# Table of Contents

1 Zscaler ZIA Integration with CrowdStrike .......................................................... 5

2 Configuring CrowdStrike ....................................................................................... 7
   2.1 Configuring CrowdStrike for ZIA Overview ...................................................... 7
   2.2 Logging into CrowdStrike .................................................................................. 8
   2.3 Access CrowdStrike Customer ID ...................................................................... 9
   2.4 Note down CrowdStrike Customer ID ............................................................... 10
   2.5 Navigate to API section ..................................................................................... 11
   2.6 Add New API Client ......................................................................................... 12
   2.7 Create API Client for ZIA ................................................................................ 13
   2.8 Make a note of API credentials ....................................................................... 14

3 Configuring Zscaler Internet Access (ZIA) ............................................................. 15
   3.1 Configuring Zscaler Internet Access for CrowdStrike ....................................... 15
   3.2 Logging into Zscaler (ZIA) Admin Portal ........................................................... 15
   3.3 Configure Partner Integration ......................................................................... 16
   3.4 Verify Partner Integration ................................................................................. 17
   3.5 Activate Pending ZIA Configuration ................................................................ 18

4 Viewing CrowdStrike Endpoint Hits ...................................................................... 19
   4.1 Navigate to Web Insights .................................................................................. 19
   4.2 Select Logs ....................................................................................................... 20
   4.3 Filter on Sandbox related logs ........................................................................ 21
   4.4 Confirm whether file was sent to sandbox ....................................................... 22
   4.5 Access Zscaler Sandbox Report ..................................................................... 23
   4.6 Zscaler Sandbox Report ................................................................................ 24
   4.7 Access CrowdStrike Endpoint Hits Report ....................................................... 25
   4.8 Network Contain an Endpoint ......................................................................... 26
   4.9 Confirm endpoint quarantine status ............................................................... 27

5 Appendix A: Requesting Zscaler Support ............................................................... 28
   5.1 Gather Support Information ............................................................................ 28
      5.1.1 Save Company ID .................................................................................... 29
      5.1.2 Enter Support Section .............................................................................. 30

6 Appendix B: Zscaler Resources .............................................................................. 31

7 Appendix C: CrowdStrike Resources ..................................................................... 32
# 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>RFC2890</em>)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (<em>RFC2409</em>)</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security (<em>RFC2411</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>RFC6101</em>)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (<em>RFC7239</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.

CrowdStrike Overview

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform’s single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world’s most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon 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 v6.0 and CrowdStrike Flacon Agent 5.27.10904 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 ZIA Integration with CrowdStrike

**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.

**CrowdStrike Falcon Endpoint Protection Enterprise Platform** sets the new standard with the first cloud-native security platform that delivers the only 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).
Primary Use Case:

- ZIA Cloud Sandbox detects zero-day malicious file via Zscaler Cloud Sandbox and produces an Insight Log about the file hash along with the relevant CrowdStrike 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 an administrator to trigger a network contain/quarantine request to CrowdStrike Falcon platform. A network contained/quarantined host can only talk to CrowdStrike backend IPs and IPs explicitly whitelisted by the CrowdStrike admin. All other network access is cut off.
- Alternatively, an administrator can click on the CrowdStrike Agent ID within the Insight Log. This will bring up the CrowdStrike console for that Agent ID to aid in further investigations and mitigation operations.

See below for a conceptual diagram of the integration

![Figure 1: High Level Overview](image-url)
# Configuring CrowdStrike

## Configuring CrowdStrike for ZIA Overview

To establish the API connection between CrowdStrike and Zscaler, an API client and key need to be first generated from the CrowdStrike console and then input into the Zscaler Admin portal.

Zscaler needs **CrowdStrike API Auth URL, Client ID, Secret** and **Customer ID** to establish the API connection. The latter three items are obtained from the CrowdStrike Console.

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

https://www.crowdstrike.com/resources/
2.2 Logging into CrowdStrike

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

Figure 2: Log into CrowdStrike
### 2.3 Access CrowdStrike Customer ID

After logging into CrowdStrike portal, access Customer ID by clicking on the icon shown below.

![Figure 3: Access CrowdStrike Customer ID](image-url)
2.4 **Note down CrowdStrike Customer ID**

This is your CrowdStrike Customer ID. We will need to paste this later in Zscaler UI.

![Figure 4: Note down CrowdStrike Customer ID](image-url)
2.5 **Navigate to API section**

After logging into CrowdStrike portal, navigate to **Support -> API Clients and Keys**.

![API Clients and Keys](image_url)

**Figure 5: Navigate to API section**
2.6 **Add New API Client**

We will create a new API client with specific permissions required for our use case. This is a one-time setup. Click **Add new API client** as shown below.

![Add New API Client](image)

**Figure 6: Add New API Client**
2.7 Create API Client for ZIA

Create an API client with following scopes:

- Read-Write permission for Hosts
- Read only permission for IOCs
- Read only permission for Detections

Once completed, click Save.

