ZSCALER AND CROWDSTRIKE DEPLOYMENT GUIDE

MAY 2025, VERSION 1.16

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following terms and acronyms are used in this document. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
API	Application Programming Interface
CA	Central Authority (Zscaler)
CID	Customer Identification (CrowdStrike)
CLI	Command Line Interface
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
EDR	Endpoint Detection and Response
GRE	Generic Routing Encapsulation (RFC2890)
HEC	HTML Ethernet Channel
IKE	Internet Key Exchange (RFC2409)
IoC	Indicator of Compromise
IOA	Indicater of Attack
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
KPI	Key Performance Indicator
NGAV	Next-Generation Antivirus
NSS	Nanolog Streaming Service
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
RFM	Reduced Functionality Mode (CrowdStrike)
SaaS	Software as a Service
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SSL	Secure Socket Layer (RFC6101)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)
ZTA	Zero Trust Assessment

Trademark Notice

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. To learn more, see the Zscaler website or follow us 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. To learn more, refer to CrowdStrike's website.

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:

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

Software Versions

This document was authored using ZIA and ZPA (with Zscaler Client Connector) along with CrowdStrike Falcon Agent 6.18.13211 on Windows 11.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact 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.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—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, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a 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, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler UVM Overview

Avalor Unified Vulnerability Management: Zscaler Avalor Unified Vulnerability Management (UVM), now a part of a Zscaler, offers a fresh perspective and innovative solutions to age-old challenges. Avalor UVM approach is grounded in the belief that effective risk management requires a holistic, data-centric strategy. It stands apart from traditional and second-generation UVM aggregation solutions because it starts with a focus on how to handle security data broadly, not just how to manage CVEs. Its innovation lies in the Data Fabric for Security, which uses security data to address a range of challenges. The Data Fabric for Security enables a breadth of capabilities that help companies uplevel their UVM programs with far less time and effort, including:

- Comprehensive Data Integration: Aggregate and correlate data from diverse sources to provide a truly unified view of an organization's security landscape.
- Rich Contextual Insights: Enrich and contextualize security findings across multiple security tools and business systems, providing actionable insights into security gaps based on an organization's specific risk factors.

- Dynamic Risk Assessment: Out-of-the-box multi-factor risk scores that include mitigating controls, derived from industry best practices, that allow teams to see and customize that risk calculation, so companies get a prioritized list rooted in their own environment and unique risk factors.
- Automated Workflows: Automated ticket assignment and tracking, built to match an organization's structure and systems, so teams can swiftly respond to the risks that are most likely to cause harm before they can be exploited.
- Customizable Dashboarding and Reporting: A rich dashboarding and reporting platform (pulling from a single aggregated and dynamic data set) allows organizations to create the views and reports they need, spanning their own KPIs, SLAs, and other key metrics and providing real-time insights into security posture and team performance.

Zscaler Resources

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler UVM Help Portal	Help articles for Zscaler UVM.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.
ZPA and CrowdStrike ZTA integration	Blog on the benefits of ZPA and CrowdStrike integration.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler UVM Help Portal	Help articles for Zscaler UVM.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.
ZPA and CrowdStrike ZTA integration	Blog on the benefits of ZPA and CrowdStrike integration.

CrowdStrike Falcon Endpoint Protection Enterprise Platform 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 Overview

CrowdStrike Zero Trust Assessment (ZTA) delivers real-time security posture assessments across all endpoints regardless of location, network, and user. CrowdStrike 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 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.

Name	Definition
CrowdStrike Falcon Admin Portal	Link to CrowdStrike administration portal.
CrowdStrike Support Portal	CrowdStrike support portal for submitting requests and issues.
CrowdStrike Documentation	Link to all CrowdStrike online documentation.
CrowdStrike ZTA Documentation	Documentation for CrowdStrike ZTA.
CrowdStrike ZTA Demo	Link to a video demonstration of CrowdStrike ZTA.
CrowdStrike Falcon IoC Sharing integration with ZIA	GitHub repository of examples that show CrowdStrike and Zscaler integration.

Use Case 1: ZPA Posture Check Integration with CrowdStrike ZTA

In this use case:

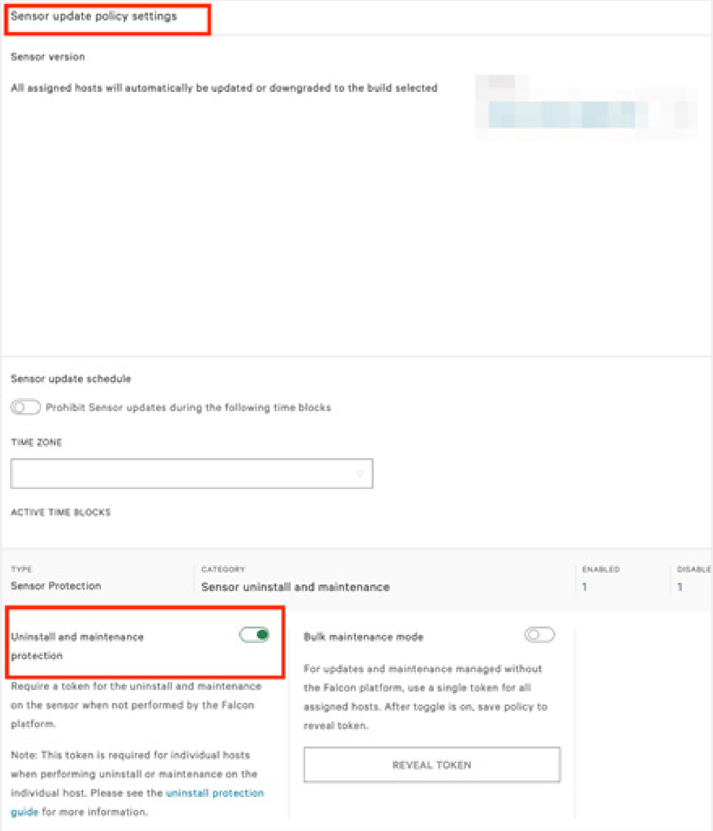
- CrowdStrike calculates a ZTA security score from 1 to 100 for each host. A higher score indicates a better security posture for the host. Security scores are derived from two distinct assessment sources:
  - OS settings: Settings that track native OS security options, firmware availability, and Common Vulnerabilities and Exposures (CVE) mitigations.
  - CrowdStrike Falcon sensor settings (Windows and macOS): CrowdStrike 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 allows only 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 macOS endpoints.
- ZPA achieves conditional access by evaluating ZPA access policies that, in turn, reference device-level posture check profiles. ZPA administrators can specify that a minimum ZTA score is needed for the endpoint to grant 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.

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

   You can reach the CrowdStrike Support team at support@crowdstrike.com. Any device trying to access applications over ZPA must be running Zscaler Client Connector version 3.4 or later for this integration to work. The CrowdStrike sensor must be version 6.20 or later.
2. The data.zta file is regularly deleted and recreated for security reasons, typically during system reboots or when updating score changes. This process takes about 15 seconds to one minute but endpoint system performance, network bandwidth, CrowdStrike backend processing delays, and other factors can affect the update time of this file. If a partner app accesses the ZTA data file during these delays, it could find it empty, partially filled, or missing—which would prevent the partner app from retrieving the ZTA score. In this case, the endpoint might be deemed untrustworthy, and partner products blocked from access to essential services. To avoid this issue, CrowdStrike implemented a ZTA caching feature. Contact the CrowdStrike Support team to enable the ZTA caching feature on your CID. To learn more, refer to the CrowdStrike documentation.

If interoperability issues arise, update your CrowdStrike policy's sensor visibility exclusions to account for Zscaler Client Connector-related details and re-test. To learn more, see Zscaler Client Connector Processes to Allowlist (government agencies, see Zscaler Client Connector Processes to Allowlist).

As a best practice, Zscaler recommends turning on **Uninstall and maintenance protection** via the CrowdStrike Sensor Update Policy settings, and enabling Sensor Tamper Prevention via CrowdStrike Prevention Policy settings.



Sensor update policy settings

Sensor version

All assigned hosts will automatically be updated or downgraded to the build selected [redacted]

Sensor update schedule

○ Prohibit Sensor updates during the following time blocks

TIME ZONE

ACTIVE TIME BLOCKS

TYPE	CATEGORY	ENABLED	DISABLE
Sensor Protection	Sensor uninstall and maintenance	1	1

Uninstall and maintenance protection ●

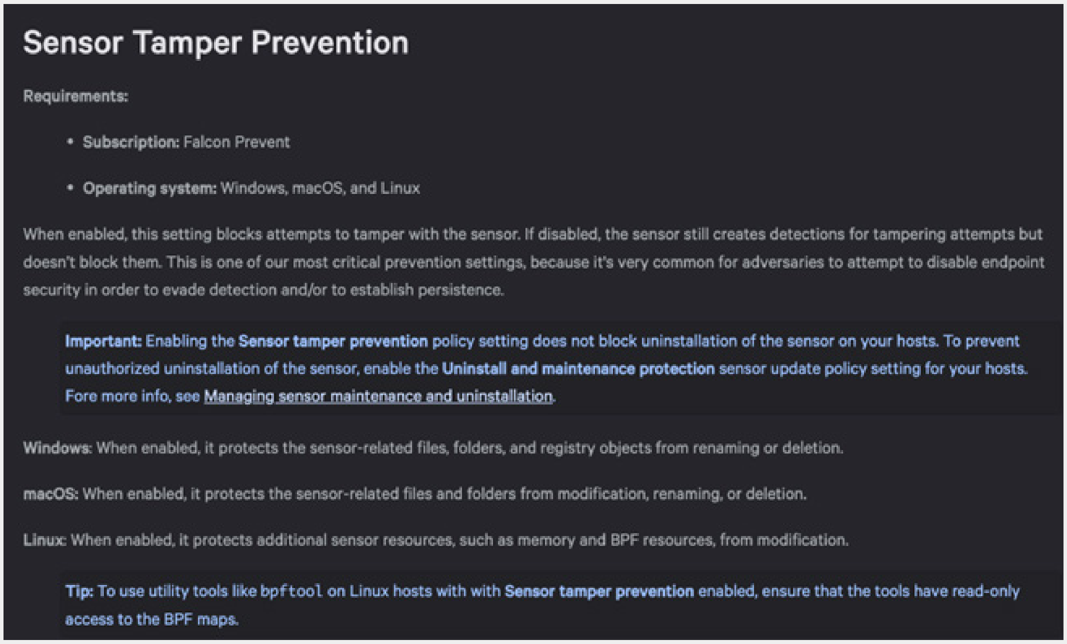
Require a token for the uninstall and maintenance on the sensor when not performed by the Falcon platform.

Note: This token is required for individual hosts when performing uninstall or maintenance on the individual host. Please see the uninstall protection guide for more information.

Bulk maintenance mode ○

For updates and maintenance managed without the Falcon platform, use a single token for all assigned hosts. After toggle is on, save policy to reveal token.

Figure 1. Uninstall and maintenance protection



Sensor Tamper Prevention

Requirements:

- **Subscription:** Falcon Prevent
- **Operating system:** Windows, macOS, and Linux

When enabled, this setting blocks attempts to tamper with the sensor. If disabled, the sensor still creates detections for tampering attempts but doesn't block them. This is one of our most critical prevention settings, because it's very common for adversaries to attempt to disable endpoint security in order to evade detection and/or to establish persistence.

> **Important:** Enabling the **Sensor tamper prevention** policy setting does not block uninstallation of the sensor on your hosts. To prevent unauthorized uninstallation of the sensor, enable the **Uninstall and maintenance protection** sensor update policy setting for your hosts. Fore more info, see Managing sensor maintenance and uninstallation.

Windows: When enabled, it protects the sensor-related files, folders, and registry objects from renaming or deletion.

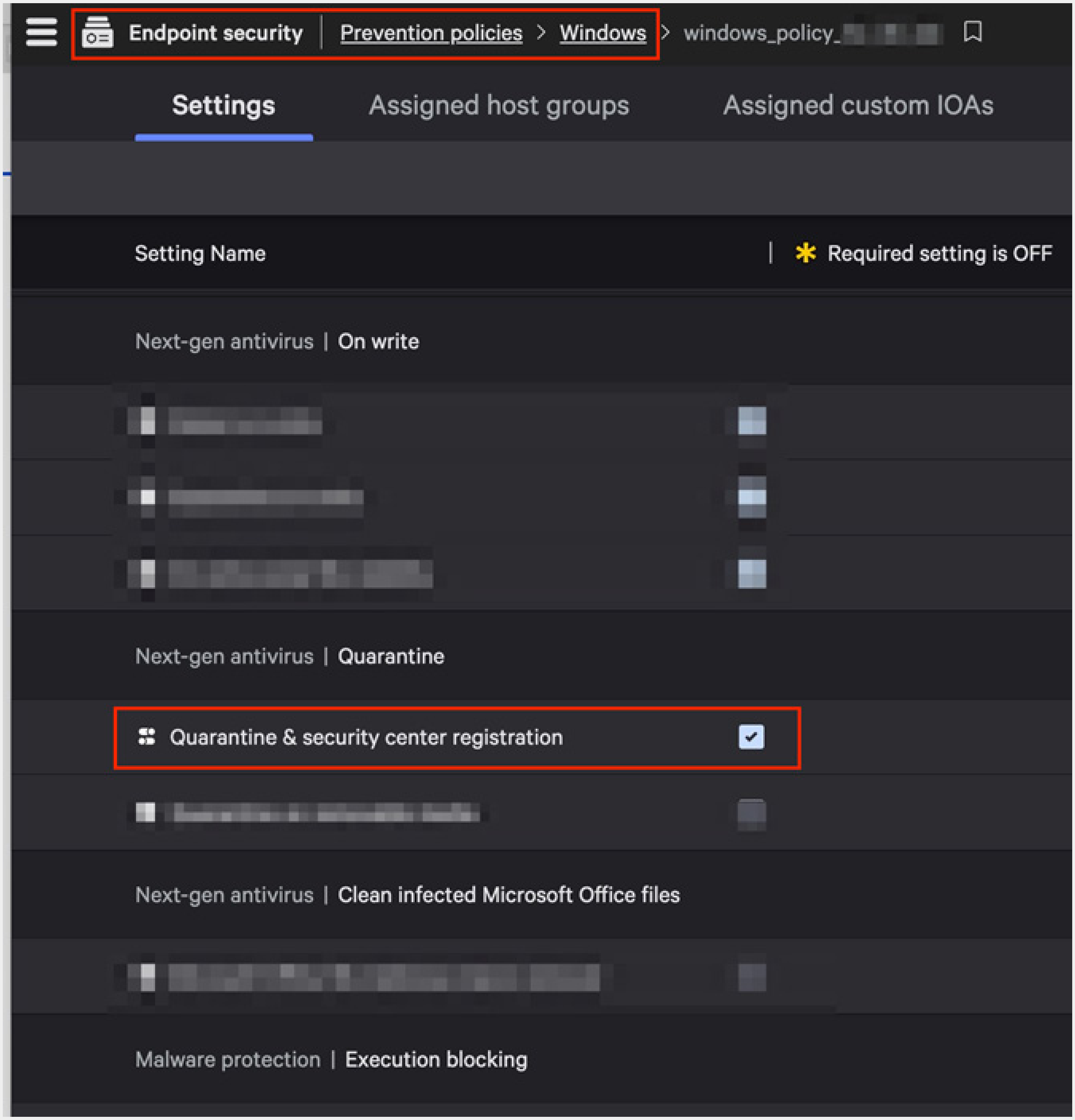
macOS: When enabled, it protects the sensor-related files and folders from modification, renaming, or deletion.

Linux: When enabled, it protects additional sensor resources, such as memory and BPF resources, from modification.

> **Tip:** To use utility tools like `bpftool` on Linux hosts with with **Sensor tamper prevention** enabled, ensure that the tools have read-only access to the BPF maps.

Figure 2. Sensor Tamper Prevention

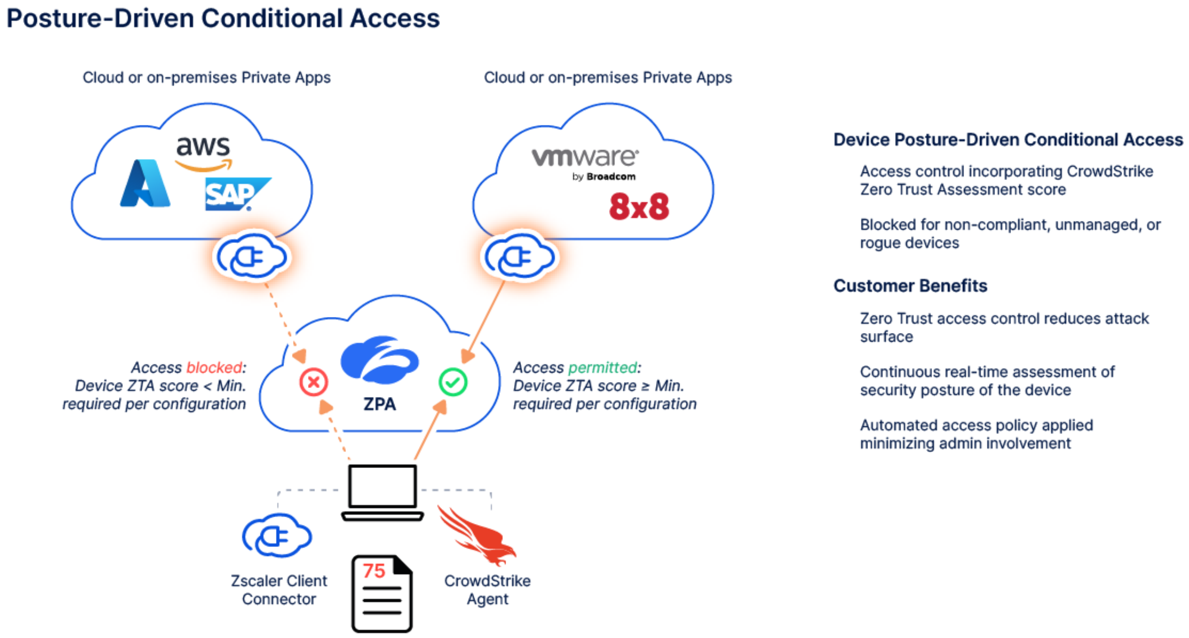
Zscaler recommends enabling the **Quarantine & security center registration** option when using Windows.


Endpoint security
Prevention policies
Windows
windows_policy_[redacted]
Settings
Assigned host groups
Assigned custom IOAs
Setting Name
Required setting is OFF
Next-gen antivirus | On write
Next-gen antivirus | Quarantine
Next-gen antivirus | Clean infected Microsoft Office files
Malware protection | Execution blocking

Quarantine & security center registration ☑

Figure 1. Quarantine & security center registration

The following diagram shows a conceptualization of the integration.



Posture-Driven Conditional Access

Cloud or on-premises Private Apps
aws
SAP
Cloud or on-premises Private Apps
vmware by Broadcom
8x8
Access blocked: Device ZTA score < Min. required per configuration
ZPA
Access permitted: Device ZTA score ≥ Min. required per configuration
Zscaler Client Connector
75
CrowdStrike Agent

Device Posture-Driven Conditional Access

Access control incorporating CrowdStrike Zero Trust Assessment score

Blocked for non-compliant, unmanaged, or rogue devices

Customer Benefits

Zero Trust access control reduces attack surface

Continuous real-time assessment of security posture of the device

Automated access policy applied minimizing admin involvement

Figure 1. High-level overview

Configuring CrowdStrike ZTA Integration in the CrowdStrike Tenant

Currently, to integrate with Zscaler, you must contact the CrowdStrike Support team to turn on a ZTA feature flag in your CrowdStrike tenant.

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

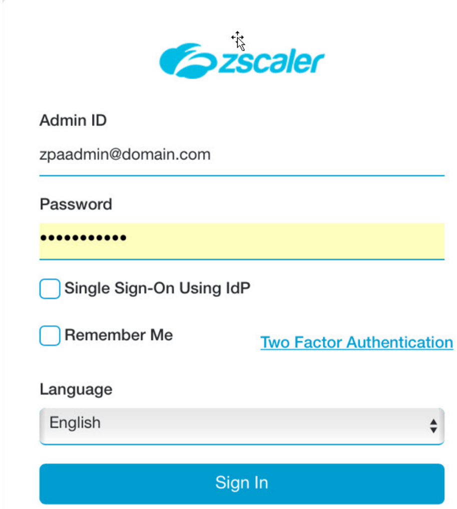
Before proceeding further, reach out to support@crowdstrike.com to turn on this flag.

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

Configuring ZPA

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

Log In to ZPA Admin Portal



Admin ID

zpaadmin@domain.com

Password

••••••••••••

□ Single Sign-On Using IdP

□ Remember Me

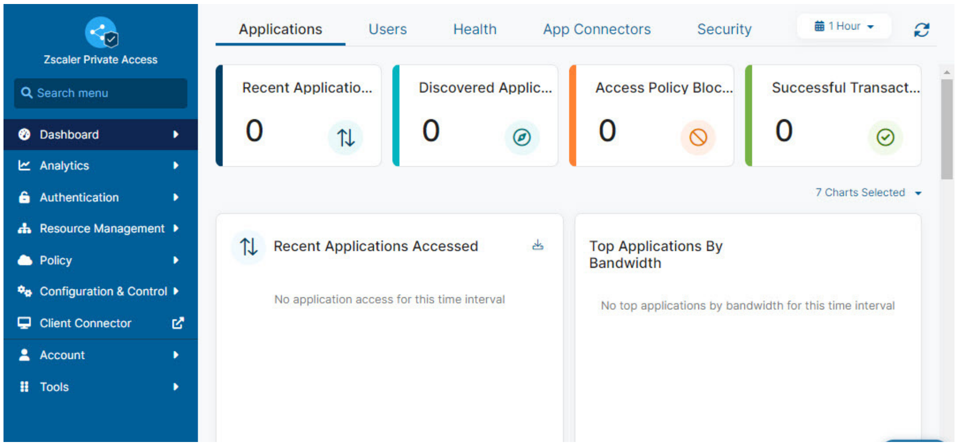
Language

English

Figure 2. Log in to ZPA Admin Portal

Go to Zscaler Client Connector

Click the **Client Connector** icon to access the Zscaler Client Connector.



Recent Applicatio...	Discovered Applic...	Access Policy Bloc...	Successful Transact...
0	0	0	0

Recent Applications Accessed

No application access for this time interval

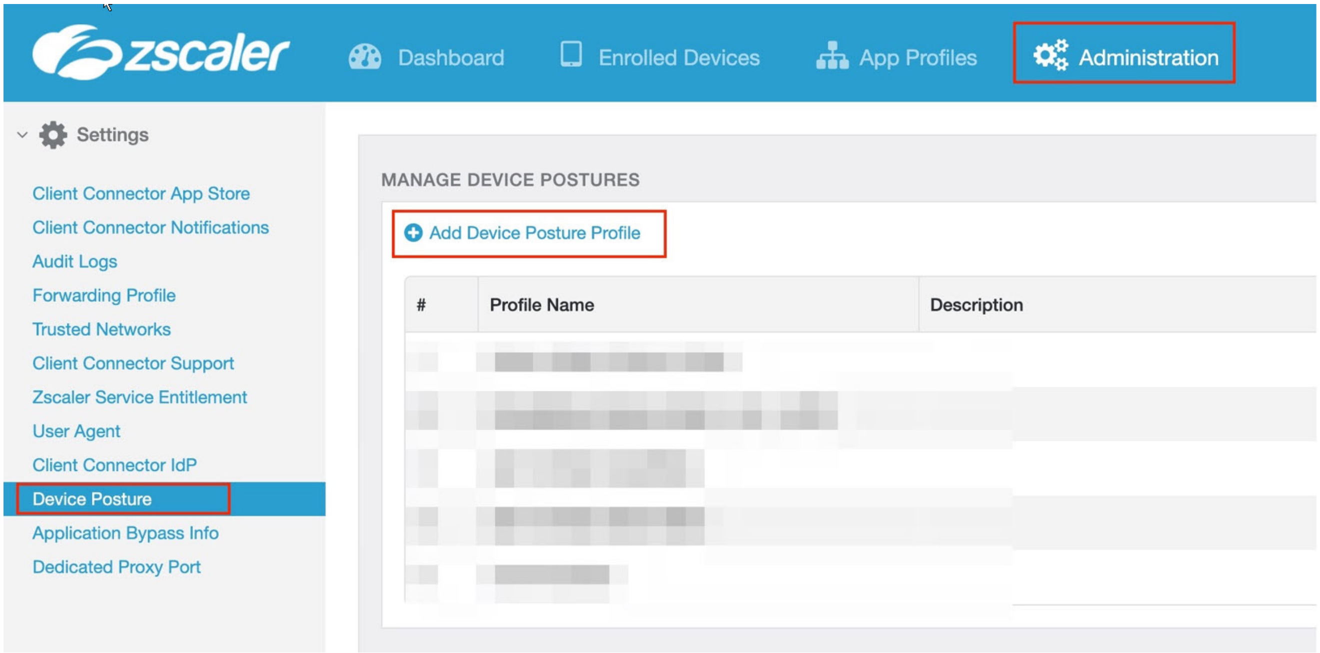
Top Applications By Bandwidth

No top applications by bandwidth for this time interval

Figure 3. Click the Client Connector icon

Create New Posture Profile

Log in to the Zscaler Client Connector Portal and go to **Administration** > **Device Posture**. Then click **Add Device Posture Profile**.



#	Profile Name	Description
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	

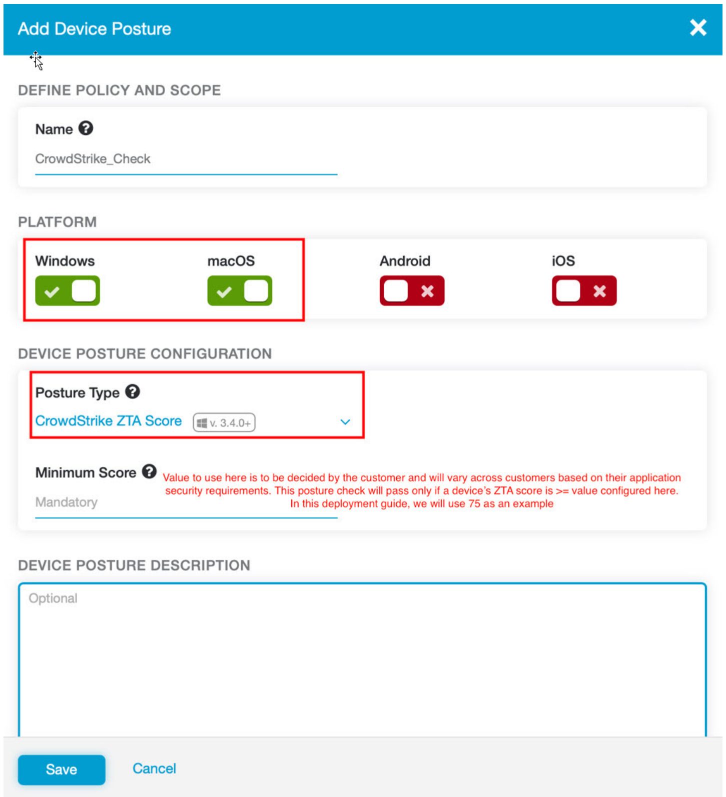
Figure 4. Add a device posture profile

Add a New CrowdStrike ZTA Posture Profile

Complete the following steps:

1. Enter a **Name** for this policy.
2. Select only **Windows** and **macOS**.
3. Click the **Posture Type** drop-down menu.
4. Select **CrowdStrike ZTA Score**.
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. You can set up access policies to allow or deny application access based on whether the posture check passes or fails.



DEFINE POLICY AND SCOPE

Name: CrowdStrike_Check

PLATFORM

Windows	macOS	Android	iOS
✓	✓	✕	✕

DEVICE POSTURE CONFIGURATION

Posture Type: CrowdStrike ZTA Score v. 3.4.0+

Minimum Score: Mandatory

Value to use here is to be decided by the customer and will vary across customers based on their application security requirements. This posture check will pass only if a device's ZTA score is >= value configured here. In this deployment guide, we will use 75 as an example

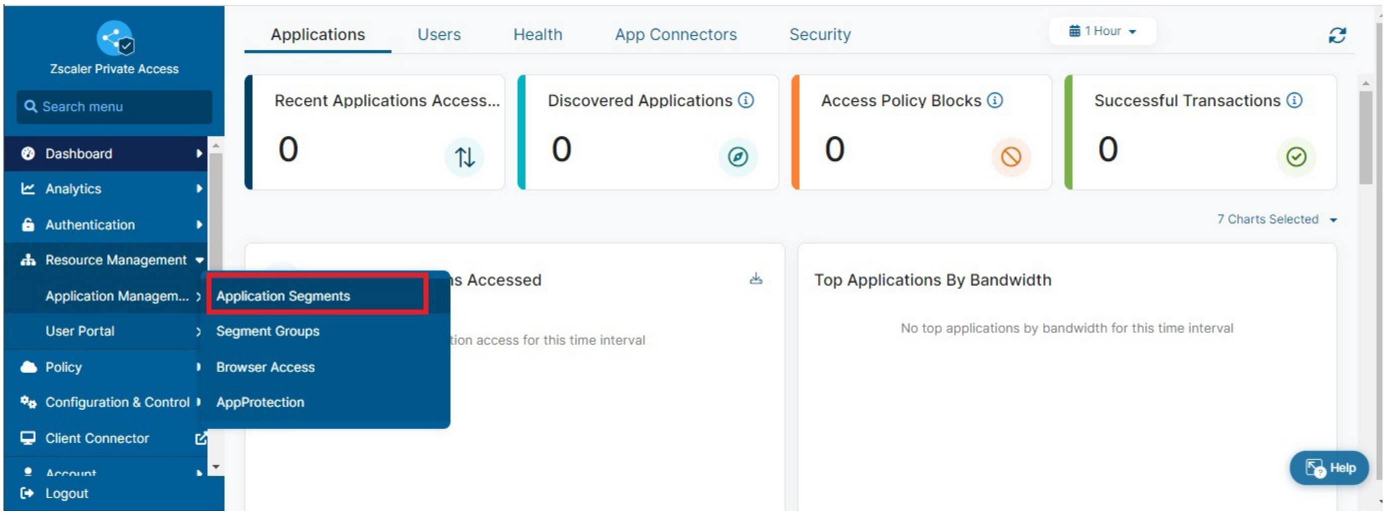
DEVICE POSTURE DESCRIPTION

Optional

Figure 5. Add a CrowdStrike ZTA posture profile

Decide Which Applications Need Conditional Access Based on ZTA

From the ZPA Admin Portal, go to **Resource Management** > **Application Management** > **Application Segments**. This page lists applications that are 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 an end device's ZTA score.



Recent Applications Access...	Discovered Applications	Access Policy Blocks	Successful Transactions
0	0	0	0

...s Accessed

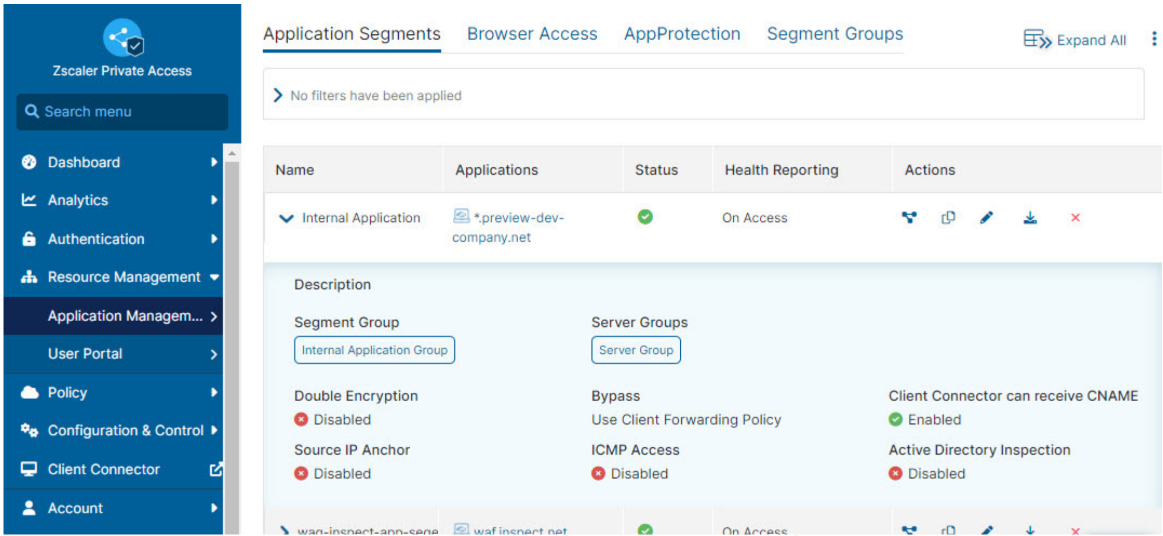
...tion access for this time interval

Top Applications By Bandwidth

No top applications by bandwidth for this time interval

Figure 6. Go to Application Segments

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



No filters have been applied

Name	Applications	Status	Health Reporting	Actions
Internal Application	*.preview-dev-company.net	✓	On Access	
waa-inspect-app-sege	waf inspect net	✓	On Access	

Description

Segment Group: Internal Application Group

Server Groups: Server Group

Double Encryption: Disabled

Bypass: Use Client Forwarding Policy

Client Connector can receive CNAME: Enabled

Source IP Anchor: Disabled

ICMP Access: Disabled

Active Directory Inspection: Disabled

Figure 7. Decide which application has conditional access (based on the ZTA score)

Set Up an Access Policy

From the ZPA Admin Portal, go to **Policy** > **Access Policy**.

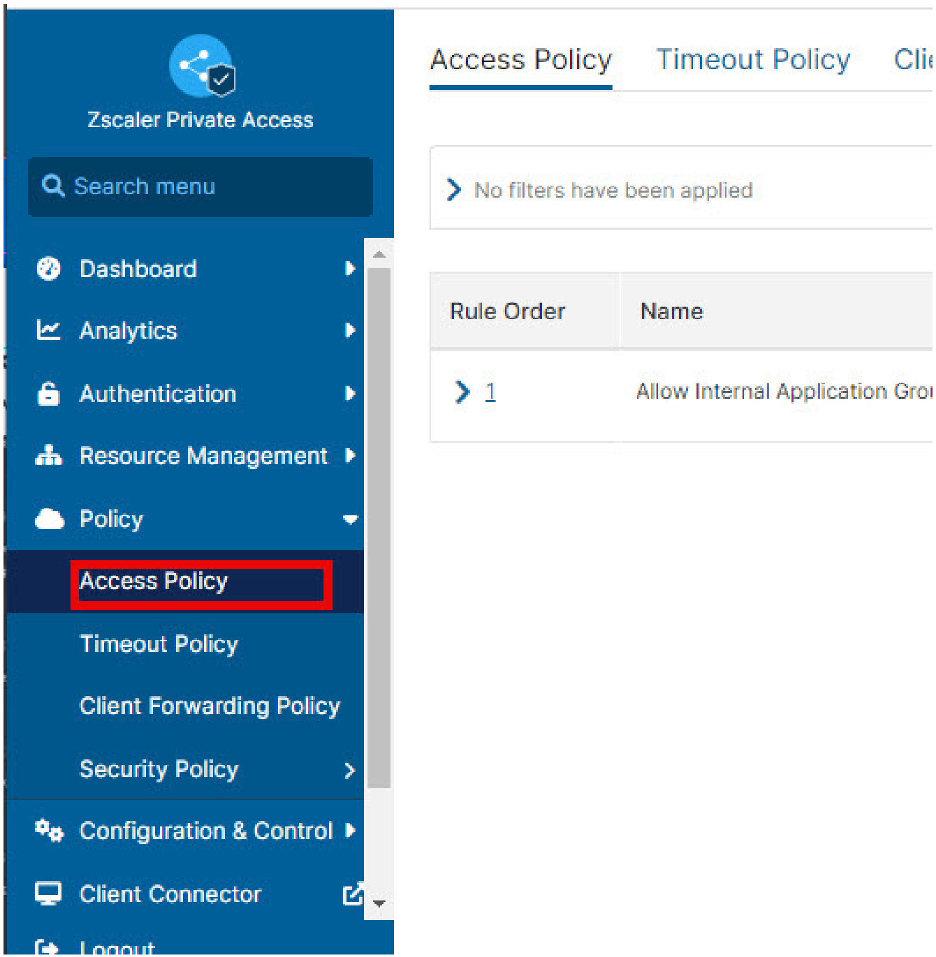


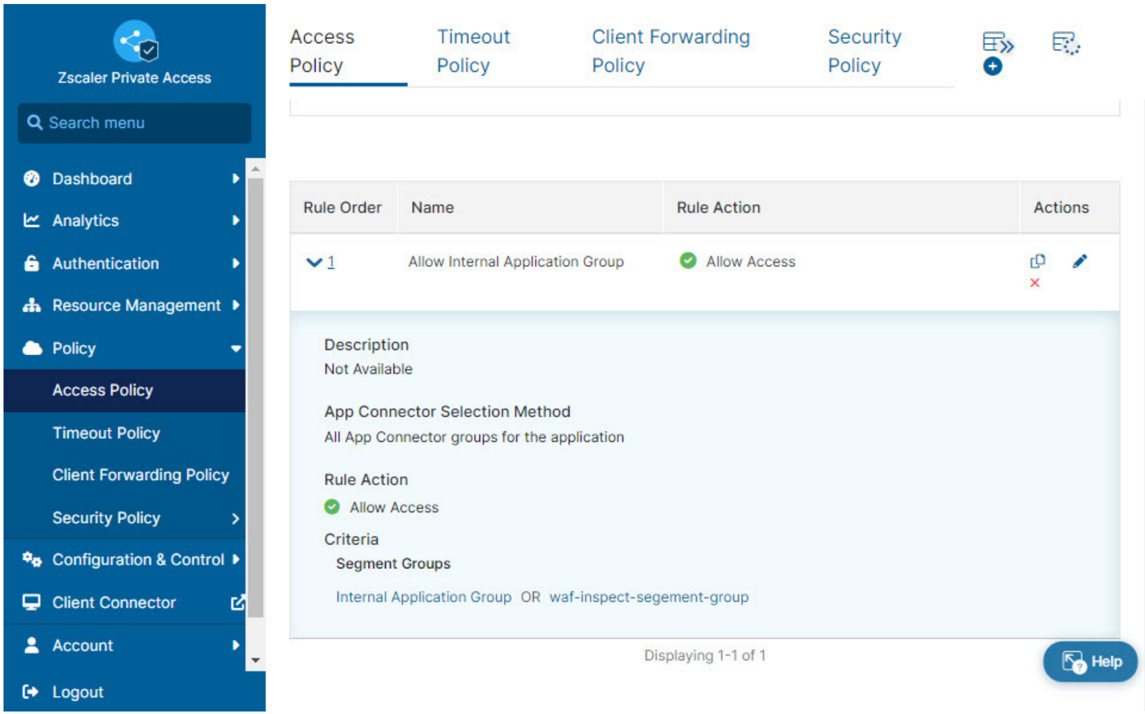
Figure 8. Open the access policy configuration dialog

Tie the Posture Profile to the Access Policy

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

You can set up 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) notification message is shown to the end users when application access is allowed or denied, informing them about policy evaluation.

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



Rule Order	Name	Rule Action	Actions
1	Allow Internal Application Group	Allow Access	

Description
Not Available

App Connector Selection Method
All App Connector groups for the application

Rule Action
Allow Access

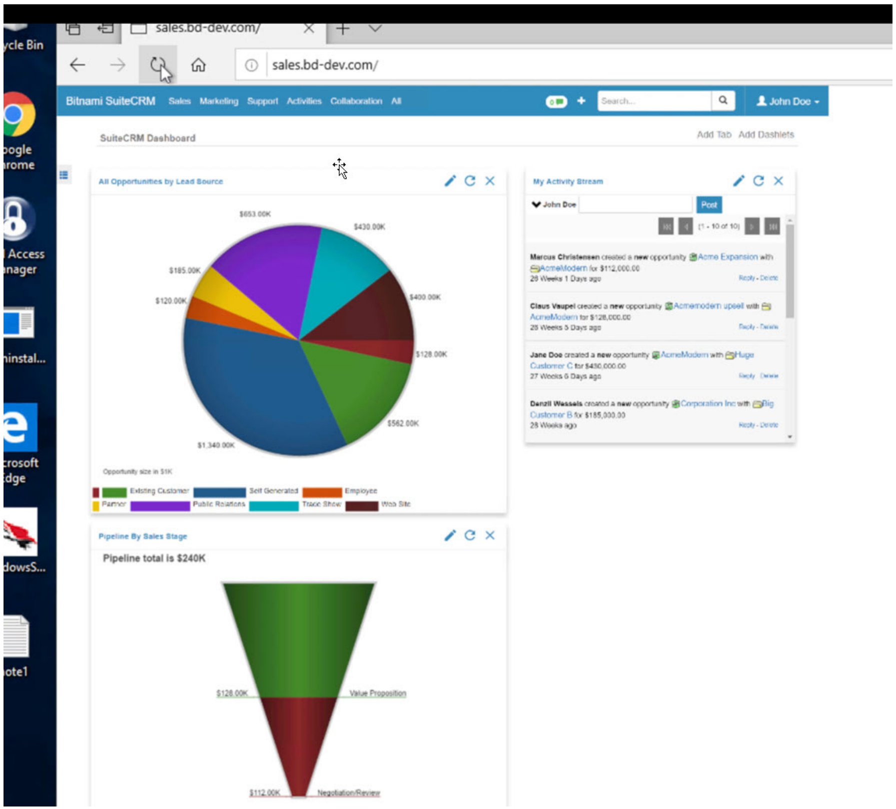
Criteria
Segment Groups
Internal Application Group OR waf-inspect-segement-group

Displaying 1-1 of 1

Figure 9. Set up an access policy

Verify ZTA-Based Conditional Access from an Endpoint

Ensure that you are logged in to ZPA with Zscaler Client Connector version 3.4 or later, and access the application referenced in the previous step's access policy. The app is accessible from the endpoint if the device's CrowdStrike-calculated ZTA score is greater than or equal to the value configured in the posture profile. Otherwise, the access is blocked by ZPA.



Marcus Christensen created a new opportunity Acme Expansion with AcmeModern for $112,000.00
28 Weeks 1 Days ago

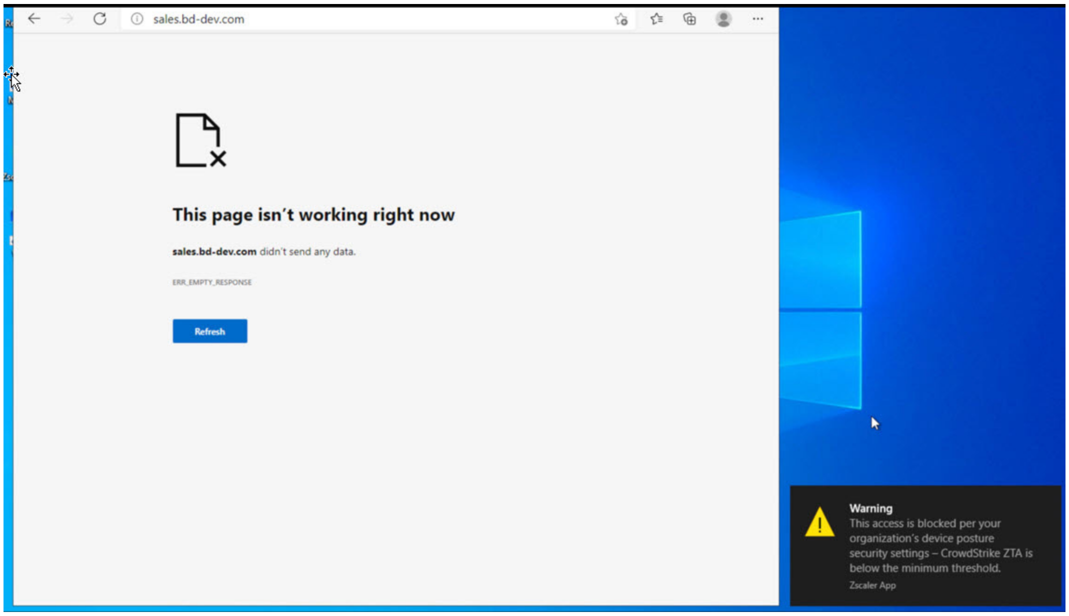
Claus Vaupel created a new opportunity Acmemodern upsell with AcmeModern for $128,000.00
28 Weeks 5 Days ago

Jane Doe created a new opportunity AcmeModern with Huge Customer C for $430,000.00
27 Weeks 6 Days ago

Denzil Wessels created a new opportunity Corporation Inc with Big Customer B for $185,000.00
28 Weeks ago

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

If access is blocked, the following message is displayed.



This page isn't working right now

sales.bd-dev.com didn't send any data.

ERR_EMPTY_RESPONSE

Warning
This access is blocked per your organization's device posture security settings – CrowdStrike ZTA is below the minimum threshold.
Zscaler App

Figure 11. Access blocked from an endpoint with a ZTA score less than the configured value in the posture profile

Use Case 2: ZIA Posture Check Integration with CrowdStrike ZTA

In this use case:

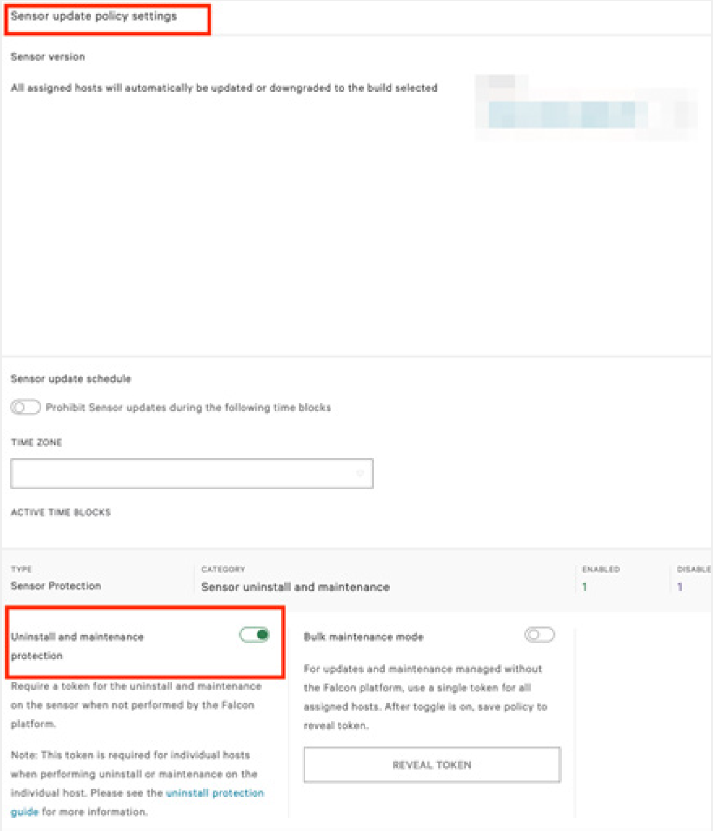
- CrowdStrike calculates a ZTA security score from 1 to 100 for each host. A higher score indicates a better security posture for the host.
- Security scores are derived from two distinct assessment sources:
  - OS settings: Settings that track native OS security options, firmware availability, and CVE mitigations.
  - CrowdStrike Falcon sensor settings (Windows and macOS): CrowdStrike Falcon sensor configurations that track RFM status as well as prevention and Real-Time Response policies.
- ZIA uses CrowdStrike's ZTA score (also known as a device posture score) and allows only compliant endpoints to access selected applications. ZIA checks for any changes to the CrowdStrike's device posture score because the score can change over time. ZTA check integration is supported currently for Windows and macOS endpoints.
- ZIA achieves conditional access based on Device Trust level. Device Trust levels are determined by ZIA posture profiles that, in turn, reference device level posture check profiles. ZIA administrators can simply specify that a minimum ZTA score is needed for the endpoint to grant access to resources that are referenced via various ZIA policies (such as URL Filtering policy, Firewall policy, File Control policy, Cloud Apps policy, or SSL Inspection policy). You can combine the ZTA score threshold requirement with other device posture policies to allow only compliant devices to access resources through ZIA.

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

   You can reach the CrowdStrike Support team at support@crowdstrike.com. Any device trying to access applications over ZPA must be running Zscaler Client Connector version 3.4 or later for this integration to work. The CrowdStrike sensor must be version 6.20 or later.
2. The data.zta file is regularly deleted and recreated for security reasons, typically during system reboots or when updating score changes. This process takes about 15 seconds to one minute but endpoint system performance, network bandwidth, CrowdStrike backend processing delays, and other factors can affect the update time of this file. If a partner app accesses the ZTA data file during these delays, it could find it empty, partially filled, or missing—which would prevent the partner app from retrieving the ZTA score. In this case, the endpoint might be deemed untrustworthy, and partner products blocked from access to essential services. To avoid this issue, CrowdStrike implemented a ZTA caching feature. Contact CrowdStrike Support team to enable the ZTA caching feature on your CID. To learn more, refer to the CrowdStrike documentation.

If interoperability issues arise, update your CrowdStrike policy's sensor visibility exclusions to account for Zscaler Client Connector-related details and re-test. To learn more, see Zscaler Client Connector Processes to Allowlist. (government agencies, see Zscaler Client Connector Processes to Allowlist).

As a best practice, Zscaler recommends turning on **Uninstall and maintenance protection** via the CrowdStrike Sensor Update Policy settings, and enabling Sensor Tamper Prevention via CrowdStrike Prevention Policy settings.



Sensor update policy settings

Sensor version

All assigned hosts will automatically be updated or downgraded to the build selected

Sensor update schedule

○ Prohibit Sensor updates during the following time blocks

TIME ZONE

ACTIVE TIME BLOCKS

TYPE	CATEGORY	ENABLED	DISABLE
Sensor Protection	Sensor uninstall and maintenance	1	1

Uninstall and maintenance protection ●

Require a token for the uninstall and maintenance on the sensor when not performed by the Falcon platform.

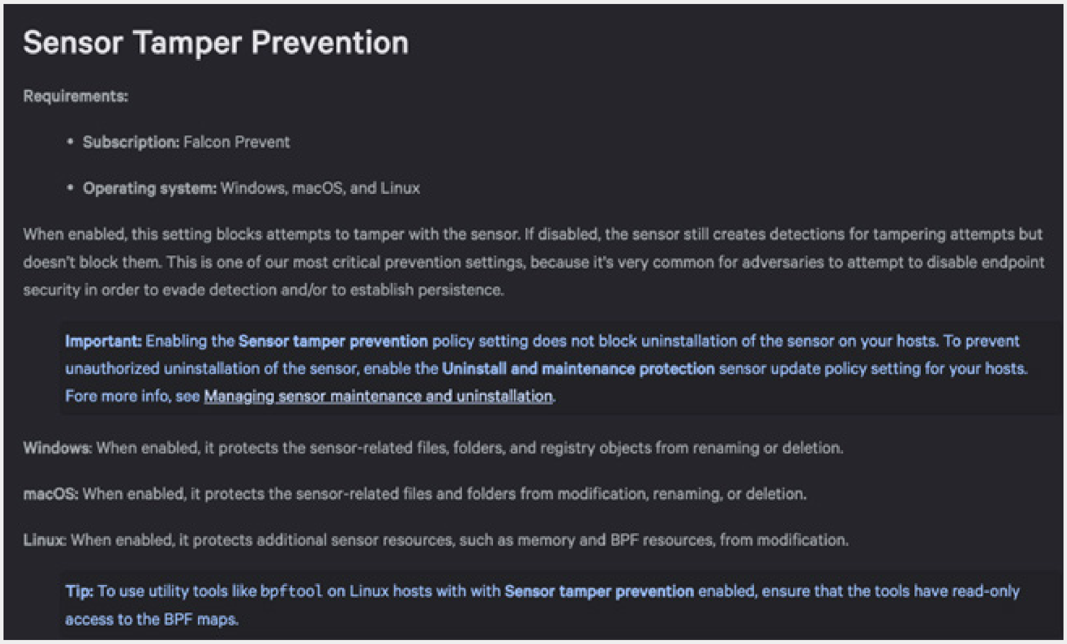
Note: This token is required for individual hosts when performing uninstall or maintenance on the individual host. Please see the uninstall protection guide for more information.

Bulk maintenance mode ○

For updates and maintenance managed without the Falcon platform, use a single token for all assigned hosts. After toggle is on, save policy to reveal token.

REVEAL TOKEN

Figure 1. Uninstall and maintenance protection



Sensor Tamper Prevention

Requirements:

- **Subscription:** Falcon Prevent
- **Operating system:** Windows, macOS, and Linux

When enabled, this setting blocks attempts to tamper with the sensor. If disabled, the sensor still creates detections for tampering attempts but doesn't block them. This is one of our most critical prevention settings, because it's very common for adversaries to attempt to disable endpoint security in order to evade detection and/or to establish persistence.

> **Important:** Enabling the **Sensor tamper prevention** policy setting does not block uninstallation of the sensor on your hosts. To prevent unauthorized uninstallation of the sensor, enable the **Uninstall and maintenance protection** sensor update policy setting for your hosts. Fore more info, see Managing sensor maintenance and uninstallation.

Windows: When enabled, it protects the sensor-related files, folders, and registry objects from renaming or deletion.

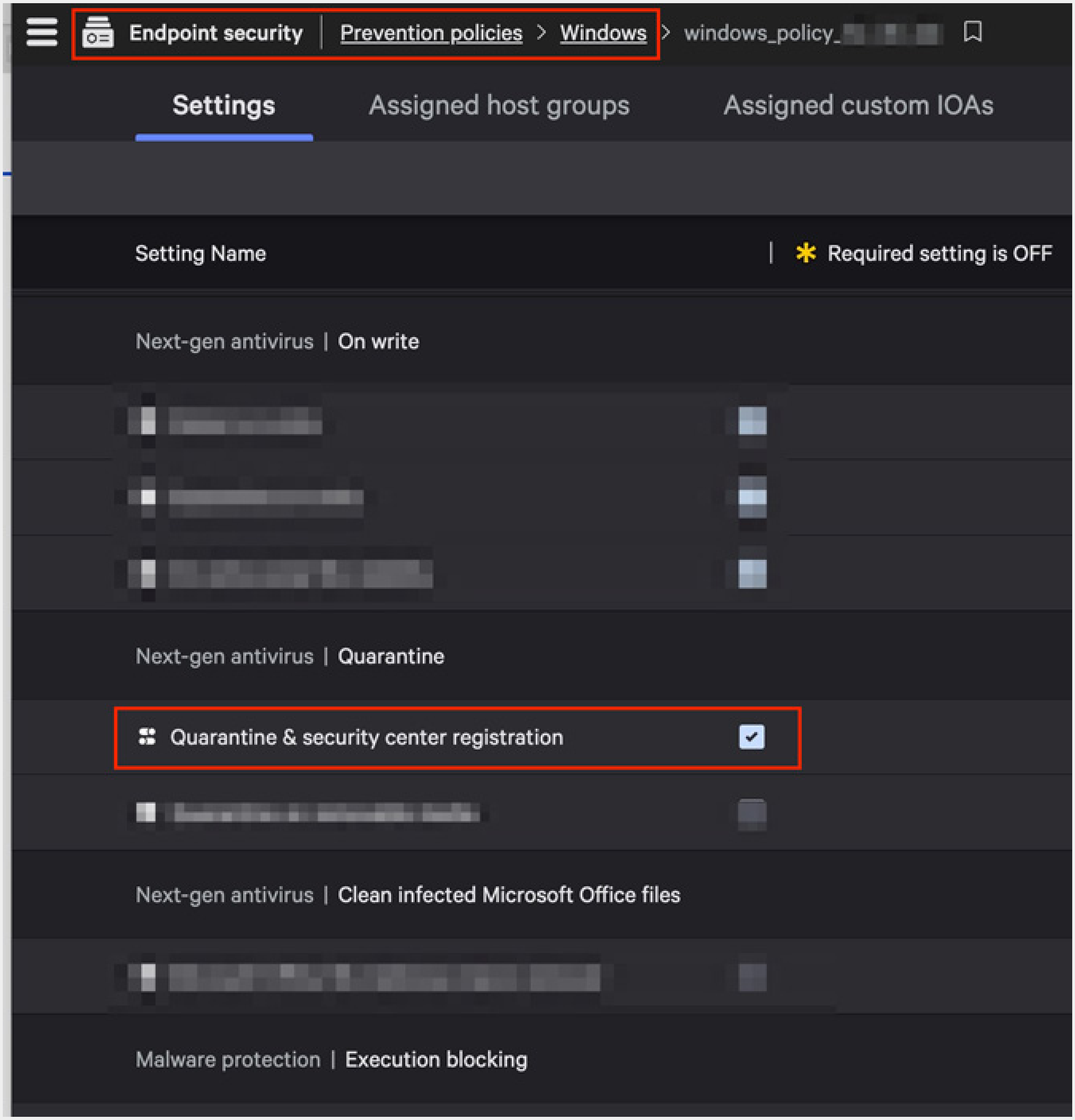
macOS: When enabled, it protects the sensor-related files and folders from modification, renaming, or deletion.

