ZSCALER AND ARISTA DEPLOYMENT GUIDE

NOVEMBER 2023, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

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)
IoC	Indicators of Compromise
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
NDR	Network Detection and Response
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)

Trademark Notice

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.

Arista Overview

Arista Networks is an industry leader in data-driven, client to cloud networking for large data center, campus, and routing environments. Arista's award-winning platforms deliver availability, agility, automation, analytics, and security through an advanced network operating stack. To learn more, refer to Arista NDR'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:

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

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 Arista Introduction

Overviews of the Zscaler and Arista 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:

- 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.
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.

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
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.

Arista NDR Overview

Today, a Zero Trust networking approach to security is paramount for organizations looking to build a robust cybersecurity program. Irrespective of which device, application, or user is accessing an enterprise resource, Zero Trust focuses on complete visibility and control over all activity on the network.

Arista's Zero Trust networking principles, based on NIST 800-207, help customers address this challenge with three cornerstones: visibility, continuous diagnostics, and enforcement. The Arista NDR platform delivers continuous diagnostics for the entire enterprise threat landscape, processes countless points of data, senses abnormalities or threats, and reacts if necessary—all in a matter of seconds.

Arista Resources

The following table contains links to Arista support resources.

Name	Definition
Arista Customer Support	Online customer support.
Arista Product Documentation	Product documentation.

Arista NDR and Zscaler Integration

The Arista NDR and Zscaler integration provides improved visibility and contextual information on potential security threats present on your network, enabling prompt response actions against the detected threats. This integration enriches and associates IoC information, such as domains, identified in the network by Arista NDR with the global classification data from Zscaler. Additionally, administrators can directly execute response actions from the Arista NDR platform UI by adding or removing these IoCs detected by Arista NDR to the custom categories maintained within the ZIA product for immediate enforcement of policy rules.

This integration guide includes necessary instructions to configure and access the Zscaler integration within Arista NDR.

Configuring Zscaler Integration

Gather the following information to configure and enable the ZIA integration on the Arista NDR deployment.

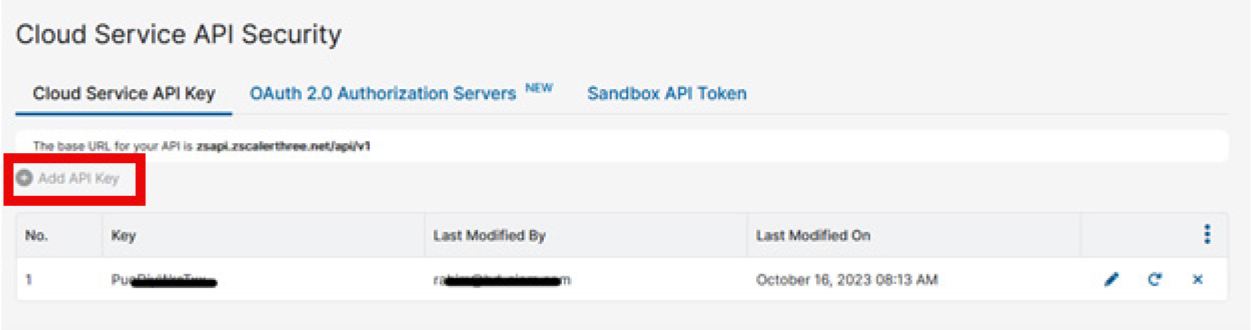
Configuration Item	Description
API server URL	ZIA API URL
API key	ZIA API key
API user name	ZIA API user
API password	ZIA API password for the administrator

The ZIA API user should have full policy access permissions with access control functional scope enabled for Policy and Resource Management, Custom URL category management, and Override Existing Categories.

Generating API Key

To generate an API key from the ZIA Admin Portal:

1. Go to **Administration** > **Cloud Service API Security**.
2. Click **Add API Key**.



Cloud Service API Security

The base URL for your API is **zsapi.zscalerthree.net/api/v1**

No.	Key	Last Modified By	Last Modified On
1	Pu[redacted]	ra[redacted]m	October 16, 2023 08:13 AM

Figure 1. Cloud Service API Security

Creating a Role

To create a role:

1. API user must be tied to a **Role**. Generate the role by going to **Administration** > **Role Management**. The **Add API Role** window is displayed.
2. Click **Add API Role**.

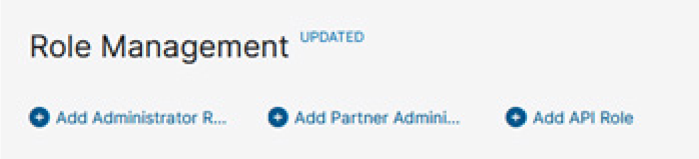
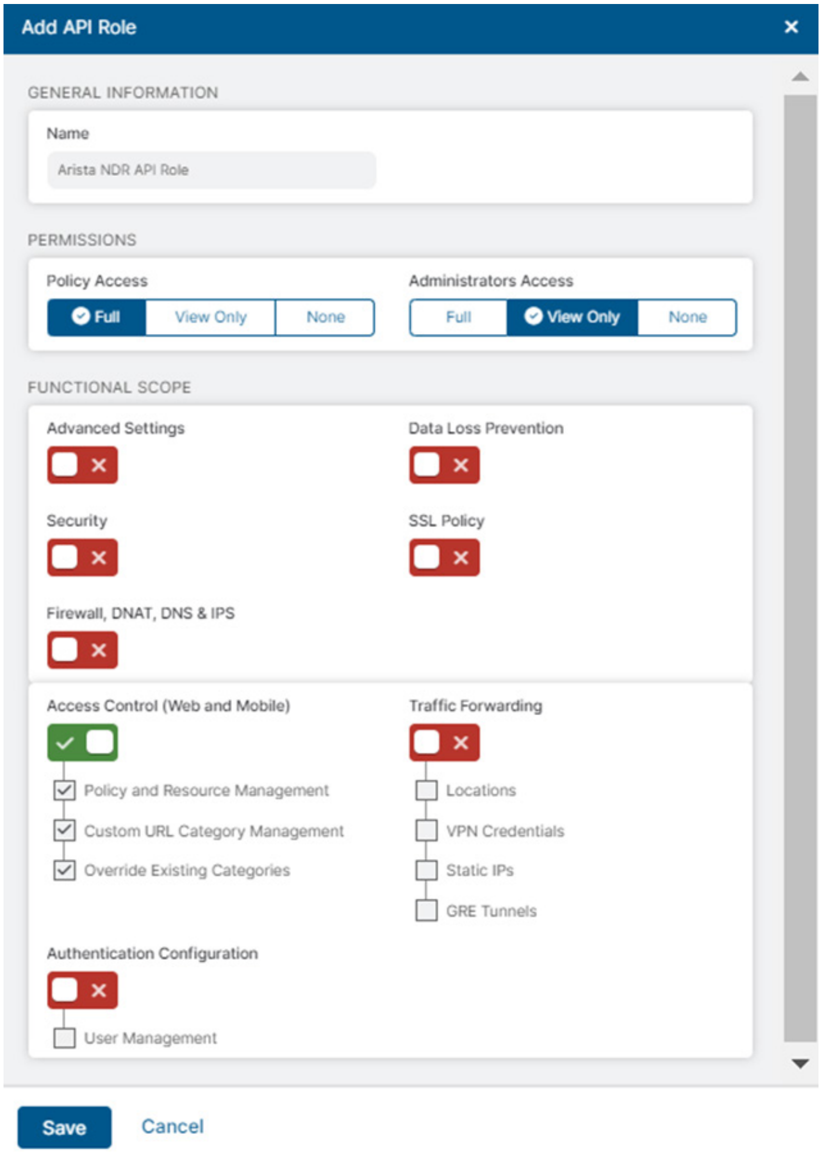


