Contents

Terms and Acronyms 5

About This Document 6
  Zscaler Overview 6
  CrowdStrike Overview 6
  Audience 6
  Software Versions 6
  Request for Comments 6

Zscaler and CrowdStrike Introduction 7
  Zscaler Internet Access (ZIA) Overview 7
  Zscaler Private Access (ZPA) Overview 7
    Zscaler Resources 7
  CrowdStrike Overview 8
    CrowdStrike Falcon Overview 8
    CrowdStrike Zero Trust Assessment (ZTA) Overview 8
    CrowdStrike Resources 8

Use Case 1: ZPA Posture Check Integration with CrowdStrike ZTA 9
  Configuring CrowdStrike ZTA Integration in the CrowdStrike Tenant 10
  Configuring ZPA 10
    Log into ZPA Admin Portal 10
    Navigate to Zscaler Client Connector 10
    Create New Posture Profile 11
    Add a New CrowdStrike ZTA Posture Profile 12
    Decide Which Applications Need Conditional Access Based on ZTA 13
    Set Up an Access Policy 14
    Tie the Posture Profile to the Access Policy 15
    Verify ZTA-Based Conditional Access from an Endpoint 16
Use Case 2: ZPA Posture Check Integration with CrowdStrike

Configuring ZPA
- Log into ZPA Admin Portal
- Navigate to the Zscaler Client Connector
- Create a New Posture Profile
- Add a New CrowdStrike Posture Profile
- Decide Which Applications Need Conditional Access
- Set Up an Access Policy
- Tie the Posture Profile to this Access Policy
- Verify Conditional Access from an Endpoint

Use Case 3: ZIA Sandbox Integration with CrowdStrike

Configuring CrowdStrike for ZIA
- Logging into CrowdStrike
- Access Your CrowdStrike Customer ID
- Note Your CrowdStrike Customer ID
- Navigate to the API Section
- Add a New API Client
- Create API Client for ZIA
- Make a Note of the API Credentials

Configuring ZIA for CrowdStrike
- Logging into ZIA Admin Portal
- Configure Partner Integration
- Verify the Partner Integration
- Activate Pending ZIA Configuration

Viewing CrowdStrike Endpoint Hits
- Navigate to Web Insights
- Select Logs
- Filter on Sandbox Related Logs
- Confirm the File Was Sent to the Sandbox
- Access Sandbox Report
ZSCALER AND CROWDSTRIKE DEPLOYMENT GUIDE

Sandbox Detail Report 32
Access the CrowdStrike Endpoint Hits Report 33
Network Contain an Endpoint 33
Confirm Endpoint Quarantine Status 34

Use Case 4: Threat Intelligence Sharing—CrowdStrike FalconX and ZIA 35
Overview 35
Prerequisites 36
Flow of Events 36
Create Zscaler URL Category 37
Clone the Integration from GitHub 37
Populate the Credentials Needed for the Integration 37
Further Details About the Integration 38

Use Case 5: CrowdStrike Humio Essential Configuration (Using Cloud-to-Cloud logging - HTTPS POST) 39
Configure CrowdStrike Humio Cloud to Ingest ZIA Logs over HEC Input 39
Log into CrowdStrike Humio Cloud Tenant 40
Install Zscaler Package in Your Cloud Tenant 41
Create and Add Ingest Tokens in CrowdStrike Humio 42

Configure Zscaler for Cloud-to-Cloud Logging 44
Navigate to Cloud-to-Cloud Logging Section in ZIA Portal 44
Setup the Cloud NSS Log Feed (Web) 45
Setup the Cloud NSS Log Feed (Firewall) 47
Add Other Log Sourcetypes 48
Validate NSS Cloud Configuration 48
Verify Log Flow Using Humio’s Zscaler Package 49

Appendix A: Requesting Zscaler Support 50
Gather Support Information 50
Save Company ID 50
Enter Support Section 51

©2022 Zscaler, Inc. All rights reserved.
### Terms and Acronyms

The following terms and acronyms are used in this document.

<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 (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC2409)</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security (RFC2411)</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 (RFC6101)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC7239)</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

This document provides information on how to configure Zscaler and Crowdstrike for deployment.

