Cb Enterprise Response

# How to Customize the Web UI Connection

CARBON BLACK
ARM YOUR ENDPOINTS
The Most Complete Endpoint Security Platform

Cb Enterprise Response

# How to Customize the Web UI Connection

## Table of Contents

Cb Enterprise Response

# How to Customize the Web UI Connection

## Overview

Carbon Black (Cb) Enterprise Response utilizes a browser-based User Interface (UI) referred to as the Cb Enterprise Response Web UI or console. The Web UI is a web server that also supports and facilitates the RESTful API connections. This server allows for the connection to be customized to be able to distinctly configure the interface to utilize a unique port and/or certificate. By default, the Web UI shares the same port and server SSL certificate utilized by the sensors. In many instances, it is preferred that the Web UI utilize its own port and/or certificate to uniquely control its interaction with the end user. Whether it is control access or to utilize an internal or third party SSL certificate. This document will describe the necessary steps and configuration changes required to properly implement a unique port and/or certificate for the Web UI and API connections.

### Important Note:

These steps should be performed on the **master** only.

## Changing the Web UI Port

### Prerequisites

- An initialized Cb Enterprise Response server
- An available HTTP port number
  - See Appendix A for details
  - Port 8443 will be used for this example

### Modify the Cb NGINX configuration file.

1. Rename the default configuration file.

```
# mv /etc/cb/nginx/conf.d/cb.conf
/etc/cb/nginx/conf.d/cb.conf.default
```

2. Copy and rename multi-home template configuration file.

```
# cp /etc/cb/nginx/conf.d/cb.multihome.conf.example
/etc/cb/nginx/conf.d/cb.conf
```

3. Modify multi-home configuration file.

```
# vi /etc/cb/nginx/conf.d/cb.conf
```

   a. Disable at least one of the port 80 listener configuration.

   b. If a “listen” line referencing port 80 exists, remove or comment it out.
   **Note:** Comments are indicated by a leading ‘#’

   **From**

```
listen [::]:80 ipv6only=off;
```

   **To**

```
# listen [::]:80 ipv6only=off;
```

## Modify the Cb NGINX configuration file, continued.

c. Modify Web UI server configuration sectionk.

i. Identify the proper server section by the following comment:

```
Server
{
     # This server configuration is used for CB
Enterprise Server’s Web UI
```

ii. Within that server configuration section modify the listening port.

**From**

```
# listen [::]:80 ipv6only=off;
listen [::]:443 ssl ipv6only=off;
```

**To**

```
# listen [::]:80 ipv6only=off;
listen [::]:8443 ssl ipv6only=off;
```

d. Write changes and exit.

## Update iptables configuration.

1. Edit iptables.

```
# vi /etc/sysconfig/iptables
```

a. Add the following entry before the first “-AINPUT – j REJECT” lines:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport
8443 –j ACCEPT
```

b. Write changes and exit.

2. Load new iptables configuration.

```
# service iptables reload
```

## Update main Cb configuration file (cb.conf)

1. Edit cb.conf

```
# vi /etc/cb/cb.conf
```

2. Update the Web UI/API endpoint setting.

**From**

```
# TCP port on which Web UI/API HTTP endpoint is listening
on
NginxWebApiHttpPort=443
```

**To**

```
# TCP port on which Web UI/API HTTP endpoint is listening
on
NginxWebApiHttpPort=8443
```

   a. Write the changes and exit.

## Redirect port 80 to 8443 (optional)

**Note:** Only perform this step if port 80 is open and redirection to HTTPS **is desired**.

1. Backup the http.conf file before making changes.

