Bastille

Bastille Enterprise

Fusion Center Administrative Guidance for Common Criteria

bastille.net

Notice for Bastille Networks, Inc. Software and Documentation

Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria 3.6

Table of Contents

1.0 About This Document

The *Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria* provides guidance to operate the Bastille Enterprise Fusion Center 3.6 (“Fusion Center”) in an environment consistent with the National Information Assurance Partnership (NIAP) Common Criteria (CC) for the Protection Profile for Application Software (APP). This document also explains how to use the security functional requirements (SFRs) claimed as part of the CC evaluation. Only the features and functionality required to use the Fusion Center are included in this document. Any functionality that is not explained in this document or in the Bastille Enterprise Fusion Center Security Target (ST) was not evaluated. For more information about Bastille Enterprise as a complete system, see 13.0 "References and Additional Resources".

1.1 Intended Audience

The *Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria* is intended for security administrators responsible for configuring and maintaining the Fusion Center and some related components. To get the most out of this document, the reader should be familiar with the following:

- Bastille Enterprise Fusion Center Security Target (ST)
- Linux® Ubuntu® 18.04
- VMware® ESXi™ 7 or later
- Microsoft® Windows Server® 2019 or 2022 running Microsoft Active Directory® Federation Services (ADFS)
- Networking and network engineering concepts

This document assumes that administrators are not careless, willfully negligent, or hostile, and that they use the software in compliance with the applied security policy.

1.2 Document Conventions

The following formatting conventions are used in this document.

Convention	Meaning
Bold text	User interface controls, including buttons, checkboxes, lists, menus, menu items, options, radio buttons, and text boxes
Italicized text	• Document titles • Variables
`Monospace text`	• Code examples • Directories

Convention	Meaning
	• File names and paths • Text as it appears on-screen in a terminal window
`Bold monospace text`	Text the user must type
`Italicized monospace text`	Variables in code examples and file paths
`Highlighted monospace text`	Commands entered into a terminal window

2.0 Introduction

Bastille Enterprise is a security product that detects and identifies wireless devices using software-defined radio (SDR) technology to monitor the electromagnetic spectrum for wireless devices' radio frequency (RF) emissions in specific spaces. You can use Bastille Enterprise in varied situations. One objective of a Bastille Enterprise deployment is situational awareness of a facility that includes many RF devices. In other cases, the objective is to alert security to devices that enter a restricted area.

Bastille Enterprise detects devices based on RF activity and delivers device observations. The site under observation includes the Bastille Enterprise Sensors and the Bastille Enterprise Concentrator. The Sensors receive RF device data from the site under observation and decode the information. The Sensors pass the data to the Concentrator, which refines the data. The Concentrator sends the data to the Fusion Center, which is usually housed outside the site under observation, in a data center.

The device data comes to the Fusion Center and the Fusion Center serves data to the systems that require it. An Elasticsearch® cluster stores all device observations and related events. Bastille Enterprise APIs interact with the Fusion Center to provide access to the device data in the Bastille Enterprise DVR Console, Device Dashboard, and Admin Console.

A customer may also choose to integrate Bastille Enterprise with other systems, such as Splunk®. Integrations are outside the scope of this certification.

Bastille Enterprise Components

Component	Purpose
Sensors	Sensors receive RF data from the site under observation. They send that data to the Concentrator.

Component	Purpose
Concentrator	The Concentrator receives RF data from the Sensors and refines that data. The Concentrator sends the data to the Fusion Center.
Fusion Center	The Fusion Center receives data from the Concentrator and serves data to the systems that require that data.
Elasticsearch	An Elasticsearch cluster receives data from the Fusion Center and stores all device observations and related events.
Apache® Kafka®	Bastille Enterprise uses Apache Kafka for message buffering. The Fusion Center passes data that is being transformed to Kafka. Final results are placed into Elasticsearch.
Microsoft Active Directory Federation Services	Bastille Enterprise uses Microsoft ADFS to authenticate user sign-ins and API requests. The Fusion Center integrates with Microsoft ADFS for user authentication and API authorization.
Splunk and other third-party integrations	Customers can integrate Splunk and other third-party applications to receive data from the Fusion Center.

2.1 Deployment Architecture

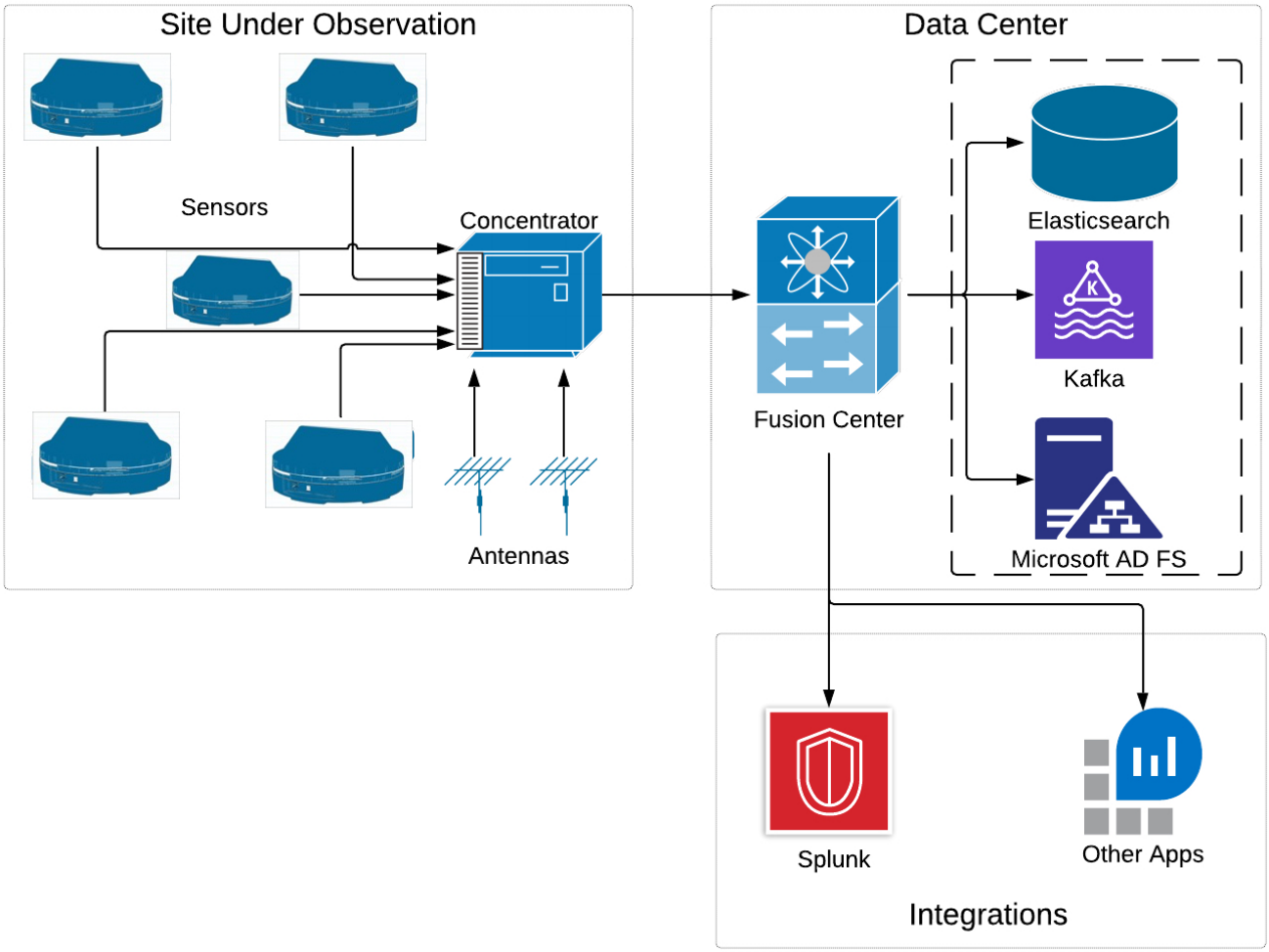
The site under observation includes the Bastille Enterprise Sensor array and the Bastille Enterprise Concentrator. The customer IT infrastructure includes an Elasticsearch® cluster, an Apache Kafka® cluster, and an OpenID Connect (OIDC) identity provider (IdP), such as Microsoft® Active Directory® Federation Services (ADFS). The Fusion Center and Airspace Defense Analytics Module (ADAM) (ADAM Explorer) can run within the Bastille Appliance or can be deployed to a customer-controlled environment. A customer may also choose to integrate other systems, such as Splunk®, with Bastille Enterprise. These integrations are optional.

