platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption clear to the end user.

Platforms:Oracle Solaris...
The Solaris platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption clear to the end user.

Platforms:Apple macOS...
The macOS platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption clear to the end user.

Test Number	1
Test Objective	Identify sensitive data managed by the TOE, then perform the appropriate platform-specific test.

[3] Modified by TD0756

Test Steps Performed	[ST] Section 6.1.1.3 selected "invoke the functionality provided by the platform to securely store [TLS server private key]." [ST] does not select "leverage platform-provided functionality to encrypt sensitive data." [ST] Section 7.1.3 states that "The TOE does not store other credentials in non-volatile memory."
	[ST] does not list or describe any sensitive data other than the TLS server private key(s) whose security was evaluated in FCS_STO_EXT.1., Assurance activity states that "*Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1.".* As there is no sensitive data other than those covered by FCS_STO_EXT.1, this test is implicitly satisfied.
Test Result	Pass

2.7 FIA_X509_EXT.1 X.509 Certificate Validation (Selection-Based)

FIA_X509_EXT.1.1

TSS

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.

[ST] Section 7.3.1 states that the check of validity of certificates is performed using the platform-provided OpenSSL module in accordance with RFC 5280.

[ST] Section 7.3.1 states that validation is performed for every certificate in the certificate trust chain, up to the root certificate that is stored in the platform-managed root store.

Guidance Documentation

None.

Tests[4]

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 tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, 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. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created.

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.

[4] Modified by TD0780

Test Number	1
Test Objective	a) Verify that TOE properly accepts certificates with valid certification path. b) Verify that TOE rejects validation of a leaf certificate issued by an Intermediate CA without the basicConstraints field. c) Verify that TOE rejects validation of a leaf certificate issued by an Intermediate CA with basicConstraints field and CA=FALSE. d) Verify that TOE rejects validation of a leaf certificate issued by an Intermediate CA without the keyCertSign bit in a Key Usage field. e) Verify that TOE rejects validation of a leaf certificate issued by an Intermediate CA which was issued by another intermediate CA with path field=0. f) Verify that TOE rejects validation of a leaf certificate issued not by a CA certificate (resolved by objectives b) and c))
Test Steps Performed	a) The evaluator configured a TLS Server and started a CRL server. The evaluator established a successful TLS connection and verified the certificate chain with the configured webhooks on TOE. b) The evaluator created a certificate chain where one of the intermediate certificates did not have the basicConstraints extension and initiated a TLS connection and observed that the connection was refused by the TOE. c) The evaluator created a certificate chain where one of the intermediate certificates did not have the CA field enabled and initiated a TLS connection and observed that the connection was refused by the TOE. d) The evaluator created a certificate chain where one of the intermediate certificates did not have the keyCertSign bit in a Key Usage field and initiated a TLS connection and observed that the connection was refused by the TOE. e) The evaluator created a certificate chain where the leaf certificate was issued by an Intermediate CA which was issued by another intermediate CA with path field=0, and initiated a TLS connection and observed that the connection was refused by the TOE.
Test Result	Pass

Test 2*: The evaluator shall demonstrate that validating an expired certificate results in the function failing.*

Test Number	2
Test Objective	Verify that TOE rejects the expired certificate.
Test Steps Performed	The evaluator created a certificate chain with an expired certificate and initiated a TLS connection to the TOE with the configuration mentioned in Test 1 and observed that the connection was rejected by the TOE.
Test Result	Pass

Test 3: *The evaluator shall test that the TOE can properly handle revoked certificates-conditional on whether CRL, OCSP, OCSP Stapling or OCSP Multi-stapling is selected; if multiple methods are selected, then the following tests shall be performed for each method:*
The evaluator shall test revocation of the node certificate.
The evaluator shall also test revocation of an intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA), if intermediate CA certificates are supported.
If OCSP stapling per RFC 6066 is the only supported revocation method, 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.

Test Number	3
Test Objective	a) Verify that TOE rejects the connection where node certificate is revoked. b) Verify that TOE rejects the connection where Intermediate CA certificate is revoked. c) Verify that a valid certificate is accepted [covered by Test 1 Objective a)] and revoked certificate is rejected (covered by objective a and b of this test).
Test Steps Performed	a) The evaluator used the configuration and the certificate chain used in Test 1 and configured the CRL server to revoke a node certificate. The evaluator observed that the connection was rejected by the TOE. b) The evaluator used the configuration and the certificate chain used in Test 1 and configured the CRL server to revoke the intermediate certificate. The evaluator observed that the connection was rejected by the TOE. c) This is completed by Objective a and Objective b of the above tests.
Test Result	Pass

Test 4: If any OCSP option is selected, the evaluator shall configure the TSF to reject certificates if it cannot access valid status information, if so configurable. Then the evaluator shall ensure the TSF has no other source of revocation information available and configure the OCSP server or use a man-in-the-middle tool to present an OCSP response signed by a certificate that does not have the OCSP signing purpose and which is the only source of revocation status information advertised by the CA issuing the certificate being validated. The evaluator shall verify that validation of the OCSP response fails and that the TOE treats the certificate being checked as invalid and rejects the connection. If CRL is selected, the evaluator shall likewise configure the CA to be the only source of revocation status information, and sign a CRL with a certificate that does not have the cRLsign key usage bit set. The evaluator shall verify that validation of the CRL fails and that the TOE treats the certificate being checked as invalid and rejects the connection.

Test Number	4
Test Objective	a) Note: TOE does not claim OCSP. b) Verify that TOE rejects the CRL that is signed by unauthorized CA, and invalidates the certificate.

Test Steps Performed	The evaluator created a trust chain where the Intermediate CA does not have CRLSign bit and attempted to establish a TLS connection and observed that the TOE rejected the connection.
Test Result	Pass

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 Number	5
Test Objective	Verify that the TOE rejects malformed certificate.
Test Steps Performed	The evaluator configured a test script to create a corrupt certificate during handshake and observed that the TOE rejected the connection.
Test Result	Pass

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 Number	6
Test Objective	Verify that the TOE rejects certificate with corrupt signatures.
Test Steps Performed	The evaluator configured a test script to corrupt the certificate's signature during handshake and observed that the TOE rejected the connection.
Test Result	Pass

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 Number	7
Test Objective	Verify that the TOE rejects certificates with a modified public key.
Test Steps Performed	The evaluator created a modified public key in the certificate chain and established a connection. The evaluator observed that the connection was rejected by the TOE.
Test Result	Pass

Test 8: (Conditional on support for EC certificates as indicated in FCS_COP.1/Sig). 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 Number	8

Test Objective	N/A
Test Steps Performed	Not applicable, TOE does not claim EC certificates.
Test Result	Pass

Test 9: (Conditional on support for EC certificates as indicated in FCS_COP.1/Sig). 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 Number	9
Test Objective	N/A
Test Steps Performed	Not applicable, TOE does not claim EC certificates.
Test Result	Pass

FIA_X509_EXT.1.2

TSS

None.