Linux: When enabled, it protects additional sensor resources, such as memory and BPF resources, from modification.

> **Tip:** To use utility tools like `bpftool` on Linux hosts with with **Sensor tamper prevention** enabled, ensure that the tools have read-only access to the BPF maps.

Figure 2. Sensor Tamper Prevention

Zscaler recommends enabling the **Quarantine & security center registration** option when using Windows.



Endpoint security | Prevention policies > Windows > windows_policy_[redacted]

Settings | Assigned host groups | Assigned custom IOAs

Setting Name | * Required setting is OFF

Next-gen antivirus | On write

Next-gen antivirus | Quarantine

Quarantine & security center registration ☑

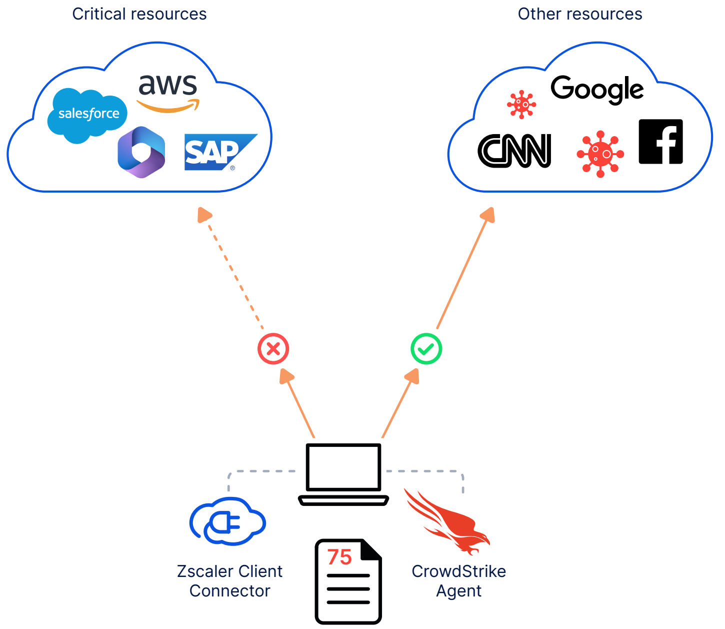
Next-gen antivirus | Clean infected Microsoft Office files

Malware protection | Execution blocking

Figure 1. Quarantine & security center registration

The following diagram shows a conceptualization of the integration.

Posture-Driven Conditional Access



Device Posture-Driven Conditional Access

Access control incorporating CrowdStrike Zero Trust Assessment score

Blocked for non-compliant, unmanaged, or rogue devices

Customer Benefits

Extending Zero Trust access to ZIA to restrict access to sensitive resources, effectively reducing attack surfaces

Continuous real-time verification of trust based on changing posture of the device

Automated access policy applied minimizing admin involvement

Figure 12. High-level overview

Configuring CrowdStrike ZTA Integration in the CrowdStrike Tenant

Currently, to integrate with Zscaler, you must contact the CrowdStrike Support team to turn on a ZTA feature flag in your CrowdStrike tenant.

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

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

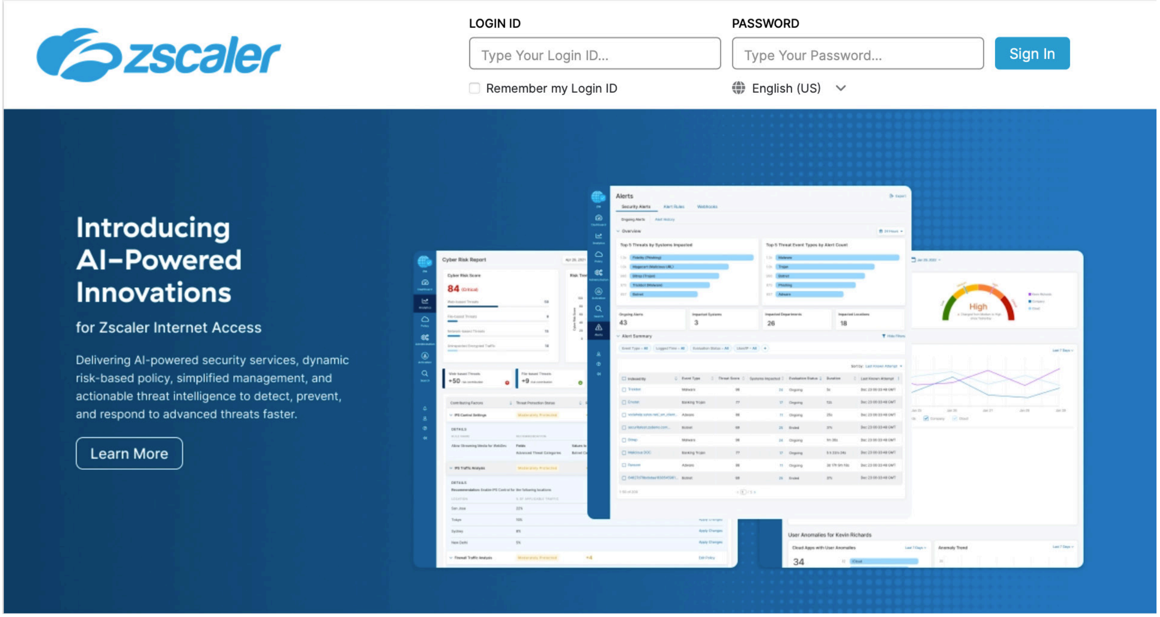
Also, ensure that you use Zscaler Client Connector version 3.4 or later on the end host from which you are testing. CrowdStrike sensor version must be 6.20 or later.

Configuring ZIA

This guide assumes that you have a working ZIA set up and provides instructions to integrate ZTA-based conditional access into your existing ZIA deployment.

Log In to ZIA Admin Portal

Log in to the ZIA Admin Portal as an administrator.



Introducing AI-Powered Innovations

for Zscaler Internet Access

Delivering AI-powered security services, dynamic risk-based policy, simplified management, and actionable threat intelligence to detect, prevent, and respond to advanced threats faster.

Figure 13. Log in to ZIA Admin Portal

Go to Zscaler Client Connector

Click the **Zscaler Client Connector Portal** link under the **Policy** section to access the Zscaler Client Connector Portal.

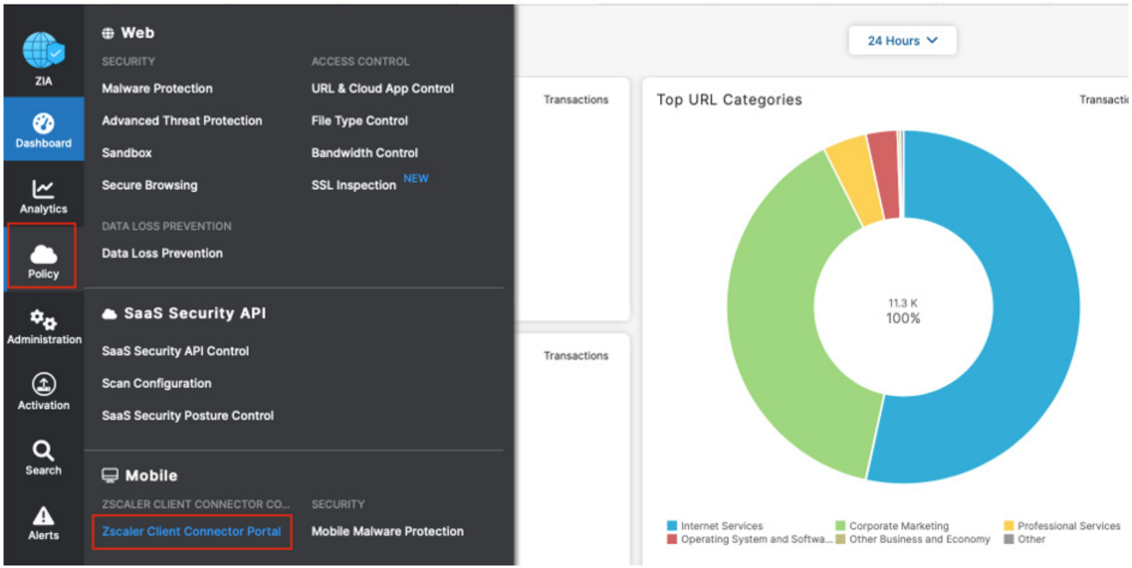


Figure 14. Click the Zscaler Client Connector Portal

Create New Posture Profile

Log in to the Zscaler Client Connector Portal and go to **Administration** > **Device Posture** > **Add Device Posture Profile**.

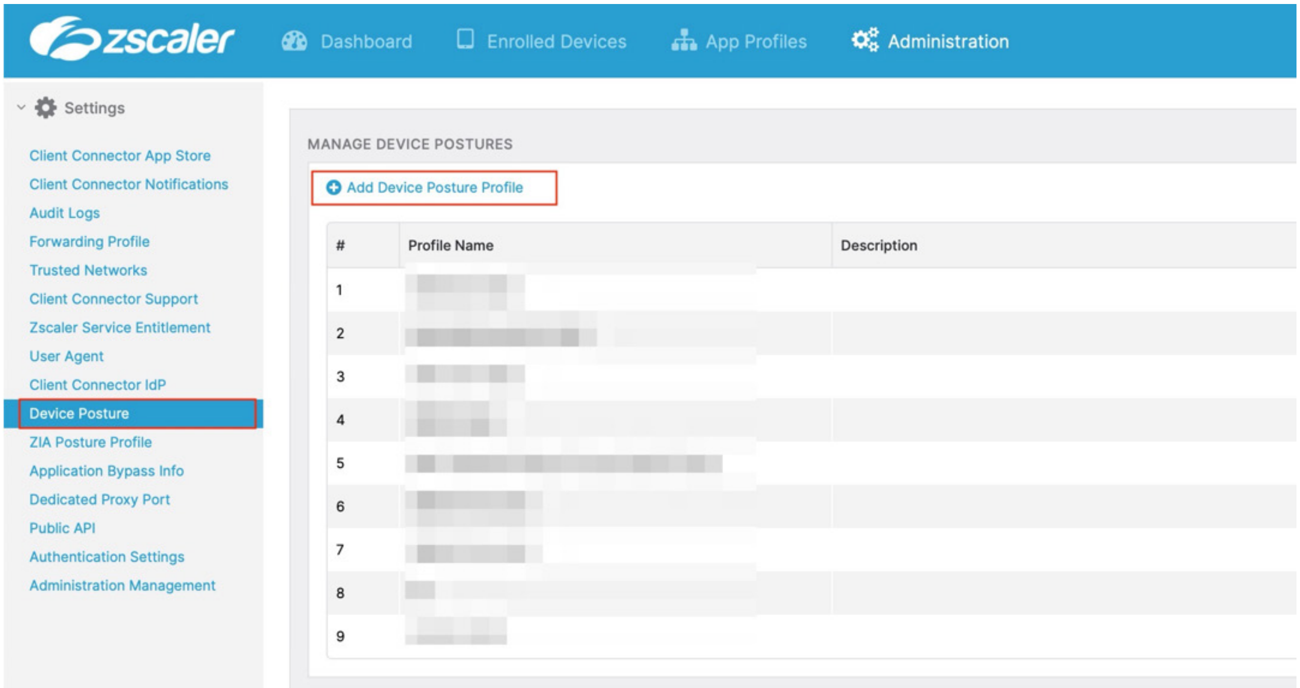


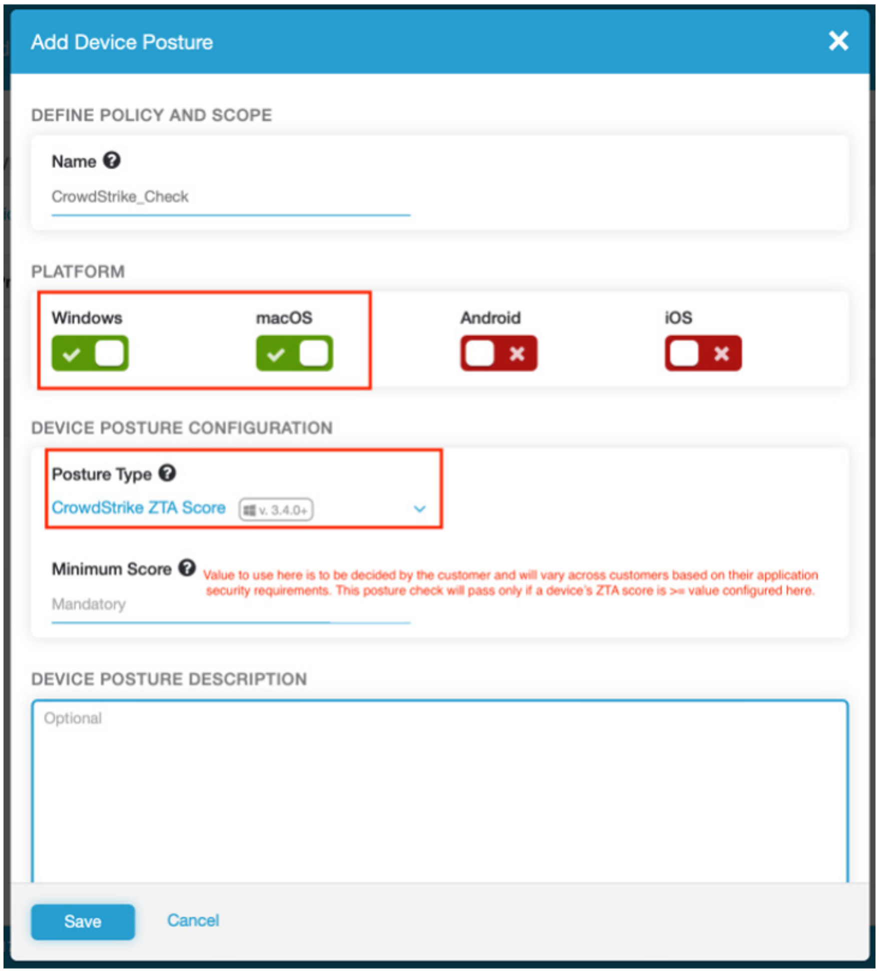
Figure 15. Add a device posture profile

Add a New CrowdStrike ZTA Posture Profile

To add a new CrowdStrike ZTA posture profile:

1. Enter a **Name** for this policy.
2. Select only **Windows**, **macOS**, or both.
3. Select **CrowdStrike ZTA Score** under the **Posture Type** drop-down menu.
4. Provide the minimum value for the **CrowdStrike ZTA Score**.
5. Click **Save**.

The device posture check passes if the end device's ZTA score (calculated by CrowdStrike) is greater than or equal to the value configured in this procedure. This device posture profile is, in turn, referenced in a ZIA posture profile to determine the trust bucket or level that a device falls in. You can set up conditional access policies to allow or deny access through ZIA based on device trust levels.



Add Device Posture

DEFINE POLICY AND SCOPE

Name: CrowdStrike_Check

PLATFORM

Windows ✓ macOS ✓ Android ✗ iOS ✗

DEVICE POSTURE CONFIGURATION

Posture Type: CrowdStrike ZTA Score (v. 3.4.0+)

Minimum Score: Mandatory

Value to use here is to be decided by the customer and will vary across customers based on their application security requirements. This posture check will pass only if a device's ZTA score is >= value configured here.

DEVICE POSTURE DESCRIPTION

Optional

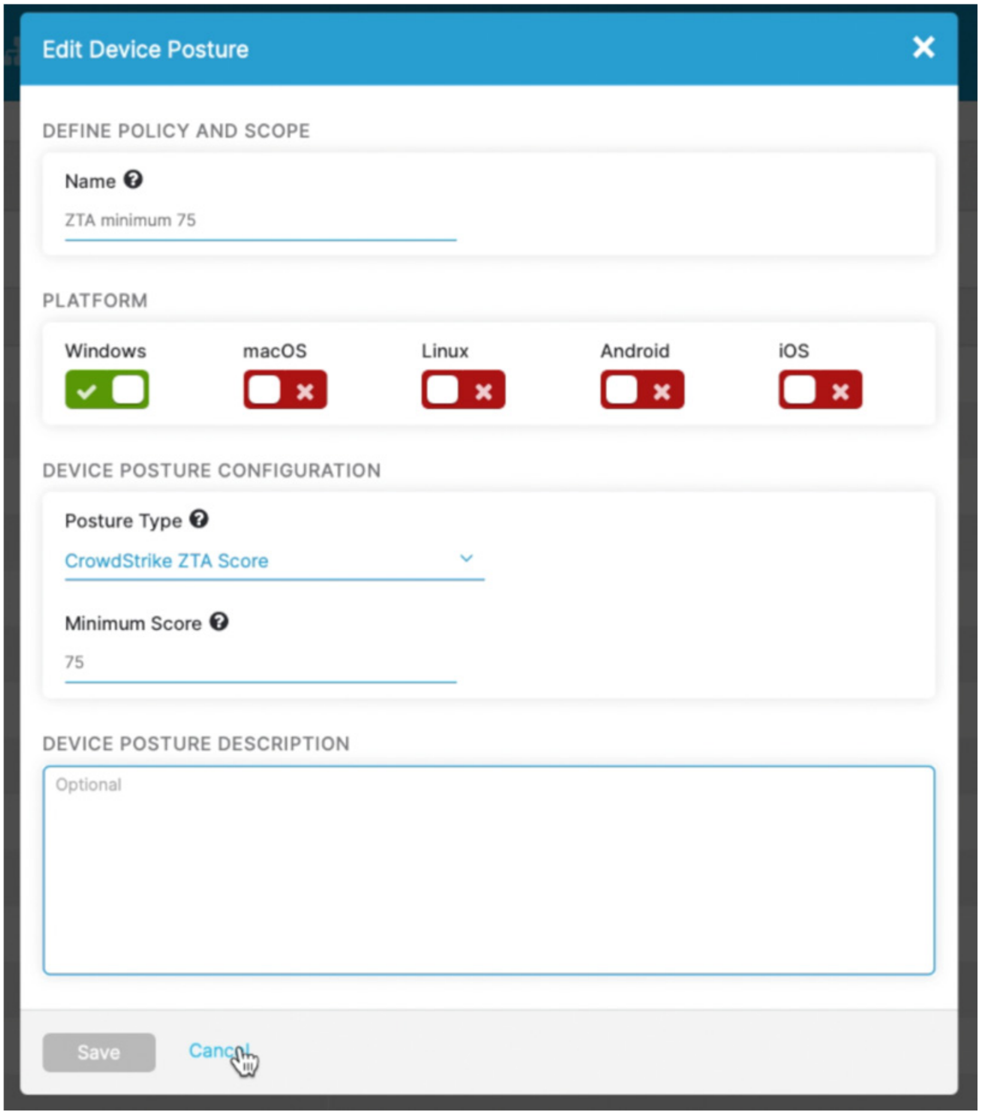
Figure 16. Add a CrowdStrike ZTA posture profile

Multiple Device Posture Profiles Defined Referencing Different ZTA Scores

You can define multiple ZTA-based device posture templates to correspond to different Device Trust levels. As an example, you can set up multiple device posture profiles referencing different ZTA scores.

The following example defines three different device posture profiles, which set the minimum device ZTA threshold scores to be 75, 65, and 50 respectively. These are used for qualifying a device to fall in the High, Medium, Low trust level (respectively) via ZIA posture profile configuration.

The following figure shows the posture based on a ZTA of 75.



Edit Device Posture

DEFINE POLICY AND SCOPE

Name: ZTA minimum 75

PLATFORM

Windows ✓ macOS ☒ Linux ☒ Android ☒ iOS ☒

DEVICE POSTURE CONFIGURATION

Posture Type: CrowdStrike ZTA Score

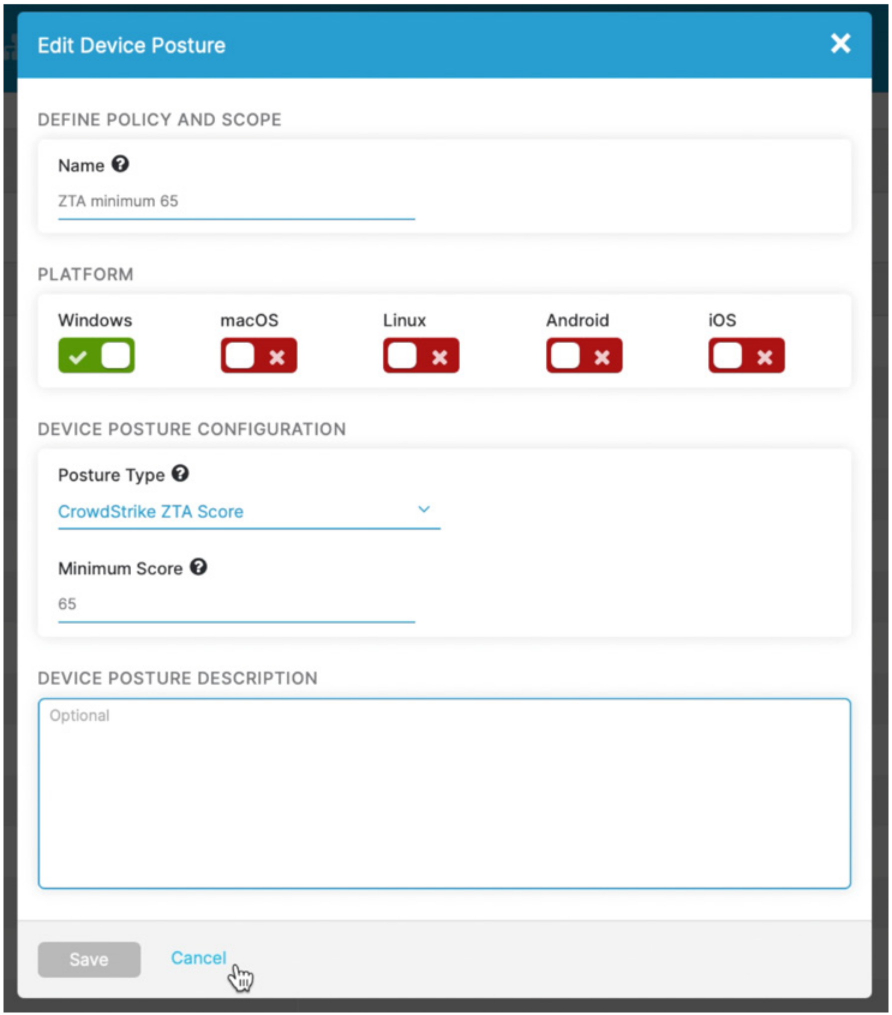
Minimum Score: 75

DEVICE POSTURE DESCRIPTION

Optional

Figure 17. Device posture policy based on 75 ZTA score

The following figure shows the posture based on a ZTA of 65.



Edit Device Posture

DEFINE POLICY AND SCOPE

Name: ZTA minimum 65

PLATFORM

Windows ✓ macOS ✗ Linux ✗ Android ✗ iOS ✗

DEVICE POSTURE CONFIGURATION

Posture Type: CrowdStrike ZTA Score

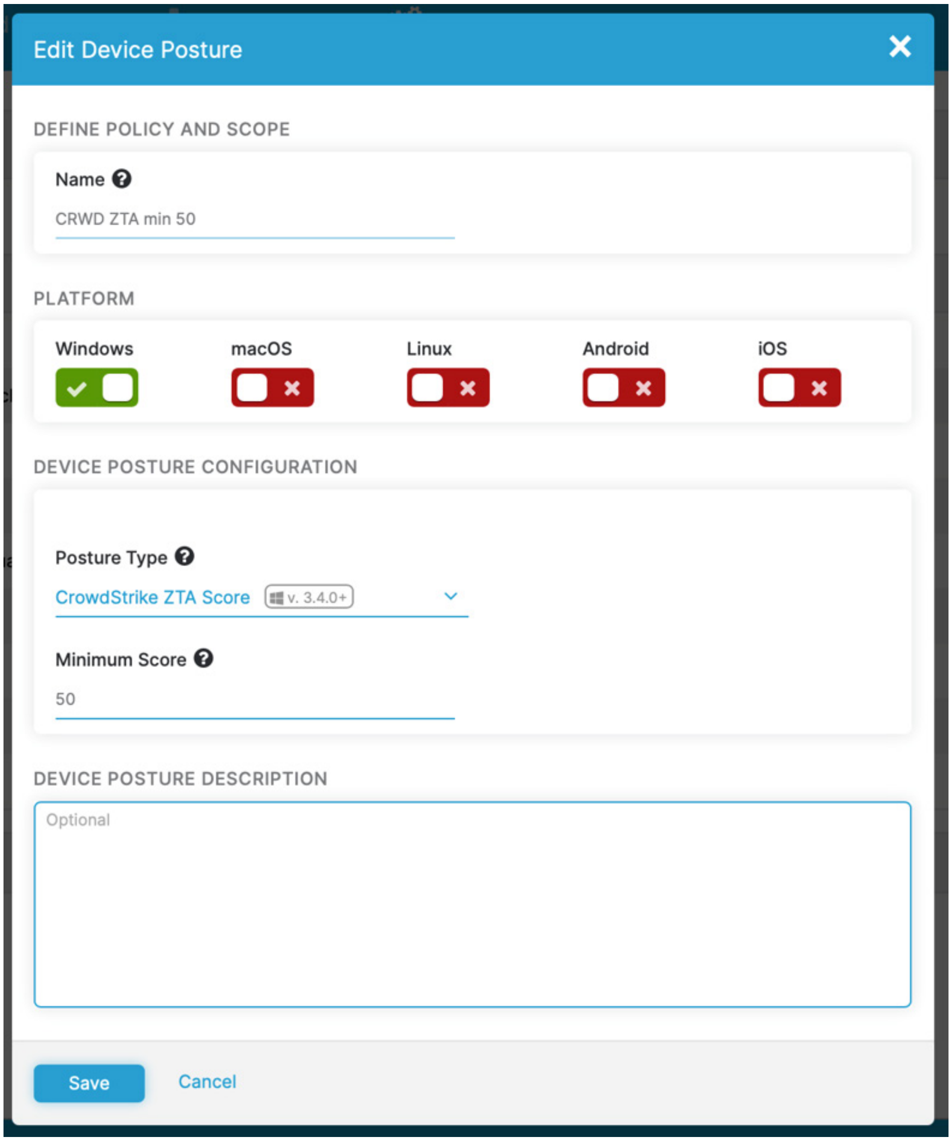
Minimum Score: 65

DEVICE POSTURE DESCRIPTION

Optional

Figure 18. Device posture policy based on 65 ZTA score

The following figure shows the posture based on a ZTA of 50.



Edit Device Posture

DEFINE POLICY AND SCOPE

Name: CRWD ZTA min 50

PLATFORM

Windows ✓ macOS ✗ Linux ✗ Android ✗ iOS ✗

DEVICE POSTURE CONFIGURATION

Posture Type: CrowdStrike ZTA Score v. 3.4.0+

Minimum Score: 50

DEVICE POSTURE DESCRIPTION

Optional

Figure 19. Device posture policy based on 50 ZTA score

Reference the Device Posture Profile in ZIA Posture Profile

In the Zscaler Client Connector Portal, go to **Administration** > **ZIA Posture Profile** > **Add ZIA Posture Profile**.

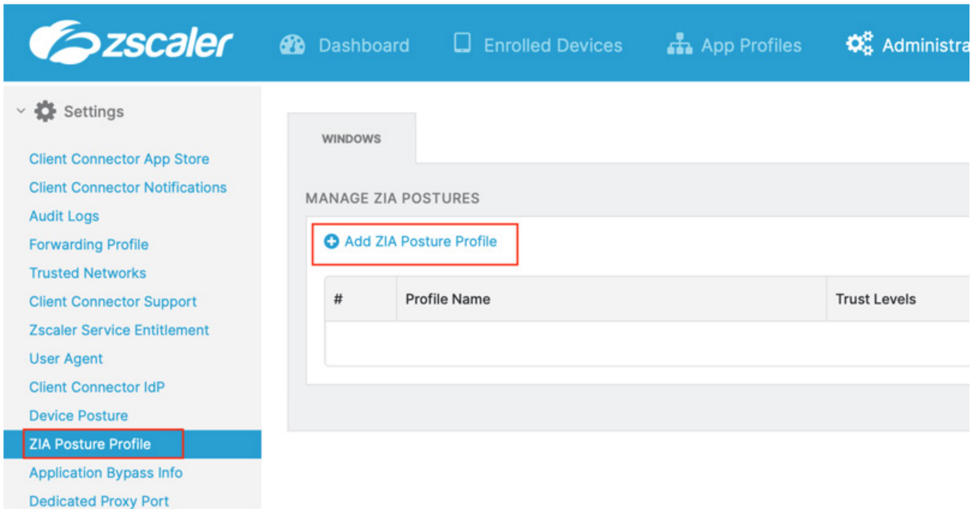


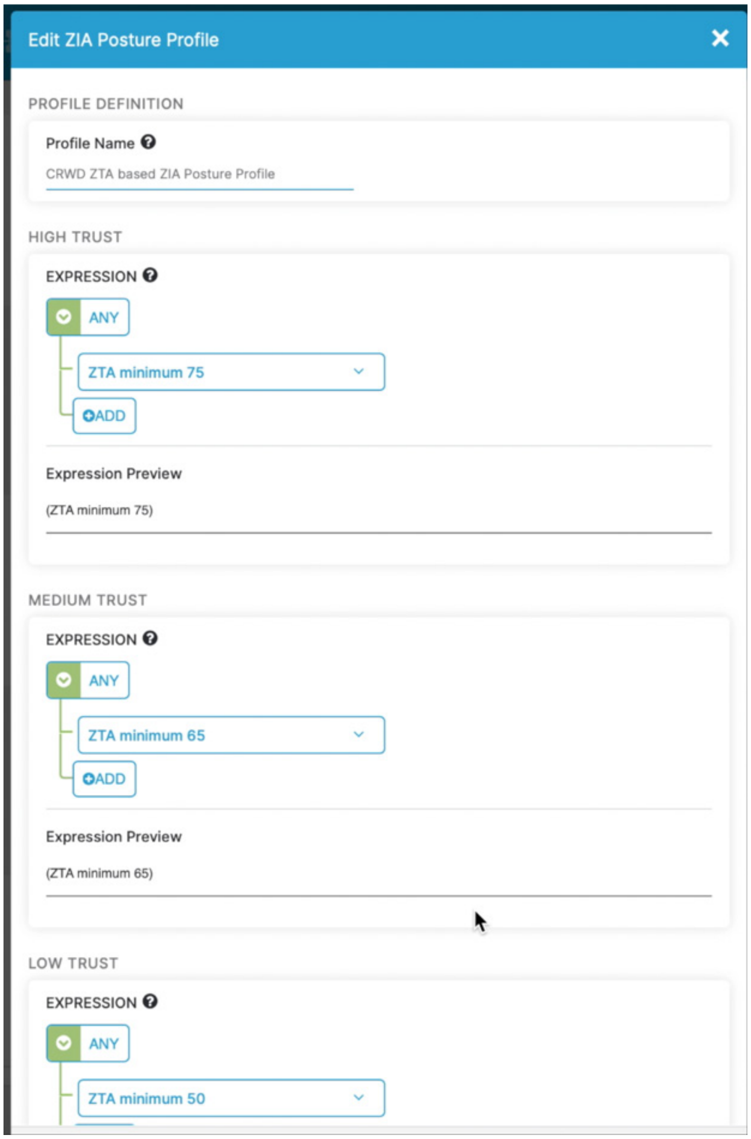
Figure 20. Add a new ZIA Posture Profile

In this new ZIA Posture Profile, you reference the previously created device posture profiles to establish Device Trust criteria.

In the following example, as long as the device's ZTA score is greater than or equal to 75, it falls into the High trust level. A device with a ZTA score greater than or equal to 65 (but less than 75) falls into the Medium trust level. A device with a ZTA score greater than or equal to 50 (but less than 65) falls into the Low trust bucket.

Trust criteria are evaluated in the top-down order, and the evaluation stops at the first match.

The following figure shows the posture based on a ZTA of 65.



Edit ZIA Posture Profile

PROFILE DEFINITION

Profile Name: CRWD ZTA based ZIA Posture Profile

HIGH TRUST

EXPRESSION: ANY — ZTA minimum 75

Expression Preview: (ZTA minimum 75)

MEDIUM TRUST

EXPRESSION: ANY — ZTA minimum 65

Expression Preview: (ZTA minimum 65)

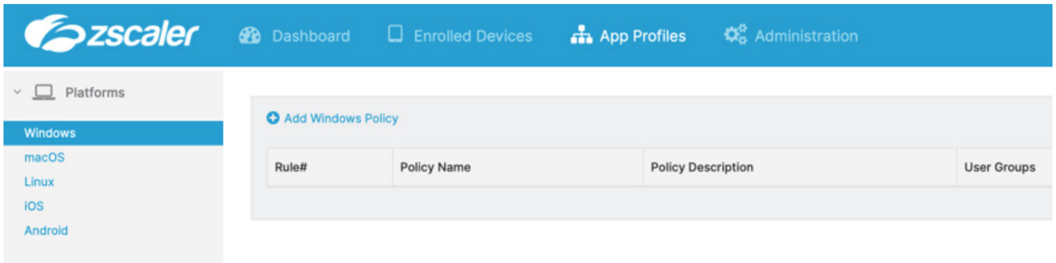
LOW TRUST

EXPRESSION: ANY — ZTA minimum 50

Figure 21. Add a new ZIA Posture Profile referencing previously created device posture profiles

Create an App Profile to Reference the ZIA Posture Profile

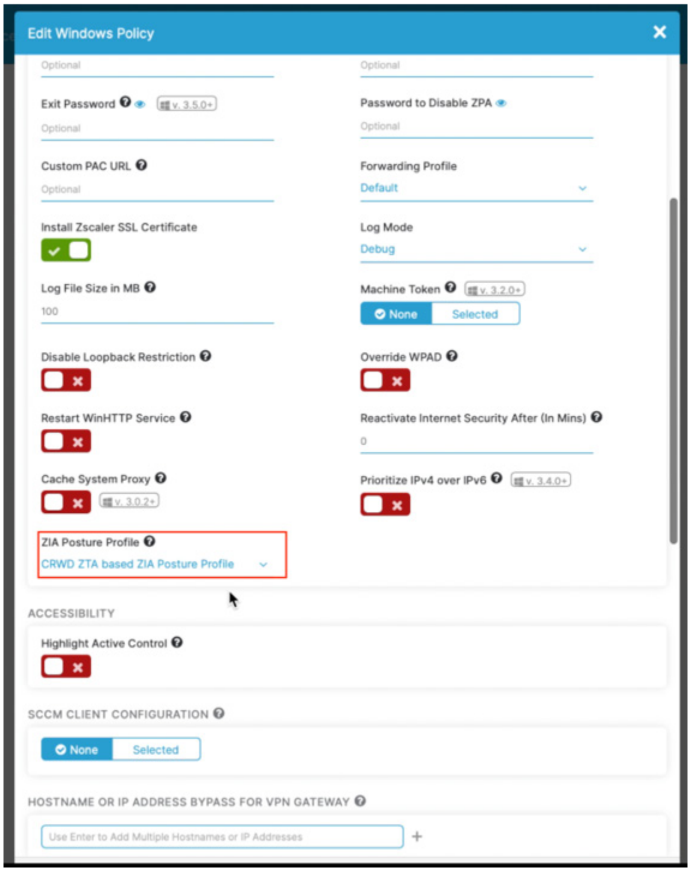
Go to the App Profile section and create a new App Profile. The following example creates an App Profile for Windows machines. The previously created ZIA Posture Profile is referenced in this App Profile.



Rule#	Policy Name	Policy Description	User Groups

Figure 22. Create new App Profile that references previously created ZIA Posture Profile

Configure the App Profile.



Edit Windows Policy

Optional

Optional

Exit Password (v. 3.5.0+): Optional

Password to Disable ZPA: Optional

Custom PAC URL: Optional

Forwarding Profile: Default

Install Zscaler SSL Certificate: ✓

Log Mode: Debug

Log File Size in MB: 100

Machine Token (v. 3.2.0+): ● None ○ Selected

Disable Loopback Restriction: ✗

Override WPAD: ✗

Restart WinHTTP Service: ✗

Reactivate Internet Security After (In Mins): 0

Cache System Proxy (v. 3.0.2+): ✗

Prioritize IPv4 over IPv6 (v. 3.4.0+): ✗

ZIA Posture Profile: CRWD ZTA based ZIA Posture Profile

ACCESSIBILITY

Highlight Active Control: ✗

SCCM CLIENT CONFIGURATION

● None ○ Selected

HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY

Use Enter to Add Multiple Hostnames or IP Addresses +

Figure 23. Select previously created CrowdStrike ZTA-based posture profile

Create a Traffic Enforcement Policy Using Device Trust Level as Criteria

The following example creates a URL & Cloud App Control policy that uses Device Trust level as a criterion for conditional access that allows access, shows a caution page, or blocks access through ZIA based on Device Trust level. You can set up such policies for File type control, SSL inspection, Firewall control, etc.

1. Go to **Policy** > **URL & Cloud App Control**.

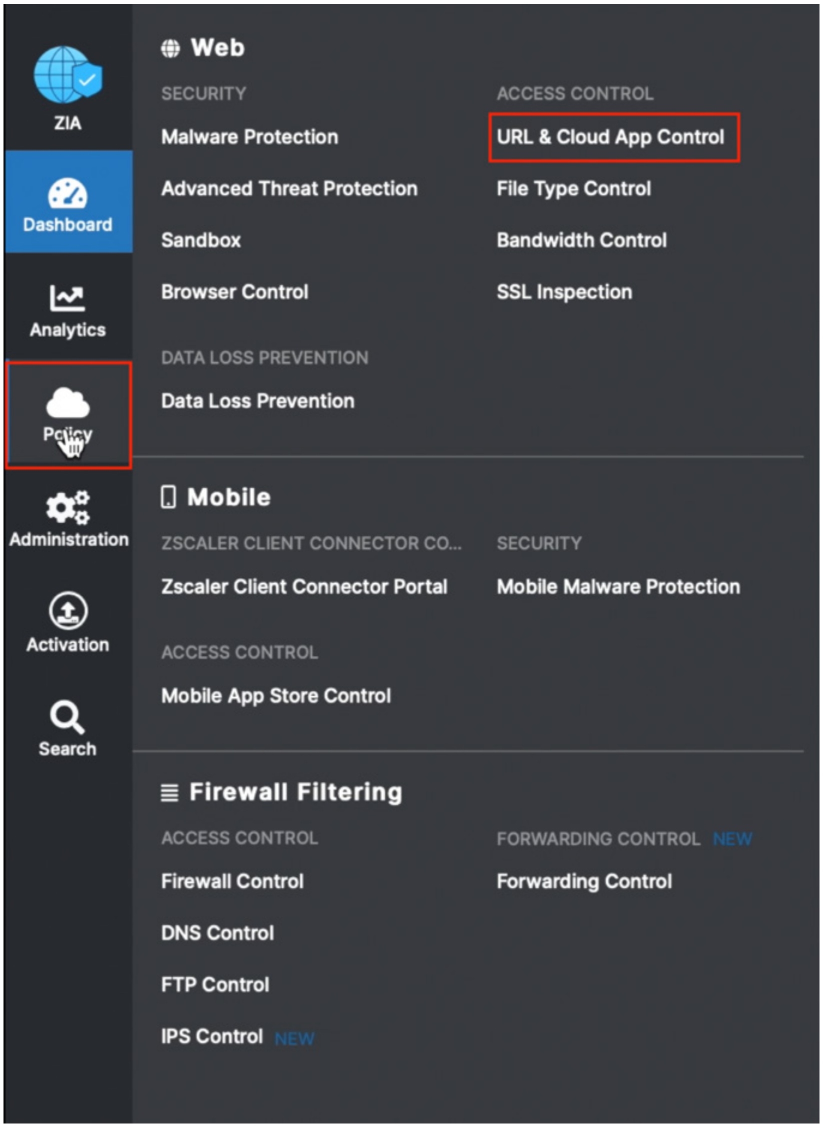
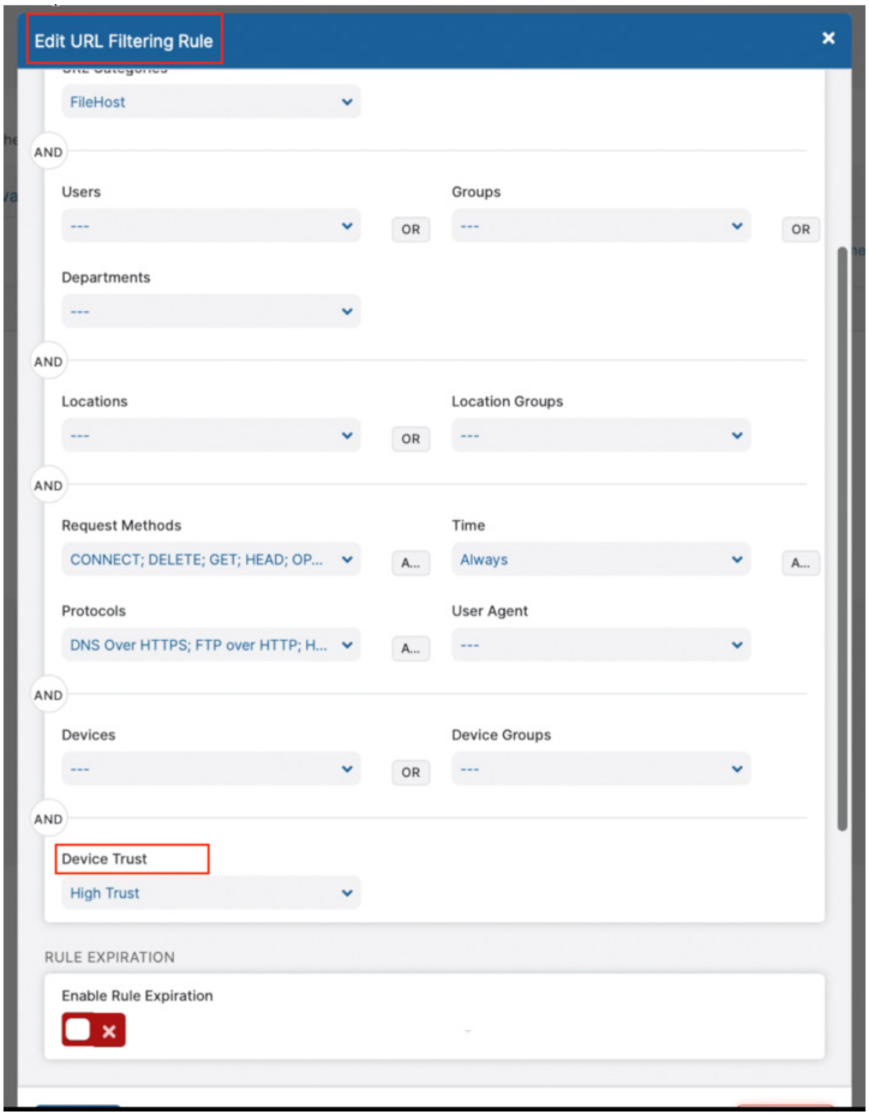


Figure 24. Create a URL filtering policy

2. Use the **Device Trust** level as a criterion for policy enforcement.



Edit URL Filtering Rule

FileHost

AND

Users: ---

OR

Groups: ---

OR

Departments: ---

AND

Locations: ---

OR

Location Groups: ---

AND

Request Methods: CONNECT; DELETE; GET; HEAD; OP...

Time: Always

Protocols: DNS Over HTTPS; FTP over HTTP; H...

User Agent: ---

AND

Devices: ---

OR

Device Groups: ---

AND

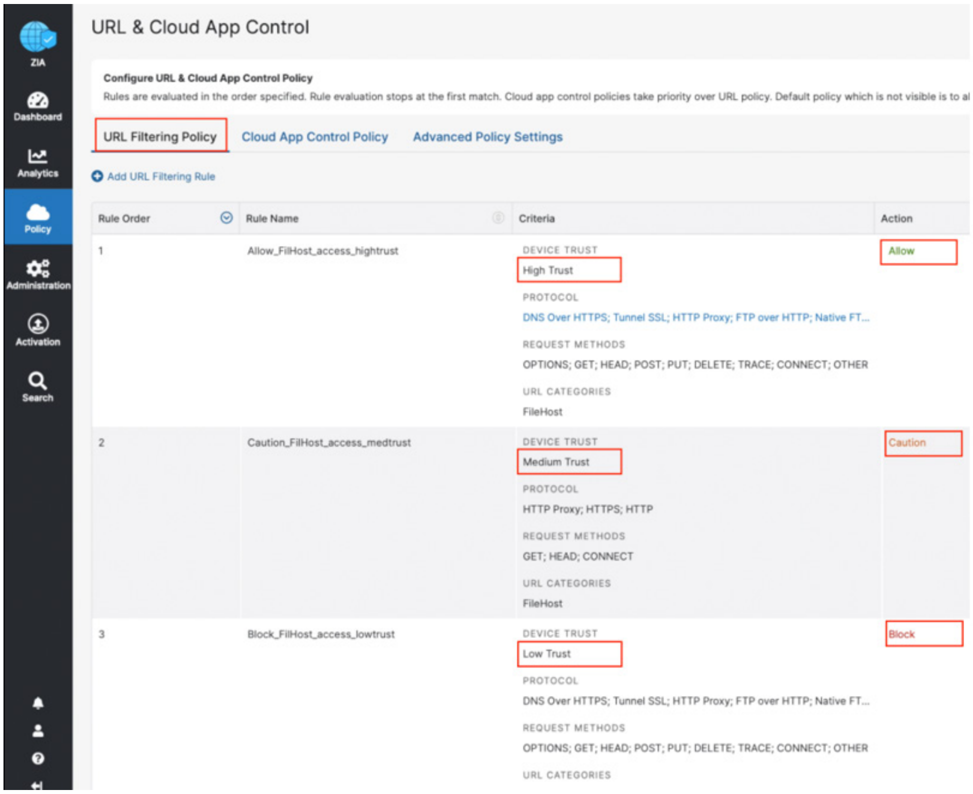
Device Trust: High Trust

RULE EXPIRATION

Enable Rule Expiration

Figure 25. Device Trust level being used as a policy enforcement criterion

The following image shows different actions associated in URL filtering policy based on the Device Trust level.



URL & Cloud App Control

Configure URL & Cloud App Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is to al

Rule Order	Rule Name	Criteria	Action
1	Allow_FilHost_access_hightrust	DEVICE TRUST High Trust PROTOCOL DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FT... REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER URL CATEGORIES FileHost	Allow
2	Caution_FilHost_access_medtrust	DEVICE TRUST Medium Trust PROTOCOL HTTP Proxy; HTTPS; HTTP REQUEST METHODS GET; HEAD; CONNECT URL CATEGORIES FileHost	Caution
3	Block_FilHost_access_lowtrust	DEVICE TRUST Low Trust PROTOCOL DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; Native FT... REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER URL CATEGORIES	Block

Figure 26. URL filtering policy based on Device Trust criterion

The same user logged in to Zscaler Client Connector on three different machines sees pertinent URL filtering policies enforced based on Device Trust level.

In this case, you see the same user accessing a file hosting website from three different machines that fall under High (in the following example, a ZTA greater than or equal to 75), Medium (a ZTA greater than or equal to 65, but less than 75), and Low (greater than or equal to 50, but less than 65) trust levels due to those machines' CrowdStrike ZTA scores.

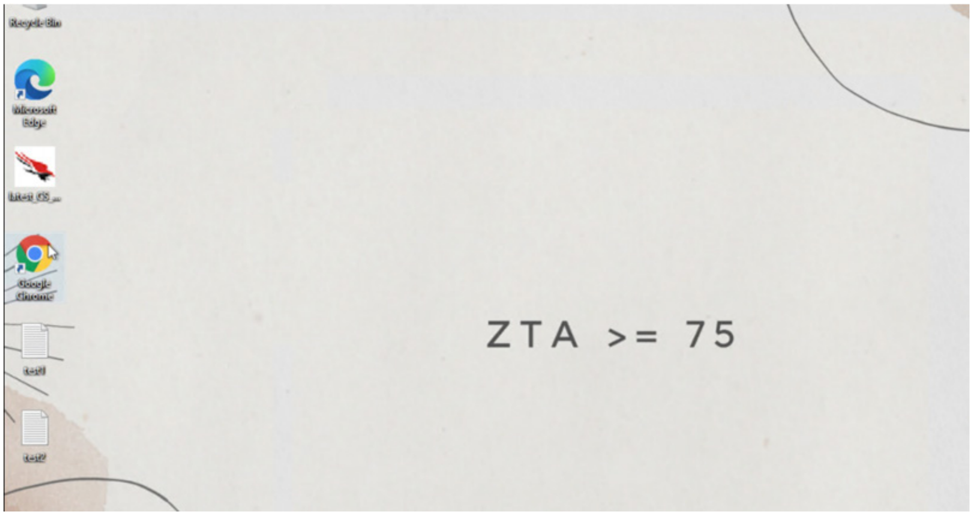
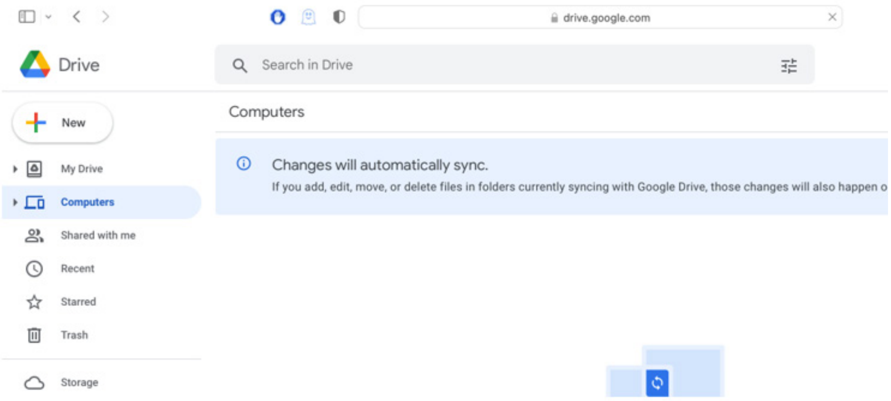


Figure 27. Accessing a file hosting website from a device that falls in High trust level based on defined ZIA posture policies

Access is allowed by ZIA per the URL filtering policy:

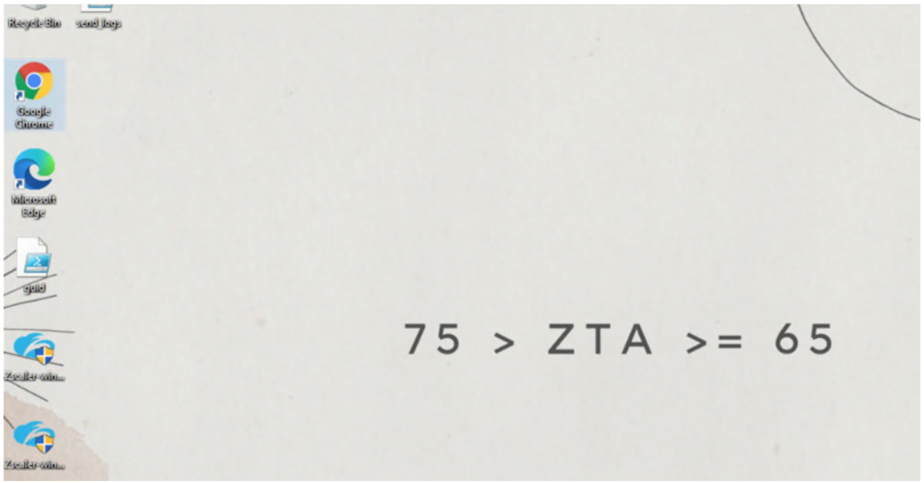


Changes will automatically sync.

If you add, edit, move, or delete files in folders currently syncing with Google Drive, those changes will also happen o

Figure 28. Access allowed by ZIA per the URL filtering policy due to Device Trust level

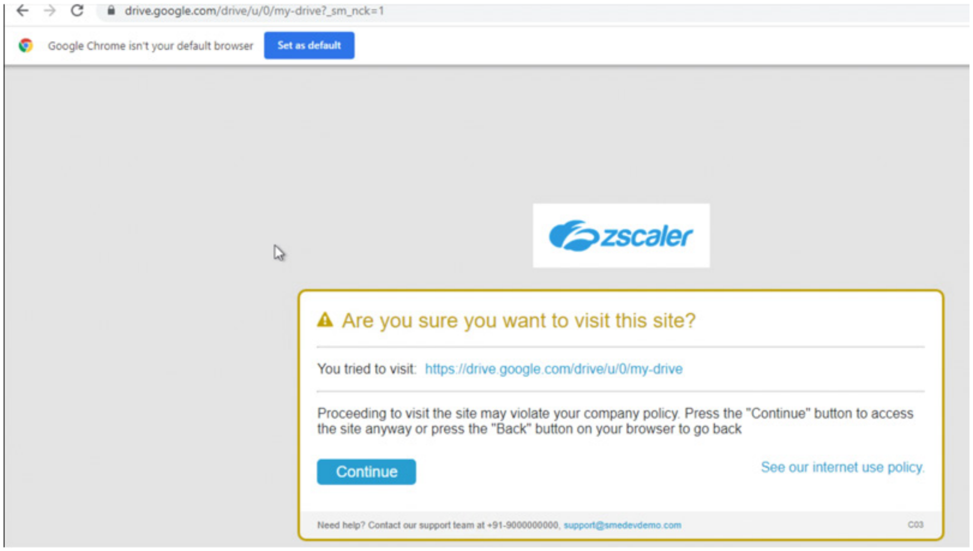
Devices that fall in the Medium trust level:



75 > ZTA >= 65

Figure 29. Accessing a file hosting website from a device that falls in Med. trust level based on defined ZIA posture policies

Caution warning from a URL filtering policy based on trust level:


drive.google.com/drive/u/0/my-drive?_sm_nck=1
Google Chrome isn't your default browser
Set as default
zscaler

Are you sure you want to visit this site?