Bastille Networks provides the following items:

- Sensor arrays
- Concentrator
- Fusion Center
- Outgoing webhooks for integration with other systems

Note: Stack-based buffer overflow protections, as well as memory and address space protections, are enabled by default and cannot be disabled or configured.

Bastille Enterprise System Architecture



2.2 Fusion Center Services and Resources

The Fusion Center is a VMware ESXi virtual machine (VM) running on Linux® Ubuntu® 18.04. The Fusion Center depends on an Elasticsearch cluster, an Apache Kafka cluster, and an OIDC IdP, such as Microsoft ADFS. You have the option to use external webhooks to connect and send event data to other systems, such as Splunk.

Fusion Center Dependencies

Component	Purpose
APIs	Bastille Enterprise REST APIs interact with the Fusion Center to provide access to data, web-based user interfaces, and data processing components. For more information about the Bastille Enterprise REST APIs, see the *Bastille Enterprise API Getting Started Guide*.
NGINX®	NGINX is an open source network communications gateway.
Filebeat™	Filebeat is an open source log forwarding service.

The customer is expected to provide the following items for the Fusion Center and its associated services and resources. These items can be at the site under observation or can be housed in the customer's IT infrastructure, for example, in a data center.

Fusion Center Components

Component	Purpose	Additional Information
SSL certificates	Wildcard certificate to authenticate users in the Bastille Enterprise domain.	The customer can specify the domain. There is no password for private key.
DNS host names	Enables Fusion Center and Concentrator access to Bastille Enterprise services.	The Fusion Center must be able to reach the DNS server that resolves these hosts.
NTP server	Synchronizes the clocks on computers and networks across the Internet.	Configured via the Fusion Center.
VMware ESXi (vCenter®, vSphere®)	Hosts the Fusion Center virtual appliance.	VMware ESXi 7 or later (Hardware Version 10 or higher) Minimum virtual machine resources: • 32 GB RAM • 100 GB disk (local to VM)

3.0 System Requirements and Prerequisites

The Bastille Enterprise Fusion Center requires only general computing hardware and network adapters. The hardware must be capable of running VMware ESXi 7 or later with a minimum of 32 GB RAM and 100 GB disk space, local to the VM.

The Fusion Center also requires the following items:

- NTP server
- Five hostnames with DNS resolution

  For more information, see the *Bastille Enterprise Installation Requirements Guide*.
- A single server certificate with Subject Alternative Name (SAN) entries for each of the five hostnames, the full certificate chain, and the associated private key for the server certificate in unencrypted PEM format
- Microsoft Windows Server® 2019 or 2022, running Microsoft ADFS

  For more information, see the *Bastille Enterprise OpenID Connect Identity Provider Integration Guide*.
- Elasticsearch cluster 7.12–7.17 with TLS 1.2 enabled, with a hostname with DNS resolution
- Apache Kafka cluster with TLS 1.2 enabled, with a hostname with DNS resolution
- Certificate chains for both Elasticsearch and Apache Kafka, which must contain non-public root CA certificates

  Fusion Center will import and trust the root certificates for the Elasticsearch and Apache Kafka servers.

4.0 User Accounts and Authentication

The Fusion Center uses Microsoft ADFS as the Identity Provider (IdP). All user accounts are maintained in Microsoft ADFS. User login attempts are redirected to Microsoft ADFS for user authentication. Upon successful user authentication, the user is granted a temporary access token. The Fusion Center verifies the token for this login session to allow the user access to the Bastille Enterprise Admin Console.These tokens are verified based on the installation configuration parameters in the `fusion_center.yml` file. For more information, see 5.0 "Set Up the Fusion Center Image".

The Fusion Center has one user role. Users who can access the Fusion Center can perform all functions possible in the Fusion Center.

5.0 Set Up the Fusion Center Image

There are several parts to setting up the Fusion Center image:

1. Make sure you have created and set up the Fusion Center VM.
2. Make sure you have created the Fusion Center DNS entries. For more information, see the *Bastille Enterprise Installation Requirements Guide*.
3. Create the `fusion_center.yml` file. For more information, see 5.1 "Create the Fusion Center YML File".

4. Upload the necessary certificate files and add certificates to the trust store, if necessary. For more information, see 5.2 "Certificate Files".
5. Install the Fusion Center image. For more information, see 5.3 "Install the Fusion Center Image".

   When you install the Fusion Center image, you set the Fusion Center mode, enable or disable SSH access, and enter a passphrase to unlock the keyring.

This process applies to both new installations and upgrades of Bastille Enterprise.

5.1 Create the Fusion Center YML File

The Fusion Center YML file—by default, `fusion_center.yml`—contains settings for Bastille Enterprise, including fully qualified domain names, certificate data, and OIDC IdP and Apache Kafka information. Unless identified as optional, each setting must have a value. Only the settings that are listed in the table "Fusion Center Configuration File Settings" are editable.

Bastille Enterprise obtains the certificate key and endpoint directly from the OIDC IdP you specify in the Fusion Center YML file. Bastille Enterprise uses TLS (Transport Layer Security) to provide communications security between systems and applications. The Bastille Fusion Center must trust all certificates. During installation, you must provide information for certificates, including certificate information for third-party systems, such as Splunk and Elastic Logstash®, or for self-signed certificates.

To create the Fusion Center YML file:

1. From the VMware ESXi web application, go to the VM console for the Fusion Center and log in.

   Bastille Networks Support provides the default login credentials.
2. Get the `fusion_center.yml` file example by running the following command:

   ```
   file edit fusion_center.yml
   ```

   Note: Bastille Networks recommends naming the Fusion Center YML file `fusion_center.yml`, but you can choose to use a different name.
3. Copy the information.
4. To create the new file, enter the following command:

   ```
   file edit fusion_center.yml
   ```
5. Edit the file by providing the appropriate information. If the setting is not listed in the following table, you must not change that setting.

Note: The `installer_yaml_version` setting indicates the Fusion Center YML file version. For Bastille Enterprise 3.6, this value must be `1.4`.