![Create & Save API Client](image-url)
2.8 Make a note of API credentials

Once the API Client is created, you will be shown Client ID and Secret. Please note down your Secret value before clicking Done. We will need to paste this later in Zscaler UI.

Once you click Done, there is no way to re-access this Secret. If you lose the Secret, CrowdStrike API credentials will need to be reset.

Figure 8: Note down API credentials
3 Configuring Zscaler Internet Access (ZIA)

3.1 Configuring Zscaler Internet Access for CrowdStrike

Endpoint telemetry data from CrowdStrike Falcon 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 CrowdStrike 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 ID and Key generated in the previous section.

3.2 Logging into Zscaler (ZIA) Admin Portal

Log into Zscaler Internet Access (ZIA) portal using your administrator account, as show in Figure 9. If you are unable to log in using your administrator account, please contact support: https://help.zscaler.com/submit-ticket.

![Zscaler Login](image)

Figure 9: Log into Zscaler Admin portal
3.3 **Configure Partner Integration**

After logging in, you will arrive at the main landing page of the admin portal. From here navigate to: **Administration -> Partner Integration**. The **API Auth URL** should be: [http://api.crowdstrike.com](http://api.crowdstrike.com). Next, paste your CrowdStrike API credentials and Customer ID here. Click Save.

![Configure Partner Integration](image)

*Figure 10: Configure Partner Integration*
3.4 Verify Partner Integration

We now need to verify the Partner Integration. Select Test and wait a few seconds. If you see the green message “Your token is valid”, then you have successfully configured the API connection for the ZIA integration to work!

![Partner Integrations](image)

Figure 11: Verify Partner Integration
3.5 **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. See Figure 12.

![Figure 12: Activate Pending ZIA Configuration](image)
4 Viewing CrowdStrike Endpoint Hits

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

4.1 Navigate to Web Insights

In Zscaler Admin Portal, Select Analytics tab, and then Web Insights. See Figure 13.

Figure 13: Navigate to Web Insights
4.2 Select Logs

Next, click on the **Logs** tab and **Add Filter**, as shown in *Figure 14*.

![Select Logs](image)

*Figure 14: Select Logs*

In the Add Filter dropdown box, enter “sandbox” to bring up the Sandbox filter category, Select **Sandbox** as shown in *Figure 15*. 
4.3 Filter on Sandbox related logs

In the Add Filter dropdown box, enter “sandbox” to bring up the Sandbox filter category, Select Sandbox.

Under the Sandbox Filter category, you will need to select the filter option. Click on None and select Sent for Analysis as a filter option. Once the check mark appears next to this Selected Item, click Done. See Figure 16. Next, Click on Apply Filters.
4.4  **Confirm whether file was sent to sandbox**

Under the Sandbox Filter category, you will need to select the filter option. Click on **None** and select **Sent for Analysis** as a filter option. Once the check mark appears next to this Selected Item, click **Done**. Next, Click on **Apply Filters**

![Image of sandbox filter setup]

*Figure 16: Confirm whether file was sent to sandbox*
4.5 **Access Zscaler Sandbox Report**

On the left panel, a list of sandbox detonation log is displayed. Select a particular MD5 hash of interest, right-click to bring up the dropdown option menu, and select **View CrowdStrike Endpoint Hits**. See Figure 17.

![Figure 17: Access Zscaler Sandbox report](image)
4.6 Zscaler Sandbox Report

Zscaler Sandbox report provide detailed information regarding file detonation results.

![Zscaler Sandbox Report](image)

Figure 18: Zscaler Sandbox Report
4.7 **Access CrowdStrike Endpoint Hits Report**

Click on **View CrowdStrike Endpoint Hits Report** (from step 4.5) to see CrowdStrike endpoint hits.

![CrowdStrike Endpoint Hits Report](image)

**Figure 19: CrowdStrike Endpoint Hits Report**
4.8 **Network Contain an Endpoint**

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

![Figure 20: Contain an Endpoint](image)

---

**Copyright ©, Zscaler, Inc.**

Page 26 of 32
4.9 **Confirm endpoint quarantine status**

Click again on the **CrowdStrike Endpoint Hits Report** (step 4.5) to confirm the containment status.

![CrowdStrike Endpoint Hits Report](image)

*Figure 21: Confirm Containment Status*
5 Appendix A: Requesting Zscaler Support

5.1 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 hours a day, year-round.

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

![Figure 22: Collecting details to open support case with Zscaler TAC](image)
### 5.1.1 Save Company ID

Copy the Company ID, as shown below.

![Company Profile](image)

Figure 23: Company ID
5.1.2 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 24: Submit ticket
6 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/
7 Appendix C: CrowdStrike Resources

CrowdStrike Falcon Admin Portal
https://www.falcon.crowdstrike.com/

CrowdStrike Documentation
https://falcon.crowdstrike.com/support/documentation

CrowdStrike Support Portal
https://supportportal.crowdstrike.com/

CrowdStrike Blog
https://www.crowdstrike.com/blog/