Table of Contents

1 Zscaler and CrowdStrike Introduction ................................................................. 7
  1.1 Zscaler Overview ............................................................................................. 7
  1.2 CrowdStrike Overview .................................................................................... 8

2 Use Case I: ZPA Posture Check Integration with CrowdStrike ZTA .................. 10
  2.1 Configuring CrowdStrike .................................................................................. 13
     2.1.1 Getting ZTA integration enabled in CrowdStrike tenant ......................... 13
  2.2 Configuring Zscaler Private Access (ZPA) ...................................................... 14
     2.2.1 Log into ZPA portal .................................................................................. 14
     2.2.2 Navigate to Mobile Admin Portal .............................................................. 15
     2.2.3 Create new Posture profile ...................................................................... 16
     2.2.4 Add new CrowdStrike ZTA Posture profile ............................................. 17
     2.2.5 Decide which applications need conditional access based on ZTA .......... 18
     2.2.6 Setup an Access Policy ........................................................................... 20
     2.2.7 Tie the Posture Profile to this Access Policy .......................................... 21
     2.2.8 Verify ZTA based conditional access from endpoint ............................. 22

3 Use Case II: ZPA Posture Check Integration with CrowdStrike ..................... 24
  3.1 Configuring Zscaler Private Access (ZPA) ...................................................... 27
     3.1.1 Log into ZPA portal .................................................................................. 27
     3.1.2 Navigate to Mobile Admin Portal .............................................................. 28
     3.1.3 Create new Posture profile ...................................................................... 29
     3.1.4 Add new CrowdStrike Posture profile .................................................... 30
     3.1.5 Decide which applications need conditional access ............................... 31
     3.1.6 Setup an Access Policy ........................................................................... 33
     3.1.7 Tie the Posture Profile to this Access Policy .......................................... 34
     3.1.8 Verify conditional access from endpoint ................................................ 35

4 Use Case III: ZIA Sandbox Integration with CrowdStrike ............................ 37
  4.1 Configuring CrowdStrike .................................................................................. 39
     4.1.1 Configuring CrowdStrike for ZIA ............................................................. 39
     4.1.2 Logging into CrowdStrike ...................................................................... 40
     4.1.3 Access CrowdStrike Customer ID ............................................................. 41
     4.1.4 Note down CrowdStrike Customer ID ..................................................... 42
     4.1.5 Navigate to API section .......................................................................... 43
     4.1.6 Add New API Client .............................................................................. 44
     4.1.7 Create API Client for ZIA ..................................................................... 45
     4.1.8 Make a note of API credentials ............................................................... 46
  4.2 Configuring Zscaler Internet Access (ZIA) ..................................................... 47
     4.2.1 Configuring Zscaler Internet Access for CrowdStrike ......................... 47
     4.2.2 Logging into Zscaler (ZIA) Admin Portal ................................................ 47
     4.2.3 Configure Partner Integration ................................................................. 48
     4.2.4 Verify Partner Integration ..................................................................... 49
     4.2.5 Activate Pending ZIA Configuration ...................................................... 50
4.3 Viewing CrowdStrike Endpoint Hits

4.3.1 Navigate to Web Insights

4.3.2 Select Logs

4.3.3 Filter on Sandbox related logs

4.3.4 Confirm whether file was sent to sandbox

4.3.5 Access Zscaler Sandbox Report

4.3.6 Zscaler Sandbox Report

4.3.7 Access CrowdStrike Endpoint Hits Report

4.3.8 Network Contain an Endpoint

4.3.9 Confirm endpoint quarantine status

5 Use Case IV: Threat Intelligence sharing - CrowdStrike FalconX & ZIA

5.1 Overview

5.1.1 Prerequisites

5.1.2 Flow of events

5.2 Getting Started

5.2.1 Create Zscaler URL Category

5.2.2 Clone the integration from Github

5.2.3 Populate credentials needed for the integration

5.2.4 Launch the integration

5.2.5 Further details about the integration

6 Appendix A: Requesting Zscaler Support

6.1 Gather Support Information

6.1.1 Save Company ID

6.1.2 Enter Support Section

7 Appendix B: Zscaler Resources

8 Appendix C: CrowdStrike Resources
## 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 (Nasdaq: CRWD), is a leading cybersecurity company protecting customers from all cyber threats by leveraging its Security Cloud to stop breaches. From its inception in 2011, driven by George Kurtz’s vision, CrowdStrike was created as a different kind of cybersecurity company. Cloud-native, CrowdStrike immediately brought a threat perspective, effectiveness, scalability, and flexibility never seen before in the industry – seamlessly aligning People, Technology, and Processes. The CrowdStrike Falcon platform has revolutionized enterprise security for the cloud era. Its single lightweight-agent architecture leverages artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network.
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.