You tried to visit: https://drive.google.com/drive/u/0/my-drive

Proceeding to visit the site may violate your company policy. Press the "Continue" button to access the site anyway or press the "Back" button on your browser to go back

Continue

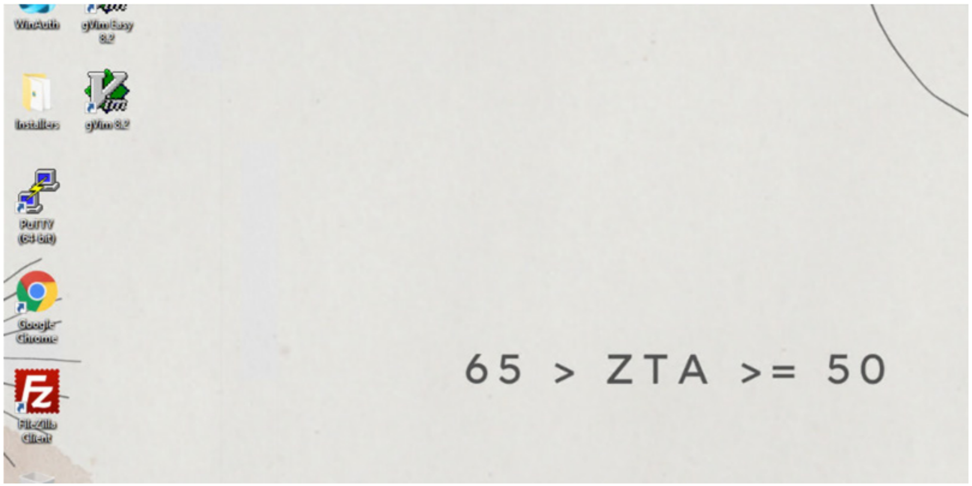
See our internet use policy.

Need help? Contact our support team at +91-9000000000, support@smedevdemo.com

C03

Figure 30. Caution page shown by ZIA per the URL filtering policy due to Device Trust level

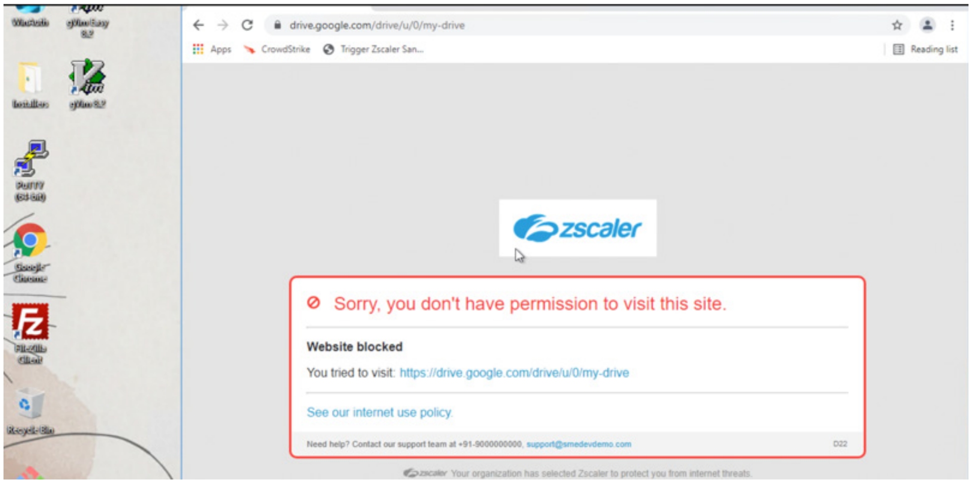
Low Trust level based on posture policy:



65 > ZTA >= 50

Figure 31. Accessing a file hosting website from a device that falls in Low trust level based on defined ZIA posture policies

Access blocked due to Device Trust level:



Sorry, you don't have permission to visit this site.

Website blocked

You tried to visit: https://drive.google.com/drive/u/0/my-drive

See our internet use policy.

Need help? Contact our support team at +91-9000000000, support@smedevdemo.com D22

zscaler Your organization has selected Zscaler to protect you from internet threats.

Figure 32. Access blocked by ZIA per the URL filtering policy due to Device Trust level

The same user logged into different machines under different trust levels gets pertinent enforcement policies applied by ZIA.

Use Case 3: 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 is 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 specifies (for Windows and macOS workstations) that a CrowdStrike Falcon agent is installed and running on the endpoint so that the endpoint is granted access to internal applications referenced via the ZPA access policy.

> This ZPA integration was implemented before ZTA functionality was available from CrowdStrike.
>
> ZTA-based posture check (Use Case 1 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.

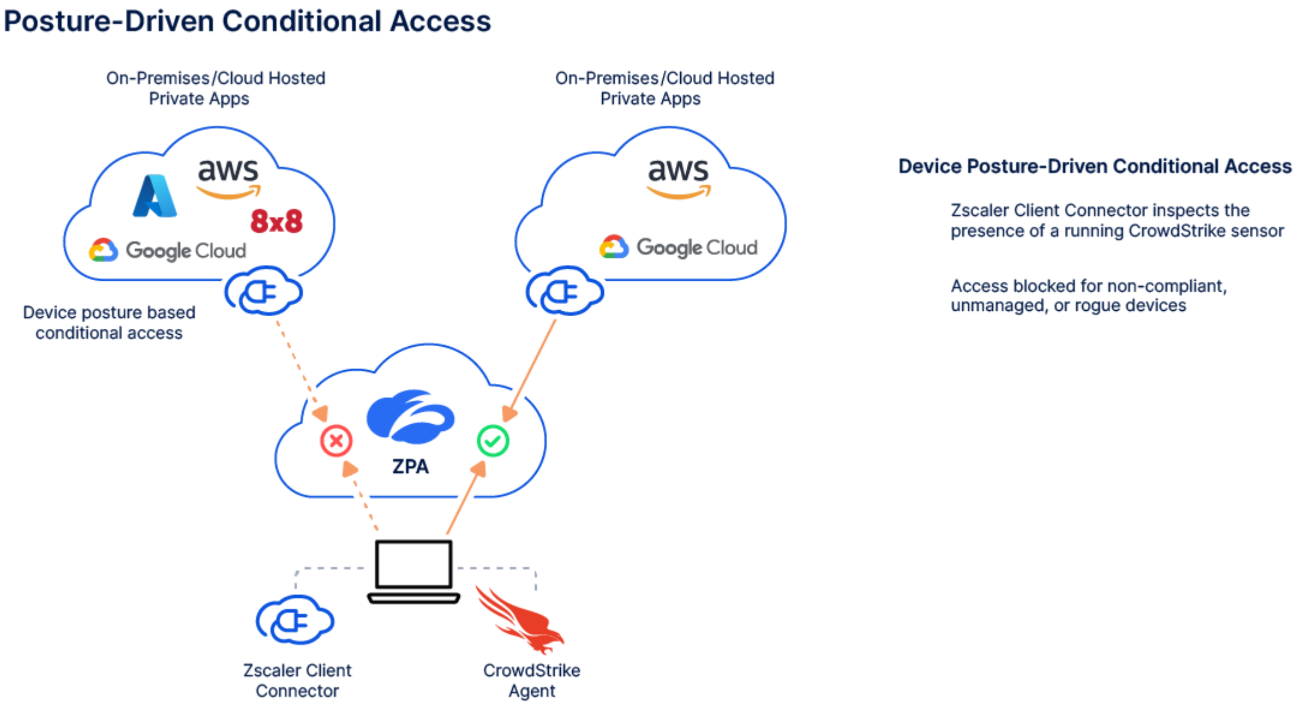
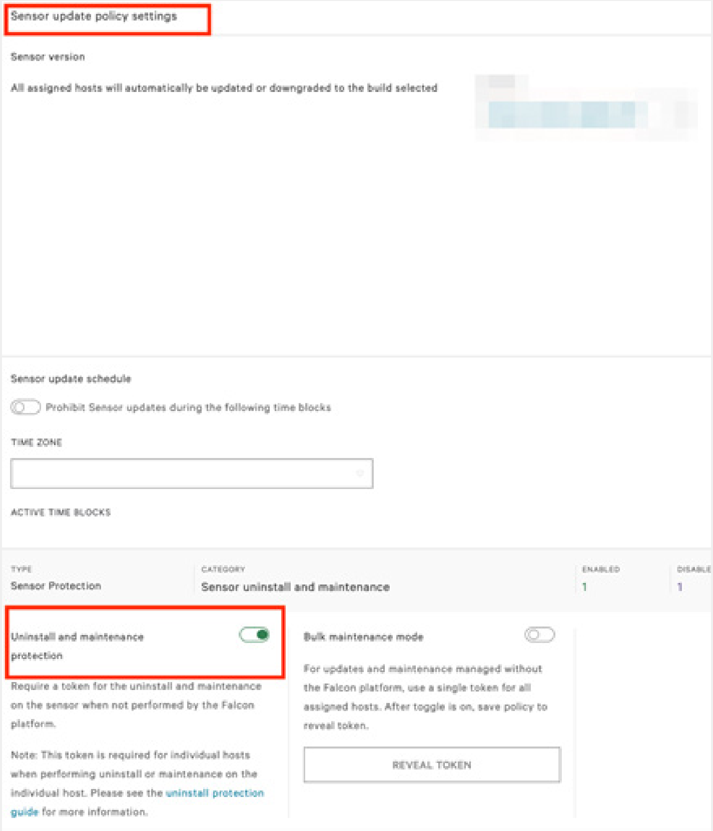

Posture-Driven Conditional Access
On-Premises/Cloud Hosted Private Apps
aws
8x8
Google Cloud
On-Premises/Cloud Hosted Private Apps
aws
Google Cloud
Device posture based conditional access
ZPA
Zscaler Client Connector
CrowdStrike Agent
Device Posture-Driven Conditional Access
Zscaler Client Connector inspects the presence of a running CrowdStrike sensor
Access blocked for non-compliant, unmanaged, or rogue devices

Figure 33. High-level overview

As a best practice, Zscaler recommends turning on **Uninstall and maintenance protection** via the CrowdStrike Sensor Update Policy settings, and enabling Sensor Tamper Prevention via CrowdStrike Prevention Policy settings.



Sensor update policy settings

Sensor version

All assigned hosts will automatically be updated or downgraded to the build selected [redacted]

Sensor update schedule

○ Prohibit Sensor updates during the following time blocks

TIME ZONE

ACTIVE TIME BLOCKS

TYPE	CATEGORY	ENABLED	DISABLE
Sensor Protection	Sensor uninstall and maintenance	1	1

Uninstall and maintenance protection ●

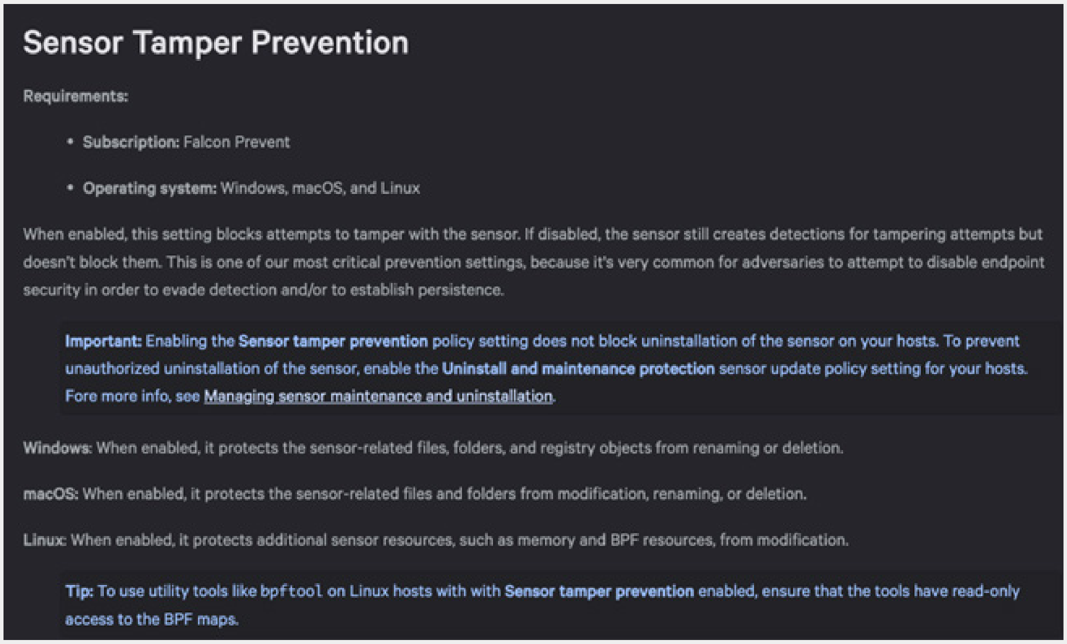
Require a token for the uninstall and maintenance on the sensor when not performed by the Falcon platform.

Note: This token is required for individual hosts when performing uninstall or maintenance on the individual host. Please see the uninstall protection guide for more information.

Bulk maintenance mode ○

For updates and maintenance managed without the Falcon platform, use a single token for all assigned hosts. After toggle is on, save policy to reveal token.

Figure 1. Uninstall and maintenance protection



Sensor Tamper Prevention

Requirements:

- **Subscription:** Falcon Prevent
- **Operating system:** Windows, macOS, and Linux

When enabled, this setting blocks attempts to tamper with the sensor. If disabled, the sensor still creates detections for tampering attempts but doesn't block them. This is one of our most critical prevention settings, because it's very common for adversaries to attempt to disable endpoint security in order to evade detection and/or to establish persistence.

> **Important:** Enabling the **Sensor tamper prevention** policy setting does not block uninstallation of the sensor on your hosts. To prevent unauthorized uninstallation of the sensor, enable the **Uninstall and maintenance protection** sensor update policy setting for your hosts. Fore more info, see Managing sensor maintenance and uninstallation.

Windows: When enabled, it protects the sensor-related files, folders, and registry objects from renaming or deletion.

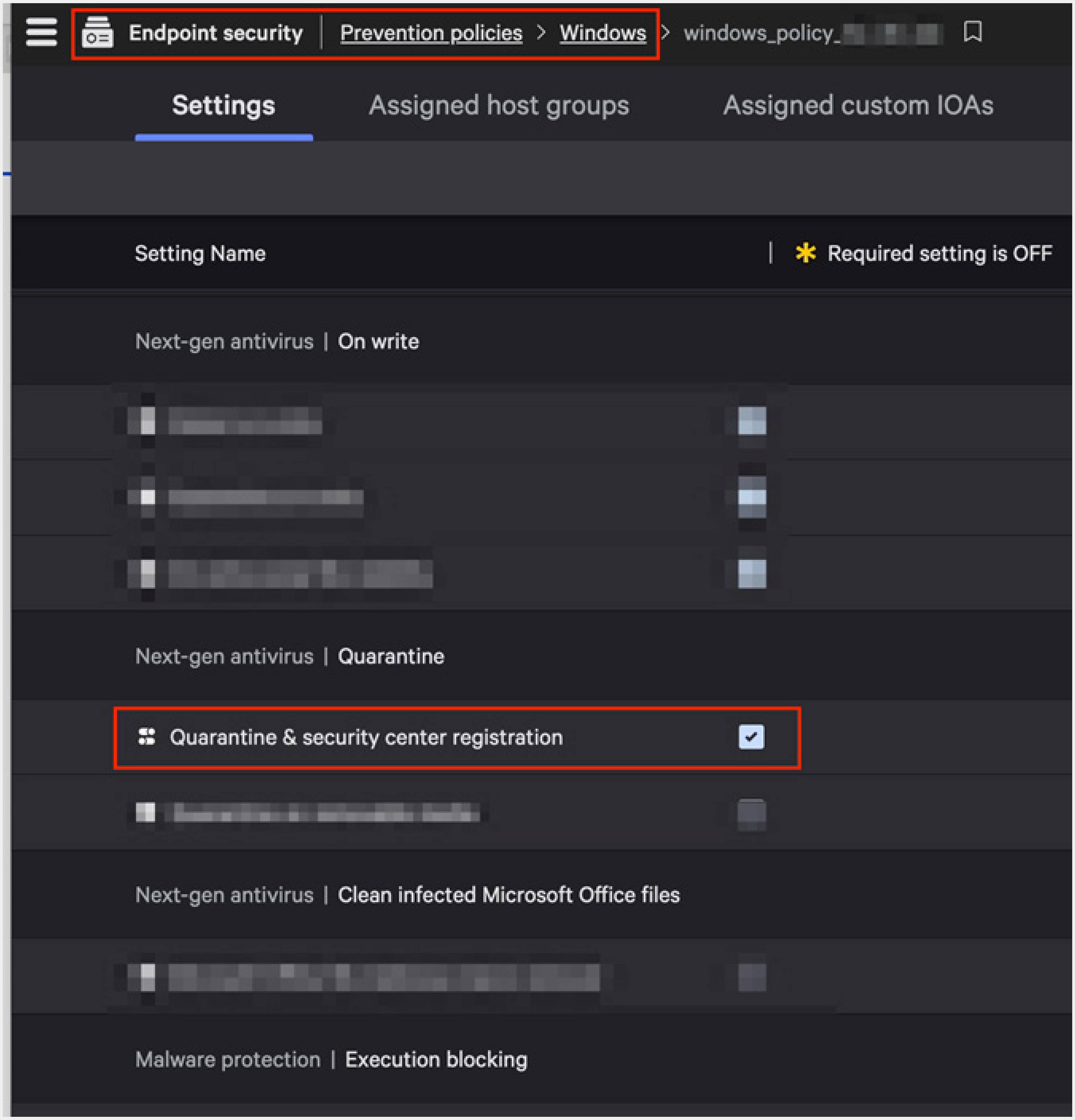
macOS: When enabled, it protects the sensor-related files and folders from modification, renaming, or deletion.

Linux: When enabled, it protects additional sensor resources, such as memory and BPF resources, from modification.

> **Tip:** To use utility tools like `bpftool` on Linux hosts with with **Sensor tamper prevention** enabled, ensure that the tools have read-only access to the BPF maps.

Figure 2. Sensor Tamper Prevention

Zscaler recommends enabling the **Quarantine & security center registration** option when using Windows.



Endpoint security
Prevention policies > Windows > windows_policy_
Settings
Assigned host groups
Assigned custom IOAs
Setting Name
Required setting is OFF
Next-gen antivirus | On write
Next-gen antivirus | Quarantine
Next-gen antivirus | Clean infected Microsoft Office files
Malware protection | Execution blocking

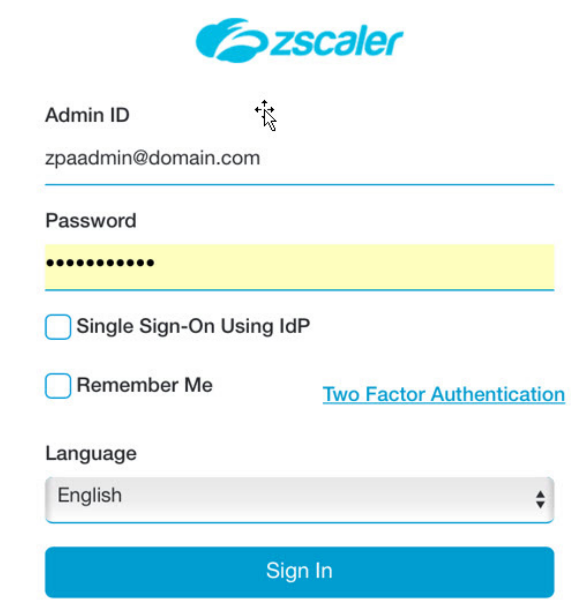
Quarantine & security center registration ☑

Figure 1. Quarantine & security center registration

Configuring ZPA

This guide assumes that you have a working ZPA set up and provides instructions to integrate posture-based conditional access as part of your existing ZPA deployment.

Log In to ZPA Admin Portal



Admin ID

zpaadmin@domain.com

Password

•••••••••••

□ Single Sign-On Using IdP

□ Remember Me

Two Factor Authentication

Language

English

Figure 34. Log in to ZPA Admin Portal

Go to the Zscaler Client Connector

Click **Client Connector** to open the Zscaler Client Connector window.

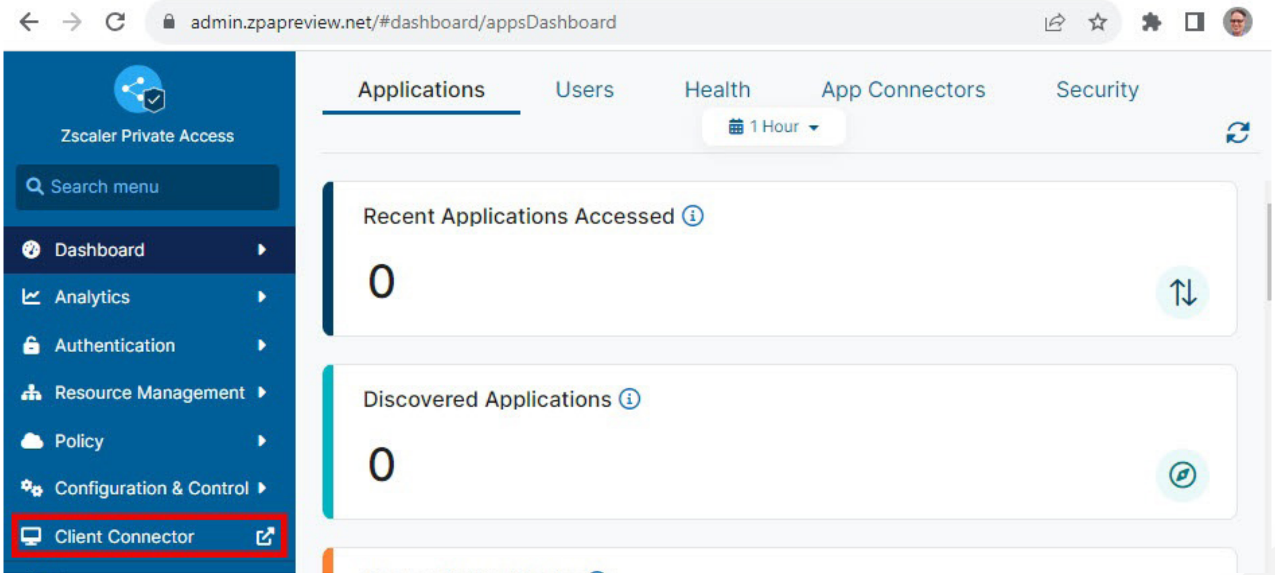


Figure 35. Click the Client Connector icon

Create a New Posture Profile

Log in to the Zscaler Client Connector Portal, go to **Administration** > **Device Posture**. Then click **Add Device Posture Profile**.

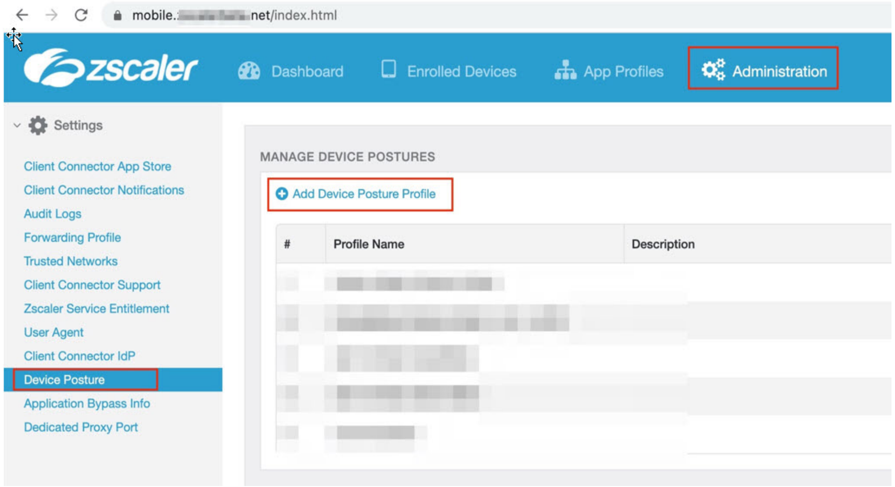


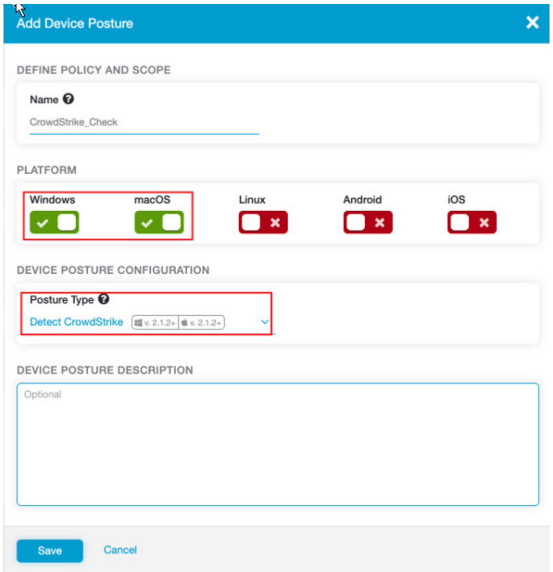
Figure 36. Add a Device Posture Profile in the ZPA Admin Portal

Add a New CrowdStrike Posture Profile

Complete the following steps:

1. Enter a **Name** for the policy.
2. Select only **Windows** and **macOS**.
3. Click the **Posture Type** drop-down menu.
4. Select **Detect CrowdStrike**.
5. Click **Save**.

   This posture profile is referenced in a ZPA access policy. You can set up access policies to allow or deny application access based on whether the posture check passes or fails.


Add Device Posture

DEFINE POLICY AND SCOPE

Name: CrowdStrike_Check

PLATFORM

Windows ✓ macOS ✓ Linux ✗ Android ✗ iOS ✗

DEVICE POSTURE CONFIGURATION

Posture Type: Detect CrowdStrike (v. 2.1.2+ | v. 2.1.2+)

DEVICE POSTURE DESCRIPTION

Optional

Figure 37. Add a detect CrowdStrike posture profile

Decide Which Applications Need Conditional Access

From the ZPA Admin Portal, go to **Resource Management** > **Application Management** > **Application Segments**.

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

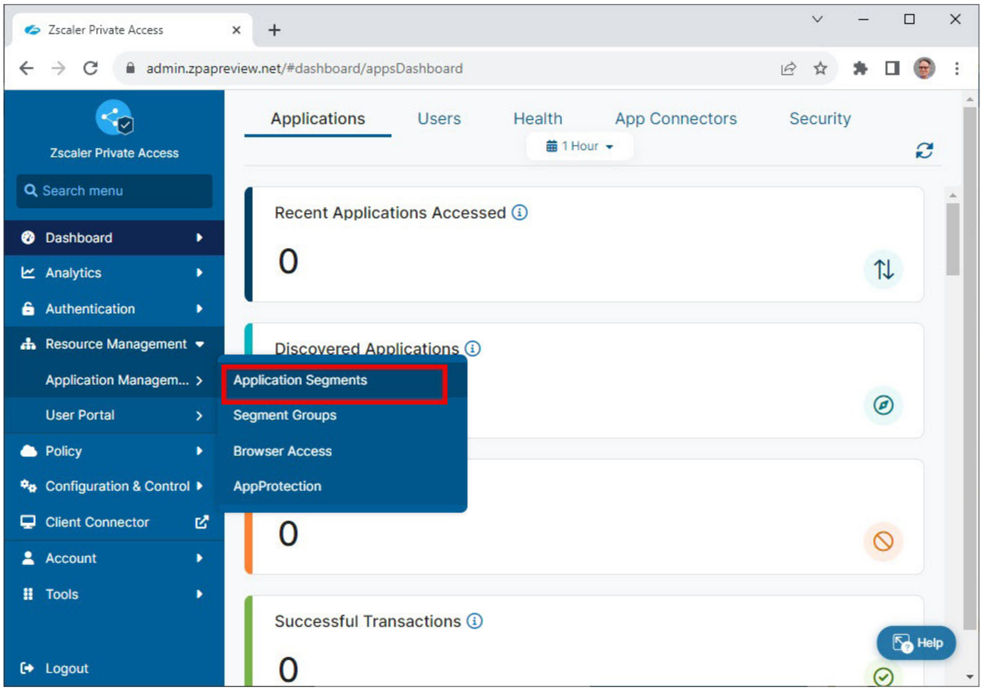
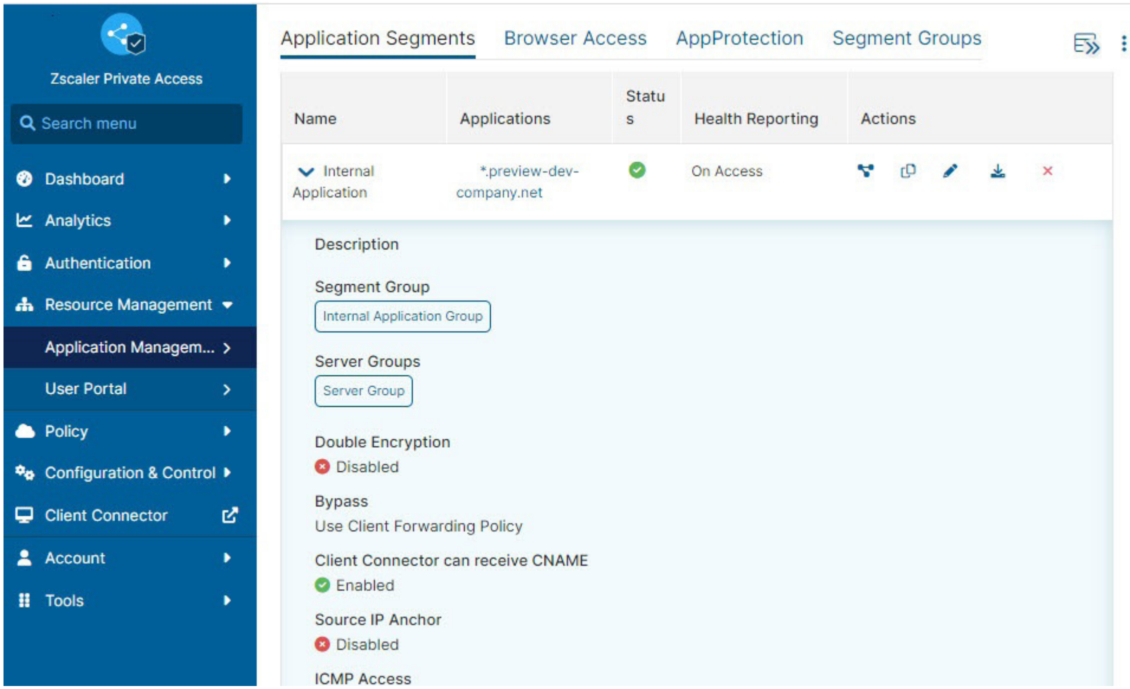


Figure 38. Go to Application Segments in the ZPA Admin Portal

In the following example, ZPA can access applications hosted under the domain *.preview-dev-company.net, based on the posture of the end device.



Name	Applications	Status	Health Reporting	Actions
Internal Application	*.preview-dev-company.net	✓	On Access	

Description

Segment Group
Internal Application Group

Server Groups
Server Group

Double Encryption
Disabled

Bypass
Use Client Forwarding Policy

Client Connector can receive CNAME
Enabled

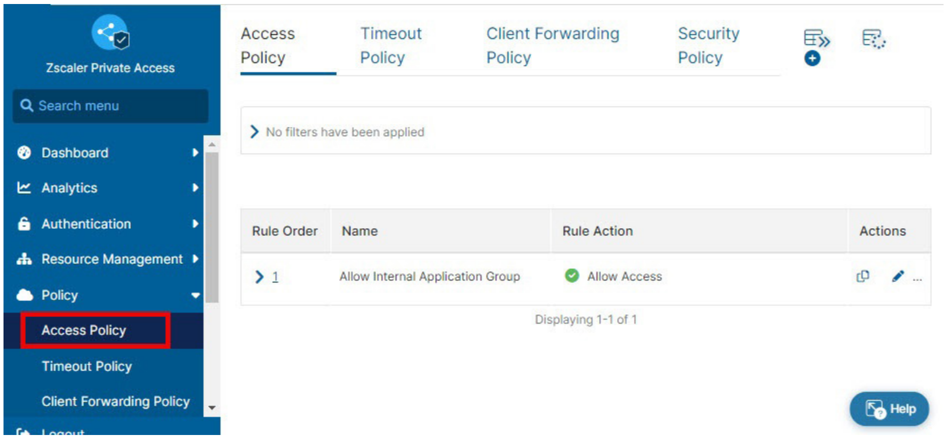
Source IP Anchor
Disabled

ICMP Access

Figure 39. Decide which application needs conditional access

Set Up an Access Policy

From the ZPA Admin Portal, go to **Policy** > **Access Policy**.



No filters have been applied

Rule Order	Name	Rule Action	Actions
1	Allow Internal Application Group	Allow Access	

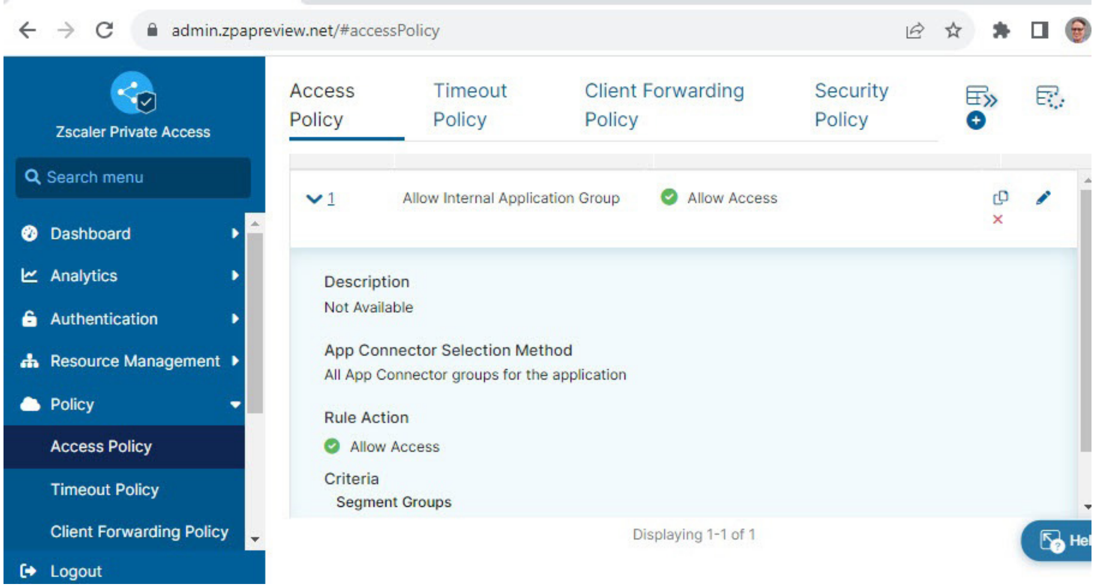
Displaying 1-1 of 1

Figure 40. Open access policy configuration dialog

Tie the Posture Profile to this Access Policy

Create a new access policy by clicking **Add Rule** and referencing the previously created posture profile. You can set up different access policies to protect different internal applications. You can show a customizable (and optional) notification message to the end users when application access is allowed or denied, informing them about the policy evaluation.

In the following example, an access policy is added 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 grants application access).



1 Allow Internal Application Group Allow Access

Description
Not Available

App Connector Selection Method
All App Connector groups for the application

Rule Action
Allow Access

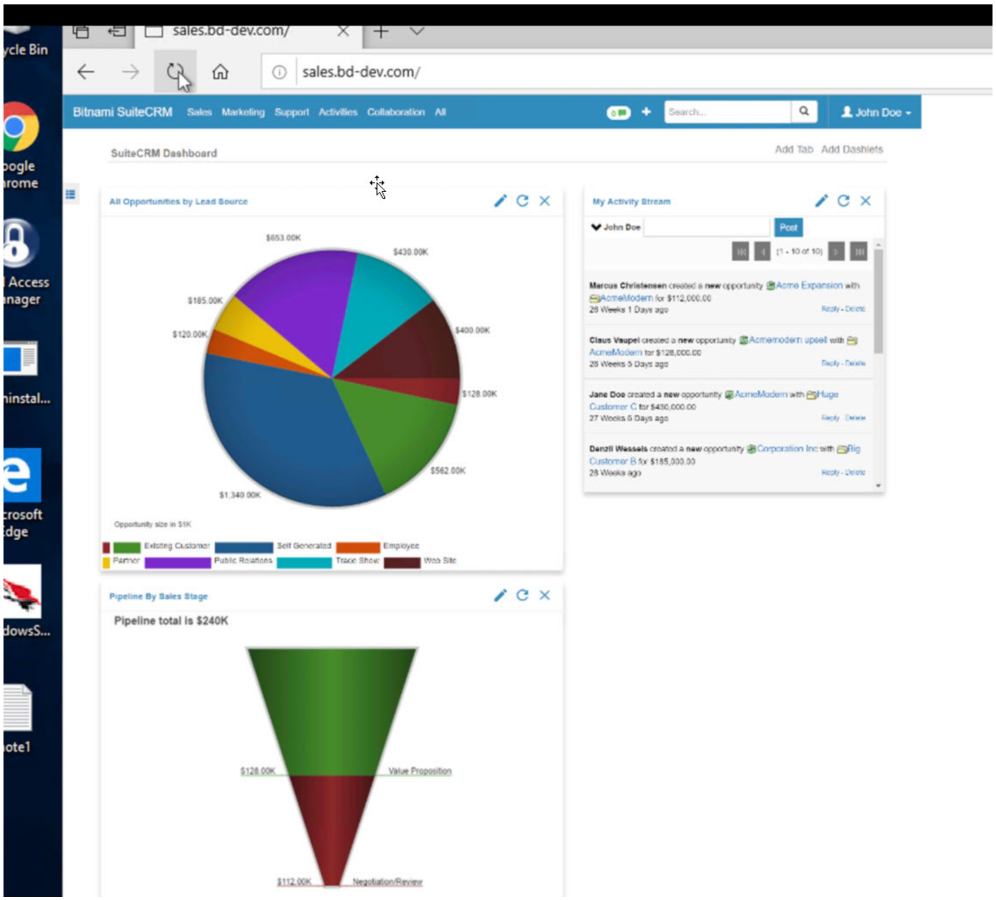
Criteria
Segment Groups

Displaying 1-1 of 1

Figure 41. Set up an access policy

Verify Conditional Access from an Endpoint

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



Marcus Christensen created a new opportunity Acme Expansion with AcmeModern for $112,000.00
28 Weeks 1 Days ago
Reply - Delete

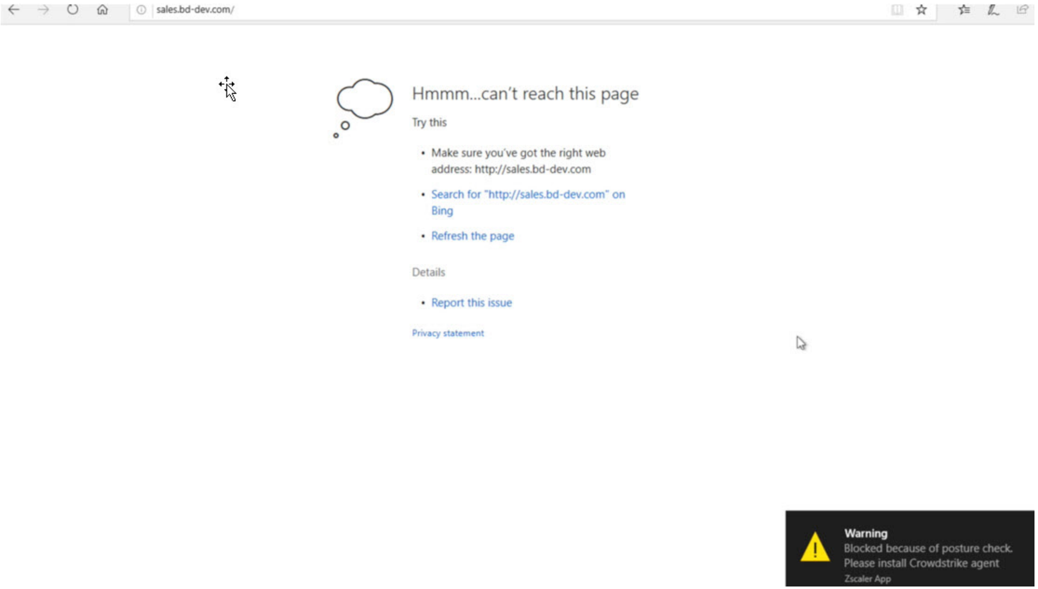
Claus Vaupel created a new opportunity Acmemodern upsell with AcmeModern for $128,000.00
28 Weeks 5 Days ago
Reply - Delete

Jane Doe created a new opportunity AcmeModern with Huge Customer C for $430,000.00
27 Weeks 6 Days ago
Reply - Delete

Denzil Wessels created a new opportunity Corporation Inc with Big Customer B for $185,000.00
28 Weeks ago
Reply - Delete

Figure 42. Access granted from an endpoint with the CrowdStrike agent installed and running

The following message is displayed if access is blocked because CrowdStrike isn't running:



Hmmm...can't reach this page

Try this

- Make sure you've got the right web address: http://sales.bd-dev.com
- Search for "http://sales.bd-dev.com" on Bing
- Refresh the page

Details

- Report this issue

Privacy statement

Warning
Blocked because of posture check.
Please install Crowdstrike agent
Zscaler App

Figure 43. Access blocked from an endpoint if the CrowdStrike agent is not running

Use Case 4: Zscaler Sandbox Integration with CrowdStrike

In this use case:

- Zscaler Sandbox detects zero-day malicious files via 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 or quarantine action button, which enables the administrator to trigger a network contain or quarantine request to the 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 suspended.
- Alternatively, an administrator can click the CrowdStrike Agent ID within the insight log to access the Falcon Console. Then, in the Falcon Console, the administrator can further investigate and mitigate operations for that Agent ID.

The following diagram shows a conceptualization of the integration.

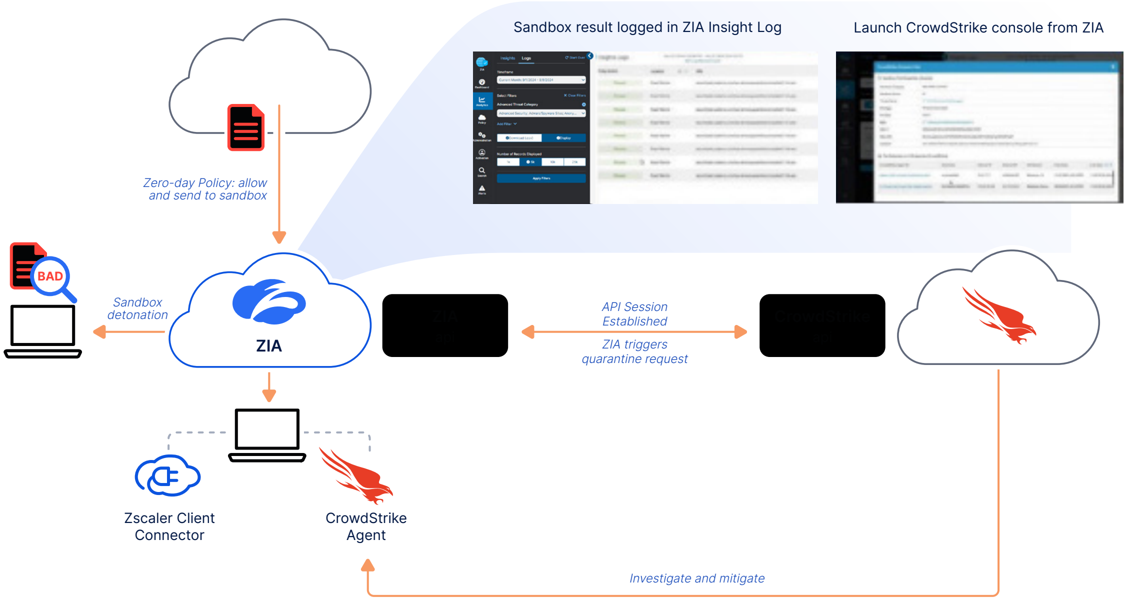

Sandbox result logged in ZIA Insight Log
Launch CrowdStrike console from ZIA
Zero-day Policy: allow and send to sandbox
BAD
Sandbox detonation
ZIA
[redacted]
API Session Established
ZIA triggers quarantine request
[redacted]
Zscaler Client Connector
CrowdStrike Agent
Investigate and mitigate

Figure 44. High-level overview

Configuring CrowdStrike for ZIA

To establish the API connection between CrowdStrike and Zscaler, you must first generate an OAuth 2.0 token from the Falcon 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 Falcon 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. To learn more, refer to the CrowdStrike documentation on how to deploy and configure CrowdStrike components before proceeding.

Log In to CrowdStrike

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

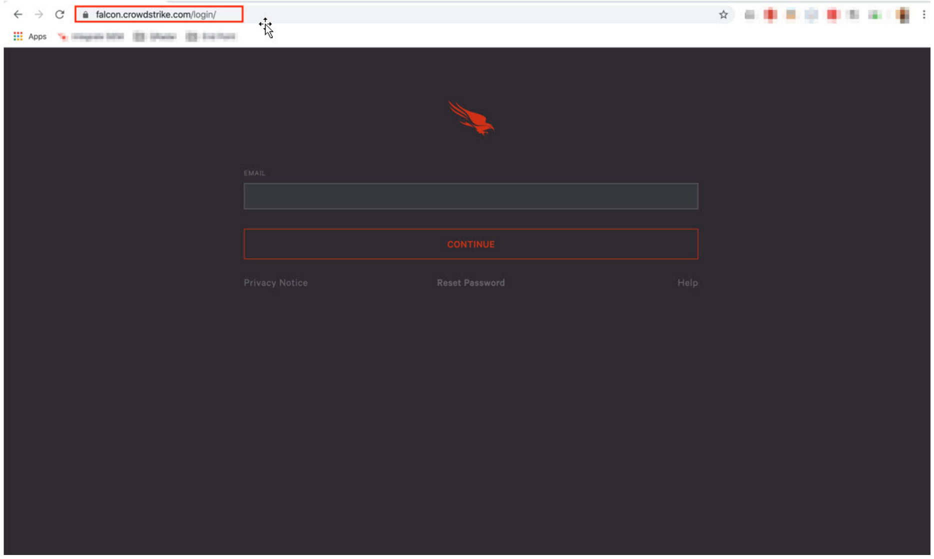
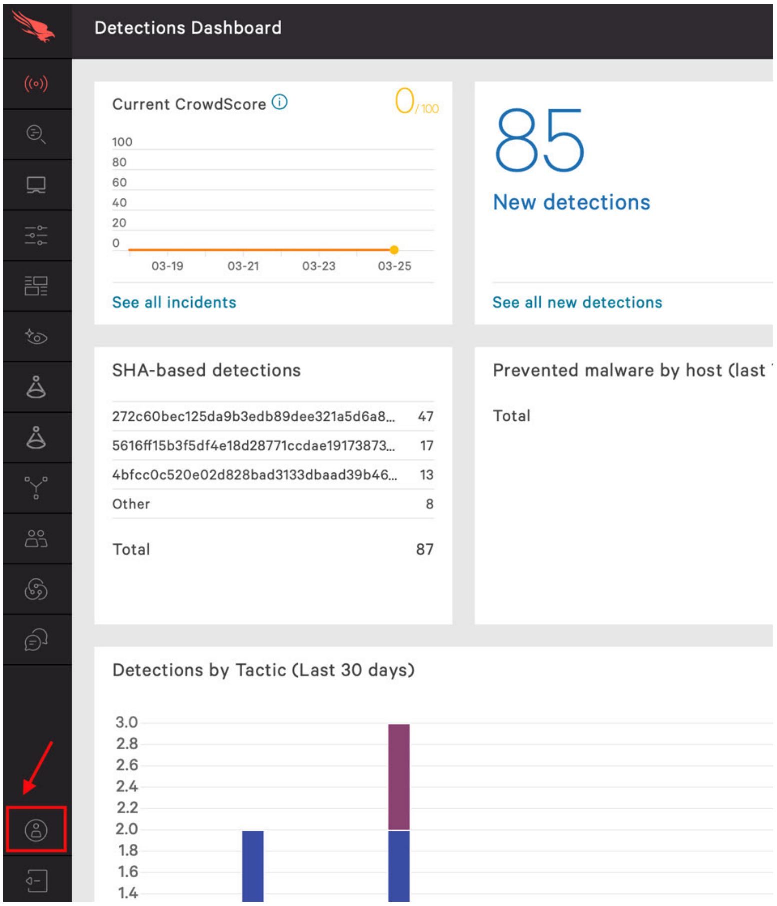


Figure 45. Log in to CrowdStrike

Access Your CrowdStrike Customer ID

After logging in to the Falcon Console, click the **User** icon to access your Customer ID.



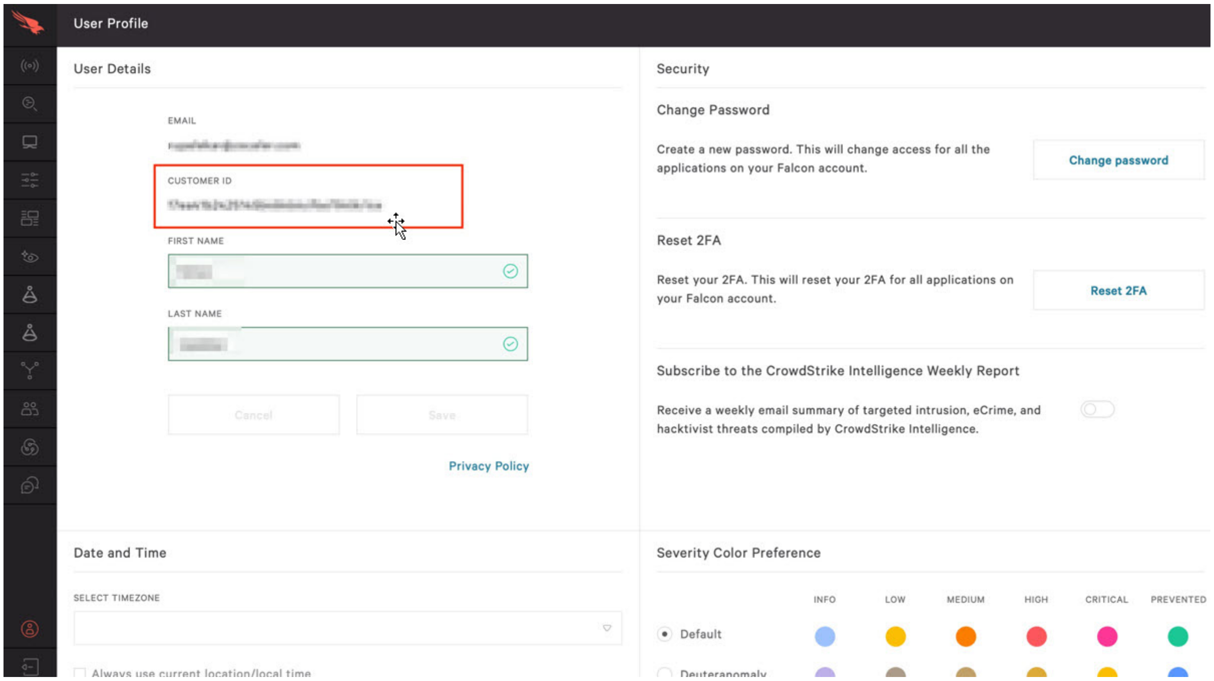
SHA-based detections

272c60bec125da9b3edb89dee321a5d6a8...	47
5616ff15b3f5df4e18d28771ccdae19173873...	17
4bfcc0c520e02d828bad3133dbaad39b46...	13
Other	8
Total	87

Figure 46. Click the User icon to access your CrowdStrike Customer ID

Note Your CrowdStrike Customer ID

You see your CrowdStrike Customer ID. You enter this ID in the ZIA Admin Portal later.



User Profile

User Details

EMAIL
[redacted]

CUSTOMER ID
[redacted]

FIRST NAME
[redacted]

LAST NAME
[redacted]

Security

Change Password

Create a new password. This will change access for all the applications on your Falcon account.

Reset 2FA

Reset your 2FA. This will reset your 2FA for all applications on your Falcon account.

Subscribe to the CrowdStrike Intelligence Weekly Report

Receive a weekly email summary of targeted intrusion, eCrime, and hacktivist threats compiled by CrowdStrike Intelligence.

Date and Time

SELECT TIMEZONE

□ Always use current location/local time

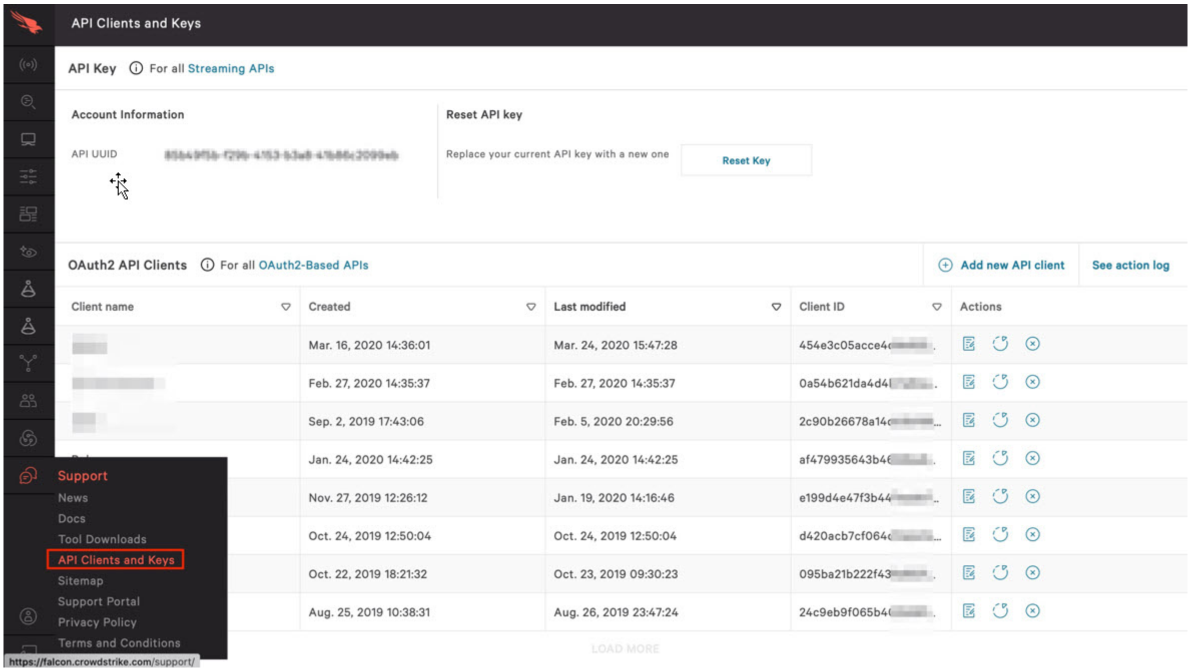
Severity Color Preference

	INFO	LOW	MEDIUM	HIGH	CRITICAL	PREVENTED
● Default	●	●	●	●	●	●
○ Deuteranomaly	●	●	●	●	●	●

Figure 47. Access your CrowdStrike Customer ID

Go to the API Section

While still in the Falcon Console, go to **Support** > **API Clients and Keys**.