Guidance

None.

Tests

The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. If the application supports chains of length four or greater, 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. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created.

***Test 1:** The evaluator shall ensure that the certificate of at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator shall confirm that validation of the certificate path fails (i) as part of the validation of the peer certificate belonging to this chain; and/or (ii) when attempting to add the CA certificate without the basicConstraints extension to the TOE's trust store.*

Test Number	1
Test Objective	a) Verify that TOE rejects a certificate issued by an Intermediate CA without basicConstraints field when connecting to server. b) Verify that TOE rejects a certificate issued by an Intermediate CA without basicConstraints field when importing this CA to the trust store.
Test Steps Performed	Objective a) is resolved by test FIA_X509_EXT.1.1 Test 1 Objective b) Objective b) TOE does not have functionality to add CA to the trust store after installation.
Test Result	Pass

Test 2: *The evaluator shall ensure that the certificate of at least one of the CAs in the chain has the CA flag in the basicConstraints extension not set (or set to FALSE). The evaluator shall confirm that validation of the certificate path fails (i) as part of the validation of the peer certificate belonging to this chain; and/or (ii) when attempting to add the CA certificate with the CA flag not set (or set to FALSE) in the basicConstraints extension to the TOE's trust store.*

Test Number	2
Test Objective	a) Verify that TOE rejects a leaf certificate issued by an Intermediate CA with basicConstraints field and CA=FALSE, when connecting to server. b) Verify that TOE rejects a leaf certificate issued by an Intermediate CA with basicConstraints field and CA=FALSE, when importing this CA to the trust store.
Test Steps Performed	Objective a) is resolved by test FIA_X509_EXT.1.1 Test 1 Objective c) Objective b) TOE does not have functionality to add CA to the trust store after installation.
Test Result	Pass

2.8 FIA_X509_EXT.2 X.509 Certificate Authentication (Selection-Based)

FIA_X509_EXT.2.1

TSS

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.

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. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.

[ST] Section 7.3.1 states that the TOE uses only one certificate chain configured by the administrator.

[ST] Section 7.3.1 states, “The TOE will reject a certificate without key usage or an incorrect key usage field.”

[ST] Section 7.3.1 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 stating: “If revocation status is impossible to verify, the certificate is considered invalid.”

[ST] does not describe any distinctions made between the trusted channels.

Guidance Documentation

None.

Tests

The evaluator shall perform the following test for each trusted channel:

Test 1: *The evaluator shall demonstrate that using a valid certificate that requires 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 Number	1
Test Objective	a) Verify that the TOE performs revocation checking using CRL. (satisfied by testing FIA_X509_EXT.1 Test 3) b) Verify that the TOE performs action defined in the [ST] when validity of certificate cannot be established. [ST] defined action as "not accept certificate" and this action is not configurable. Note: TOE requires valid CRL for certificate to be accepted, so testing in FIA_X509_EXT.1.1 was performed with valid CRL server. This test is also repeated here for consistency. TOE performs CRL caching, so test was performed in reversed order.
Test Steps Performed	a) The evaluator loaded the new CRLs on the CRL server and established a connection. The evaluator observed that the TOE's webhook accepted the connection successfully. b) The evaluator configured the CRL server to not load the new CRLs that were configured in the new certificate and tried to establish a TLS connection. The evaluator observed that the TOE's webhook rejected the connection.
Test Result	Pass

Test 2*: The evaluator shall demonstrate that an invalid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity cannot be accepted.*

Test Number	2
Test Objective	Verify that invalid certificate will not be accepted when revocation checking is overridden when TOE supports actions "*allow the administrator to choose whether to accept the certificate in these cases*, *accept the certificate*." TOE does not claim support for those actions.
Test Steps Performed	This objective is not applicable as the TOE did not select actions "*allow the administrator to choose whether to accept the certificate in these cases*, *accept the certificate*." TOE only performs "not accept certificate" action.
Test Result	Pass

2.9 FMT_MEC_EXT.1 Supported Configuration Mechanism

TSS

The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.

Conditional: If "implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption" is selected, the evaluator shall ensure that the TSS identifies those options, as well as indicates where the encrypted representation of these options is stored.

[ST] Section 7.4.2 describes the domain names of external non-TOE entities, domain names of the incoming connections that the TOE would accept, x509 certificates, and private keys.

[ST] Section 7.4.2 states that, “The TOE stores the following settings on the platform:

- List of domain names of external non-TOE entities the TOE will need to perform a network connection when functioning as listed in FDP_NET_EXT.1:
  - NTP server FQDN or IP
  - ADFS server FQDN or IP
  - ADFS web application id value
  - Kafka Server FQDN or IP
- Domain names the TOE will be using to accept incoming connections
- x509 certificates and private key for use with TLS connections as defined in FTP_DIT_EXT.1.”

[ST] Section 7.4.2 states that the configuration files are stored in /var/lib/bastille/ and /etc/opt/bastille/.

[ST] Section 7.4.2 states that the configuration of connections to external webhook subscribers is stored in Elasticsearch database.

[ST] Section 7.4.2 states that the settings are created at initial deployment and cannot be modified during normal operation.

Guidance Documentation

None.

Tests[5]

If "invoke the mechanisms recommended by the platform vendor for storing and setting configuration options" is chosen, the method of testing varies per platform as follows:

Platforms:Android...
The evaluator shall inspect the TSS and verify that it describes what Android API is used (and provides a link to the documentation of the API) when storing configuration data. The evaluator shall run the application and verify that the behaviour of the TOE is consistent with where and how the API documentation says the configuration data will be stored.