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. Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't 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, visit www.zscaler.com or follow Zscaler 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 for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- CrowdStrike Resources

Software Versions

This document was authored using ZIA and ZPA (with Zscaler Client Connector) along with CrowdStrike Falcon Agent 6.18.13211 on Windows 10.

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Please contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- For Zscaler Employees: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.
Zscaler and CrowdStrike Introduction

Overviews of the Zscaler and CrowdStrike applications are described in this section.

Zscaler Internet Access (ZIA) Overview

ZIA is a secure Internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure Internet onramp—just make Zscaler your next hop to the Internet via one of the following methods:

- Set up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forward traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

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. ZIA sits between your users and the Internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and Internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, CASB, and Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides secure remote access to internal applications running on cloud or data center using a zero trust framework. 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 rather than 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 administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector 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.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZPA Help Portal</td>
<td>Help articles for ZPA</td>
</tr>
<tr>
<td>ZPA Posture Profiles</td>
<td>Help link for how to configure ZPA posture profiles.</td>
</tr>
<tr>
<td>ZPA Access Policies</td>
<td>Help link for how to configure ZPA access policies with a set of configuration examples.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
<tr>
<td>ZPA and CrowdStrike ZTA integration</td>
<td>Blog on the benefits of ZPA and CrowdStrike integration.</td>
</tr>
</tbody>
</table>
CrowdStrike Falcon Overview
CrowdStrike Falcon Endpoint Protection Enterprise Platform sets the new standard with the first cloud-native security platform that delivers an endpoint breach prevention solution. It is 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.

CrowdStrike Resources
The following table contains links to CrowdStrike support resources.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Falcon Admin Portal</td>
<td>Link to CrowdStrike administration portal.</td>
</tr>
<tr>
<td>CrowdStrike Support Portal</td>
<td>CrowdStrike support portal for submitting requests and issues.</td>
</tr>
<tr>
<td>CrowdStrike Documentation</td>
<td>Link to CrowdStrike online documentation.</td>
</tr>
<tr>
<td>CrowdStrike Documentation for ZTA</td>
<td>Documentation for CrowdStrike ZTA.</td>
</tr>
<tr>
<td>CrowdStrike ZTA Demo</td>
<td>Link to a video demonstration of CrowdStrike ZTA.</td>
</tr>
<tr>
<td>CrowdStrike FalconX IOC Sharing integration with ZIA</td>
<td>GitHub repository of examples that show CrowdStrike and Zscaler integration.</td>
</tr>
</tbody>
</table>
Use Case 1: ZPA Posture Check Integration with CrowdStrike ZTA

In this use case:

- CrowdStrike's calculates a Zero Trust Assessment (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: 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.
- ZPA uses CrowdStrike's ZTA score (also known as a device posture score) and only allows compliant endpoints to access selected applications. ZPA checks for any changes to the CrowdStrike's device posture score because the score can change over time. ZTA check is supported currently by CrowdStrike for Windows and Mac endpoints.
- ZPA achieves conditional access by evaluating ZPA “Access Policies” which, in turn, reference device level “posture check profiles.” ZPA administrators can specify that a minimum ZTA score is needed for the endpoint to be granted access to internal applications that are referenced in the ZPA access policy. The end-device’s ZTA score must be greater than or equal to the threshold referenced in ZPA access policy (via posture check profile), otherwise ZPA blocks the application access from that host.

Currently, customers who want to use this integration must contact CrowdStrike support team to turn on a feature flag in their CrowdStrike tenant. When enabled on CrowdStrike backend, ZPA can access and use the per-device ZTA score.

You can reach the CrowdStrike support team at the support@crowdstike.com email alias. Any device trying to access applications over ZPA must be running Zscaler Client Connector version 3.4 or greater for this integration to work. CrowdStrike sensor must be version 6.20 or greater.

The following diagram shows a conceptualization of the integration.

Figure 1. High-Level overview
Configuring CrowdStrike ZTA Integration in the CrowdStrike Tenant

Currently, customers who want to integrate with Zscaler must contact the CrowdStrike support team to turn on a ZTA feature flag in their CrowdStrike tenant.

