



ZSCALER AND ARMIS DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	6
Zscaler Overview	6
Armis Overview	6
Audience	6
Software Versions	6
Prerequisites	6
Request for Comments	7
Zscaler and Armis Introduction	8
ZIA Overview	8
ZPA Overview	8
Zscaler UVM	8
Zscaler Resources	9
Armis Centrix Overview	9
Armis Resources	9
Overview of the Zscaler and Armis Integration	10
Use Cases	10
How the Integration Works	10
Capabilities	10
Creating Zscaler API Keys	11
Configuring ZPA Log Receiver	13
Creating a Zscaler Integration in the Armis Console	15
Viewing Data Retrieved from Zscaler	17
API Calls	18

Contextualizing Risk using Zscaler UVM and Armis	19
Required Parameters	19
Roles and Permissions	19
Retrieving the Parameters	19
Retrieving the API Token	19
Retrieving the Armis Instance	20
Configure the Zscaler UVM Data Connectors	21
Configure Authentication for the Armis Data Source	21
Configure the Armis Devices Data Source	22
Configure the Armis CVE Data Source	25
Review and Adjust Risk Scoring	27
Map the Armis Data Source	27
Review and Adjust Risk Scoring	29
Appendix A: Requesting Zscaler Support	31

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)
UVM	Unified Vulnerability Management
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

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](#).

Armis Overview

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time. In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, protect, and manage all critical assets. Armis secures Fortune 100, 200, and 500 companies as well as national governments, state, and local entities to help keep critical infrastructure, economies, and society stay safe and secure 24/7. To learn more, refer to [Armis' 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](#)
- [Armis Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

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

Prerequisites

To use this integration, make sure the following prerequisites are met:

- Open a Zscaler support ticket to enable the Zscaler Client Connector API for your environment. The Zscaler API is required for this integration, and it is not enabled by default.
- Ensure that firewall rules are opened in the Armis collector to the corresponding Zscaler domain.
- Have an active instance of Zscaler Unified Vulnerability Management (UVM).
- Have administrator login credentials to Zscaler UVM.
- Have an active Armis tenant.
- Have administrator login credentials to Armis.
- Have an active instance of Zscaler Internet Access (ZIA).
- Have administrator login credentials to ZIA.

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 Armis Introduction

Overviews of the Zscaler and Armis 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 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

Zscaler UVM offers a groundbreaking approach to tackling persistent challenges in vulnerability management. Despite decades of focus, traditional vulnerability management tools often fall short due to fragmented data, lack of context, and inefficient prioritization, leaving organizations exposed to threats.

Zscaler UVM redefines the landscape by utilizing its innovative Data Fabric for Security to integrate and enrich data from diverse sources, delivering a holistic and actionable view of an organization's risk posture.

With features like dynamic risk scoring, automated workflows, and real-time reporting, Zscaler UVM empowers organizations to prioritize critical vulnerabilities, streamline remediation efforts, and strengthen collaboration across teams. Designed for rapid deployment and measurable impact, UVM helps security leaders transition from reactive, manual processes to a proactive, data-driven strategy, ensuring a more resilient and efficient approach to modern vulnerability management.

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.

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.

Armis Centrix Overview

Armis Centrix, the cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects, and manages billions of assets around the world in real time. Its seamless, frictionless, cloud-based platform proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats, and protects your entire attack surface.

Armis Resources

The following table contains links to Armis support resources.

Name	Definition
Armis Support	Online help for Armis products.

Overview of the Zscaler and Armis Integration

ZIA and ZPA provide cloud-based Firewall and VPN capabilities.

Use Cases

The following are use cases for the Zscaler and Armis integration:

- Full visibility of asset details on devices connecting to or from the network via Zscaler.
- Enrich existing devices with traffic and services metadata ingested from the Zscaler traffic logs via the Zscaler App Connector. This is currently supported for ZPA only.

How the Integration Works

The integration periodically connects to the Zscaler cloud to retrieve asset details on devices connected via the Zscaler Client Connector.

The Zscaler platform sends continuous traffic logs to the integration for retrieving traffic and service metadata.

Capabilities

The following are the capabilities of the Zscaler and Armis integration:

- Enrich device data.
- Identify the user used by the device to connect to Zscaler.
- Provide traffic data enrichment for connected devices. This capability is optional, available for ZPA only, and requires additional configuration. To learn more, see [Configuring ZPA Log Receiver](#).

Creating Zscaler API Keys


The following steps describe creating the Zscaler API keys.

1. To access the Zscaler Client Connector API:
 - a. In the ZPA Admin Portal, click **Client Connector** from the left-side navigation.
 - b. In the ZIA Admin Portal, go to **Policy > Mobile > Zscaler Client Connector Portal**.
2. In the Zscaler Client Connector Portal, go to **Administration > Public API**.
3. Click **Add API Key**.



Figure 1. Add API Key

4. Configure the API key details as follows:
 - a. **Name**: Enter a description for the API key. This is only used for display purposes.
 - b. **Status**: Verify that the status is set to **Enabled**.

 This is mainly used for disabling previously active keys without entirely revoking them.

- c. **Role**: Verify that **Read** is selected. Currently, this is optional because the API is read-only.
- d. **Session Validity Interval**: The time in seconds before an authorization expires. When the API is accessed, the first call is to authenticate. This call provides the auth header to use for subsequent calls. Session validity determines how long this auth header stays valid.