Figure 2. Role Management

3. Create the API Role by configuring the fields as shown in the image.



GENERAL INFORMATION

Name: Arista NDR API Role

PERMISSIONS

Policy Access: [✓ Full] View Only None

Administrators Access: Full [✓ View Only] None

FUNCTIONAL SCOPE

Advanced Settings ✗

Data Loss Prevention ✗

Security ✗

SSL Policy ✗

Firewall, DNAT, DNS & IPS ✗

Access Control (Web and Mobile) ✓
- ☑ Policy and Resource Management
- ☑ Custom URL Category Management
- ☑ Override Existing Categories

Traffic Forwarding ✗
- □ Locations
- □ VPN Credentials
- □ Static IPs
- □ GRE Tunnels

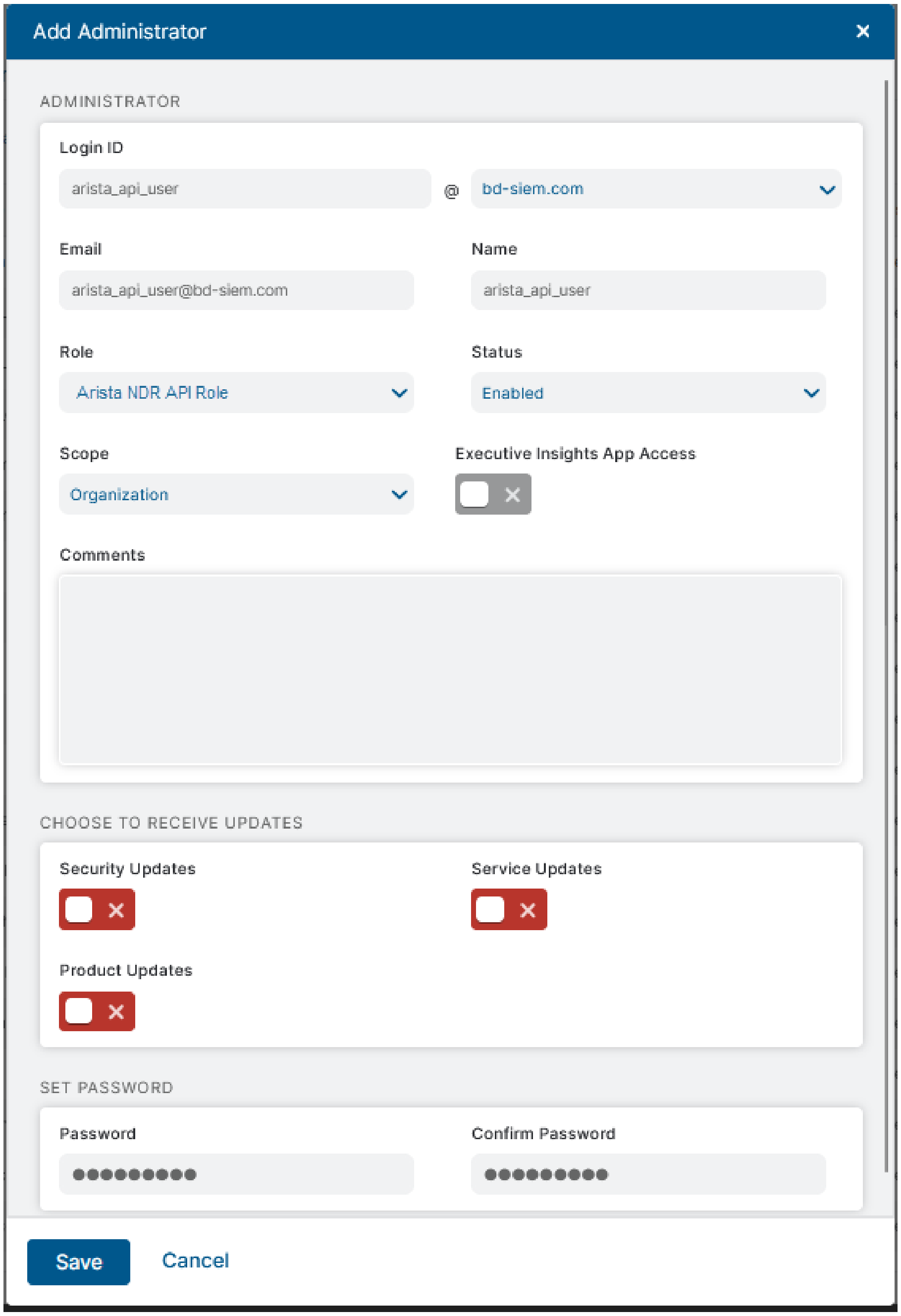
Authentication Configuration ✗
- □ User Management

Figure 3. Add API Role

Creating an API User

To create an API user:

1. Go to **Administration** > **Administrator Management**.
2. Click **Add Administrator** and assign the created **Role**.
3. Enter the **Login ID** and **Password**.
4. Click **Save**.



Add Administrator

ADMINISTRATOR

Login ID: arista_api_user @ bd-siem.com

Email: arista_api_user@bd-siem.com

Name: arista_api_user

Role: Arista NDR API Role

Status: Enabled

Scope: Organization

Executive Insights App Access: ✕

Comments:

