Zscaler and Carbon Black Deployment Guide

August 2020

Version 1.0
# Table of Contents

1 **Zscaler Integrations with Carbon Black** ......................................................... 7  
   1.1 Use Case I: Zscaler Sandbox Patient Zero .............................................................. 8  
   1.2 Use Case II: Zscaler Sandbox Connector ................................................................. 9  
   1.3 Use Case III: ZPA Posture Check ......................................................................... 10  

2 **Use Case I: Configure CB Enterprise EDR (CB Threat Hunter)** .............. 11  
   2.1 Configuring Carbon Black for ZIA - Overview ....................................................... 11  
   2.2 Logging into Carbon Black ..................................................................................... 12  
   2.3 Navigate to API Access .......................................................................................... 13  
   2.4 Carbon Black Org Key and Org ID ........................................................................ 14  
   2.5 Navigate to Access Levels ..................................................................................... 15  
   2.6 Add New API Access Level ................................................................................... 16  
   2.7 Create API Access level ........................................................................................ 17  
   2.8 Add API Key .......................................................................................................... 18  
   2.9 Create API Key tied to Access Level from previous step ....................................... 19  
   2.10 Note the API Credentials ................................................................................... 20  

3 **Use Case I: Configure CB Endpoint Standard (CB Defense)** ................ 21  
   3.1 Configuring Carbon Black for ZIA - Overview ....................................................... 21  
   3.2 Logging into Carbon Black ..................................................................................... 22  
   3.3 Navigate to API Access .......................................................................................... 23  
   3.4 Carbon Black Org Key and Org ID ........................................................................ 24  
   3.5 Navigate to Access Levels ..................................................................................... 25  
   3.6 Add New API Access Level ................................................................................... 26  
   3.7 Create API Access level ........................................................................................ 27  
   3.8 Add API Key .......................................................................................................... 28  
   3.9 Create API Key tied to Access Level from previous step ....................................... 29  
   3.10 Note the API Credentials ................................................................................... 30  
   3.11 Add API Key .......................................................................................................... 31  
   3.12 Create API Key tied to Access Level type - “API” .................................................. 32  
   3.13 Note the API Credentials ................................................................................... 33  

4 **Use Case I: Configuring Zscaler Internet Access (ZIA)** ............................ 34  
   4.1 Configuring Zscaler Internet Access for Carbon Black ........................................ 34  
   4.2 Logging into Zscaler (ZIA) Admin Portal ............................................................... 34  
   4.3 Configure Partner Integration ................................................................................ 35  
      4.3.1 If integrating with Enterprise EDR (Threat Hunter) only ..................................... 35  
      4.3.2 If integrating with Endpoint Standard (CB Defense) only .................................. 37  
      4.3.3 If integrating with both, Endpoint Standard and Enterprise EDR (TH & Defense) .... 39  
   4.4 Activate Pending ZIA Configuration .................................................................... 41
5 Use Case I: Viewing Carbon Black Endpoint Hits................................................. 42

5.1 Navigate to Web Insights......................................................................................... 42
5.2 Select Logs.................................................................................................................. 43
5.3 Filter on Sandbox related logs.................................................................................. 44
5.4 Confirm whether sandbox was involved ................................................................. 45
5.5 Access Zscaler Sandbox Report .............................................................................. 46
5.6 Zscaler Sandbox Report............................................................................................ 47
5.7 Access Carbon Black Endpoint Hits Report ............................................................ 48
5.8 Network Contain an Endpoint ................................................................................ 49
5.9 Confirm endpoint quarantine status.......................................................................... 50

6 Use Case II: Zscaler Sandbox Connector for Carbon Black Cloud..................... 51

6.1 Overview....................................................................................................................... 51
6.2 Requirements ................................................................................................................ 51
6.3 License.......................................................................................................................... 51
6.4 Support........................................................................................................................ 52
6.5 Installation....................................................................................................................... 52
6.6 Configuration ................................................................................................................ 53
  6.6.1 Carbon Black Configuration....................................................................................... 53
  6.6.2 Zscaler Configuration ............................................................................................... 55
6.7 Running the Script ....................................................................................................... 57
  6.7.1 Examples .................................................................................................................. 57

