



ATTACKIQ

ZSCALER AND ATTACKIQ DEPLOYMENT GUIDE

Contents

Terms and Acronyms	5
About This Document	6
Zscaler Overview	6
AttackIQ Overview	6
Audience	6
Software Versions	6
Request for Comments	6
Zscaler and AttackIQ Introduction	7
ZIA Overview	7
AttackIQ Platform Overview	8
AttackIQ Resources	8
What is the Goal of this Assessment Template?	9
Why is this Relevant to Me?	9
What Security Control Policy or Configuration is Tested?	9
Malware Protection	9
Advanced Threat Protection	10
Sandbox	11
URL Filtering	11
File Type Control	12
SSL Inspection	12
IPS	13
What Results Should I Expect?	14
Tests in the Assessment Template	14
Malware Protection	14
Advanced Threat Protection	14

Sandbox	14
URL Filtering	14
File Type Control	14
Required Configuration	15
Architecture Overview	15
General Checklist	15
Zscaler ZIA	16
Select Tunnel 2.0 Protocol for Zscaler Client Connector	16
Ensure the Appropriate Zscaler ZIA Policy is Applied to the Asset	16
Configure NSS Service to Send Web Log Type to the SIEM	16
Ensure the AttackIQ Agent Allowlisting Configuration Applied	17
Configure the SIEM to Receive and Parse the Fields Accordingly	18
Ensure the AttackIQ Agent is Appropriately Configured	18
OS Considerations	18
AttackIQ Integration	19
Ensure the Integration Manager Plugin is Appropriately Configured	19
Set IOC Field Mappings	19
Set Property Mappings	20
AttackIQ Assessment	20
Scheduling Considerations	21
Expected Results	22
AttackIQ Platform	22
ZIA	22
Troubleshooting	23
Assets Not Active in the AttackIQ Platform	23
Integration Manager Not Active	24
SIEM Integration Not Active	25

Zscaler ZIA is Not Preventing or Detecting All Scenarios	25
Use Mitigations to Ensure You are Well Protected	25
Use IOCs/Observables for Troubleshooting	26
Appendix A: Requesting Zscaler Support	27
Save Company ID	27
Enter Support Section	28

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: [ZS](#)) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services 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 [Zscaler's website](#) or follow Zscaler on Twitter @zscaler.

AttackIQ Overview

AttackIQ is the industry leading provider of breach and attack simulation products for security control validation. AttackIQ emulates adversary tactics, techniques, and procedures, aligned to the MITRE ATT&CK framework, and provides visibility into your security program performance with clear data-driven analysis and mitigation guidance. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. A proud member of the Microsoft Intelligent Security Association (MISA), the Company is committed to giving back to the cybersecurity community through its free award-winning AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat-Informed Defense. For more information, refer to [AttackIQ'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, see:

- [Appendix A: Requesting Zscaler Support](#)
- [Zscaler Resources](#)
- [AttackIQ Resources](#)

Software Versions

This document was authored using the latest version of Zscaler software.

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 AttackIQ Introduction

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

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:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding 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 Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

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.
ZPC Help Portal	Help articles for ZPC.
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.

AttackIQ Platform Overview

AttackIQ emulates adversary tactics, techniques, and procedures, aligned to the MITRE ATT&CK framework, and provides visibility into your security program performance with clear data-driven analysis and mitigation guidance. AttackIQ products are built on the company's core emulation platform, which tests adversary tactics, techniques, and procedures with realistic attack scenarios and real-time performance metrics and recommendations:

- AttackIQ Flex: An on-demand, agentless test as a service. It enables organizations to quickly emulate adversary behavior through a simplified user experience, delivering detailed security control performance metrics and mitigations in minutes.
- AttackIQ Ready!: A fully managed breach and attack simulation as a service (BaSaaS), leveraging the core AttackIQ platform. It provides weekly and monthly validation with reporting, remediation guidance, cyberinsurance reporting, and curated access to AttackIQ Adversary Research Team products. It assesses the effectiveness of seven key security controls within the framework of MITRE ATT&CK, providing comprehensive performance data.
- AttackIQ Enterprise: Continuous readiness testing, combining the power of AttackIQ's breach and attack simulation platform with the benefits of a co-managed service. It provides flexibility and customization, allowing customers to leverage AttackIQ's expertise while tailoring the software to their specific needs. A trainer, coach, and FitBit combined into one, AttackIQ puts customers through tests, coaches them to enhance security program performance, and provides continuous data for measurement.

AttackIQ Resources

The following table contains links to AttackIQ support resources.

Name	Definition
AttackIQ Support	Support site for AttackIQ customers.
AttackIQ Community	AttackIQ online community resources.
AttackIQ Knowledge Base	Online articles, documentation, and glossaries for AttackIQ products.

What is the Goal of this Assessment Template?

The Zscaler ZIA Recommended Policies Health Check template was created to provide a basic function check of a ZIA deployment for Windows assets protected by the Zscaler Client Connector and the Zscaler recommended policies exercising the ability to both detect and block adversarial behaviors. This document provides a guide and some troubleshooting examples to ensure the assessment template runs as intended.

Why is this Relevant to Me?

This assessment has been created to help:

- Validate that the selected assets are protected by Zscaler ZIA.
- Validate that the Zscaler ZIA is generating events.
- Validate your detection and response workflow by triggering events in Zscaler ZIA.
- Have an out-of-the-box list of AttackIQ scenarios that are detected or prevented by Zscaler ZIA.
- Test the security measures in assets protected by Zscaler ZIA with the recommended policy.

The assessment does not verify that the applied policy settings to the traffic between the assets is the recommended one. The same results could be obtained with other configurations that are similar or more restricted in terms of security.

What Security Control Policy or Configuration is Tested?

AttackIQ created this assessment template to exercise the recommended security policies provided by Zscaler. See details of the policies in the following pages.

Malware Protection

From the **ZIA Admin Portal**, go to **Policy > Malware Protection > Recommended Policy**.

View Recommended Malware Protection Policy [X]

Configure Malware Protection Policy
Malware Protection Policy protects your traffic against Malware and Adware/Spyware.

TRAFFIC INSPECTION

Inspect Inbound Traffic: ☒ Allow ☐ Block

Inspect Outbound Traffic: ☒ Allow ☐ Block

PROTOCOL INSPECTION

Inspect HTTP: ☒ Allow ☐ Block

Inspect FTP over HTTP: ☒ Allow ☐ Block

Inspect FTP: ☒ Allow ☐ Block

MALWARE PROTECTION

Viruses: ☐ Allow ☒ Block

Unwanted Applications: ☐ Allow ☒ Block

Trojans: ☐ Allow ☒ Block

Worms: ☐ Allow ☒ Block

Ransomware: ☐ Allow ☒ Block

ADWARE/SPYWARE PROTECTION

Adware: ☐ Allow ☒ Block

Spyware: ☐ Allow ☒ Block

Figure 1. Recommended Malware Protection Policy

Advanced Threat Protection

From the **ZIA Admin Portal**, go to **Policy > Advanced Threat Protection > Recommended Policy**.

