National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Bastille Networks, Inc

Bastille Enterprise Fusion Center Version 3.6

Report Number: CCEVS-VR-VID11600-2026
Dated: January 15, 2026
Version: 1.0

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

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

Acknowledgements

Validation Team

Clare Parran
Sheldon Durrant
Randy Heimann
The MITRE Corporation

Meredith Martinez
Swapna Katikaneni
The Aerospace Corporation

Russ Fink
Alex Lee
Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Oleg Andrianov
Meghana Achanta
Michael Baron
UL Verification Services Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Enterprise Fusion Center 3.6 by Bastille Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by UL Verification Services Inc., a Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, CA, United States of America, and was completed January 15, 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by UL Verification Services Inc. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the Protection Profile for Application Software, Version 1.4, dated 2021-10-07 [PP].

The Target of Evaluation (TOE) is the Bastille Enterprise Fusion Center Version 3.6.

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

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced.

The technical information included in this report was obtained from the Bastille Enterprise Fusion Center Version 3.6 Security Target, Version 1.8, January 09, 2026 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

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

Evaluation Scheme	United States NIAP Common Criteria Evaluation Validation Scheme

Evaluated Target of Evaluation	Bastille Enterprise Fusion Center Version 3.6
Protection Profile (PP)	Protection Profile for Application Software, Version 1.4, dated 2021-10-07
Security Target (ST)	*Bastille Enterprise Fusion Center Version 3.6 Security Target,* version 1.8, January 09, 2026
Dates of Evaluation	June 2025 – January 2026
Conformance Result	Pass
Common Criteria Version	CC Version 3.1r5, April 2017
Common Evaluation Methodology (CEM) Version	CEM Version 3.1r5, April 2017
Evaluation Technical Report (ETR)	*Common Criteria Evaluation Technical Report*, UL15574582-ETR Rev1.2
Sponsor/Developer	Bastille Enterprise Fusion Center
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc. San Luis Obispo, CA
CCEVS Validators	Meredith Martinez, Swapna Katikaneni, Russ Fink, Alex Lee, Clare Parran, Sheldon Durrant, Randy Heimann

Table 1: Product Identification

3 Assumptions and Clarification of Scope

3.1 Assumptions

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

- *Protection Profile for Application Software*, Version 1.4, dated 2021-10-07

That information has not been reproduced here and the Protection Profiles should be consulted if there is interest in that material.

3.2 Clarification of Scope

The evaluation of security functionality and scope are inherently tied to the specific assurance activities performed and the defined scope of the evaluation methodology. This evaluation provides no assurance that the TOE counters any threats which are not identified in the above Protection Profiles. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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

- This evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Protection Profile for Application Software Version 1.4and performed by the evaluation team).
- This evaluation covers only the specific TOE version as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific TOE version was not included in the scope of the evaluation and should not be relied upon when configuring or operating the product as evaluated.

- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Protection Profiles and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

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

4.1 TOE description

The TOE is Bastille Enterprise Fusion Center 3.6 running on the VMware ESXi Virtualization Server (vCenter®, vSphere®) (herein referred to as the TOE).

4.2 Evaluated Configuration

Details regarding the evaluated configuration and any excluded functionality are provided in Section 8.

4.3 TOE Physical Boundaries

The TOE consists of the following modules and scripts: core Fusion Center Modules, NGINX web server, Elastic Filebeat, Confluent Kafka Python client, libraries as described in the ST, Appendix B. The TOE runs on an Ubuntu Linux LTS 18.04 or 22.04 virtual machine running on a VMware ESXI virtualization server.

The TOE is delivered to the customer in the form of a virtual appliance with all TOE parts already pre-installed to the /opt/bastille folder in a virtual appliance virtual drive. The appliance is provided through the developer support website, https://bastille.net/support/, and contacting Bastille support, to receive the VM in the OVA file format. Appliance integrity is verified using a digital signature of the file.