Fusion Center Configuration File Settings

Setting	Description	Example
`ntp_server`	The NTP server IP address	`172.30.11.10`
`deployment_ shared_secret`	Shared secret for sub-systems	`examplesecret`
`elasticsearch: host`	Elasticsearch storage cluster location The Elasticsearch cluster must support `https`. Optionally, the indexes can have a prefix to establish a namespace for Bastille Enterprise. Enter that namespace here, using the fully qualified domain name or the IPv4 address. The Elasticsearch host must support TLS. TLS is the default behavior. No special configuration is necessary to ensure that the Fusion Center uses TLS with the Elasticsearch cluster.	`elastic.example. bastille.cloud`
`elasticsearch: port`	Elasticsearch storage cluster location port	`9200`
`elasticsearch: username` (optional)	Elasticsearch username To enable authentication in Elasticsearch, enter the username here. If you are using the storage VM that Bastille Networks supplies, you must first add this information to the storage VM.	`bn`
`elasticsearch:`	Elasticsearch password	`bnbnbn`

Setting	Description	Example
`password` (optional)	To enable authentication in Elasticsearch, enter the password here. If you are using the Elasticsearch instance that Bastille Networks provides, the password must be six characters or more. If you are using the storage VM that Bastille Networks supplies, you must first add this information to the storage VM.	
`hostnames: admin`	Fully qualified domain name for the Bastille Enterprise Admin Console	`admin.example.bastille.cloud`
`hostnames: api`	Fully qualified domain name for the Bastille Enterprise API	`api.example.bastille.cloud`
`hostnames: dvr`	Fully qualified domain name for the Bastille Enterprise DVR Console	`dvr.example.bastille.cloud`
`hostnames: streaming`	Fully qualified domain name for the Bastille Enterprise Fusion Center	`streaming.example.bastille.cloud`
`hostnames: device`	Fully qualified domain name for the Bastille Enterprise Device Dashboard	`device.example.bastille.cloud`
`https: cert_chain`	The full server certificate chain for the Fusion Center, including any root certificate authority not embedded in the virtual appliance Each certificate must be PEM encoded.	`global.pem`
`https: key_file`	The private key for the specified server certificate The key must be PEM encoded.	`global.key`

Setting	Description	Example
`initial_install_or_upgrade_overrides: auth: oidc: idp`	OIDC identity provider You can use Microsoft ADFS (`adfs`), Oracle Identity Cloud Services (`oics`), or WebADM (`webadm`).	`adfs`
`initial_install_or_upgrade_overrides: auth: oidc: host`	Fully qualified domain name for the OIDC IdP server	`auth.test.adfs.bastille.cloud`
`initial_install_or_upgrade_overrides: auth: oidc: oauth_client_ids: admin`	Client ID for the Bastille Enterprise Admin Console The same client ID for all three apps is allowed.	`bn-cid-web-id-1`
`initial_install_or_upgrade_overrides: auth: oidc: idp: oauth_client_ids: device`	Client ID for the Bastille Enterprise Device Dashboard The same client ID for all three apps is allowed.	`bn-cid-web-id-2`
`initial_install_or_upgrade_overrides: auth: oidc: idp: oauth_client_ids: dvr`	Client ID for the Bastille Enterprise DVR Console The same client ID for all three apps is allowed.	`bn-cid-web-id-2`

Setting	Description	Example
`initial_install_or_upgrade_overrides: kafka: host`	Fully qualified domain name for the Apache Kafka host	`kafka.example.bastille.cloud`
`initial_install_or_upgrade_overrides: port`	Apache Kafka port	`9092`
`initial_install_or_upgrade_overrides: kafka: username` (optional)	Apache Kafka username To enable authentication in Kafka, enter the username here. You must also add this information to the storage VM.	`bn`
`initial_install_or_upgrade_overrides: kafka: password` (optional)	Apache Kafka password To enable authentication in Kafka, enter the password here. You must also add this information to the storage VM.	`bn`
`trust_store: additions` (optional)	A list of files, each of which holds one root certificate You can include certificates for webhooks here. For more information about webhooks, see the *Bastille Enterprise Admin Console Guide*.	`- "corporate_ca.pem"` `- "webhook_ca.pem"`
`web_console_ports: admin` (optional)	Custom port for the Admin Console	`7000`
`web_console_ports: dvr`	Custom port for the DVR Console	`7001`

Setting	Description	Example
(optional)		
`web_console_ports: device` (optional)	Custom port for the Device Dashboard	`7002`

6. Save the file.

Example fusion_center.yml File

```
trust_store:
   additions:
      - "corporate_ca.pem"
      - "webhook_ca.pem"


web_console_ports:
      admin: "7000"
      dvr: "7001"
      device: "7002"

required:
   installer_yaml_version: "1.4"
   ntp_server: "172.30.11.10"
   deployment_shared_secret: "examplesecret"
   elasticsearch:
      host: "elastic.example.bastille.cloud"
      port: "9200"
      username: "bn"
      password: "bnbnbn"

   hostnames:
      admin: "admin.example.bastille.cloud"
      api: "api.example.bastille.cloud"
      dvr: "dvr.example.bastille.cloud"
      streaming: "streaming.example.bastille.cloud"
      device: "device.example.bastille.cloud"
   https:
      cert_chain: "global.pem"
      key_file: "global.key"
   initial_install_or_upgrade_overrides:
      auth:
         oidc:
            idp: "adfs"
            # valid values for `idp` are "adfs", "oics", "other", or "webadm"
            host: "auth.test.adfs.bastille.cloud"
            oauth_client_ids:
```

```
            # same client id for all three apps is allowed.
            admin: "bn-cid-web-id-1"
            device: "bn-cid-web-id-2"
            dvr: "bn-cid-web-id-2"
      kafka:
         host: "kafka.example.bastille.cloud"
         port: "9092"
         username: "bn"
         password: "bn"
```

5.2 Certificate Files

The Bastille Enterprise Fusion Center must trust all certificates. You must upload certificate files to the Fusion Center for installation. If you use third-party or self-signed certificates, you must add that information to the `fusion_center.yml` file. Before installation, you run a command to add those certificates to the trust store.

5.2.1 Certificate Format

The certificate must be an X.509 version three certificate, issued by a trusted certification authority (CA) or be a self-signed certificate that is explicitly trusted by the application. The certificate must include the Extended Key Usage (EKU) extension with the id-kp-serverAuth Object Identifier (OID: 1.3.6.1.5.5.7.3.1), indicating its intended use for TLS WWW server authentication.

The certificate must contain a valid digital signature and must not be expired or revoked at the time of use. For revocation checking, the certificate must specify a Certificate Revocation List (CRL) Distribution Point and the Authority Information Access (AIA) extension must specify the CA issuer URI. The application shall perform CRL validation at runtime using the most recent CRL issued by the CA.

The certificate path must terminate in a known and trusted root, ensuring a valid certification path for trust establishment.

5.2.2 X.509 CRL Behavior

The Bastille Fusion Center refreshes its CRL information from CRL distribution points every 24 hours using Fetch CRL, which is a Linux utility. The Bastille applications also reload their SSL context after this fetch is complete. After the Fusion Center fetches the CRL information, the platform caches this information. If the CRLs expire before the next fetch, the applications' TLS connections will be dropped until the next Fetch CRL session.

5.2.3 Root Certificates

If a new trusted root is needed, the certificate can be installed by uploading the root certificate to the Fusion Center. You must then update the `fusion_center.yml` file by editing the `trust_store: additions` setting, as shown in "Example fusion_center.yml File" and running the Fusion Center installer.

At the time of the initial installation, you can specify only one root certificate, which must adhere to the requirements outlined in this section. You can add additional certificates to the trust store by editing the `trust_store: additions`setting, as shown in "Example fusion_center.yml File" and running the Fusion Center installer.

Note: Do not install multiple certificates for the same domain if they are signed by different root CAs. OpenSSL selects a single trust path during verification. All certificates for a given domain must chain to the same trusted root to ensure deterministic and secure validation.

5.2.4 Upload Certificates

To upload certificate files:

- Upload the `.pem` and `.key` files to `/home/bn`.