View Recommended Advanced Threat Protection Policy

Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.

SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)

35

Low Risk | Moderate Risk | High Risk

BOTNET PROTECTION

Command & Control Servers

Command & Control Traffic

MALICIOUS ACTIVE CONTENT PROTECTION

Malicious Content & Sites

Vulnerable ActiveX Controls

Browser Exploits

File Format Vulnerabilities

FRAUD PROTECTION

Known Phishing Sites

Suspected Phishing Sites

Spyware Callback

Web Spam

Crypto Mining

Known Adware & Spyware Sites

UNAUTHORIZED COMMUNICATION PROTECTION

IRC Tunneling

SSH Tunneling

Anonymizers

CROSS-SITE SCRIPTING (XSS) PROTECTION

Cookie Stealing

Potentially Malicious Requests

P2P FILE SHARING PROTECTION

BitTorrent

P2P ANONYMIZER PROTECTION

Tor

P2P VOIP PROTECTION

Google Talk

Figure 2. Recommended Advanced Threat Protection Policy

Sandbox

From the **ZIA Admin Portal**, go to **Policy > Sandbox > Recommended Policy**.

View Recommended Sandbox Policy [X]

Configure Sandbox Policy
Sandbox supports the scanning and execution of files.

SANDBOX RULE

Rule Order: 1 Rule Status: Enabled

CRITERIA

File Types: Select all file types for sandboxing	URL Categories: Any
Users: Any	Groups: Any
Departments: Any	Locations: Any
Location Groups: Any	Sandbox Categories: Any
Protocols: Any	

ACTION

First Time Action: Allow and scan Machine Learning Intelligent Action: ☐ [X]

Action for Subsequent Downloads: Block

Figure 3. Recommended Sandbox Policy

URL Filtering

From the **ZIA Admin Portal**, go to **Policy > URL & Cloud App Control > URL Filtering Policy > Recommended Policy**.

View Recommended URL & Cloud App Control Policy [X]

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 allow all.

URL FILTERING RULE

Rule Order: Select order depending on your business needs and corporate policy. Rule Status: Enabled

CRITERIA

Cloud Applications: Any	Cloud Application Instances: None
Cloud Application Risk Profile: Any	URL Categories: Adult Material, Drugs, Gambling, Illegal or Questionable, Militancy/Hate and Extremism
HTTP Requests: All	Users: Any
Groups: Any	Departments: Any
Locations: Any	Location Groups: Any
Time: Always	Protocols: HTTP, HTTPS
Device Groups: OS Type, No Client Connector, Cloud Browser Isolation	Device Trust Level: Trust levels based on posture definition

ACTION

Web Traffic: Block

CLOUD APP CONTROL POLICY

You can allow sites, depending on your business needs and corporate policy.

ADVANCED URL FILTERING OPTIONS

Enable AI/ML based Content Categorization: <input checked="" type="checkbox"/>	Enable Embedded Sites Categorization: <input type="checkbox"/> [X]
Enforce SafeSearch: <input checked="" type="checkbox"/>	Enable Suspicious New Domains Lookup: <input checked="" type="checkbox"/>

Figure 4. Recommended URL & Cloud App Control Policy

File Type Control

From the **ZIA Admin Portal**, go to **Policy > File Type Control > Recommended Policy**.

View Recommended File Type Control Policy [X]

Configure File Type Control Policy
Rules are evaluated in the order specified. Rule evaluation stops at first match.

FILE TYPE CONTROL RULE

Rule Order: 1 Rule Status: Enabled

CRITERIA

File Types: Executable	URL Categories: Any
Users: Any	Groups: Any
Departments: Any	Locations: Any
Location Groups: Any	Time: Always
Protocols: Any	

ACTION

Action: Caution Upload/Download: Download

FILE TYPE CONTROL RULE

Rule Order: 2 Rule Status: Enabled

CRITERIA

File Types: Select all file types	URL Categories: Any
Users: Any	Groups: Any
Departments: Any	Locations: Any
Time: Always	Protocols: Any

ACTION

Action: Allow Upload/Download: Download

Figure 5. Recommended File Type Control Policy

SSL Inspection

From the **ZIA Admin Portal**, go to **Policy > SSL Inspection > Recommended Policy**.

View Recommended SSL Inspection Policy [X]

Configure SSL Inspection Policy
Rules are evaluated in the order specified. Rule evaluation stops at the first match.

- Start by enabling SSL inspection for 'risky' URL categories only, such as Security Risk and Legal Liability categories such as Adult Content, Gambling, and Unknown/Miscellaneous. Include all other categories in the list of URL categories for which SSL transactions will not be decrypted. Then, when your organization is ready, **enable SSL inspection for all URL categories except Finance and Health** to allay privacy concerns within the organization.

Figure 6. Recommended SSL Inspection Policy

IPS

From the **ZIA Admin Portal**, go to **Policy > Firewall Filtering > IPS Control**.

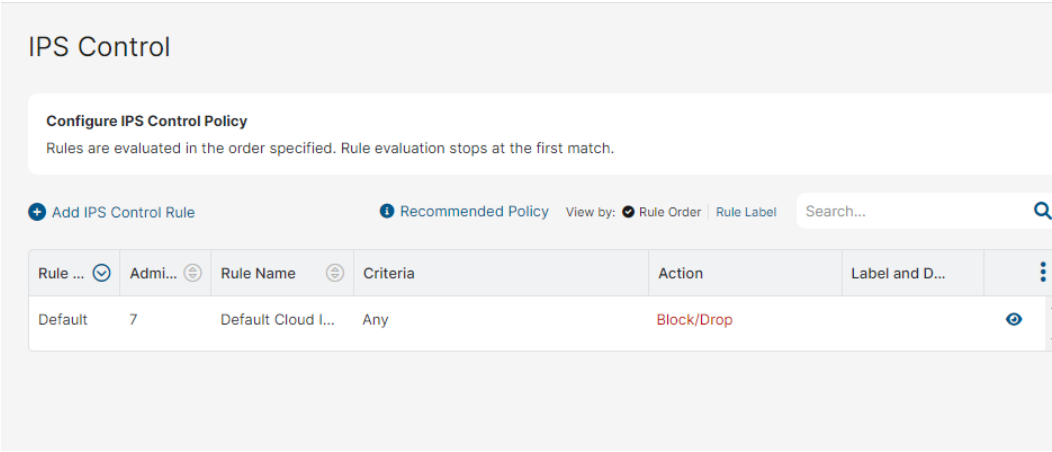


Figure 7. IPS Control

What Results Should I Expect?

When running the assessment on Zscaler Client Connector protected assets with the recommended policies, it is expected that all tests are successfully prevented or detected.