Platforms:Microsoft Windows...
The evaluator shall determine and verify that Windows Universal Applications use either the Windows.Storage namespace, Windows.UI.ApplicationSettings namespace, or the IsolatedStorageSettings namespace for storing application specific settings. For .NET applications, the evaluator shall determine and verify that the application uses one of the locations listed in https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/ or https://learn.microsoft.com/en-us/previous-versions/dotnet/netframework-4.0/zzdt0e7f(v=vs.100) or https://learn.microsoft.com/en-us/aspnet/core/fundamentals/configuration/ or https://learn.microsoft.com/en-us/aspnet/core/host-and-deploy/iis/web-config for storing application specific settings. For Classic Desktop applications, the evaluator shall run the application while monitoring it with the SysInternals tool ProcMon and make changes to its configuration. The evaluator shall verify that ProcMon logs show corresponding changes to the the Windows Registry or C:\ProgramData\ directory.

Platforms:Apple iOS...
The evaluator shall verify that the app uses the user defaults system or key-value store for storing all settings.

Platforms:Linux...
The evaluator shall run the application while monitoring it with the utility strace. The evaluator shall make security-related changes to its configuration. The evaluator shall verify that strace logs corresponding

[5] Modified by TD0747 & TD0893

changes to configuration files that reside in /etc (for system-specific configuration), in the user's home directory (for user-specific configuration), or /var/lib/ (for configurations controlled by UI and not intended to be directly modified by an administrator).

Platforms:Oracle Solaris...
The evaluator shall run the application while monitoring it with the utility dtrace. The evaluator shall make security-related changes to its configuration. The evaluator shall verify that dtrace logs corresponding changes to configuration files that reside in /etc (for system-specific configuration) or in the user's home directory(for user-specific configuration).

Platforms:Apple macOS...
The evaluator shall verify that the application stores and retrieves settings using the NSUserDefaults class.
If "implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption" is selected, for all configuration options listed in the TSS as being stored and protected using encryption, the evaluator shall examine the contents of the configuration option storage (identified in the TSS) to determine that the options have been encrypted.

Test Number	1
Test Objective	"Invoke the mechanisms recommended by the platform vendor for storing and setting configuration options" was selected; perform the platform-specific testing as prescribed above. Make security related changes to the TOE while monitoring the application with 'strace' utility.
Test Steps Performed	The evaluator created a webhook and successfully tested the webhook as part of making security related changes to the TOE while monitoring the TOE with 'strace' and observed that the changes were detected by 'strace.'
Test Result	Pass

2.10 FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

TSS

The evaluator shall check the TSS to determine if the application requires any type of credentials and if the application installs with default credentials.

[ST] Section 7.4.1 states that the TOE uses no credentials and the application cannot be used until the initial configuration is performed.

Guidance Documentation

None.

Tests

If the application uses any default credentials the evaluator shall run the following tests.
Test 1: The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality required to set new credentials is available.

Test Number	1
Test Objective	If the application uses default credentials, run tests 1 through 3 as described above.
Test Steps Performed	[ST] Section 7.4.1 states that "The TOE uses no credentials"; therefore, Tests 1 through 3 are not applicable.
Test Result	Pass

Test 2: *The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available.*

Test Number	2
Test Objective	If the application uses default credentials, run tests 1 through 3 as described above.
Test Steps Performed	[ST] Section 7.4.1 states that “The TOE uses no credentials”; therefore, Tests 1 through 3 are not applicable.
Test Result	Pass

Test 3: *The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application.*

Test Number	3
Test Objective	If the application uses default credentials, run tests 1 through 3 as described above.
Test Steps Performed	[ST] Section 7.4.1 states that “The TOE uses no credentials”; therefore, Tests 1 through 3 are not applicable.
Test Result	Pass

FMT_CFG_EXT.1.2

TSS

None.

Guidance Documentation

None.

Test

The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform.

Platforms:Android...
The evaluator shall run the command find -L . -perm /002 inside the application's data directories to ensure that all files are not world-writable. The command should not print any files.

Platforms:Microsoft Windows...
The evaluator shall run the SysInternals tools, Process Monitor and Access Check (or tools of equivalent capability, like icacls.exe) for Classic Desktop applications to verify that files written to disk during an application's installation have the correct file permissions, such that a standard user cannot modify the application or its data files. For Windows Universal Applications the evaluator shall consider the requirement met because of the AppContainer sandbox.

Platforms:Apple iOS...
The evaluator shall determine whether the application leverages the appropriate Data Protection Class for each data file stored locally.

Platforms:Linux...
The evaluator shall run the command find -L . -perm /002 inside the application's data directories to ensure that all files are not world-writable. The command should not print any files.

Platforms:Oracle Solaris...

The evaluator shall run the command find . \(-perm -002 \) inside the application's data directories to ensure that all files are not world-writable. The command should not print any files.

Platforms:Apple macOS...
The evaluator shall run the command find . -perm +002 inside the application's data directories to ensure that all files are not world-writable. The command should not print any files.

Test Number	1
Test Objective	Verify that the application files associated with the TOE are not world-writeable. NOTES: The TOE is distributed pre-installed on the Platform OS; therefore, there is no installation step. The TOE is comprised of multiple software components which, together, comprise a web-based application interface. These components are identified as follows: • Elastic Filebeat • Confluent Kafka • NGINX • Fusion Center Modules: • Comprised of python scripts
Test Steps Performed	The evaluator identified the TOE's "data directories" and used the command '***"find -L . -perm /002"*** to determine if the files were marked as "world-writeable". The evaluator then used the tools provided by the Platform to navigate the system's directories and identify all entities with "kafka" in it; then ran the FMT_CFG_EXT.1.2.bsh tool on the list to identify any files which are world-writable. The evaluator verified that no TOE files were identified as world-writable. The evaluator repeated this step for each of the following keywords associated with the TOE: • Elastic Filebeat • Confluent Kafka • NGINX The evaluator observed that the fusion center modules did not have any keywords.
Test Result	Pass

2.11 FMT_SMF.1 Specification of Management Functions

TSS

None.

Guidance Documentation

The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.

[PP] does not mandate any management function.

[ST] Section 6.1.4.3 states that the TOE is capable of performing "set up connections to external webhook subscribers."

[AGD] Section 8.0 states the steps required for configuring network parameters required to set up “webhooks;” it would require access to “network resources".”

Tests

The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.

Test Number	1
Test Objective	The management functions listed in the [ST] are exercisable and consistent with their descriptions provided in [ST] and [AGD]. NOTES: • [ST] Section 6.1.4.3 selected “set up connections to external Webhook subscribers and perform initial configuration” for FMT_SMF.1.1. o [AGD] Section 8.0 provides guidance on configuring Webhooks. o [AGD] Section 5.0 provides guidance on initial configuration of the TOE.
Test Steps Performed	Webhooks: The evaluator configured a “webhook” in the TOE GUI and tested the connection to a non-TOE IT entity and verified that the webhook configuration was successful. Initial Configuration of the TOE: The evaluator generated a new TOE .yaml configuration file and edited the configuration file to meet the needs of the operational environment then ran the installation command to install/configure the TOE. After the installation completed and the Platform rebooted, the evaluator verified that the TOE was successfully installed and running.
Test Result	Pass

2.12 FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

TSS

The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.