CHOOSE TO RECEIVE UPDATES

Security Updates: ✕

Service Updates: ✕

Product Updates: ✕

SET PASSWORD

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

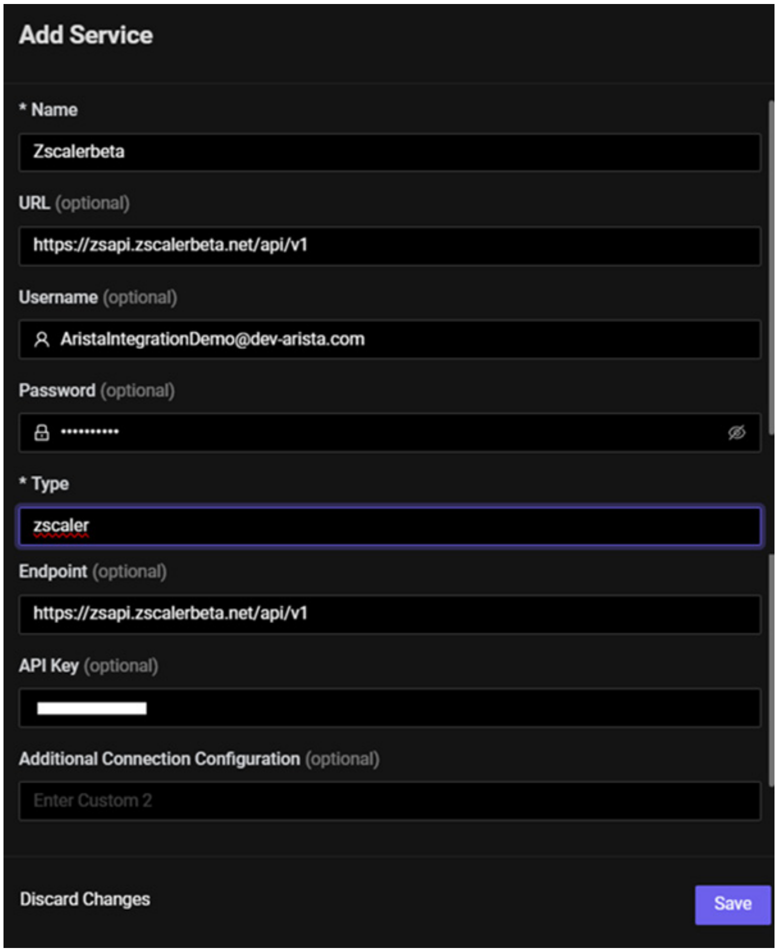
Figure 4. Add Administrator

Configuring Arista NDR

Steps to configure the Zscaler integration with Arista NDR. From the Arista NDR Home page:

1. Go to **Settings** and select **Connected services**.
2. Add a new service by clicking **Add Service** and selecting **Custom**.
3. Fill in the appropriate ZIA configuration details as shown in the following example.

Enter a unique name for this custom service, and enter `zscaler` as the **Type**.



Add Service

* Name: Zscalerbeta

URL (optional): https://zsapi.zscalerbeta.net/api/v1

Username (optional): AristaIntegrationDemo@dev-arista.com

Password (optional): ••••••••••

* Type: zscaler

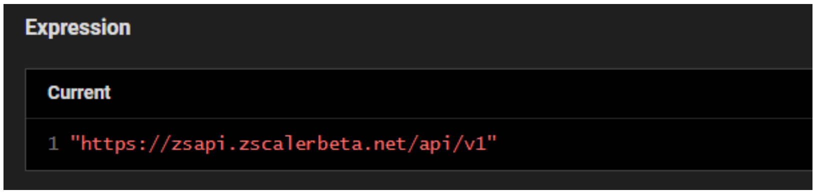
Endpoint (optional): https://zsapi.zscalerbeta.net/api/v1

API Key (optional):

Additional Connection Configuration (optional): Enter Custom 2

Figure 5. Add Service

4. Click **Save**.
5. Go to **Manage Detections** and click **Skills** from the left-side menu of the Arista NDR home page.
6. Use `Reference Identifier` to filter the config.Zscaler.apiServer package.
7. Open the config.Zscaler.apiServer package and click **Duplicate**.
8. Make changes to the expression by updating it with the ZIA API URL as shown in the following example:



```
"https://zsapi.zscalerbeta.net/api/v1"
```

Figure 6. Expression

9. **Save** the changes.
10. Send an email to **supportsecurity@arista.com** or visit **Arista Customer Support** in case of any issues.

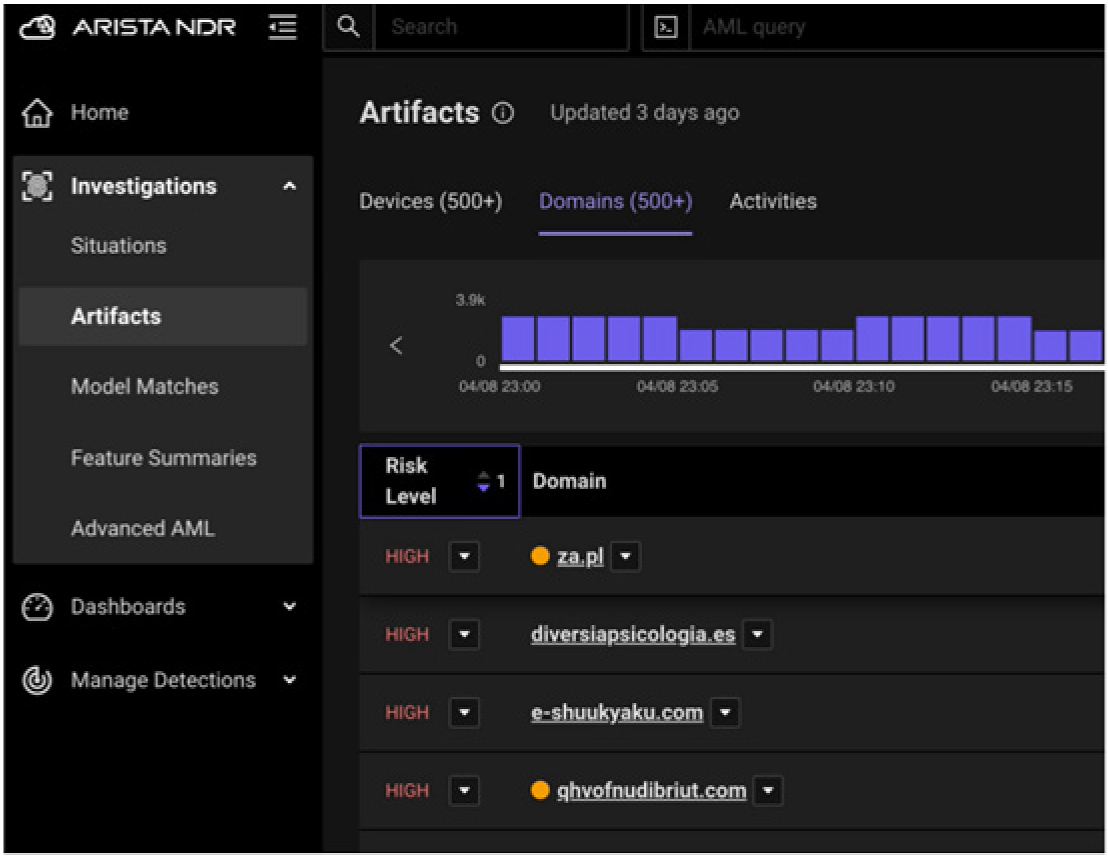
Accessing Zscaler Integration

When the Zscaler integration is enabled on the Arista NDR appliance, it initiates Zscaler API calls that gather information on IoCs, such as Domains, as identified by the Zscaler service. This information is then linked with the corresponding Domain entities discovered on the network through Arista NDR. Subsequently, the details pages of the Domain entities display the data sourced from the Zscaler service, including the custom categories that these IoCs might belong to in Zscaler, any security alerts identified by Zscaler against these IoCs, and their general classifications such as music, travel, news, and media, among others.