Document Authors

This document was authored by Solution Architects in the Zscaler Business Development / Technical Alliances team (aka “BD SA”). All solutions validated within this guide have been jointly reviewed by both vendors.

Software Versions

This document was authored using Zscaler Internet Access and Zscaler Private Access (with Zscaler Client Connector/Z-App version 3.4) along with CrowdStrike Falcon Agent 6.18.13211 on Windows 10.

Request for Comments

- **For Prospects / Customers:** 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

- **For Zscaler Employees:** If you are trying to reach the team that validated and authored the integrations contained within this document, please contact us at:
  - z-bd-sa@zscaler.com
1 Zscaler and CrowdStrike Introduction

1.1 Zscaler Overview

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (ZIA) is a secure Internet and web gateway delivered as a service from the cloud. Think of it as a secure Internet onramp — all you do is make Zscaler your next hop to the Internet. This is often accomplished using one of the following methods:

- For offices, simply set up a tunnel (GRE or IPSEC) to the closest Zscaler data center.
- For mobile employees, you can forward traffic via our lightweight Z-App or PAC file.

No matter where users connect — a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea — they get identical protection. Zscaler Internet Access sits between your users and the Internet, inspecting every transaction inline across multiple security techniques, even within SSL.

You get full protection from web and Internet threats. And with a cloud platform that supports Cloud Firewall, IPS, Sandboxing, DLP, CASB and Browser Isolation, you can start with the services you need today and activate others as your needs grow.

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides zero trust, secure remote access to internal applications running on cloud or data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity versus extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT admin within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler app is installed. Zscaler app ensures the user’s device posture and extends a secure micro-tunnel out to the Zscaler cloud when a user attempts to access an internal application.
1.2 CrowdStrike Overview

CrowdStrike Falcon Overview

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.

CrowdStrike Zero Trust Assessment (ZTA) Overview

CrowdStrike ZTA delivers real-time security posture assessments across all endpoints regardless of location, network, and user. Falcon ZTA enables enforcement of dynamic conditional access based on device health and compliance checks that mitigate the risk to users and the organization. Every endpoint is granted least privileged access and is assessed before gaining access to sensitive data and corporate assets – ensuring Zero Trust enforcement across all endpoints. By expanding Zero Trust beyond authentication and including device security, CrowdStrike Falcon ZTA helps organizations maintain a holistic cybersecurity approach that protects their data and users from the sophisticated tactics of cyber adversaries.
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.

Document Authors

This document was authored by Solution Architects in the Zscaler Business Development / Technical Alliances team (aka “BD SA”). All solutions validated within this guide have been jointly reviewed by both vendors.

Software Versions

This document was authored using Zscaler Internet Access and Zscaler Private Access (with Zscaler Client Connector/Z-App version 3.4) along with CrowdStrike Falcon Agent 6.18.13211 on Windows 10.

Request for Comments

- **For Prospects / Customers:** 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

- **For Zscaler Employees:** If you are trying to reach the team that validated and authored the integrations contained within this document, please contact us at:
  - z-bd-sa@zscaler.com
2 Use Case I: ZPA Posture Check Integration with CrowdStrike ZTA

Zscaler Private Access (ZPA) is a cloud service that provides zero trust, secure remote access to internal applications running on cloud or data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity versus extending the network to them.

CrowdStrike ZTA delivers real-time security posture assessments across all endpoints regardless of location, network, and user. Falcon ZTA enables enforcement of dynamic conditional access based on device health and compliance checks that mitigate the risk to users and the organization. Every endpoint is granted least privileged access and is assessed before gaining access to sensitive data and corporate assets – ensuring Zero Trust enforcement across all endpoints. By expanding Zero Trust beyond authentication and including device security, CrowdStrike Falcon ZTA helps organizations maintain a holistic cybersecurity approach that protects their data and users from the sophisticated tactics of cyber adversaries.
Use Case:

- CrowdStrike’s Zero Trust Assessment calculates a (ZTA) security score from 1 to 100 for each host. A higher score indicates a better security posture for the host.
  - Security scores are derived from two distinct assessment sources:
    - OS settings (Windows only): Settings that track native OS security options, firmware availability, and Common Vulnerabilities and Exposures (CVE) mitigations.
    - Falcon sensor settings (Windows and Mac): Falcon sensor configurations that track Reduced Functionality Mode (RFM) status as well as prevention and Real Time Response policies.