 A screenshot of a web-based configuration dialog titled 'Add API Key' in a blue header bar with a close button (X) on the right. The dialog contains several fields:

- Name**: A text input field with a question mark icon. The placeholder text is 'Sample Name'.
- Status**: A toggle switch with a question mark icon. The 'Enabled' option is selected and highlighted in blue, while 'Disabled' is in a light gray box.
- Role**: A dropdown menu with a question mark icon. The selected value is 'Read'.
- Session Validity Interval (In Seconds)**: A text input field with a question mark icon. The value '600' is entered.

 At the bottom of the dialog, there are two buttons: 'Save' (in blue) and 'Cancel' (in light gray).

Figure 2. Configure API Key

5. Click **Save**.
6. Copy the **Client Secret Key**. The key is used to authenticate with the API. This key is the value for the Zscaler Client Connector API Key Secret (see [Creating a Zscaler Integration in the Armis Console](#)).



The client's secret key is only displayed at this time. It is important to copy it now.

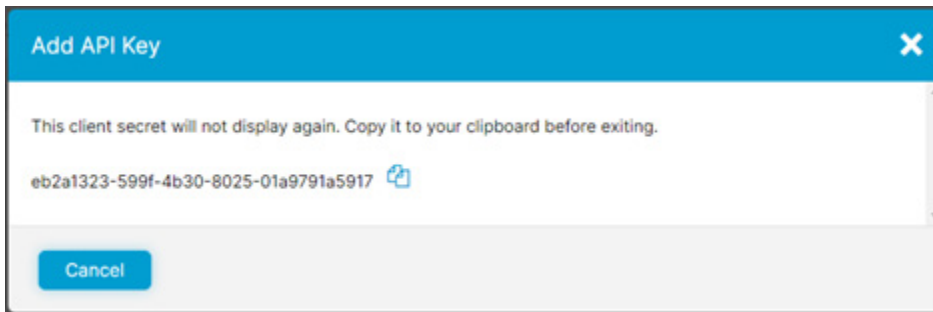


Figure 3. Client Secret Key

7. Go to the main **Public API** window. The new key (Client ID) is displayed in the list.

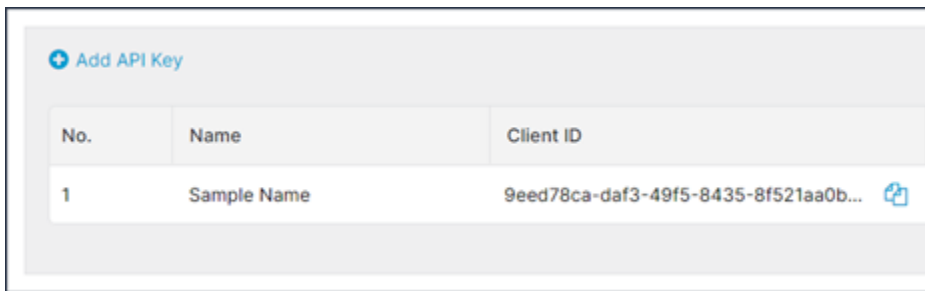


Figure 4. Public API window

8. Copy the **Client ID** from the page. This is the value for the Zscaler Client Connector API Key Client ID (see [Creating a Zscaler Integration in the Armis Console](#)).

Configuring ZPA Log Receiver

The following steps demonstrate how to configure the ZPA log receiver.



The following procedure is only relevant if the **Import Traffic Logs** checkbox is selected when creating the integration (see [Creating a Zscaler Integration in the Armis Console](#)).