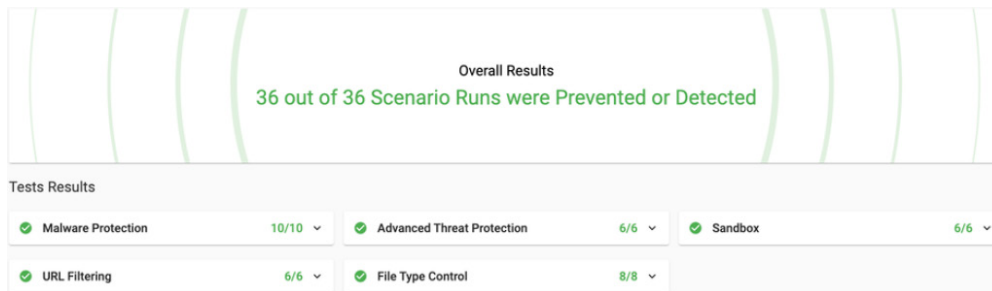


Figure 8. Overall results

The results page also shows information on the outcome for each of the tests by combining information on the prevention outcome and the scenario detection outcome. In other words, you can be protected because the scenario attack is either prevented, detected, or both at the same time. Otherwise, you are not protected.

Tests in the Assessment Template

The Zscaler ZIA Recommended Policies Health Check has five tests that evaluate different Zscaler ZIA capabilities.

Malware Protection

Ten scenarios simulate the download of different malicious samples.

Advanced Threat Protection

Six scenarios replicate the web traffic communication sent by different malware to communicate with their respective C2 server, together with extra malicious download attempts.

Sandbox

Six scenarios simulate the download of different malicious samples that are vetted by Zscaler ZIA sandbox service.

URL Filtering

Six scenarios simulate the connection to different web categories including Porn, Hacking, Mature Humor, Anonymizer, Gambling, and Extremism.

File Type Control

Eight scenarios that simulate the download of different types of clean files including .vbs, .bat, .ps1, .bash, .dll, .cmd, .scr, and .reg.

Tests (5)	Scenarios
Malware Protection	10 ▾
Advanced Threat Protection	6 ▾
Sandbox	6 ▾
URL Filtering	6 ▾
File Type Control	8 ▾

Figure 9. Assessment tests

Required Configuration

The following are required configurations for the Zscaler and AttackIQ integration.

Architecture Overview

- Zscaler Client Connector is installed at endpoint level and set to forward logs to Zscaler.
- Logs from Zscaler are sent to your SIEM solution.
- AttackIQ's Integration Manager consumes logs from your SIEM to correlate attack emulations on the endpoint.

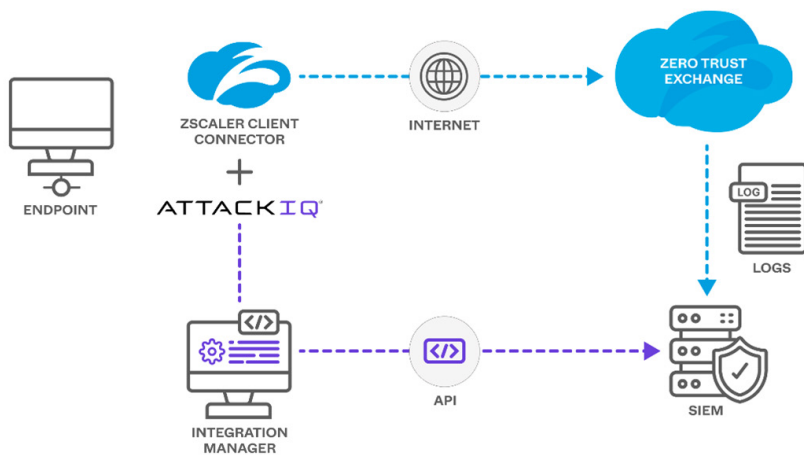


Figure 10. Architecture Overview

General Checklist

1. Install Zscaler Client Connector agent as the traffic forwarding method.
2. Select Tunnel 2.0 protocol for Zscaler Client Connector.
3. Ensure the appropriate Zscaler ZIA policy is applied to the asset.
4. Configure NSS service to send Web Log type to the SIEM.
5. Validate the minimum required fields are being sent under Web Log feed.
6. Ensure the AttackIQ agent allowlisting configuration is applied.
7. Configure the SIEM to receive and parse the fields accordingly.
8. Ensure the AttackIQ agent is appropriately configured.
9. Ensure the Integration Manager plugin is appropriately configured.

Zscaler ZIA

The following sections describe how to configure ZIA for the AttackIQ integration.

Install Zscaler Client Connector Agent as the Traffic Forwarding Method

To learn more, see:

- [Best Practices for Deploying Z-Tunnel 2.0](#)
- [Configuring Zscaler Client Connector Profiles](#)

A selection of any other traffic forwarding method does not guarantee the same results as stated in this document.

To learn more details about other traffic forwarding methods, see [Choosing Traffic Forwarding Methods](#).

Select Tunnel 2.0 Protocol for Zscaler Client Connector

This guarantees the asset can benefit from all Zscaler ZIA security protections.

In case this protocol is not enabled in the tenant, create a support ticket to Zscaler and request to enable Tunnel 2.0 protocol. After, select it accordingly.

Ensure the Appropriate Zscaler ZIA Policy is Applied to the Asset

Depending on the internal set up, review that Locations, Users, Groups, Departments, Devices and Device Groups were properly configured to allow the asset inherit the policies. You should review the following:

- Zscaler **ZIA Admin Portal** > **Policy** > **File Type Control**
- Zscaler **ZIA Admin Portal** > **Policy** > **URL Filtering**
- Zscaler **ZIA Admin Portal** > **Policy** > **SSL Inspection**
- Zscaler **ZIA Admin Portal** > **Policy** > **IPS Control**
- Zscaler **ZIA Admin Portal** > **Policy** > **Mobile** > **Zscaler Client Connector Portal** > **App Profiles** > **Windows Policy**

Configure NSS Service to Send Web Log Type to the SIEM

To learn more, see:

- [About NSS Servers](#)
- [Adding NSS Feeds for Web Logs](#)

Validate the minimum required fields are sent under NSS Web feed output format.

1. Must have: `fieldsclientip=%s{cip}, devicehostname=%s{devicehostname}, clientsrcport=%d{clt_sport}, url=%s{eurl}, filehashmd5=%s{bamd5}, filehash256=%s{sha256}, filename=%s{filename}, uploadfilename=%s{upload_filename}`
2. Nice to have: `fieldsreason=%s{reason}, ruletype=%s{ruletype}`

To learn more, see [NSS Feed Output Format: Web Logs](#).

Ensure the AttackIQ Agent Allowlisting Configuration Applied

To apply an allowlist configuration:

1. Select the list of sites to allowlist from the [support portal article on Allowlisting](#).
2. Add URLs to Allowlist for Security Scans. To learn more, see [Adding URLs to the Allowlist](#).