When enabled on the CrowdStrike backend, ZPA can access and use the per-device ZTA score.

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

Also ensure that you use Zscaler Client Connector version 3.4 or higher on the end host from which you will be testing. CrowdStrike sensor version must be 6.20 or higher.

Configuring 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.

Log into ZPA Admin Portal

Log into ZPA Admin Portal

Navigate to Zscaler Client Connector

Click the Zscaler Client Connector icon to access the Zscaler Client Connector.
Create New Posture Profile

Log into the Zscaler Client Connector and navigate to Administration > Device Posture. Then click Add Device Posture Profile.

Figure 4. Add a device posture profile
Add a New CrowdStrike ZTA Posture Profile

Complete the following steps:

1. Select only Windows and macOS.
2. Click the Posture Type drop-down menu.
3. Select CrowdStrike ZTA Score.
4. Name this policy.
5. Provide the minimum value for a ZTA score.
6. Click Save.

ZPA passes a posture check if the end device’s ZTA score (calculated by CrowdStrike) is greater than or equal to the value configured in this procedure. This posture profile is referenced in a ZPA Access Policy. Access policies can be setup to allow or deny application access based on whether posture check passes or fails.

**Figure 5. Add a CrowdStrike ZTA posture profile**
Decide Which Applications Need Conditional Access Based on ZTA

Within the ZPA Admin Portal, navigate to Administration > Application Segment. This page lists applications that can be accessed over ZPA. 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.

In this example, applications hosted under the domain *.bd-dev.com are accessed over ZPA (and allowed conditional access based on the ZTA score of the end device).

Figure 6. Navigate to Application Segments

Figure 7. Decide which application to provide conditional access to (based on the ZTA score)
Set Up an Access Policy

Within the ZPA Admin Portal, navigate to Administration > Access Policy.

Figure 8. Open the access policy configuration dialog
Tie the Posture Profile to the Access Policy

In the Access Policy tab, click Add Rule and reference the previously created posture profile.

Customers can setup different access policies to protect different internal applications. These access policies, in turn, can reference different ZTA posture check profiles based on the ZTA score requirement. A customizable (and optional) popup message can be shown to the end users when application access is allowed or denied, informing them about policy evaluation.

In this example, we added an access policy to block user access to an application if the ZTA posture check fails (Rule#1). If the end device’s ZTA score is equal to or greater than the configured threshold (75 in this example), then Rule#1 is failed and the policy evaluation proceeds to Rule#2 (which grants application access).

![Access Policy](image)

---

Figure 9. Setup an access policy
Verify ZTA-Based Conditional Access from an Endpoint

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

Figure 10. Access granted from an endpoint with a ZTA score that is greater than or equal to the value configured in the posture profile

Figure 11. Access blocked from an endpoint with a ZTA score less than the configured value in the posture profile
Use Case 2: ZPA Posture Check Integration with CrowdStrike

In this use case:

- ZPA verifies the presence of a 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 evaluates ZPA “Access Policies” for conditional access. The policies, in turn, reference device level “posture check profiles.” The ZPA administrator can specify (for Windows and Mac workstations) that a CrowdStrike Falcon agent must be installed and running on the endpoint so that the endpoint can be granted access to internal applications referenced via ZPA Access policy.

This ZPA integration was implemented before ZTA functionality was available from CrowdStrike. ZTA-based posture check (the previous use case in this guide) is an enhancement to this use case and is preferred due to its nuanced posture checking abilities.

See the following conceptual diagram for an overview of the integration.

![Device Posture-Driven Conditional Access Diagram](image-url)
Configuring ZPA
This guide assumes that you have a working ZPA setup and provides instructions to integrate posture-based conditional access as part of your existing ZPA deployment.

Log into ZPA Admin Portal

![Log into ZPA Admin Portal](image)

Navigate to the Zscaler Client Connector
Click the Zscaler Client Connector icon to open the Zscaler Client Connector.