[ST] Section 7.5.1 states that the application does not request or collect PII from the users.

Guidance Documentation

None.

Tests

If “require user approval before executing” is selected, the evaluator shall run the application and exercise the functionality responsibly for transmitting PII and verify that user approval is required before transmission of the PII.

Test Number	1
Test Objective	N/A

Test Steps Performed	[ST] did not select “require user approval before executing” in FPR_ANO_EXT.1.1; therefore, this test is implicitly satisfied.
Test Result	Pass

2.13 FPT_API_EXT.1 use of Supported Services and APIs

TSS

The evaluator shall verify that the TSS lists the platform APIs used in the application.

[ST] Section 7.6.2 states that [ST] Appendix A describes the platform APIs used in the application.

Guidance Documentation

None.

Tests

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.

Test Number	1
Test Objective	Verify that the list of supported platform APIs listed in [ST] Appendix A and [ST] section 7.7.1 are supported by the platform.
Test Steps Performed	The evaluator copied the list of platform APIs that the TOE utilizes and verified that platform developer from the [ST] and verified that the associated documentation was accessible.
Test Result	Pass

2.14 FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

TSS[6]

The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled. If any explicitly-mapped exceptions are claimed, the evaluator shall check that the TSS identifies these exceptions, describes the static memory mapping that is used, and provides justification for why static memory mapping is appropriate in this case.

(Conditional: The PE or ELF automated tests fail) The evaluator shall ensure that the TSS describes the stack-based buffer overflow compiler flags.

[ST] Section 7.6.1 describes the compiler flags used to enable ASLR when the application is compiled.

[ST] does not claim any explicitly-mapped exceptions.

[ST] Section 7.6.1 states, “-fPIC” and “buildmode=pie” ensure binaries are compiled with ASLR support” and “The underlying platform (Ubuntu 18.04 or 22.04.5) is able to perform ASLR when running TOE binaries. Python scripts are not susceptible to buffer overflow attacks.”

[ST] Section 7.6.1, Table 5 provides the TOE module compilation flags and describes that the compilation flags ensure exploit-prevention capabilities.

[6] Modified by TD0798

Guidance

None.

Tests[7]

The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address except for any exceptions claimed in the SFR. For these exceptions, the evaluator shall verify that this analysis shows explicit mappings that are consistent with what is claimed in the TSS. The method of doing so varies per platform. For those platforms requiring the same application running on two different systems, the evaluator may alternatively use the same device. After collecting the first instance of mappings, the evaluator must uninstall the application, reboot the device, and reinstall the application to collect the second instance of mappings.

Platforms:Android...
The evaluator shall run the same application on two different Android systems. Both devices do not need to be evaluated, as the second device is acting only as a tool. Connect via ADB and inspect /proc/PID/maps. Ensure the two different instances share no memory mappings made by the application at the same location.

Platforms:Microsoft Windows...
The evaluator shall run the same application on two different Windows systems and run a tool that will list all memory mapped addresses for the application. The evaluator shall then verify the two different instances share no mapping locations. The Microsoft SysInternals tool, VMMap, could be used to view memory addresses of a running application. The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application has ASLR enabled.

Platforms:Apple iOS...
The evaluator shall perform a static analysis to search for any mmap calls (or API calls that call mmap), and ensure that no arguments are provided that request a mapping at a fixed address.

Platforms:Linux...
The evaluator shall run the same application on two different Linux systems. The evaluator shall then compare their memory maps using pmap -x PID to ensure the two different instances share no mapping locations.

Platforms:Oracle Solaris...
The evaluator shall run the same application on two different Solaris systems. The evaluator shall then compare their memory maps using pmap -x PID to ensure the two different instances share no mapping locations.

Platforms:Apple macOS...
The evaluator shall run the same application on two different Mac systems. The evaluator shall then compare their memory maps using vmmap PID to ensure the two different instances share no mapping locations.

Test Number	1
Test Objective	Verify that the TOE-processes do not map memory to explicit addresses.
Test Steps Performed	The evaluator started with a new installation of the TOE; ensured that all TOE processes were running and identified the PIDs for each TOE process; ran ‘pmap -x’ on each TOE process and wrote the results to individual files; The evaluator rebooted the TOE software again and then ran the same steps on the new PIDs. The evaluator parsed the files and

[7] Modified by TD0798

	compared each respective TOE process from the initial TOE installation to its instantiation after the reinstallation. The evaluator verified that no TOE processes mapped memory.
Test Result	Pass

FPT_AEX_EXT.1.2

TSS

None.

Guidance

None.

Tests

The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform.

Platforms:Android...
The evaluator shall perform static analysis on the application to verify that mmap is never invoked with both the PROT_WRITE and PROT_EXEC permissions, and mprotect is never invoked.

Platforms:Microsoft Windows...
The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application passes the NXCheck. The evaluator may also ensure that the /NXCOMPAT flag was used during compilation to verify that DEP protections are enabled for the application.

Platforms:Apple iOS...
The evaluator shall perform static analysis on the application to verify that mprotect is never invoked with the PROT_EXEC permission.

Platforms:Linux...
The evaluator shall perform static analysis on the application to verify that both mmap is never be invoked with both the PROT_WRITE and PROT_EXEC permissions, and mprotect is never invoked with the PROT_EXEC permission.

Platforms:Oracle Solaris...
The evaluator shall perform static analysis on the application to verify that both mmap is never be invoked with both the PROT_WRITE and PROT_EXEC permissions, and mprotect is never invoked with the PROT_EXEC permission.

Platforms:Apple macOS...
The evaluator shall perform static analysis on the application to verify that mprotect is never invoked with the PROT_EXEC permission.

Test Number	1
Test Objective	Verify that the following is true for each of the TOE executables: • mmap is never invoked with both the PROT_WRITE and PROT_EXEC permissions; • mprotect is never invoked with the PROT_EXEC permission
Test Steps Performed	The evaluator ensured all TOE-processes were running; identified the PID of each TOE process; then stopped all TOE-processes from running; ran

	'strace' targeting the initiating/executing commands for each TOE-process identified in the step above; parsed the resulting files and verified that mmap was never invoked with both the PROT_WRITE and PROT_EXEC permissions and that mprotect was never invoked with the PROT_EXEC permission.
Test Result	Pass

FPT_AEX_EXT.1.3

TSS

None.