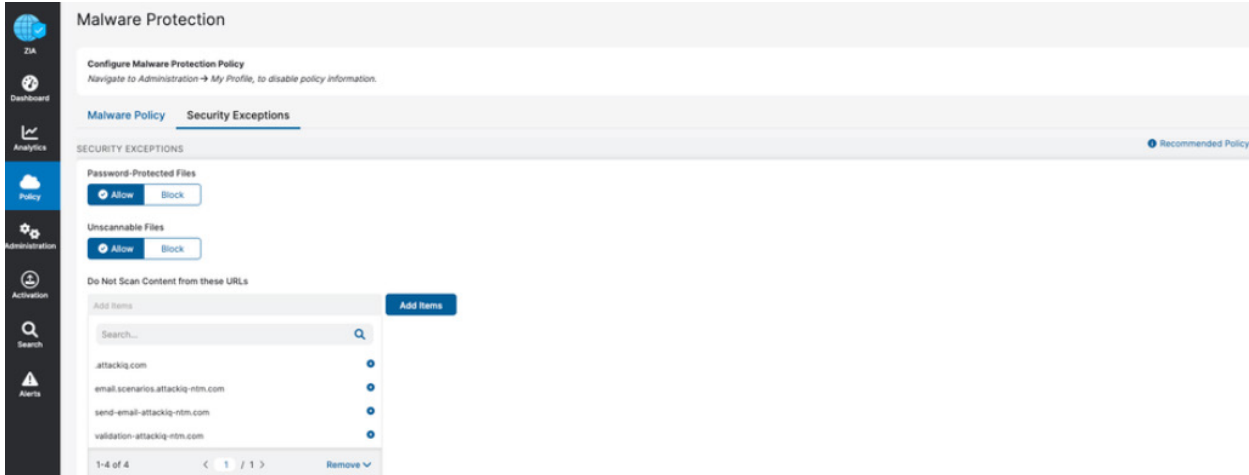


Figure 11. Malware Protection

3. Add URLs to Allowlist for URL Filtering. To learn more, see [Adding URLs to the Allowlist](#).

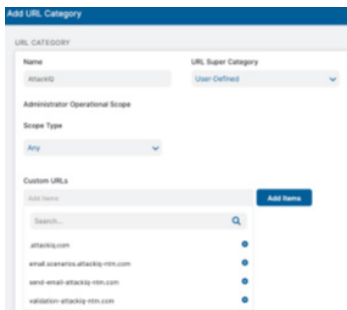


Figure 12. Add URL Category

The following is the URL Filtering Policy window.

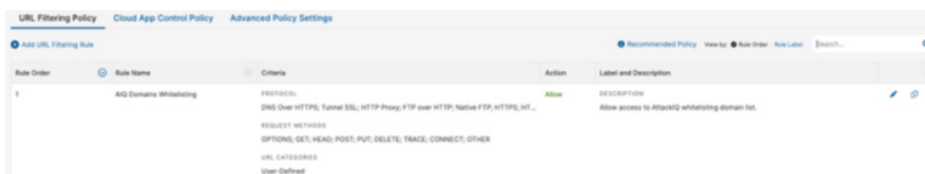


Figure 13. URL Filtering Policy



Do not use an asterisk (“*”) as a wildcard character at the beginning of a domain. For example, .attackiq.com is permitted, while *http://attackiq.com is not permitted. To learn more, see [URL Format Guidelines](#).

Configure the SIEM to Receive and Parse the Fields Accordingly

Depending on the type of NSS deployed (on-premises or cloud), select the guide that applies to the selected SIEM:

- For NSS on-premises, see [Integrating VM-Based NSS with SIEMs](#).
- For NSS cloud, see [Integrating Cloud NSS with Cloud-Based SIEMs](#).

Ensure the AttackIQ Agent is Appropriately Configured

To execute the assessment template and validate the Zscaler ZIA configuration, at least one asset protected by Zscaler ZIA is required.

You must meet the following requirements:

- All the assets selected have the AttackIQ Agent installed with the latest version and appear active in the AttackIQ Platform: **AttackIQ Platform > Assets > Assets Status**.
- All the assets selected have been configured as explained in the previous sections of this document.

OS Considerations

The assessment was created to run on assets with Windows 10.

AttackIQ confirms an overall combined outcome of 100 percent in this assessment for assets with the latest version of Windows 10.

AttackIQ Integration

Ensure the Integration Manager server is appropriately configured.

For more information on configuring the Integration Manager, refer to:

- [Integration Manager](#)
- [Non OVA Integration Manager](#)

Ensure the Integration Manager Plugin is Appropriately Configured

For detailed information on how to configure SIEM integrations, refer to the [SIEM/Log Aggregation documentation](#).

It is necessary to configure the integration following the guide and to ensure it appears Active in the AttackIQ Platform.

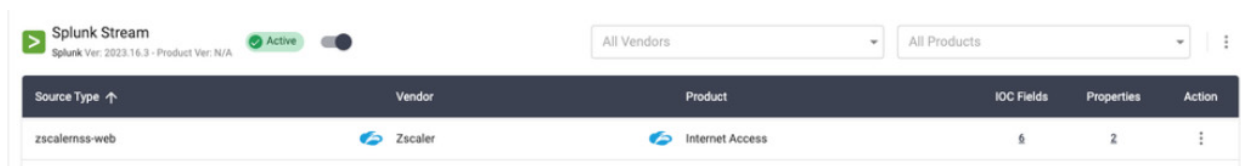


Figure 14. Splunk Stream

The following sections contain tips when configuring the SIEM integration to obtain the best results and information.

Set IOC Field Mappings

The Field name might change depending on the SIEM selected and/or if the default fields names were changed by Zscaler/SIEM administrator. These are the Zscaler official names that are set at NSS Feed. To learn more, see [NSS Feed Output Format: Web Logs](#).

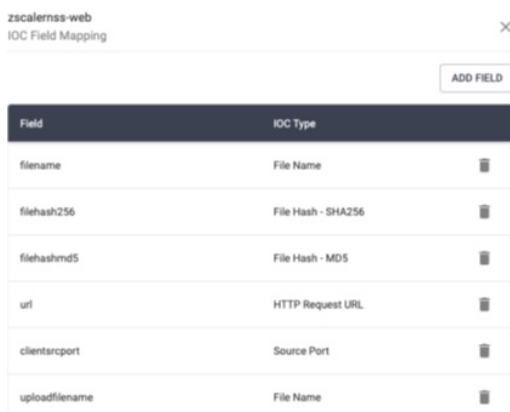


Figure 15. IOC Field Mappings

Zscaler Name	Field Description
%s{filename}	The name of downloaded files during the transaction.
%s{bamd5}	The MD5 hash of the malware file that was detected in the transaction or the md5 of the file that was sent for analysis to the Sandbox engine.
%s{sha256}	The SHA-256 hash of the malware file that was detected in the transaction or the sha256 of the file that was sent for analysis to the Sandbox engine.
%s{eurl}	URL
%d{clt_srcport}	The client source port.
%s{upload_filename}	The name of uploaded files during the transaction.