API Clients and Keys

API Key ⓘ For all Streaming APIs

Account Information

API UUID [redacted]

Reset API key

Replace your current API key with a new one

OAuth2 API Clients ⓘ For all OAuth2-Based APIs

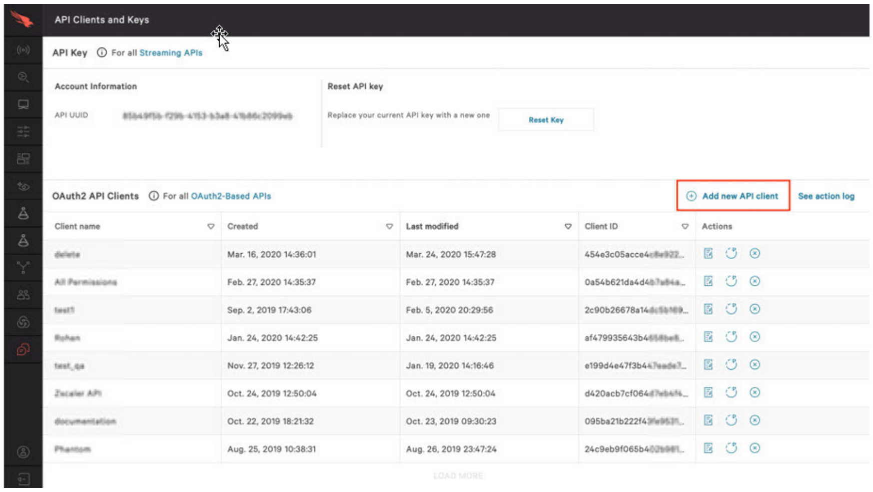
Client name	Created	Last modified	Client ID	Actions
[redacted]	Mar. 16, 2020 14:36:01	Mar. 24, 2020 15:47:28	454e3c05acce4c[redacted]...	
[redacted]	Feb. 27, 2020 14:35:37	Feb. 27, 2020 14:35:37	0a54b621da4d4[redacted]...	
[redacted]	Sep. 2, 2019 17:43:06	Feb. 5, 2020 20:29:56	2c90b26678a14c[redacted]...	
	Jan. 24, 2020 14:42:25	Jan. 24, 2020 14:42:25	af479935643b4[redacted]...	
	Nov. 27, 2019 12:26:12	Jan. 19, 2020 14:16:46	e199d4e47f3b44[redacted]...	
	Oct. 24, 2019 12:50:04	Oct. 24, 2019 12:50:04	d420acb7cf064c[redacted]...	
	Oct. 22, 2019 18:21:32	Oct. 23, 2019 09:30:23	095ba21b222f43[redacted]...	
	Aug. 25, 2019 10:38:31	Aug. 26, 2019 23:47:24	24c9eb9f065b4[redacted]...	

Figure 48. Go to the API section

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**.



Account Information

API UUID [redacted]

Reset API key

Replace your current API key with a new one

Client name	Created	Last modified	Client ID	Actions
[redacted]	Mar. 16, 2020 14:36:01	Mar. 24, 2020 15:47:28	454e3c05acce4[redacted]...	
[redacted]	Feb. 27, 2020 14:35:37	Feb. 27, 2020 14:35:37	0a54b621da4d4[redacted]...	
[redacted]	Sep. 2, 2019 17:43:06	Feb. 5, 2020 20:29:56	2c90b26678a14[redacted]...	
[redacted]	Jan. 24, 2020 14:42:25	Jan. 24, 2020 14:42:25	af479935643b4[redacted]...	
[redacted]	Nov. 27, 2019 12:26:12	Jan. 19, 2020 14:16:46	e199d4e47f3b4[redacted]...	
[redacted]	Oct. 24, 2019 12:50:04	Oct. 24, 2019 12:50:04	d420acb7cf064[redacted]...	
[redacted]	Oct. 22, 2019 18:21:32	Oct. 23, 2019 09:30:23	095ba21b222f4[redacted]...	
[redacted]	Aug. 25, 2019 10:38:31	Aug. 26, 2019 23:47:24	24c9eb9f065b4[redacted]...	

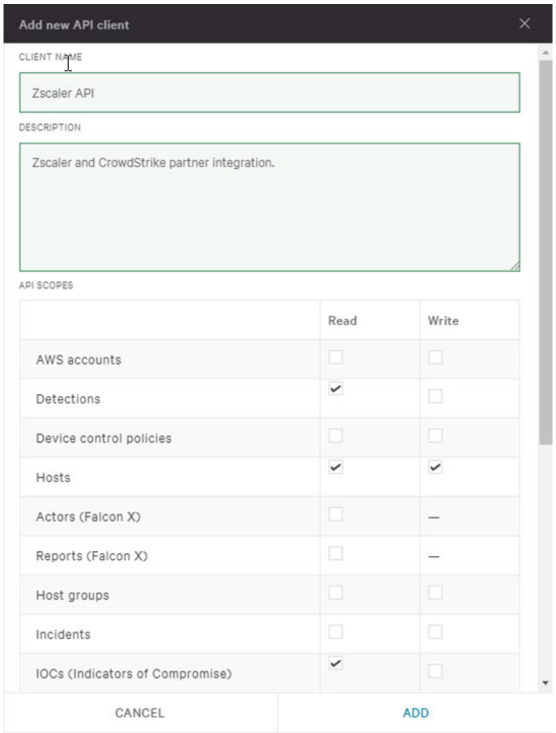
Figure 49. Add new API client

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**.



Add new API client

CLIENT NAME

Zscaler API

DESCRIPTION

Zscaler and CrowdStrike partner integration.

API SCOPES

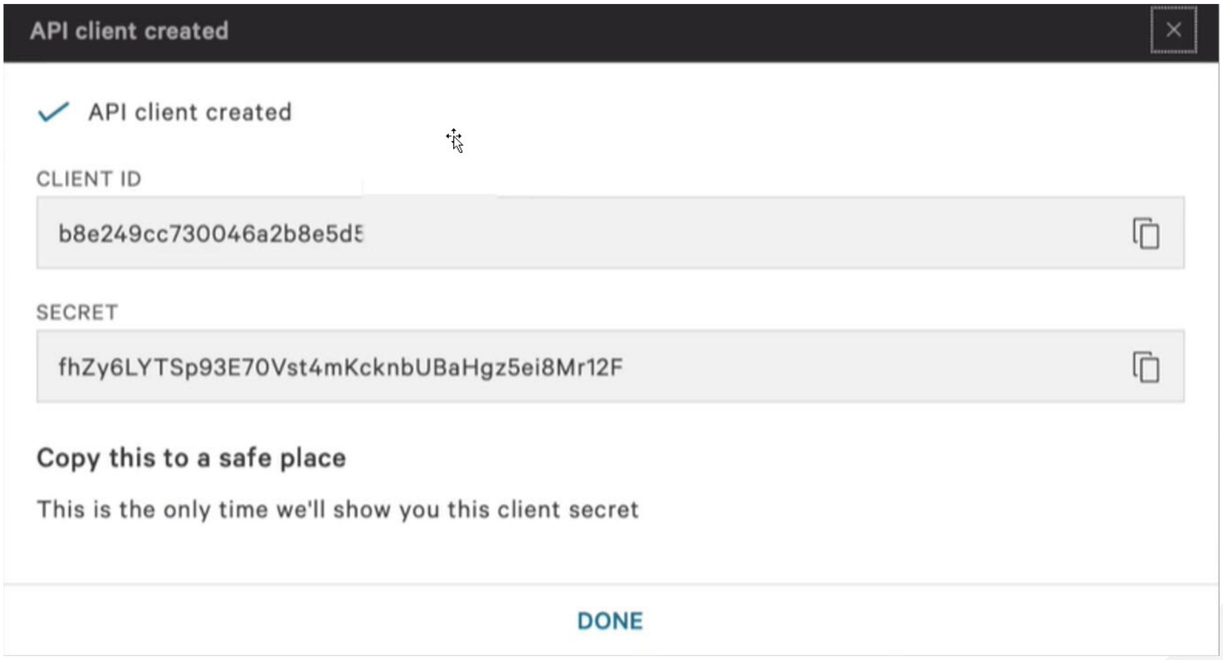
	Read	Write
AWS accounts	□	□
Detections	☑	□
Device control policies	□	□
Hosts	☑	☑
Actors (Falcon X)	□	—
Reports (Falcon X)	□	—
Host groups	□	□
Incidents	□	□
IOCs (Indicators of Compromise)	☑	□

Figure 50. Create and save API client

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 must provide the ID and secret in the ZIA Admin Portal.

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

✓ API client created

CLIENT ID

b8e249cc730046a2b8e5d5

SECRET

fhZy6LYTSp93E70Vst4mKcknbUBaHgz5ei8Mr12F

Copy this to a safe place

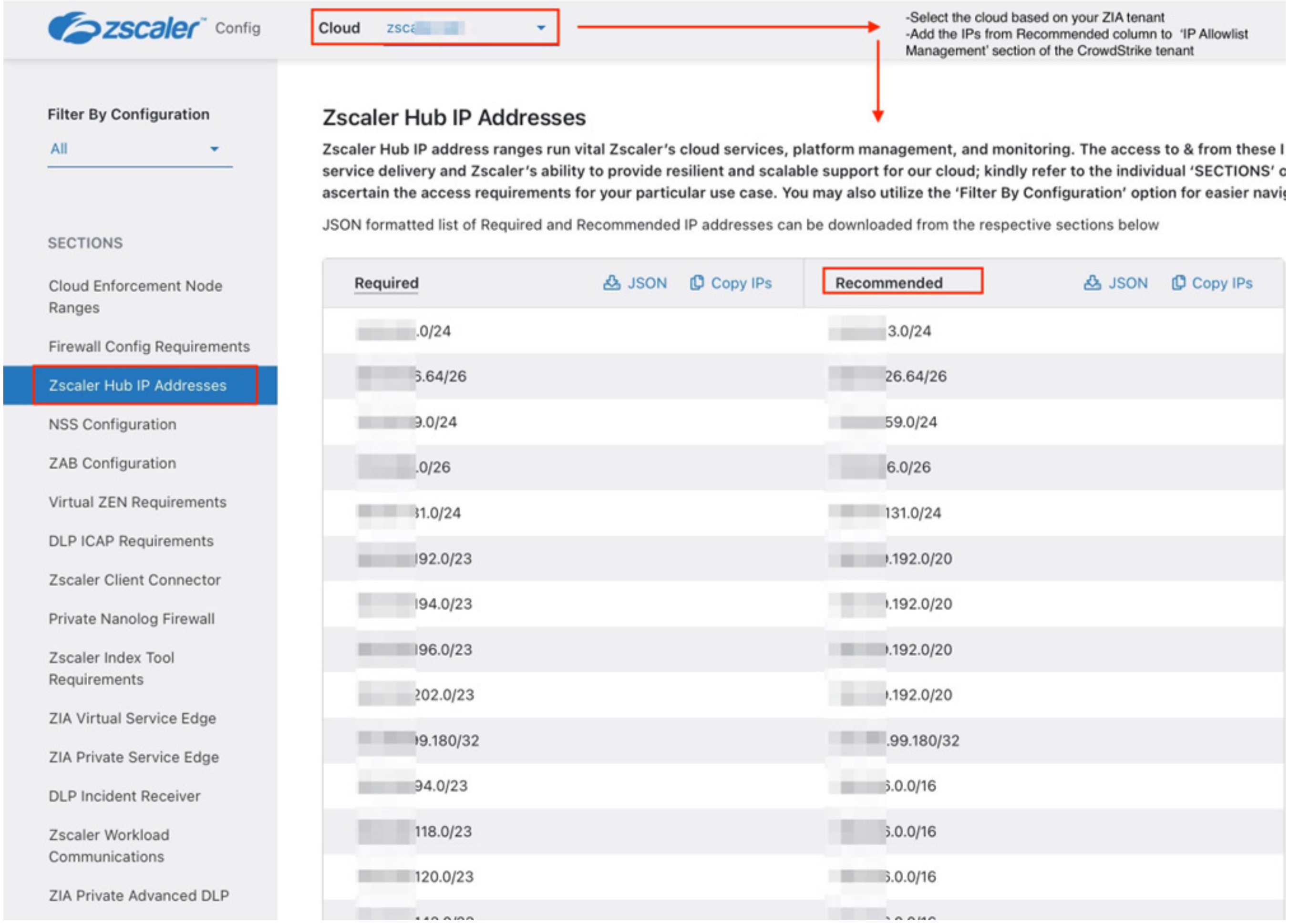
This is the only time we'll show you this client secret

Figure 51. Note the API credentials

Allowlist Zscaler Hub IP Range Used to Make API Calls to CrowdStrike

Optionally, you can lock down which public IPs are allowed to make API calls to your CrowdStrike tenant. If IP-based restriction is in place, you must allowlist Zscaler hub IP ranges (since ZIA initiates API calls to CrowdStrike for this integration) based on which Zscaler cloud you use. You must add the Zscaler cloud IP range to the IP Allowlist Management under the Host Setup and Management section in the CrowdStrike tenant.

Zscaler hub IP ranges are found at https://config.zscaler.com/zscaler.net/hubs (government agencies, see https://config.zscaler.us/zscalergov.net/hubs). Filter for the cloud where your ZIA tenant resides. Allowlist IPs in the Recommended column for API call purposes.



-Select the cloud based on your ZIA tenant
-Add the IPs from Recommended column to 'IP Allowlist Management' section of the CrowdStrike tenant

Zscaler Hub IP Addresses

Zscaler Hub IP address ranges run vital Zscaler's cloud services, platform management, and monitoring. The access to & from these I service delivery and Zscaler's ability to provide resilient and scalable support for our cloud; kindly refer to the individual 'SECTIONS' o ascertain the access requirements for your particular use case. You may also utilize the 'Filter By Configuration' option for easier navi

JSON formatted list of Required and Recommended IP addresses can be downloaded from the respective sections below

Required	Recommended
[redacted].0/24	[redacted]3.0/24
[redacted]5.64/26	[redacted]26.64/26
[redacted]9.0/24	[redacted]59.0/24
[redacted].0/26	[redacted]6.0/26
[redacted]31.0/24	[redacted]131.0/24
[redacted]92.0/23	[redacted].192.0/20
[redacted]94.0/23	[redacted].192.0/20
[redacted]96.0/23	[redacted].192.0/20
[redacted]202.0/23	[redacted].192.0/20
[redacted]9.180/32	[redacted].99.180/32
[redacted]94.0/23	[redacted]5.0.0/16
[redacted]118.0/23	[redacted]5.0.0/16
[redacted]120.0/23	[redacted]5.0.0/16

Figure 52. Zscaler IP range for API calls

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:

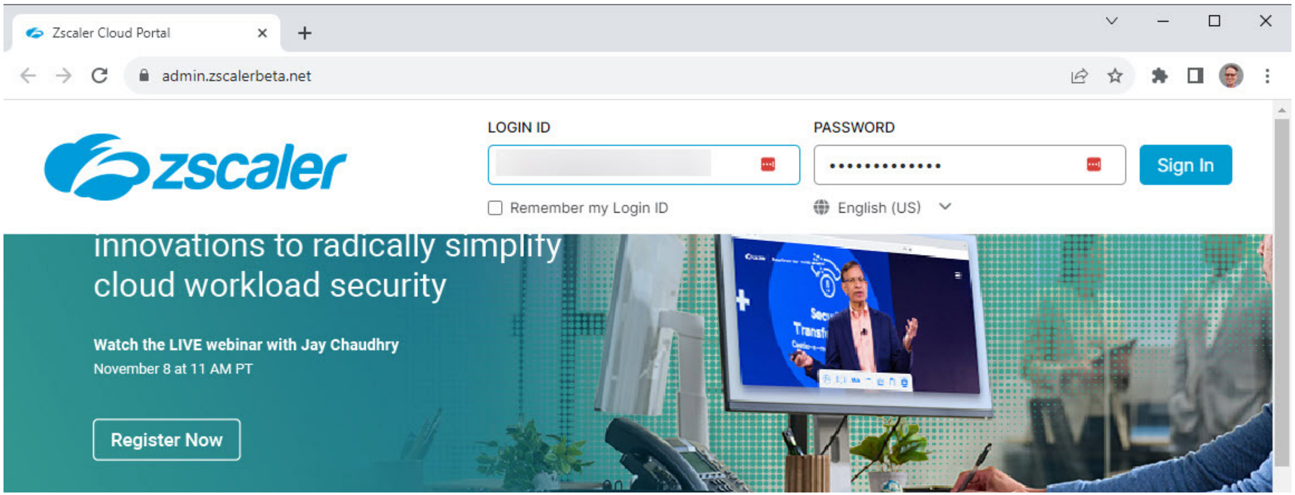
- CrowdStrike Agent ID.
- Host Name.
- Timestamps that capture when malicious files appear on the endpoint (e.g., an infection via a different attack surface, such as via a USB thumb drive).

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.

Log In to ZIA Admin Portal

Log in to ZIA Admin Portal using your admin account. If you are unable to log in using your administrator account, contact Zscaler Support (government agencies, see Zscaler Support).



Zscaler Cloud Portal

admin.zscalerbeta.net

LOGIN ID

PASSWORD ••••••••••••••

Sign In

□ Remember my Login ID

English (US)

zscaler
innovations to radically simplify
cloud workload security
Watch the LIVE webinar with Jay Chaudhry
November 8 at 11 AM PT
Register Now

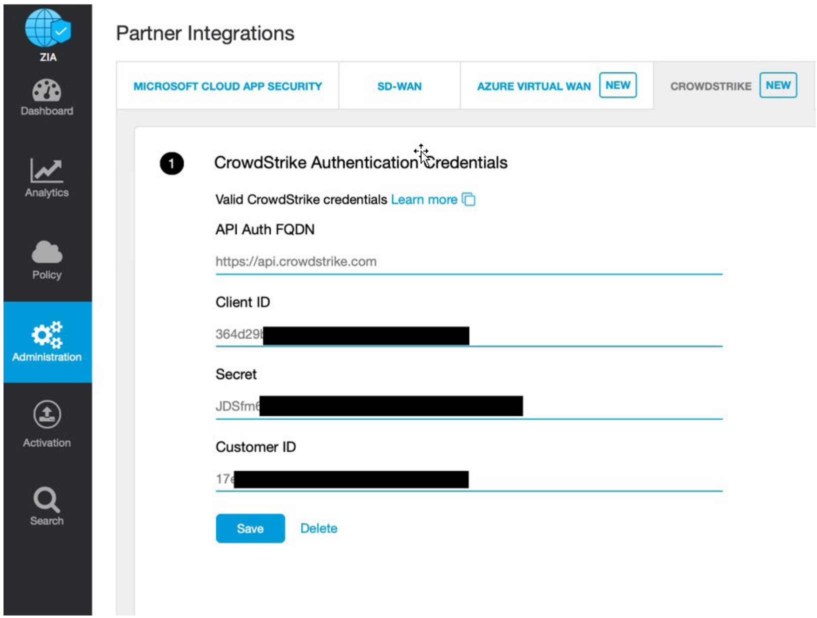
Figure 53. Log in to ZIA Admin Portal

Configure Partner Integration

From the ZIA Admin Portal, go to **Administration** > **Partner Integrations**. The **API Auth FQDN** URL depends on which CrowdStrike cloud you use.

Complete the following steps:

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



Partner Integrations

MICROSOFT CLOUD APP SECURITY | SD-WAN | AZURE VIRTUAL WAN NEW | CROWDSTRIKE NEW

1 CrowdStrike Authentication Credentials

Valid CrowdStrike credentials Learn more

API Auth FQDN: https://api.crowdstrike.com

Client ID: 364d29[redacted]

Secret: JDSfm[redacted]

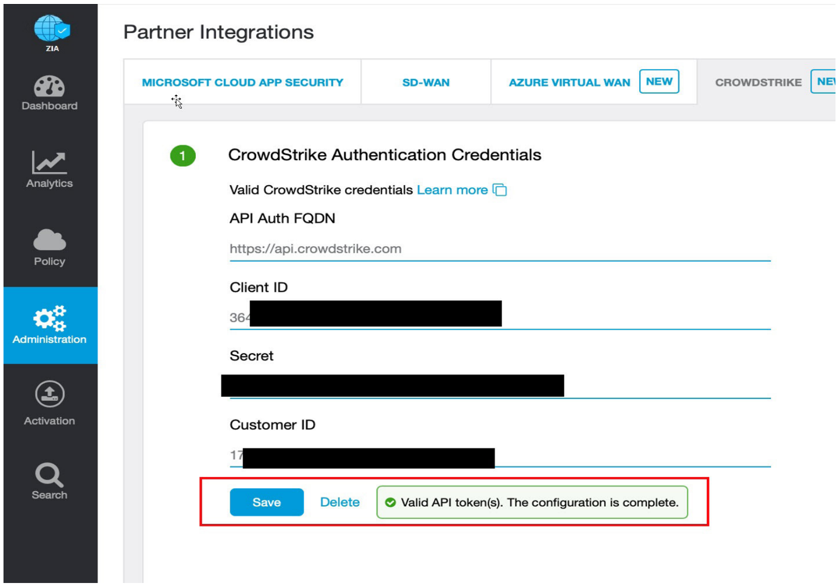
Customer ID: 17[redacted]

Save Delete

Figure 54. Configure partner integration in the ZIA Admin Portal

Verify the Partner Integration

When you see the message `Valid API token(s). The configuration is complete` in green background, you have successfully configured the API connection for the ZIA integration.



Partner Integrations

MICROSOFT CLOUD APP SECURITY | SD-WAN | AZURE VIRTUAL WAN NEW | CROWDSTRIKE NEW

1 CrowdStrike Authentication Credentials

Valid CrowdStrike credentials Learn more

API Auth FQDN: https://api.crowdstrike.com

Client ID: 364[redacted]

Secret: [redacted]

Customer ID: 17[redacted]

Save Delete ✓ Valid API token(s). The configuration is complete.

Figure 55. Verify partner integration

Activate Pending ZIA Configuration

Any time you make a change in ZIA, you see a number displayed over the **Activation** icon on the left-side navigation. This lets you know that you have changes pending in the queue for activation.

When you are ready to commit all changes in the queue, hover your cursor over the **Activation** icon and click **Activate**.

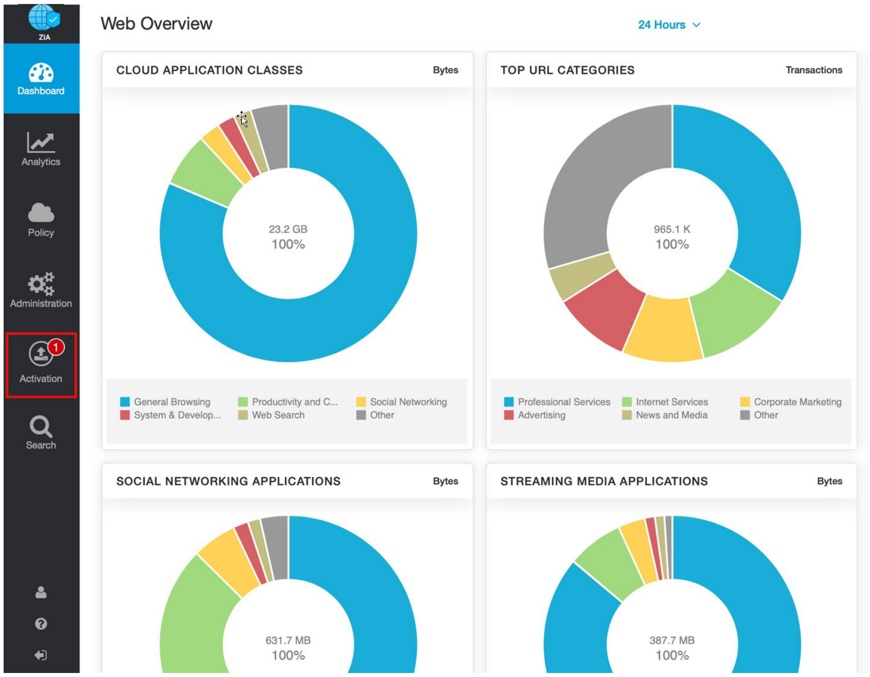


Figure 56. Activate pending ZIA configuration

Viewing CrowdStrike Endpoint Hits

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

From the ZIA Admin Portal, complete the following steps:

1. Go to **Analytics** > **Web Insights**.

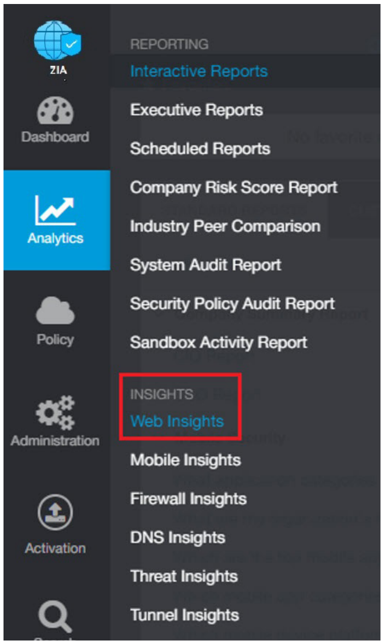


Figure 57. Go to Web Insights

2. On the **Logs** tab, click **Add Filter**.

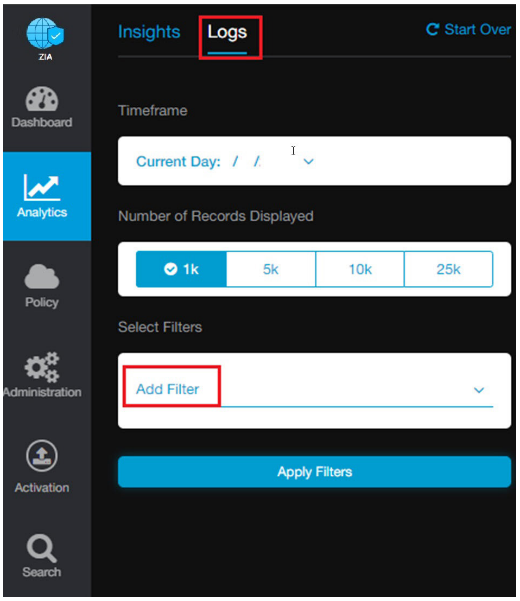
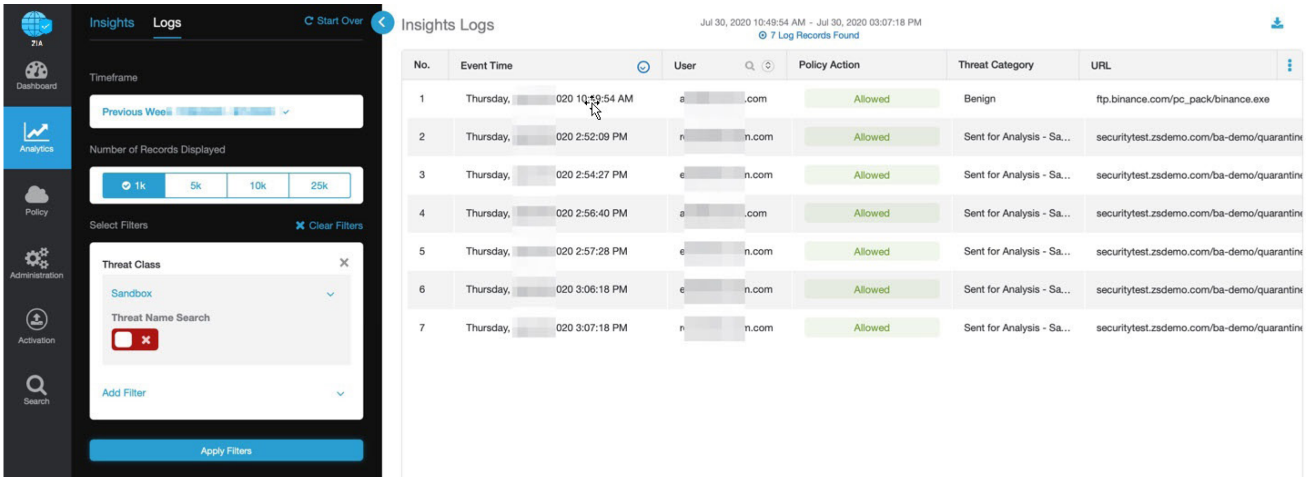


Figure 58. Select Logs

3. Select **Sandbox** as the **Threat Class** and click **Apply Filters**. After clicking **Apply Filters**, if the file in question was detonated or is currently being detonated by the Sandbox, corresponding log entries are displayed.



Timeframe: Previous Wee[redacted]

Number of Records Displayed: 1k ✓ | 5k | 10k | 25k

Select Filters — ✖ Clear Filters

Threat Class: Sandbox

Threat Name Search: ☒

Add Filter

Apply Filters

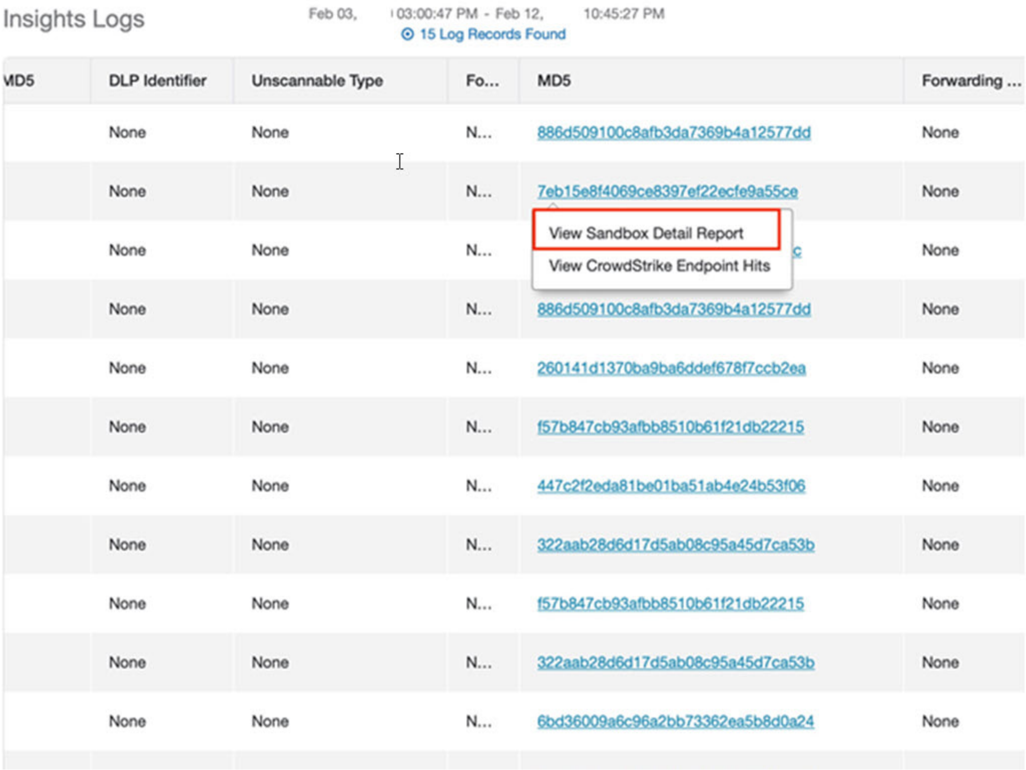
Insights Logs

Jul 30, 2020 10:49:54 AM - Jul 30, 2020 03:07:18 PM
7 Log Records Found

No.	Event Time	User	Policy Action	Threat Category	URL
1	Thursday, [redacted] 020 10:49:54 AM	a[redacted].com	Allowed	Benign	ftp.binance.com/pc_pack/binance.exe
2	Thursday, [redacted] 020 2:52:09 PM	r[redacted]n.com	Allowed	Sent for Analysis - Sa...	securitytest.zsdemo.com/ba-demo/quarantine
3	Thursday, [redacted] 020 2:54:27 PM	e[redacted]n.com	Allowed	Sent for Analysis - Sa...	securitytest.zsdemo.com/ba-demo/quarantine
4	Thursday, [redacted] 020 2:56:40 PM	a[redacted].com	Allowed	Sent for Analysis - Sa...	securitytest.zsdemo.com/ba-demo/quarantine
5	Thursday, [redacted] 020 2:57:28 PM	e[redacted]n.com	Allowed	Sent for Analysis - Sa...	securitytest.zsdemo.com/ba-demo/quarantine
6	Thursday, [redacted] 020 3:06:18 PM	e[redacted]n.com	Allowed	Sent for Analysis - Sa...	securitytest.zsdemo.com/ba-demo/quarantine
7	Thursday, [redacted] 020 3:07:18 PM	r[redacted]n.com	Allowed	Sent for Analysis - Sa...	securitytest.zsdemo.com/ba-demo/quarantine

Figure 59. Confirm whether file was sent to Sandbox

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



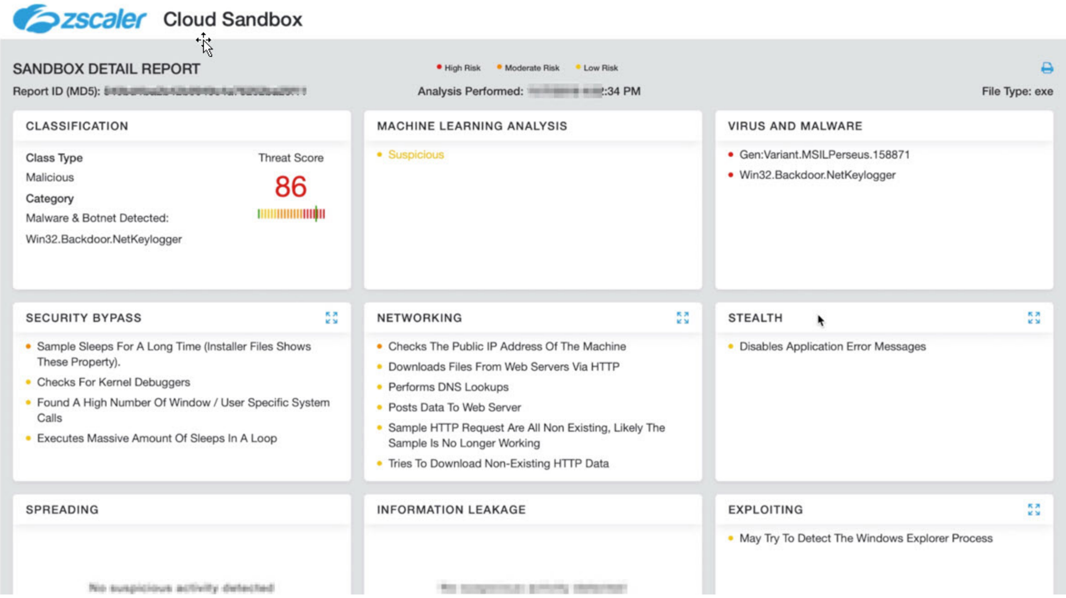
Insights Logs

Feb 03, 03:00:47 PM - Feb 12, 10:45:27 PM
15 Log Records Found

MD5	DLP Identifier	Unscannable Type	Fo...	MD5	Forwarding ...
	None	None	N...	886d509100c8afb3da7369b4a12577dd	None
	None	None	N...	7eb15e8f4069ce8397ef22ecfe9a55ce	None
	None	None	N...	c	None
	None	None	N...	886d509100c8afb3da7369b4a12577dd	None
	None	None	N...	260141d1370ba9ba6ddef678f7ccb2ea	None
	None	None	N...	f57b847cb93afbb8510b61f21db22215	None
	None	None	N...	447c2f2eda81be01ba51ab4e24b53f06	None
	None	None	N...	322aab28d6d17d5ab08c95a45d7ca53b	None
	None	None	N...	f57b847cb93afbb8510b61f21db22215	None
	None	None	N...	322aab28d6d17d5ab08c95a45d7ca53b	None
	None	None	N...	6bd36009a6c96a2bb73362ea5b8d0a24	None

Figure 60. Access the Sandbox report

5. Review the Sandbox Detail report for detailed information regarding file detonation results.



SANDBOX DETAIL REPORT

Report ID (MD5): [redacted]

Analysis Performed: [redacted]:34 PM

File Type: exe

CLASSIFICATION

Class Type
Malicious

Category
Malware & Botnet Detected:
Win32.Backdoor.NetKeylogger

Threat Score
86

MACHINE LEARNING ANALYSIS

- Suspicious

VIRUS AND MALWARE

- Gen:Variant.MSILPerseus.158871
- Win32.Backdoor.NetKeylogger

SECURITY BYPASS

- Sample Sleeps For A Long Time (Installer Files Shows These Property).
- Checks For Kernel Debuggers
- Found A High Number Of Window / User Specific System Calls
- Executes Massive Amount Of Sleeps In A Loop

NETWORKING

- Checks The Public IP Address Of The Machine
- Downloads Files From Web Servers Via HTTP
- Performs DNS Lookups
- Posts Data To Web Server
- Sample HTTP Request Are All Non Existing, Likely The Sample Is No Longer Working
- Tries To Download Non-Existing HTTP Data

STEALTH

- Disables Application Error Messages

SPREADING

No suspicious activity detected

INFORMATION LEAKAGE

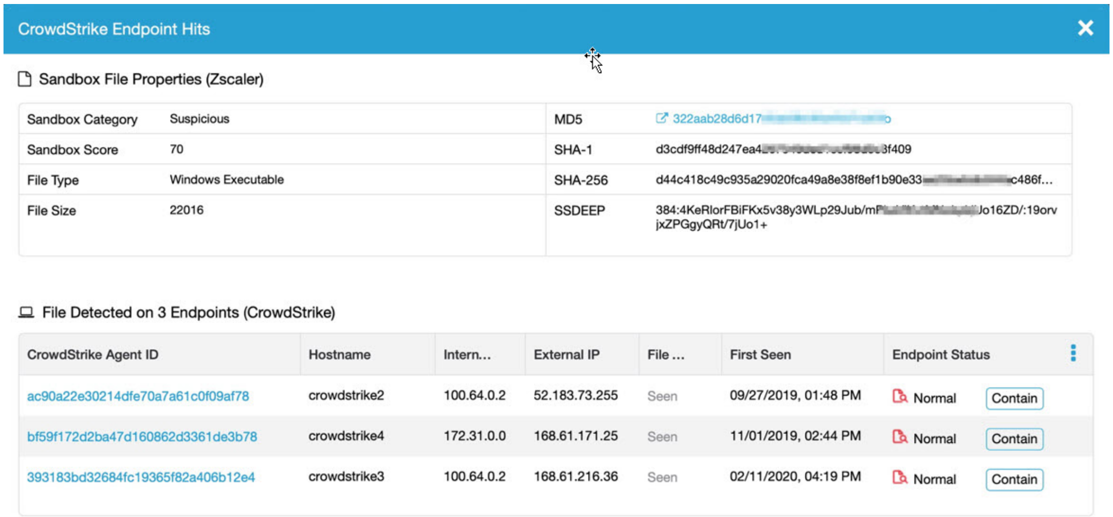
[illegible]

EXPLOITING

- May Try To Detect The Windows Explorer Process

Figure 61. Sandbox Detail report

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



CrowdStrike Endpoint Hits

Sandbox File Properties (Zscaler)

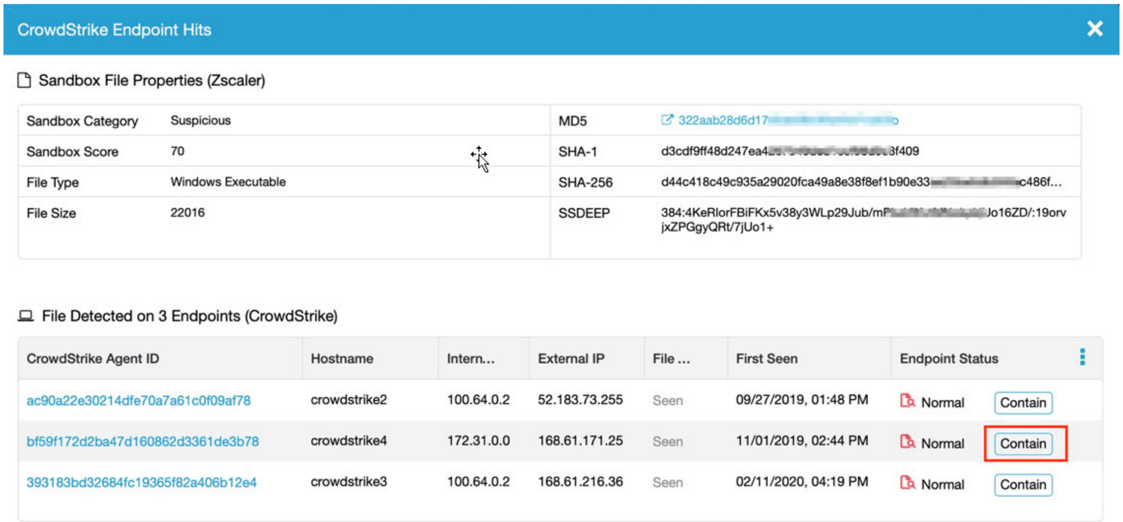
Sandbox Category	Suspicious	MD5	322aab28d6d17[redacted]
Sandbox Score	70	SHA-1	d3cdf9ff48d247ea4[redacted]3f409
File Type	Windows Executable	SHA-256	d44c418c49c935a29020fca49a8e38f8ef1b90e33[redacted]c486f...
File Size	22016	SSDEEP	384:4KeRlorFBiFKx5v38y3WLp29Jub/mP[redacted]Jo16ZD/:19orv jxZPGgyQRt/7jUo1+

File Detected on 3 Endpoints (CrowdStrike)

CrowdStrike Agent ID	Hostname	Intern...	External IP	File ...	First Seen	Endpoint Status	
ac90a22e30214dfe70a7a61c0f09af78	crowdstrike2	100.64.0.2	52.183.73.255	Seen	09/27/2019, 01:48 PM	Normal	Contain
bf59f172d2ba47d160862d3361de3b78	crowdstrike4	172.31.0.0	168.61.171.25	Seen	11/01/2019, 02:44 PM	Normal	Contain
393183bd32684fc19365f82a406b12e4	crowdstrike3	100.64.0.2	168.61.216.36	Seen	02/11/2020, 04:19 PM	Normal	Contain

Figure 62. CrowdStrike Endpoint Hits report

7. Click **Contain** to trigger an API call to CrowdStrike. When you trigger the API to contain the endpoint, CrowdStrike prevents the endpoint from connecting to the network. This isolates the endpoint and prevents it from allowing malicious software on the endpoint from accessing the rest of the network via the network connection.



CrowdStrike Endpoint Hits

Sandbox File Properties (Zscaler)

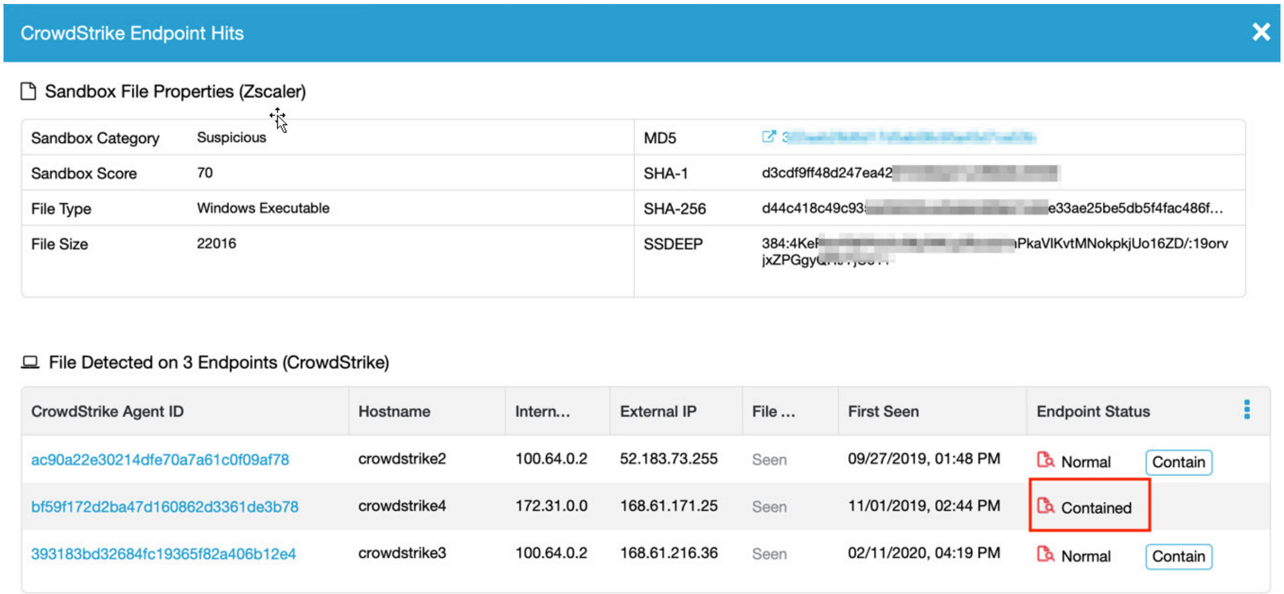
Sandbox Category	Suspicious	MD5	322aab28d6d17[redacted]o
Sandbox Score	70	SHA-1	d3cdf9ff48d247ea4[redacted]3f409
File Type	Windows Executable	SHA-256	d44c418c49c935a29020fca49a8e38f8ef1b90e33[redacted]c486f...
File Size	22016	SSDEEP	384:4KeRlorFBiFKx5v38y3WLp29Jub/mP[redacted]Jo16ZD/:19orv jxZPGgyQRt/7jUo1+

File Detected on 3 Endpoints (CrowdStrike)

CrowdStrike Agent ID	Hostname	Intern...	External IP	File ...	First Seen	Endpoint Status
ac90a22e30214dfe70a7a61c0f09af78	crowdstrike2	100.64.0.2	52.183.73.255	Seen	09/27/2019, 01:48 PM	Normal Contain
bf59f172d2ba47d160862d3361de3b78	crowdstrike4	172.31.0.0	168.61.171.25	Seen	11/01/2019, 02:44 PM	Normal Contain
393183bd32684fc19365f82a406b12e4	crowdstrike3	100.64.0.2	168.61.216.36	Seen	02/11/2020, 04:19 PM	Normal Contain

Figure 63. Contain an endpoint

8. Access the CrowdStrike Endpoint Hits report again to confirm the containment status.



CrowdStrike Endpoint Hits

Sandbox File Properties (Zscaler)

Sandbox Category	Suspicious	MD5	3[redacted]
Sandbox Score	70	SHA-1	d3cdf9ff48d247ea42[redacted]
File Type	Windows Executable	SHA-256	d44c418c49c93[redacted]e33ae25be5db5f4fac486f...
File Size	22016	SSDEEP	384:4KeF[redacted]PkaVlKvtMNokpkjUo16ZD/:19orv jxZPGgy[redacted]

File Detected on 3 Endpoints (CrowdStrike)

CrowdStrike Agent ID	Hostname	Intern...	External IP	File ...	First Seen	Endpoint Status
ac90a22e30214dfe70a7a61c0f09af78	crowdstrike2	100.64.0.2	52.183.73.255	Seen	09/27/2019, 01:48 PM	Normal Contain
bf59f172d2ba47d160862d3361de3b78	crowdstrike4	172.31.0.0	168.61.171.25	Seen	11/01/2019, 02:44 PM	Contained
393183bd32684fc19365f82a406b12e4	crowdstrike3	100.64.0.2	168.61.216.36	Seen	02/11/2020, 04:19 PM	Normal Contain

Figure 64. Confirm containment status

Use Case 5: Threat Intelligence Sharing—CrowdStrike Falcon and ZIA

When CrowdStrike's Falcon threat intelligence data is shared with Zscaler Zero Trust Exchange (ZTE), seamless usage integrations 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 indicators of compromise (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.

You 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 database of malicious IPs, Domains, or URLs (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. You can bring in your own custom threat feeds and populate these URL lists. You can then reference these custom URL lists in ZIA URL policies for granularly controlling end user access within that ZIA tenant.
- CrowdStrike Falcon expands your defenses with real-time access to global IoCs delivered by CrowdStrike. An existing CrowdStrike Falcon intelligence and ZIA customer can set up 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.

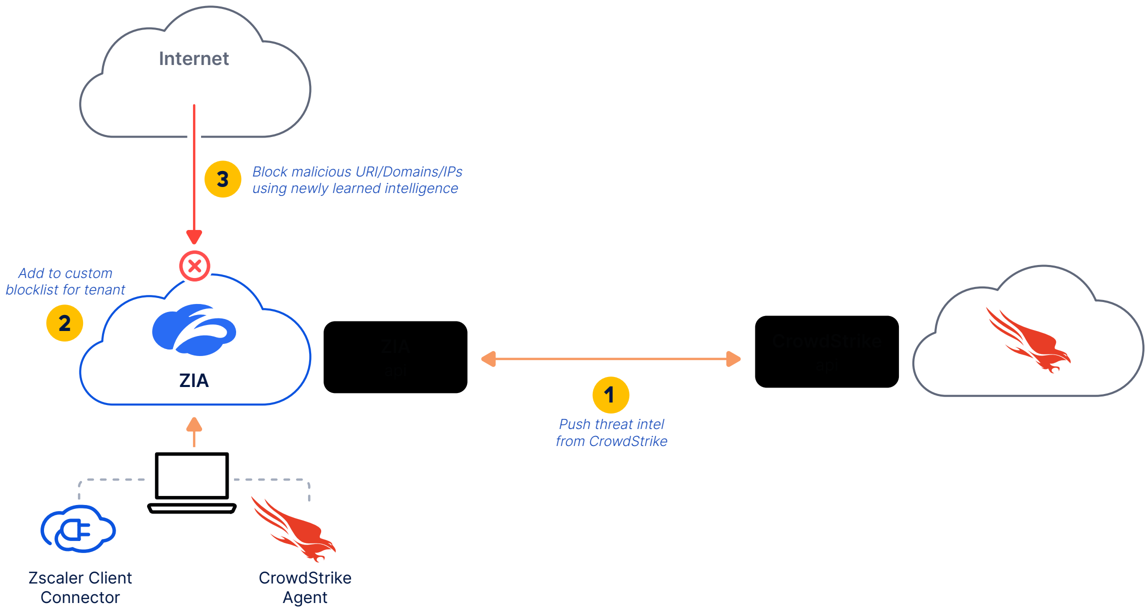

Internet
3
Block malicious URI/Domains/IPs using newly learned intelligence
Add to custom blocklist for tenant
2
ZIA
[redacted]
[redacted]
1
Push threat intel from CrowdStrike
Zscaler Client Connector
CrowdStrike Agent

Figure 65. High-level overview

This version of the CrowdStrike Falcon ZIA Intel Bridge features a codebase overhaul rewritten for legibility, ease of modification, and simplicity in troubleshooting. CrowdStrike Falcon programmatic operations provide a more modularized source code and comprehensible modification process.

Furthermore, improved logging capabilities and error handling simplifies troubleshooting and support. Any user challenged with excessive runtime troubles can find detailed logs in the /logs directory. Including the log information in a support case ensures efficient, effective remediation.

CrowdStrike Falcon approaches this use case slightly differently. Originally, the CrowdStrike Falcon Indicators database included 175K high-confidence, malicious URLs, which was compatible with Zscaler's 275K custom URL limit. Over the past year and a half, the number of high-confidence malicious URLs in the CrowdStrike Falcon Indicators database has grown to several million. A different approach to maintaining the Intel Bridge was required.

The integration version ensures that multiple indicators are present in the ZIA custom URL category. You can configure the number of indicators to your environment's unique limit. ZIA users get the latest indicators from CrowdStrike's intelligence team. By the time those indicators start to appear in other third-party feeds, the Intel Bridge already updates the ZIA URL category with the most recent indicators available.

Prerequisites

Make sure the following prerequisites are met:

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

You can push the default number, 25K, of custom IoCs into a ZIA tenant.

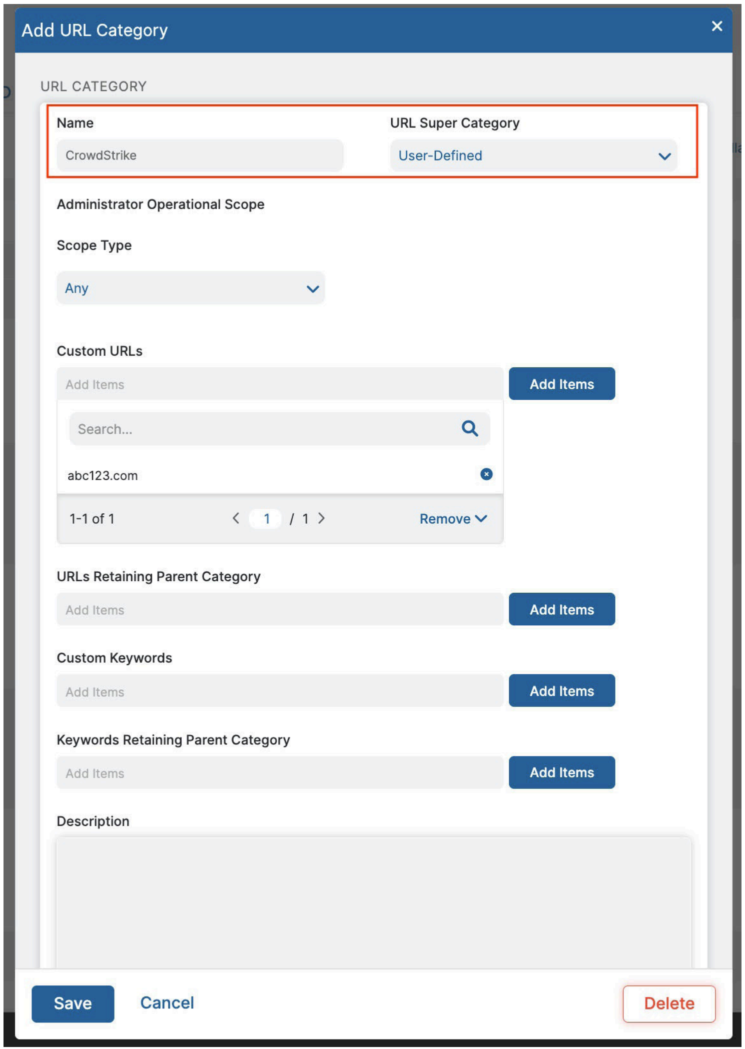
You can increase the IoC quota (with a maximum up to 275K) by contacting your Zscaler Account team and purchasing licenses for additional custom URLs.

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.

Create a Zscaler URL Category

To create a Zscaler URL category:

1. Log in to your ZIA Admin Portal.
2. Go to **Administration** > **URL Categories**.
3. Add a new URL category with the name **CrowdStrike**.
4. From the **URL Super Category** drop-down menu, select **User-Defined**.
5. Click **Save**.



Add URL Category

URL CATEGORY

Name: CrowdStrike

URL Super Category: User-Defined

Administrator Operational Scope

Scope Type: Any

Custom URLs: abc123.com

1-1 of 1

URLs Retaining Parent Category

Custom Keywords

Keywords Retaining Parent Category

Description

Figure 66. Create a custom URL category in the ZIA Admin Portal

CrowdStrike OAuth 2.0 Token Scope

In the CrowdStrike Falcon Console:

1. Go to **API Clients and Keys**.
2. Click **Add a New API Client**.
3. Create a client with READ permissions for **Indicators (Falcon X)**.
4. Save the resulting values. You need them to run the integration.