1. In the ZPA Admin Portal, go to **Configuration & Control > Private Infrastructure > Log Receivers**.

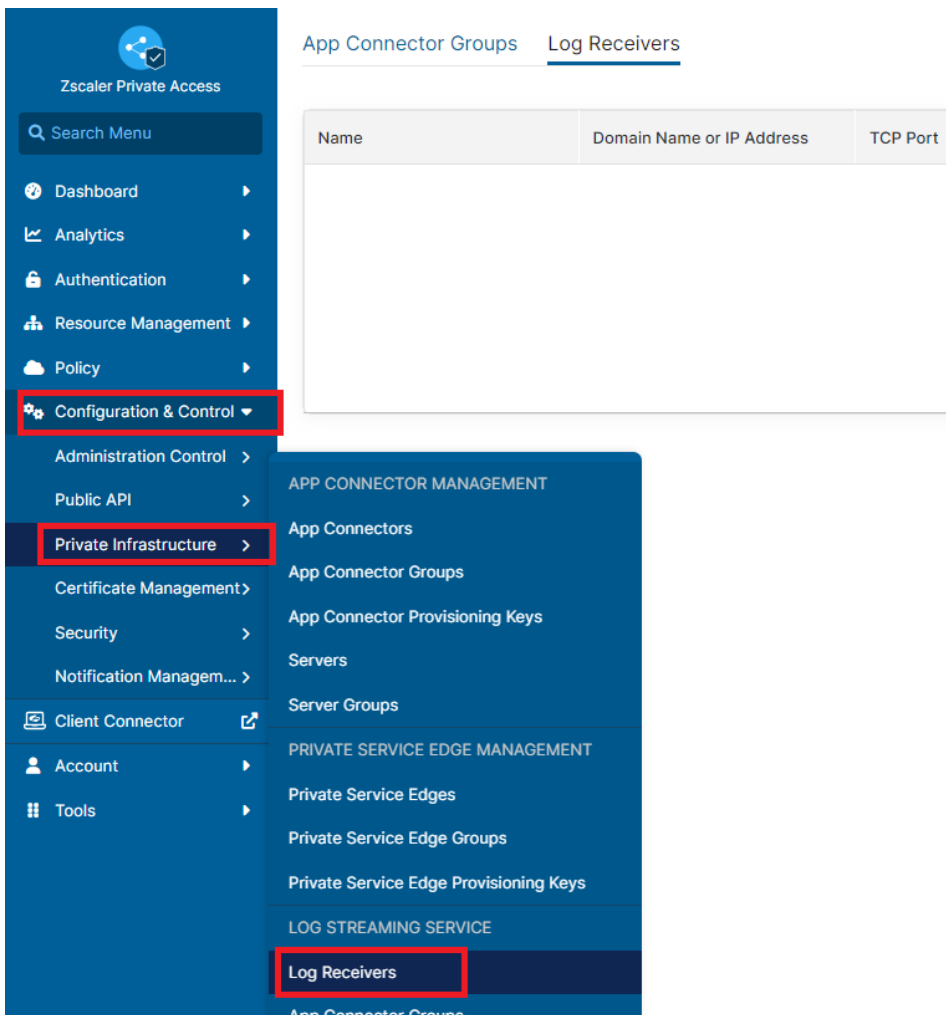


Figure 5. Log Receivers

2. Click **Add Log Receiver**.

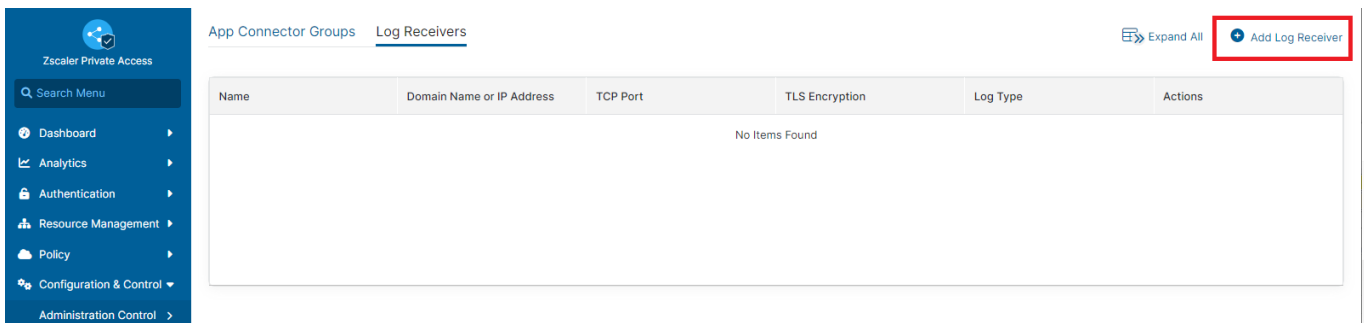


Figure 6. Add Log Receiver

3. Enter a name for the new Log Receiver and in the **Domain or IP Address** field, enter the Armis collectors IP.
4. In the **TCP Port** field, enter port 8282 (leave **TLS Encryption** as **Disabled**).
5. Select one or more **App Connector Groups** to use for the environment in which the Armis collector resides.

Figure 7. Log Receiver

6. Click **Next**.
7. In **Log Type**, select **User Activity**.
8. In **Log Template**, select **JSON**.



Do not make any changes to the **Log Stream Content** field.

Figure 8. Log Stream

9. Click **Next**.
10. On the last page, click **Save**.
11. Repeat the process to add an additional Log Receiver, but this time, for **Log Type**, select **User Status**.

Creating a Zscaler Integration in the Armis Console

The following steps demonstrate how to create a Zscaler integration in the Armis console.

1. In the Armis console, go to **Settings** > **Integrations**.
2. Click **Connect Integration** and search for **Zscaler** in the **Firewall & NAC** category.

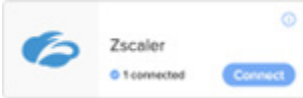


Figure 9. Connect integration

3. Click **Connect** to open the integration parameters.

Integrations > Library > Connect Zscaler Integration

Before You Start

Provide Access Details

Manage Data

Set Schedule

Name

Enter name

Before You Start

Prior to configuring this integration, please accomplish the prerequisites described at [Full Documentation > Prerequisites](#).

Provide Access Details

Zscaler Company ID

Zscaler Client Connector Dashboard API key Client ID ⓘ

Zscaler Client Connector Dashboard API key Secret. ⓘ

Test connection

Connect From

Select

Manage Data

☒ Mark Discovered Devices as Managed

☐ Import Traffic Logs ⓘ

Set Schedule

☒ Default interval: 1 Hour

☐ Custom Interval ⓘ

☐ Selected days of week ⓘ

[Full Documentation](#)

[About](#)

Figure 10. Connect Zscaler integration

4. In the **Name** field, enter the name that is displayed on the **Integrations** page in the Armis console.
5. In the **Provide Access Details** section, configure the following:
 - a. **Zscaler Company ID:** Paste the Company ID from the Company Profile. You can find the Company Profile by logging in to the ZPA Admin Portal and going to **Administration > Company Profile**.
 - b. **Zscaler Client Connector API Key Client ID:** Paste the API Key Client ID, which is your unique identifier required for authenticating API calls. See [Creating Zscaler API Keys](#).
 - c. **Zscaler Client Connector API Key Secret:** Paste the API Key Secret, which is the unique token used to authenticate the API Key. See [Creating Zscaler API Keys](#).