![Click the Zscaler Client Connector icon](image)
Create a New Posture Profile

Log into the Zscaler Client Connector and navigate to Administration > Device Posture. Then click Add Device Posture Profile.

Figure 15. Add a device posture profile

Add a New CrowdStrike Posture Profile

Complete the following steps:

1. Select only Windows and macOS.
2. Click the Posture Type drop-down menu.
3. Select Detect CrowdStrike.
4. Name this policy and click Save.

This posture profile is referenced in a ZPA Access Policy. Access policies can be setup to allow or deny application access based on whether the posture check passes or fails.

Figure 16. Add a detect CrowdStrike posture profile
Decide Which Applications Need Conditional Access

Within the ZPA Admin Portal, navigate to Administration > Application Segment.

This page lists which applications can be accessed by ZPA. Select one of these applications and reference it in an access policy so that access to it is granted based on the end device's posture.

In this example, ZPA can access applications hosted under the domain *.bd-dev.com, based on posture of the end device.
Set Up an Access Policy

Within the ZPA Admin Portal, navigate to Administration > Access Policy.

Tie the Posture Profile to this Access Policy

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

In this example, we added an access policy to block user access to the application if the CrowdStrike posture check fails (Rule#1). If CrowdStrike is not running on the endpoint, Rule#1 is marked true and access is blocked. Otherwise, the policy evaluation proceeds to Rule#2 (which will grant application access).
Verify Conditional Access from an Endpoint

The endpoint should be able to access the application if the endpoint device has a CrowdStrike agent installed and running. Otherwise, the access is blocked by ZPA.

![Access granted from an endpoint with the CrowdStrike agent installed and running](image1)

![Access blocked from an endpoint if the CrowdStrike agent is not running](image2)
Use Case 3: ZIA Sandbox Integration with CrowdStrike

In this use case:

- ZIA Cloud Sandbox detects zero-day malicious files via Zscaler Cloud Sandbox and produces an insight log about the file hash. In the same report, you receive relevant CrowdStrike endpoint telemetry data. The endpoint data is retrieved dynamically via an API session established by a one-time setup process in the ZIA Admin Portal.
- The same report also includes a contain and quarantine action button, which enables administrator to trigger a network contain or quarantine request to CrowdStrike Falcon platform. A network contained or quarantined host can talk to only CrowdStrike backend IPs and IPs explicitly placed on the allowlist by the CrowdStrike admin. All other network access is cut off.
- Alternatively, an administrator can click the CrowdStrike Agent ID within the Insight log to access the CrowdStrike console. Then, in the CrowdStrike console, the administrator can further investigate and mitigate operations for that Agent ID.

The following diagram shows a conceptualization of the integration.

![High level overview](image)

**Figure 23. High level overview**

Configuring CrowdStrike for ZIA

To establish the API connection between CrowdStrike and Zscaler, you must first generate an oauth2 token from the CrowdStrike console and then copy it to the ZIA Admin Portal.

Zscaler requires the following values to establish the API connection. You can get the values from the CrowdStrike console.

- CrowdStrike API Auth URL
- Client ID
- Secret
- Customer ID

The following steps assume that the CrowdStrike Falcon platform and CrowdStrike sensors are deployed and properly configured. Refer to the [CrowdStrike documentation](#) on how to deploy and configure CrowdStrike components before proceeding.
Logging into CrowdStrike

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

Access Your CrowdStrike Customer ID

After logging into CrowdStrike portal, click the User icon to access your Customer ID.
Note Your CrowdStrike Customer ID

You see your CrowdStrike Customer ID. You will need to enter this ID into the ZIA Admin Portal later.

Navigate to the API Section

While still the CrowdStrike portal, navigate to Support > API Clients and Keys.
Add a New API Client

In this use case, you create a new API client with specific permissions required for the use case. This is a one-time setup.

Click **Add new API client**.

![Add new API client](image)

Create API Client for ZIA

Create an API client with following settings:

- Read-Write permission for Hosts (write permission is required for containment action)
- Read only permission for indicator of compromise (IOC)
- Read only permission for detections

When complete, click **Save**.