Note: Ensure that the `key_file` setting in the `fusion_center.yml` file is set to *`filename`*`.key`. You can run **`cat /home/bn/fusion_center.yml`** to check the settings.

5.3 Install the Fusion Center Image

When you install the Fusion Center image, you set the Fusion Center mode, enable or disable SSH access, and enter a passphrase to unlock the keyring.

There are two modes of operation available, National Information Assurance Partnership (NIAP) and normal operation. There are no additional error or diagnostic modes. To install the Fusion Center in NIAP mode, use the **`--niap`** installation flag. The Fusion Center version information indicates if NIAP mode is enabled. For more information, see 10.1 "Determine the Fusion Center Version".

When you install the Fusion Center image, you decide whether you will allow SSH access to the VM.

To install the Fusion Center image:

1. Log in to the VMware ESXi web console for the Fusion Center VM.
2. To set up the Fusion Center in NIAP mode, enter the following command:

   ```
   install fusion_center -c fusion_center.yml --ssh disable --from-console --niap install
   ```

3. If prompted to do so, change the Fusion Center VM password.
4. If prompted to do so, enter the keyring passphrase in the VMware ESXi console.

> **Note:** You must enter a passphrase to unlock the keyring. You can't use the Fusion Center until you unlock the keyring.

5. To reboot the system, enter the following command:

   ```
   system reboot now
   ```

6. After the system restarts, in the VMware ESXi Console for the Fusion Center VM, enter the following command:

   ```
   install fusion_center -c fusion_center.yml --ssh disable --from-console --niap resume
   ```

After set up is complete, access the Fusion Center VM through VMware ESXi only when you are directed to do so by Bastille Networks Support.

6.0 Edit Fusion Center Settings

You typically set Fusion Center settings during installation or upgrades. Changing Fusion Center settings outside of those contexts could result in leaving Bastille Enterprise inoperable. You can, however, set up webhooks at any time without affecting system operation. For more information about webhooks, see 8.0 "Set Up Webhooks".

7.0 Troubleshooting the Fusion Center

The Admin Console dashboard displays the Fusion Center status tree. You can navigate this tree to determine Bastille Enterprise Fusion Center health. You can expand the branches to see all of the elements.

There are four states:

- Green indicates the component is functioning as intended, or OK.
- Yellow indicates a warning.
- Red indicates an error.
- Gray indicates an unknown status.

The **Host** status group shows the memory, load, disk space, and timing synchronization for the physical or virtual Fusion Center machine. It also indicates the availability of space in the Elasticsearch cluster. When the Elasticsearch disk space gets to 80%, the status moves to the warning, or yellow, state. When the Elasticsearch disk space gets to 88%, the status moves to the error, or red, state.

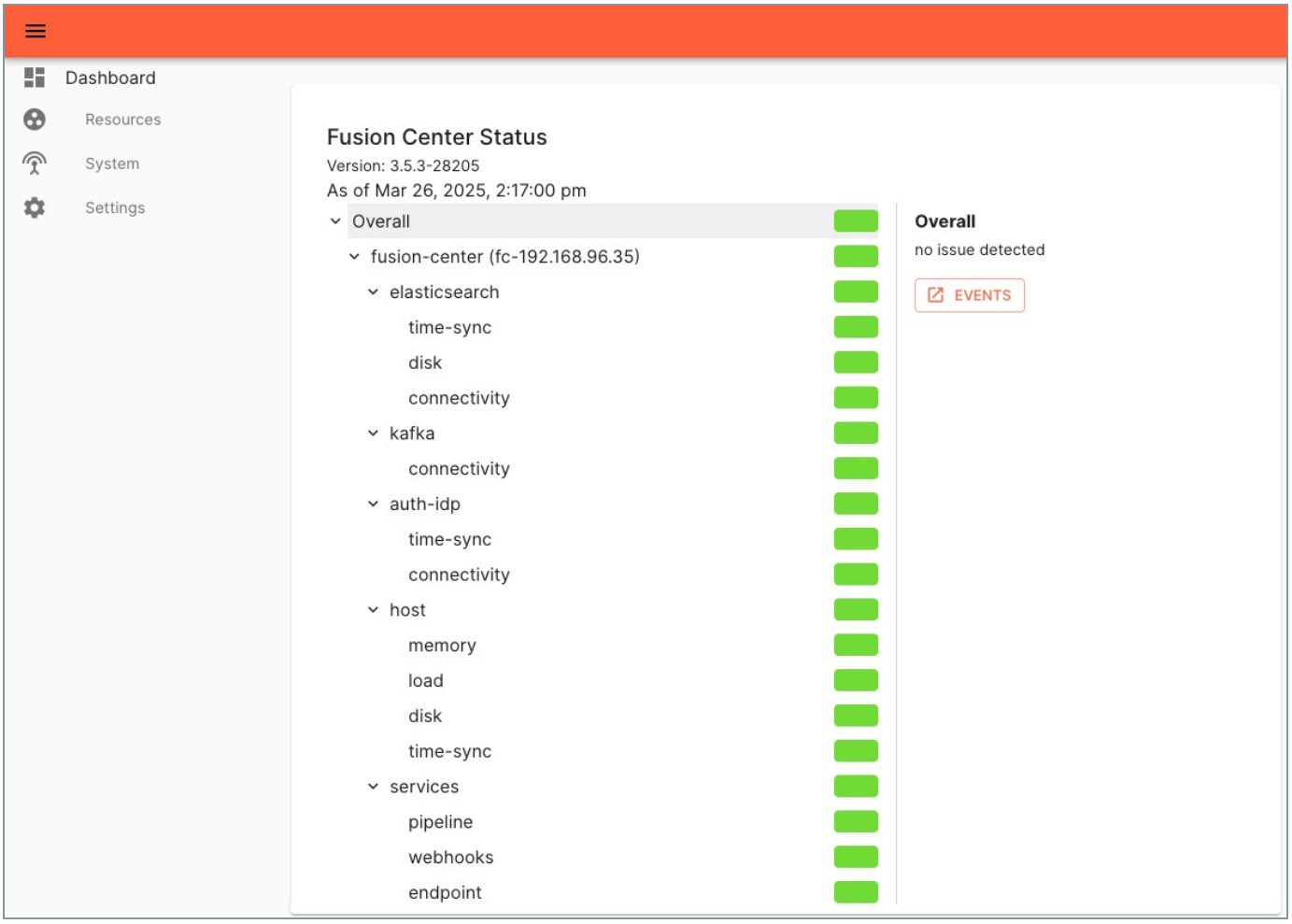
Fusion Center Status Troubleshooting

Status Item	Status	Troubleshooting Actions
elasticsearch: time-sync	red	The time between the Fusion Center and Elasticsearch is not synchronized. • Restart the Storage VM. • If the problem persists, the timing between the Storage VM and the Network Services VM might be off.
elasticsearch: disk	yellow	Elasticsearch storage is 80% full. Contact Bastille Networks to determine which indexes can be deleted to free space. Contact Bastille Networks Support to plan for a storage replacement.
elasticsearch: disk	red	Elasticsearch storage is 88% full. Contact Bastille Networks to determine which indexes can be deleted to free space. Contact Bastille Networks Support to plan for a storage replacement. If Elasticsearch is already in read-only mode, refer to the Elasticsearch documentation to restore normal operation.
elasticsearch: connectivity	red	The Fusion Center cannot reach Elasticsearch. • Verify that the Elasticsearch cluster is running and available outside of the Fusion Center. • Verify the Elasticsearch configuration settings in the `fusion_center.yml` file. For more information, see 5.0 "Set Up the Fusion Center Image".
auth-idp: time-sync	red	The time between the Fusion Center and the IdP is not synchronized. • Restart the IdP instance. • If the problem persists, the timing between the IdP instance and the Network Services VM might be out of sync.
auth-idp: connectivity	red	The Fusion Center cannot reach the OIDC IdP. • Verify that the OIDC IdP server is running and available outside of the Fusion Center. • Verify the OIDC IdP configuration settings in the `fusion_center.yml` file. For more information, see 5.0 "Set Up the Fusion Center Image".