7 Use Case III: ZPA Posture Check ............................................................................. 58

7.1 Use Case III: Overview.............................................................................................. 58

8 Appendix A: Requesting Zscaler Support................................................................. 59

  8.1 Gather Support Information......................................................................................... 59
    8.1.1 Save Company ID................................................................................................. 60
    8.1.2 Enter Support Section........................................................................................... 61

9 Appendix B: Zscaler Resources................................................................................. 62

10 Appendix C: Carbon Black Resources ................................................................. 63
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Central Authority (Zscaler)</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection <em>(RFC 3706)</em></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation <em>(RFC 2890)</em></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange <em>(RFC 2409)</em></td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security <em>(RFC 2411)</em></td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Share Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer <em>(RFC 6101)</em></td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For <em>(RFC 7239)</em></td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
About This Document

Zscaler Overview

Zscaler (Nasdaq: ZS), enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, please visit www.zscaler.com or follow them on Twitter @zscaler.

Carbon Black Overview

VMware Carbon Black (Nasdaq: VMW) is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The VMware Carbon Black Cloud consolidates endpoint protection and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, VMware Carbon Black has key insights into attacker’s behaviors, enabling customers to detect, respond to and stop emerging attacks.

With Carbon Black, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native platform.
Audience

This guide is written for network administrators, endpoint / IT administrators, and security analysts responsible for deploying, monitoring and managing enterprise security systems. For additional product and company resources, please refer to the Appendix section.

Software Revisions

This document was authored using Zscaler Internet Access and Carbon Black Agent version 3.5.0.1756 on Windows 7 and Windows 10.

Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at partner-doc-support@zscaler.com.
1 Zscaler Integrations with Carbon Black

**Zscaler Internet Access (ZIA)** is a Secure internet and Web Gateway delivered from the cloud. Offered as a service from the world’s largest security cloud, ZIA provides a fully integrated security stack including SSL inspection, web gateway, firewall, bandwidth control, DLP and more. Its single-scan, multi-action architecture enables highly performant security protection to companies large and small over 185 countries worldwide.

**Zscaler Private Access (ZPA)** is a cloud service that uses a distributed architecture to provide fast and secure access to private applications running on-prem or in the public cloud.

**Carbon Black Security products** set the new standard with cloud-native security platform that delivering endpoint breach prevention solution that unifies NGAV, EDR, managed threat hunting and threat intelligence automation in a single cloud-delivered agent.

The integration of the two platforms unites the two market leaders and provides end-to-end visibility and protection from endpoint to applications in the cloud. The resulting integrated solution can enable cross-platform workflows that reduce dwell time and mean-time-to-remediate (MTTR).
1.1 Use Case I: Zscaler Sandbox Patient Zero

- ZIA detects zero-day malicious file via Zscaler Cloud Sandbox and produces an Insight Log about the file hash along with the relevant Carbon Black endpoint telemetry data in the same report. The endpoint data is retrieved dynamically via an API session established by a one-time setup process at the Zscaler console.
- The same report also includes a contain/quarantine action button, which enables administrator to trigger a network contain/quarantine request to Carbon Black platform. A network contained/quarantined host can only talk to Carbon Black backend IPs and IPs explicitly whitelisted by the Carbon Black admin. All other network access is cut off.

See below for a conceptual diagram of the integration

![Figure 1: Zscaler Sandbox Patient Zero - High Level Overview](image)
1.2 Use Case II: Zscaler Sandbox Connector

- While Zscaler can scan all files before they reach the endpoint if they come through the network, what happens when a file comes in via another method? Also, how do we find more information about files that landed on the end host prior to CB sensor installation?

- The connector will scan for any CBC Enterprise Standard (formerly CB Defense) events or CBC Enterprise EDR (formerly CB Threat Hunter) processes. After pulling the processes, it checks all of the unique hashes against a database of files that have been checked in the past. If the file is not known, a request to Zscaler’s ZIA Sandbox is made to see if they have any information on it. If they do, or if the file is known bad from the local database, action is taken.