Accessing Domain Artifact Page with Zscaler Data

To proceed:

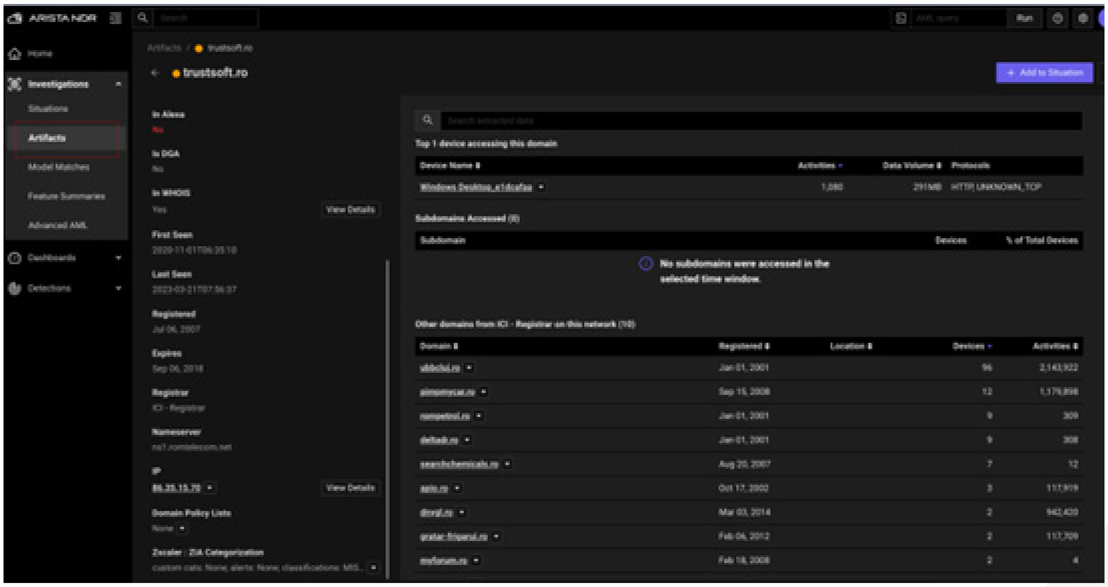
1. Go to the **Artifacts** section and select the **Domains** tab.
2. Click any domain from the list.



Risk Level 1	Domain
HIGH	za.pl
HIGH	diversiapsicologia.es
HIGH	e-shuukyaku.com
HIGH	qhvofnudibriut.com

Figure 7. Artifacts

This redirects to the **Domain Entity Details** page.



In Alexa
No

In DGA
No

In WHOIS
Yes

First Seen
2020-11-01T06:35:18

Last Seen
2023-03-21T07:56:37

Registered
Jul 06, 2007

Expires
Sep 06, 2018

Registrar
ICI - Registrar

Nameserver
ns1.romtelecom.net

IP
86.35.15.70

Domain Policy Lists
None

Zscaler : ZIA Categorization
custom cats: None, alerts: None, classifications: MIS...

Top 1 device accessing this domain

Device Name	Activities	Data Volume	Protocols
Windows Desktop_e1dcafaa	1,080	291MB	HTTP, UNKNOWN_TCP

Subdomains Accessed (0)

Subdomain	Devices	% of Total Devices

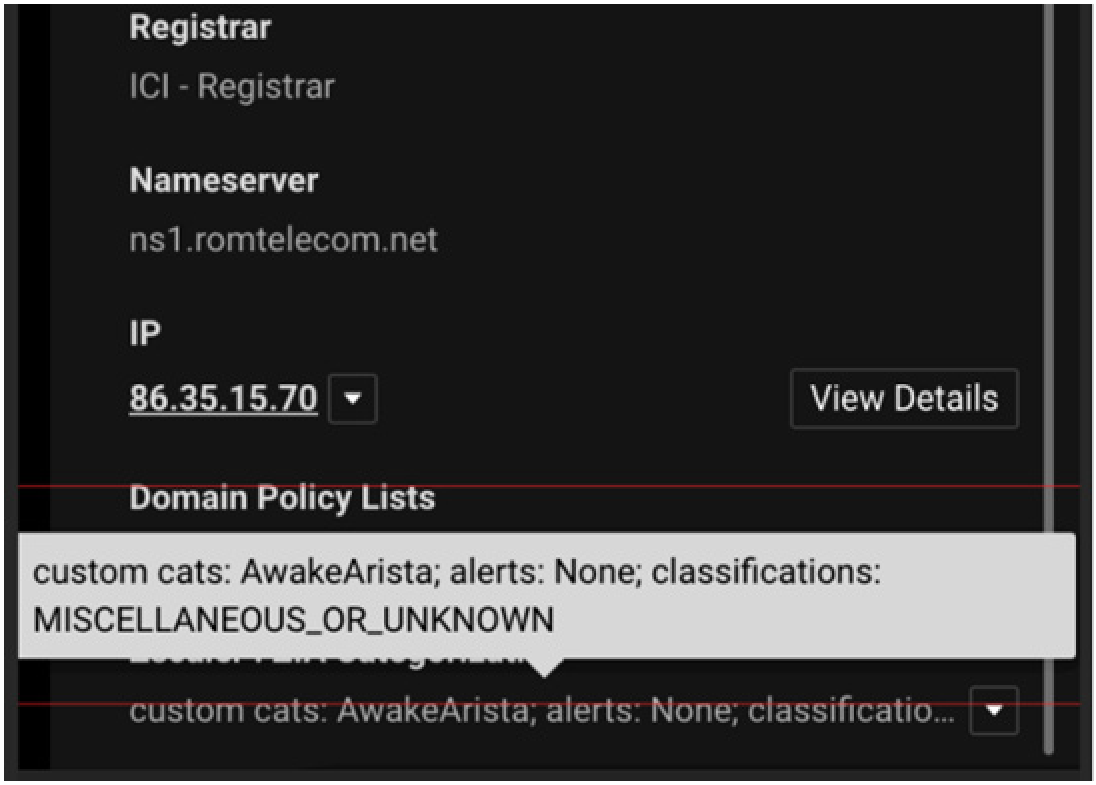
No subdomains were accessed in the selected time window.