- Zscaler Private Access (ZPA) utilizes CrowdStrike’s ZTA device posture score to only allow compliant endpoints to access selected applications. ZPA checks for any changes to the CrowdStrike’s device posture score (i.e., ZTA) whenever a new connection request is made, as a device’s posture may change over time. ZTA check is supported currently for Windows and Mac endpoints.

- ZPA achieves this conditional access by evaluating ZPA “Access Policies” which in turn reference device level “posture check profiles”. ZPA admin can specify that a minimum ZTA score of ‘X’ (from scale 0-100, with higher score implying better security posture) is needed for the endpoint to be granted access to internal applications referenced in the ZPA Access policy. Unless that end-device’s ZTA score is greater than or equal to the threshold referenced in ZPA access policy (via posture check profile), ZPA will block that application access from that host.

! NOTE !

As of now, customers who wish to use this integration will need to get in touch with CrowdStrike support team to turn on a feature flag in their Crowdstrike tenant. Once this is enabled on CrowdStrike backend, ZPA will be able to access and utilize the per device ZTA score. CrowdStrike support team can be reached at following email alias support@crowdstrike.com

End device trying to access applications over ZPA needs to be running Zscaler Client Connector (ZCC, formerly known as Zapp) version >= 3.4 for this integration to work.
See below for a conceptual diagram of the integration

**Figure 1: High Level Overview**
2.1 Configuring CrowdStrike

2.1.1 Getting ZTA integration enabled in CrowdStrike tenant

As of now, customers who wish to use this integration with Zscaler will need to get in touch with CrowdStrike support team to turn on a ZTA feature flag in their Crowdstrike tenant.

Once this is enabled on CrowdStrike backend, ZPA will be able to access and utilize the per device ZTA score.

Before proceeding further, reach out to support@crowdstrike.com to get this flag turned on

Please also ensure that Zscaler Client Connector (ZCC, formerly known as Z-App) version installed on the end host that you will be testing from is 3.4 or higher
2.2 Configuring Zscaler Private Access (ZPA)

This guide assumes that you have a working ZPA setup and provides instructions to integrate ZTA based conditional access into your existing ZPA deployment.

2.2.1 Log into ZPA portal

Figure 2: Log into ZPA portal
2.2.2 Navigate to Mobile Admin Portal

Click on the Client Connector icon shown below. This will bring you to Mobile Admin portal.

Figure 3: Click on Client Connector portal icon
2.2.3 Create new Posture profile

Once logged into mobile admin portal, navigate to Administration >> Device Posture and click on Add Device Posture Profile

![Add Device Posture Profile](image)

Figure 4: Add Device Posture Profile
2.2.4 Add new CrowdStrike ZTA Posture profile

Select Windows and MacOS only. Then, you will be able to click the dropdown and select “CrowdStrike ZTA Score” as Posture Type. Name this policy, provide the minimum value for ZTA score and hit save.

**Note:** ZPA will consider posture check to pass as long as end device’s ZTA score (calculated by CrowdStrike) >= value configured here. This posture profile will be referenced in a ZPA Access Policy. Access policy can be setup to (dis)allow application access based on whether posture check passes or fails.

![Add CrowdStrike ZTA Posture Profile](image_url)

**Figure 5:** Add CrowdStrike ZTA Posture Profile
2.2.5 Decide which applications need conditional access based on ZTA

Within the ZPA portal, Navigate to **Administration >> Application Segment**

This page lists applications that can be accessed over ZPA. We will select one of these applications and reference it in an access policy so that access to it is granted conditionally based on end device’s ZTA score

![Application Segments](image-url)

Figure 6: Navigate to Application Segments
In this example, applications hosted under domain *.bd-dev.com are accessed over ZPA (to which we will allow conditional access based on ZTA score of the end device)

Figure 7: Decide which Application to provide conditional access to (based on ZTA score)
2.2.6 Setup an Access Policy

Within the ZPA portal, Navigate to Administration >> Access Policy

![Setup Access Policy](image)

Figure 8: Setup Access Policy
2.2.7 **Tie the Posture Profile to this Access Policy**

Create new Access Policy by clicking on “Add Rule” and reference previously created posture profile. Customers can setup different access policies to protect different internal applications and these access policies can in turn reference different ZTA posture check profiles (based on ZTA score requirement). Customizable (and optional) popup message can be shown to the end users when application access is (dis)allowed, informing them about policy evaluation.