See below for a conceptual diagram of the integration

![Zscaler connector – share threat intel](https://github.com/carbonblack/cbc-zscaler-sandbox-connector)

Figure 2: Zscaler Sandbox Connector - High Level Overview
1.3 **Use Case III: ZPA Posture Check**

- The device posture profile is a set of criteria that a user’s device must meet in order to access applications with ZPA. You can select a device posture profile when configuring access policies in the ZPA Admin Portal. However, you must configure these device posture profiles in the Zscaler Client Connector Portal.

- ZPA can be configured to make Zscaler App (client connector) check and confirm for the presence of running Carbon Black agent and allow access to sensitive applications only if this posture check passes.

See below for a conceptual diagram of the integration.

![Figure 3: ZPA Posture Check - High Level Overview](image)
2 Use Case I: Configure CB Enterprise EDR (CB Threat Hunter)

2.1 Configuring Carbon Black for ZIA - Overview

Zscaler ZIA sandbox integrates with two Carbon Black endpoint protections products - Enterprise EDR (formerly known as Threat Hunter) and Endpoint Standard (formerly known as CB Defense)

- If you license to CB Threat Hunter only, follow setup instructions in this section
- If you license to CB Defense only, skip this section and follow setup instructions in the next section (section 3)
- If you license to both CB products, follow setup instructions in both the sections

To establish the API connection between Carbon Black and Zscaler, an API client and key need to be first generated from the Carbon Black console and then input into the Zscaler Admin portal along with a few other Carbon Black tenant specific details.

Zscaler needs Carbon Black Cloud Service hostname, API ID/Secret Key and Org ID/key to establish the API connection.

The following steps assume that Carbon Black platform as well as Carbon Black sensors have been deployed and properly configured. If this has not been done, please refer to Carbon Black documentation to deploy and configure Carbon Black components first.

2.2 Logging into Carbon Black

Log into Carbon Black using your administrator account. If you are unable to log in using your administrator account, please contact Carbon Black support (Appendix C).

Figure 4: Log into Carbon Black portal
2.3 **Navigate to API Access**

After logging into Carbon Black portal, navigate to **API Access** option as shown below.

![Figure 5: Navigate to API Access](image)

Figure 5: Navigate to API Access
2.4 **Carbon Black Org Key and Org ID**

Note down your **Org Key** and **Org ID**. We will need to paste this later in Zscaler UI.

![Image of Carbon Black Org Key/ID](image)

*Figure 6: Note down Carbon Black Org Key/ID*
2.5 **Navigate to Access Levels**

Navigate to **Access Levels**

![Image of Zscaler & Carbon Black Deployment Guide](image)

**Figure 7: Navigate to Access Level**
2.6 Add New API Access Level

We will create a new API Access level i.e. API Scope with specific permissions required for our Zscaler Sandbox integration use case. This is a part of one-time setup. Click Add Access Level as shown below.

![Add Access Level](image)

Figure 8: Add Access Level
2.7 Create API Access level

Create an API Access Level (scope) with following permissions:

- Execute only for Device Quarantine
- Create and Read for Threat Hunter events
- Read only for Device General information

Once completed, click **Save**.

![Figure 9: Create & Save custom API Access Level](image)

Figure 9: Create & Save custom API Access Level
2.8 Add API Key

Now we will create the actual API ID/Secret key and associate it with the newly created Access Level. Navigate back to API Keys section and click on Add API Key

Figure 10: Add API Key
2.9 **Create API Key tied to Access Level from previous step**

Select **Custom** from the **Access Level type** drop down and then in **Custom Access Level** dropdown, select the access level created in previous step. After naming the key, click **Save**.

![Create API credentials](image)

*Figure 11: Create API credentials*
2.10 Note the API Credentials

Take a note of your API ID and API Secret key. We will need to paste them in ZIA UI

![Figure 12: Note down API credentials](image-url)
3 Use Case I: Configure CB Endpoint Standard (CB Defense)

3.1 Configuring Carbon Black for ZIA - Overview

Zscaler ZIA sandbox integrates with two Carbon Black endpoint protections products - **Endpoint Standard** (formerly known as **CB Defense**) and **Enterprise EDR** (formerly known as **Threat Hunter**)

- **If you license to CB Defense only, follow setup instructions in this section**
- **If you license to CB Threat Hunter only, skip this section and follow setup instructions in the previous section (section 2)**
- **If you license to both CB products, follow setup instructions in both sections**

To establish the API connection between Carbon Black and Zscaler, two separate API clients and keys need to be first generated from the Carbon Black console and then input into the Zscaler Admin portal along with a few other Carbon Black tenant specific details.