Other domains from ICI - Registrar on this network (10)

Domain	Registered	Location	Devices	Activities
ubbcluj.ro	Jan 01, 2001		96	2,143,922
aimomecar.ro	Sep 15, 2008		12	1,179,898
rompetrol.ro	Jan 01, 2001		9	309
deltadn.ro	Jan 01, 2001		9	308
searchchemicals.ro	Aug 20, 2007		7	12
apis.ro	Oct 17, 2002		3	117,919
dnrgl.ro	Mar 03, 2014		2	942,420
gratar-frigarui.ro	Feb 06, 2012		2	117,709
myforum.ro	Feb 18, 2008		2	4

Figure 8. Domain Entity Details

3. Hover over the **ZIA Categorization** data to view the complete Zscaler Classification data for this domain.



Registrar

ICI - Registrar

Nameserver

ns1.romtelecom.net

IP

86.35.15.70 ▾

Domain Policy Lists

custom cats: AwakeArista; alerts: None; classifications: MISCELLANEOUS_OR_UNKNOWN

custom cats: AwakeArista; alerts: None; classificatio... ▾

Figure 9. Zscaler Classification data

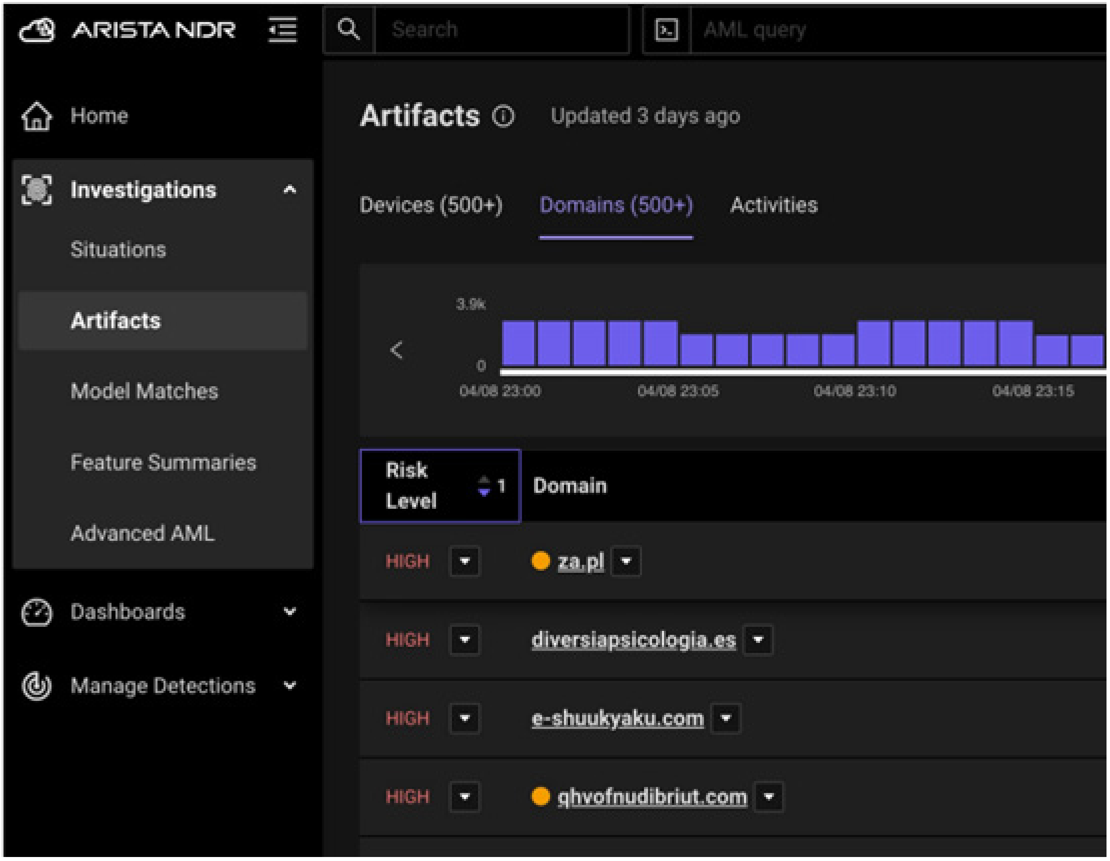
Zscaler Response Integration Actions

Apart from retrieving data from ZIA and linking it with the Domain entities discovered on the network by Arista NDR to enhance security context, the integration also facilitates administrators to take prompt response actions through the Arista NDR platform UI. You can achieve this by adding or removing malicious IoCs detected directly into the desired Zscaler customer categories. Then you can immediately apply the resulting policy enforcement rules against these IoCs.

Taking Response Action against Domain Entity

To initiate a response action:

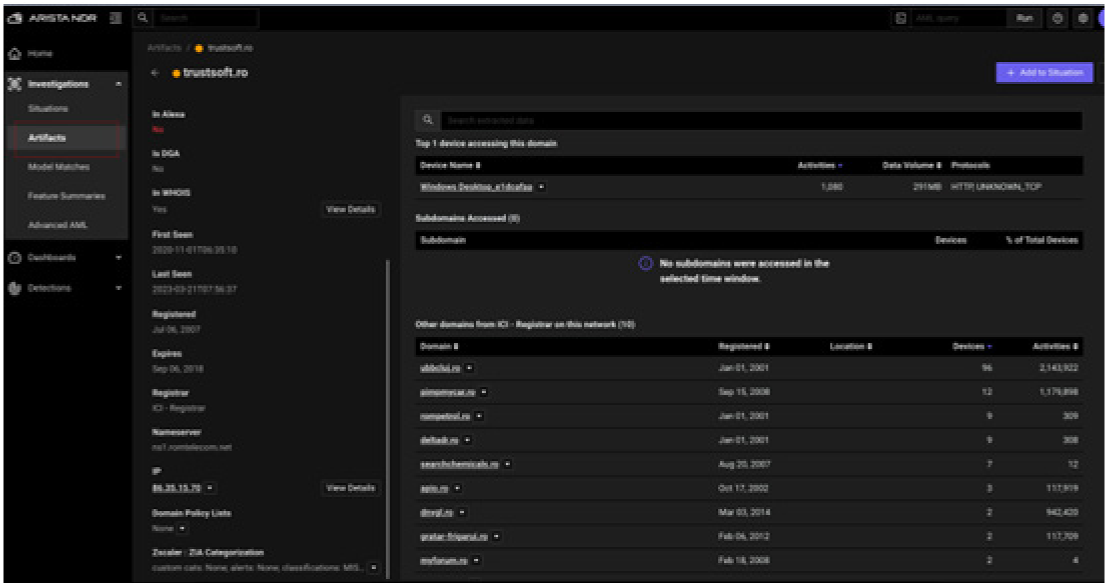
1. From the Arista NDR Home page, go to the **Domains** tab within the **Artifacts** section and click the desired domain from the **Domain** list.