Download Repository

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

cd zscaler-FalconX-integration
```

Install Dependencies with pip3

```
pip3 install -r requirements.txt
```

Configure

Input your configurations in config.ini. Do not use quotes or ticks for any of these values.

Most of the fields are self-explanatory, but be sure to put some thought into the LIMIT field. This field determines how many malicious URLs the Intel Bridge maintains in your ZIA tenant. Zscaler offers different subscription tiers with varying maximum custom URLs (from 25K to 275K). Consider this and your existing custom URL categories when you choose a value, as going over the limit causes runtime errors.

For example, if you have a limit of 25K, and are already using 10K in another URL category, a value like 14000 won't exceed the limit and leaves some overhead.

```
[CROWDSTRIKE]

client=<Your Falcon API Client ID>

secret=<Your Falcon API Client Secret>

base_url=<Your Falcon API Base URL> (ex: https://api.crowdstrike.com)

limit=<Number of indicators to maintain> (Max: 275,000 Default 10,000)

[ZSCALER]

hostname=<Your zscaler Hostname> (Hostname only requires the base URL (i.e. https://
zsapi.zscalerthree.net))

username=<Your ZIA Username>

password=<Your ZIA Passsword>

token=<Your ZIA API token>

[CHRON]

disable_loop=Change this value to 1 if you are running the Intel Bridge via Chron job.
This will force the program to quit after running. (Default 0, looping enabled)

[LOG]

log_indicators=Change this value to 1 for indicators to be logged in logs/data_log as
they are deleted and loaded.
```

Running the Integration

With Python 3.7+ installed:

```
python3 intelbridge
```

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.

To learn more on how to get the ZIA API key, see the ZIA Cloud Service API Developers Guide (government agencies, see ZIA Cloud Service API Developers Guide).

Use Case 6: CrowdStrike Humio Essential Configuration (Cloud-to-Cloud)

This section details the steps required to stream ZIA logs to a CrowdStrike Humio cloud from Zscaler, using Humio's HTTP/HTTPS 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`).

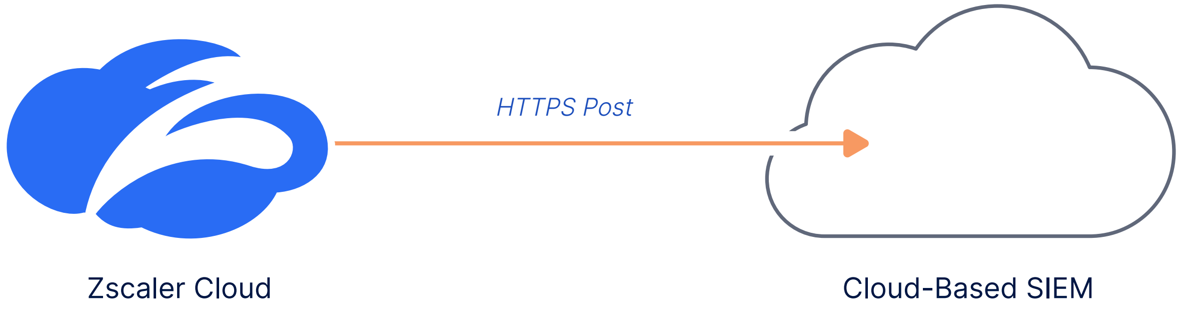


Figure 67. High-level overview of cloud-to-cloud logging

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

To learn more, see:

- Understanding Nanolog Streaming Service (government agencies, see Understanding Nanolog Streaming Service).
- About Cloud NSS Feeds (government agencies, see About Cloud NSS Feeds).
- Adding Cloud NSS Feed for Web Logs (government agencies, see Adding Cloud NSS Feed for Web Logs).

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.

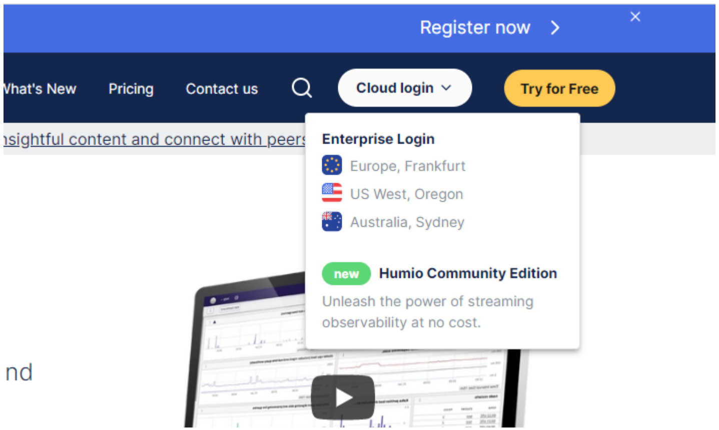
Installation of the package is straightforward, and the installation deploys the parser, saved queries, and dashboards directly into the repository that you select. You must add 5 ingest tokens, one for each NSS log source assigned to its corresponding parser.

Then create a new cloud NSS feed in the ZIA Admin Portal for the sources included in this package. Configure these feeds with your Humio API URL and ingest token.

Log In to CrowdStrike Humio Cloud Tenant

Log in to CrowdStrike Humio tenant via the online portal.

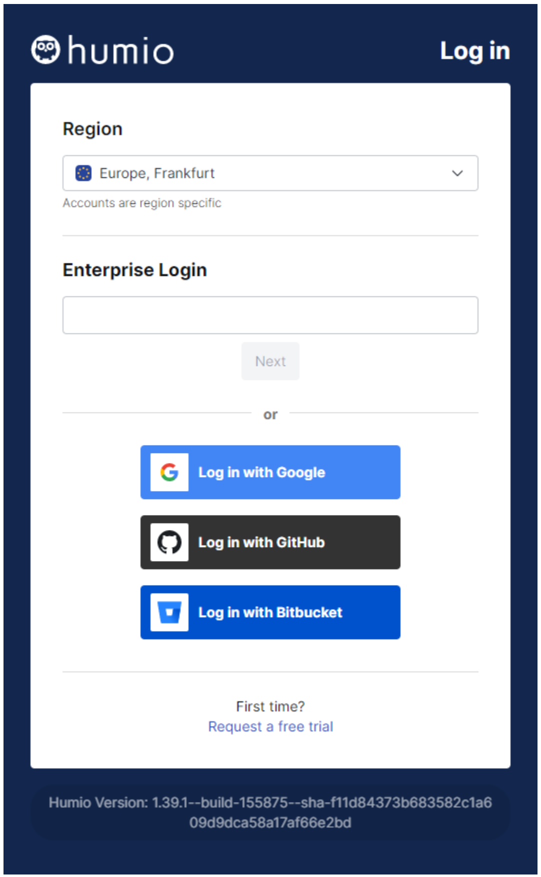
1. Go to humio.com and select **Cloud login** > **Enterprise Login**.



Unleash the power of streaming observability at no cost.

Figure 68. Humio.com Cloud login

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



Humio Version: 1.39.1--build-155875--sha-f11d84373b683582c1a6 09d9dca58a17af66e2bd

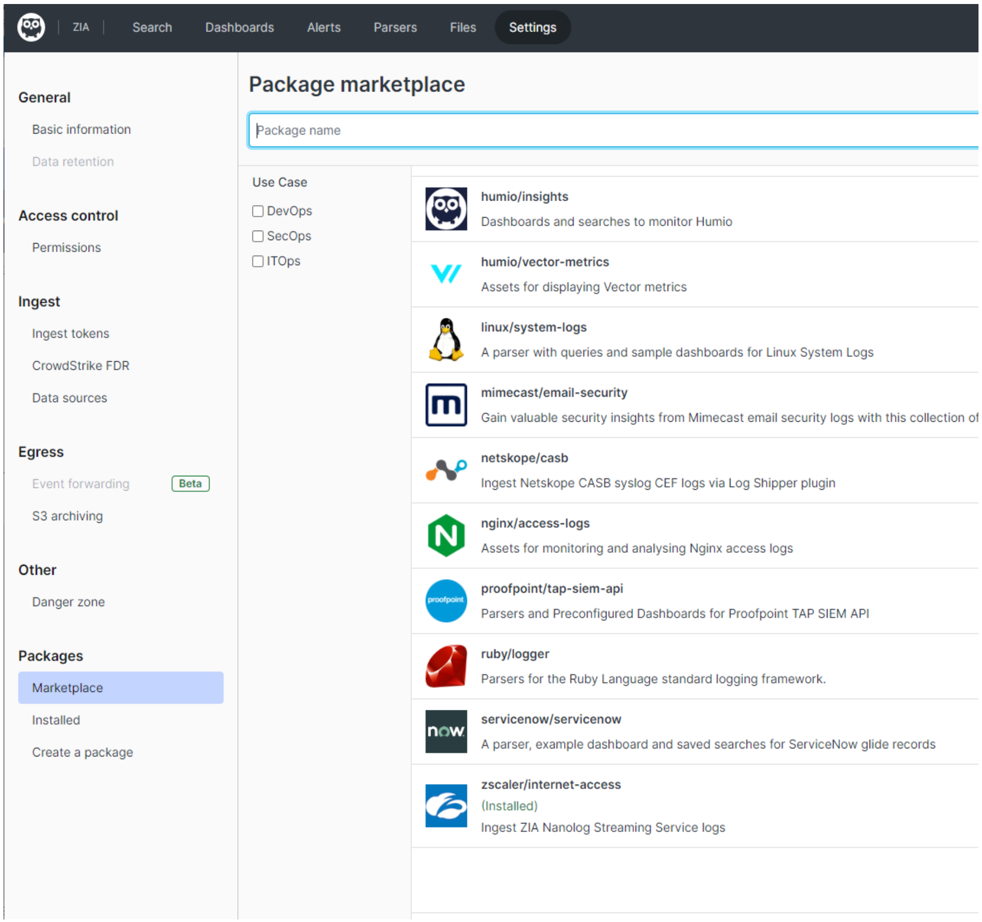
Figure 69. Log in to Humio Cloud tenant

3. Log in to the cloud with admin credentials.

Install the ZIA Package in Your Cloud Tenant

After logging in:

1. Go to **Settings** > **Packages** > **Marketplace**.



humio/insights
Dashboards and searches to monitor Humio

humio/vector-metrics
Assets for displaying Vector metrics

linux/system-logs
A parser with queries and sample dashboards for Linux System Logs

mimecast/email-security
Gain valuable security insights from Mimecast email security logs with this collection of

netskope/casb
Ingest Netskope CASB syslog CEF logs via Log Shipper plugin

nginx/access-logs
Assets for monitoring and analysing Nginx access logs

proofpoint/tap-siem-api
Parsers and Preconfigured Dashboards for Proofpoint TAP SIEM API

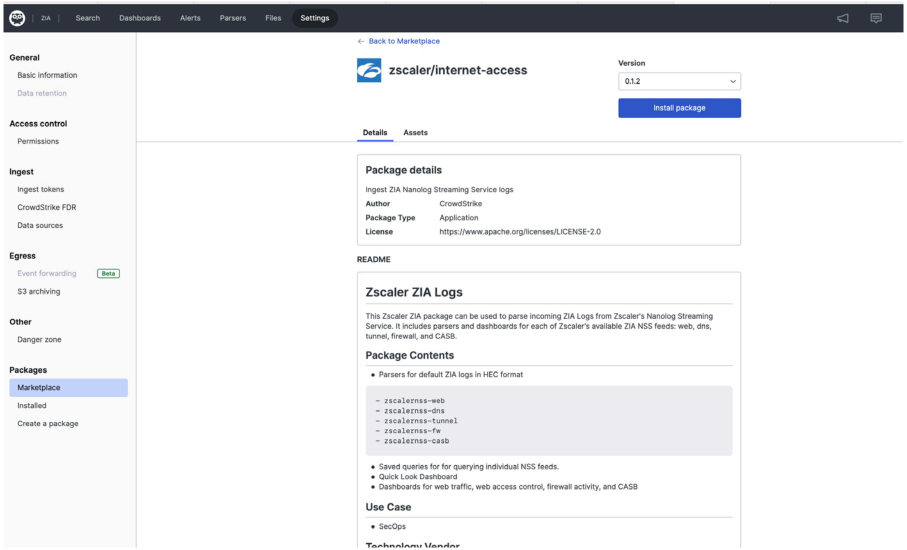
ruby/logger
Parsers for the Ruby Language standard logging framework.

servicenow/servicenow
A parser, example dashboard and saved searches for ServiceNow glide records

zscaler/internet-access
(Installed)
Ingest ZIA Nanolog Streaming Service logs

Figure 70. Humio Marketplace

2. Select **zscaler/internet-access** from the list of apps.



zscaler/internet-access

Version: 0.1.2

Package details

Ingest ZIA Nanolog Streaming Service logs

Author	CrowdStrike
Package Type	Application
License	https://www.apache.org/licenses/LICENSE-2.0

README

Zscaler ZIA Logs

This Zscaler ZIA package can be used to parse incoming ZIA Logs from Zscaler's Nanolog Streaming Service. It includes parsers and dashboards for each of Zscaler's available ZIA NSS feeds: web, dns, tunnel, firewall, and CASB.

Package Contents

- Parsers for default ZIA logs in HEC format

```
- zscalernss-web
- zscalernss-dns
- zscalernss-tunnel
- zscalernss-fw
- zscalernss-casb
```

- Saved queries for for querying individual NSS feeds.
- Quick Look Dashboard
- Dashboards for web traffic, web access control, firewall activity, and CASB

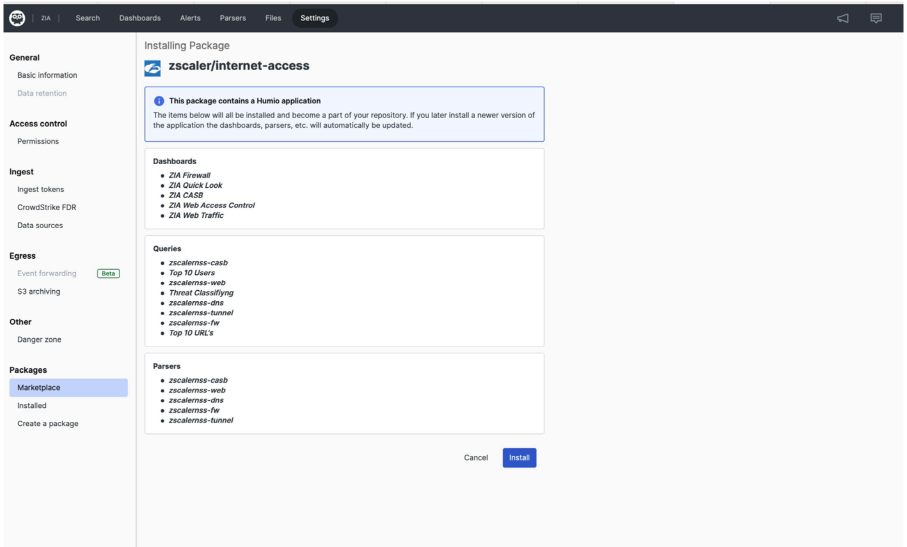
Use Case

- SecOps

Technology Vendor

Figure 71. Install ZIA package

3. Click **Install package**. A list of app features is displayed.



Installing Package

zscaler/internet-access

This package contains a Humio application

The items below will all be installed and become a part of your repository. If you later install a newer version of the application the dashboards, parsers, etc. will automatically be updated.

Dashboards

- *ZIA Firewall*
- *ZIA Quick Look*
- *ZIA CASB*
- *ZIA Web Access Control*
- *ZIA Web Traffic*

Queries

- *zscalernss-casb*
- *Top 10 Users*
- *zscalernss-web*
- *Threat Classifiyng*
- *zscalernss-dns*
- *zscalernss-tunnel*
- *zscalernss-fw*
- *Top 10 URL's*

Parsers

- *zscalernss-casb*
- *zscalernss-web*
- *zscalernss-dns*
- *zscalernss-fw*
- *zscalernss-tunnel*

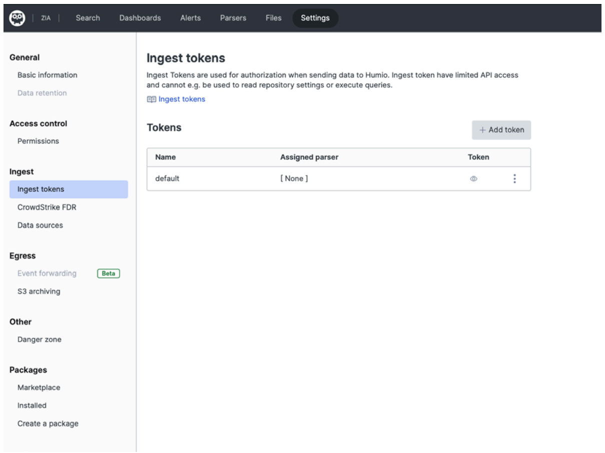
Figure 72. List of ZIA package features

4. Click **Install**.

Create and Add Ingest Tokens in CrowdStrike Humio

After installing the ZIA package:

1. Go to **Settings** > **Ingest** > **Ingest tokens**.
2. Click **Add token**.



Ingest tokens

Ingest Tokens are used for authorization when sending data to Humio. Ingest token have limited API access and cannot e.g. be used to read repository settings or execute queries.

Ingest tokens

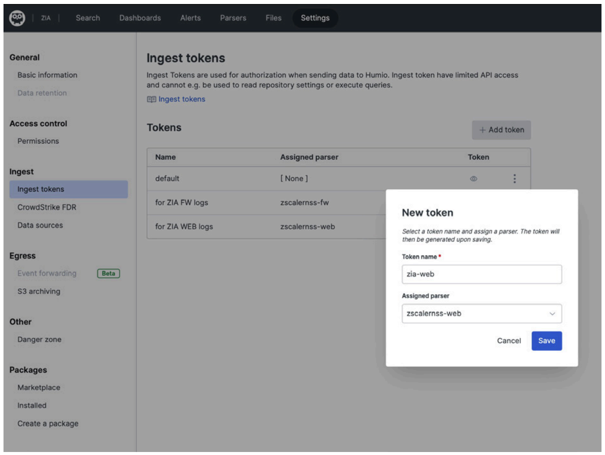
Tokens

Name	Assigned parser	Token
default	[None]	

Figure 73. Ingest tokens window

3. In the **New token** window:
   - **Token name**: Enter 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:
     - zscalernss-web
     - zscalernss-dns
     - zscalernss-tunnel
     - zscalernss-fw
     - zscalernss-casb

4. Click **Save**. The **Token** dialog displays with the token value.



Ingest tokens

Ingest Tokens are used for authorization when sending data to Humio. Ingest token have limited API access and cannot e.g. be used to read repository settings or execute queries.

Ingest tokens

Tokens

Name	Assigned parser	Token
default	[None]	
for ZIA FW logs	zscalernss-fw	
for ZIA WEB logs	zscalernss-web	

New token

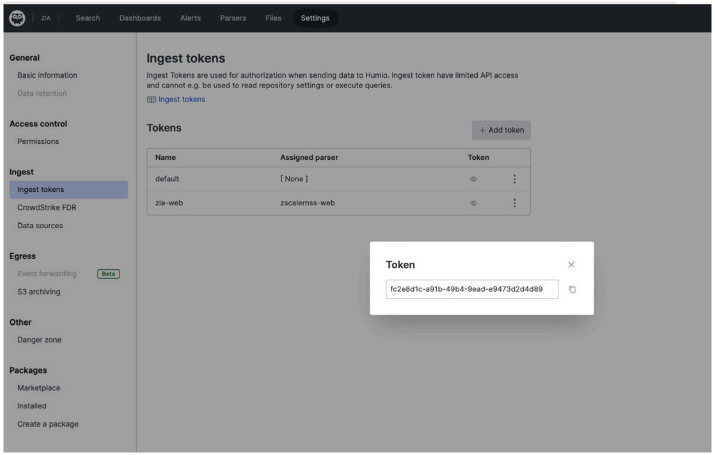
Select a token name and assign a parser. The token will then be generated upon saving.

Token name *: zia-web

Assigned parser: zscalernss-web

Figure 74. New token dialog

5. Copy this token value to paste into Zscaler when creating the Cloud NSS feed for Humio.



Ingest tokens

Ingest Tokens are used for authorization when sending data to Humio. Ingest token have limited API access and cannot e.g. be used to read repository settings or execute queries.

Ingest tokens

Tokens

Name	Assigned parser	Token
default	[None]	
zia-web	zscalernss-web	

Token

fc2e8d1c-a91b-49b4-9ead-e9473d2d4d89

Figure 75. Token value

Configure Zscaler 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/HTTPS API feed that pushes logs from the Zscaler cloud service into an HTTP/HTTPS API endpoint on the SIEM. The following steps show how to set up the log feed for web logs. Repeat these steps to set up other Zscaler log types (e.g., Firewall or DNS logs).

Go to Cloud-to-Cloud Logging Section in the ZIA Admin Portal

From the ZIA Admin Portal, go to **Administration** > **Nanolog Streaming Service** > **Cloud NSS Feeds** > **Add Cloud NSS Feed**.

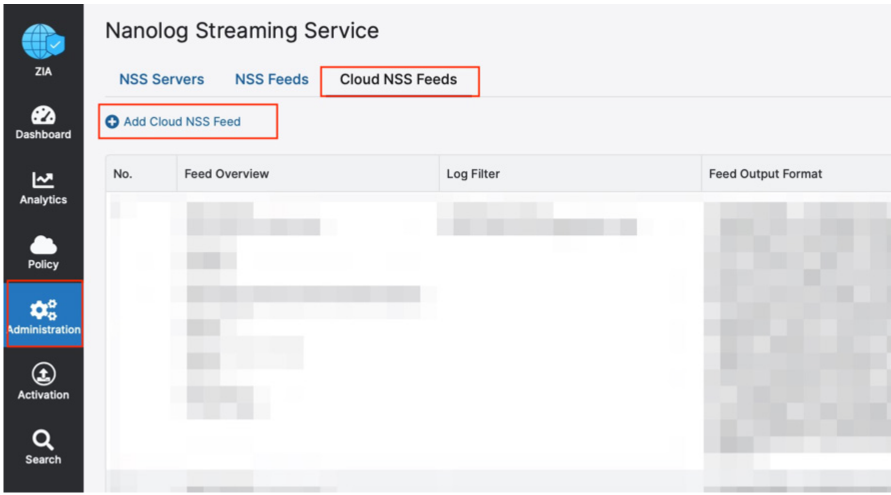
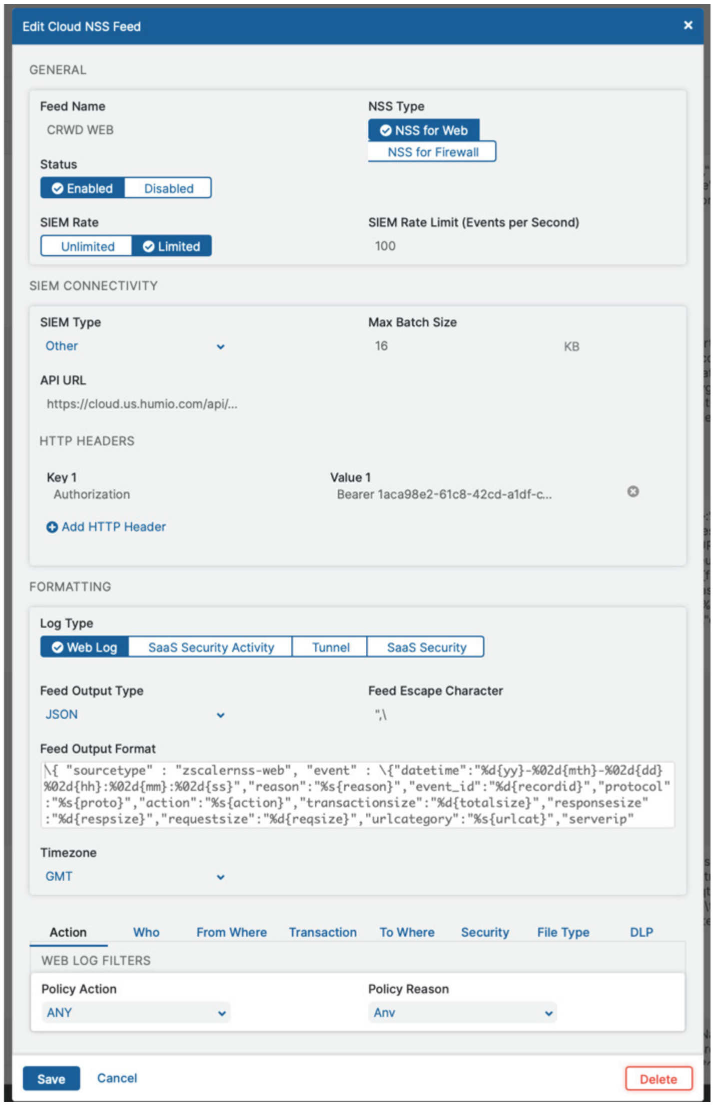


Figure 76. Go to cloud-to-cloud logging section in ZIA

Set Up 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, which is dependent on the customer's Humio cloud location. The authorization header contains the relevant Humio HEC token created in previous steps.
2. In the **Add Cloud NSS Feed** dialog:
   a. **Key1**: Enter `Authorization`.
   b. **Value1**: Enter the Humio HEC token in the format `Bearer XXX-XXX-XXX` (replace xxx with actual HEC token value).
3. **Feed Output Type** is **JSON** from the drop-down menu. Save the configuration after providing the required parameters. Add **",** \ (double quote, comma, backslash) to the **Feed Escape Character** list.



Edit Cloud NSS Feed

GENERAL

Feed Name: CRWD WEB

NSS Type: ● NSS for Web ○ NSS for Firewall

Status: ● Enabled ○ Disabled

SIEM Rate: ○ Unlimited ● Limited

SIEM Rate Limit (Events per Second): 100

SIEM CONNECTIVITY

SIEM Type: Other

Max Batch Size: 16 KB

API URL: https://cloud.us.humio.com/api/...

HTTP HEADERS

Key 1: Authorization

Value 1: Bearer 1aca98e2-61c8-42cd-a1df-c...

Add HTTP Header

FORMATTING

Log Type: ● Web Log ○ SaaS Security Activity ○ Tunnel ○ SaaS Security

Feed Output Type: JSON

Feed Escape Character: ",\

Feed Output Format:

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd}
%02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol"
:"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize"
:"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip"
```

Timezone: GMT

WEB LOG FILTERS

Policy Action: ANY

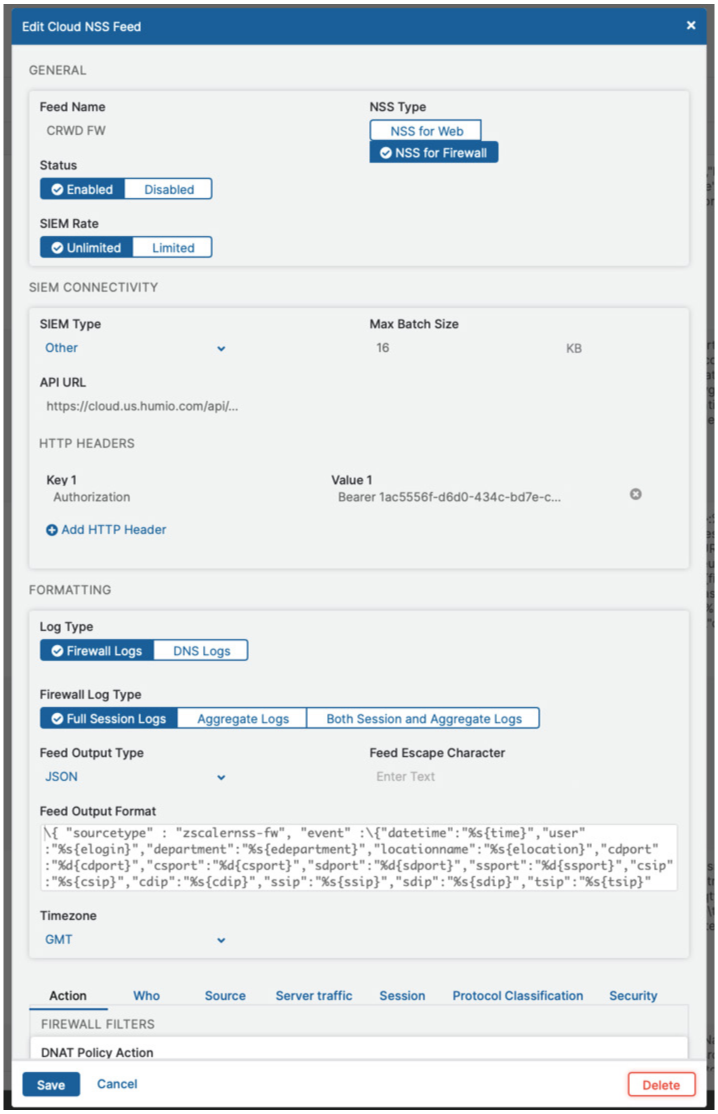
Policy Reason: Anv

Figure 77. Example with all fields populated (web)

Set Up 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 the 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. The authorization header contains the relevant Humio HEC token.
3. In the **Add Cloud NSS Feed** dialog:
   a. **Key1**: Enter `Authorization`.
   b. **Value1**: Enter the HEC token in format `Bearer XXX-XXX-XXX` (replace `xxx` with actual HEC token value).
4. Select the **Feed Output Type** of **JSON** from the drop-down menu.
5. Provide the required parameters and then click **Save**.



Edit Cloud NSS Feed

GENERAL

Feed Name: CRWD FW

NSS Type: NSS for Web / ✓ NSS for Firewall

Status: ✓ Enabled / Disabled

SIEM Rate: ✓ Unlimited / Limited

SIEM CONNECTIVITY

SIEM Type: Other

Max Batch Size: 16 KB

API URL: https://cloud.us.humio.com/api/...

HTTP HEADERS

Key 1: Authorization

Value 1: Bearer 1ac5556f-d6d0-434c-bd7e-c...

FORMATTING

Log Type: ✓ Firewall Logs / DNS Logs

Firewall Log Type: ✓ Full Session Logs / Aggregate Logs / Both Session and Aggregate Logs

Feed Output Type: JSON

Feed Escape Character: Enter Text

Feed Output Format:

```
\{ "sourcetype" : "zscalernss-fw", "event" :\{"datetime":"%s{time}","user"
:"%s{elogin}","department":"%s{edepartment}","locationname":"%s{elocation}","cdport"
:"%d{cdport}","csport":"%d{csport}","sdport":"%d{sdport}","ssport":"%d{ssport}","csip"
:"%s{csip}","cdip":"%s{cdip}","ssip":"%s{ssip}","sdip":"%s{sdip}","tsip":"%s{tsip}"
```

Timezone: GMT

FIREWALL FILTERS

DNAT Policy Action

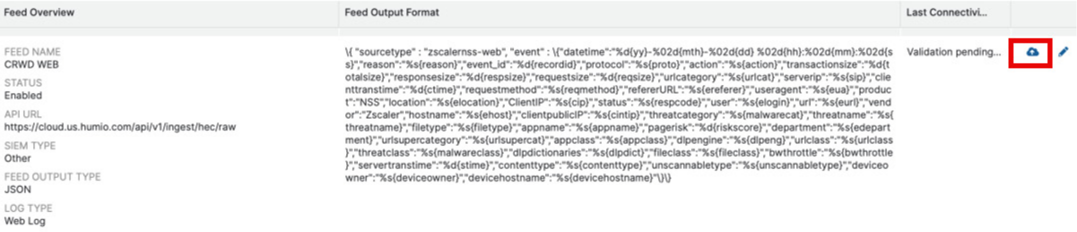
Figure 78. Example with all fields populated (firewall)

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

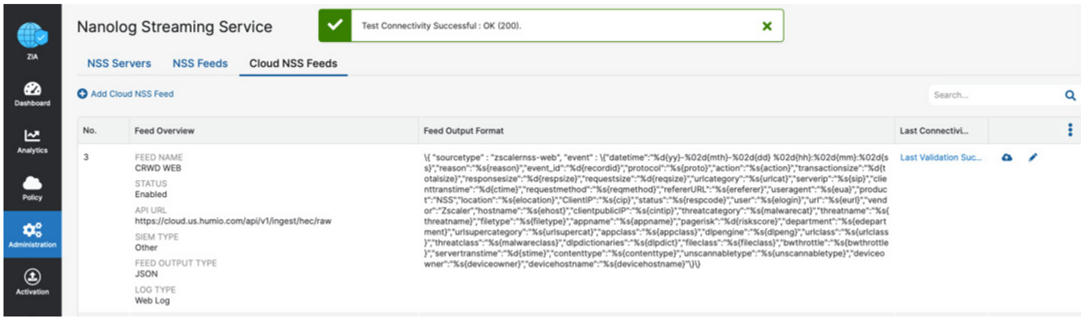
After you save the configuration, click the **Verify** icon shown in the following figure to verify connectivity from ZIA cloud to the Humio cloud. This sends a sample or test log message from the ZIA cloud to Humio. Cloud-to-cloud connectivity is verified if Humio sends the expected response.



Feed Overview	Feed Output Format	Last Connectivi...
FEED NAME CRWD WEB STATUS Enabled API URL https://cloud.us.humio.com/api/v1/ingest/hec/raw SIEM TYPE Other FEED OUTPUT TYPE JSON LOG TYPE Web Log	\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize":"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip":"%s{sip}","clienttranstime":"%d{ctime}","requestmethod":"%s{reqmethod}","refererURL":"%s{ereferer}","useragent":"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP":"%s{cip}","status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}","threatcategory":"%s{malwarecat}","threatname":"%s{threatname}","filetype":"%s{filetype}","appname":"%s{appname}","pagerisk":"%d{riskscore}","department":"%s{edepartment}","urlsupercategory":"%s{urlsupercat}","appclass":"%s{appclass}","dlpengine":"%s{dlpeng}","urlclass":"%s{urlclass}","threatclass":"%s{malwareclass}","dlpdictionaries":"%s{dlpdict}","fileclass":"%s{fileclass}","bwthrottle":"%s{bwthrottle}","servertranstime":"%d{stime}","contenttype":"%s{contenttype}","unscannabletype":"%s{unscannabletype}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"\}\}	Validation pending...

Figure 79. Verify connectivity to Humio cloud

When the connectivity is verified, the **Last Connectivity Test** column changes from **Last Validation Pending** to **Last Validation Successful**.



Test Connectivity Successful : OK (200).

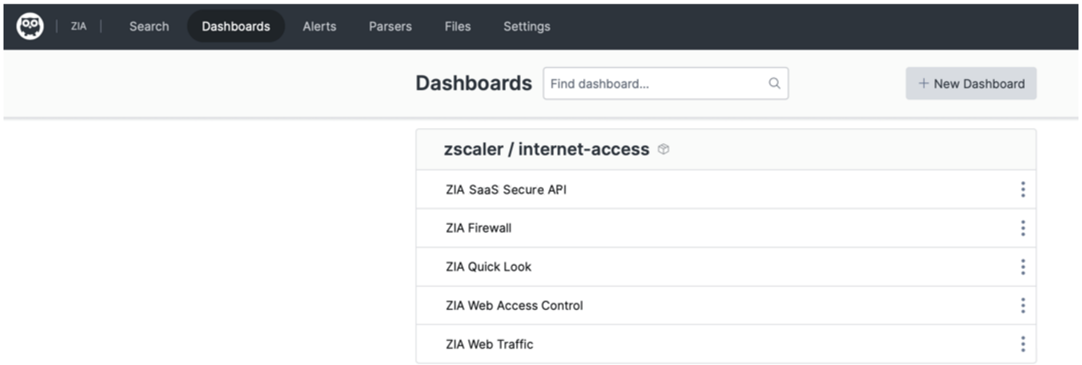
No.	Feed Overview	Feed Output Format	Last Connectivi...
3	FEED NAME CRWD WEB STATUS Enabled API URL https://cloud.us.humio.com/api/v1/ingest/hec/raw SIEM TYPE Other FEED OUTPUT TYPE JSON LOG TYPE Web Log	\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize":"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip":"%s{sip}","clienttranstime":"%d{ctime}","requestmethod":"%s{reqmethod}","refererURL":"%s{ereferer}","useragent":"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP":"%s{cip}","status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}","threatcategory":"%s{malwarecat}","threatname":"%s{threatname}","filetype":"%s{filetype}","appname":"%s{appname}","pagerisk":"%d{riskscore}","department":"%s{edepartment}","urlsupercategory":"%s{urlsupercat}","appclass":"%s{appclass}","dlpengine":"%s{dlpeng}","urlclass":"%s{urlclass}","threatclass":"%s{malwareclass}","dlpdictionaries":"%s{dlpdict}","fileclass":"%s{fileclass}","bwthrottle":"%s{bwthrottle}","servertranstime":"%d{stime}","contenttype":"%s{contenttype}","unscannabletype":"%s{unscannabletype}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"\}\}	Last Validation Suc...

Figure 80. Humio cloud connectivity verified

Verify Log Flow Using Humio's Zscaler Package

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

The dashboard is populated with incoming Zscaler log data.


ZIA | Search | Dashboards | Alerts | Parsers | Files | Settings

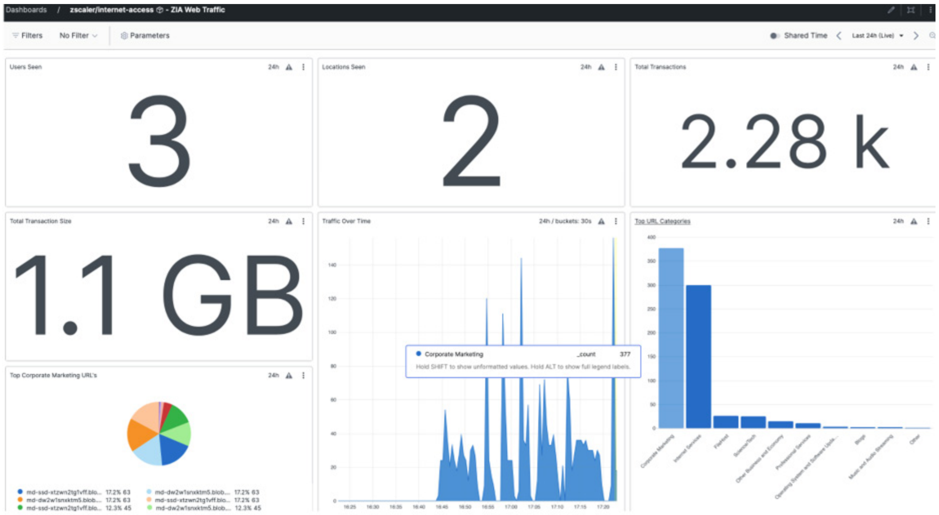
Dashboards | Find dashboard... | + New Dashboard

zscaler / internet-access

- ZIA SaaS Secure API
- ZIA Firewall
- ZIA Quick Look
- ZIA Web Access Control
- ZIA Web Traffic

Figure 81. Check Humio Zscaler dashboards

If you see that a particular widget is not populated, click the **More** icon (vertical ellipsis) next to it to see the query that the panel is running. Understanding the query helps you troubleshoot.


Dashboards / zscaler/internet-access - ZIA Web Traffic

Users Seen: 3

Locations Seen: 2

Total Transactions: 2.28 k

Total Transaction Size: 1.1 GB

Corporate Marketing _count 377

Hold SHIFT to show unformatted values. Hold ALT to show full legend labels.

Filters
No Filter
Parameters
Shared Time
Last 24h (Live)
24h
Traffic Over Time
24h / buckets: 30s
Top URL Categories
Top Corporate Marketing URL's
0
20
40
60
80
100
120
140
16:25
16:30
16:35
16:40
16:45
16:50
16:55
17:00
17:05
17:10
17:15
17:20
50
150
200
250
300
350
400
Corporate Marketing
Internet Services
FileHost
Science/Tech
Other Business and Economy
Professional Services
Operating System and Software Upda...
Blogs
Music and Audio Streaming
Other
md-ssd-xtzwn2tg1vff.blo... 17.2% 63
md-dw2w1snxktm5.blob... 17.2% 63
md-ssd-xtzwn2tg1vff.blo... 12.3% 45
md-dw2w1snxktm5.blob... 17.2% 63
md-ssd-xtzwn2tg1vff.blo... 17.2% 63
md-dw2w1snxktm5.blob... 12.3% 45

Figure 82. Widgets within Humio Zscaler dashboards

Use Case 7: CrowdStrike NG-SIEM Essential Configuration (Cloud-to-Cloud)

This section details the steps required to stream ZIA logs to CrowdStrike Next-Generation SIEM (NG-SIEM) from Zscaler, using NG-SIEM's HTTPS 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 ZIA log types: Web, SaaS Security, Tunnel, Firewall, DNS, etc.

For the CrowdStrike NG-SIEM, the log ingestion API is /v1/services/collector/raw

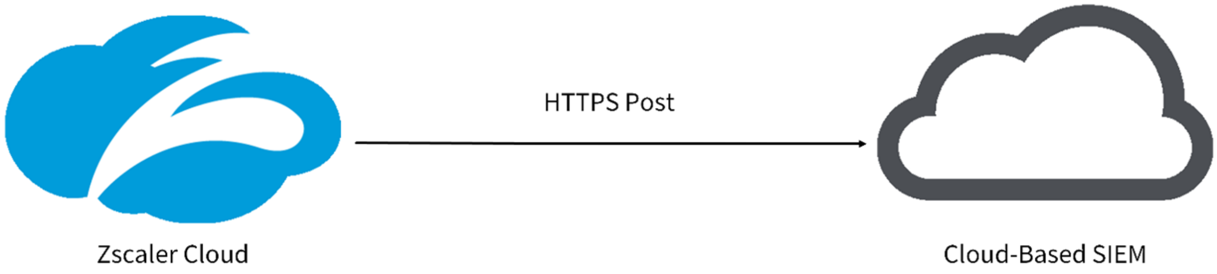


Figure 83. High-level overview of cloud-to-cloud logging

You can subscribe to Cloud NSS, which allows direct cloud-to-cloud log streaming for all types of ZIA logs into a CrowdStrike NG-SIEM.

For more information about cloud-to-cloud logging, see:

- About Nanolog Streaming Service (government agencies, see About Nanolog Streaming Service)
- About Cloud NSS Feeds (government agencies, see About Cloud NSS Feeds)
- Adding Cloud NSS Feeds for Web Logs (government agencies, see Adding Cloud NSS Feeds for Web Logs)

Configure CrowdStrike NG-SIEM to Ingest ZIA Logs using Cloud NSS

This section requires that you have admin access to the CrowdStrike NG-SIEM tenant.

You would then create new cloud NSS feeds in the ZIA Admin Portal for the sources you want to ingest into NG-SIEM. Configure these feeds with your NG-SIEM API URL and ingest token.

Log In to CrowdStrike NG-SIEM Tenant

Log in to CrowdStrike NG-SIEM tenant via the online portal.

1. Log in to your CrowdStrike tenant using admin credentials.

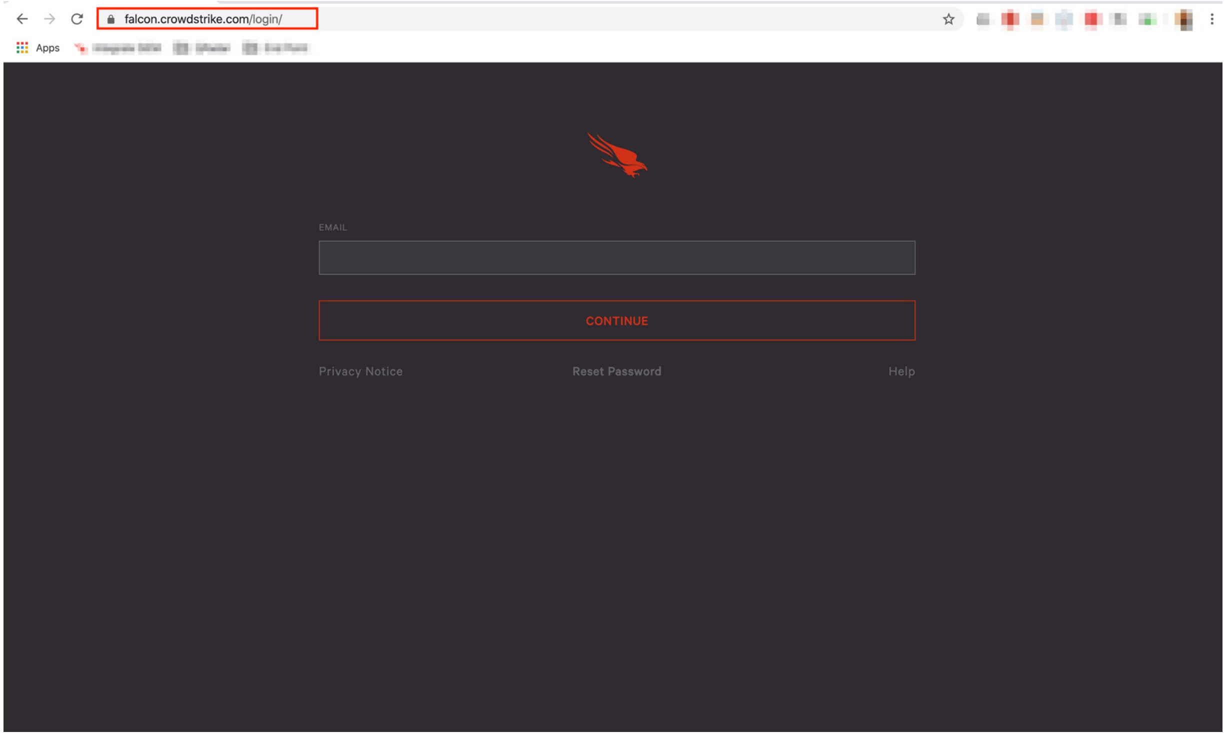


Figure 84. CrowdStrike Falcon Console login

2. Go to **Data onboarding** in the **Next-Gen SIEM** section.

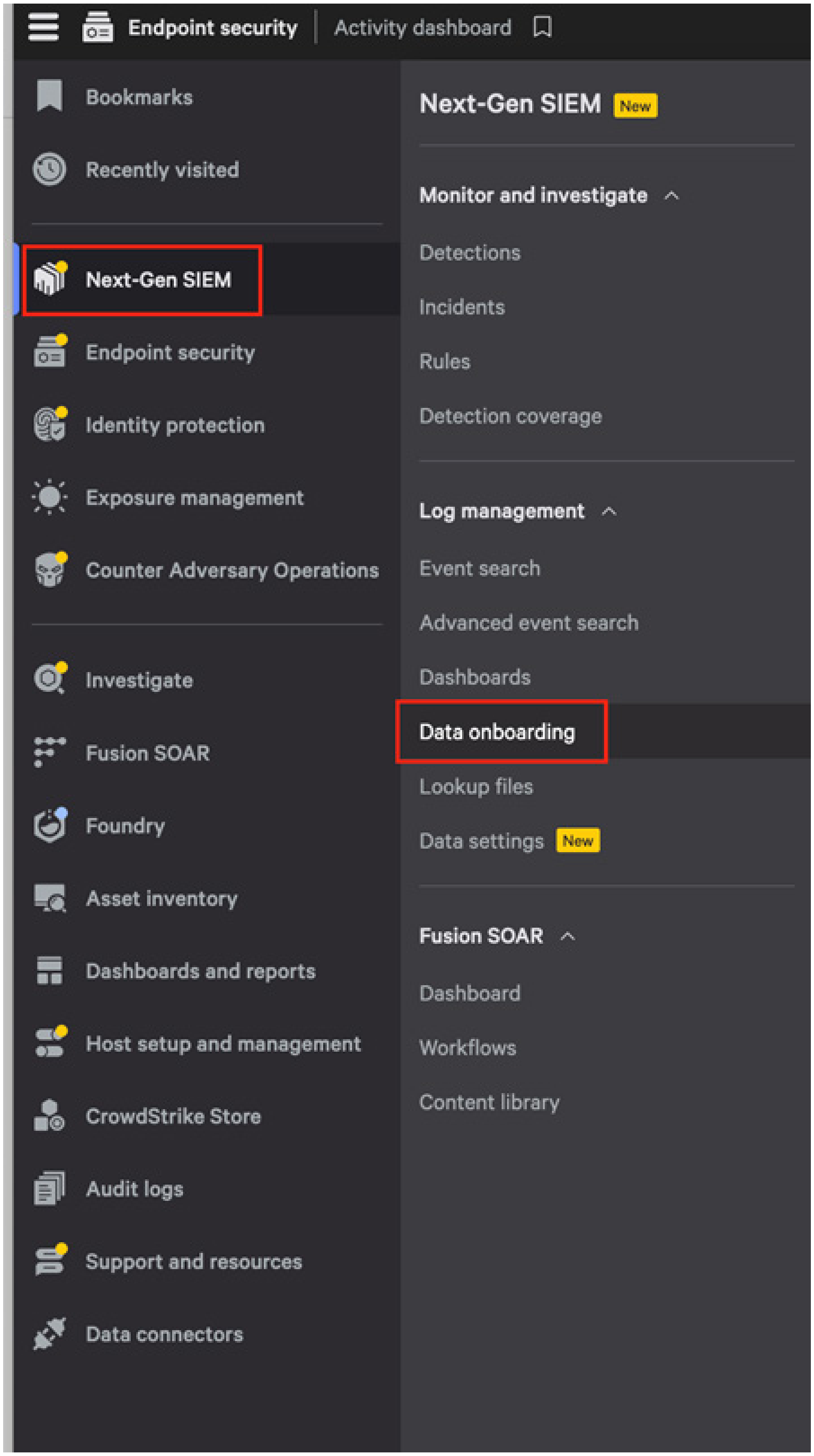
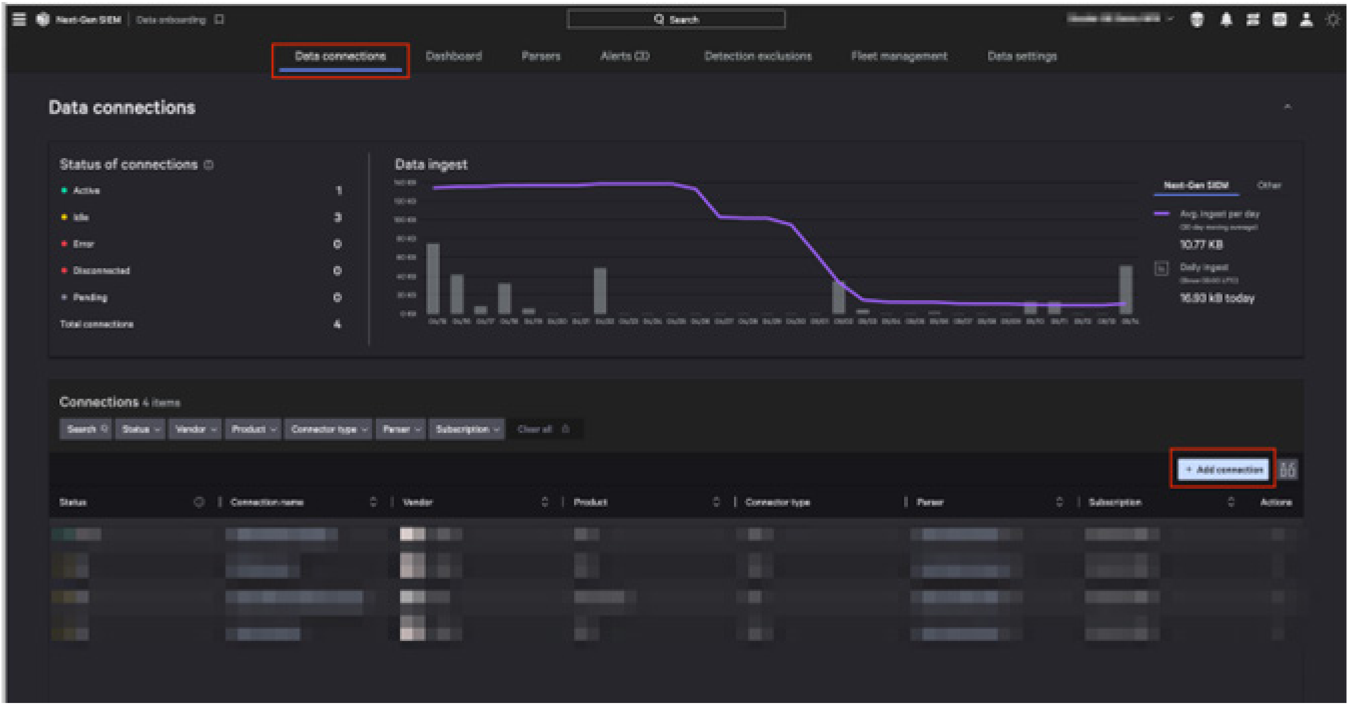


Figure 85. Select Data onboarding under Next-Gen SIEM

3. Click **Add Connection** under **Data Connections**.



Data connections

Status of connections

Active	1
Idle	3
Error	0
Disconnected	0
Pending	0
Total connections	4

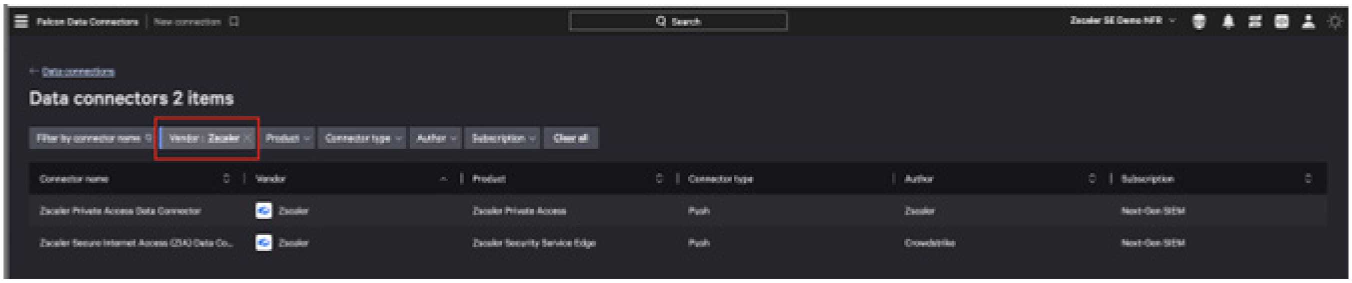
Connections 4 items

Search | Status | Vendor | Product | Connector type | Parser | Subscription | Clear all

Status	Connection name	Vendor	Product	Connector type	Parser	Subscription	Actions
[redacted]							

Figure 86. Click Add connection

4. Search for `Zscaler` under the vendor list.



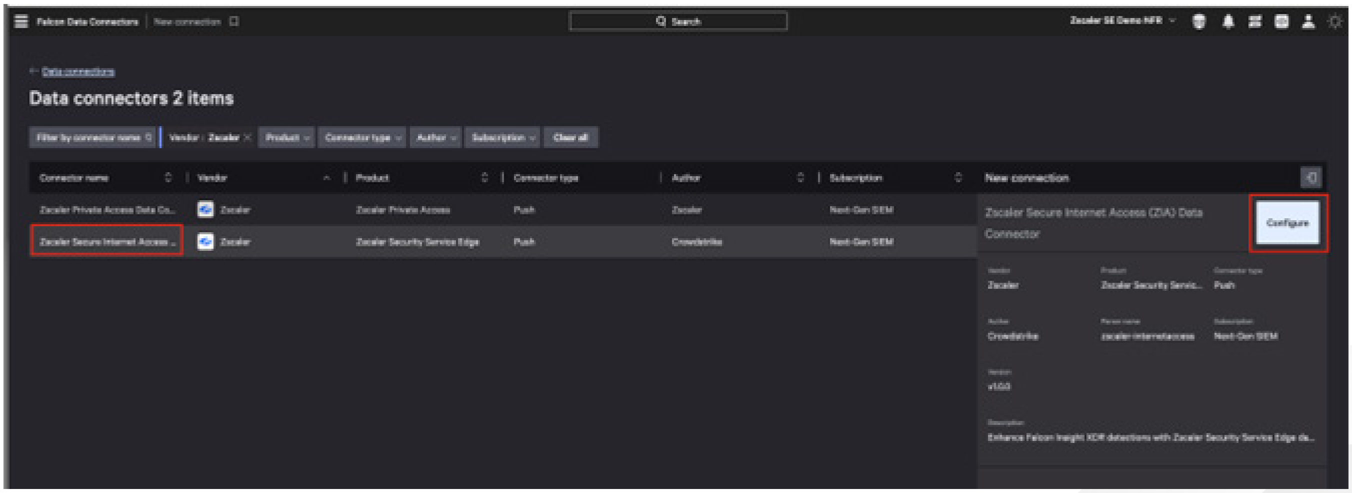
Data connectors 2 items

Filter by connector name | Vendor : Zscaler | Product | Connector type | Author | Subscription | Clear all

Connector name	Vendor	Product	Connector type	Author	Subscription
Zscaler Private Access Data Connector	Zscaler	Zscaler Private Access	Push	Zscaler	Next-Gen SIEM
Zscaler Secure Internet Access (ZIA) Data Co...	Zscaler	Zscaler Security Service Edge	Push	Crowdstrike	Next-Gen SIEM

Figure 87. Search for Zscaler under the Vendor list

5. Select **ZIA specific connector** and click **Configure**.



Data connectors 2 items

Filter by connector name | Vendor : Zscaler | Product | Connector type | Author | Subscription | Clear all

Connector name	Vendor	Product	Connector type	Author	Subscription
Zscaler Private Access Data Co...	Zscaler	Zscaler Private Access	Push	Zscaler	Next-Gen SIEM
Zscaler Secure Internet Access ...	Zscaler	Zscaler Security Service Edge	Push	Crowdstrike	Next-Gen SIEM

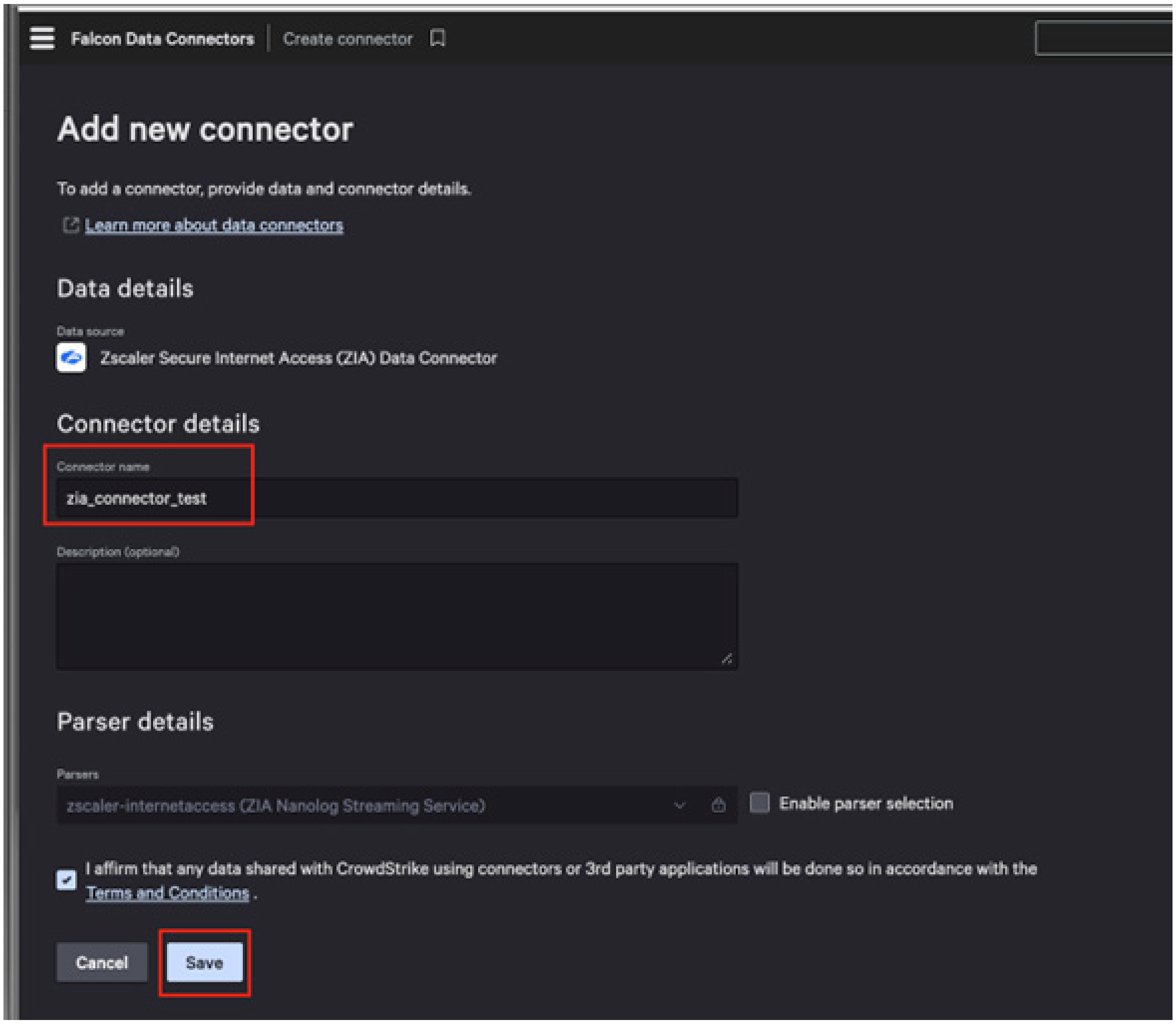
New connection

Zscaler Secure Internet Access (ZIA) Data Connector

Vendor: Zscaler
Product: Zscaler Security Servic...
Connector type: Push
Author: Crowdstrike
Parser name: zscaler-internetaccess
Subscription: Next-Gen SIEM
Version: v1.0.0
Description: Enhance Falcon Insight XDR detections with Zscaler Security Service Edge da...