Zscaler needs **Carbon Black Cloud Service hostname**, **2 separate API IDs/Secret Keys** and **Org ID/key** to establish the API connection.

The following steps assume that Carbon Black platform as well as Carbon Black sensors have been deployed and properly configured. If this has not been done, please refer to Carbon Black documentation to deploy and configure Carbon Black components first.

3.2 **Logging into Carbon Black**

Log into Carbon Black using your administrator account. If you are unable to log in using your administrator account, please contact Carbon Black support (Appendix C).

![Figure 13: Log into Carbon Black portal](image)

Figure 13: Log into Carbon Black portal
3.3 **Navigate to API Access**

After logging into Carbon Black portal, navigate to **API Access** option as shown below.

![Figure 14: Navigate to API Access](image)

Copyright ©, Zscaler, Inc.  Page 23 of 63
3.4  **Carbon Black Org Key and Org ID**

Note down your **Org Key** and **Org ID**. We will need to paste this later in Zscaler UI.

![Figure 15: Note down Carbon Black Org Key/ID](image)
3.5 **Navigate to Access Levels**

Navigate to **Access Levels**. CB Defense integration requires **2 different** API keys (in addition to Org key/ID) that are tied to **2 different Access Levels**.

![Figure 16: Navigate to Access Level](image-url)
3.6 **Add New API Access Level**

We will create a new API Access level i.e. API Scope with specific permissions required for our Zscaler Sandbox integration use case. This will be used to create 1st set of API credentials required for integration with ZIA sandbox. This is a part of one-time setup. Click **Add Access Level** as shown below.

![Add Access Level](image)

**Figure 17: Add Access Level**
3.7 **Create API Access level**

Create an API Access Level (scope) with following permissions:

- Execute only for Device Quarantine
- Read only for Org alerts
- Read only for Device General information

Once completed, click **Save**.

![Figure 18: Create & Save custom API Access Level](image)
3.8 Add API Key

Now we will create the actual API ID/Secret key and associate it with the newly created Access Level. Navigate back to API Keys section and click on **Add API Key**.

![Figure 19: Add API Key](image-url)
3.9 Create API Key tied to Access Level from previous step

Select **Custom** from the **Access Level type** drop down and then in **Custom Access Level** dropdown, select the access level created in previous step. After naming the key, click **Save**.

![Figure 20: Create API credentials tied to Custom Access Level for CB Defense](image)

---

Copyright ©, Zscaler, Inc.  
Page 29 of 63
3.10 Note the API Credentials

Take a note of your API ID and API Secret key. We will need to paste them in ZIA UI.

![API Credentials](image)

Figure 21: Note down 1st set of API credentials
### 3.11 Add API Key

Now we'll create one more set of API keys. We don't need to create any custom Access Level. Navigate back to API Keys section & click **Add API Key**

![Add API Key](image)

**Figure 22: Add API Key**
3.12 Create API Key tied to Access Level type - “API”

Select API from the Access Level type drop down. After naming the key, click Save.

Figure 23: Create API credentials tied to built-in “API” Access Level for CB Defense
3.13 Note the API Credentials

Take a note of your API ID and API Secret key. We will need to paste them in ZIA UI. This is the 2nd pair of credentials required for integrating Zscaler Sandbox with CB Defense.

![API Credentials](image)

Figure 24: Note down 2nd set of API credentials.
4 Use Case I: Configuring Zscaler Internet Access (ZIA)

4.1 Configuring Zscaler Internet Access for Carbon Black

Endpoint telemetry data from Carbon Black Platform is passed onto Zscaler console via an API integration. Correlating the endpoint data enables Zscaler console to display the Sandbox report along with information about the originating endpoint device and other infected endpoints in the environment, including Carbon Black Agent ID, Host Name, the time when the malicious file appeared on the endpoint (perhaps infection via a different attack surface, such as via a USB thumb drive). This automatic correlation of malware detection with an endpoint device reduce time and effort needed for investigation and remediation. In this section, we will configure the Zscaler Admin Portal with the credentials gathered in the previous section.