Risk Level	Domain
HIGH	za.pl
HIGH	diversiapsicologia.es
HIGH	e-shuukyaku.com
HIGH	ghvofnudibriut.com

Figure 10. Artifacts

You are redirected to the **Domain Entity profile** page.



trustsoft.ro

In Alexa
No

Is DGA
No

In WHOIS
Yes

First Seen
2020-11-01T06:35:10

Last Seen
2023-03-21T07:56:37

Registered
Jul 06, 2007

Expires
Sep 06, 2018

Registrar
ICI - Registrar

Nameserver
ns1.romtelecom.net

IP
86.35.15.70

Domain Policy Lists
None

Zscaler : ZIA Categorization
custom cats: None; alerts: None; classifications: MIS...

Top 1 device accessing this domain

Device Name	Activities	Data Volume	Protocols
Windows Desktop_e1dcafaa	1,080	291MB	HTTP, UNKNOWN_TCP

Subdomains Accessed (0)

Subdomain	Devices	% of Total Devices

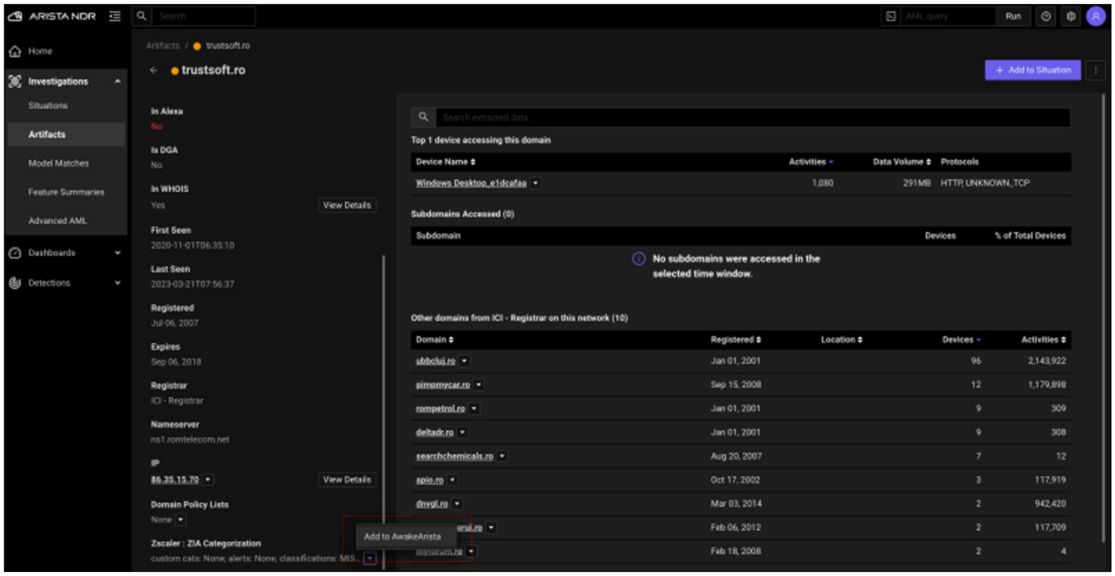
No subdomains were accessed in the selected time window.

Other domains from ICI - Registrar on this network (10)

Domain	Registered	Location	Devices	Activities
ubbcluj.ro	Jan 01, 2001		96	2,143,922
pimpmycar.ro	Sep 15, 2008		12	1,179,898
rompetrol.ro	Jan 01, 2001		9	309
deltadr.ro	Jan 01, 2001		9	308
searchchemicals.ro	Aug 20, 2007		7	12
apio.ro	Oct 17, 2002		3	117,919
dnvgl.ro	Mar 03, 2014		2	942,420
gratar-friparul.ro	Feb 06, 2012		2	117,709
myforum.ro	Feb 18, 2008		2	4

Figure 11. Domain Entity

2. To add the **Domain** artifact within ZIA, click the drop-down button located next to the ZIA data for this Domain and select the relevant **Custom** category. For instance, in the following example, you assign the **Domain** to a **Custom** category named `AwakeArista` within ZIA.



trustsoft.ro

In Alexa
No

Is DGA
No

In WHOIS
Yes

First Seen
2020-11-01T06:35:10

Last Seen
2023-03-21T07:56:37

Registered
Jul 06, 2007

Expires
Sep 06, 2018

Registrar
ICI - Registrar

Nameserver
ns1.romtelecom.net

IP
86.35.15.70

Domain Policy Lists
None

Zscaler : ZIA Categorization
custom cats: None; alerts: None; classifications: MIS...

Top 1 device accessing this domain

Device Name	Activities	Data Volume	Protocols
Windows Desktop_e1dcafaa	1,080	291MB	HTTP, UNKNOWN_TCP

Subdomains Accessed (0)

Subdomain	Devices	% of Total Devices

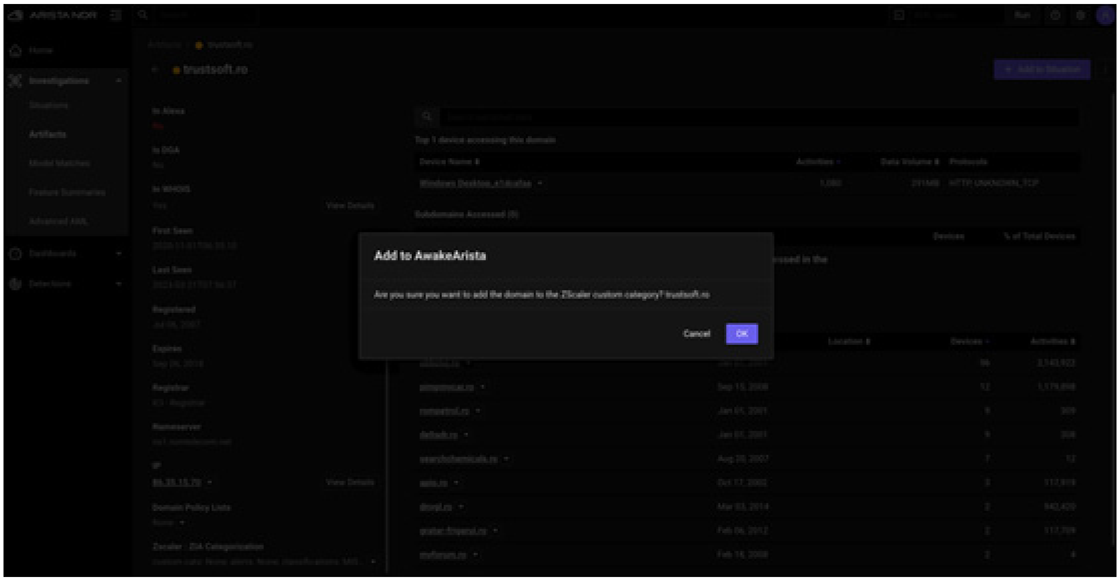
No subdomains were accessed in the selected time window.