In this example, we added access policy to block user access to application if ZTA posture check fails (Rule#1). If the end device’s ZTA score >= configured threshold (75 in this example), rule #1 will evaluate to be false and policy evaluation will proceed to rule#2 (which will grant application access).

![Setup Access Policy](image)

**Figure 9: Setup Access Policy**
2.2.8 Verify ZTA based conditional access from endpoint

Ensure that you are logged into ZPA with ZCC version being 3.4 or higher and try accessing application that was referenced in the access policy in previous steps. The app should be accessible from the endpoint if device’s CrowdStrike calculated ZTA score is greater than or equal to the value configured in posture profile. Otherwise, the access will be blocked by ZPA.

![Figure 10: Access granted from endpoint having ZTA >= configured value in Posture profile](image-url)
Figure 11: Access blocked from endpoint having ZTA < configured value in Posture profile
3 Use Case II: ZPA Posture Check Integration with CrowdStrike

Zscaler Private Access (ZPA) is a cloud service that provides zero trust, secure remote access to internal applications running on cloud or data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity versus extending the network to them.

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.
Primary Use Case:

- Zscaler Private Access (ZPA) verifies the presence of running CrowdStrike Falcon process on the endpoint as an assessment of end device posture. ZPA can be configured to allow only compliant endpoints (ones that pass the posture check) to access selected applications.

- ZPA achieves this conditional access by evaluating ZPA “Access Policies” which in turn reference device level “posture check profiles”. ZPA admin can specify (for Windows and Mac workstations) that CrowdStrike falcon agent is needed to be installed and running on the endpoint for the endpoint to be granted access to internal applications referenced via ZPA Access policy.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
</table>

*This ZPA integration was implemented before ZTA functionality was available from CrowdStrike.*

*ZTA based posture check (previous use case in this guide) is an enhancement to this use case and should be preferred due to its nuanced posture checking abilities*
See below for a conceptual diagram of the integration

![Device Posture Driven Conditional Access Diagram](image)

**Figure 12: High Level Overview**
3.1  **Configuring Zscaler Private Access (ZPA)**

This guide assumes that you have a working ZPA setup and provides instructions to integrate posture based conditional access into your existing ZPA deployment.

3.1.1  **Log into ZPA portal**

![Log into ZPA portal](image)

Figure 13: Log into ZPA portal
3.1.2 Navigate to Mobile Admin Portal

Click on the Client Connector icon shown below. This will bring you to Mobile Admin portal.

Figure 14: Click on Client Connector portal icon
3.1.3  Create new Posture profile

Once logged into mobile admin portal, navigate to Administration >> Device Posture and click on Add Device Posture Profile

![Add Device Posture Profile](image)

Figure 15: Add Device Posture Profile
3.1.4 Add new CrowdStrike Posture profile

Select Windows and MacOS only. Then, you will be able to click the dropdown and select “Detect CrowdStrike” as Posture Type. Name this policy and hit save.

This posture profile will be referenced in a ZPA Access Policy. Access policy can be setup to (dis)allow application access based on whether posture check passes or fails.

![Add Device Posture](image)

Figure 16: Add Detect CrowdStrike Posture Profile
3.1.5 Decide which applications need conditional access

Within the ZPA portal, Navigate to Administration >> Application Segment
This page lists your applications that can be accessed over ZPA. We will select one of these applications and reference it in an access policy so that access to it is granted conditionally based on end device’s posture.

Figure 17: Navigate to Application Segments
In this example, applications hosted under domain *.bd-dev.com are accessed over ZPA (to which we will allow conditional access based on posture of the end device)

Figure 18: Decide which Application to provide conditional access to
3.1.6 Setup an Access Policy

Within the ZPA portal, Navigate to Administration >> Access Policy

Figure 19: Setup Access Policy
3.1.7 Tie the Posture Profile to this Access Policy

Create new Access Policy by clicking on “Add Rule” and reference previously created posture profile. Customers can setup different access policies to protect different internal applications. Customizable (and optional) popup message can be shown to the end users when application access is (dis)allowed, informing them about policy evaluation.