4.2 Logging into Zscaler (ZIA) Admin Portal

Log into Zscaler Internet Access (ZIA) portal using your administrator account, as show in Figure 11. If you are unable to log in using your administrator account, please contact support:


Figure 25: Log into Zscaler Admin portal
4.3 Configure Partner Integration

4.3.1 If integrating with Enterprise EDR (Threat Hunter) only

After logging in, you will arrive at the main landing page of the admin portal. From here navigate to: Administration -> Partner Integration -> Carbon Black. Select Threat Hunter tab. Paste your Threat Hunter API ID/Secret key and Org ID/key here. Cloud Service Hostname depends on the location of your Carbon Black tenant. Please refer to link below for identifying the Hostname pertinent to your CB environment (Appendix C). Click Save.

![Configure Partner Integration (Threat Hunter)](image_url)

Figure 26: Configure Partner Integration (Threat Hunter)
Clicking Save will trigger an API call to Carbon Black to verify the credentials. If you see the green message “Valid API token(s)”, then you have successfully configured the API connection for the ZIA sandbox and Threat Hunter integration to work.

Figure 27: Verify Partner Integration
4.3.2 If integrating with Endpoint Standard (CB Defense) only

After logging in, you will arrive at the main landing page of the admin portal. From here navigate to: Administration -> Partner Integration -> Carbon Black. Select CB Defense tab. Paste both of your CB Defense API IDs/Secret keys and Org ID/key to corresponding sections. Cloud Service Hostname depends on the location of your Carbon Black tenant. Please refer to link below for identifying the Hostname pertinent to your CB environment (Appendix C). Click Save.

Figure 28: Configure Partner Integration (CB Defense)
Clicking Save will trigger an API call to Carbon Black to verify the credentials. If you see the green message “Valid API token(s)”, then you have successfully configured the API connection for the ZIA sandbox and Threat Hunter integration to work.

Figure 29: Verify Partner Integration
4.3.3 If integrating with both, Endpoint Standard and Enterpriser EDR (TH & Defense)

After logging in, you will arrive at the main landing page of the admin portal. From here navigate to: **Administration -> Partner Integration -> Carbon Black**.

Select **CB Defense and Threat Hunter** tab
Paste Threat Hunter **API ID/Key**, both of your CB Defense **API IDs/Secret keys** and **Org ID/key** to corresponding sections.

**Cloud Service Hostname** depends on the location of your Carbon Black tenant. Please refer to link below for identifying the Hostname pertinent to your CB environment (Appendix C)

Click Save.

![Configure Partner Integration (CB Defense & Threat Hunter)](image-url)

Figure 30: Configure Partner Integration (CB Defense & Threat Hunter)
Clicking Save will trigger an API call to Carbon Black to verify the credentials. If you see the green message “Valid API token(s)”, then you have successfully configured the API connection for the ZIA sandbox and Threat Hunter integration to work.

Figure 31: Verify Partner Integration
4.4 **Activate Pending ZIA Configuration**

Anytime you make a change in ZIA, you will see a number over the Activation icon on the left-hand side menu. This lets you know that you have changes pending in queue for activation.

When you are ready to commit all changes in queue, Hover mouse over the Activation menu and click the blue **Activate** button.

![Figure 32: Activate Pending ZIA Configuration](image-url)
5 Use Case I: Viewing Carbon Black Endpoint Hits

Thanks to this integration, you should be able to expect that malware detected by Zscaler Cloud Sandbox will be automatically correlated with Carbon Black endpoint device information, as shown below, all within the Zscaler admin portal.

5.1 Navigate to Web Insights

In Zscaler Admin Portal, Select Analytics tab, and then Web Insights.

![Navigate to Web Insights](image)

Figure 33: Navigate to Web Insights
5.2 **Select Logs**

Next, click on the **Logs** tab and **Add Filter**
In the Add Filter dropdown box, enter “**Threat Class**”
5.3 Filter on Sandbox related logs

Select Sandbox as the Threat Class and click on Apply Filters

Figure 35: Select Sandbox filter
5.4 Confirm whether sandbox was involved

Once you click Apply Filters, if the file in question was detonated by Zscaler sandbox or is currently being detonated by Zscaler sandbox - you'll see corresponding log entries on right.