![Create and save API client](image)
Make a Note of the API Credentials

After the API Client is created, you can access a Client ID and a Secret. Note your Secret value and then click Done. You will need to provide the ID and secret in Zscaler.

You cannot re-access the Secret after you click Done. If you lose the Secret, you must reset the CrowdStrike API credentials.

![API client created](image)

Figure 30. Note down API credentials

Configuring ZIA for CrowdStrike

Endpoint telemetry data from the CrowdStrike Falcon Platform is passed to the ZIA Admin Portal via an API integration. Correlating the endpoint data enables the ZIA Admin Portal to display the Sandbox report. In addition, you see information about the originating endpoint device and other infected endpoints in the environment, including the following:

- CrowdStrike Agent ID
- Host Name
- Timestamps that capture when malicious files appear on the endpoint (e.g., an infection via a different attack surface, such as via a USB thumb drive).

This automatic correlation of malware detection with an endpoint device reduces the time and effort needed for investigation and remediation.

In this section, you configure the ZIA Admin Portal with the ID and Key generated in the previous section.
Logging into ZIA Admin Portal
Log into ZIA Admin Portal using your admin account. If you are unable to log in using your administrator account, contact Zscaler Support.

![Log into Zscaler Admin Portal](image)

Figure 31. Log into Zscaler Admin Portal

Configure Partner Integration
From the Zscaler Admin Portal landing navigate to Administration > Partner Integration. The API Auth URL depends on which CrowdStrike cloud you use.

Complete the following steps:

1. Paste or enter your CrowdStrike API credentials (Client ID and Secret) in the appropriate fields.
2. Click Save. Then wait a few seconds for a status message.

![Configure partner integration](image)

Figure 32. Configure partner integration
Verify the Partner Integration

When you see the message **Valid API token** in green text, you have successfully configured the API connection for the ZIA integration.

![Partner Integrations](image)

**Figure 33. Verify partner integration**

Activate Pending ZIA Configuration

Anytime you make a change in ZIA, you see a number displayed 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 your cursor over the **Activation** menu and click the blue **Activate** button.

![Web Overview](image)

**Figure 34. Activate pending ZIA configuration**
Viewing CrowdStrike Endpoint Hits

Thanks to this integration, a file detonated by Zscaler Cloud Sandbox is automatically correlated with CrowdStrike endpoint device information within the Zscaler Admin Portal.

Navigate to Web Insights

In Zscaler Admin Portal, complete the following steps:

1. Select the **Analytics** tab.
2. Click **Web Insights**.

![Navigate to Web Insights](image)

Select Logs

Select the **Logs** tab and click **Add Filter**.

![Select logs](image)
Filter on Sandbox Related Logs

Select Sandbox as the Threat Class and click Apply Filters.

Confirm the File Was Sent to the Sandbox

After you click Apply Filters, if the file in question was detonated or is currently being detonated by the Cloud Sandbox, you’ll see corresponding log entries listed on right side of the portal.
## Access Sandbox Report

Within the list of log entries, select an MD5 hash, and right-click on the entry to access the drop-down menu. Select **View Sandbox Detail Report**.

<table>
<thead>
<tr>
<th>MD5</th>
<th>DLP Identifier</th>
<th>Uncancellable Type</th>
<th>Fo...</th>
<th>MD5</th>
<th>Forwarding...</th>
</tr>
</thead>
<tbody>
<tr>
<td>866e50910cc8afbd3a7669b4e12d77dd</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>866e50910cc8afbd3a7669b4e12d77dd</td>
<td>None</td>
</tr>
<tr>
<td>7eb15e8469ca8397ef22e1f9a55e6</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>7eb15e8469ca8397ef22e1f9a55e6</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>2601441d1370b89a6d6e6f780c928ea</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>2601441d1370b89a6d6e6f780c928ea</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>N...</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Figure 39. Access the Cloud Sandbox report

## Sandbox Detail Report

The Sandbox Detail report provides detailed information regarding file detonation results.

Figure 40. Sandbox Detail report
Access the CrowdStrike Endpoint Hits Report

Within the list of log entries, select the same or a different MDS entry, and click on the entry to access the drop-down menu. Select View CrowdStrike Endpoint.