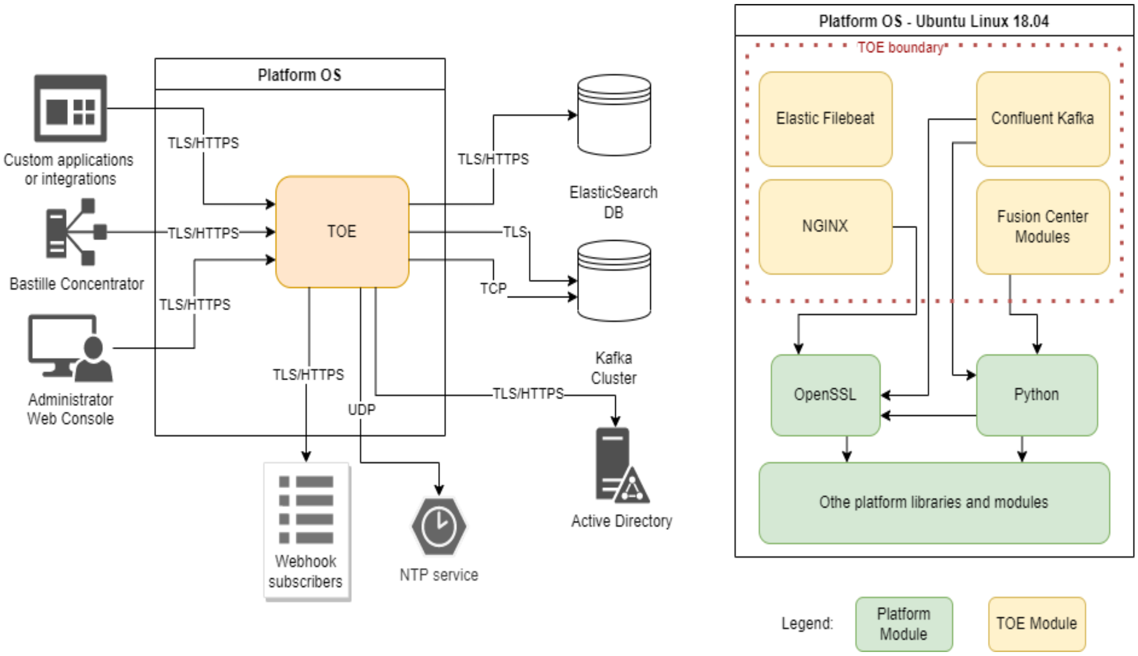

Figure 1 TOE and TOE Environment

5 Security Policy

This section contains the product security features and services and contains the policies or rules that the TOE must comply with and/or enforce.

5.1 Cryptographic Support

The TOE does not directly perform cryptographic services, but rather calls the platform-provided crypto library, so cryptographic operations are out of the TOE logical scope.

5.2 User Data Protection

The TOE protects confidential data using platform provided mechanisms and does not collect sensitive information from the platform or users. The TOE restricts its access to platform resources to network connections.

5.3 Identification and Authentication

The TOE uses x509 certificates to verify the authenticity of the remote services when initiating secure communications with them.

5.4 Security Management

The TOE provides security management functionality for users to perform initial configuration and to configure external connections. Configuration is stored in a way recommended by the platform. The TOE requires users to change the built-in OS credentials during initial configuration of the TOE. TOE configures file permissions for its binaries to protect from modification by unprivileged users.

5.5 Privacy

The TOE does not collect or transmit Personal Identifiable Information.

5.6 Protections of the TSF

The TOE employs built-in anti-exploitation capabilities and uses only supported platform APIs and a limited number of 3rd party libraries. The TOE uses SemVer format to track TOE versions.

The TOE provides its current version number and capabilities to check for existing updates to the TOE. The TOE is distributed with the OS as a Virtual Appliance, and updates are distributed as a complete virtual appliance image.

5.7 Trusted Path/Channels

The TOE performs encryption of transmitted sensitive data using platform provided functionality.

6 Documentation

The following documents are provided with the product by the developer to the consumer and were evaluated along with the TOE:

- Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria, Version 3.6, 2025

Any additional documentation provided with the product, or that is available online was not included in the scope of the evaluation and should not be relied upon when configuring or operating the product as evaluated. To use the product in the evaluated configuration, it must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the documentation from the NIAP website to ensure the product is configured as evaluated.

7 IT Product Testing

The evaluation team configured the TOE according to the vendor-provided guidance documentation and performed the tests specified in the [PP]. These results are summarized in the evaluation Assurance Activity Report with the approach summarized here.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities of this product.

7.2 Evaluation Team Independent Testing

The CCTL evaluation team created the test plan.

The functional testing was performed by CCTL evaluation team according to a Common Criteria Certification document and ran the tests specified in the [PP], including tests associated with optional requirements. The CCTL evaluation team generated a proprietary Detailed Test Report using the evidence collected by the CCTL evaluation team during the testing.

7.3 Vulnerability Analysis

The evaluation team performed each AVA_VAN.1 CEM work unit (as refined by the SD) and each AVA_VAN evaluation activity defined in the SD. A vulnerability analysis was performed following the processes described in the PP. The vulnerability analysis included a public domain search for potential vulnerabilities. This search was performed on December 29, 2025, and no applicable vulnerabilities were discovered.

8 Evaluated Configuration

This section briefly identifies the evaluated configuration(s) and any excluded and out of scope functionality.

8.1 Evaluated Configuration

This evaluation covers the TOE only in its evaluated configuration. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation identified in Section 6. The TOE is running on Ubuntu Linux LTS 18.04 and 22.04, running on VMware ESXI Virtualization Server. Ubuntu Linux is not part of the TOE but is provided together with the TOE as a virtual appliance.