Click **Test connection** to verify the connection with the API before clicking the **Connect** button. Recommended actions are provided if an authentication error occurs.

- d. **Connect From:** Select the Armis collector on which the integration runs.
6. In the **Manage Data** section, select or clear the following checkboxes:
 - a. **Mark Discovered Devices as Managed:** This checkbox is enabled by default. It automatically labels every device that is returned by the integration as Managed.
 - b. **Import Traffic Logs:** Select this checkbox (not enabled by default) to automatically pull traffic logs for the ZPA integration. Currently, traffic logs for ZIA are not supported.
7. Click **Connect** to initialize the first-time analysis of Zscaler data sources. The analysis time might vary, depending on multiple factors, such as the number of devices and the network bandwidth.

When the integration is active, the green status indicator appears on the Integrations page.

The devices associated with Zscaler appear in the Armis inventory with the Zscaler icon in the Data Sources column. Hovering above the icon shows when the device was first and last seen.



<input type="checkbox"/>	Risk	Alerts	Name	Data Sources	Category	Type	Model	Brand
<input type="checkbox"/>	2 Low		desktop-aa0jo7m		Computers	Virtual Machines	VMware73	VMware
<input type="checkbox"/>	2 Low		device-6-g6mf	 Zscaler First seen: Jul 21, 2022 1:56 AM Last seen: Jul 21, 2022 1:56 AM	Computers	Personal Computers	MacBook Pro 16,2	Apple

Figure 11. Data Sources

Viewing Data Retrieved from Zscaler

To view Zscaler data, click a device name to open the single-device page.

The screenshot shows the Zscaler single-device page for a MacBook Pro 16,2. The page is divided into several sections:

- Left Sidebar:**
 - Device Name: MacBook Pro 16,2
 - Manufacturer: Apple
 - Risk: Low
 - Alerts: 0
 - Type / Category: Personal Computers, Computers
 - OS: macOS Version 12.3.1 (Build 21E258) ...
 - Data sources: [Icon]
 - IP: 10.200.1199, fe80::1417:6a75:406f:906
 - MAC: [Redacted]
 - Boundaries: + Associate Boundary
 - Tags: + Add Tag
 - Site: ...
 - Last Seen By: SPAN 8154 eth1 (test span)
 - First Seen: Jun 9, 2022 12:09 PM
 - Last Seen: Sep 6, 2022 4:00 AM
- Top Tabs:** Inventory (selected), Network, Alerts (0), Activities (480), Vulnerabilities (0), Risk Factors (2), Enforcements (0), Applications (16)
- Main Content Area:**
 - Identifiers:**
 - Name: [Redacted]
 - Serial Number: ...
 - Network Interfaces: (3 interfaces)
 - Zscaler User: [Redacted]
 - Profile:**
 - Type: Personal Computers
 - Category: Computers
 - Model: MacBook Pro 16,2
 - Brand: Apple
 - Product Level: 4.0
 - Status:**
 - Inventory Status: Managed
 - Zscaler VPN State: Disconnected
 - OS / Firmware:**
 - OS Name: macOS
 - OS Version: Version 12.3.1 (Build 21E258) x86
 - Other:**
 - Zscaler Policy Name: macOS Policy

Figure 12. Zscaler data

API Calls

To retrieve device information, Armis uses the Zscaler API and sends the following API calls:

API	Definition
POST /auth/v1/login	Authenticates to an API token.
GET /public/v1/getDevices	Fetches the devices.

Contextualizing Risk using Zscaler UVM and Armis

Zscaler'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.

Zscaler UVM offers the following preconfigured Armis connectors:

- Armis Devices: Retrieves information about the discovered devices, including their attributes and states.
- Armis CVE: Retrieves vulnerability data related to devices, including matched device details.

Required Parameters

The source authentication configuration requires the following parameters:

- API Token: Your generated API token.
- Armis Instance: The instance ID of your tenant.

Roles and Permissions

The supplied token must carry at least the following permission:

- Armis Devices: Device > Read
- Armis CVE: Vulnerability > Read

Retrieving the Parameters

The following sections describe retrieving parameters.

Retrieving the API Token

To retrieve your API token in the Armis Management Console, perform the following:

1. Go to **Settings > API Management**.

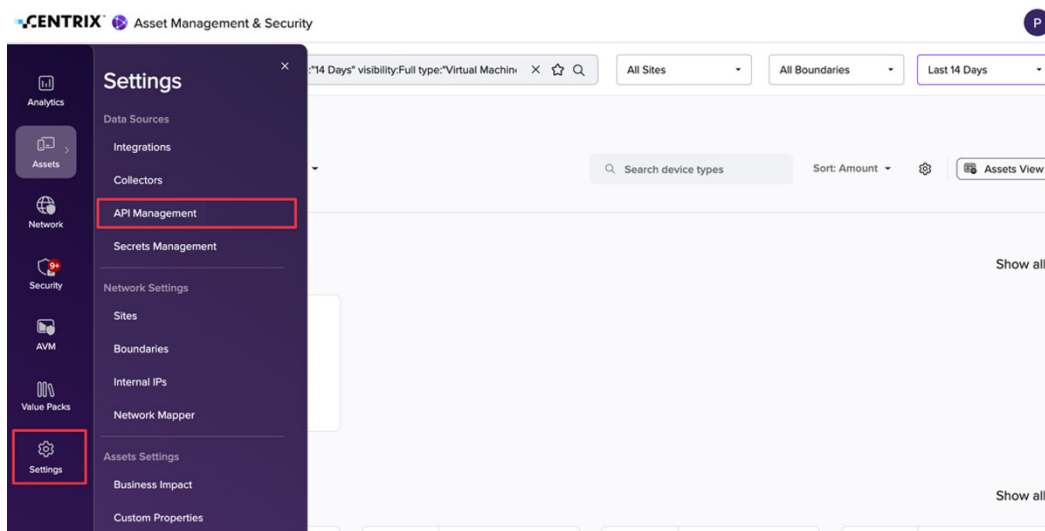


Figure 13. API Management

2. Click **Create**.

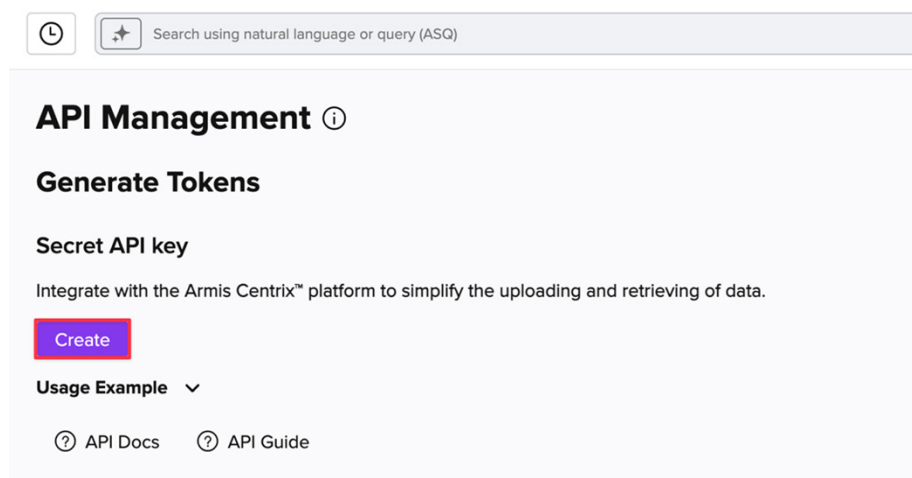


Figure 14. Create secret API key

3. Click **Copy** to copy your **API Secret Key**.

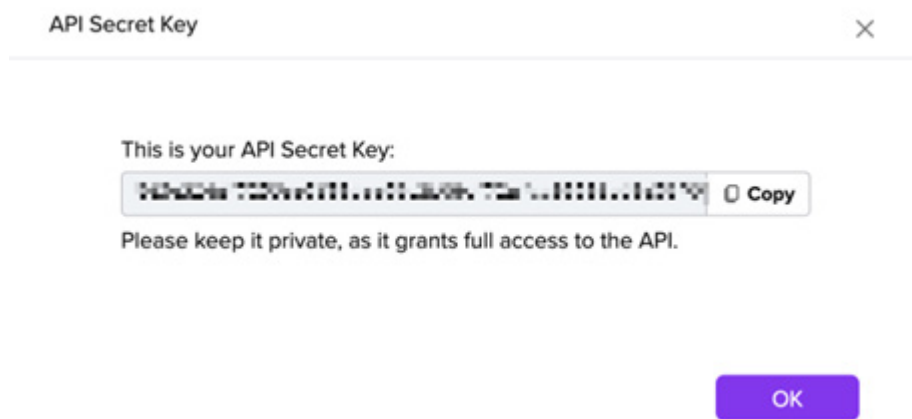


Figure 15. Secret API key

Retrieving the Armis Instance

You can find your Armis Instance in your Armis Management Console URL, in the format:

`https://<your-instance>.armis.com`

Configure the Zscaler UVM Data Connectors

The following sections describe how to configure the Zscaler UVM data connector.