<table>
<thead>
<tr>
<th>CrowdStrike Endpoint Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandbox File Properties (Zscaler)</td>
</tr>
<tr>
<td>Sandbox Category</td>
</tr>
<tr>
<td>Sandbox Score</td>
</tr>
<tr>
<td>File Type</td>
</tr>
<tr>
<td>File Size</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Detected on 3 Endpoints (CrowdStrike)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Agent ID</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>ac00d200014dfe7b510c6f6ef8</td>
</tr>
<tr>
<td>b591720001dfe7b510c6f6ef8</td>
</tr>
<tr>
<td>3018b0d200014dfe7b510c6f6ef8</td>
</tr>
</tbody>
</table>

Network Contain an Endpoint

Click Contain to trigger an API call to CrowdStrike. When you trigger the API to contain the endpoint, CrowdStrike cuts off that endpoint's network access.

<table>
<thead>
<tr>
<th>CrowdStrike Endpoint Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandbox File Properties (Zscaler)</td>
</tr>
<tr>
<td>Sandbox Category</td>
</tr>
<tr>
<td>Sandbox Score</td>
</tr>
<tr>
<td>File Type</td>
</tr>
<tr>
<td>File Size</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Detected on 3 Endpoints (CrowdStrike)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Agent ID</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>ac00d200014dfe7b510c6f6ef8</td>
</tr>
<tr>
<td>b591720001dfe7b510c6f6ef8</td>
</tr>
<tr>
<td>3018b0d200014dfe7b510c6f6ef8</td>
</tr>
</tbody>
</table>
Confirm Endpoint Quarantine Status

Access the CrowdStrike Endpoint Hits Report again to confirm the containment status.

**Figure 43. Confirm containment status**
Use Case 4: Threat Intelligence Sharing—CrowdStrike FalconX and ZIA

CrowdStrike’s Falcon X threat intelligence data can be 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 fetches malicious IPs or URLs from CrowdStrike’s Intel platform and pushes them to that customer’s ZIA custom URL list. This custom URL list is then referenced by ZIA URL policies to block the end-user access. Before the push happens from CrowdStrike to ZIA, all the IOCs are checked against Zscaler’s global IOC database and only IOCs that ZIA doesn’t currently qualify as malicious are pushed into the ZIA tenant. Customers must download and run Python code (hosted on GitHub) in order for the integration to work. The integration is maintained by CrowdStrike. Updates and improvements are added to the GitHub page and the GitHub repository is the authoritative and latest resource.

Overview

Use Case:

- ZIA maintains a global data base of malicious IPsDomainsURLs (i.e., IOCs) and blocks these threats inline in all ZIA customer tenants if pertinent security engines are enabled by ZIA admins. ZIA also maintains 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 expands your defenses with real-time access to global IOCs delivered by CrowdStrike. An existing FalconX intelligence and ZIA customer can setup this integration to continually push high value threats from the Falcon platform into their ZIA tenant.

The following diagram shows a conceptualization of the integration.

![High-Level overview](image)

The default number of custom IOCs that can be pushed into a ZIA a tenant is 25K.

Customers can increase the IOC quota (with a maximum of up to 275k) by contacting their Zscaler account team and purchasing additional custom URL SKUs.

The integration scripts consider the urllookup API rate limit on the ZIA side (~40K lookups per hour) and throttles the lookups to avoid running into any rate limit issues.
Prerequisites

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

Flow of Events

Figure 45. Flow of events in the integration
Create Zscaler URL Category

To create a Zscaler URL category:

1. Log into your ZIA Admin Portal.
2. Navigate to Administration > URL-Categories.
3. Add a new URL category with the name CrowdStrike Malicious URLs – High.
4. In the URL Super Category drop-down menu, select User-Defined. New categories require at least one entry, so enter an arbitrary URL.
5. Click Save.

![Add URL Category](image)

Figure 46. Create a custom URL category

Clone the Integration from GitHub

Use the following commands to clone the GitHub integration:

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

cd zscaler-FalconX-integration
```
Populate the Credentials Needed for the Integration

Collect the following values. From the CrowdStrike portal, get the Read permission for the indicators API key.