Other domains from ICI - Registrar on this network (10)

Domain	Registered	Location	Devices	Activities
ubbcluj.ro	Jan 01, 2001		96	2,143,922
pimpmycar.ro	Sep 15, 2008		12	1,179,898
rompetrol.ro	Jan 01, 2001		9	309
deltadr.ro	Jan 01, 2001		9	308
searchchemicals.ro	Aug 20, 2007		7	12
apio.ro	Oct 17, 2002		3	117,919
dnvgl.ro	Mar 03, 2014		2	942,420
...arul.ro	Feb 06, 2012		2	117,709
myforum.ro	Feb 18, 2008		2	4

Figure 12. Assign domain to a category

3. After you have selected the desired **Custom** category, click **OK** to confirm the addition of the Domain to the selected category.

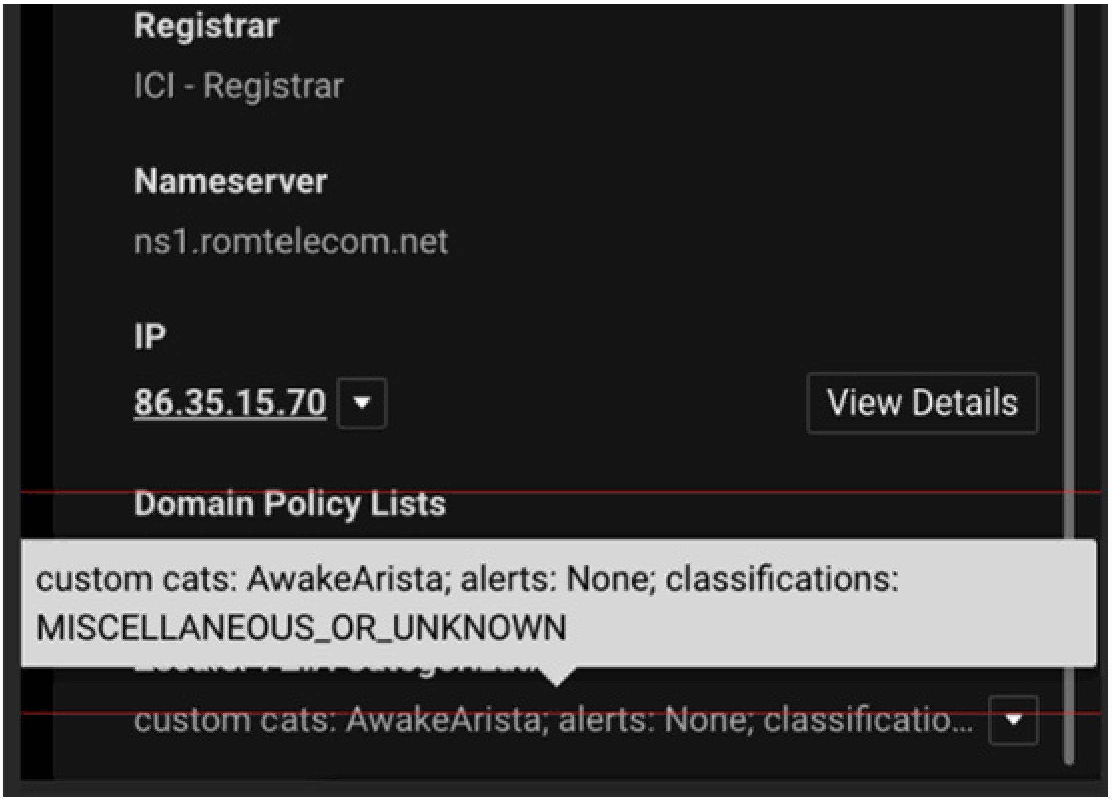


Add to AwakeArista

Are you sure you want to add the domain to the ZScaler custom category? trustsoft.ro

Figure 13. Confirm category selection

4. To ensure that the Domain has been added to the selected Custom category within ZIA, verify that the Domain appears as a part of the chosen category. In the following example, the Domain is visible under the AwakeArista custom category.



Registrar
ICI - Registrar

Nameserver
ns1.romtelecom.net

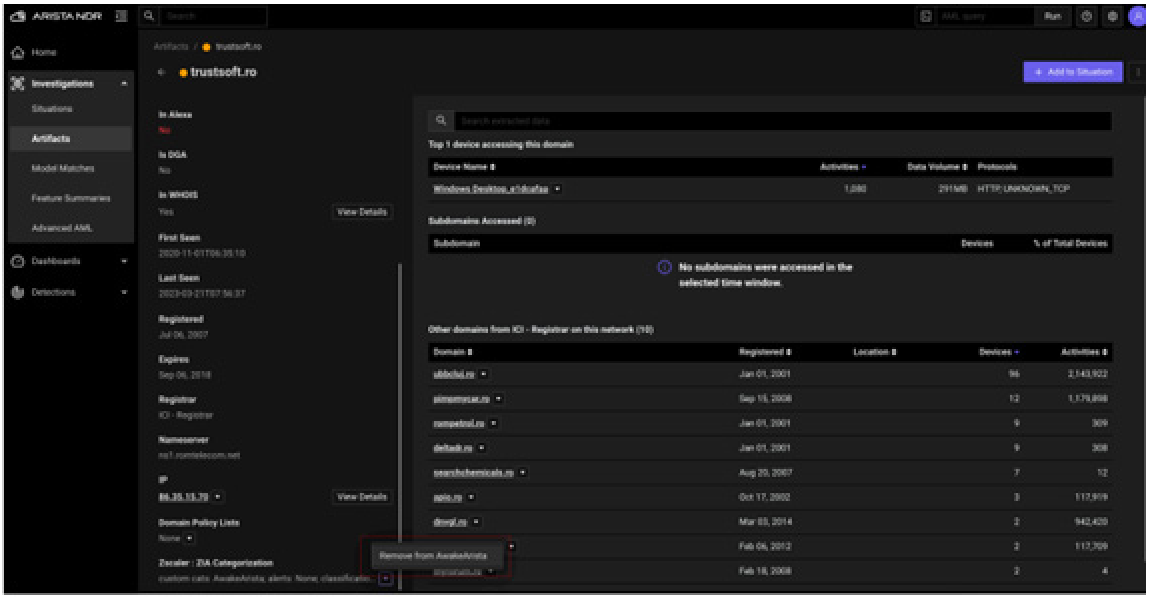
IP
86.35.15.70

Domain Policy Lists
custom cats: AwakeArista; alerts: None; classifications: MISCELLANEOUS_OR_UNKNOWN

custom cats: AwakeArista; alerts: None; classificatio...

Figure 14. Confirm category

5. If needed, remove the Domain artifact from the ZIA Custom category list by selecting Remove against the corresponding Domain. In the following example, click **Remove** from AwakeArista to eliminate the categorization from the ZIA Custom category.



trustsoft.ro

In Alexa
No

Is DGA
No

In WHOIS
Yes

First Seen
2020-11-01T06:35:10

Last Seen
2023-03-21T07:56:37

Registered
Jul 06, 2007

Expires
Sep 06, 2018

Registrar
ICI - Registrar

Nameserver
ns1.romtelecom.net

IP
86.35.15.70

Domain Policy Lists
None

Zscaler : ZIA Categorization
custom cats: AwakeArista, alerts: None, classificatio...