Configure Authentication for the Armis Data Source

1. Log in to the Zscaler UVM Platform.
2. Click **Configure**.

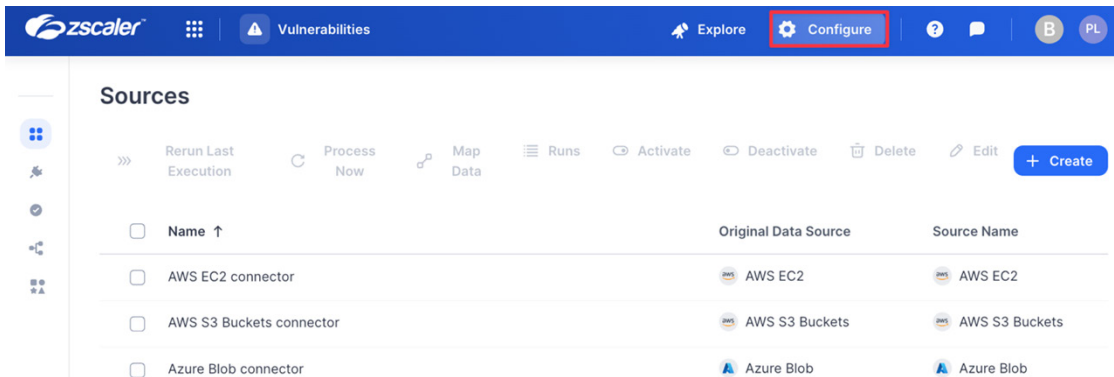


Figure 16. Configure

3. Click **Authentications**.

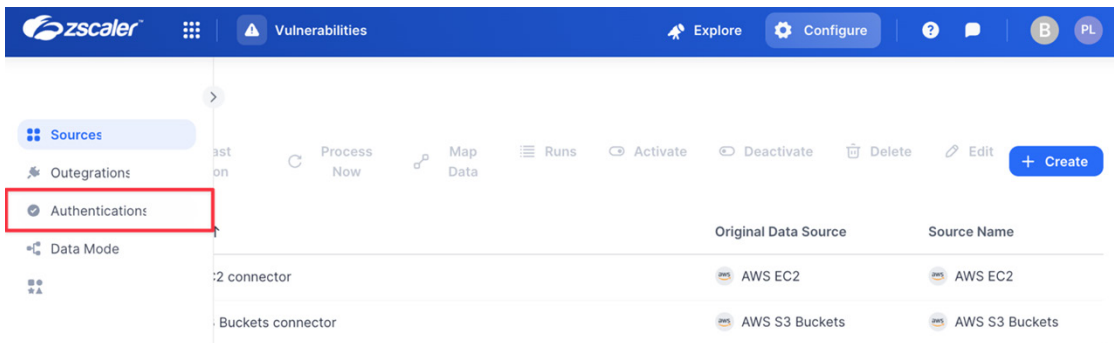


Figure 17. Authentications

4. Click **Create**, enter **Armis**, then click **Armis**.

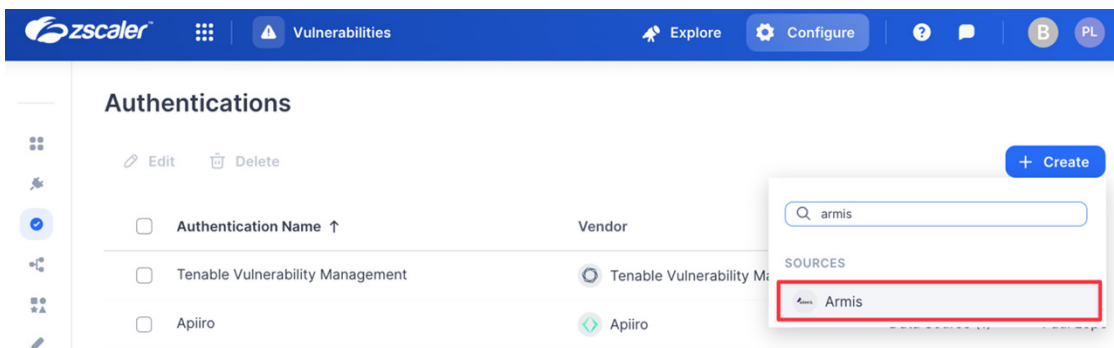
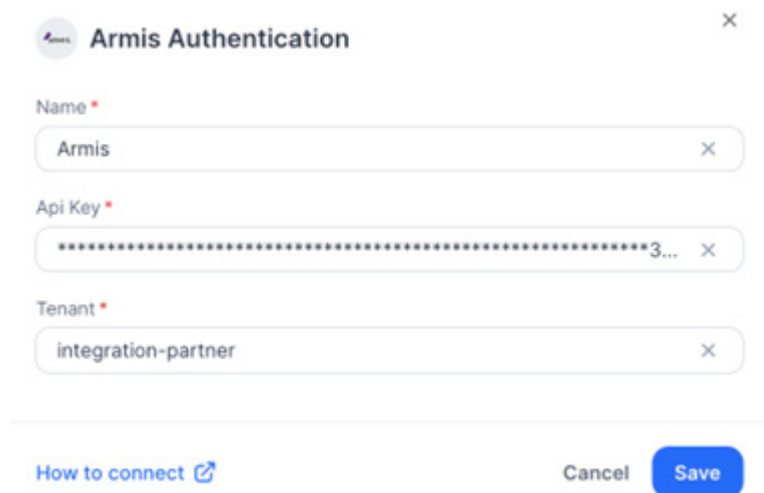


Figure 18. Add Armis authentication

5. Enter the following:
 - a. **Name:** Enter an authentication name (e.g., Armis).
 - b. **API Key:** Enter the API Key.
 - c. **Tenant:** Enter your tenant's name (e.g., `<your-instance>`).