![Figure 36: Confirm whether file was sent to sandbox](image-url)
5.5 Access Zscaler Sandbox Report

On the right-hand panel, a list of sandbox detonation logs is displayed. Click on a particular MD5 hash to bring up the dropdown option menu and select View Sandbox Detail Report.

If **Sandbox has not yet finished analyzing** the file, then, you’ll see a message indicating that the Zscaler sandbox detonation is still in progress and you would need to wait for it to complete.

If **Sandbox has finished analyzing** the file, you’ll see the detailed Zscaler sandbox report.

![Figure 37: Access Zscaler Sandbox report](image-url)
5.6 Zscaler Sandbox Report

Once the file detonation is finished, sandbox report provides detailed information regarding activities attempted by the file within isolated sandboxed environment.

![Zscaler Sandbox Report](image)

Figure 38: Zscaler Sandbox Report
### 5.7 Access Carbon Black Endpoint Hits Report

Once sandbox detonation is finished, click on **View Carbon Black Endpoint Hits Report** (from step 4.5) to see Carbon Black endpoint hits.

**Figure 39: Carbon Black Endpoint Hits Report**

<table>
<thead>
<tr>
<th>Carbon Black Agent ID</th>
<th>Hostname</th>
<th>Internal IP</th>
<th>OS Version</th>
<th>Last Seen</th>
<th>Detected By</th>
<th>File Status</th>
<th>Endpoint Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10090087</td>
<td>DedicatedEHST1</td>
<td>10.2.10.7</td>
<td>Windows 10 x64</td>
<td>07/10/2020, 01:37 PM</td>
<td>CB Threat Hunter</td>
<td>Detected</td>
<td>Active</td>
</tr>
<tr>
<td>2349463</td>
<td>DedicatedEHST3</td>
<td>10.2.10.10</td>
<td>Windows 10 x64</td>
<td>07/10/2020, 09:46 PM</td>
<td>CB Threat Hunter</td>
<td>Detected</td>
<td>Active</td>
</tr>
<tr>
<td>2349525</td>
<td>DedicatedEHST4</td>
<td>10.2.10.11</td>
<td>Windows 10 x64</td>
<td>07/10/2020, 09:47 PM</td>
<td>CB Threat Hunter</td>
<td>Detected</td>
<td>Active</td>
</tr>
</tbody>
</table>
5.8 **Network Contain an Endpoint**

Clicking **Contain** button triggers an API call to Carbon Black. This cuts off that endpoint’s network access.

![Carbon Black Endpoint Hits](image)

![File Detected on 3 Endpoints (Carbon Black)](image)

Figure 40: Contain an Endpoint
5.9 **Confirm endpoint quarantine status**

After clicking the Contain option, the containment status will be reflected within the Endpoint hits report. A host being contained or quarantined imply the same - Network access of the host being cut off to all destinations except the ones required to contact Carbon Black cloud.

![Image](image_url)

**Figure 41: Confirm Containment/Quarantine Status**
6 Use Case II: Zscaler Sandbox Connector for Carbon Black Cloud

6.1 Overview

This is an integration between Zscaler's ZIA Sandbox and VMware Carbon Black Cloud (CBC) Endpoint Standard (formerly CB Defense) and CBC Enterprise EDR (formerly CB Threat Hunter). While Zscaler can scan all files before they reach the endpoint if they come through the network, what happens when a file comes in via another method, or prior to sensor installation?

The connector will scan for any CBC Enterprise Standard events or CBC Enterprise EDR processes. After pulling the processes it checks all of the unique hashes against a database of files that have been checked in the past. If the file is not known, a request to Zscaler's ZIA Sandbox is made to see if they have any information on it. If they do, or if the file is known bad from the local database, action is taken.