Guidance

None.

Tests[8]

The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests:

Platforms:Android...
Applications running on Android cannot disable Android security features, therefore this requirement is met and no evaluation activity is required.

Platforms:Microsoft Windows...
If the OS platform supports Windows Defender Exploit Guard (Windows 10 version 1709 or later), then the evaluator shall ensure that the application can run successfully with Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The following link describes how to enable Exploit Protection, https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide.
If the OS platform supports the Enhanced Mitigation Experience Toolkit (EMET) which can be installed on Windows 10 version 1703 and earlier, then the evaluator shall ensure that the application can run successfully with EMET configured with the following minimum mitigations enabled; Memory Protection Check, Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), and Data Execution Prevention (DEP).

Platforms:Apple iOS...
Applications running on iOS cannot disable security features, therefore this requirement is met and no evaluation activity is required.

Platforms:Linux...
The evaluator shall ensure that the application can successfully run on a system with either SELinux or AppArmor enabled and in enforce mode.

Platforms:Oracle Solaris...
The evaluator shall ensure that the application can run with Solaris Trusted Extensions enabled and enforcing.

Platforms:Apple macOS...

[8] Modified by TD0823

The evaluator shall ensure that the application can successfully run on macOS without disabling any security features.

Test Number	1
Test Objective	Verify that the application can successfully run on a system with AppArmor enabled and in enforcing mode.
Test Steps Performed	The evaluator placed the AppArmor profiles (generated by the vendor) in the appropriate directory on the TOE platform; set the appropriate TOE executables to AppArmour enforce mode; ran a command and verified that the AppArmor profiles were listed under “profiles are in enforce mode;” rebooted the TOE platform; resumed the TOE execution; verified that all TOE processes were running; verified that the PIDs listed from “sudo supervisorctl status” were covered in the AppArmor controlled PIDs as evident from the output of the “sudo aa-status” command. The evaluator then ran through functions of the TOE web GUI and ensured normal functionality.
Test Result	Pass

FPT_AEX_EXT.1.4

TSS

None.

Guidance

None.

Tests

The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform:

Platforms:Android...
The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored under /data/data/package/ where package is the Java package of the application.

Platforms:Microsoft Windows...
For Windows Universal Applications the evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox). For Windows Desktop Applications the evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.

Platforms:Apple iOS...
The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).

Platforms:Linux...
The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.

Platforms:Oracle Solaris...

The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.

Platforms:Apple macOS...
The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.

Test Number	1
Test Objective	Verify that there are no executable files stored in the same directories to which the application wrote user-modifiable files.
Test Steps Performed	The evaluator ran a command on the TOE platform OS to watch the entire Platform filesystem for new file creation operations. The evaluator, for 15 minutes following the execution of the previous command, ran through every configuration option within the TOE Web GUI. This included adding new items, deleting items, and using all available exporting functions. For the directories which were identified by the tool as having contained newly created files during the test period of 15 minutes, the evaluator verified that no executables were identified within those directories.
Test Result	Pass

FPT_AEX_EXT.1.5

TSS[9]

(Conditional: The PE or ELF automated tests fail) The evaluator shall ensure that the TSS describes the stack-based buffer overflow compiler flags.

Not applicable to the TOE.

Guidance

None.

Tests[10]

The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present.

Platforms:Microsoft Windows...
Applications that run as Managed Code in the .NET Framework do not require these stack protections. Applications developed in Object Pascal using the Delphi IDE compiled with RangeChecking enabled comply with this element. For other code, the evaluator shall review the TSS and verify that the /GS flag was used during compilation. The evaluator shall run a tool like, Binskim, that can verify the correct usage of /GS.
For PE , the evaluator will disassemble each and ensure the following sequence appears:

```
mov rcx, QWORD PTR [rsp+(...)]
xor rcx, (...)
call (...)
.
```

[9] Modified by TD0815
[10] Modified by TD0815

For ELF executables, the evaluator will ensure that each contains references to the symbol __stack_chk_fail.

Tools such as Canary Detector may help automate these activities.
If these automated tests fail, the evaluator shall perform the above, conditional TSS activity.

Test Number	1
Test Objective	Ensure that stack-based buffer overflow protection is present for every ELF file of the TOE.
Test Steps Performed	The evaluator identified all ELF files associated with the TOE; ran the elf.bsh BASH script on each ELF file identified. The script produces two file outputs which identify which ELF files pass the test and those that fail the test. The evaluator verified that all identified ELF files passed the test. The evaluator performed the same steps for the remaining directories (/usr/share/filebeat/) and verified that all identified ELF files contain the **__stack_chk_fail** symbol.
Test Result	Pass

2.15 FPT_IDV_EXT.1 Software Identification and Versions

TSS

If "other version information" is selected the evaluator shall verify that the TSS contains an explanation of the versioning methodology.

[ST] Section 7.6.3 states
'The TOE uses Semantic Versioning ("SemVer") versioning methodology to track TOE versions Major.Minor.Patch (e.g. 2.1.0).'

Guidance

None.

Tests

The evaluator shall install the application, then check for the existence of version information. If SWID tags are selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that it contains at least a SoftwareIdentity element and an Entity element.

Test Number	1
Test Objective	Verify that the current running TOE software version is provided in SemVer format.
Test Steps Performed	The testing performed in FPT_TUD_EXT.1.2 provided the evidence for this test. The evaluator verified, using that evidence, that the software versioning was provided in SemVer format.
Test Result	Pass

2.16 FPT_LIB_EXT.1 Use of Third Party Libraries

TSS

None.

Guidance

None.

Tests

The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.