Set Property Mappings

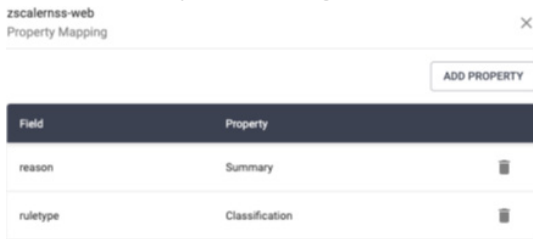


Figure 16. Property Mappings

Zscaler Name	Field Description
%s{reason}	Action that the service took and the policy that was applied, if the transaction was blocked.
%s{ruletype}	Policy type. Applies only to Block rules, not Allow.

AttackIQ Assessment

To create a new assessment using the Zscaler ZIA template:

1. Go to the **Assessments** page.
2. Click **Create New Assessment**.
3. Select **Choose Template**.
4. Search for **Zscaler ZIA Recommended Policies Health Check**.
5. Select the **Assessment**.
6. After you've created the assessment, click the **Selected Assets** icon and add as many Zscaler ZIA-protected assets as desired.

Zscaler ZIA Recommended Policies Health Check

Description

Test how you are doing against Zscaler ZIA recommended security policies. This template will allow you to exercise the following ones: Malware Protection, Advanced Threat Protection, Sandbox, URL Filtering, File Type Control and analyze if you are successfully protected.

Documentation: <https://support.attackiq.com/articles/zscaler-zia-health-check/>

Tests (5)	Scenarios
Malware Protection	10 ▼
Advanced Threat Protection	6 ▼
Sandbox	6 ▼
URL Filtering	6 ▼
File Type Control	8 ▼

Figure 17. Recommended Policies Health Check

7. After everything has been configured, execute the assessment.

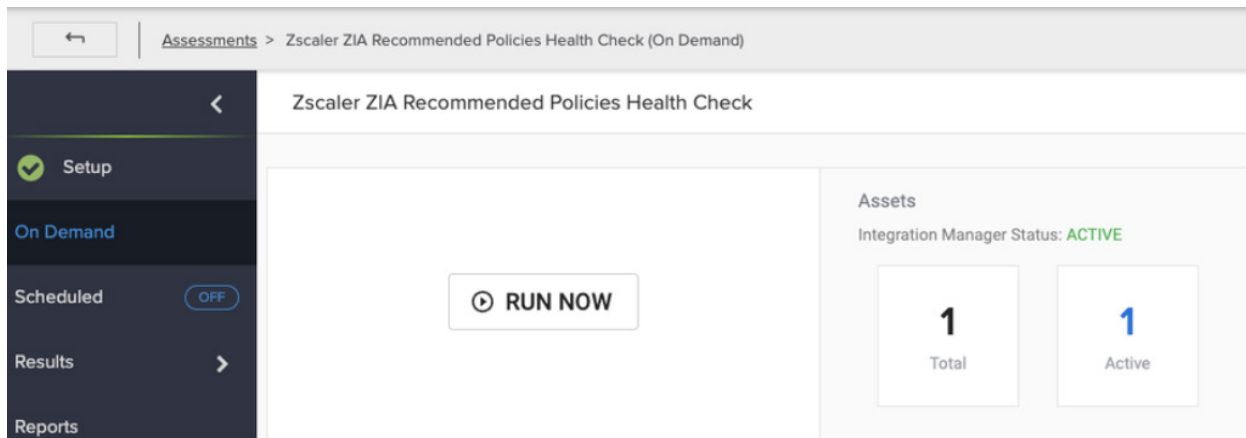


Figure 18. Assessment

Scheduling Considerations

No specific consideration must be taken when scheduling the assessment with the Zscaler ZIA Recommended Policies Health Check template, as Zscaler is not suppressing alerts.

Expected Results

The following sections describe the expected integration results.

AttackIQ Platform

When running the assessment on assets protected by Zscaler ZIA with the recommended security policies, you can expect to have a green box stating that all tests were successfully prevented or detected.

AttackIQ is constantly monitoring security product vendors' deviations in prevention and detection engines. It might be the case that, for a period of time, detection and prevention results do not add up to 100 percent. If you see small deviations in the expected results, it might mean that the engines of the security products changed their logic. AttackIQ is constantly monitoring these changes and updating the assessments appropriately. However, if the deviation in the results is considerable, this is, most likely, an indication that a less restrictive security product policy has been configured.

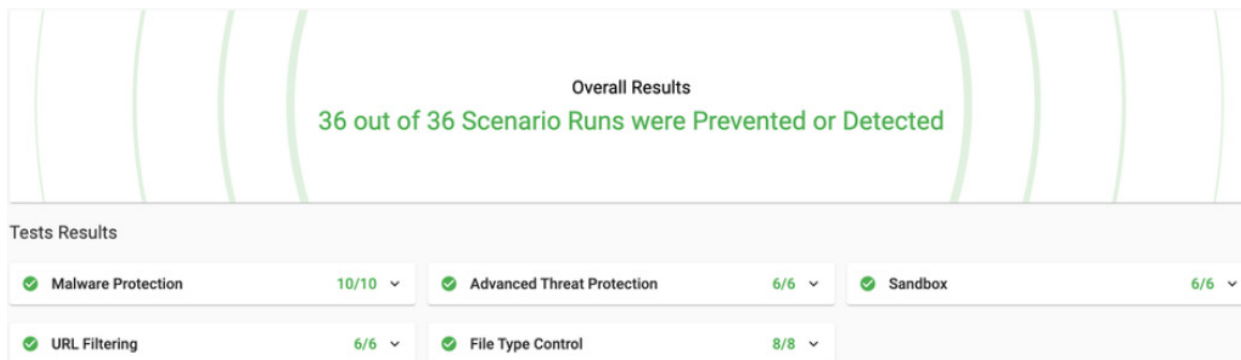


Figure 19. Overall Results

Also, when checking the scenario results, all the scenarios show their corresponding detection.