```
 cs_clientID
 cs_secret
```

From the Zscaler (ZIA) portal, get the following:

```
 zs_username
 zs_password
 zs_apiKey
```

You must have Python installed before you can complete the following step. Enter the required configuration values in `config.py`. `Config.py` is the main configuration file in Python.

Launch the Integration

After providing the required configuration values in `config.py`, you can launch the integration by running:

```
 python main.py
```

Further Details About the Integration

The integration is maintained by CrowdStrike. Updates and improvements are added to the GitHub page. The [GitHub repository](#) is the authoritative and latest resource.

You can find instructions on how to get the ZIA API key in the [ZIA Cloud Service API Developers Guide](#) section of the online documentation.
Use Case 5: CrowdStrike Humio Essential Configuration (Using Cloud-to-Cloud logging - HTTPS POST)

This section details the steps required to stream ZIA logs to a CrowdStrike Humio cloud from Zscaler, using Humio’s HTTP(S) API based log ingestion functionality.

Cloud NSS is Zscaler’s cloud-to-cloud log streaming service that allows you to stream logs directly from the ZIA cloud into a supported SIEM, without the need to deploy, manage and monitor an NSS VM for web or Firewall. The service supports all ZIA log types: web, SaaS security, tunnel, Firewall, and DNS.

For the CrowdStrike Humio cloud, the log ingestion API is the HEC input (/api/v1/ingest/hec/raw).

Customers can subscribe to Cloud NSS, which allows direct cloud-to-cloud log streaming for all types of ZIA logs into a CrowdStrike Humio instance.

The following links provide information about cloud-to-cloud logging:

  • NSS as service for cloud to cloud logging
  • About Cloud NSS Feeds

Add NSS Feeds

  • Adding Cloud NSS Feeds

Configure CrowdStrike Humio Cloud to Ingest ZIA Logs over HEC Input

This section requires that you have admin access to a working instance of CrowdStrike Humio cloud.

Installation of the package is straightforward, and the installation deploys the parser, saved queries, and dashboards directly into the repository that you select. You need to add five ingest tokens, one for each NSS log source assigned to its corresponding parser.

Then you need to create a new cloud NSS feed in the ZIA Admin Portal dashboard for the sources included in this package. Configure these feeds with your Humio API URL and ingest token.
Log into CrowdStrike Humio Cloud Tenant

Log into CrowdStrike Humio tenant via the online portal.

1. Go to humio.com and select **Cloud login > Enterprise Login**.

![Humio.com Cloud login](image)

**Figure 48. Humio.com Cloud login**

2. Select the **Region** from the drop-down menu, then select your login option.

![Log into Humio Cloud tenant](image)

**Figure 49. Log into Humio Cloud tenant**

3. Login to the cloud with admin credentials.
Install Zscaler Package in Your Cloud Tenant

After logging in:

1. Navigate to Marketplace > Zscaler.

![Humio Marketplace](image)

Figure 50. Humio Marketplace

2. Select Zscaler/Internet Access from the list of apps.

3. Click Install package.

![Install ZIA package](image)

Figure 51. Install ZIA package
4. A list of app features gets shown. Click Install.

![Figure 52. Install ZIA package](image)

Create and Add Ingest Tokens in CrowdStrike Humio

After installing the ZIA package:

1. Navigate to Settings > Ingest > Ingest Tokens.
2. Click + Add token.

![Figure 53. Ingest tokens window](image)

3. This displays the New token dialog. Enter:
   - **Token name**: an intuitive name for the token
   - **Assigned parser**: Select the corresponding parser from the drop-down menu depending on which logs you want ZIA to send to Humio:
     - zscaler-nss-web
     - zscaler-nss-dns
     - zscaler-nss-tunnel
     - zscaler-nss-fw
     - zscaler-nss-casb
4. Click **Save**.

![New token dialog](image1.png)

**Figure 54. New token dialog**

5. The **Token** dialog displays with the token value. Copy this token value to paste into Zscaler when creating the cloud NSS feed for Humio.

![Token value](image2.png)

**Figure 55. Token value**
Configure Zcaler for Cloud-to-Cloud Logging