Action options consist of:

- Adding to a CBC Enterprise EDR Watchlist Feed
- Passing the event and sandbox report to a webhook
- Running a script
- Isolating the endpoint
- Moving the endpoint into a policy

6.2 Requirements

- Python 3.x with sqlite3
- VMware Carbon Black Cloud Endpoint Standard or Enterprise EDR
- Zscaler ZIA with licensed Sandbox

6.3 License

Use of the Carbon Black API is governed by the license found in LICENSE.
6.4 Support

1. View all API and integration offerings on the Developer Network along with reference documentation, video tutorials, and how-to guides.
2. Use the Developer Community Forum to discuss issues and get answers from other API developers in the Carbon Black Community.

6.5 Installation

Clone the repository into a local folder.

```bash
git clone git@github.com:carbonblack/cbc-zscaler-sandbox-connector.git
```

Install the requirements

```bash
pip install -r requirements.txt
```

Edit the config.conf file and update with your configurations
6.6  **Configuration**

All of the configurable settings for the integration can be found in `config.conf`.

### 6.6.1  Carbon Black Configuration

You will need to create 1 API Access Level and 3 API keys

### 6.6.1.1  Custom Access Level Permissions

<table>
<thead>
<tr>
<th>Category</th>
<th>Permission Name</th>
<th>.Notation Name</th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Detections</td>
<td>Feeds</td>
<td>org.feeds</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>General Information</td>
<td>device</td>
<td></td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Policy assignment</td>
<td>device.policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td>Events</td>
<td>org.search.events.</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Binary Store</td>
<td>SHA-256</td>
<td>ubs.org.sha256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>☑</td>
</tr>
</tbody>
</table>
### 6.6.1.2 **Access Levels (API key type)**

1. API
2. Custom [Select your Custom Access Level]
3. Live Response (optional, used in action.py)

The Organization Key can be found in the upper-left of the **Settings > API Keys** page.

<table>
<thead>
<tr>
<th><strong>CarbonBlack</strong></th>
<th><strong>Configure Carbon Black Cloud</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>URL of CBC instance</td>
</tr>
<tr>
<td>org_key</td>
<td>Org Key</td>
</tr>
<tr>
<td>api_id</td>
<td>API ID</td>
</tr>
<tr>
<td>api_key</td>
<td>API Secret Key</td>
</tr>
<tr>
<td>custom_api_id</td>
<td>Custom API ID</td>
</tr>
<tr>
<td>custom_api_key</td>
<td>Custom API Secret Key</td>
</tr>
<tr>
<td>lr_api_id</td>
<td>LiveResponse API ID</td>
</tr>
<tr>
<td>lr_api_key</td>
<td>LiveResponse API Secret Key</td>
</tr>
<tr>
<td>cbd_enabled</td>
<td>Enable CBC Endpoint Standard? [true/false]</td>
</tr>
<tr>
<td>cbth_enabled</td>
<td>Enable CBC Enterprise EDR? [true/false]</td>
</tr>
<tr>
<td>cbd_timespan</td>
<td>How far back to pull CB Defense events? [3h, 1d, 1w, 2w,1m, all]</td>
</tr>
<tr>
<td>reputation_filter</td>
<td>Filter CB ThreatHunter processes by reputation. Default is NOT_LISTED</td>
</tr>
</tbody>
</table>
6.6.2 Zscaler Configuration

The API key can be found in Administration > API Key Management

<table>
<thead>
<tr>
<th>Zscaler</th>
<th>Configure Zscaler ZIA Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>URL for Zscaler ZIA</td>
</tr>
<tr>
<td>api_key</td>
<td>API Key</td>
</tr>
<tr>
<td>username</td>
<td>Login Username</td>
</tr>
<tr>
<td>password</td>
<td>Login Password</td>
</tr>
<tr>
<td>bad_types</td>
<td>Bad Types in Sandbox Reports. [MALICIOUS, SUSPICIOUS, BENIGN]</td>
</tr>
</tbody>
</table>

Python 3.x ships by default with sqlite. If for some reason you don't have sqlite, you will need to install it (pip install sqlite3)

<table>
<thead>
<tr>
<th>sqlite3</th>
<th>Configure sqlite3</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Filename of the sqlite3 database</td>
</tr>
</tbody>
</table>

When a file is detected to match the types defined in the Zscaler > bad_types configuration, actions are triggered. By default, all actions are disabled.
6.6.2.1 **watchlist**

When this field is populated, a Threat Feed is either created or updated with a Report of the detected file. The Report contains a short description, some tags and the severity from the Zscaler Sandbox report. Indicators are not duplicated if they already exist.