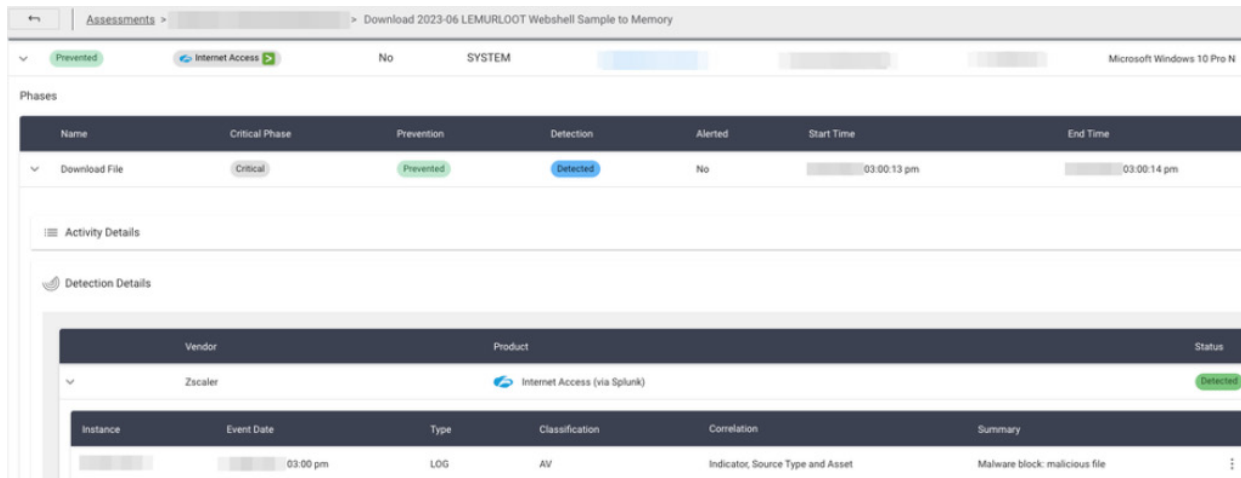


Figure 20. Corresponding Detection

ZIA

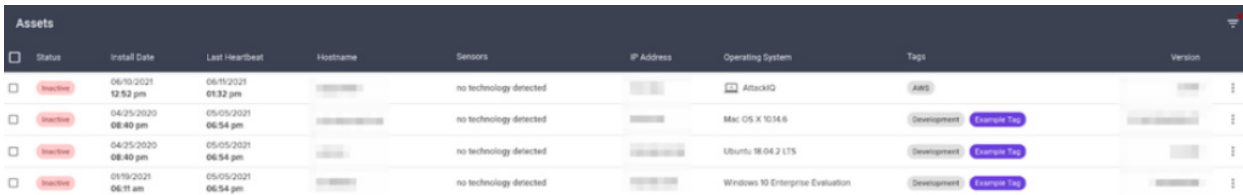
After executing the assessment, the events in the document, Zscaler-HealthCheck-AT-expected-results.xlsx, appear in the Zscaler ZIA Admin Portal.

Troubleshooting

The following describes how to troubleshoot various integration scenarios.

Assets Not Active in the AttackIQ Platform

If the assets that you want to use in the assessment do not have an AttackIQ agent running correctly, they appear as inactive in the AttackIQ Platform.



Status	Install Date	Last HeartBeat	Hostname	Sensors	IP Address	Operating System	Tags	Version
Inactive	06/10/2021 12:52 pm	06/10/2021 01:32 pm	[redacted]	no technology detected	[redacted]	AttackIQ	AWES	[redacted]
Inactive	04/25/2020 08:40 pm	05/05/2021 06:54 pm	[redacted]	no technology detected	[redacted]	Mac OS X 10.14.6	Development Example Top	[redacted]
Inactive	04/25/2020 08:40 pm	05/05/2021 06:54 pm	[redacted]	no technology detected	[redacted]	Ubuntu 18.04.2 LTS	Development Example Top	[redacted]
Inactive	05/19/2021 06:11 am	05/05/2021 06:54 pm	[redacted]	no technology detected	[redacted]	Windows 10 Enterprise Evaluation	Development Example Top	[redacted]

Figure 21. Assets

To ensure that the AttackIQ Agent service is working properly:

- Ensure that the AttackIQ Agent is installed on the asset.
 - If it is not, install the AttackIQ Agent. There are several related guides on the AttackIQ Support Portal, including the [AttackIQ Agent User Guide](#).
- Ensure that the AttackIQ service is running on the asset.
 - If it is not, start the service.

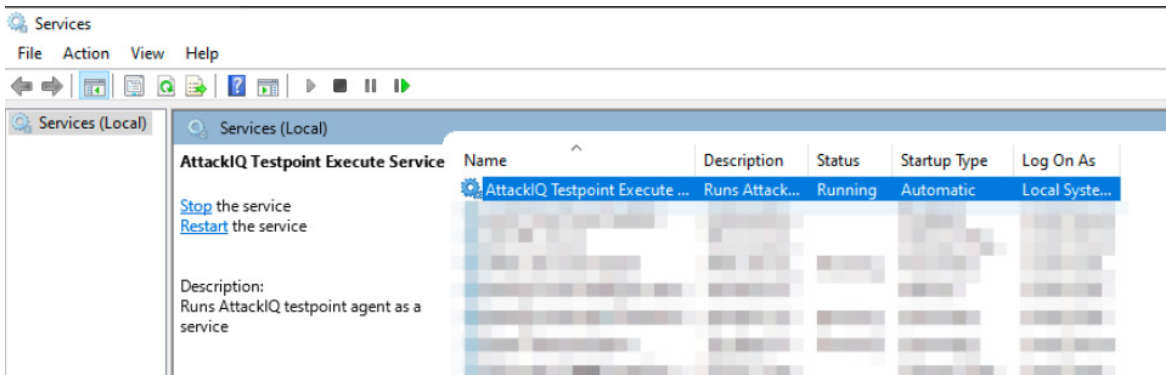


Figure 22. Services

- Ensure that your Endpoint Security Control has not deleted or quarantined the AttackIQ Agent.
 - For more information on the whitelisting recommendation guidelines, refer to the [AttackIQ documentation](#).

Integration Manager Not Active

Check if the Integration Manager is active in **AttackIQ Platform > Technology Stack > Integration Configuration**.

If no Integration Manager has been deployed, use these documents to configure it:

- [Integration Manager](#)
- [Non OVA Integration Manager](#)

If it has been deployed but doesn't appear as active, checking the logs in `/opt/attackiq/plugin/logs/` can give more details on the specific issue that is affecting the Integration Manager.