Armis Authentication

Name *

Armis

Api Key *

*****3...

Tenant *

integration-partner

[How to connect](#) [Cancel](#) [Save](#)

Figure 19. Configure Armis Authentication

6. Click **Save**.

Configure the Armis Devices Data Source

1. Log in to the Zscaler UVM Platform.
2. Click **Configure**.

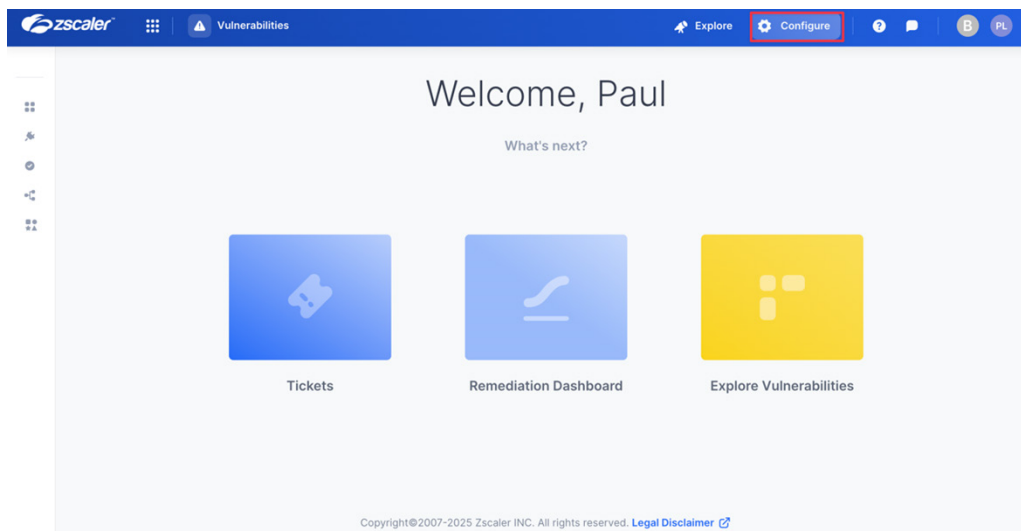


Figure 20. Configure

- Click **Create**, then search for Armis Devices.

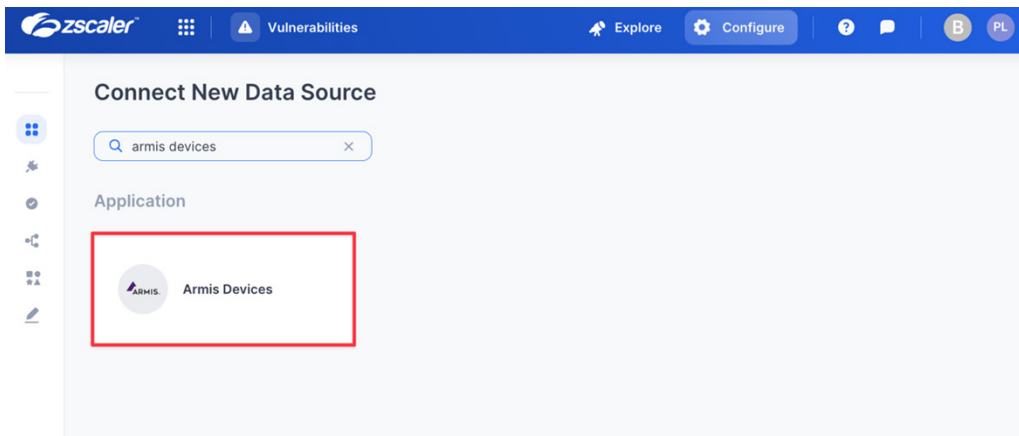


Figure 21. Connect New Data Source

- Click the **Armis Devices** application.
- On the **Create Armis Devices Source** page, complete the following:
 - Name:** Enter a name for the Data Connector.
 - Active:** Toggle the switch to enable the Data Connector.
 - Authentication:** Select the authentication source.
 - Days to Fetch:** Enter the number of days of data to fetch.
 - Full Refresh Frequency:** Set your desired schedule for extracting all data.
 - Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, see the [Zscaler documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - Suppression Rules:** Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, see the [Zscaler documentation](#).
- Click **Test**. If the API key and region have been entered correctly, the system responds with **Test Passed**.

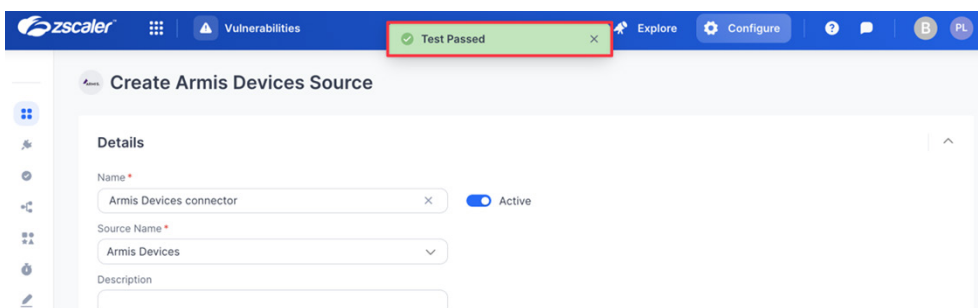


Figure 22. Test Passed

7. Click **Save**.

Create Armis Devices Source

Details

Name *
Armis Devices connector x Active

Source Name *
Armis Devices v

Description
v

Retrieval

Authentication *
Armis v + Create New

Days to Fetch
7 x

Scheduling

Full Refresh Frequency *
Daily v

Time (UTC) *
Auto: 02:00 AM v

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 + Add Rule
☐ Age immediately if Finding was not seen, while Asset was seen in the latest full data refresh

Fallback
☐ Age immediately if Finding was not seen for v day(s)

Advanced Settings

Suppression Rules

Configure suppression rules to exclude specific data before it is ingested into the platform ⓘ