Status Item	Status	Troubleshooting Actions
host: memory	yellow	The Fusion Center is using more than 80% of the assigned memory. Continue to monitor the memory use, but the system is functioning within normal parameters.
host: memory	red	The Fusion Center is using more than 90% of the assigned memory. Verify and adjust the memory and CPU for the Fusion Center VM. For more information see 5.0 "Set Up the Fusion Center Image".
host: load	yellow	The Fusion Center is using more than 80% of the CPU resources. Watch the status to see if it improves or worsens.
host: load	red	The Fusion Center is using more than 90% of the CPU resources. Restart the Fusion Center.
host: disk	yellow	The Fusion Center is using more than 80% of the mounted storage. Continue to monitor the disk use, but the system is functioning within normal parameters.
host: disk	red	The Fusion Center is using more than 90% of the mounted storage. Clean up the logs on the Fusion Center.
host: time-sync	red	The time between one or more of the physical or virtual machines is not synchronized.
services: pipeline	red	The information flow is interrupted.
services: webhooks	red	The Fusion Center cannot reach one or more webhooks. • Verify that the third-party system is running and available outside of the Fusion Center. • Verify that the webhooks have been set up properly. For more information, see 8.1 "Set Up an HTTPS Webhook".
services: endpoint	yellow	The Concentrator has not been running long enough for observations to stream to the Fusion Center. This problem should resolve itself, as the Concentrator starts streaming.

Status Item	Status	Troubleshooting Actions
services: endpoint	red	The Fusion Center is not processing observations from the Concentrator. • Check the Fusion Center logs for anomalies. • Restart the Fusion Center. • Restart the Storage VM.

Fusion Center Status Tree



8.0 Set Up Webhooks

Using webhooks, Bastille Enterprise can send event data streams to other web applications, such as Splunk and Elastic Logstash. Bastille Enterprise sends the event type and payload to the configured web-hook in JSON format.

When you set up a webhook, you must enter the complete URL, beginning with **`https`** and including the fully qualified domain name or IPv4 address, for example:

- https://204.279.30.251:8080/ingest
- https://splunk.staging.customer.cloud:8080/services/collector

Note: Bastille Enterprise does not support the IPv6 format.

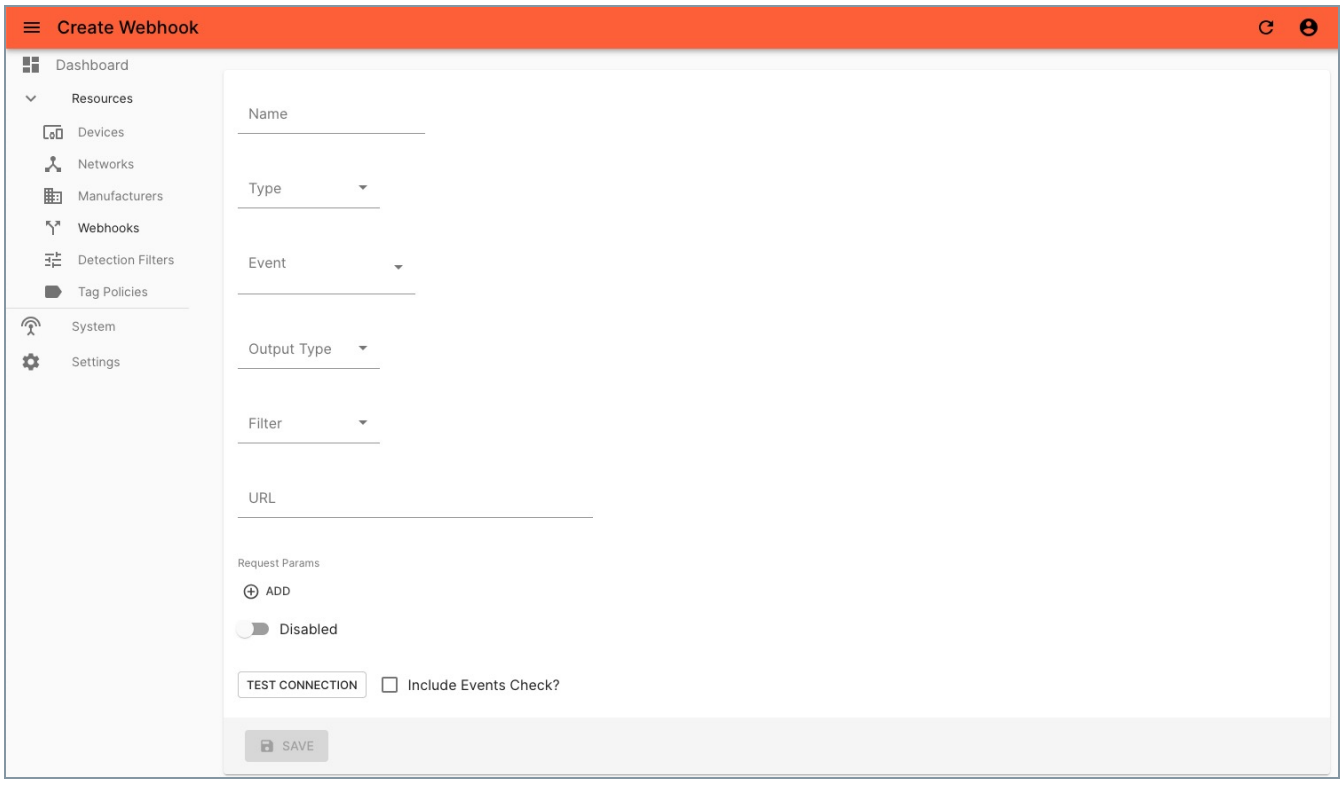
Changes to webhooks automatically take effect, and don't require deployment to the Concentrator.

8.1 Set Up an HTTPS Webhook

In NIAP mode, Bastille Enterprise allows only the HTTPS protocol. You cannot use HTTP.

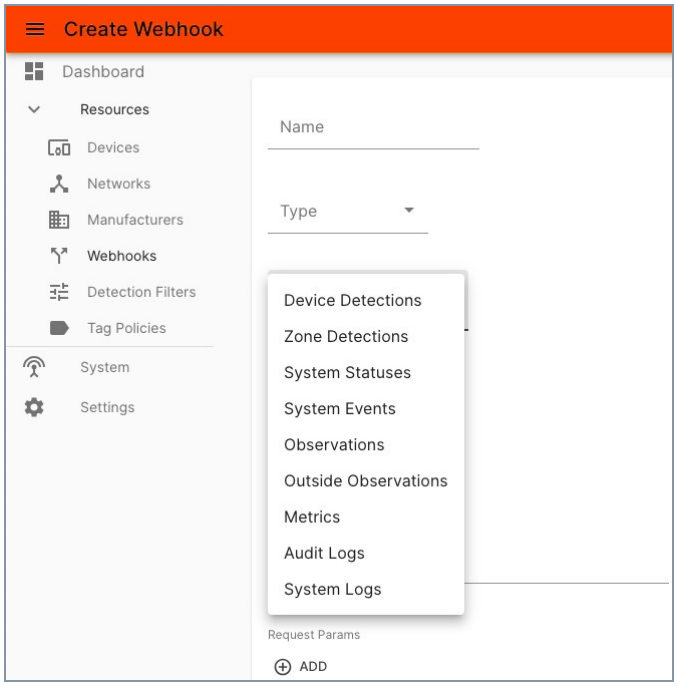
To set up an HTTPS webhook:

1. In the **Resources** group, click **Webhooks**.
2. Click **Create**.

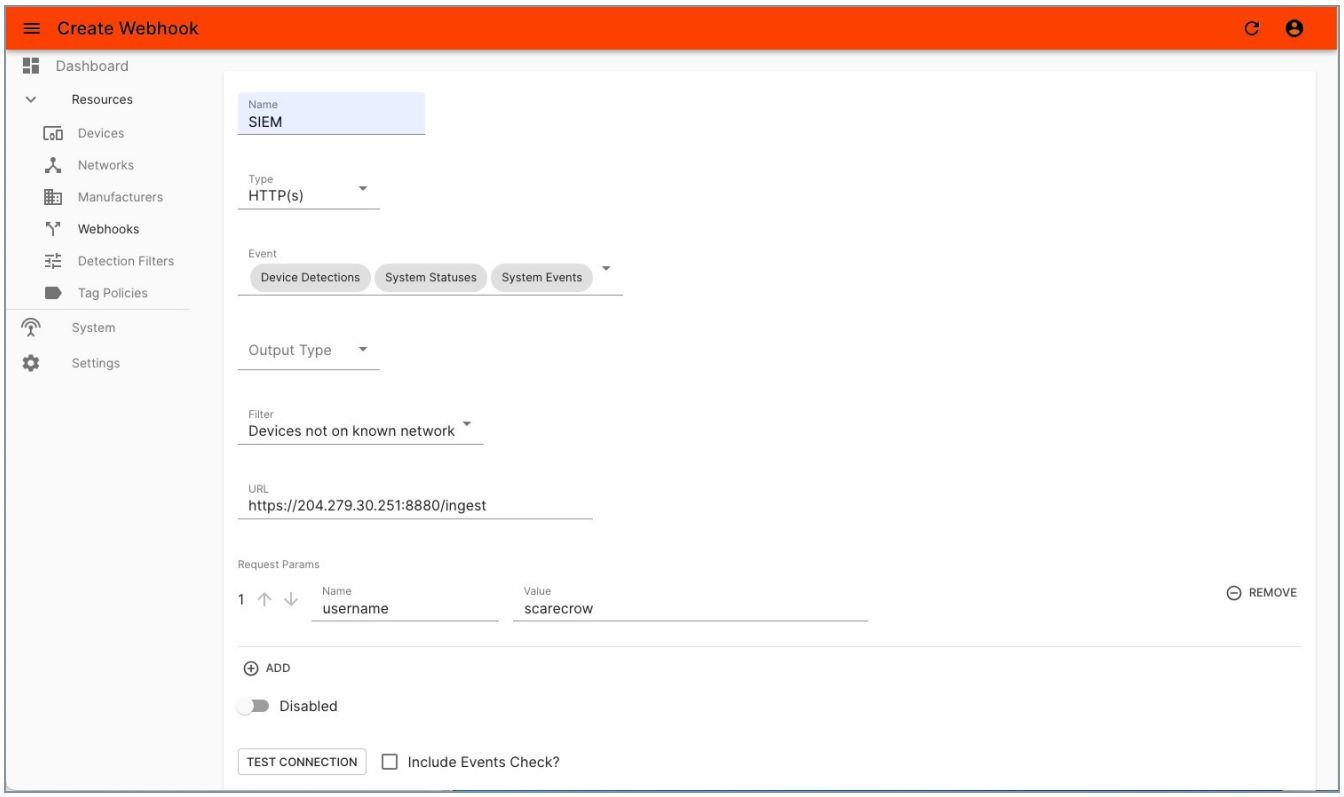


3. Enter a **Name** to identify the webhook.
4. From the **Type** list, select **HTTP(s)**.

5. From the **Event** list, choose one or more event streams to send.
   - **Device Detections** include the first and last times Bastille Enterprise detects a device.
   - **Zone Detections** include the first and last times Bastille Enterprise detects a device in a defined zone.
   - **System Statuses** include Concentrator and Fusion Center status streams, which you can also see on the **System Statuses** page.
   - **System Events** include system upgrade, system health, system configuration, system survey, and restart events, which you can also see on the **System Events** page.
   - **Observations** include the stream of device observations seen in the DVR Console. This could be, at most, one device per device ID per second.
   - **Metrics** include some system and protocol metrics.
   - **Audit Logs** include API calls and responses.
   - **Logs** include Fusion Center and Concentrator log files. Audit logs are mostly useful for Bastille Networks Support.



6. From the **Output Type** list, select **NDJSON** or **JSON Array**.
7. From the **Filter** list, select a detection filter. For more information about detection filters, see "Create a Detection Filter" in the *Bastille Enterprise Admin Console Guide*.
8. Enter the endpoint **URL**.
9. To add request parameters to the webhook, below **Request Params**, click **Add**.



10. Enter the parameter **Name** and **Value**.
11. If necessary, click **Add** to add more parameters.
12. To disable the webhook, select **Disabled**.
13. Select **Include Events Check** to send a test message for each event selected.
14. Click **Test Connection** to create a test event and POST it to the configured webhook system.

    Bastille Enterprise reports success if all messages resolve. If one or more events experiences a problem, Bastille Enterprise reports a failure.

    The Fusion Center automatically adds the CA certificate for the webhook to the trust store.
15. Click **Save**.

Note: If you run the Fusion Center installer after creating webhooks, you must return to each webhook and click the **Test Connection** button.