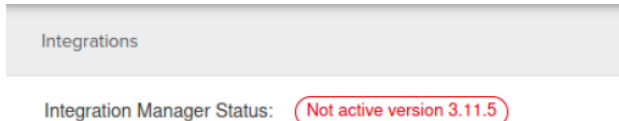


Figure 23. Integrations

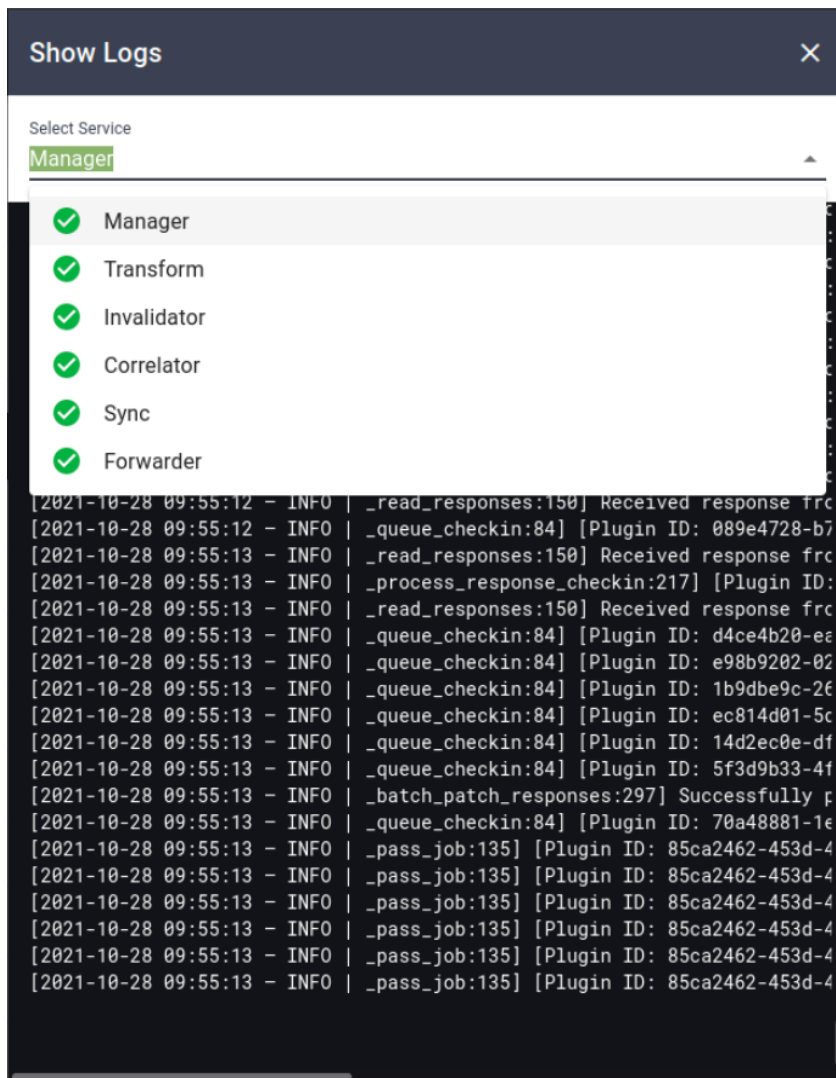


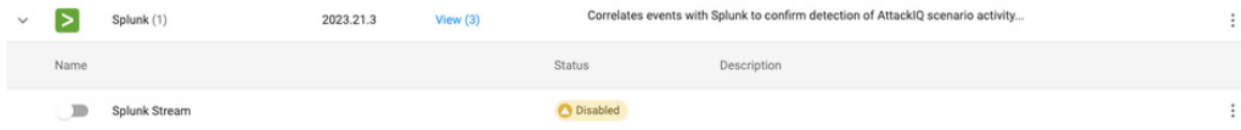
Figure 24. Show Logs

SIEM Integration Not Active

You can check if the SIEM integration is active in AttackIQ Platform > Technology Stack > Integration Configuration.

If the SIEM integration has not been configured, refer to the [AttackIQ documentation](#).

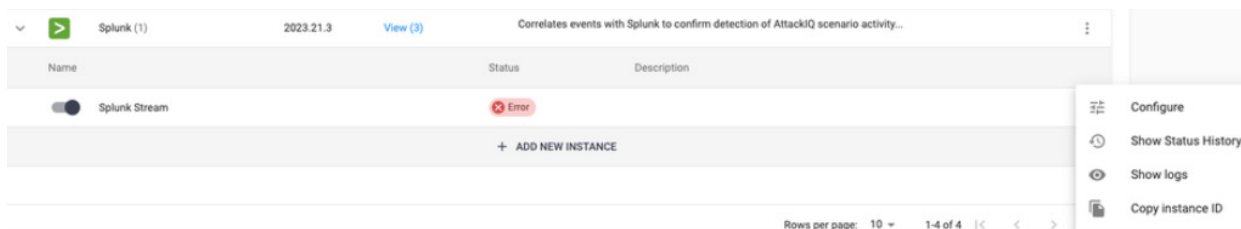
If it has been properly configured but appears with the Disabled status, clicking the slider on the left enables the integration. You should take into account that it can take up to one to two minutes for the process to finish.



▼	Splunk (1)	2023.21.3	View (3)	Correlates events with Splunk to confirm detection of AttackIQ scenario activity...	⋮
Name	Status	Description			
Splunk Stream	Disabled				

Figure 25. SIEM integration

If it has been deployed but appears with the Error status, checking the logs can give more details on the specific issue that is affecting the SIEM integration. Clicking the right menu and selecting Show logs allows you to see the integration logs and identify what specific issue is affecting the integration.



▼	Splunk (1)	2023.21.3	View (3)	Correlates events with Splunk to confirm detection of AttackIQ scenario activity...	⋮
Name	Status	Description			
Splunk Stream	Error				
		+ ADD NEW INSTANCE			

Configure
 Show Status History
 Show logs
 Copy instance ID

Rows per page: 10 1-4 of 4

Figure 26. SIEM status

Clicking Details next to Error also shows information on the specific error.

Zscaler ZIA is Not Preventing or Detecting All Scenarios

If the assessment shows unexpected results, such as some scenarios not being prevented or detected, it is displayed in the following way.



Tests Results	
Malware Protection	Advanced Threat Protection
URL Filtering	File Type Control
	Sandbox

Figure 27. Test results

Use Mitigations to Ensure You are Well Protected

After the assessment has finished, the mitigations section includes information on specific configurations to be able to prevent or detect the scenarios of the assessment. Each mitigation contains details on the necessary steps to ensure the expected protection.

Use IOCs/Observables for Troubleshooting

The IOCs/Observables in the scenario results can be used to build a query to check the Zscaler ZIA traffic logs and see if the traffic has been analyzed.

For example, if a scenario not being detected or prevented, you can do the following:

1. In the scenario results, check the connection in the Source Port (in the following figure, it's 57567).



Destination	HTTP Method	Protocols	Request Path	Source Port	Format
malware.scenarios.attackiq-ntm.com	GET	tcp, http	/Dea05169d111415903a1098110c34c0b0d390c23016cd4e179d9ef507104495/human.aspx	57567	STIX

Figure 28. Activity Details

2. Using the IP of the target asset, the source port and the URL destination, build a query to search for the traffic on Zscaler ZIA: Client IP matches AssetIP AND URL Search contains RequestPath AND Client Source Port From 57567 To 57567.

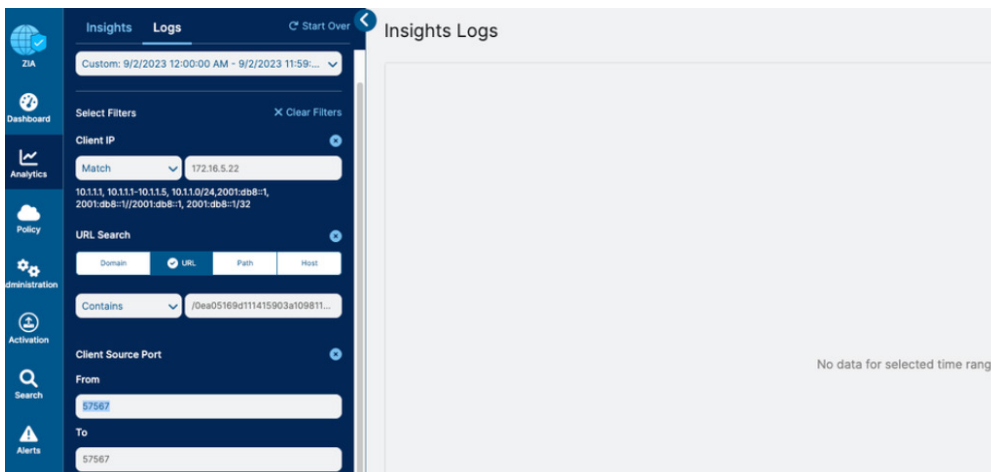


Figure 29. Logs

3. If the query doesn't show any results, it means that this traffic hasn't gone through Zscaler ZIA or there is a misconfiguration of Zscaler logs. In this case, it's important to review the network maps and the Zscaler ZIA configuration to ensure that the traffic between the selected assets is analyzed and stored by Zscaler ZIA.