```
cp /etc/cb/nginx/conf.d/http.conf
/etc/cb/nginx/conf.d/http.conf.default
```

2. Edit this line in the /etc/cb/nginx/conf.d/http.conf configuration file to redirect port 80 to port 8443 (HTTPS):

**From**

```
return          301 https://$host$request_uri;
```

**To**

```
return          301 https://$host:8443$request_uri;
```

## Load new port configuration.

1. For a standalone server restart cb-enterprise

```
# service cb-enterprise stop
# service cb-enterprise start
```

**Or:**

For a cluster environment, restart cluster

```
# /usr/share/cb/cbcluster stop
# /usr/share/cb/cbcluster start
```

## Verify configuration.

1. Web browse to the Web UI with the new port: https://cberserver.myco.com:8443

## Changing the SSL Server Certificate

### Prerequisites

- An initialized Cb Enterprise Response server
- An available HTTP port number
  - See Appendix A for details
  - Port 8443 will be used for this example
- A new SSL Server certificate and private key
  - Openssl compatible X.509 certificate and RSA key
  - Certificate mycert.crt and mycert.key uploaded to /root directory will be used for this example.

## Store new SSL Server certificate and private key files.

1. Upload files and move to Cb certificate directory.

```
# mv /root/mycert.* /etc/cb/certs/
```

## Change the Web UI Port.

1. Follow procedures identified above.

## Modify Web UI server configuration section.

```
# vi /etc/cb/nginx/conf.d/cb.conf
```

1. Identify the proper server section by the following comment:

```
server
{
     # This server configuration is used for CB Enterprise
Server’s Web UI
```

2. Within that server configuration section, remove the use of the default certificate and key.

   a. Comment out the following lines:

**From**

```
     include
/var/cb/nginx/props/nginx.runtime.ssl_certificate.prop
;
     include
/var/cb/nginx/props/nginx.runtime.ssl_certificate_key.
prop;
```

**To**

```
#    include
/var/cb/nginx/props/nginx.runtime.ssl_certificate.prop
;
#    include
/var/cb/nginx/props/nginx.runtime.ssl_certificate_key.
prop;
```

Cb Enterprise Response

# How to Customize the Web UI Connection

## Store new SSL Server certificate and private key files, continued.

3. Add the new certificate configuration.
   a. Directly below the commented lines, add the following lines with the same indention:

```
ssl_certificate /etc/cb/certs/mycert.crt;
ssl_certificate_key /etc/cb/certs/cert.key;
```

4. Write changes and exit.

## Load new certificate configuration.

1. For a standalone server, restart cb-enterprise.

```
# service cbenterprise stop
# service cbenterprise start
```

**Or:**

For a cluster environment, restart cluster.

```
# /usr/share/cb/cbcluster stop
# /usr/share/cb/cbcluster start
```

## Verify configuration.

1. Web browse to the Web UI with the new port: https://cberserver.myco.com:8443
2. Verify new certificate is presented.
   a. Select the 🔒 next to the URL of the web browser.
   b. Select the **Connection** tab.
   c. Select **Certificate information**.
   d. Verify certificate information.

## Appendix A

### Allowed HTTP Ports

In order for a certain port to be configurable for the CB Enterprise Web UI and API, the port must meet two criteria:

- The port is not currently utilized.
- SELinux will allow the port to bind with HTTP protocol.

If the port is currently utilized by another process, the operating system will not allow the listener to be created. To verify, run the **netstat** command with CB Enterprise Response running to verify the ports currently being utilized.

If SELinux is in enforcing mode, it will only allow certain ports to bind with certain services/protocols. To verify the current allowed ports, run the following command:

```
# semanage port –l | grep http_port_t
Http_port_t       tcp 4433, 80, 81, 443, 488, 8008, 8009,
8443, 9000
```

If the desired port is not listed, you must add that port to the allowed ports. However, first you must make sure that port is not reserved by another SELinux enforced protocol. To verify, run the following command:

**Note:** In this example, port 4433 will be used.

```
# semanage port –l | grep 4433
```

If it is not already used/defined, you can add the port to the allowed ports by running the following command:

```
# semanage port –a –t http_port_t –p tcp 4433
```

SELinux will now allow that port to bind with HTTP.