The IT environment should contain the following hardware and services that are not considered parts of the TOE, but required for correct functioning of the TOE:

Non-TOE Software and Hardware

Component	Purpose	Specific Requirements.
Bastille Concentrator or other compatible data source	Source of data for the TOE.	Support of the TOE API
Network equipment	Enabling TOE connection to non-TOE entities listed in this table over network.	None
Microsoft Windows Server 2019, running Active Directory Federation Service (MS ADFS)	Authentication that uses OAuth, specifically, OIDC.	Microsoft Windows Server 2019 or 2022
NTP Server	Synchronizes the clocks on computers and networks across the Internet.	Any NTPv4-compliant server

VMware ESXi Virtualization Server (vCenter®, vSphere®)	Hosts Fusion Center virtual appliance.	VMware ESXi 7 or higher (Virtual Hardware Version 17 or higher) running Intel® Xeon® Gold 6242 CPU @ 2.80GHz. Minimum virtual machine resources: 32 GB RAM 100 GB disk (local to VM) 100 GB network mounted partition (NFS/external to VM)
Database Elasticsearch Cluster	Storage for data, data at rest.	Version 7.12 or higher 500 GB storage for index data
Data Queue Apache Kafka	Ephemeral data buffer or queue.	Version 2.7.0 or higher 20 GB storage or higher Minimum retention: 2 days

Table 2 Non-TOE Software and Hardware

8.2 Excluded Functionality

Any functionality not explicitly described in the [ST] or tested and reported in the [AAR] is considered excluded functionality for the purpose of this evaluation.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation was successful and provides a level of assurance that the TOE meets the Security Functional Requirements identified in the Security Target. This assurance comes from the performance of the work units associated with the Security Assurance Requirements. A detailed description of those Assurance Requirements as well as the details of how the product meets each of them can be found in the Security Target. A more detailed account of the evaluation assurance activities and the results obtained can be found in the Assurance Activity Report.

9.1 Security Target Evaluation (ASE)

The evaluation team applied each ASE CEM work unit. The [ST] evaluation ensured the [ST] contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the target PPs.

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

9.2 TOE Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit as refined by the target PPs. This activity is considered implicitly resolved.

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

9.3 Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work units as refined by the target PPs. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the target PPs.

The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator's guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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

9.4 TOE Life Cycle Support (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

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

9.5 TOE Tests (ATE)

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the target PPs and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validation team reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the target PPs and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment (AVA)

The evaluation team applied each EAL 1 AVA CEM work unit as refined by the target PPs. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing, and did not discover any issues with the TOE. The evaluation team also performed additional Assurance Activities as required by the target PPs and documented that in the AAR.

9.6.1 Software Bill of Materials

A Software Bill of Materials was provided to NIAP with a comprehensive list of first and third-party libraries that comprise the TOE. The SBOM was used in the vulnerability analysis during the evaluation period and was updated by the Vendor as requested by NIAP.

9.6.2 Vulnerability Search

The evaluation team performed several public searches over the course of the evaluation against the following sources to ensure there are no publicly known and exploitable vulnerabilities in the TOE:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

The most recent search was performed on December 29, 2025. The search was conducted with the following terms. A list of search terms, databases searched, and evaluation findings may also be found in the AVA.:

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:1.10:*:*:*:*:node.js:*:*
jackson-core
UL Verification Services Inc. and Bastille Networks, Inc.
2026-01-12
cpe:2.3:a:fasterxml:jackson-databind:2.9.7:*:*:*:*:*:*:*
cpe:2.3:a:apache:kafka:1.1.1:-:*:*:*:*:*:*
cpe:2.3:a:xerial:snappy-java:1.1.7.1:*:*:*:*:*:*:*
cpe:2.3:a:apache:zookeeper:3.4.10:-:*:*:*:*:*:*
xz
aiofiles
torchmetrics

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the target PPs and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the [ST] are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the [ST].

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM and correctly verified that the product meets the claims in the [ST].

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria Version 3.6, 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the [ST], and the only evaluated functionality was that which was described by the SFRs claimed in the [ST]. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

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

Evaluation activities are strictly bound by the assurance activities described in the Protection Profile for Application Software v1.4 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Security Target

Bastille Enterprise Fusion Center Version 3.6 Security Target, version 1.8, January 9, 2026

12 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[5] Protection Profile for Application Software, Version 1.4, 2021-10-07.

[6] Bastille Enterprise Fusion Center Version 3.6 Security Target, version 1.8, January 9, 2026

[7] Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria Version 3.6, 2025

[8] UL15574582-ATE-18, Bastille Test Report v1.3_18, January 12, 2026

[9] UL15574582-ATE-22, Bastille Test Report v1.3_22, January 12, 2026

[10] UL15574582-AAR, Assurance Activity Report, January 12, 2026

[11] UL15574582-ETR, Common Criteria Evaluation Technical Report Rev1.2, January 12, 2026

[12] UL15574582-ASE, ASE Verdicts V1.3, December 22, 2025

[13] UL15574582-AVA, Bastille Enterprise Fusion Center AVA Rev.1.1, December 31, 2025