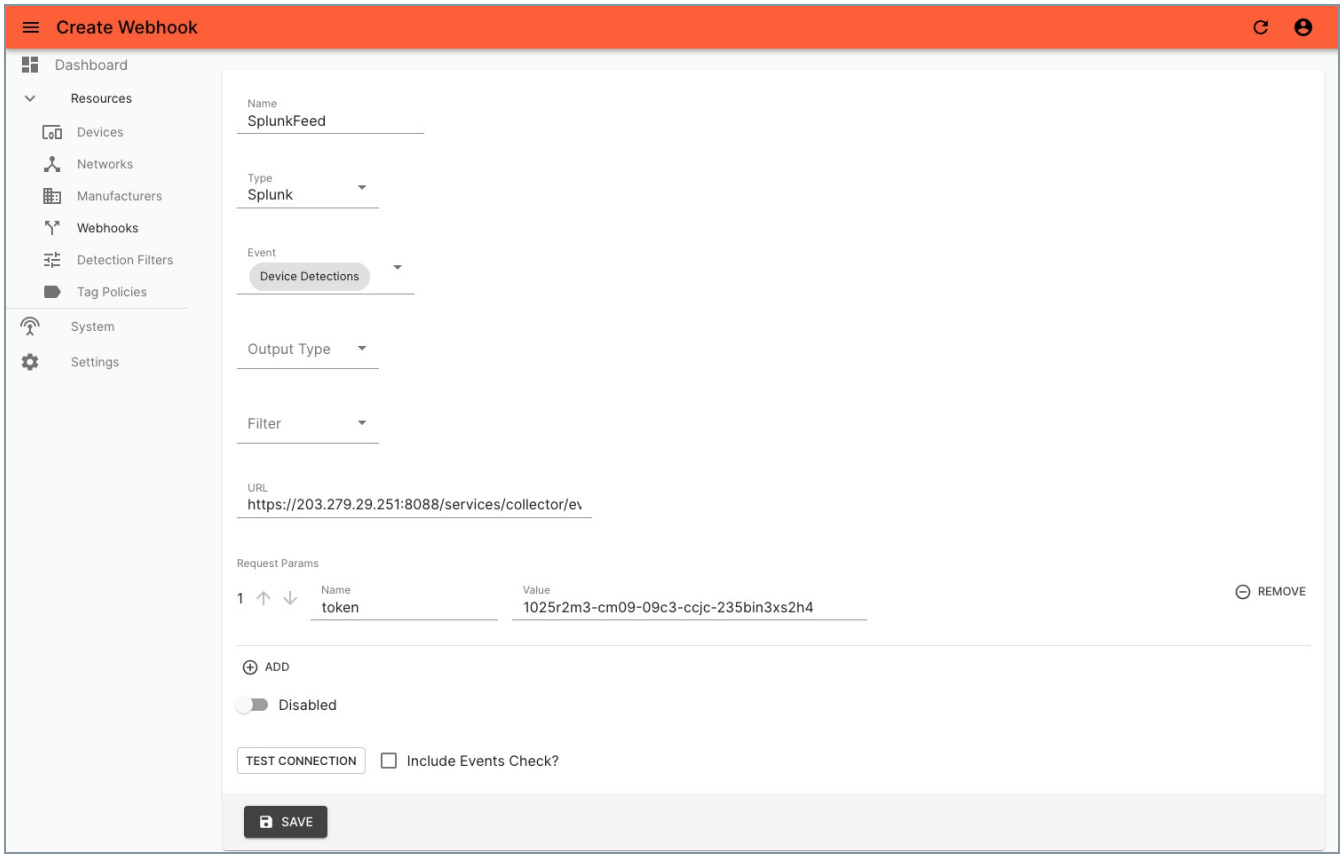
8.2 Set Up a Splunk Webhook

To configure your integration between Bastille Enterprise and Splunk, the administrator copies the Splunk URL and token to the Bastille Enterprise Admin Console. After entering the URL, all system events, including device and zone events, will stream to Splunk in real time.

Use the Bastille Enterprise Admin Console to enter Splunk settings for the Fusion Center. You may need to contact your Splunk administrator to obtain the Splunk URL. The Splunk token value comes from your Splunk instance.

To set up Bastille Enterprise Splunk settings:

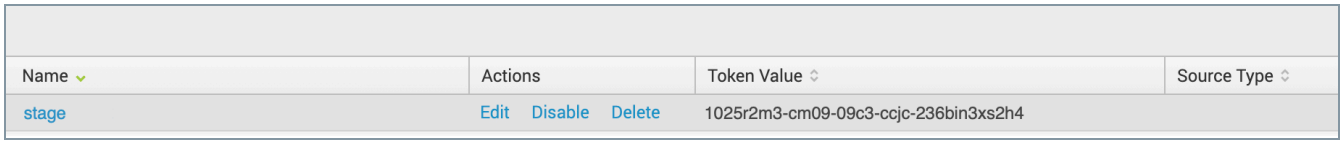
1. Log into the Bastille Enterprise Admin Console.
2. In the **Resources** group, click **Webhooks**.
3. In the upper right corner, click **Create**.



4. Enter a **Name** for the webhook.
5. From the **Type** list, select **Splunk**.
6. From the **Event** list, select one or more of the event feeds to send from Bastille Enterprise to Splunk.
7. Enter the Splunk **URL**.

   This is the Splunk HTTP Event Collector URL. You may need to speak with your Splunk administrator to obtain this URL.
8. In the **Request Parameters** group, click **Add**.
9. Enter the Splunk token **Name** and **Value**.

The Splunk token value comes from your Splunk instance.



10. Select **Include Events Check** to send a test message for each event selected.
11. Click **Test Connection** to create a test event and POST it to Splunk.

Bastille Enterprise reports success if all messages resolve. If one or more events experiences a problem, Bastille Enterprise reports a failure.

12. If the test succeeds, click **Save**.

9.0 Restart the Fusion Center

You must restart the Fusion Center VM from the VMware ESXi browser. There, you can open the console for the Fusion Center and enter the passphrase to unlock the keyring. You will not be able to use the Fusion Center until you unlock the keyring using the console.

To restart the Fusion Center:

1. Log into the VMware ESXi browser.
2. Open the console for the Fusion Center VM.
3. Enter the passphrase to unlock the keyring.

10.0 Update the Fusion Center

To update the Fusion Center, check for updates. If updates exist, contact Bastille Networks Support at support@bastille.net for access to the Bastille Networks secure portal to obtain updated versions of the Fusion Center.

After you receive the update, follow the instructions 5.0 "Set Up the Fusion Center Image" to create a Fusion Center VM for the update.

10.1 Determine the Fusion Center Version

To determine the Bastille Fusion Center version:

1. Log in to the Bastille Enterprise Admin Console.
2. On the Dashboard, just below “Fusion Center Status” you find the Fusion Center Version.

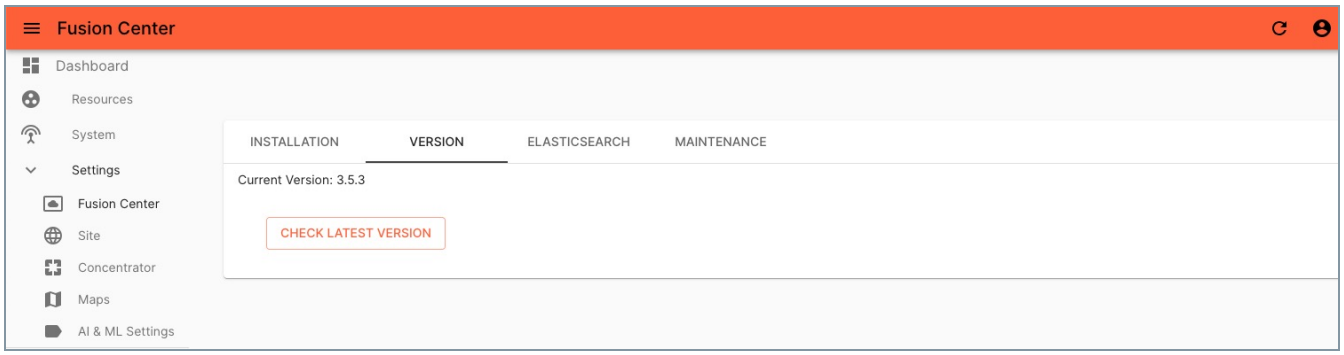
If NIAP mode is enabled, “NIAP Mode: Enabled” appears below the version number.

10.2 Check for Fusion Center Updates

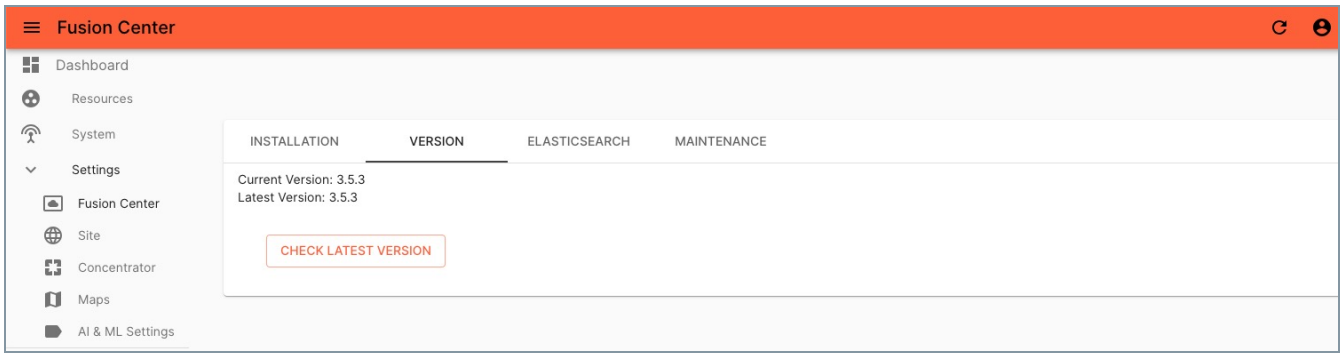
You can check for Fusion Center updates in the Bastille Enterprise Admin Console.