You can subscribe to Cloud NSS, which allows direct cloud-to-cloud log streaming for all types of ZIA logs into a Humio instance. Rather than deploying, managing, and monitoring on-premises NSS VMs, you can configure an HTTP(S) API feed that pushes logs from the Zcaler cloud service into an HTTP(S) API endpoint on the SIEM. The following steps show how to setup the log feed for web logs. You must repeat these steps to setup other Zcaler log types (e.g., Firewall or DNS logs).

Navigate to Cloud-to-Cloud Logging Section in ZIA Portal

After logging into ZIA admin portal, navigate to Administration > Nanolog Streaming Service > Cloud NSS Feeds > Add Cloud NSS Feed.

Figure 56. Navigate to cloud-to-cloud logging section in ZIA
Setup the Cloud NSS Log Feed (Web)

1. Select Other as the SIEM type from the drop-down menu. The API URL is a Humio URL dependent on customer’s Humio cloud location.

2. The authorization header contains the relevant Humio HEC token created in previous steps.

3. In the Add Cloud NSS Feed dialog, Key1 is “Authorization”. Value1 is the Humio HEC token in the format “Bearer XXX-XXX-XXX” (replace XXX with actual HEC token value).

4. Feed Output Type is JSON from the drop-down menu. Save the configuration after providing the required parameters. Add “", \ (double quotes, comma, backslash) to the Feed Escape Character list.

![Add Cloud NSS Feed](image)

Figure 57. Configure cloud NSS feed
Figure 58. Example with all fields populated (web)
Setup the Cloud NSS Log Feed (Firewall)

To set up the Cloud NSS log feed:

1. Select Other as the SIEM Type from the drop-down menu. The API URL is a Humio URL, which is dependent on customer’s Humio cloud location.
2. Repeat the steps from Create and Add Ingest Tokens in CrowdStrike Humio section of this document to create a new ingest token for use with the Firewall log type. Each log type (web, Firewall, DNS, etc.) requires its own unique ingest token on the Humio side.
3. The authorization header contains the relevant Humio HEC token.
4. In the Add Cloud NSS Feed dialog, Key1 is “Authorization”. Value1 is the HEC token in format “Bearer XXX-XXX-XXX” (replace XXX with actual HEC token value).
5. Select the Feed Output Type of JSON from the drop-down menu.
6. Provide the required parameters and then click Save.

![Add Cloud NSS Feed dialog](Figure 59. Configure cloud NSS feed)
Add Other Log Sourcetypes

Repeat the previous steps to add other log source types (e.g., DNS logs, tunnel logs, etc.).

Validate NSS Cloud Configuration

After you save the configuration, click the icon shown in the following screenshot to verify connectivity from ZIA cloud to the Humio cloud. This sends a sample or test log message from the ZIA cloud to Humio. Cloud-to-cloud connectivity is verified if Humio sends the expected response.
When the connectivity is verified, the **Connectivity Test** column changes from **Validation Pending** to **Validation Successful**.

![Figure 62. Humio cloud connectivity verified](image)

**Verify Log Flow Using Humio’s Zscaler Package**

Log back into your Humio cloud tenant and navigate to **Dashboards** section. Then select appropriate Zcaler dashboard depending on the type of logs being sent from ZIA to Humio.

The dashboard is populated with incoming Zcaler log data.

![Figure 63. Check Humio Zcaler dashboards](image)

If you see that a particular panel is not populated, click on the vertical ellipsis next to it to see the query that the panel is running. Understanding the query helps you troubleshoot.

![Figure 64. Widgets within Humio Zcaler dashboards](image)
Appendix A: Requesting Zscaler Support

The following appendix shows how to contact your Zscaler support team.

Gather Support Information

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round. To contact Zscaler support, select Administration > Settings > Company profile.

Save Company ID

Copy your Company ID.

Figure 65. Collecting details to open support case with Zscaler TAC

Figure 66. Company ID
Enter Support Section

With your company ID information, you can open a support ticket. Navigate to Dashboard > Support > Submit a Ticket.

Figure 67. Submit a ticket