Test Number	1
Test Objective	Verify that the TOE and its packaged components, are limited to those in the assignment in the [ST]. [ST] Appendix B describes 3rd-party libraries that the TOE is packaged with. TOE: The following 3rd party tools and libraries are included in the TOE: NGINX, Elastic FileBeat, and Confluent Kafka Python Client. Javascript libraries: @appbaseio/reactivesearch, @appbaseio/reactivesearch aws4 axios change-case chart.js classnames date-fns dateformat @date-io/date-fns @date-io/moment dom-to-image-more downloadjs elastic-builder @elastic/datemath elasticsearch emotion history js-file-download jsonexport leaflet leaflet-draw lodash lodash.clonedeep, lodash.drop, lodash.get, lodash.groupby, lodash.isequal, lodash.uniq, @material-ui/core, @material-ui/icons @material-ui/lab @material-ui/pickers, @material-ui/pickers, mobx-react, moment, multidict, ngeohash, numeral, object-hash papaparse pluralize printable-characters qs ra-core rc-slider react react-admin react-chartjs-2, react-color, react-dom, react-emotion, react-final-form, react-icons, react-json-view react-leaflet, react-leaflet-control, react-leaflet-draw, react-leaflet-heatmap-layer, @react-pdf/layout @react-pdf/renderer, react-redux, react-resize-detector, react-router, react-router-dom, react, router-dom, react-select, react-select, react-sizeme, react-spinkit, react-spinners-kit, react-to-print, react-use, react-use, react-vis, react-vis, js-timeline, shorted, uppy, @uppy/react, url-search-params, vis. Python 3.11.3 with the following python libraries: Aiofiles, aiohttp, aiokafka, backoff, cachetools, cffi, greenlit, scipy, sql alchemy, shortuuid, skops, starlette, streamz, torch, tornado, ujson, uvicorn, uvloop, redis, requestsscikit-learn, shapely, psutil, pydantic, pydash, PyJWT, pyOpenSSL, pypager, PyYAML, optuna, polars-lts-cpu, ntplib, cmd2, configclasses, configclasses confluent-kafka, cryptography, dictdiffer, querystring-parser, MarkupSafe, lightning, validators, fastapi, fastavro, frozenlist, httptools jinja2, numpy, websockets, yarl .
Test Steps Performed	The evaluator identified software packages that were included in Ubuntu but that are not installed on the TOE Platform OS; identified software packages that were not included in Ubuntu but that are installed on the TOE Platform OS and verified that the TOE platform OS had no additional packages installed other than what is listed for the entirety of the Ubuntu 18.04.6 and Ubuntu 22.04.5 Linux distribution. <u>Third-party Libraries:</u> The evaluator verified the installed versions of the 3rd party libraries utilized by the TOE; verified that NGINX, Elastic FileBeat and Confluent Kafka were installed on the Platform.

Test Result	Pass

2.17 FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1

TSS

None.

Guidance

The evaluator shall check to ensure the guidance includes a description of how updates are performed. The evaluator shall verify guidance includes a description of how to query the current version of the application.

[AGD] Section 10.0 contains the guidance on updating the TOE. The steps include:

- Check for updates on the Fusion Center.
- If updates exist, contact support@bastille.net for access to the Bastille Networks secure portal to obtain updated versions of the Fusion Center.
- After receiving the instructions, follow the instructions mentioned in [AGD] Section 5.0 to create a Fusion Center VM for the update.

Tests

The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met.

Test Number	1
Test Objective	Verify that the TOE can check for the presence of a software update.
Test Steps Performed	Using the TOE Web GUI the evaluator verified the installed version of the TOE software and then used the TOE's function to check for the availability of an update to the TOE software. The evaluator observed that it successfully displayed the installed version of the TOE.
Test Result	Pass

FPT_TUD_EXT.1.2

TSS

None.

Guidance

The evaluator shall verify guidance includes a description of how to query the current version of the application.

[AGD] Section 10.1 contains the guidance on how to query for the most recent version of the TOE. The steps to query the version include:

- Log in to the Bastille Enterprise Admin Console.
- On the Dashboard, just below "Fusion Center Status" the Fusion Center Version is present.

Tests

The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version.

Test Number	1
Test Objective	Verify that the TOE reports used by the current executing version of TOE software matche that of the documented and installed version.
Test Steps Performed	Using the TOE Web GUI, the evaluator verified the installed version of the TOE software and that the installed version was consistent with that which was listed in [ST].
Test Result	Pass

FPT_TUD_EXT.1.3

TSS

None.

Guidance

None.

Tests

The evaluator shall verify that the application's executable files are not changed by the application. *Platforms:Apple iOS...* *The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).* *For all other platforms, the evaluator shall perform the following test:* *Test 1: The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as described in the ST. The evaluator shall then compare each executable file with either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.*

Test Number	1
Test Objective	Verify that the application's executable files are not changed by the application using sha1sum calculations.
Test Steps Performed	The evaluator located all executable files of the TOE; created a SHA1SUM of each executable file and wrote that to a file; ran through every available user action through the TOE Web GUI; created a new SHA1SUM off each executable file identified in the previous steps; created a SHA1SUM of each file that contained the SHA1SUMs of executables and compared the checksums, verifying that they were identical.
Test Result	Pass

FPT_TUD_EXT.1.4

TSS

The evaluator shall verify that the TSS identifies how updates to the application are signed by an authorized source. The definition of an authorized source must be contained in the TSS. The evaluator shall also ensure that the TSS (or the operational guidance) describes how candidate updates are obtained.

[ST] Section 7.6.4 states, “The TOE is distributed to customers from a secure developer portal or via a tracked courier delivery service. The Developer publishes the public key on a developer support website https://www.bastille.net/support. The delivery package also contains a detached digital signature in the .sig file. Customers are required to verify integrity of the package using this detached signature and developers public key obtained from the developer support website prior to installation of the package”

Guidance

None.

Tests

None.

FPT_TUD_EXT.1.5

TSS

The evaluator shall verify that the TSS identifies how the application is distributed. If "with the platform" is selected the evaluator shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "as an additional package" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2.

FPT_TUD_EXT.1.5 selected "with the platform".
[ST] Section 7.6.4 states that the application is distributed as a delivery package containing a virtual appliance image (.OVA), which contains the Ubuntu Linux 18.04 operating system with the TOE pre-installed.
[ST] Section 7.6.4 states, ‘In order to update the TOE, customers decommission the virtual appliance with the previous version of the TOE, then import and initialize the new version of the appliance.’

Guidance

None.

Tests

None.

2.18 FPT_DIT_EXT.1 Protection of Data in Transit

TSS

For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.

[ST] Section 7.7.1 describes the communication channel and the method of protection provided.

[ST] Section 7.7.1 describes a table of NGINX API calls and a table of confluent Kafka API calls that provide channel encryption.

Guidance

None.