No...	Event Time	Policy Action	Blocked Policy Type...	Response Code...	URL
1	Thursday, October 26, 2023 12:00:19 AM	Malware Block: Malicious File	Malware Protection	403 - Forbidden	malware.scenarios.attackiq-ntm.com/Dea05169d111415903a1098110c34c0b0d390c23016cd4e179d9ef507104495/human.aspx

Figure 30. Query results

4. After the traffic has gone through Zscaler ZIA, check if has been detected using the same query before.
 - Use the Zscaler queries in the Support Portal - ZIA section to easily find the different threats generated by the AttackIQ scenarios.
 - Depending on the policy configurations, there might be scenarios that are detected by Zscaler but not prevented. In this case, only a detection appears in the AttackIQ results.
 - If a detection appears on the Zscaler ZIA but not in the AttackIQ platform, it is important to review the Integration Manager and the SIEM integration to ensure that there are no issues related to them.

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

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

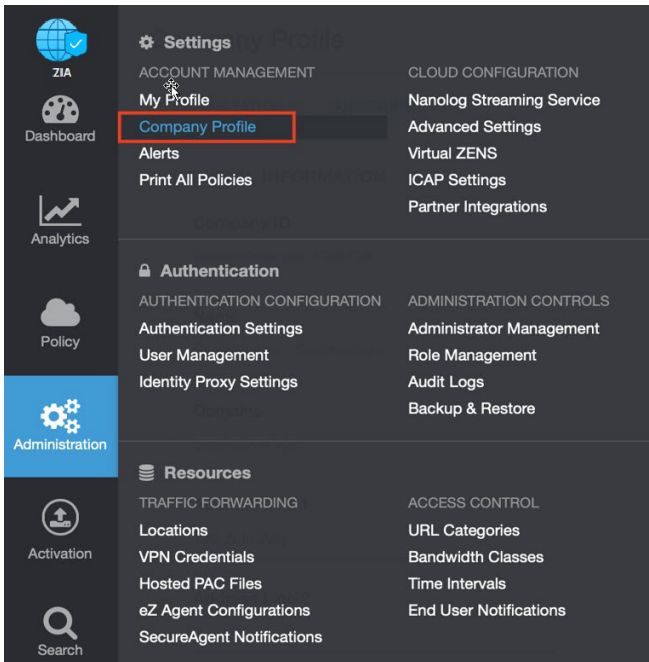


Figure 31. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.

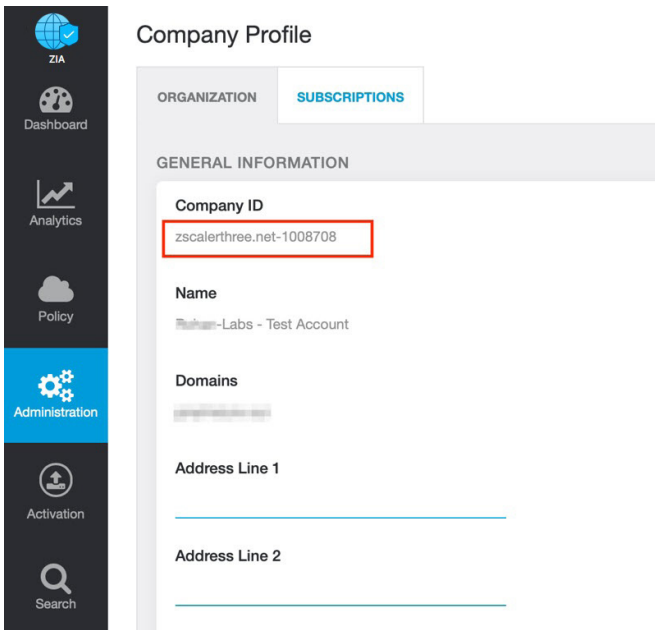


Figure 32. Company ID

Enter Support Section

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

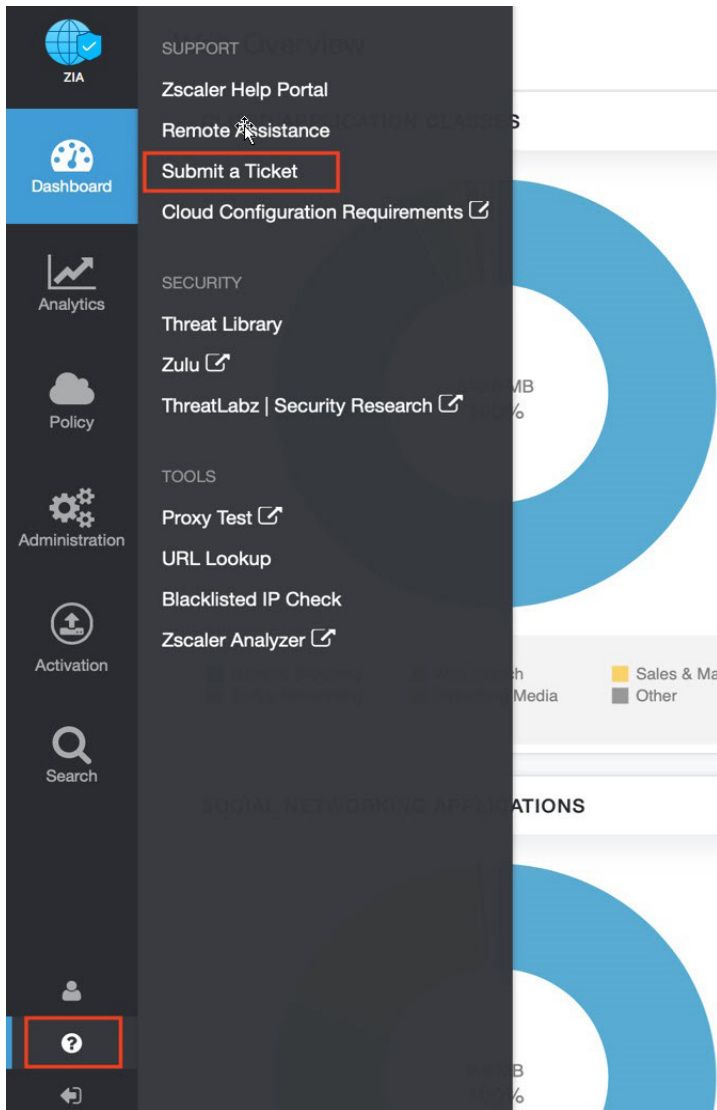


Figure 33. Submit a ticket