6.6.2.2 **webhook**

When this field is populated, a POST request is made to the http endpoint provided in the value of the configuration. The body of the POST request is an array of the Carbon Black event/process and the Zscaler report ([cb_event, zs_report]). Duplication may occur on this action.

6.6.2.3 **script**

When this field is populated, a script is executed at the path and with the parameters provided in the value of the configuration. There are 3 find/replace that occur {{device_id}, {command}, {argument}}. An example is provided in the config.conf. This will execute the provided example action.py which will kill the triggered process.

6.6.2.4 **isolate**

When this field is populated with true the device will be isolated.

6.6.2.5 **policy**

When this field is populated, the device will be moved to the policy named with the configuration value. This is not the policy ID.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Configure Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>watchlist</td>
<td>Name of watchlist to populate</td>
</tr>
<tr>
<td>webhook</td>
<td>URL to POST a JSON object of the event and sandbox report</td>
</tr>
<tr>
<td>script</td>
<td>A script to execute</td>
</tr>
<tr>
<td>isolate</td>
<td>Isolate the endpoint?</td>
</tr>
<tr>
<td>Policy</td>
<td>Policy to move offending devices</td>
</tr>
</tbody>
</table>
6.7 Running the Script

The script has the following CLI options:

```
optional arguments:
  -h, --help             show this help message and exit
  --last_pull LAST_PULL  Set the last pull time in ISO8601 format
  --cbd                  Pull CBD events
  --cbth                 Pull CBTH processes
```

The `--last_pull` option overwrites the last_pull value stored in the database and will pull Cloud EDR processes since that time. The `--cbd` and `--cbth` options will pull NGAV events and Cloud EDR processes respectively, even if they are disabled in the configuration file.

6.7.1 Examples

Typical usage:

```
python app.py
```

Specify Cloud EDR start date:

```
python app.py --last_pull 2020-01-01T12:34:56.000Z
```
7 Use Case III: ZPA Posture Check

The device posture profile is a set of criteria that a user's device must meet in order to access applications with ZPA. You can select a device posture profile when configuring access policies in the ZPA Admin Portal. However, you must configure device posture profiles in the Zscaler Client Connector Portal.

7.1 Use Case III: Overview

This is an integration between Zscaler Private Access (ZPA) platform and Carbon Black. Within ZPA, policies can be setup to control access to sensitive applications based on certain endpoint posture assessments.

In this case, Client Connector (Zapp) will check for the presence of running Carbon Black agent on the endpoint. This will constitute the posture check that can be tied to access policies. This posture check is supported for laptops/desktops running MacOS or Windows.

Detect Carbon Black

This is only applicable if you're using Zscaler Client Connector version 2.1.2 or later. If you choose Windows or macOS, select Detect Carbon Black. The user must have Carbon Black running on the device to pass the posture validation check.

Figure 42: Company ID
8 Appendix A: Requesting Zscaler Support

8.1 Gather Support Information

Zscaler support is sometimes required for the provisioning of certain services. Zscaler support is also available to help troubleshoot configuration and service issues. Zscaler support is available 24/7.

The navigation is: Administration -> Settings -> and then click Company profile

Figure 43: Collecting details to open support case with Zscaler TAC
8.1.1 Save Company ID

Copy the Company ID, as shown below.

Figure 44: Company ID
8.1.2 Enter Support Section

Now that we have our company ID, we are ready to open a support ticket. The navigation is: **Dashboard -> Support -> Submit a Ticket.**

![Figure 45: Submit ticket](image)
9  Appendix B: Zscaler Resources

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/
Appendix C: Carbon Black Resources

Carbon Black Threat Hunter API Documentation

Carbon Black Defense API Documentation

Carbon Black Support Portal
https://community.carbonblack.com

Identify Cloud Service Hostname:

Network Containment/Quarantine:

Carbon Black Blog
https://www.carbonblack.com/blog/

Carbon Black Zscaler Connector Page
https://github.com/carbonblack/cbc-zscaler-sandbox-connector

Carbon Black Github Page
https://github.com/carbonblack

Carbon Black Community page
https://community.carbonblack.com