Tests

The evaluator shall perform the following tests:

***Test 1**: The evaluator shall exercise the application (attempting to transmit data; for example, by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall verify from the packet capture that the traffic is encrypted with HTTPS, TLS, DTLS, SSH, or IPsec in accordance with the selection in the ST.*

Test Number	1
Test Objective	Verify that all traffic between the TOE and remote non-TOE IT entities are protected utilizing TLS.
Test Steps Performed	The evaluator verified that the network traffic initiated by the TOE, initiated by the user of the TOE, and traffic the TOE responds to for specific incoming traffic (from Bastille Concentrators), were all protected via TLS channels using packet captures.
Test Result	Pass

***Test 2:** The evaluator shall exercise the application (attempting to transmit data; for example, by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall review the packet capture and verify that no sensitive data is transmitted in the clear.*

Test Number	2
Test Objective	N/A
Test Steps Performed	Test 2 is satisfied by the testing performed for Test 1 in 'FDP_NET_EXT.1.1 Network Communications'. In that test, the evaluator verified that the network traffic initiated by the TOE, initiated by the user of the TOE, and traffic the TOE responds to for specific incoming traffic (from Bastille Concentrators), were all protected via TLS channels using packet captures. All other traffic that was identified in the network packet captures were initiated by and/or destined for, the TOE platform host. This traffic included DNS queries/responses, NTP queries/responses, ARP queries/responses.
Test Result	Pass

***Test 3:** The evaluator shall inspect the TSS to determine if user credentials are transmitted. If credentials are transmitted the evaluator shall set the credential to a known value. The evaluator shall capture packets from the application while causing credentials to be transmitted as described in the TSS. The evaluator shall perform a string search of the captured network packets and verify that the plaintext credential previously set by the evaluator is not found.*

Platforms:Android...
If "not transmit any data" is selected, the evaluator shall ensure that the application's AndroidManifest.xml file does not contain a uses-permission or uses-permission-sdk-23 tag containing android:name="android.permission.INTERNET". In this case, it is not necessary to perform the above Tests 1, 2, or 3, as the platform will not allow the application to perform any network communication.

Platforms:Apple iOS...
If "encrypt all transmitted data" is selected, the evaluator shall ensure that the application's Info.plist file does not contain the NSAllowsArbitraryLoads or NSExceptionAllowsInsecureHTTPLoads keys, as these keys disable iOS's Application Transport Security feature.

Test Number	3
Test Objective	N/A

Test Steps Performed	Not applicable, since the TOE does not transmit user credentials.
Test Result	Pass

3 SAR Assurance Activities and Results

3.1 ASE: Security Target Evaluation

3.1.1 General ASE:

When evaluating a Security Target, the evaluator performs the work units as presented in the CEM. In addition, the evaluator ensures the content of the TSS in the ST satisfies the EAs specified in Section 2 (Evaluation Activities for SFRs).

Result:

For TSS EAs for SFRs, see Section 2 above.

3.2 ADV: Development

3.2.1 Basic Functional Specification (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 (PP) Section 5.1 Security Functional Requirements, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information are 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.

Result:

The requirements on the content of the functional specification information are implicitly assessed by virtue of the other evaluation activities being performed.

ADV_FSP.1.1E

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

Result:

The evaluator confirmed that the information provided in [AGD] and [ST] 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.

Result:

The requirements on the content of the functional specification information are implicitly assessed by virtue of the other evaluation activities being performed. The evaluator was able to perform all evaluation and assurance activities.

3.3 AGD: Guidance Documents

3.3.1 Operational User Guidance (AGD_OPE.1)

The guidance documents will be provided with the ST. Guidance must include a description of how the IT personnel verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by the IT personnel. Guidance must be

provided for every operational environment that the product supports as claimed in the ST. This guidance includes instructions to successfully install the TSF in that environment; and Instructions to manage the security of the TSF as a product and as a component of the larger operational environment. Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the evaluation activities specified with each requirement.

PP Evaluation Activities:
Some of the contents of the operational guidance will be verified by the evaluation activities in Section 5.1 Security Functional Requirements 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 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.

Result:

[ST] Section 6.1.1 states that cryptographic functions are not provided by the TOE.

[AGD] Section 10 describes how to perform updates.

[AGD] Section 10.3 describes how to verify the update using a digital signature, performed via the underlying platform.

[AGD] Section 10 describes how to obtain the update candidate.

[AGD] Section 10.3 describes how to obtain the signing public key and the command to verify the fusion center update.

3.3.2 Preparative Procedures (AGD_PRE.1)

PP Evaluation Activities:
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.

Result:

[ST] Section 1.3.4 identifies the platform that the TOE is evaluated with. The following are the details:

- Platform OS: Ubuntu Linux LTS 18.04, Ubuntu 22.04
- Hypervisor: VMware ESXi 7 or higher (Virtual Hardware Version 17 or higher).

3.4 ALC: Life-cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor'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 is a reflection on the information to be made available for evaluation at this assurance level.

3.4.1 Labelling of the TOE (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 web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Result:

[ST] Section 1.2 provides the 'TOE version: 3.6' that is unique to the application.

[AGD] Section 1.0 contains notice that it is applicable to version 3.6.

Sample received for testing displayed software version 3.6.3.

The evaluator reviewed https://bastille.net/ for listings of advertisements of the TOE. The Evaluator found that the web site only contained general references to the Fusion Center product. No versioning information could be found on the site and thus no inconsistencies or ambiguities were identified between the TOE version identifiers listed in the evaluation and what is reported on the vendor's web site.

3.4.2 TOE CM Coverage (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 developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. 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.

Result:

The TOE is specifically identified in both [ST] and [AGD]. The identification is consistent between these documents.

[ST] Section 1.3.4 states that the TOE executes on Linux Ubuntu 18.04 or Linux Ubuntu 22.04.5 as the platform OS and requires VMware ESXi 7.0 or later.

TOE does not provide development environment to users and administrators. TOE comes with a pre-configured execution environment with security features enabled, and compiles binaries with security-enforcing compiler flags where applicable, as verified by the ATE activities.

[AGD] Section 1.0 uniquely identifies the TOE as Bastille Enterprise Fusion Center 3.6 which is the same as the TOE name provided in [ST] Section 1.2.

3.5 ALC_TSU_EXT.1 Timely Security Updates

This component requires the TOE developer, in conjunction with any other necessary parties, to provide information as to how the end-user devices are updated to address security issues in a timely manner. The documentation describes the process of providing updates to the public from the time a security flaw is reported/discovered, to the time an update is released. This description includes the parties involved (e.g., the developer, carriers(s)) and the steps that are performed (e.g., developer testing, carrier testing), including worst case time periods, before an update is made available to the public.

The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described.
The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days.
The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.

Result:

[ST] Section 7.6.5 states, "The TOE developer has implemented internal processes for receiving reports of security flaws, tracking product vulnerabilities, and distributing software updates to customers in a timely manner."