In this example, we added access policy to block user access to application if CrowdStrike posture check fails (Rule#1). If CrowdStrike is not running on the endpoint, rule #1 will evaluate to be true and access will be blocked. Otherwise, policy evaluation will proceed to rule#2 (which will grant application access)

![Access Policy Diagram](image)

Figure 20: Setup Access Policy
3.1.8 Verify conditional access from endpoint

The app should be accessible from the endpoint if device has CrowdStrike agent installed and running. Otherwise, the access will be blocked by ZPA.

Figure 21: Access granted from endpoint having CrowdStrike agent installed and running
Figure 22: Access blocked from endpoint if CrowdStrike agent is not running
4 Use Case III: ZIA Sandbox 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).
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 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 23: High Level Overview](image-url)
4.1 Configuring CrowdStrike

4.1.1 Configuring CrowdStrike for ZIA

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/
4.1.2 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).

![Log into CrowdStrike](image)

Figure 24: Log into CrowdStrike
### 4.1.3 Access CrowdStrike Customer ID

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

![Access CrowdStrike Customer ID](image)

*Figure 25: Access CrowdStrike Customer ID*
4.1.4 Note down CrowdStrike Customer ID

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

Figure 26: Note down CrowdStrike Customer ID
4.1.5 **Navigate to API section**

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

![API Clients and Keys](image)

**Figure 27: Navigate to API section**
4.1.6 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.

Figure 28: Add New API Client
4.1.7 **Create API Client for ZIA**

Create an API client with following scopes:

- Read-Write permission for Hosts (Write permission is required for Containment action)
- Read only permission for IOCs
- Read only permission for Detections

Once completed, click **Save**.

![Figure 29: Create & Save API Client](image-url)
4.1.8 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 30: Note down API credentials
4.2 Configuring Zscaler Internet Access (ZIA)

4.2.1 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.

4.2.2 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:


![Log into Zscaler Admin portal](image)

Figure 31: Log into Zscaler Admin portal
4.2.3 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. Next, paste your CrowdStrike API credentials and Customer ID here. Click Save.

Figure 32: Configure Partner Integration
4.2.4 Verify Partner Integration

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

![Partner Integrations](image)

Figure 33: Verify Partner Integration
4.2.5 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.

Figure 34: Activate Pending ZIA Configuration
4.3 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.

4.3.1 Navigate to Web Insights

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

![Navigate to Web Insights](image-url)
4.3.2 Select Logs

Next, click on the Logs tab and Add Filter, as shown in Figure 14.
4.3.3 Filter on Sandbox related logs

Select **Sandbox** as the Threat Class and click on **Apply Filters**

![Select Sandbox filter](image)

Figure 37: Select Sandbox filter
4.3.4 Confirm whether file was sent to sandbox

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 38: Confirm whether file was sent to sandbox
4.3.5 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 then select View CrowdStrike Endpoint Hits.

![Table of Insights Logs]

Figure 39: Access Zscaler Sandbox report
4.3.6 Zscaler Sandbox Report

Zscaler Sandbox report provide detailed information regarding file detonation results.

Figure 40: Zscaler Sandbox Report
4.3.7 **Access CrowdStrike Endpoint Hits Report**

Click on **View CrowdStrike Endpoint Hits Report** (from step 5.3.5) to see CrowdStrike endpoint hits.

![CrowdStrike Endpoint Hits Report](image)

*Figure 41: CrowdStrike Endpoint Hits Report*
4.3.8 Network Contain an Endpoint

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

![Contain an Endpoint](image)

**Figure 42: Contain an Endpoint**
4.3.9 Confirm endpoint quarantine status

Click again on the CrowdStrike Endpoint Hits Report (step 4.3.5) to confirm the containment status.

![Confirm Containment Status](image_url)

Figure 43: Confirm Containment Status
5 Use Case IV: Threat Intelligence sharing - CrowdStrike FalconX & ZIA

CrowdStrike’s Falcon X threat intelligence data can be easily shared with Zscaler Zero Trust Exchange for seamless usage when integrations are activated to provide stronger protection and increased visibility.