To check for Fusion Center updates:

1. Log into the Bastille Enterprise Admin Console.
2. Click **Settings**.
3. Click **Fusion Center**.
4. Next to the Fusion Center name, click **Show**.
5. Click the **Version** tab.



6. Click **Check Latest Version**.
7. Click **Yes, Check Version**.
8. Compare the version numbers for the current and latest versions.



10.3 Verify Fusion Center Updates

The Fusion Center image is distributed with a digital signature file. The public key for this signature is available on the Bastille Networks website.

To verify a Fusion Center update:

1. Download the Bastille Networks public key from our website at https://www.bastille.net/support.
2. In a terminal console window, run the following command:

```
openssl dgst -sha256 -verify bastille.rsa.pub -signature fusion_
center.sig fusion_center.ova
```

After running the command, the message **`Verified OK`** appears.

11.0 Support

Your customer support entitlement is based on the Bastille Enterprise package you purchased from Bastille Networks. Contact Bastille Networks to determine your customer support entitlement. Report any security issues to Bastille Networks Support at support@bastille.net.

12.0 Terminology

ADFS (Active Directory Federation Services)

Microsoft Active Directory Federation Services provides single sign-on access to systems and applications across organizational boundaries.

Admin Console

The Bastille Enterprise Admin Console is a graphical user interface on top of the Admin API that enables Security Administrators to monitor the status of the Bastille Enterprise Concentrators and Sensors, and define devices, networks, manufacturers, users, and zones to better track those items.

API (Application Programming Interface)

An API is a set of rules enabling programmers to develop software for a system. For more information about the Bastille EnterpriseREST APIs, see the Bastille Enterprise API Getting Started Guide.

APP (Application Protection Profile)

The Application Protection Profile describes the security functionality of application software in terms of common criteria (CC) and to define functional and assurance requirements for such software.

Bluetooth

Bluetooth is a standard for short-range wireless connection of electronic devices.

CC (Common Criteria)

Common criteria provides a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation.

Certificate

A certificate is a file that identifies and authenticates a server, computer, or user.

Certificate Authority

A certificate authority is an organization that validates entity identities and binds them to cryptographic keys by issuing digital certificates.

CID (Company Identifier)

The company identifier is a 22-bit number that uniquely identifies a company.

Concentrator

The Bastille Enterprise Concentrator is hardware that receives data from the Bastille Enterprise Sensors, refines that data, and sends the refined information to the Bastille Enterprise Fusion Center.

Device

In Bastille Enterprise, a device is an individual object that emits radio frequency data.

Device Dashboard

The Bastille Enterprise Device Dashboard enables forensic analysis of specific devices.

DHCP (Dynamic Host Configuration Protocol)

Dynamic host configuration protocol is a network protocol in which a server automatically assigns an IP address and other information to each host on the network.

DNS (Domain Name System)

Domain names are common names for web sites and other Internet services. DNS translates IP addresses into domain names.

DVR Console

The Bastille Enterprise DVR Console is a graphical user interface on top of the Device API that enables users to view sites under observation and the devices and networks those sites contain.

Elasticsearch

Elasticsearch is a distributed, RESTful search and analytics engine produced by the company Elastic.

Endpoint

An API endpoint is the point at which the API interacts with another system.

Filebeat

Filebeat monitors log files and locations and collects log events to forward them to Elasticsearch.

Frequency

Frequency is the number of complete oscillations per second of energy in the form of waves.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name is the most complete name that defines a host or server.

Fusion Center

The Bastille Enterprise Fusion Center receives refined data from the Bastille Enterprise Concentrator and serves that data to the appropriate systems.

Geofence

A geofence uses technology to create a virtual geographic boundary, which enables software to trigger a response when a mobile device enters or leaves the defined area.

HTTPS (Hypertext Transfer Protocol Secure)

HTTP is the protocol used to transfer data on the Internet. HTTPS uses a secure socket layer for security purposes.

IdP (Identity Provider)

An identity provider is a service that manages digital identities for authentication purposes.

JSON (JavaScript Object Notation)

JavaScript Object Notation is a lightweight data interchange format that is easy for machines to parse and generate.

Kafka

Apache Kafka is an open-source distributed event streaming platform produced by the Apache Software Foundation.

MAC (Media Access Control)

A media access control address serves as a unique identifier for a piece of hardware. A protocol's MAC algorithm dictates how, when, and where in the spectrum an emitter transmits.

NGINX

NGINX is open source software for web serving, reverse proxying, caching, load balancing, media streaming, and other activities.

NIAP (National Information Assurance Partnership)

The National Information Assurance Partnership is responsible for implementing common criteria (CC) in the United States.

NTP (Network Time Protocol)

Network Time Protocol synchronizes computer clocks over a network.

OIDC (Open ID Connect)

Open ID Connect is a protocol used to autenticate identities when users access an HTTPS end point.

OVA/OVF (Open Virtual Appliance/Open Virtualization File)

Virtualization applications like VMware use OVA and OVF files to describe a virtual machine.

PEM (Privacy-Enhanced Mail)

Privacy-enhanced mail is a file format for storing and sending cryptographic keys and certificates.

RF (Radio Frequency)

Radio frequency refers to any of the electromagnetic wave frequencies that lie in the range extending from below three kilohertz to about 300 gigahertz.

SAN (Subject Alternative Name)

A Subject Alternative Name, also known as a SAN certificate, is a certificate that allows protection for multiple hostnames in a single certificate.

SDR (Software-defined Radio)

Software-defined radio is a radio communication system in which components that have typically been implemented in hardware are instead implemented using software on a computer or on an embedded system.

Sensor

A Bastille Enterprise Sensor is hardware that receives radio frequency data and sends that data to the Bastille Enterprise Concentrator.

SFR (Security Functional Requirement)

A security functional requirement is a requirement for security enforcement in the product under evaluation.

Site Under Observation

The site under observation is the physical location of the Bastille Enterprise Sensor array.

SSL (Secure Sockets Layer)

SSL is a secure protocol for sending information over the Internet securely.

ST (Security Target)

The Security Target is a set of security requirements for a specific product.

VM (Virtual Machine)

A virtual machine is a computer file, or image, that emulates a physical computer.

Webhook

A webhook is an event notification, typically sent as a POST request via HTTP.

WiFi (Wi-Fi)

WiFi, or Wi-Fi, is a family of wireless networking technologies based on the IEEE 802.11 standards, used for local area networking of devices and Internet access.

YAML/YML

YAML is a human friendly data serialization standard for all programming languages. The YAML acronym is recursive; it stands for “YAML Ain’t a Markup Language.”

Zone

In Bastille Enterprise, you can use zones to create specific geofences within a site under observation.

13.0 References and Additional Resources

- *Bastille Enterprise Admin Console Guide*
- *Bastille Enterprise API Getting Started Guide*
- *Bastille Enterprise Concepts and Architecture Overview*
- *Bastille Enterprise Installation Requirements Guide*
- *Bastille Enterprise Splunk Integration Guide*
- *Bastille Enterprise Fusion Center Security Target*