There are no third-party processes used for this application.

[ST] Section 7.6.5 describes that any implementation flaws will be addressed within 90 days of reporting.

[ST] Section 7.6.5 states, "Customers can submit support issues, including discovered security vulnerabilities via email to support@bastille.io. Sensitive information should be encrypted using the PGP key published on the developer support website."

3.6 ATE: Tests

3.6.1 Independent Testing (ATE_IND.1)

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operational) documentation provided. The focus of the testing is to confirm that the requirements specified in Section 5.1 Security Functional Requirements being met, although some additional testing is specified for SARs in Section 5.2 Security Assurance Requirements. The evaluation activities identify the additional testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP. Given the scope of the TOE and its associated evaluation evidence requirements, this component's evaluation activities are covered by the evaluation activities listed for ALC_CMC.1.

Evaluation Activity:

The evaluator shall prepare a test plan and report documenting the testing aspects of the system, including any application crashes during testing. The evaluator shall determine the root cause of any application crashes and include that information in the report. 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 effect; 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 AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as 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 (e.g 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.

Result:

The evaluator witnessed no application crashes during the operation of testing. If a TOE service was not operational, it was due to the evaluator turning on/off services as needed to perform specific tests.

Testing was performed on the only platform described in the [ST].

The evaluator followed [AGD] to configure and operate the TOE.

No additional drivers were necessary to complete testing. Any additional test tools necessary to perform testing were documented in the test case where the tool was utilized.

The cryptographic engine was provided by the TOE platform OS. No configuration was necessary.

This test report details the steps that were taken to carry out the test plan.

3.7 AVA: Vulnerability Assessment

3.7.1 Vulnerability Survey (AVA_VAN.1)

For the current generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, the evaluator will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future protection profiles.

Evaluation Activities:

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 find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses.

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.

For Windows, Linux, macOS and Solaris: The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious.

Result:

The evaluator performed a search on the vulnerability databases on December 29, 2025, including NVD (note that MITRE is identical to NVD), CISA KEV.

Evaluator used the following search terms:

zkclient
jopt-simple
slf4j-api
reload4j
slf4j-reload4j
metrics-core
lz4-java
scala-library
scala-logging
scala-reflect
url-search-params
uvicorn
uvloop
validators
vis
watchfiles
wcwidth
websockets
yarl
zict
NGINX
Elastic
jackson-annotations
tqdm
types-cryptography
typing-extensions
ujson
streamz
sympy
tabulate
threadpoolctl
toml
toolz
sniffio
SQLAlchemy
shapely
shortid
shortuuid
six
skops
sniffio
SQLAlchemy
scikit-learn
scipy
querystring-parser
ra-core
rc-slider
react
react-admin
react-chartjs-2
react-color
react-dom
react-emotion
react-final-form
react-icons
react-json-view
react-leaflet
react-leaflet-control
react-leaflet-draw
react-leaflet-heatmap-layer
@react-pdf-layout
@react-pdf-renderer
react-redux
react-resize-detector
react-router
react-router-dom
react-select
react-sizeme
react-spinkit
react-spinners-kit
react-to-print
react-use
react-vis
react-visjs-timeline
redis
joblib
js-file-download
jsonexport

leaflet
leaflet-draw
lightning
lightning-utilities
lodash
lodash.clonedeep
lodash.drop
lodash.get
lodash.groupby
lodash.isequal
lodash.uniq
Mako
MarkupSafe
@material-ui/core
@material-ui/icons
@material-ui/lab
@material-ui/pickers
mobx
mobx-react
moment
mpmath
multidict
networkx
ngeohash
ntplib
numeral
numpy
object-hash
optuna
packaging
papaparse
pluralize
polars-lts-cpu
printable-characters
prompt-toolkit
psutil
pycparser
pydantic
pydash
Pygments
PyJWT
pyOpenSSL
pypager
pyperclip
pyreadline3
python-dotenv
pytorch-lightning
PyYAML
dataclasses
date-fns
dateformat
@date-io/date-fns
@date-io/moment
dictdiffer
dom-to-image-more
downloadjs
elastic-builder
@elastic/datemath
elasticsearch
emotion
fastapi
fastavro
filelock
frozenlist
fsspec
greenlet
history
httptools
huggingface-hub
idna
backoff
cachetools
certifi
cffi
change-case
charset-normalizer
chart.js
classnames
click
cmd2
colorama
colorlog
configclasses
confluent-kafka
aiokafka
aiosignal
alembic
anyio
reactivesearch
@appbaseio
async-timeout
attrs
aws4
bastille
fusion center
h11
cpe:2.3:a:tornadoweb:tornado:6.3.2:*:*:*:*:*:*:*
cpe:2.3:a:python:requests:2.32.3:*:*:*:*:*:*:*
starlette
setuptools
cpe:2.3:a:python:urllib3:1.26.20:*:*:*:*:*:*:*
cpe:2.3:a:aiohttp:aiohttp:3.9.5:*:*:*:*:*:*:*
cpe:2.3:a:axios:axios:1.7.2:*:*:*:*:node.js:*:*
cpe:2.3:a:cryptography.io:cryptography:40.0.2:*:*:*:*:python:*:*
cpe:2.3:a:palletsprojects:jinja:3.1.2:*:*:*:*:*:*:*
cpe:2.3:a:qs_project:qs:6.9.4:*:*:*:*:node.js:*:*
cpe:2.3:a:tornadoweb:tornado:6.3.2:*:*:*:*:*:*:*
cpe:2.3:a:transloadit:uppy:1.11.0:*:*:*:*:node.js:*:*
jackson-core

cpe:2.3:a:fasterxml:jackson-databind:2.9.7:*:*:*:*:*:*:*	cpe:2.3:a:apache:zookeeper:3.4.10:-:*:*:*:*:*:*
cpe:2.3:a:apache:kafka:1.1.1:-:*:*:*:*:*:*	xz
cpe:2.3:a:xerial:snappy-java:1.1.7.1:*:*:*:*:*:*:*	aiofiles
	torchmetrics

The search identified no residual vulnerabilities.

Evaluator performed an antivirus search on the TOE distributable - no malware was identified.

4 References

Abbr.	Name	Version	Date
[PP]	Protection Profile for Application Software	1.4	October 7, 2021
[ST]	Bastille Enterprise Fusion Center Version 3.6 Security Target	1.8	January 09, 2026
[AGD]	Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria	3.6	2025