Top 1 device accessing this domain

Device Name	Activities	Data Volume	Protocols
Windows Desktop_a1dcafaa	1,080	291MB	HTTP, UNKNOWN_TCP

Subdomains Accessed (0)

Subdomain	Devices	% of Total Devices

No subdomains were accessed in the selected time window.

Other domains from ICI - Registrar on this network (10)

Domain	Registered	Location	Devices	Activities
ubbcluj.ro	Jan 01, 2001		96	2,143,922
simonmocar.ro	Sep 15, 2008		12	1,179,898
rompetrol.ro	Jan 01, 2001		9	309
deltadc.ro	Jan 01, 2001		9	308
searchchemicals.ro	Aug 20, 2007		7	12
apio.ro	Oct 17, 2002		3	117,919
drogl.ro	Mar 03, 2014		2	942,420
[illegible]	Feb 06, 2012		2	117,709
[illegible]	Feb 18, 2008		2	4

Figure 15. Remove category

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:

1. Go to **Administration** > **Settings** > **Company Profile**.

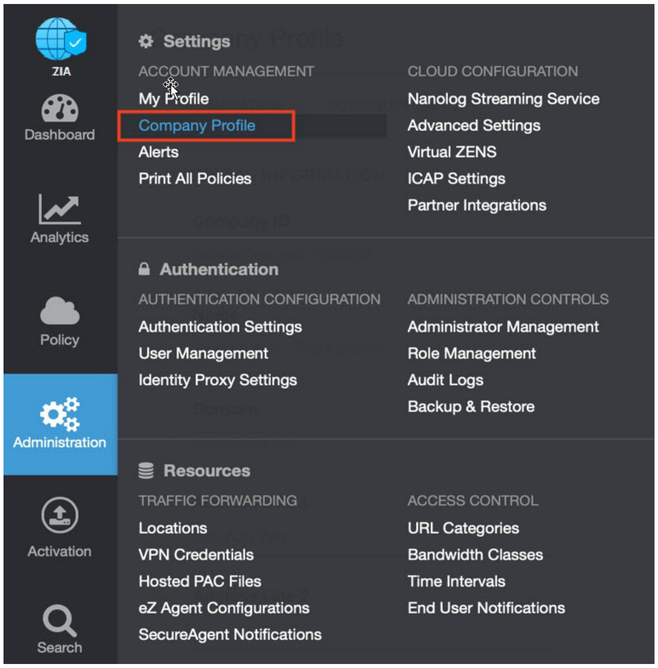
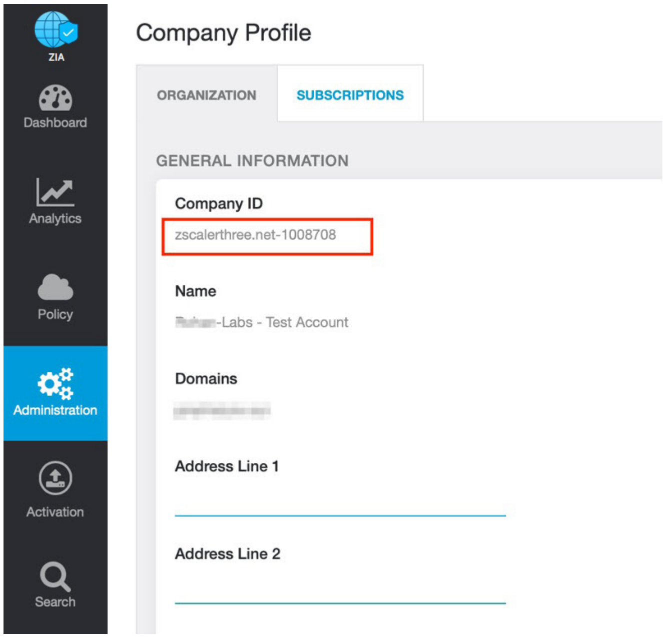


Figure 16. Collecting details to open support case with Zscaler TAC

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 17. Company ID

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

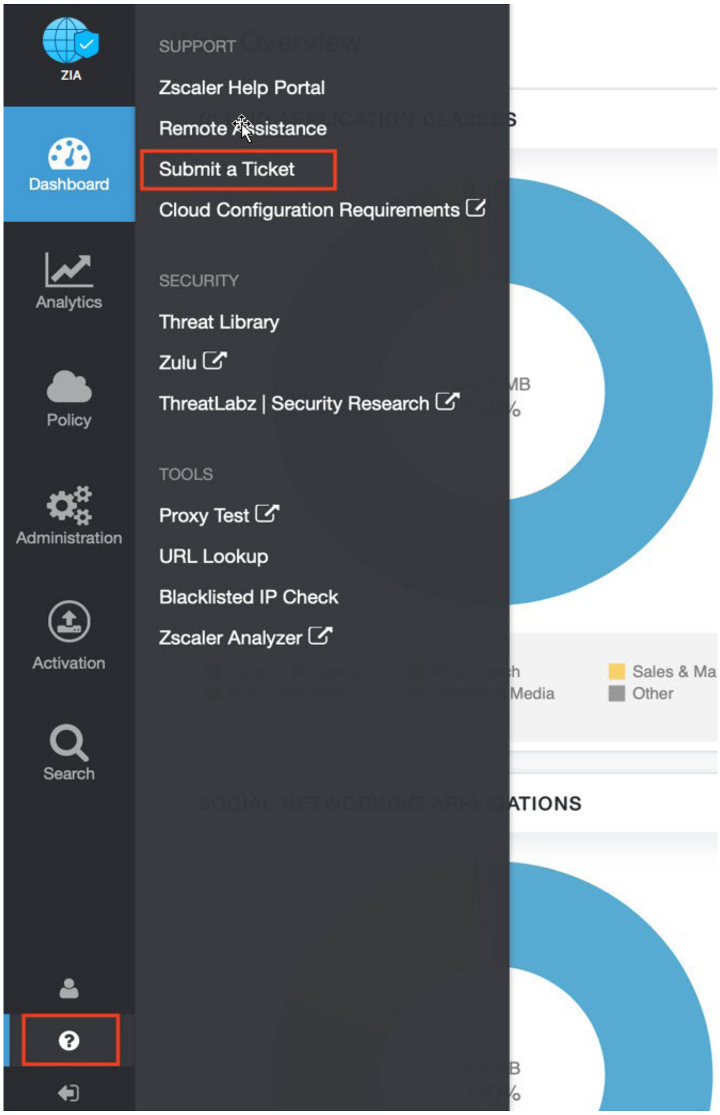


Figure 18. Submit a ticket