Figure 88. Configure ZIA connector

6. Enter the **Connector name** and click **Save**.



Add new connector

To add a connector, provide data and connector details.

Learn more about data connectors

Data details

Data source

Zscaler Secure Internet Access (ZIA) Data Connector

Connector details

Connector name

zia_connector_test

Description (optional)

Parser details

Parsers

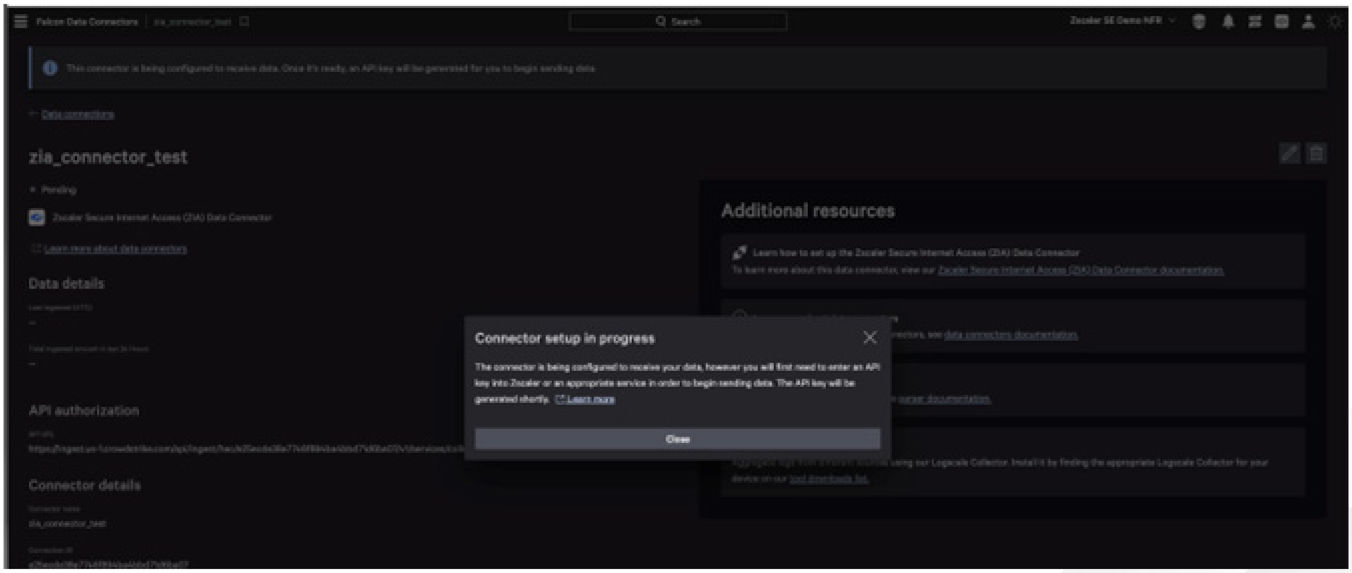
zscaler-internetaccess (ZIA Nanolog Streaming Service)

□ Enable parser selection

☑ I affirm that any data shared with CrowdStrike using connectors or 3rd party applications will be done so in accordance with the Terms and Conditions .

Figure 89. Create ZIA connector

7. Wait for the connector setup to finish.



This connector is being configured to receive data. Once it's ready, an API key will be generated for you to begin sending data.

zia_connector_test

Pending

Zscaler Secure Internet Access (ZIA) Data Connector

Learn more about data connectors

Data details

API authorization

Connector details

Connector name

zia_connector_test

Additional resources

Learn how to set up the Zscaler Secure Internet Access (ZIA) Data Connector

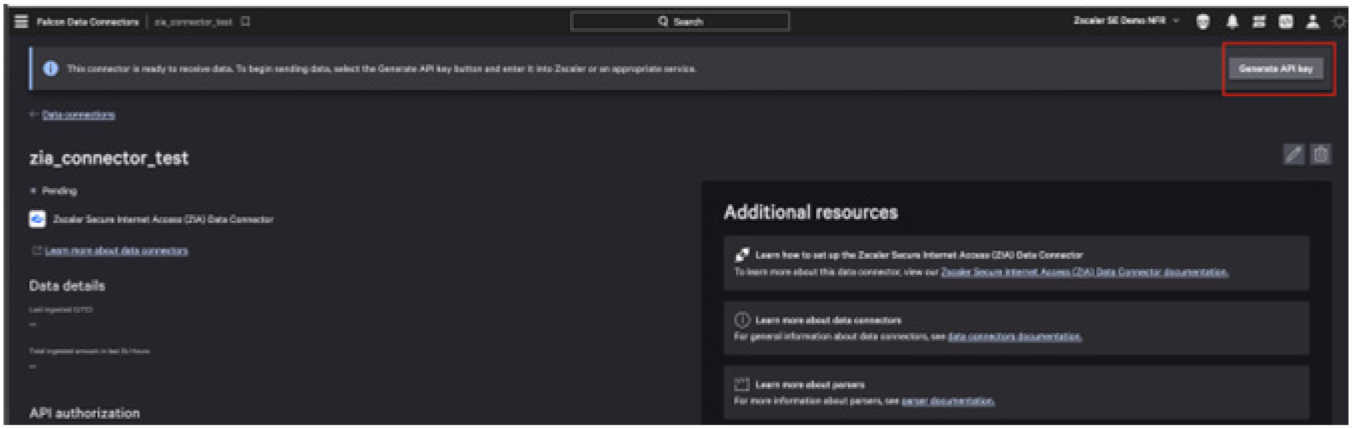
To learn more about this data connector, view our Zscaler Secure Internet Access (ZIA) Data Connector documentation.

Connector setup in progress

The connector is being configured to receive your data, however you will first need to enter an API key into Zscaler or an appropriate service in order to begin sending data. The API key will be generated shortly. Learn more

Figure 90. Connector setup in progress

8. After the connector setup finishes, click **Generate API key**.



This connector is ready to receive data. To begin sending data, select the Generate API key button and enter it into Zscaler or an appropriate service.

zia_connector_test

Pending

Zscaler Secure Internet Access (ZIA) Data Connector

Learn more about data connectors

Data details

Last ingested (UTC)
--

Total ingested amount in last 24 Hours
--

API authorization

Additional resources

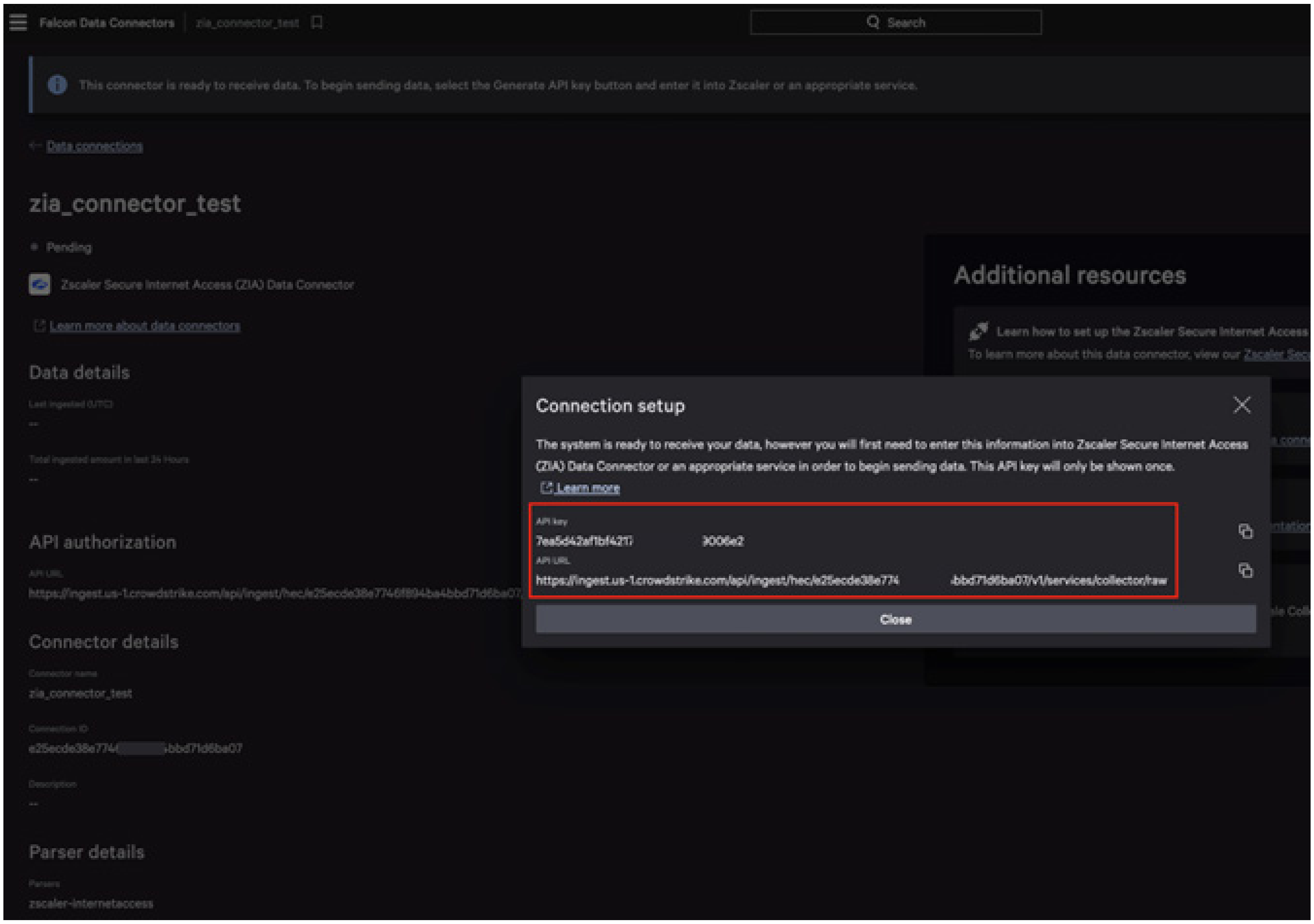
Learn how to set up the Zscaler Secure Internet Access (ZIA) Data Connector
To learn more about this data connector, view our Zscaler Secure Internet Access (ZIA) Data Connector documentation.

Learn more about data connectors
For general information about data connectors, see data connectors documentation.

Learn more about parsers
For more information about parsers, see parser documentation.

Figure 91. Generate API key

9. Copy and save the API key and the ingest API URL for later use.



This connector is ready to receive data. To begin sending data, select the Generate API key button and enter it into Zscaler or an appropriate service.

zia_connector_test

Pending

Zscaler Secure Internet Access (ZIA) Data Connector

Learn more about data connectors

Data details

Last ingested (UTC)
--

Total ingested amount in last 24 Hours
--

API authorization

API URL
https://ingest.us-1.crowdstrike.com/api/ingest/hec/e25ecde38e7746f894ba4bbd71d6ba07

Connector details

Connector name
zia_connector_test

Connection ID
e25ecde38e774[redacted]bbd71d6ba07

Description
--

Parser details

Parsers
zscaler-internetaccess

Additional resources

Learn how to set up the Zscaler Secure Internet Access
To learn more about this data connector, view our Zscaler Sec

Connection setup

The system is ready to receive your data, however you will first need to enter this information into Zscaler Secure Internet Access (ZIA) Data Connector or an appropriate service in order to begin sending data. This API key will only be shown once.

Learn more

API key
7ea5d42af1bf4217[redacted]9006e2

API URL
https://ingest.us-1.crowdstrike.com/api/ingest/hec/e25ecde38e774[redacted]bbd71d6ba07/v1/services/collector/raw

Figure 92. Copy API key and Ingest API URL for later use

Configure Zscaler 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 NG-SIEM. Rather than deploying, managing, and monitoring on-premises NSS VMs, you can configure a feed that pushes logs from the Zscaler cloud service into an HTTPS API endpoint on the SIEM. The following steps show how to set up the log feed for web logs. Repeat these steps to set up other Zscaler log types (e.g., Firewall, DNS, or Tunnel logs, etc.).

Go to Cloud-to-Cloud Logging Section in the ZIA Admin Portal

From the ZIA Admin Portal, go to **Administration** > **Nanolog Streaming Service** > **Cloud NSS Feeds** > **Add Cloud NSS Feed**.

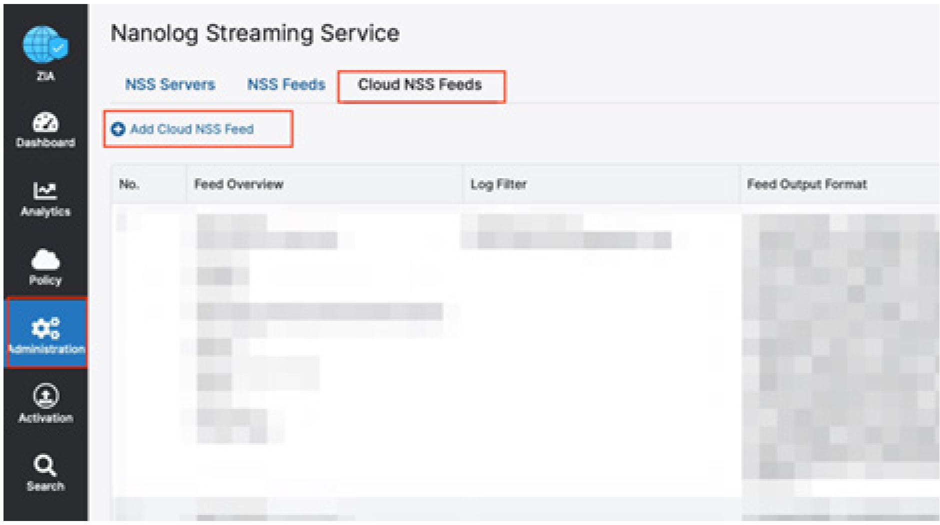
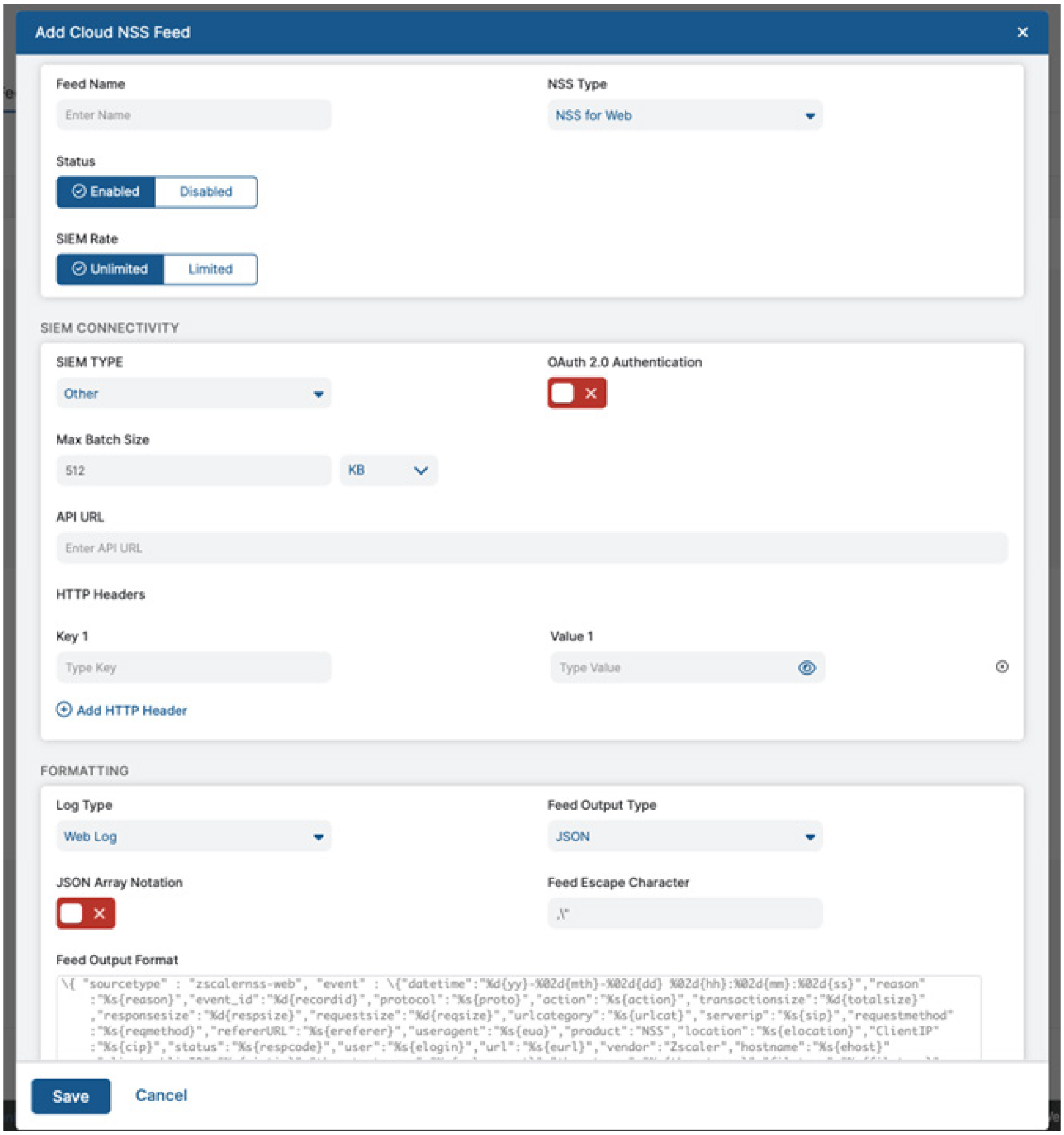


Figure 93. Go to cloud-to-cloud logging section in ZIA

Set Up the Cloud NSS Log Feed

To set up the Cloud NSS log feed:

1. Select **Other** as the **SIEM type** from the drop-down menu. The **API URL** and **Authorization Bearer** token are the ones that were created in NG-SIEM during previous steps.
2. In the **Add Cloud NSS Feed** dialog:
   a. **Key1**: Enter `Authorization`.
   b. **Value1**: Enter the NG-SIEM token in the format `Bearer xxx-xxx-xxx` (replace xxx with actual HEC token value).
3. Set **Feed Output Type** to **JSON** from the drop-down menu. Enter **“,** \ (double quote, comma, backslash) to the **Feed Escape Character** list. Turn off **JSON array notation**. Save your configuration after providing the required parameters.



Add Cloud NSS Feed

Feed Name: Enter Name

NSS Type: NSS for Web

Status: [✓ Enabled] Disabled

SIEM Rate: [✓ Unlimited] Limited

SIEM CONNECTIVITY

SIEM TYPE: Other

OAuth 2.0 Authentication: ☒

Max Batch Size: 512 KB

API URL: Enter API URL

HTTP Headers

Key 1: Type Key

Value 1: Type Value

Add HTTP Header

FORMATTING

Log Type: Web Log

Feed Output Type: JSON

JSON Array Notation: ☒

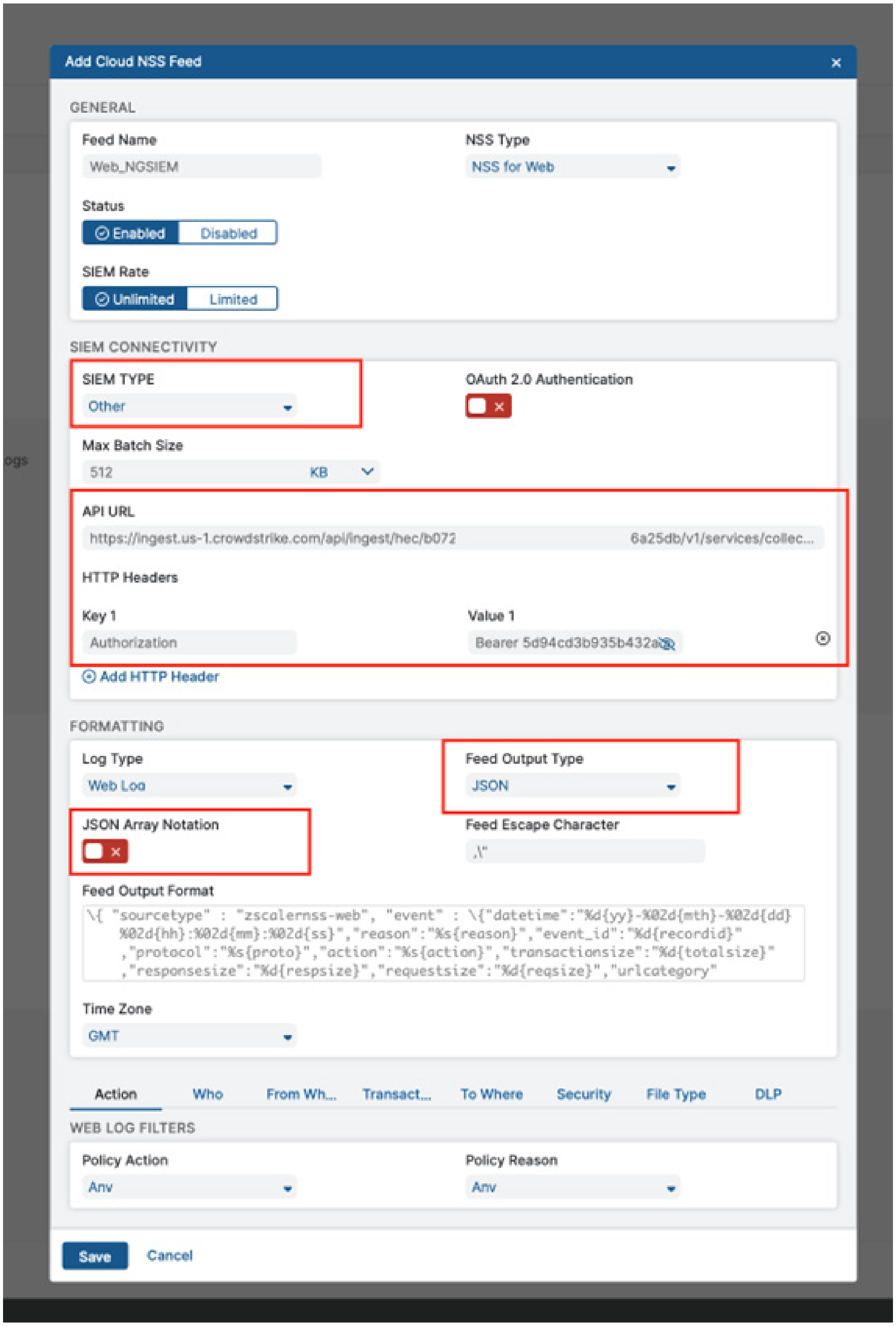
Feed Escape Character: ,\"

Feed Output Format:

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}","reason"
    :"%s{reason}","event_id":"%d{recordid}","protocol":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}"
    ,"responsesize":"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip":"%s{sip}","requestmethod"
    :"%s{reqmethod}","refererURL":"%s{ereferer}","useragent":"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP"
    :"%s{cip}","status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":"Zscaler","hostname":"%s{ehost}"
```

Figure 94. Configure cloud NSS feed

The following is an example with all the fields populated.



Add Cloud NSS Feed

GENERAL

Feed Name: Web_NGSIEM

NSS Type: NSS for Web

Status: [✓ Enabled] Disabled

SIEM Rate: [✓ Unlimited] Limited

SIEM CONNECTIVITY

SIEM TYPE: Other

OAuth 2.0 Authentication: ☒

Max Batch Size: 512 KB

API URL: https://ingest.us-1.crowdstrike.com/api/ingest/hec/b072 6a25db/v1/services/collec...

HTTP Headers

Key 1: Authorization

Value 1: Bearer 5d94cd3b935b432a

FORMATTING

Log Type: Web Log

Feed Output Type: JSON

JSON Array Notation: ☒

Feed Escape Character: ,\"

Feed Output Format:

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd}
    %02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}"
    ,"protocol":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}"
    ,"responsesize":"%d{respsize}","requestsize":"%d{reqsize}","urlcategory"
```

Time Zone: GMT

WEB LOG FILTERS

Policy Action: Any

Policy Reason: Any

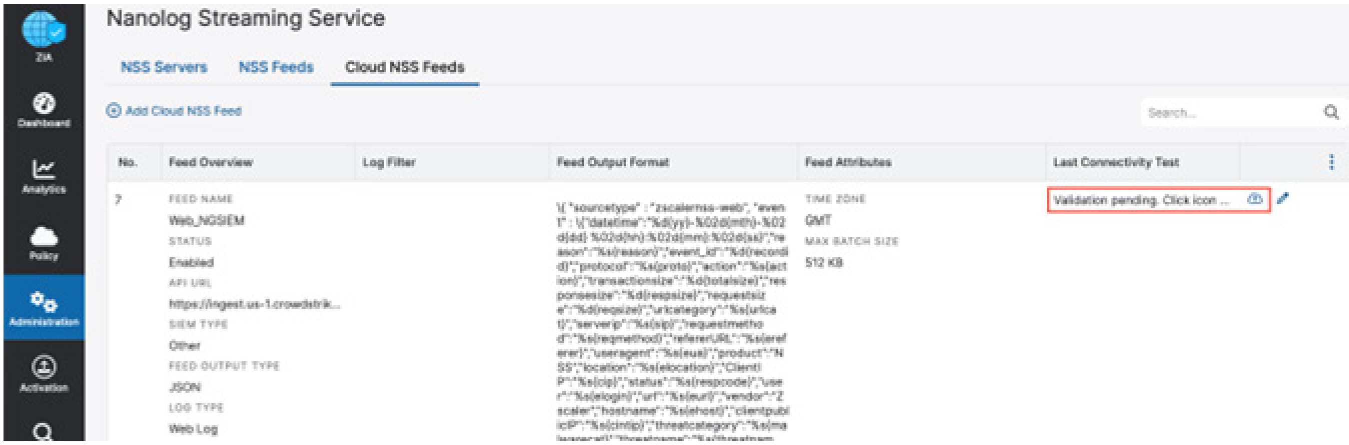
Figure 95. Example with all fields populated (web)

Add Other Log Sourcetypes

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

Validate NSS Cloud Configuration

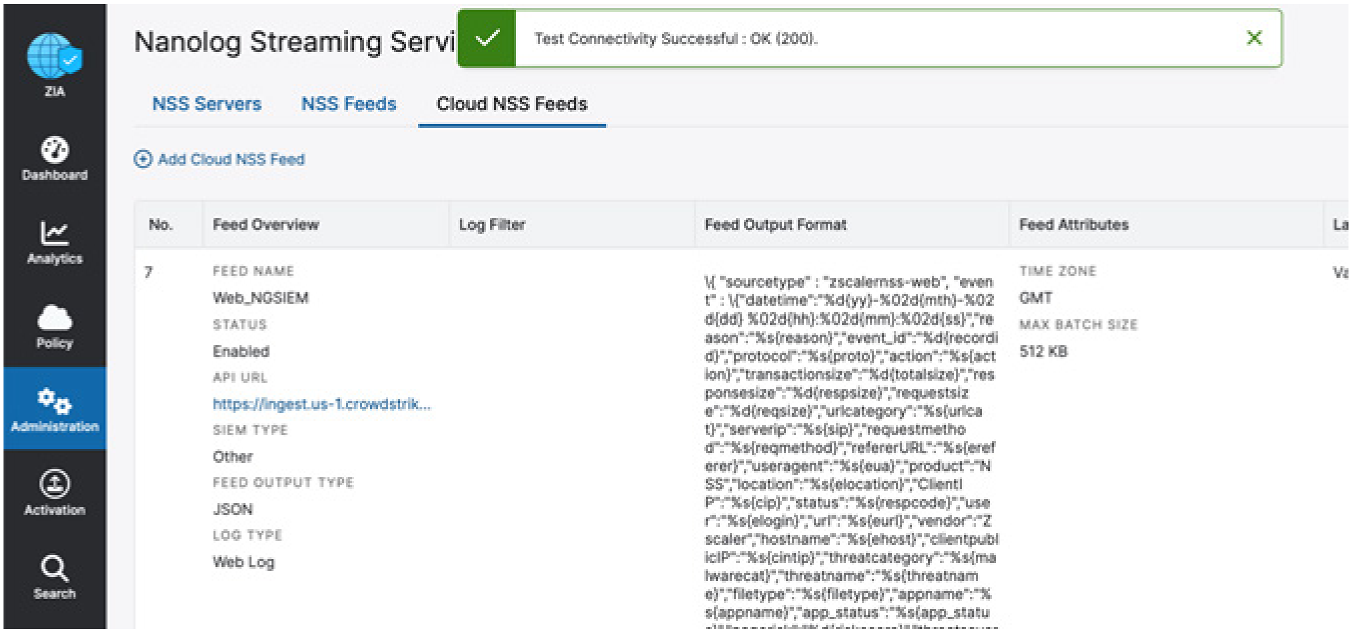
After you saved and activated the configuration, click the Test Connectivity icon shown in the following figure to verify connectivity from ZIA cloud to NG-SIEM. This sends a sample or test log message from the ZIA cloud to CrowdStrike. Cloud-to-cloud connectivity is verified if NG-SIEM sends back the expected 2XX HTTP response code.



No.	Feed Overview	Log Filter	Feed Output Format	Feed Attributes	Last Connectivity Test
7	FEED NAME Web_NGSIEM STATUS Enabled API URL https://ingest.us-1.crowdstrik... SIEM TYPE Other FEED OUTPUT TYPE JSON LOG TYPE Web Log		\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize":"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip":"%s{sip}","requestmethod":"%s{reqmethod}","refererURL":"%s{ereferer}","useragent":"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP":"%s{cip}","status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}","threatcategory":"%s{malwarecat}","threatname":"%s{threatnam	TIME ZONE GMT MAX BATCH SIZE 512 KB	Validation pending. Click icon ...

Figure 96. Verify connectivity to Humio cloud

When the connectivity is verified, the Last Connectivity Test column changes from Last Validation Pending to Last Validation Successful.



Test Connectivity Successful : OK (200).

No.	Feed Overview	Log Filter	Feed Output Format	Feed Attributes	La
7	FEED NAME Web_NGSIEM STATUS Enabled API URL https://ingest.us-1.crowdstrik... SIEM TYPE Other FEED OUTPUT TYPE JSON LOG TYPE Web Log		\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize":"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip":"%s{sip}","requestmethod":"%s{reqmethod}","refererURL":"%s{ereferer}","useragent":"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP":"%s{cip}","status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}","threatcategory":"%s{malwarecat}","threatname":"%s{threatname}","filetype":"%s{filetype}","appname":"%s{appname}","app_status":"%s{app_statu	TIME ZONE GMT MAX BATCH SIZE 512 KB	Va

Figure 97. NG-SIEM cloud connectivity verified

Verify Logs are Flowing into NG-SIEM

Navigate back to your NG-SIEM tenant and go to the Data Connections section. If the test connectivity passed in the earlier step, the connector status should now show as Active. If that is the case, under the Actions column on the right-hand side, select **Show Events**.

Incoming Zscaler log data is visible.

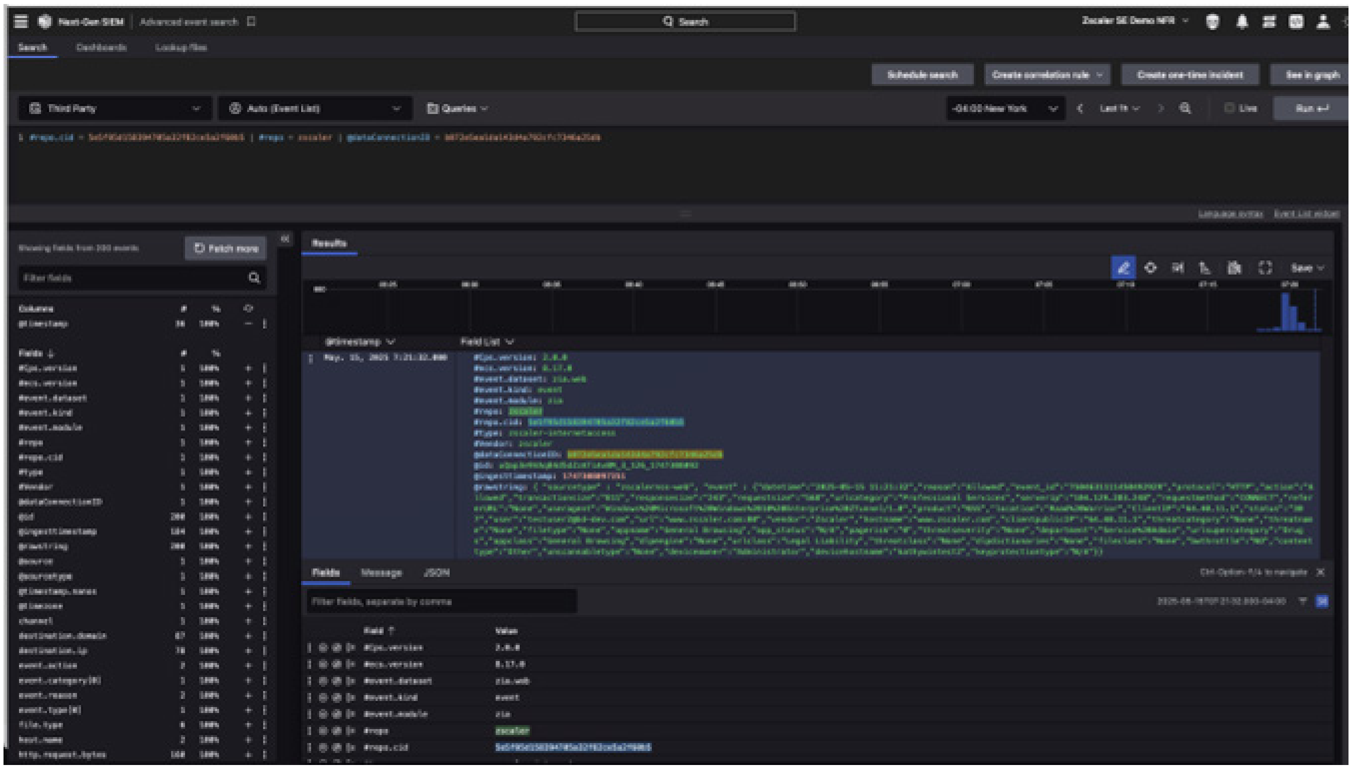


Figure 98. Check NG-SIEM for incoming Zscaler data

Use Case 8: Extended Detection and Response

Falcon's Extended Detection and Response (XDR) telemetry combined with Zscaler extends detection and response capabilities beyond the endpoint. The combination of Falcon and Zscaler automatically correlates suspicious activity across attack surfaces and leverages powerful analysis tools that help your team accelerate security operations, reduce risk, and improve threat visibility and detection across the enterprise.

Using Falcon XDR telemetry and Zscaler, you can:

- Ingest security data from supported third-party vendors.
- Search cross-domain security data in the Falcon Console.
- Create XDR scheduled searches and reports.
- Create custom XDR detections from queries.
- Triage and investigate XDR detections generated by the Falcon platform and supported third-party data sources from a unified interface.
- Perform targeted response actions from within an XDR detection or the graph view. Extend XDR response with supported third-party integrations.
- Configure response actions that execute automatically when a triggering condition occurs with Falcon Fusion workflows.

Requirements

Make sure the following prerequisites are met:

Subscriptions to Falcon Insight XDR with one or more XDR connector packs. To leverage XDR capabilities, you must have at least one additional supported Falcon subscription and the associated Falcon platform XDR connector pack, or a third-party XDR connector pack. Supported Falcon subscriptions:

- Falcon Identity Protection. To enable identity response actions, you must have Falcon Identity Protection and the associated Falcon platform XDR connector pack.
- Falcon Cloud Workload Protection (CWP).
- Falcon for Mobile.

Configure the following roles:

- Falcon Administrator
- XDR Administrator
- XDR Security Lead
- XDR Analyst
- XDR Analyst (Read Only)

Configure the following clouds:

- US-1
- US-2
- EU-1

Other requirements: For Zscaler response actions, do the following:

- Install ZIA.
- Enable SCIM API integration for ZIA. To learn more, see the Configuring SCIM (government agencies, see Configuring SCIM).
- Ensure user's machines are (Active Directory) domain-joined.

Understanding XDR

Using XDR, you can ingest third-party telemetry to unify detection and response across your security stack. You can hunt, detect, and investigate adversary activity across attack surfaces from a unified interface in the Falcon Console:

- XDR detection monitoring: Falcon monitors activity across your specified domains and data sources. Falcon correlates and analyzes data in real time upon ingestion, and automatically generates XDR detections when suspicious activity is detected.
- XDR event search: From the Falcon Console, search against cross-domain data to hunt for suspicious activity or further investigate detections.
- XDR scheduled searches: Create XDR event searches that run automatically and recur on a schedule that you set. You can download and share the search results, and your specified recipients can receive notifications each time a scheduled search completes. Configure notifications to be sent when a search produces results, when a search produces no results, or both.
- Custom XDR detections from queries: For scheduled searches that indicate suspicious activity, you can optionally generate an XDR detection each time the search returns results. These custom XDR detections support MITRE ATT&CK framework mappings, severity, and descriptions. They appear in a consolidated view alongside CrowdStrike-generated XDR detections to facilitate monitoring and triage.
- Response actions: Perform targeted response actions, either manually from within an XDR detection or automatically through a Falcon Fusion workflow. Optionally, extend XDR response capabilities with supported third-party integrations.

Data Sources

You can extend Falcon platform telemetry by ingesting security telemetry from supported third-party vendors (such as Zscaler). Upon ingestion, data is parsed and mapped into the CrowdStrike XDR data schema, which provides a common language for correlation and analysis of data from different sources.

Supported third-party vendor data sources:

- CrowdStrike supports third-party data from CrowdXDR Alliance partners. To learn more, refer to CrowdStrike documentation. Work with your CrowdStrike onboarding team for more information about vendor-specific support.
- CrowdStrike anticipates adding more third-party data sources over time. Request support for additional data sources through CrowdStrike Ideas (CrowdStrike support portal).

XDR Data Ingestion

The data ingestion setup process varies depending on the specific vendors you work with, and your unique environment and configuration. During XDR onboarding, your onboarding team provides vendor-specific instructions for each of the partners you work with.

How Data is Processed and Stored

Upon ingestion, data is automatically parsed and mapped into the CrowdStrike XDR data schema, which provides a common language for correlation and analysis of data from different sources. The XDR data schema includes XDR events and XDR indicators. Vendor-specific telemetry is also preserved and stored because it can contain relevant information for investigation and response.

XDR Telemetry

The following table defines the XDR telemetry values.

Item	Description
XDR detection	A confirmation that activity is malicious or otherwise warrants further investigation. You can compose an XDR detection of one indicator or multiple correlated indicators.
XDR indicator	A signal of activity that's interesting from a security perspective. XDR indicators are composed of one or more events and associated telemetry that represent unusual activity or behavior known to be used by threat actors. Examples: • Ten failed logins in a row. • Metasploit traffic. • Suspicious web proxy activity. • Suspicious email attachment executed. An indicator on its own isn't necessarily confirmation of suspicious activity and might not warrant further investigation. XDR indicators are the building blocks that form XDR detections.
XDR event	A signal that an activity occurred. Examples: • An email was received. • A login attempt failed. • A file was written. View events in XDR search, or in the context of indicators or correlated detections.

Setup

To set up XDR, work with your CrowdStrike onboarding team to configure ingestion of third-party data. Your onboarding team provides vendor-specific instructions during the onboarding process.

Create XDR scheduled searches and detections as needed. To learn more, refer to the CrowdStrike documentation.

Configure automated response actions, including third-party responses, and Falcon Fusion workflows as needed. To learn more, refer to the CrowdStrike documentation.

XDR Detection Monitoring

Falcon monitors activity across your specified Falcon platform and third-party domains and data sources. It surfaces suspicious collections of signals and indicators in the form of correlated XDR detections. XDR detections include output that's generated automatically by CrowdStrike and output that's generated by any custom XDR detections that you created from scheduled searches.

XDR detections appear in an XDR-specific interface in the Falcon Console, where you can triage, investigate, and respond to cross-domain alerts.

- Triage: Filter XDR detections by data domain, data source, status, severity, and more. Assign detections, update detection status, and comment on XDR detections.
- Investigate: Review detection details in the detection summary, including information about the indicators that triggered the detection. Pivot to the XDR graph explorer to visualize the detection and explore connections between events. Pivot from the summary into XDR event search to view event data associated with the alert.
- Respond: In the XDR detection summary, add users to the Falcon Identity Protection watchlist or perform a supported third-party response action.

View XDR detections at **Endpoint security** > **Monitor** > **XDR detections** in the Falcon Console.

XDR Event Investigation

With XDR event search in the Falcon Console, search against cross-domain data to hunt for suspicious activity or further investigate detections. XDR event searches are written in the LogScale Query Language. To learn more, refer to the CrowdStrike documentation.

Search XDR events at **Endpoint security** > **XDR search** > **Search** in the Falcon Console.

XDR Scheduled Searches and Custom XDR Detections

Create XDR event and indicator searches that run automatically and recur on a schedule that you set. You can download and share the search results, and your specified recipients can receive notifications each time a scheduled search is completed. Configure notifications to be sent when a search produces results, when a search produces no results, or both.

For recurring searches that indicate suspicious activity, you can opt to generate an XDR detection each time that the search returns results. These custom XDR detections appear alongside CrowdStrike-generated XDR detections to facilitate monitoring and triage.

The XDR scheduled search activity log shows the history of your completed scheduled searches, including any searches that generated errors. The XDR scheduled search audit log shows the history of changes to your configured XDR scheduled searches and custom XDR detection queries.

EDR scheduled searches are managed separately from XDR scheduled searches. To learn more, refer to the CrowdStrike documentation.

Frequency and Timing

After you save an XDR scheduled search, the first instance of that search runs at your specified start time and generates results for the specified time interval. For example, if you configured the search to run every two hours, the first run of that search generates results for the previous two hours.

If more than 5 searches are scheduled to run at the same time, they're placed in a queue and then run as resources become available. If a given search isn't complete by the time the next search is scheduled to start, the next instance of the search fails.

If a running search hasn't completed after 60 minutes, it times out. If a specific scheduled search is timing out frequently, consider editing the scheduled search to refine its query syntax. To learn more, refer to the CrowdStrike documentation.

You can retry a failed search manually. To learn more, refer to CrowdStrike documentation.

When you create a scheduled search without detections, you can configure an optional offset window. Specifying an offset window skips a period immediately before the search and looks at older, more complete data. Configure an offset time that's at least as long as the time between scheduled log uploads.

When you create a custom XDR detection query, you specify a search frequency and a search window. The search frequency determines how often Falcon runs the search for the detection. The search window determines the period of time that's searched. The first time a detection is generated for a given query, a time window is established between the first and last events. When the query runs again, a new detection is generated only if a new event is included in the result and is outside the time window from the previous result.

To ensure that all relevant XDR data is searched for detections, configure a search window that's at least as long as the search frequency. Overlapping searches help to ensure that all XDR data is included, regardless of when logs are uploaded. However, with overlapping searches, a given XDR event or indicator might appear in more than one custom detection.

Limitations

Falcon stores a maximum of 10,000 XDR events per scheduled search. Each generated search result set is retained and available for download for 30 days, after which it's permanently deleted.

Your customer ID (CID) can have a maximum of 200 active XDR searches, and an unlimited number of inactive searches. If your CID already has 200 active searches, any new searches created are inactive by default. For information about activating and deactivating scheduled searches, refer to the CrowdStrike documentation.

Deactivating a search stops the search from running any new queries, but the configured scheduled search remains available for use for 30 days. After 30 days, the deactivated scheduled search is deleted permanently.

If the user associated with a scheduled search is removed or has their permissions revoked, the search is deactivated. Additionally, a notification explaining the deactivation is sent to all notification recipients for that scheduled search. If a different user reactivates the search, that user becomes the new owner of the search.

XDR detections appear in the Falcon Console for 90 days after they're generated.

Notifications

You can set up automatic delivery of notifications to alert members of your team each time an XDR scheduled search has run, or whenever an XDR detection results in an error.

A notification contains a summary and, if applicable, a link to download the search results through the Falcon Console. For XDR scheduled searches, you can specify when to send notifications in any combination:

- When matching search results are returned.
- When no matching search results are returned.
- When errors or warnings are generated during a search.

For custom XDR detections, you can configure notifications to be sent if errors or warnings are generated.

Recipients cannot unsubscribe from scheduled search notifications. Only the scheduled search creator, an XDR Administrator, or a Falcon Administrator can remove recipients from the scheduled search notification settings.

Notification Delivery Options

Send scheduled search notifications to individual users by email or to groups of users through Slack, PagerDuty, Microsoft Teams, or webhook integrations. For each scheduled search, you can configure one or more delivery methods.

Before you can configure notifications through Slack, PagerDuty, Microsoft Teams, or webhook integration, you must set up the relevant app integrations through the CrowdStrike Store.

Email

Send scheduled search notifications to a specified list of email addresses in your approved domains. You can designate up to 10 email notification recipients per scheduled search, including people who are not Falcon users.

You can configure email notifications to include the full search result set as a JSON file attachment. Note that attaching results sends data out of Falcon to systems that might have different security standards or terms and conditions.

Slack

Send notifications to one or more channels in your integrated Slack account. A Slack integration through the CrowdStrike Store is required. To learn more, refer to CrowdStrike documentation.

PagerDuty

Configure notifications to automatically open an incident in PagerDuty and alert relevant user groups. Select the PagerDuty source and severity from your connected service to configure notification delivery. A PagerDuty integration through the CrowdStrike Store is required. To learn more, refer to CrowdStrike documentation.

Microsoft Teams

Send notifications to one or more channels in your integrated Microsoft Teams account. A Microsoft Teams integration through the CrowdStrike Store is required. To learn more, refer to CrowdStrike documentation.

Webhook

Distribute notifications to other applications through a webhook. A webhook integration through the CrowdStrike Store is required. To learn more, refer to CrowdStrike documentation.

XDR Response Actions

Perform targeted Falcon platform response actions from within XDR detection details or the graph view. Optionally, extend XDR response with supported third-party integrations. You can also automate response actions through Falcon Fusion workflows.

Response actions can take up to 10 minutes to complete.

Falcon Identity Protection Response

Perform targeted response actions by adding users to the Falcon Identity Protection watchlist from within an XDR detection or the graph view. You can configure the watchlist to enforce additional security controls such as requiring multifactor authentication.

To learn more, refer to the CrowdStrike documentation.

Third-Party Response

Extend XDR response with integrations from supported third-party vendors such as Zscaler.

ZIA Response

Integrate ZIA with Falcon so that you can perform your configured ZIA response actions from within an XDR detection or the graph view. Examples of ZIA response actions that you can configure:

- Add a user to custom-defined restricted user group.
- Remove a user from custom-defined restricted user group.

This option is available only after you add the user to the group.

You can also extend your ZIA response capabilities by creating a Falcon Fusion workflow. For example, automatically add a user to a custom-defined restricted user group when a triggering condition occurs.

To learn more, refer to the CrowdStrike documentation.

Falcon Fusion Workflows from XDR Detections

Create a Falcon Fusion workflow that initiates a specified action when Falcon generates an XDR detection:

- Send notifications by email, Slack, or webhook.
- Generate a ServiceNow or PagerDuty incident ticket.
- Change status, specify an assignee, or add a comment to the detection.

Create a Falcon Fusion workflow based on an XDR detection by selecting a Trigger category of Alert and a Subcategory of XDR detection. To learn more, refer to the CrowdStrike documentation.

XDR Scheduled Search and Custom XDR Detection Management

Your CID can have a maximum of 200 active XDR searches, including searches that generate custom XDR detections, and an unlimited number of inactive searches. If your CID already has 200 active XDR searches, any new searches created are inactive by default. To learn more, refer to the CrowdStrike documentation.

Get to XDR Scheduled Searches and Custom XDR Detections

The XDR Scheduled search and detections page is where you can view, create, edit, and delete your XDR scheduled searches and custom XDR detection queries. From this page, you can also view XDR search activity, download XDR search results, and view audit logs.

Go to **Endpoint security** > **XDR search** > **Scheduled search and detections** in the Falcon Console.

Create an XDR Scheduled Search Without Detections

To create an XDR scheduled search:

1. On the **XDR Scheduled search and detections** page, write and run the search query that you want to schedule. To learn more, refer to the CrowdStrike documentation.
2. Click **Schedule search**. The search details are prepopulated with the query information that you provided.
3. Enter a name for the scheduled search.
4. (Optional) Add a descriptive comment about the scheduled search.
5. In the **XDR query** field, confirm or modify the search query.
6. (Optional) Test the query in **XDR Search**, and then modify the query details as needed.
7. Click **Scheduled search report**, and then click **Next**.
8. Configure the schedule:
    a. **Start date** and **Start time**: Specify when the search begins running.
    b. **End date** and **End time**: (Optional) If you want the scheduled search to run for a finite period of time, specify when to stop running the search. If no end date is specified, the scheduled search runs indefinitely according to the configured frequency.
    c. **Search frequency**: Specify how often to run the search.
    d. **Search offset**: (Recommended) Configure an offset time that's at least as long as the time between scheduled log uploads. Specifying an offset window skips a period immediately before the search and looks at older, more complete data. To learn more, refer to the CrowdStrike documentation.
9. Click **Next**, and then configure notification settings as needed. To learn more, refer to the CrowdStrike documentation.
10. Click **Schedule search**.