When a mutual customer of Zscaler and CrowdStrike activates this integration, the integration starts fetching malicious IPs/URLs from CrowdStrike’s Intel platform and pushes them to that customer’s ZIA custom URL list. This custom URL list is then referenced in ZIA URL policy to block the end-user access. Before this push happens from CrowdStrike to ZIA, all of the IOCs are checked against Zscaler’s global IOC database and only those that ZIA doesn’t currently qualify as malicious, are pushed into the ZIA tenant.

Customers would need to download and run python code (hosted on Github) to enable this integration. The integration is maintained by CrowdStrike on following link. Any updates/improvements to this integration will show up on that Github page & should be considered as the authoritative/latest resource.

https://github.com/CrowdStrike/zscaler-FalconX-integration
5.1 Overview

Use Case:

- Zscaler Internet Access maintains a global data base of malicious IPs/Domains/URLs (i.e., IOCs) and blocks these threats inline in all ZIA customer tenants as long as pertinent security engines are enabled by ZIA admins. ZIA also has an ability to maintain per tenant custom URL lists. Customers can bring in their own custom threat feeds and populate these URL lists. These custom URL lists can then be referenced in ZIA URL policies for granularly controlling end-user access within that ZIA tenant.

- CrowdStrike FalconX allows you to expand your defenses with real-time access to global IOCs delivered by CrowdStrike. An existing Falcon X intelligence and ZIA customer can setup this integration to continually push high value threats from Falcon platform into their ZIA tenant.

See below for a conceptual diagram of the integration

Figure 44: High Level Overview
### 5.1.1 Prerequisites

- License for CrowdStrike Falcon X intelligence
- Admin access to CrowdStrike portal
- Admin access to ZIA portal
- Python 3.7+ environment

**Note!**

The default number of custom IOCs that can be pushed into a ZIA a tenant is 25,000. This limit can be increased by customers (up to 275k) by getting in touch with Zscaler account team.

The integration scripts take into account /urllookup API rate limit on ZIA side (~40k lookups per hour) and throttles the lookups to avoid running into any rate limit issues

Figure 45: IOC limit

### 5.1.2 Flow of events

Figure 46: Flow of events in the integration
5.2 Getting Started

5.2.1 Create Zscaler URL Category

First, log into your ZIA tenant and then navigate to “Administration” -> “URL-Categories”, and then add a new URL category with the name ‘CrowdStrike Malicious URLs - High’, in the URL Super Category select 'User-Defined'. The new category will not be accepted without any entries, so enter an arbitrary URL, and then save.

Figure 47: Create a custom URL category
5.2.2 **Clone the integration from Github**

```bash
git clone https://github.com/CrowdStrike/zscaler-FalconX-integration.git

cd zscaler-FalconX-integration
```

Figure 48: Clone integration repository from Github

5.2.3 **Populate credentials needed for the integration**

Enter missing configuration values in config.py

**Obtained from CrowdStrike portal:**
API scope needed from CrowdStrike side for API key is Read permission for Indicators (Falcon X)

- cs_clientID
- cs_secret

**Obtained from Zscaler (ZIA) portal:**

- zs_username
- zs_password
- zs_apiKey

Figure 49: Populate the script with credentials
5.2.4  Launch the integration

After missing configuration values have been filled up in config.py (above), you can launch the integration by running:

```
python main.py
```

![Launch the integration](image)

5.2.5  Further details about the integration

The integration is maintained by CrowdStrike on following link. Any updates/improvements to this integration will show up on that Github page & should be considered as the authoritative/latest resource.

[https://github.com/CrowdStrike/zscaler-FalconX-integration](https://github.com/CrowdStrike/zscaler-FalconX-integration)
6 Appendix A: Requesting Zscaler Support

6.1 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

![Image of Administration menu]

Figure 51: Collecting details to open support case with Zscaler TAC
6.1.1 Save Company ID

Copy the Company ID, as shown below.

![Company Profile](image)

Figure 52: Company ID
6.1.2 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 53: Submit ticket
7 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/

ZPA Overview
https://www.zscaler.com/products/zscaler-private-access

ZPA Posture Profiles

ZPA Access Policies
https://help.zscaler.com/zpa/configuring-access-policies
https://help.zscaler.com/zpa/access-policy-configuration-examples

ZPA integration with CrowdStrike ZTA
8 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/

CrowdStrike ZTA Demo

CrowdStrike Documentation for ZTA
https://falcon.crowdstrike.com/support/documentation/138/zero-trust-assessment

CrowdStrike FalconX IOC Sharing integration with ZIA
https://github.com/CrowdStrike/zscaler-FalconX-integration