Create a Custom XDR Detection from Scheduled Search Results

Configure Falcon to generate an XDR detection each time a given scheduled search returns results.

On the XDR Scheduled search and detections page, write and run the search query that you want to base the detection on. To learn more, refer to the CrowdStrike documentation.

1. Click **Schedule with detections**. The detection details are prepopulated with the query information that you provided.
2. Enter a name for the detection.
3. (Optional) Add a descriptive comment about the detection.
4. In the **XDR query** field, confirm or modify the search query.
5. (Optional) Test the query in **XDR Search**, and then modify the query details as needed.
6. Click **XDR detection**.
7. Select a severity for the detection.
8. (Optional) Assign a MITRE ATT&CK tactic and technique to the detection.
9. Click **Next**, and then configure a schedule for the detection:
    a. **Start date** and **Start time**: Specify when the search for this detection begins running. The start time must be at least 15 minutes from the current time.
    b. **End date** and **End time**: (Optional) If you want the search for this detection to run for a finite period of time, specify the last day on which to run the search. If no end date is specified, the scheduled search runs indefinitely according to the configured frequency.
    c. **Search frequency**: Specify how often to run the search for this detection.
    d. **Search window**: Specify the period of time that is searched. To help ensure that all relevant XDR data is searched for detections, configure a **Search window** value that's at least as long as the **Search frequency** value. To learn more, refer to the CrowdStrike documentation.
10. Click **Next**, and then configure notification settings as needed. To learn more, refer to the CrowdStrike documentation.
11. Click **Schedule**.

Edit an XDR Scheduled Search or Custom XDR Detection

To edit an exiting XDR scheduled search or custom XDR detection:

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**.
2. For the XDR scheduled search or custom XDR detection query that you want to edit, click **Edit** from the **Action** icon.
3. Modify the settings as needed. To learn more, refer to the CrowdStrike documentation to Create an XDR scheduled search without detection or Create a custom XDR detection from scheduled search results.
4. (Optional) Test the query in **XDR Search**, and then modify the query details as needed.
5. Click **Update search**.

Deactivate an XDR Scheduled Search

To stop running a scheduled search, deactivate it. If a scheduled search is deactivated, its **Status value** changes to Inactive and all further scheduled searches stop. You can resume the scheduled search by reactivating it.

Deactivating a search stops the search from running any new queries, but the configured scheduled search remains available for use for 30 days. After 30 days, the deactivated scheduled search is deleted permanently. However, any previously generated detections continue to appear in the list of detections.

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**.
2. For the scheduled search that you want to activate or deactivate, click **Activate** or **Deactivate** from the **Action** icon.

Delete an XDR Scheduled Search or Custom XDR Detection

Permanently delete a scheduled search that you no longer need. Previously generated search results remain available to download for 30 days. Delete scheduled searches with caution. Deleting a scheduled search removes all references to the search.

As an alternative to permanent deletion, you can deactivate a scheduled search. Deactivating a search stops the search from running any new queries, but the configured scheduled search remains available for use for 30 days. After 30 days, the deactivated scheduled search is deleted permanently. To learn more, refer to the CrowdStrike documentation.

If you delete a custom XDR detection query, any previously generated detections continue to appear in the list of detections.

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**.
2. For the XDR scheduled search or custom XDR detection query that you want to delete, click **Delete** from the **Action** icon.

View XDR Scheduled Searches and Custom XDR Detections

View your configured XDR scheduled searches and custom XDR detection queries, and any XDR searches that are currently running or queued. Refine the results through sorting, filtering, or specifying which columns are visible.

If the user associated with a scheduled search has been removed or has had their permissions revoked, the search is deactivated and the User field shows a value of None. To learn more, refer to the CrowdStrike documentation for Limitations or Activate or deactivate an XDR scheduled search.

For information about viewing search activity and search results, refer to the CrowdStrike documentation.

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**. A full list of your configured XDR scheduled searches and custom XDR detection queries appears.
2. Refine the list of results as needed:
   - Apply filters:
     - Click a filter at the top of the list.
     - Select or clear the filter-specific metadata options, and then click **Apply**.
   - Specify which columns are visible:
     - Click the **Configure table columns** icon.
     - Select the checkboxes for the columns that you want to see.
3. Click any scheduled search to see additional details.

View the XDR Scheduled Search and Custom Detection Audit Log

View the history of changes to your configured scheduled searches and custom XDR detection queries.

If a scheduled search has been deleted, the Name field shows a numerical unique identifier for the scheduled search instead of its configured name. To avoid this, you can deactivate a scheduled search instead of deleting it. To learn more, refer the CrowdStrike documentation to Activate or deactivate an XDR scheduled search and Delete an XDR scheduled search or custom XDR detection.

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**, and then click **Audit log**.
2. Adjust your view by filtering or sorting the log entries.
3. Click any audit log to see additional details.

View XDR Search Activity

View the activity history for your completed XDR scheduled searches, including searches that generated errors. View all of your generated scheduled search results, or refine the results through sorting and filtering. To learn more, refer to the CrowdStrike documentation.

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**, and then click **Search log**.
2. Adjust your view by filtering or sorting the log entries.
3. Click any activity event to see more details.

Download XDR Search Results

View generated XDR search results by downloading them as a JSON file.

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**, and then click **Search log**.
2. Adjust your view by filtering or sorting the log entries.
3. Click any entry to see more details.
4. Click **Download results**.

Retry an XDR Search

Retry a failed search manually. To learn more, refer to the CrowdStrike documentation.

1. Go to **Endpoint security** > **XDR search** > **Scheduled search and detections**, and then click **Search log**.
2. For the search that you want to retry, click **Retry**.

The **Retry** option appears only if a search has failed.

XDR Notification Configuration Fields

During configuration, set up notifications if you want to alert others each time that a scheduled search has run or a custom XDR detection query resulted in an error. To learn more, refer to the CrowdStrike documentation.

To learn more, refer to the following CrowdStrike documentation:

- Create an XDR scheduled search without detections
- Create a custom XDR detection from scheduled search results
- Edit an XDR scheduled search or custom detection.

Notification Methods

For each XDR scheduled search, configure one or more notification methods, or disable notifications. To set up multiple delivery methods, click **Add another notification after adding a notification method**.

Notification Method	Description and Options
Send email	Send an email notification to the specified recipients each time the scheduled search has run. In the **Recipients** field, type an email address and then press `Enter`. You can enter up to 10 email addresses. To attach the full search result set as a JSON file, select the **Send results as an attachment** checkbox. Note that attaching results sends data out of Falcon to systems that might have different security standards or terms and conditions.
Send Slack message	Send a notification to the specified Slack channel each time the scheduled search has run. From the **Name** list, select the applicable channel.
Create a PagerDuty incident	Create a PagerDuty incident each time the scheduled search has run. From the **Name** list, select the applicable configuration.
Send Microsoft Teams message	Send a notification to the specified Microsoft Teams channel each time the scheduled search has run. From the **Name** list, select the applicable channel.
Send webhook notification	Send a webhook notification each time the scheduled search has run. From the **Name** list, select the applicable webhook.
None	Don't send notifications to any recipients for this scheduled search.

When to Send Notifications

When configuring a scheduled search, for each notification method, indicate when to send notifications. Select any combination of these options.

Field	Description
No results are found	Sends a notification each time the scheduled search runs and generates no matching results.
Results are found	Sends a notification each time the scheduled search runs and generates matching results.
Errors or warnings occur	Sends a notification each time the scheduled search runs, or attempted to run, and resulted in errors or warnings.

ZIA Response Management

Configuring ZIA response actions is a multi-step process. The exact steps are determined by your ZIA response goals.

Many of these steps are performed in third-party products. The CrowdStrike Falcon platform integrates the relevant settings as you configure them. However, Falcon does not validate any third-party configurations. Perform the following steps with care, and validate your configurations before finalizing ZIA response actions in Falcon.

In this summary of the configuration process, the example goal is to enable the ability to add users to a customer-defined restricted user group:

- In your identity provider (IdP), create a user group for restricted users. See Step 1: Create a User Group for ZIA Response.
- Push the user group from your IdP to ZIA. See Step 2: Push the User Group to ZIA.
- In ZIA, create a response policy that restricts user access, and associate the policy with the user group. See Step 3: Create a ZIA Policy.
- In ZIA, enable SCIM support for your IdP. See Step 4: Enable SCIM Support.
- In the CrowdStrike Store, configure ZIA response actions for XDR. See Step 5: Configure ZIA Response Actions for XDR. After you complete this step, ZIA integration is configured, and you can perform manual response actions from within an XDR detection or the graph view.
- (Optional) Create a Falcon Fusion workflow that automatically initiates a specified ZIA action when a triggering condition occurs. To learn more, see Step 6: Create a Falcon Fusion Workflow for ZIA Response.

Step 1: Create a User Group for ZIA Response

In your IdP, create a user group for ZIA response purposes. You can add users to this group from a relevant XDR detection.

CrowdStrike recommends you use this group for ZIA response purposes only. After you create this user group, do not modify or use it for any other purpose.

These steps are performed in your IdP's administration interface. For more detailed information, refer to the applicable product documentation for your IdP.

In your IdP, create a user group. Make a note of the group name because you'll need it during subsequent steps.

Step 2: Push the User Group to ZIA

Sync the group to ZIA.

These steps are performed in your IdP's administration interface. For more detailed information, refer to the applicable product documentation for your IdP.

In your IdP, push the user group to ZIA.

Step 3: Create a ZIA Policy

Create a ZIA policy for the user group that you created. The type of policy that you create depends on your ZIA response goals. For example, the policy could restrict user access or define quarantine thresholds.

These steps are performed in the ZIA Admin Portal. For more information, see the applicable ZIA product documentation (government agencies, see ZIA product documentation).

1. Create a policy that supports your ZIA response goals.
2. Associate the new policy with the new user group that you created in an earlier step.

Step 4: Enable SCIM Support

In ZIA, enable SCIM support for your IdP. The SCIM protocol offers a generic interface for IdPs.

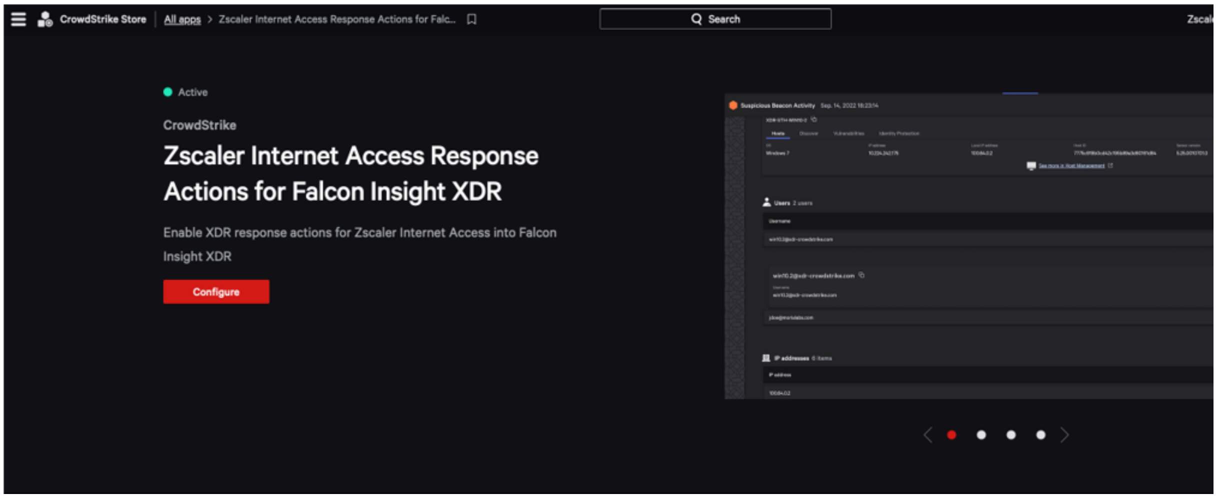
These steps are performed in the ZIA Admin Portal. For more information, see the applicable ZIA product documentation (government agencies, see ZIA product documentation).

1. Enable SCIM support for your IdP.
2. Make a note of these values because you'll need them for the next step:
   a. **Base URL**
   b. **Bearer token**

Step 5: Configure ZIA Response Actions for XDR

In the CrowdStrike Store, configure the ZIA-based response actions that you want to enable.

1. Go to the CrowdStrike Store.
2. Select **Zscaler Internet Access Response Actions for Falcon Insight XDR**.



CrowdStrike Store
All apps > Zscaler Internet Access Response Actions for Falc...
Search
Zscal
Active
CrowdStrike
Configure
Suspicious Beacon Activity

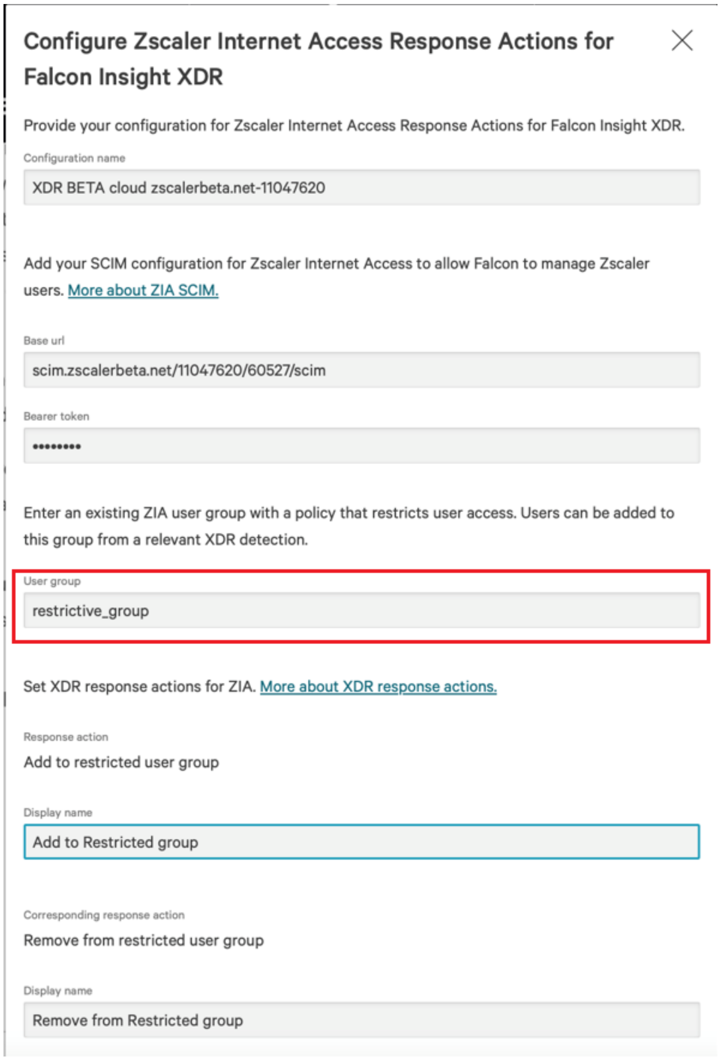
Zscaler Internet Access Response Actions for Falcon Insight XDR

Enable XDR response actions for Zscaler Internet Access into Falcon Insight XDR

Figure 99. Select ZIA Response Actions for Falcon Insight XDR

3. Click **Configure**.
4. Enter a name for the configuration. This name appears in the Falcon Fusion workflow configuration interface.
5. Enter the **Base url** and **Bearer token** values exactly as they appear in your identity provider (IdP), but omit the https:// protocol identifier.

6. Enter the name of the user group that you created earlier. To learn more, see Step 1: Create a User Group for ZIA Response.



Configure Zscaler Internet Access Response Actions for Falcon Insight XDR

Provide your configuration for Zscaler Internet Access Response Actions for Falcon Insight XDR.

Configuration name: XDR BETA cloud zscalerbeta.net-11047620

Add your SCIM configuration for Zscaler Internet Access to allow Falcon to manage Zscaler users. More about ZIA SCIM.

Base url: scim.zscalerbeta.net/11047620/60527/scim

Bearer token: ••••••••

Enter an existing ZIA user group with a policy that restricts user access. Users can be added to this group from a relevant XDR detection.

User group: restrictive_group

Set XDR response actions for ZIA. More about XDR response actions.

Response action: Add to restricted user group

Display name: Add to Restricted group

Corresponding response action: Remove from restricted user group

Display name: Remove from Restricted group

Figure 100. Configure ZIA Response Actions for Falcon Insight XDR

Enter the group name exactly as it appears in Zscaler. Falcon cannot validate the value that you enter in this field.

7. In the two **Display name** fields, enter a short, descriptive name for each response action. For example, you might create two corresponding actions of **Add to restricted user group** and **Remove from restricted user group**. These names appear as selectable ZIA response actions in Falcon Console menus.
8. Click **Save configuration**.

Step 6: Create a Falcon Fusion Workflow for ZIA Response

Optionally, create a Falcon Fusion workflow that initiates a specified ZIA response action when a triggering condition occurs. For example, automatically add a user to a customer-defined restricted user group when the severity of an XDR detection is greater than or equal to Medium.

Create a Falcon Fusion workflow for ZIA response by selecting these values.

Falcon Fusion Setting	Value
Trigger	Alert > XDR Detection.
Condition	(Optional) Customer preference.
Action	Containment > Zscaler response action that you want to take.
Configuration	Select the name of the Zscaler configuration that you created in Step 5: Configure ZIA Response Actions for XDR.

To learn more, refer to the CrowdStrike documentation.

Use Case 9: Prevent Lateral Movement—Zscaler Deception and CrowdStrike

The following steps demonstrate how to prevent malicious software from moving laterally using Zscaler Deception.

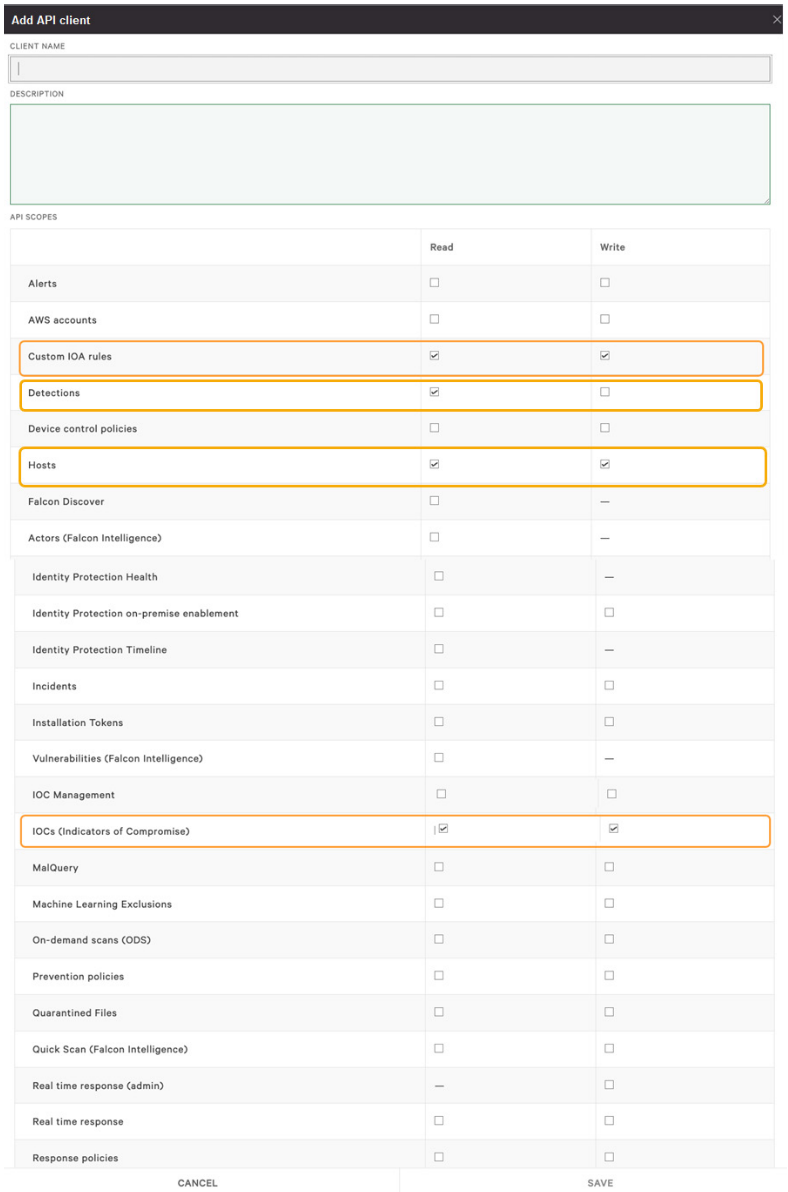
Step 1: Ensure the Prerequisites are Met

Ensure there is network connectivity from the Deception Admin Portal to CrowdStrike Falcon Insight on HTTPS port 443.

Step 2: Create a Client and Secret Key in CrowdStrike Falcon Insight

First, log in to the CrowdStrike Falcon Insight platform:

1. Go to **Support** > **API Clients and Keys**.
2. Click **Add new API client**.
3. In the **Add new API client** window:
   a. Enter the **Client Name** of the new API.
   b. Enter the **Description**.
   c. Under **API Scopes**:
      - For **Detections**, select **Read**.
      - For **Hosts**, select **Read and Write**.
      - For **Custom IoA Rules**, select **Read and Write**.
      - For **IoCs (Indicators of Compromise)**, select **Read and Write**.



Add API client

CLIENT NAME

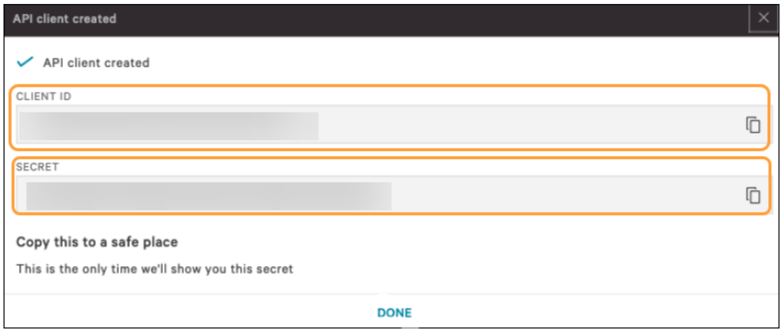
DESCRIPTION

API SCOPES

	Read	Write
Alerts	☐	☐
AWS accounts	☐	☐
Custom IOA rules	☑	☑
Detections	☑	☐
Device control policies	☐	☐
Hosts	☑	☑
Falcon Discover	☐	—
Actors (Falcon Intelligence)	☐	—
Identity Protection Health	☐	—
Identity Protection on-premise enablement	☐	☐
Identity Protection Timeline	☐	—
Incidents	☐	☐
Installation Tokens	☐	☐
Vulnerabilities (Falcon Intelligence)	☐	—
IOC Management	☐	☐
IOCs (Indicators of Compromise)	☑	☑
MalQuery	☐	☐
Machine Learning Exclusions	☐	☐
On-demand scans (ODS)	☐	☐
Prevention policies	☐	☐
Quarantined Files	☐	☐
Quick Scan (Falcon Intelligence)	☐	☐
Real time response (admin)	—	☐
Real time response	☐	☐
Response policies	☐	☐

Figure 101. Read and write options for API scopes

4. Click **Save**. The **API client created** window appears.



API client created

✓ API client created

CLIENT ID

[redacted]

SECRET

[redacted]

Copy this to a safe place

This is the only time we'll show you this secret

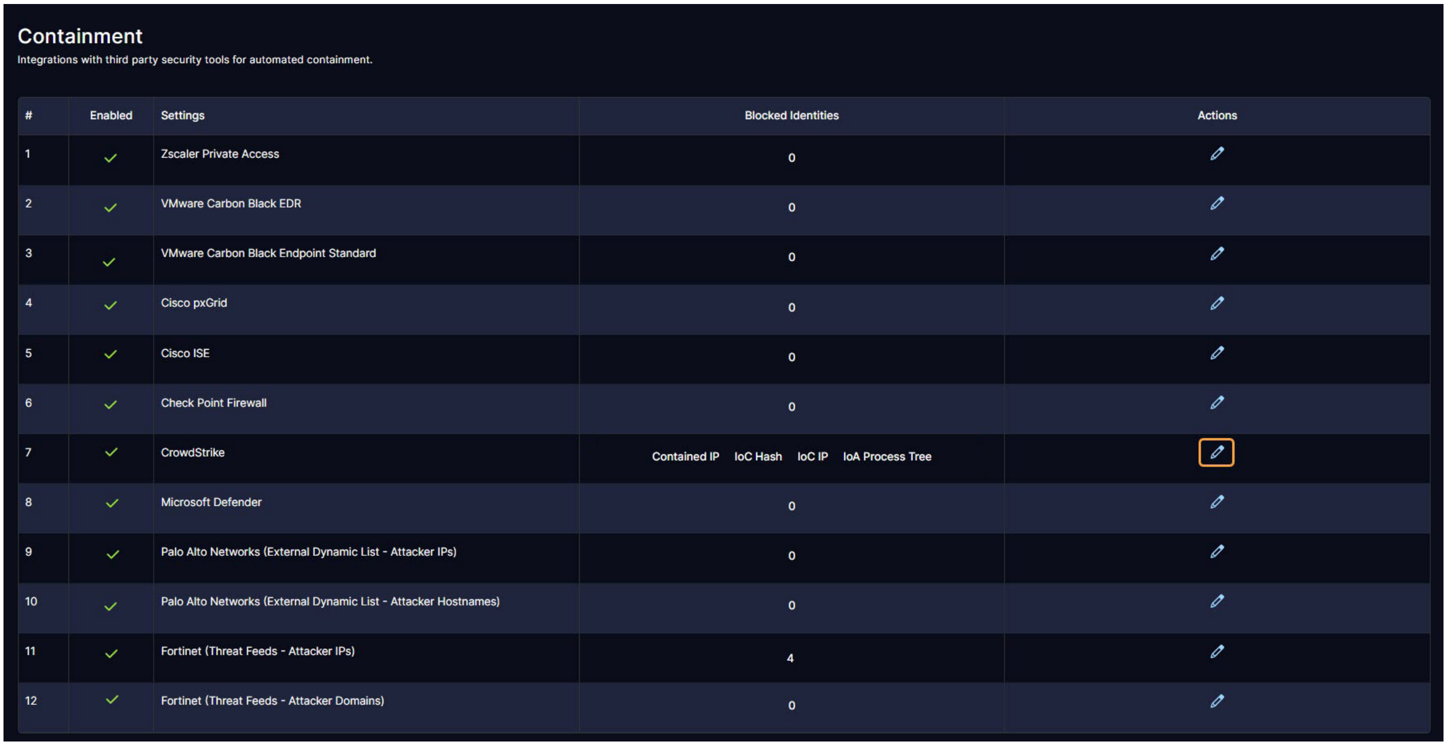
Figure 102. API Client created

5. Copy the client ID and secret key.
6. Click **Done**.

Step 3: Configure the Containment Integration Between Deception and CrowdStrike Falcon Insight

From the Deception Admin Portal:

1. Go to **Orchestrate** > **Containment**.
2. In the table, locate CrowdStrike and click the **Edit** icon under the **Actions** column.



Containment

Integrations with third party security tools for automated containment.

#	Enabled	Settings	Blocked Identities	Actions
1	✓	Zscaler Private Access	0	✎
2	✓	VMware Carbon Black EDR	0	✎
3	✓	VMware Carbon Black Endpoint Standard	0	✎
4	✓	Cisco pxGrid	0	✎
5	✓	Cisco ISE	0	✎
6	✓	Check Point Firewall	0	✎
7	✓	CrowdStrike	Contained IP IoC Hash IoC IP IoA Process Tree	✎
8	✓	Microsoft Defender	0	✎
9	✓	Palo Alto Networks (External Dynamic List - Attacker IPs)	0	✎
10	✓	Palo Alto Networks (External Dynamic List - Attacker Hostnames)	0	✎
11	✓	Fortinet (Threat Feeds - Attacker IPs)	4	✎
12	✓	Fortinet (Threat Feeds - Attacker Domains)	0	✎

Figure 103. Containment

3. Perform the following in the **CrowdStrike Falcon Insight Configuration** window.
   a. **Enabled**: Select to enable the containment.

b. **URL**: Enter the CrowdStrike API endpoint URL. For example, enter `https://api.crowdstrike.com`.

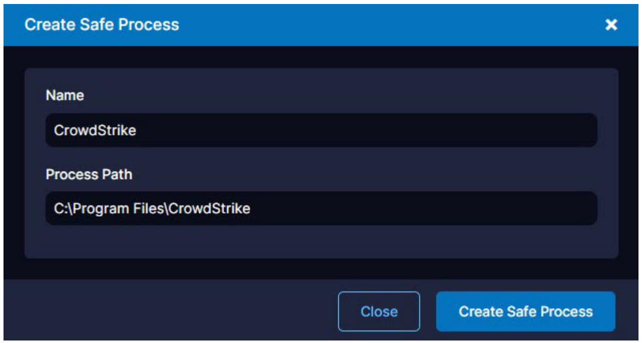
   i. **Client ID**: Enter the client ID that you copied in Step 2: Create a Client and Secret Key in CrowdStrike Falcon Insight.

   ii. **Client Secret**: Enter the client secret that you copied in Step 2: Create a Client and Secret Key in CrowdStrike Falcon Insight.

   iii. **Marking IoA Safe Processes**: (Optional) To avoid sharing legitimate process trees with CrowdStrike for IoA actions, follow these steps to designate legitimate processes as safe processes:

   - Click **IoA Safe Processes**.
   - In the **Safe Processes** window, click **Add Safe Process**.
   - In the **Create Safe Process** window, provide the following details:
     - **Name**: Enter a name for the safe process.
     - **Process Path**: Enter the path of the executable file from which the process originates.
   - Click **Create Safe Process**.

   Processes are marked as safe only if all elements of the process tree have an entry in the safe processes list.



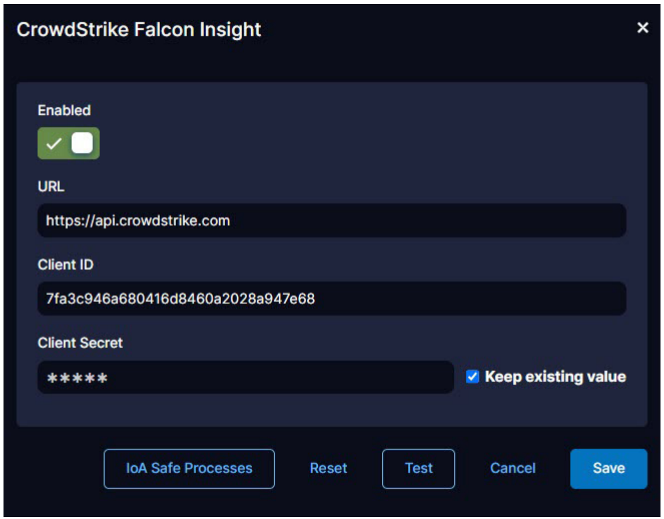
Create Safe Process

Name: CrowdStrike

Process Path: C:\Program Files\CrowdStrike

Figure 104. Create Safe Process

4. Click **Save**.
5. Click **Test** to verify the reachability of the CrowdStrike Falcon Insight platform.



CrowdStrike Falcon Insight

Enabled: ✓

URL: https://api.crowdstrike.com

Client ID: 7fa3c946a680416d8460a2028a947e68

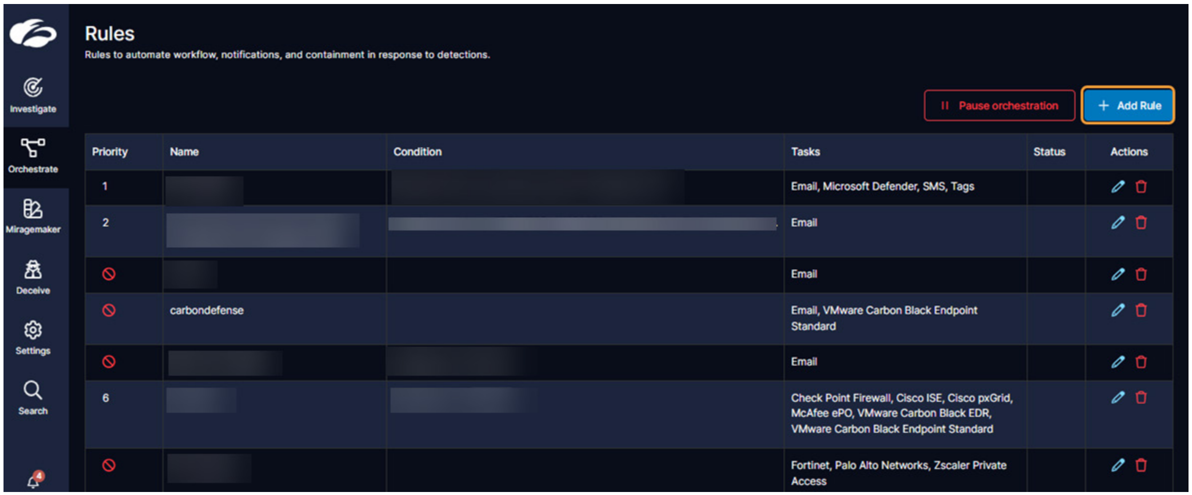
Client Secret: ***** ☑ Keep existing value

Figure 105. CrowdStrike Falcon Insight

Step 4: Configure Orchestration Rule or Take Action to Contain Detected Attackers

You can contain detected attackers automatically by creating an orchestrated rule, or manually by taking action from the Investigate page.

1. Create a rule.
    a. Go to **Orchestrate** > **Rules**.
    b. Click **Add Rule**.



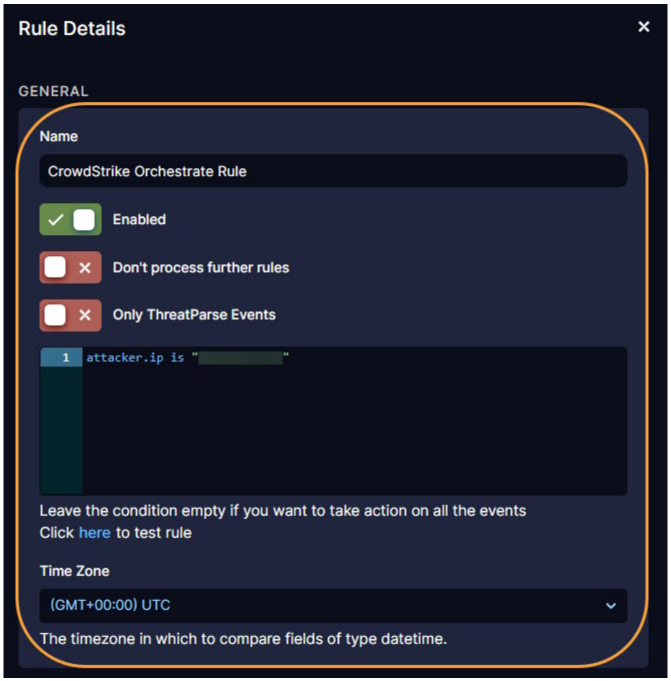
Rules

Rules to automate workflow, notifications, and containment in response to detections.

Priority	Name	Condition	Tasks	Status	Actions
1	[redacted]	[redacted]	Email, Microsoft Defender, SMS, Tags		
2	[redacted]	[redacted]	Email		
⊘	[redacted]		Email		
⊘	carbondefense		Email, VMware Carbon Black Endpoint Standard		
⊘	[redacted]	[redacted]	Email		
6	[redacted]	[redacted]	Check Point Firewall, Cisco ISE, Cisco pxGrid, McAfee ePO, VMware Carbon Black EDR, VMware Carbon Black Endpoint Standard		
⊘	[redacted]		Fortinet, Palo Alto Networks, Zscaler Private Access		

Figure 106. Rules

2. In the **Rule Details** window:
    a. Enter the name of the rule.
    b. Select **Enabled**.
    c. Create a rule using queries and conditions.



Rule Details

GENERAL

Name

CrowdStrike Orchestrate Rule

☑ Enabled

☒ Don't process further rules

☒ Only ThreatParse Events

```
attacker.ip is "[redacted]"
```

Leave the condition empty if you want to take action on all the events

Click here to test rule

Time Zone

(GMT+00:00) UTC

The timezone in which to compare fields of type datetime.

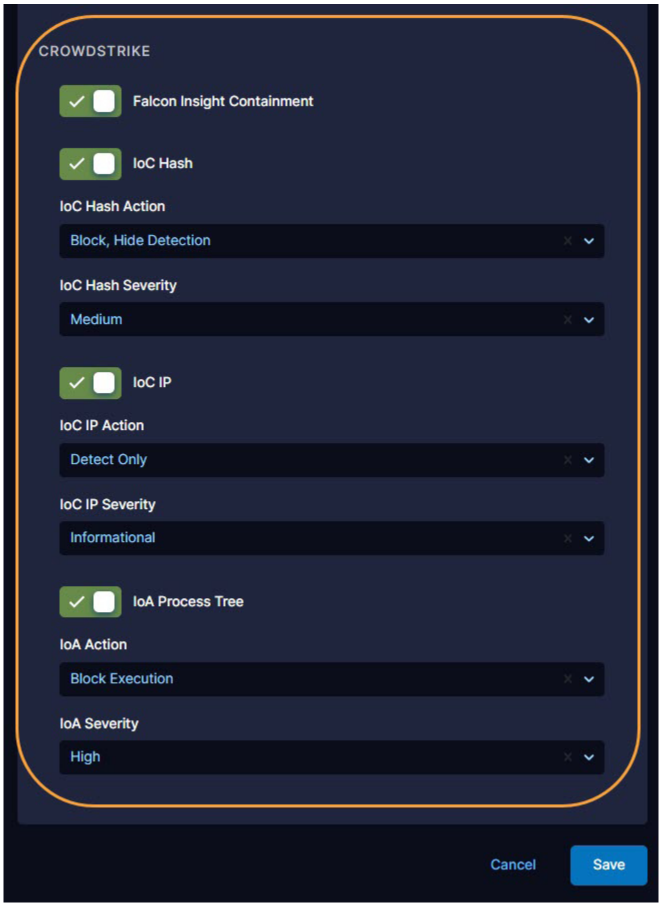
Figure 107. Rule Details

d. Under **Respond**, locate the **CrowdStrike** section, and configure the following options:

- **Falcon Insight Containment**: Enable to contain an endpoint using CrowdStrike when an event matching the configured rule occurs.
- **IoC Hash**: Enable to share file hashes that are considered indicators of compromise with CrowdStrike and select an appropriate IoC Hash Action and IoC Hash Severity.
- **IoC Hash Action**: Choose the action for CrowdStrike to perform when IoC hashes are shared:
    - **Detect Only**: Show the indicator as a detection and take no other action.
    - **Block**: Add the indicator to the blocklist and show it as a detection.
    - **Block, Hide Detection**: Add the indicator to the blocklist and do not detect it.
    - **Allow**: Add the indicator to the allowlist and do not detect it.
    - **No Action**: Save the indicator for future use and take no action.
- **IoC Hash Severity**: Designate an appropriate severity level for indicators to share with CrowdStrike for IoC hashes. The available levels are **Informational**, **Low**, **Medium**, **High**, and **Critical**.
- I**oC IP**: Enable to share IPs that are considered indicators of compromise with CrowdStrike and select an appropriate IoC IP Action and IoC IP Severity.
- **IoC IP Action**: Choose the action for CrowdStrike to perform when IPs are shared:
    - **Detect Only**: Show the indicator as a detection and take no other action.
    - **No Action**: Save the indicator for future use and take no action.
- **IoC IP Severity**: Designate an appropriate severity level for indicators to share with CrowdStrike for IoC IPs. The available levels are **Informational**, **Low**, **Medium**, **High**, and **Critical**.
- **IoA Process Tree**: Enable to share process trees that are considered indicators of attack with CrowdStrike and select an appropriate IoA Action and IoA Severity.
- **IoA Action**: Choose the action for CrowdStrike to perform when IoA process trees are shared:
    - **Detect**: Show the indicator as a detection and take no other action.
    - **Monitor**: Use the indicator for informational use only and take no action, nor show it as a detection.
    - **Block Execution**: Terminate the process and show the indicator as detection.

  Exercise caution when choosing the Block Execution action as CrowdStrike terminates all processes that match with the process tree across all endpoints in your network. To avoid terminating legitimate processes, make sure that you have configured IoA safe processes.

- **IoA Severity**: Designate an appropriate severity level for indicators to share with CrowdStrike for IoC hashes and IPs. The available levels are **Informational**, **Low**, **Medium**, **High**, and **Critical**.



CROWDSTRIKE

☑ Falcon Insight Containment

☑ IoC Hash

IoC Hash Action: Block, Hide Detection

IoC Hash Severity: Medium

☑ IoC IP

IoC IP Action: Detect Only

IoC IP Severity: Informational

☑ IoA Process Tree

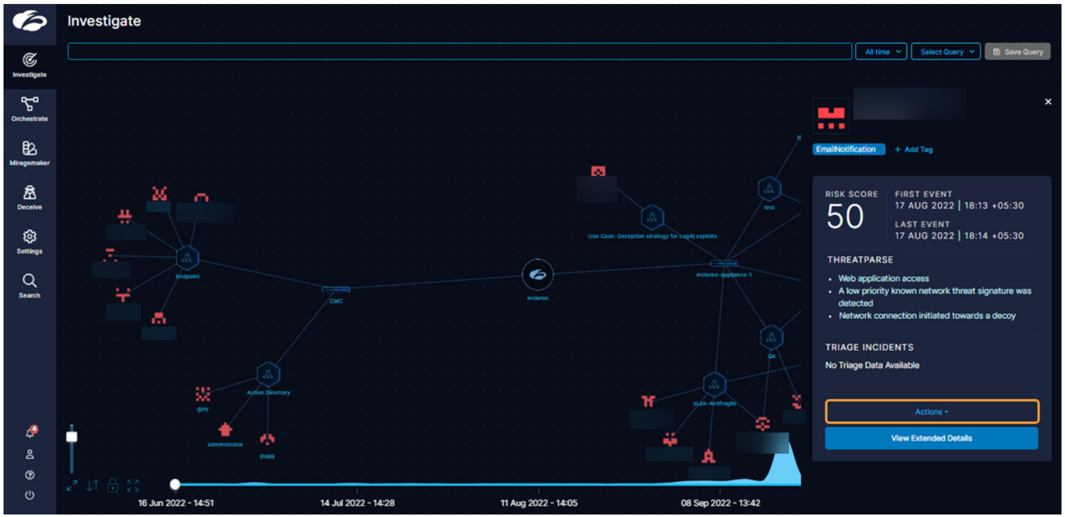
IoA Action: Block Execution

IoA Severity: High

Figure 108. Configure CrowdStrike options

e. Click **Save**.

3. Take action from the **Investigate** page. For more information, refer to the CrowdStrike documentation.
   a. On the **Investigate** page, click an **Attack** icon on the alert graph. The attacker details pane opens.



[redacted]

RISK SCORE
50

FIRST EVENT
17 AUG 2022 | 18:13 +05:30

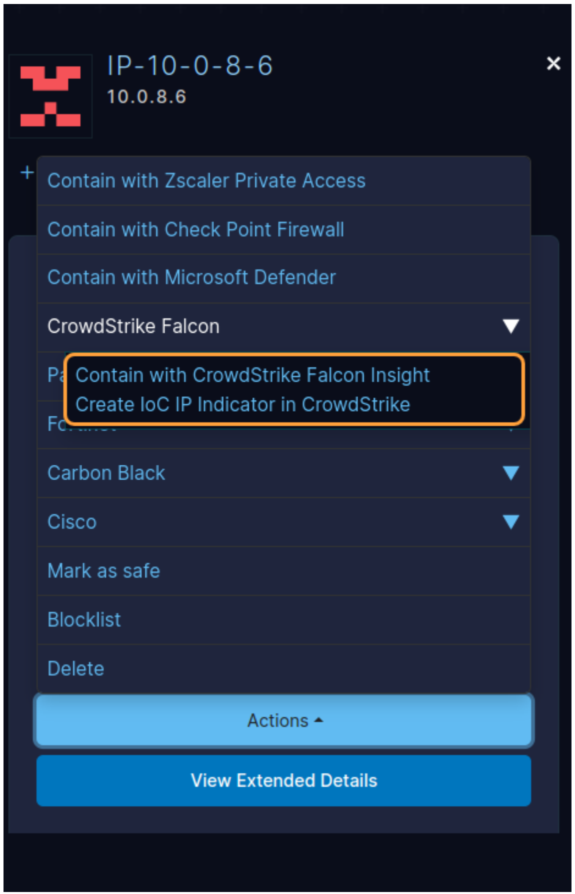
LAST EVENT
17 AUG 2022 | 18:14 +05:30

THREATPARSE
- Web application access
- A low priority known network threat signature was detected
- Network connection initiated towards a decoy

TRIAGE INCIDENTS
No Triage Data Available

Figure 109. Investigate page of the Deception Admin Portal

   b. Click **Actions**. A list of actions that you can take to remediate the threat appears. If any orchestration rules were set up to automate sharing with CrowdStrike, the IoC or IoA that has been shared with CrowdStrike appears in the Containment section of the Deception Admin Portal.
   c. (Optional) You can also select one of the following containment actions manually.


IP-10-0-8-6
10.0.8.6

Contain with Zscaler Private Access
Contain with Check Point Firewall
Contain with Microsoft Defender
CrowdStrike Falcon
Contain with CrowdStrike Falcon Insight
Create IoC IP Indicator in CrowdStrike
Carbon Black
Cisco
Mark as safe
Blocklist
Delete
Actions
View Extended Details

Figure 110. Contain with CrowdStrike Insight

Use Case 10: Contextualizing Risk–Avalor UVM and CrowdStrike

Avalor's Data Fabric and Unified Vulnerability Management (UVM) solution ingests, normalizes, and unifies data across enterprise security and business systems to deliver actionable insights, analytics, and operational efficiencies. The following steps demonstrate how Avalor UVM can leverage CrowdStrike incidents, alerts, assets, and vulnerabilities, combined with data from other sources, to contextualize and calculate personalized risk assessments for the organization.

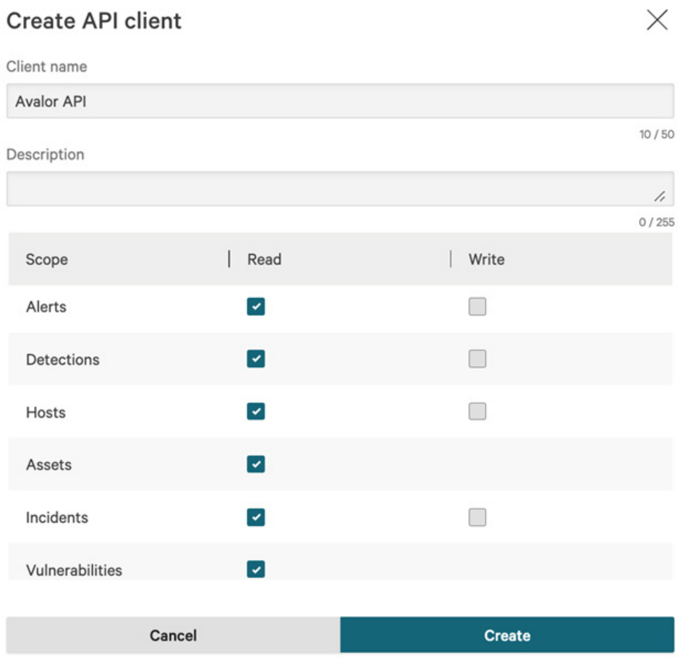
Step 1: Ensure the Prerequisites are Met

Ensure there is network connectivity from the Avalor UVM Admin Portal to CrowdStrike Falcon Insight on HTTPS port 443.

Step 2: Create a Client and Secret Key in CrowdStrike Falcon Insight

First, log in to the CrowdStrike Falcon Insight platform:

1. Go to **Support** > **API Clients and Keys**.
2. Click **Add new API client**.
3. In the **Add new API client** window:
    a. Enter the **Client Name** of the new API.
    b. Enter the **Description**.
    c. Under **API Scopes**:
        i. For **Alerts**, select **Read**.
        ii. For **Detections**, select **Read**.
        iii. For **Hosts**, select **Read**.
        iv. For **Assets**, select **Read**.
        v. For **Incidents**, select **Read**.
        vi. For **Vulnerabilities**, select **Read**.



Create API client

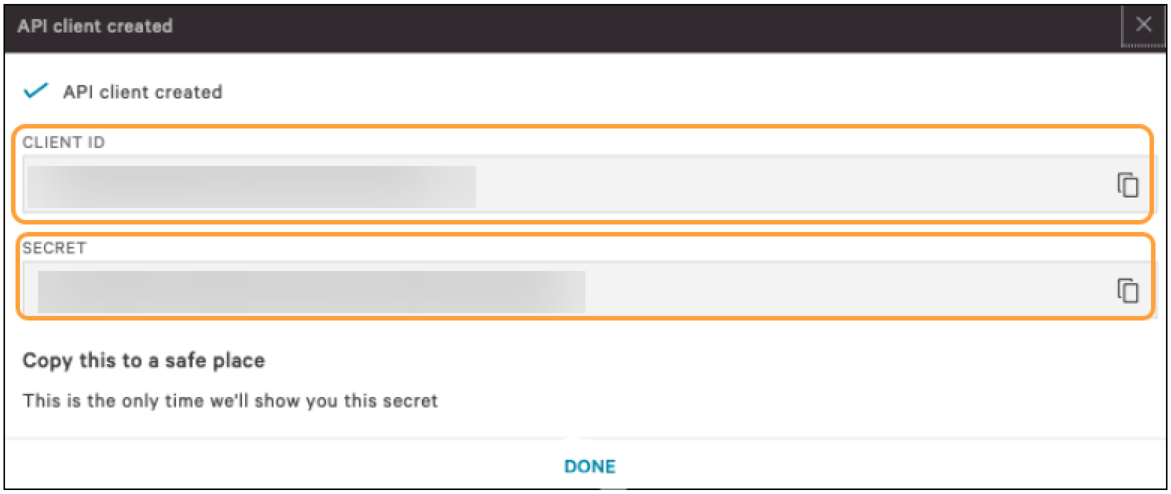
Client name: Avalor API (10 / 50)

Description: (0 / 255)

Scope	Read	Write
Alerts	☑	□
Detections	☑	□
Hosts	☑	□
Assets	☑	
Incidents	☑	□
Vulnerabilities	☑	

Figure 111. Read and write options for API scopes

4. Click **Save**. The **API client created** window is displayed.



API client created

✓ API client created

CLIENT ID

[redacted]

SECRET

[redacted]

Copy this to a safe place

This is the only time we'll show you this secret

DONE

Figure 112. API Client created

5. Copy the **Client ID** and **Secret Key**.
6. Click **Done**.

Step 3: Configure the Avalor UVM Data Connectors—CrowdStrike Alerts

From the Avalor UVM Admin Portal:

1. Click **Configure**.

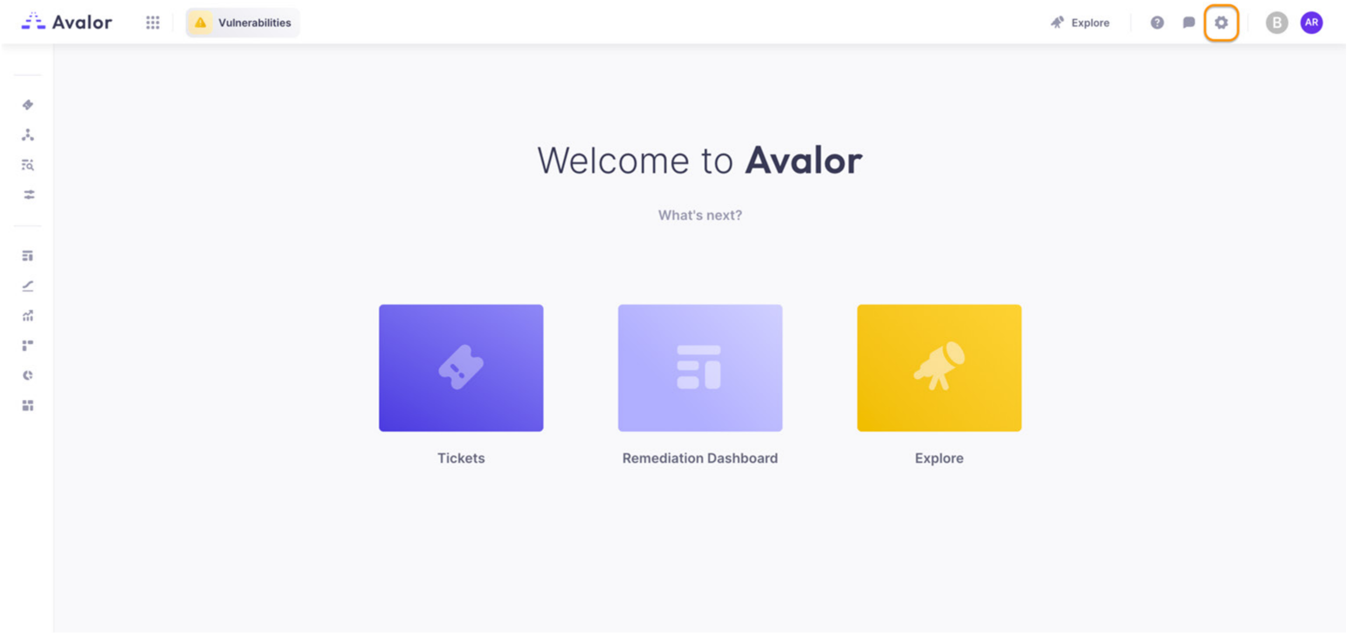
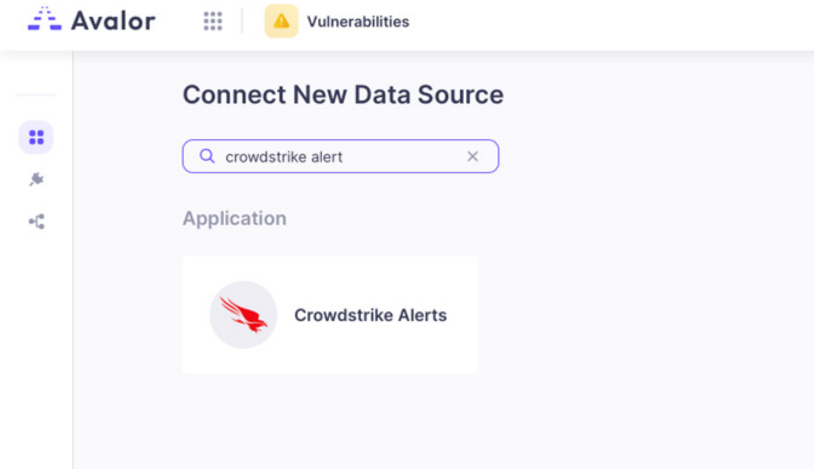


Figure 113. Configure

2. Click **Create**.
3. Locate and click the **CrowdStrike Alerts** connector.



Connect New Data Source

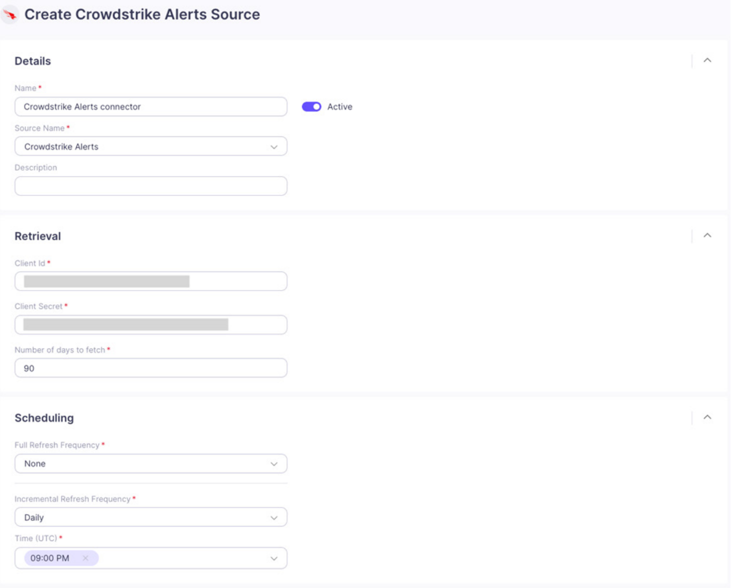
crowdstrike alert

Application

Crowdstrike Alerts

Figure 114. CrowdStrike Alerts

4. In the **Create Crowdstrike Alerts Source** window, configure the following:
    a. **Name**: Enter a name for the Data Connector.
    b. **Active**: Toggle to enable the Data Connector.
    c. **Client Id**: Enter the **Client Id**.
    d. **Client Secret**: Enter the **Client Secret**.
    e. **Number of Days to Fetch**: Enter the number of historical days the connector fetches when retrieving CrowdStrike data.
    f. **Time**: Enter the time of day the connector should fetch updated information. Zscaler recommends you set the timing for CrowdStrike to have the appropriate time to scan and update its findings so that the Data Connector can retrieve updated information.



Create Crowdstrike Alerts Source

Details

Name *
Crowdstrike Alerts connector

Active

Source Name *
Crowdstrike Alerts

Description

Retrieval

Client Id *
[redacted]

Client Secret *
[redacted]

Number of days to fetch *
90

Scheduling

Full Refresh Frequency *
None

Incremental Refresh Frequency *
Daily

Time (UTC) *
09:00 PM

Figure 115. Alerts Source created

5. Click **Save**.
6. Click **Test** to verify the reachability of the CrowdStrike Falcon Insight platform.

Step 4: Configure the Avalor UVM Data Connectors—CrowdStrike Assets

From the Avalor UVM Admin Portal:

1. Click **Configure**.

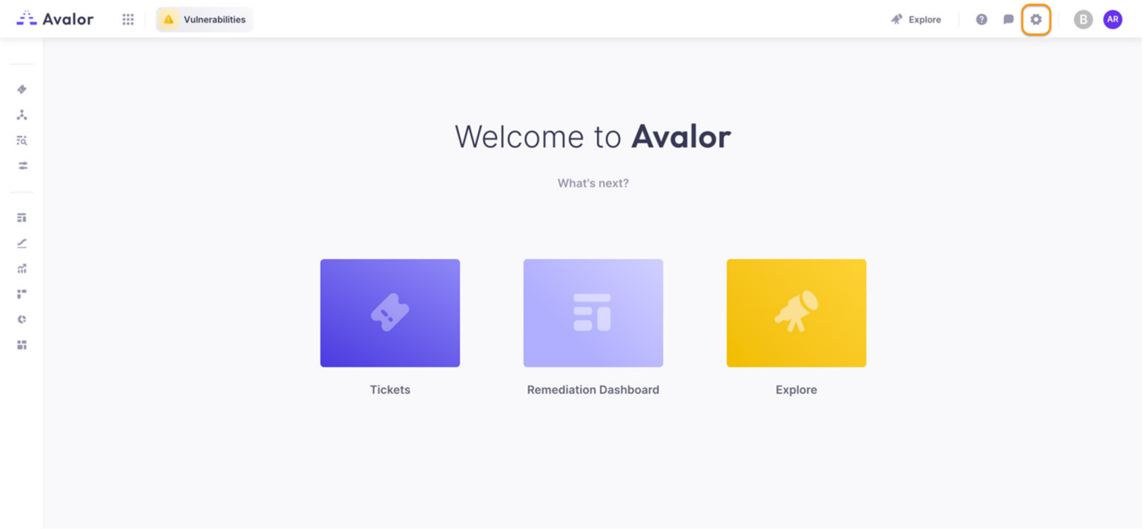


Figure 116. Configure

2. Click the **Create** button.
3. Locate and click the **CrowdStrike Assets** connector.

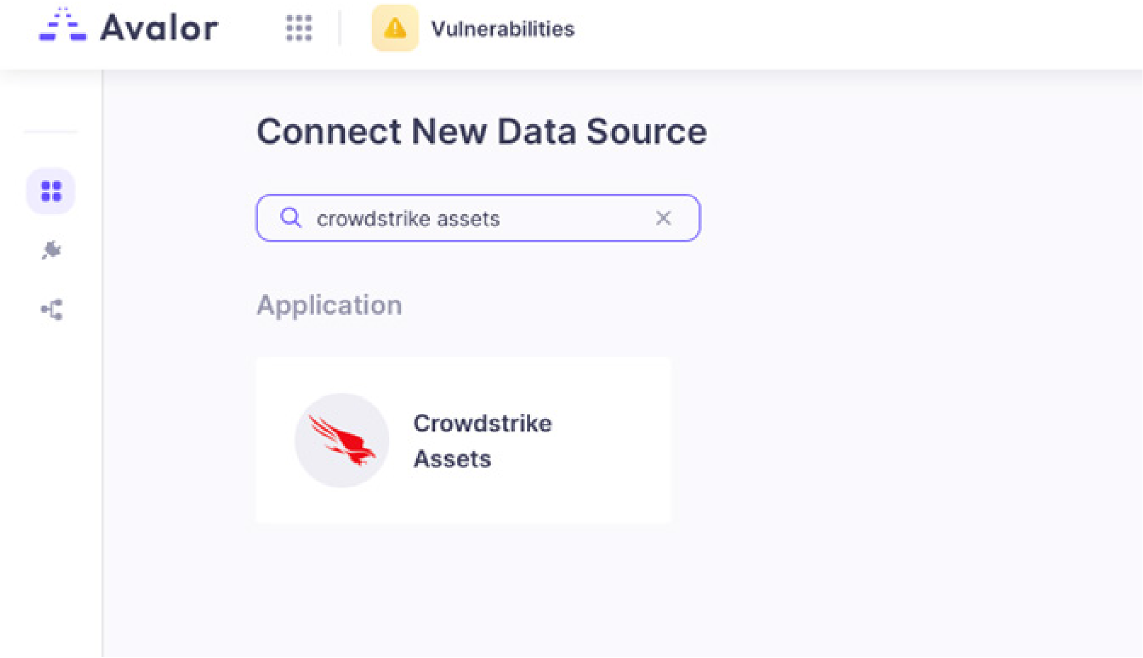
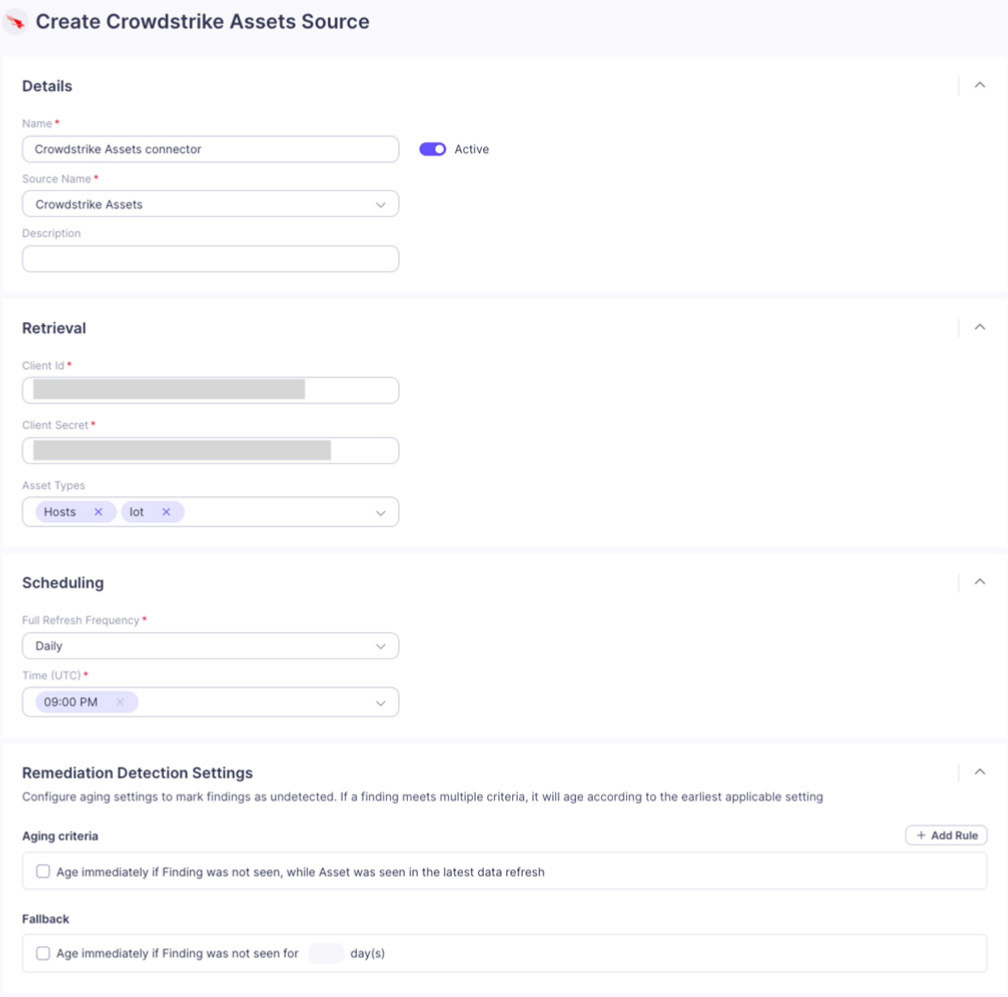


Figure 117. CrowdStrike Assets

4. Configure the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle to enable the Data Connector.
   c. **Client Id**: Enter the **Client Id**.
   d. **Client Secret**: Enter the **Client Secret**.
   e. **Asset Type**: Select the Asset Type (**Host**, **IoT**, or both) that the connector should fetch.
   f. **Time**: Enter the time of day the connector should fetch updated information. Zscaler recommends you set the timing for CrowdStrike to have the appropriate time to scan and update its findings so that the Data Connector can retrieve updated information.



Create Crowdstrike Assets Source

Details

Name *: Crowdstrike Assets connector

Active (on)

Source Name *: Crowdstrike Assets

Description:

Retrieval

Client Id *: [redacted]

Client Secret *: [redacted]

Asset Types: Hosts ×, Iot ×

Scheduling

Full Refresh Frequency *: Daily

Time (UTC) *: 09:00 PM ×

Remediation Detection Settings

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting

Aging criteria

□ Age immediately if Finding was not seen, while Asset was seen in the latest data refresh

Fallback

□ Age immediately if Finding was not seen for day(s)

Figure 118. Assets Source created

5. Click **Save**.
6. Click **Test** to verify the reachability of the CrowdStrike Falcon Insight platform.

Step 5: Configure the Avalor UVM Data Connectors—CrowdStrike Incidents

From the Avalor UVM Admin Portal:

1. Click **Configure**.

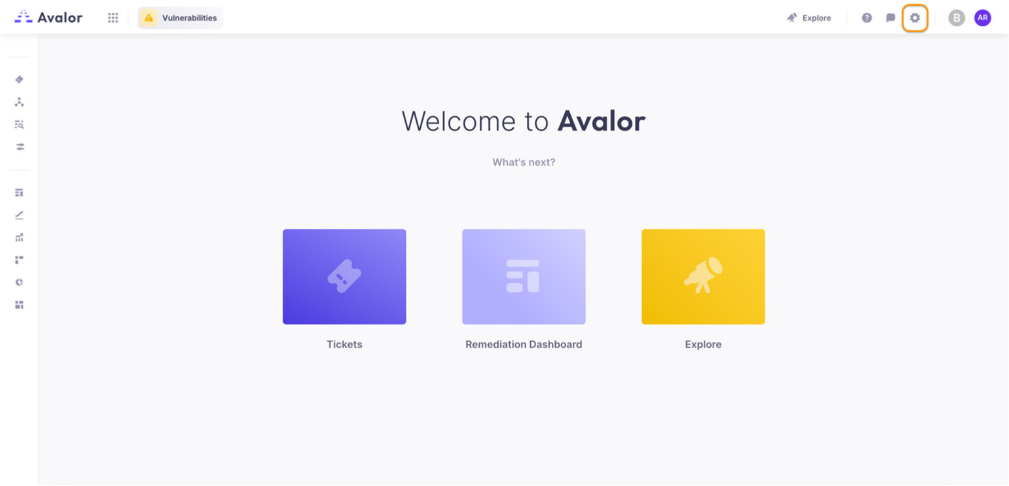


Figure 119. Configure

2. Click **Create**.
3. Locate and click the **CrowdStrike Incidents** connector.

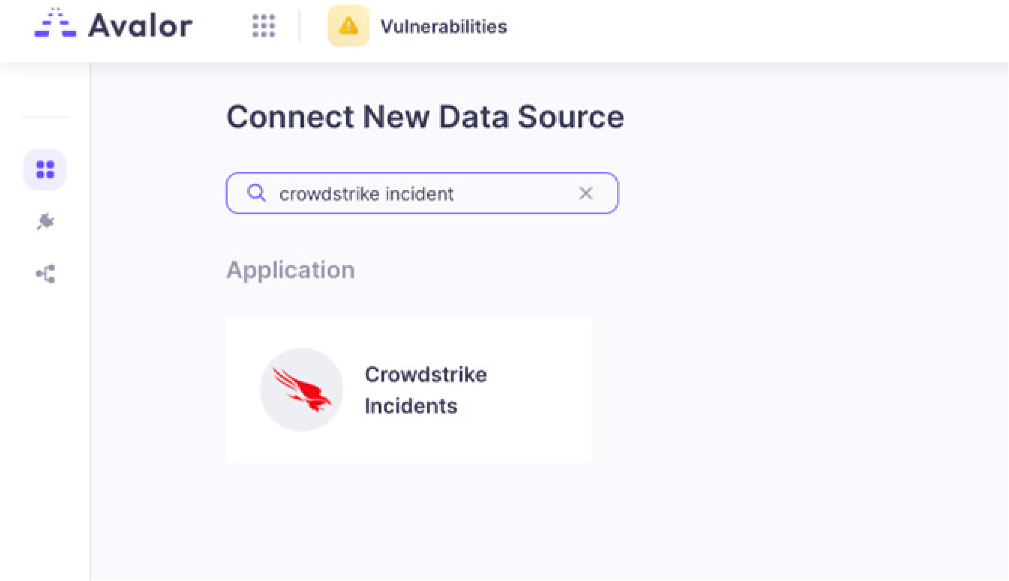
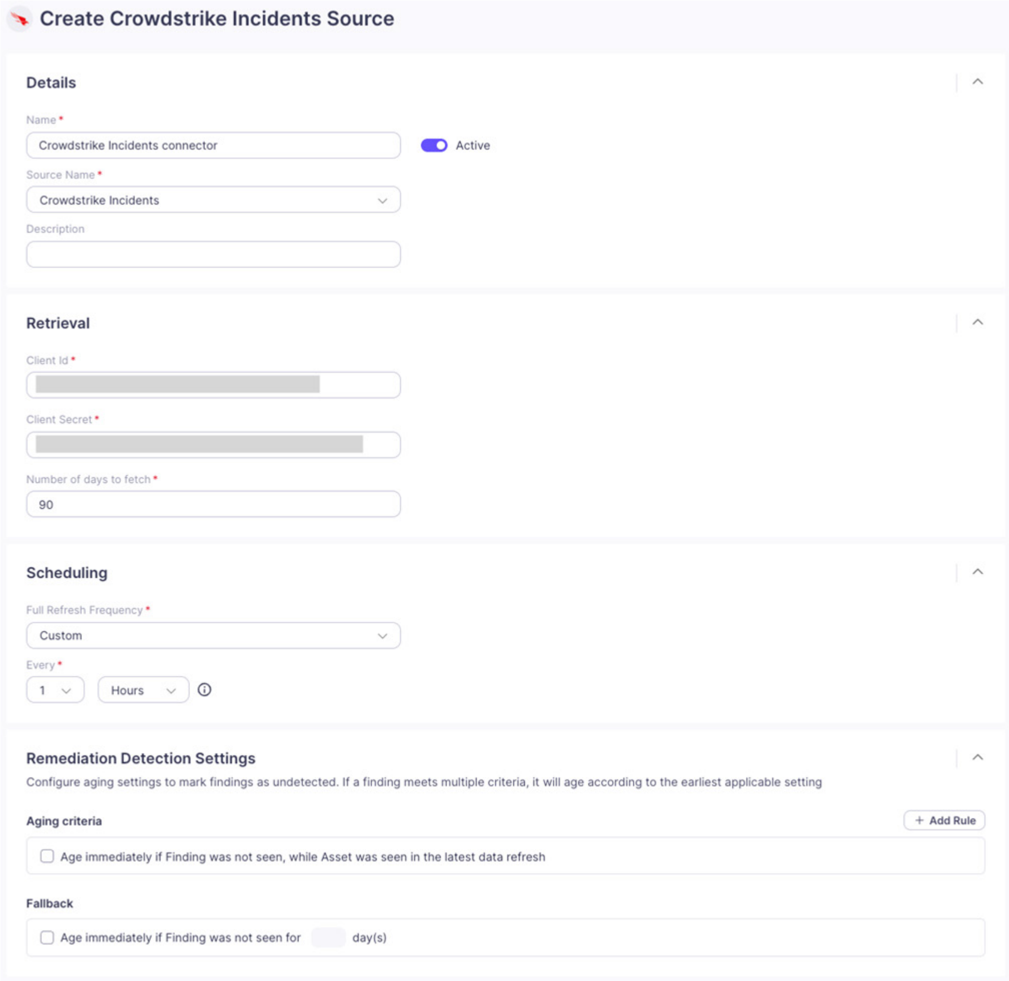


Figure 120. CrowdStrike Incidents

4. In the **Create Crowdstrike Incidents Source** window, configure the following:
    a. **Name**: Enter a name for the Data Connector.
    b. **Active**: Toggle to enable the Data Connector.
    c. **Client Id**: Enter the **Client Id**.
    d. **Client Secret**: Enter the **Client Secret**.
    e. **Number of Days to Fetch**: Enter the number of historical days the connector will fetch when retrieving CrowdStrike data.
    f. **Time**: Enter the time of day the connector should fetch updated information. Zscaler recommends you set the timing for CrowdStrike to have the appropriate time to scan and update its findings so that the Data Connector can retrieve updated information.



Create Crowdstrike Incidents Source

Details

Name *: Crowdstrike Incidents connector

Active

Source Name *: Crowdstrike Incidents

Description

Retrieval

Client Id *: [redacted]

Client Secret *: [redacted]

Number of days to fetch *: 90

Scheduling

Full Refresh Frequency *: Custom

Every *: 1 Hours

Remediation Detection Settings

Configure aging settings to mark findings as undetected. If a finding meets multiple criteria, it will age according to the earliest applicable setting

Aging criteria

□ Age immediately if Finding was not seen, while Asset was seen in the latest data refresh

Fallback

□ Age immediately if Finding was not seen for day(s)

Figure 121. Incidents Source created

5. Click **Save**.
6. Click **Test** to verify the reachability of the CrowdStrike Falcon Insight platform.

Step 6: Configure the Avalor UVM Data Connectors—CrowdStrike Vulnerabilities

From the Avalor UVM Admin Portal:

1. Click **Configure**.

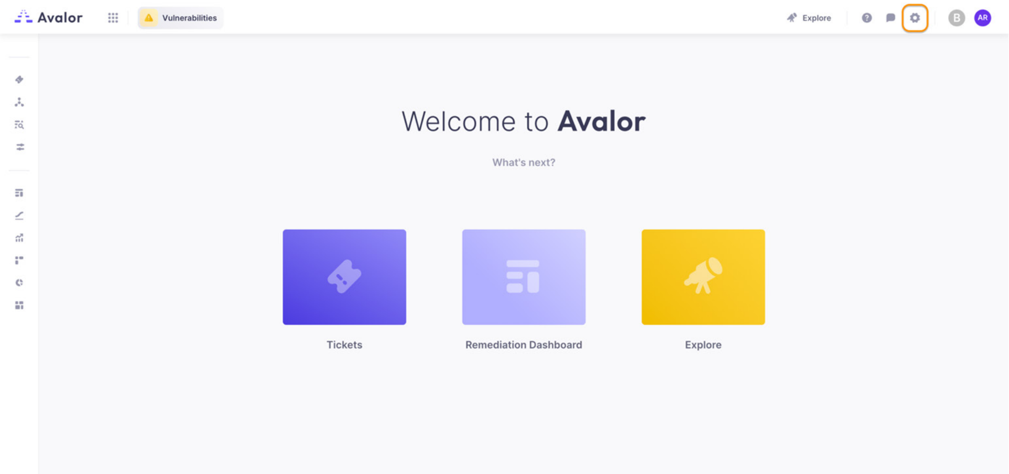


Figure 122. Configure

2. Click **Create**.
3. Locate and click the **CrowdStrike Vulnerabilities** connector.

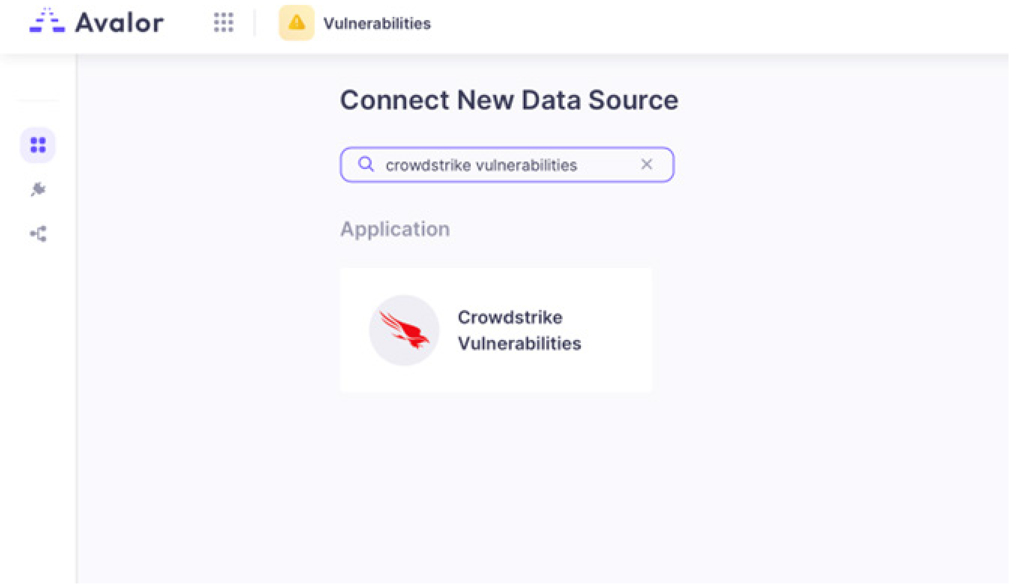
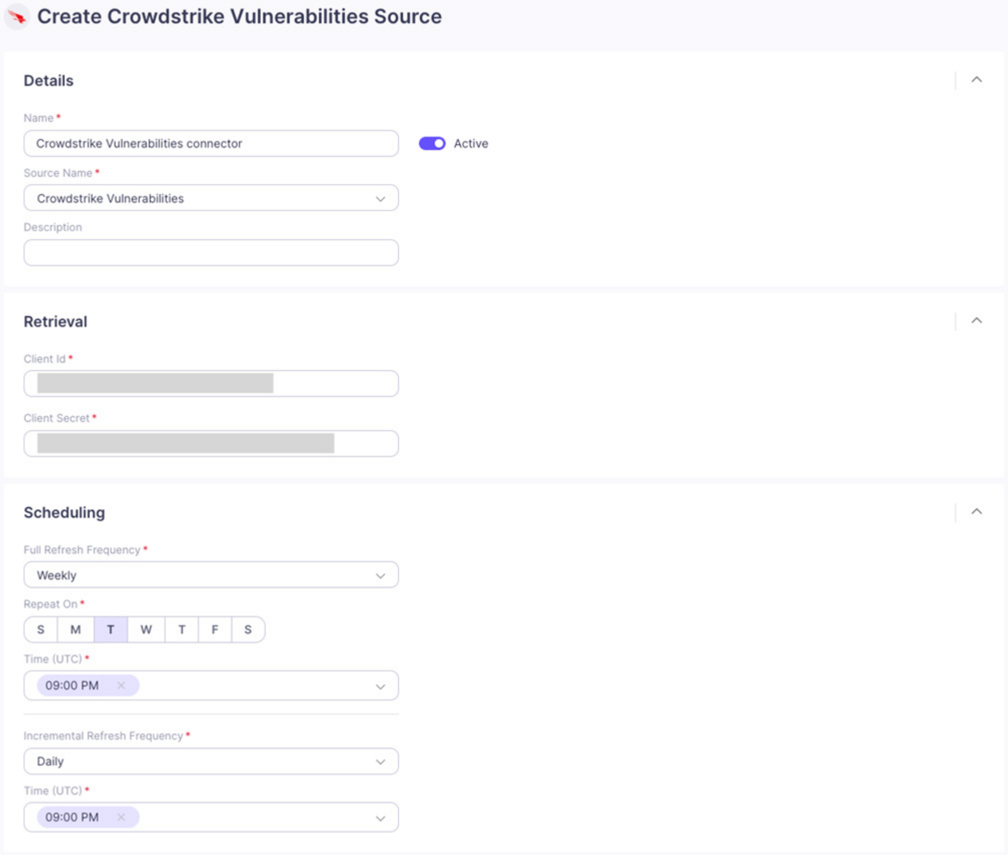


Figure 123. CrowdStrike Vulnerabilities

4. In the **Create Crowdstrike Vulnerabilities Source** window, configure the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle to enable the Data Connector.
   c. **Client Id**: Enter the **Client Id**.
   d. **Client Secret**: Enter the **Client Secret**.
   e. **Time**: Enter the time of day the connector should fetch updated information. Zscaler recommends you set the timing for CrowdStrike to have the appropriate time to scan and update its findings so that the Data Connector can retrieve updated information.



Create Crowdstrike Vulnerabilities Source

Details

Name *
Crowdstrike Vulnerabilities connector

Active

Source Name *
Crowdstrike Vulnerabilities

Description

Retrieval

Client Id *
[redacted]

Client Secret *
[redacted]

Scheduling

Full Refresh Frequency *
Weekly

Repeat On *
S M [✓ T] W T F S

Time (UTC) *
09:00 PM

Incremental Refresh Frequency *
Daily

Time (UTC) *
09:00 PM

Figure 124. Vulnerabilities Source created

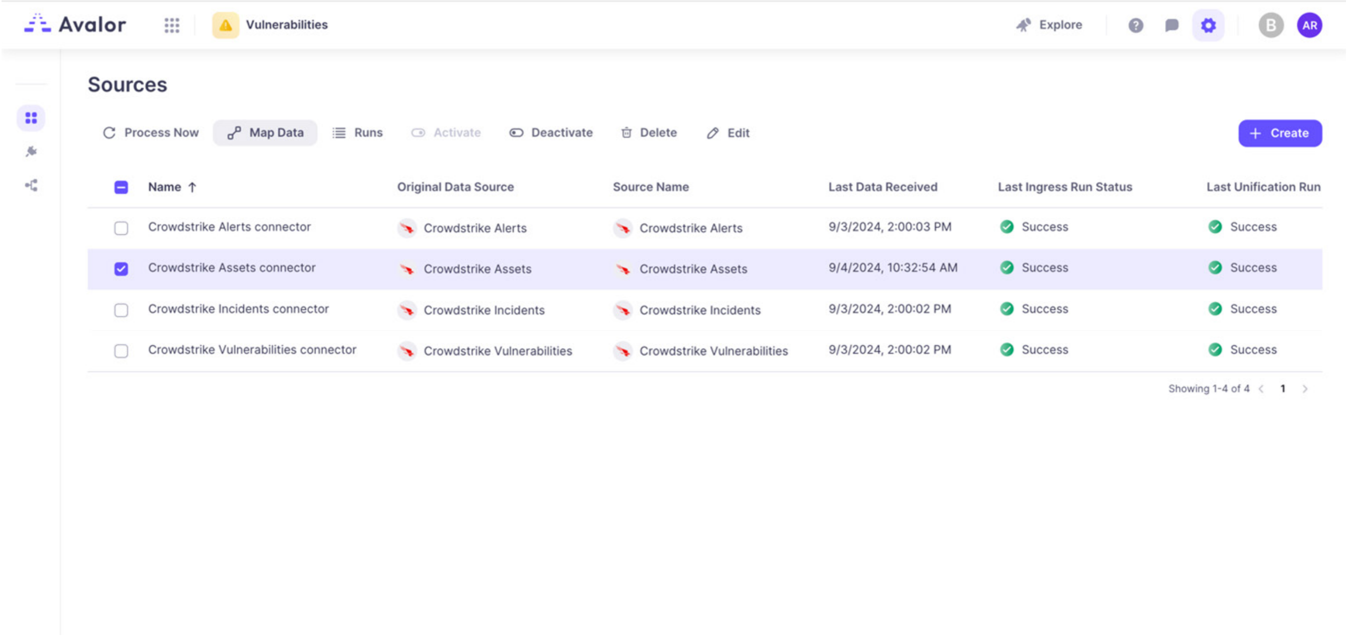
5. Click **Save**.
6. Click **Test** to verify the reachability of the CrowdStrike Falcon Insight platform.

Step 7: Review and Adjust Data Model Mapping

Avalor UVM automatically maps ingested data to the default Data Model, so analysis can begin immediately. However, many data sources also provide additional data points that might provide additional context to risk prioritization.

The following example shows how to map the Has EDR Data Model Entity to the ingested CrowdStrike Asset data so that you can use this field as a mitigating score factor when calculating risk.

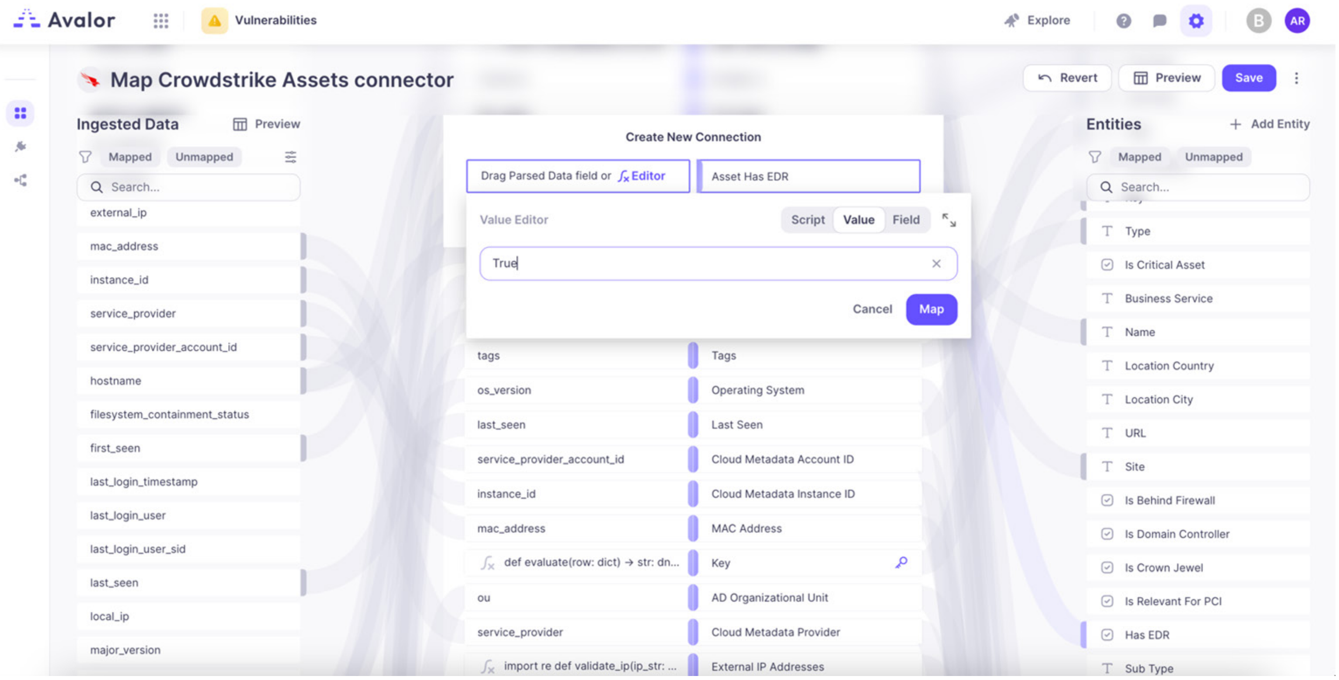
1. From the **Avalor UVM Sources** page:
    a. Select the **CrowdStrike Assets** connector configured in Step 4: Configure the Avalor UVM Data Connectors—CrowdStrike Assets.
    b. Click **Map Data**.



☐	Name ↑	Original Data Source	Source Name	Last Data Received	Last Ingress Run Status	Last Unification Run
☐	Crowdstrike Alerts connector	Crowdstrike Alerts	Crowdstrike Alerts	9/3/2024, 2:00:03 PM	✓ Success	✓ Success
☑	Crowdstrike Assets connector	Crowdstrike Assets	Crowdstrike Assets	9/4/2024, 10:32:54 AM	✓ Success	✓ Success
☐	Crowdstrike Incidents connector	Crowdstrike Incidents	Crowdstrike Incidents	9/3/2024, 2:00:02 PM	✓ Success	✓ Success
☐	Crowdstrike Vulnerabilities connector	Crowdstrike Vulnerabilities	Crowdstrike Vulnerabilities	9/3/2024, 2:00:02 PM	✓ Success	✓ Success

Figure 125. Map Data

2. In the **Map connector** window:
   a. Review the **ingested** data fields in the left-side column.
   b. Review the **Data Model Entities** in the right-side column.
   c. (Optional) Click **Add Entity** to create a custom Entity within the Data Model to map to.
   d. Review the default mappings in the center column.
   e. Double-click the **Has EDR** entity in the right-side column to bring it into the center column.
   f. Click the **Function Editor** link to set an expression for the entity.
   g. Change the **Value Editor** tab to **Value** and enter `True` in the blank field.
   h. Click **Map**.
   i. (Optional) Click **Preview** to review the updated Data Model mappings.
   j. Click **Save**.

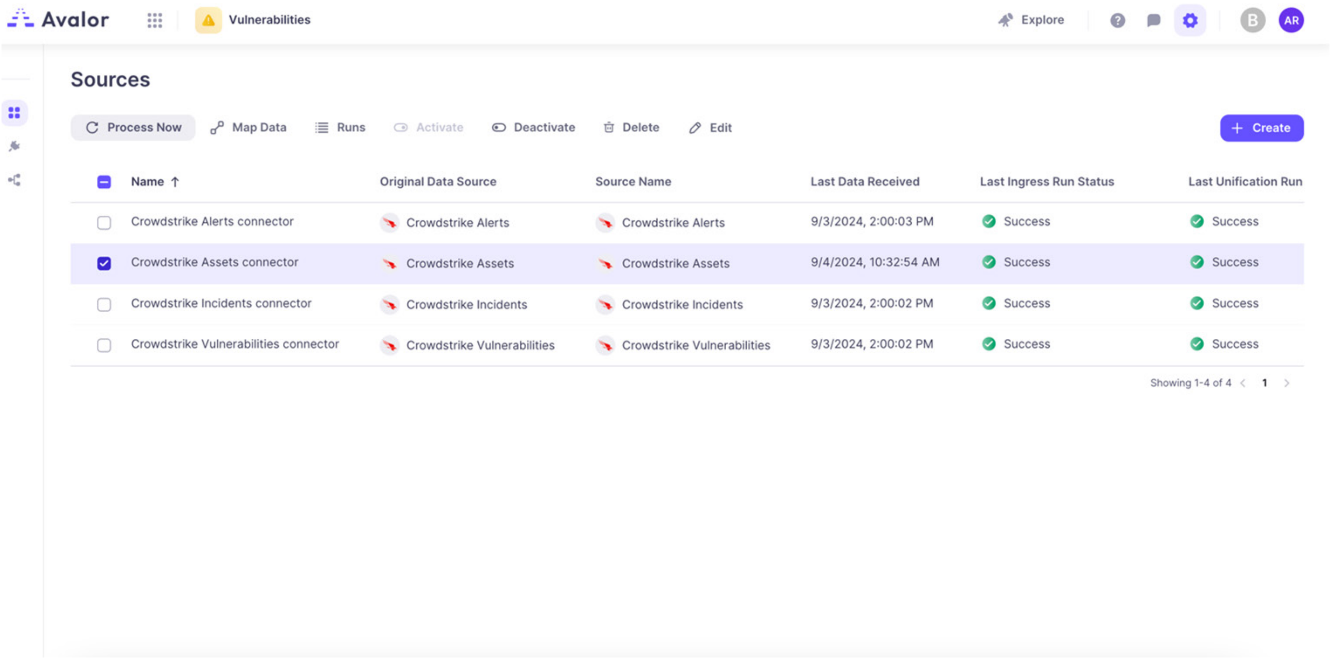


True

tags	Tags
os_version	Operating System
last_seen	Last Seen
service_provider_account_id	Cloud Metadata Account ID
instance_id	Cloud Metadata Instance ID
mac_address	MAC Address
def evaluate(row: dict) -> str: dn...	Key
ou	AD Organizational Unit
service_provider	Cloud Metadata Provider
import re def validate_ip(ip_str: ...	External IP Addresses

Figure 126. Has EDR

3. In the **Data Sources** page, select the **CrowdStrike Assets connector** and click **Process Now**.



▬	Name ↑	Original Data Source	Source Name	Last Data Received	Last Ingress Run Status	Last Unification Run
□	Crowdstrike Alerts connector	Crowdstrike Alerts	Crowdstrike Alerts	9/3/2024, 2:00:03 PM	✓ Success	✓ Success
☑	Crowdstrike Assets connector	Crowdstrike Assets	Crowdstrike Assets	9/4/2024, 10:32:54 AM	✓ Success	✓ Success
□	Crowdstrike Incidents connector	Crowdstrike Incidents	Crowdstrike Incidents	9/3/2024, 2:00:02 PM	✓ Success	✓ Success
□	Crowdstrike Vulnerabilities connector	Crowdstrike Vulnerabilities	Crowdstrike Vulnerabilities	9/3/2024, 2:00:02 PM	✓ Success	✓ Success

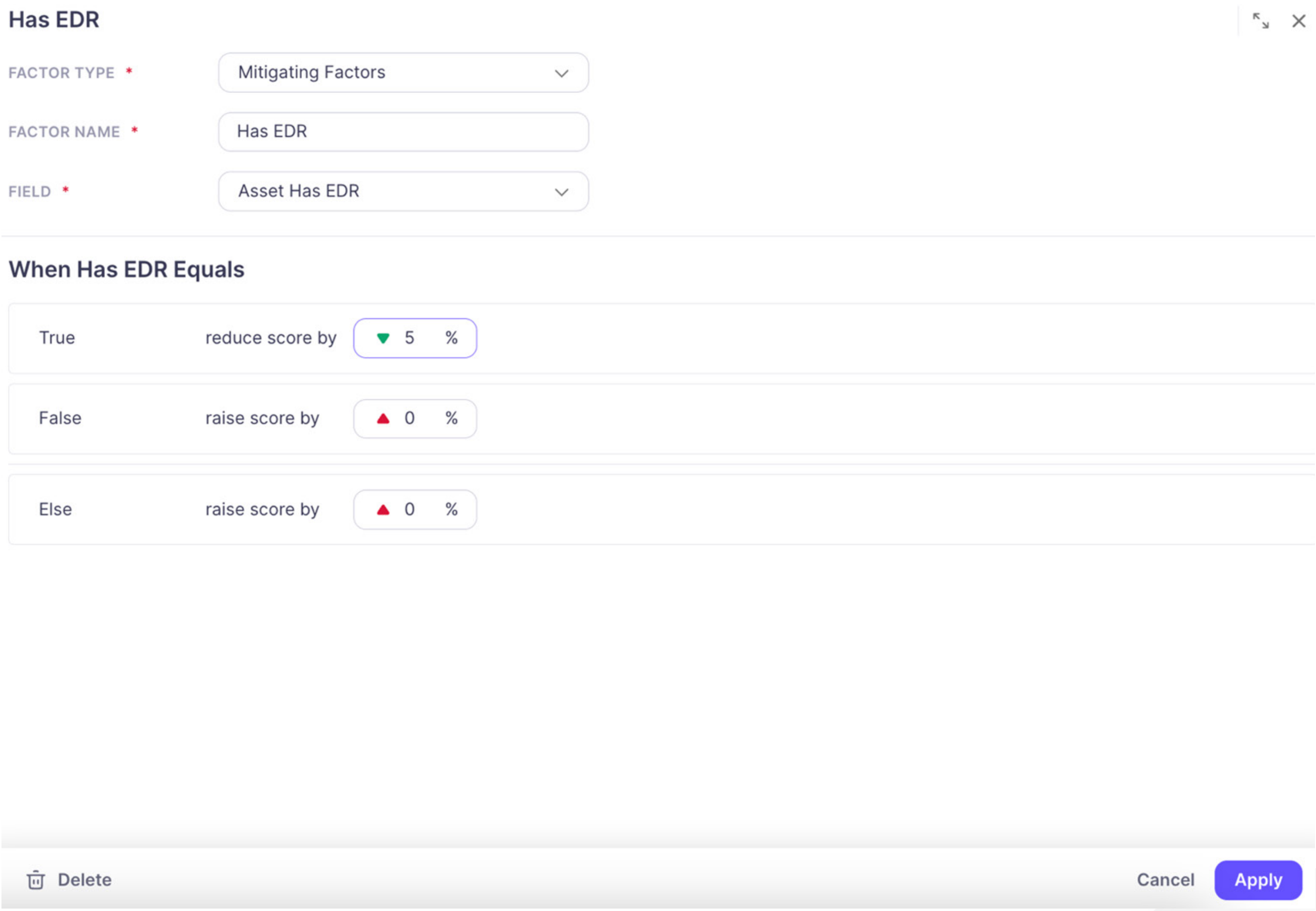
Figure 127. Process Now

Step 8: Review and Adjust Risk Scoring

After ingested data has been normalized and mapped to the Data Model, Avalor UVM evaluates the risk.

The following example shows how the Has EDR entity is added as a mitigating factor for risk scoring. A value of True reduces the risk calculation (since the asset has mitigating software installed). A value of False increases the risk calculation (since the asset has a higher vulnerability without EDR).

1. From the **Vulnerabilities** tab in the **Avalor** dashboard (Remediation Hub):
   a. In the left-side pane, select **Settings** > **Score**.
   b. Click **Add Factor** in the **Risk & Mitigating Factors** section.
2. In the **Add new factor modal**:
   a. Choose **Mitigating Factors** for **Factor Type** (Mitigating Factors generally lowers the risk scoring, while Risk Factors generally increase the risk scoring).
   b. Enter a **Factor Name**.
   c. Choose **Asset Has EDR** for **Field**.
   d. In the **When Has EDR Equals** section, under **True**, enter a percentage by which the risk is reduced.
   e. Click **Apply**.



Has EDR

FACTOR TYPE * Mitigating Factors

FACTOR NAME * Has EDR

FIELD * Asset Has EDR

When Has EDR Equals

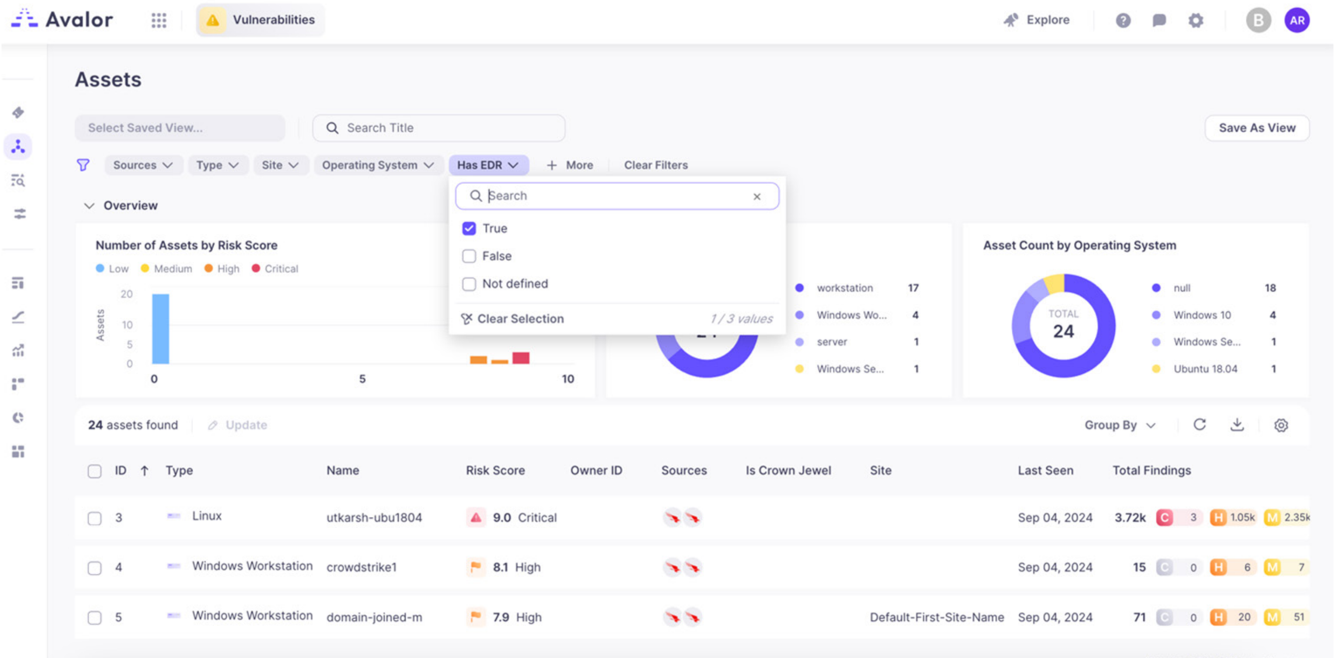
True reduce score by ▼ 5 %

False raise score by ▲ 0 %

Else raise score by ▲ 0 %

Figure 128. Adjusting Risk Scoring

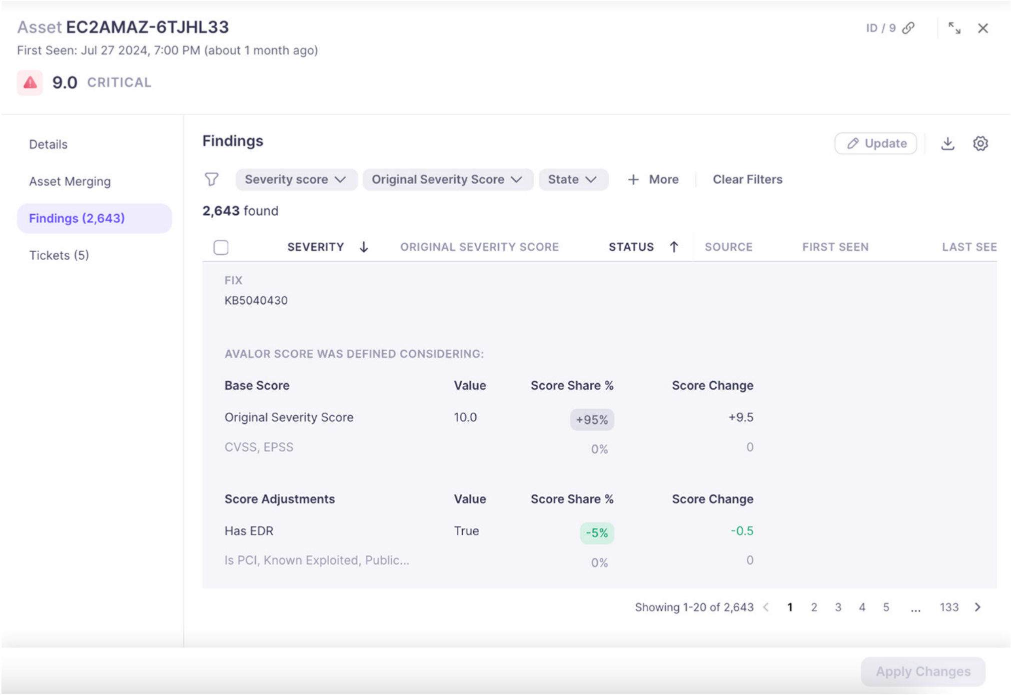
3. In the left-side pane, select the **Assets** dashboard. From the **Assets** dashboard:
   a. Set a filter by clicking **More** and selecting the **Has EDR** entity.



ID	Type	Name	Risk Score	Owner ID	Sources	Is Crown Jewel	Site	Last Seen	Total Findings
3	Linux	utkarsh-ubu1804	9.0 Critical					Sep 04, 2024	3.72k C 3 H 1.05k M 2.35k
4	Windows Workstation	crowdstrike1	8.1 High					Sep 04, 2024	15 C 0 H 6 M 7
5	Windows Workstation	domain-joined-m	7.9 High				Default-First-Site-Name	Sep 04, 2024	71 C 0 H 20 M 51

Figure 129. Filtered Assets

   b. Click one of your **Assets** in the filtered list.
   c. In the **Asset** modal that appears, click the **Findings** tab.
   d. Click one of the **Findings**.
   e. Review the output (notice the **Score Adjustments** section and whether **Has EDR** has modified the risk scoring).



FIX
KB5040430

AVALOR SCORE WAS DEFINED CONSIDERING:

Base Score	Value	Score Share %	Score Change
Original Severity Score	10.0	+95%	+9.5
CVSS, EPSS		0%	0

Score Adjustments	Value	Score Share %	Score Change
Has EDR	True	-5%	-0.5
Is PCI, Known Exploited, Public...		0%	0

Figure 130. Risk Scoring

Appendix A: Requesting Zscaler Support

If you need Zscaler Support for provisioning certain services, or troubleshooting configuration and service issues, it is available 24/7/365.

1. To contact Zscaler Support, go to **Administration** > **Settings** > **Company Profile**.

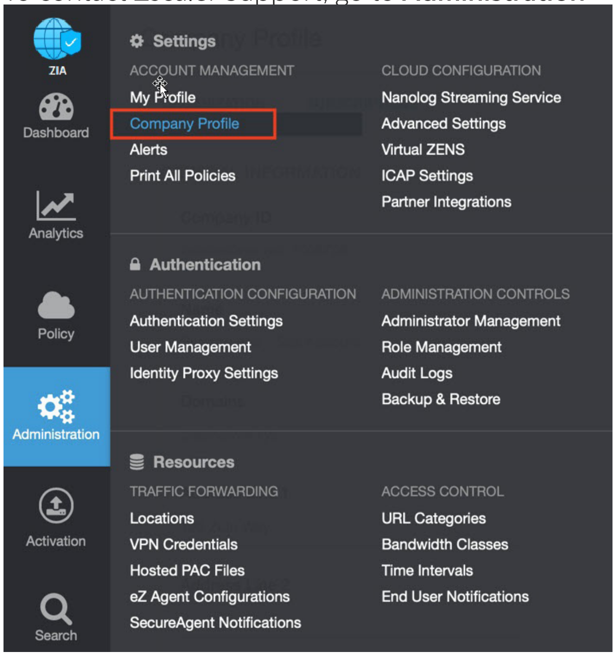
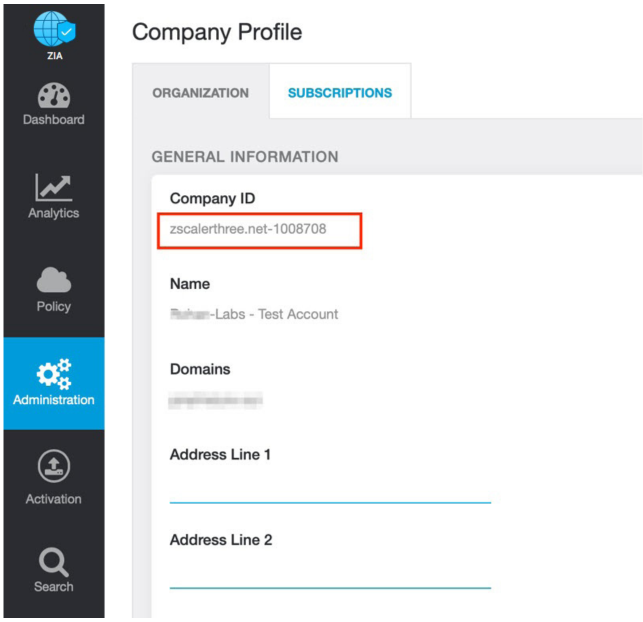


Figure 131. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 132. Company ID

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

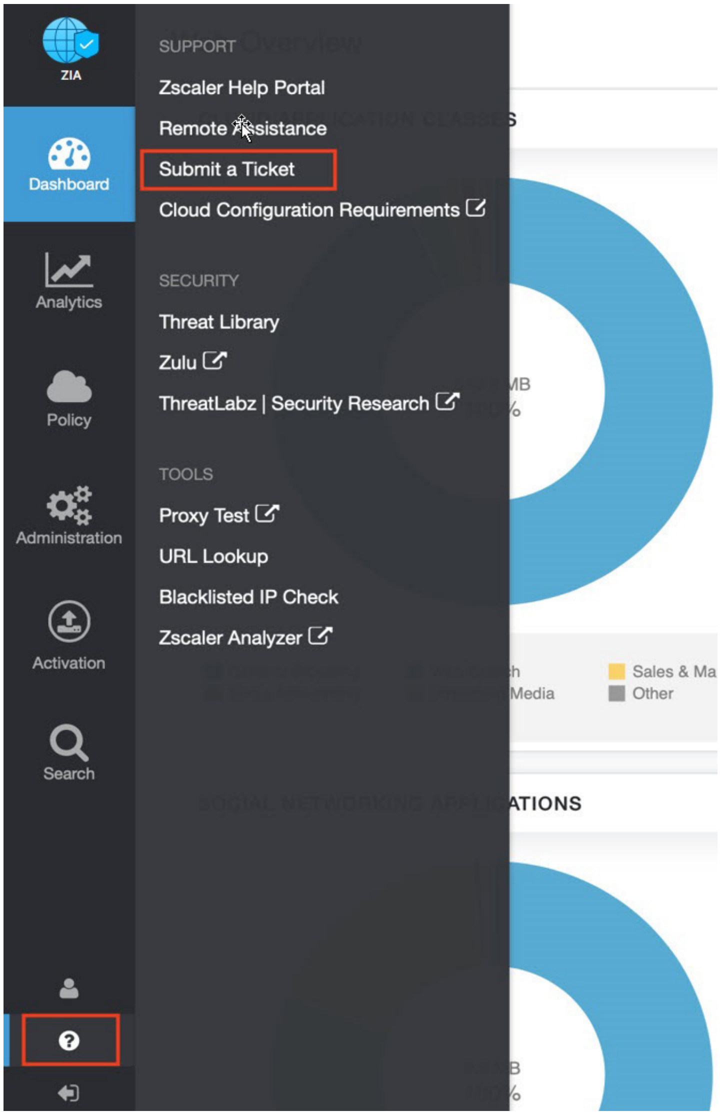


Figure 133. Submit a ticket