Type
☒ Exclude Rows ☐ Include Rows

Select Field v Contains v v

+ AND + OR

☒ Prevent NULL from overriding existing values

Cancel Test **Save**

Figure 23. Create Armis Devices Services

Configure the Armis CVE Data Source

1. Log in to the Zscaler UVM Platform.
2. Click **Configure**.

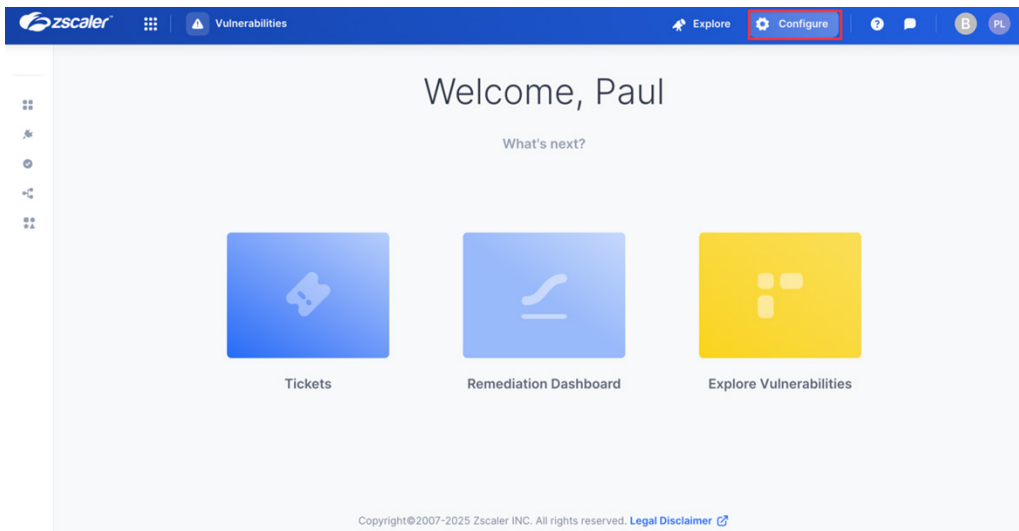


Figure 24. Configure

3. Click **Create**, then search for Armis CVE.

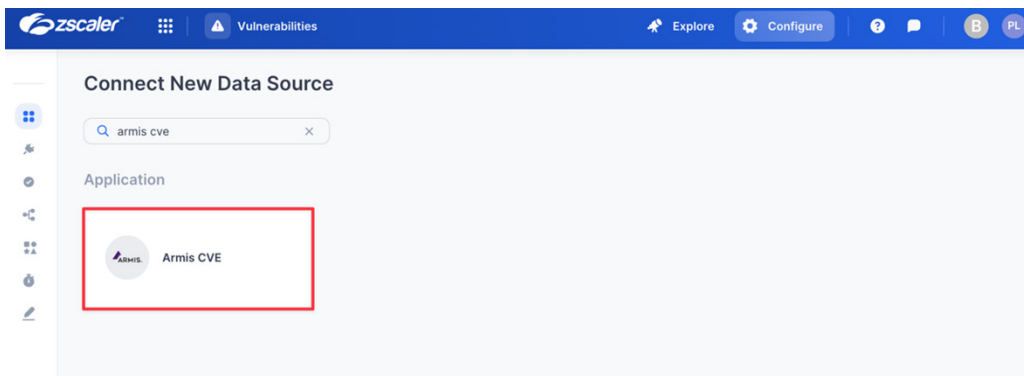


Figure 25. Connect New Data Source

4. Click the **Armis Devices** application.
5. On the **Create Armis Devices Source** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle the switch to enable the Data Connector.
 - c. **Authentication:** Select the authentication source.
 - d. **Full Refresh Frequency:** Set your desired schedule for extracting all data.
 - e. **Time:** Set the time for data extraction.
 - f. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, see the [Zscaler documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
 - g. **Suppression Rules:** Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, see the [Zscaler documentation](#).

6. Click **Test**. If the API key and region have been entered correctly, the system responds with **Test Passed**.

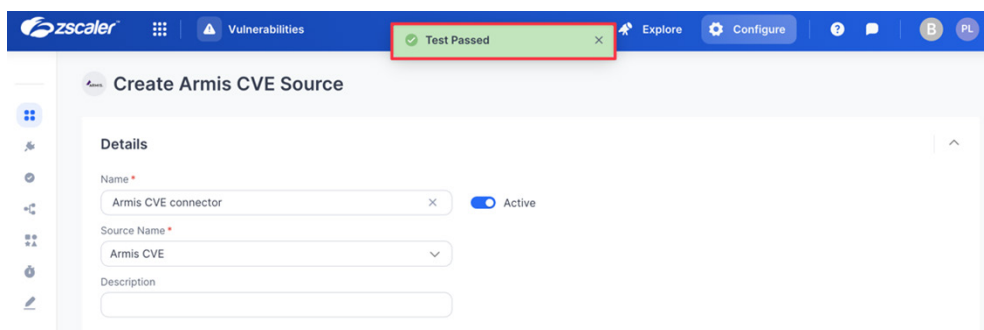


Figure 26. Test Passed

7. Click **Save**.

Create Armis CVE Source

Details

Name *
Armis CVE connector ☐ Active

Source Name *
Armis CVE

Description

Retrieval

Authentication *
Armis [+ Create New](#)

Scheduling

Full Refresh Frequency *
Daily

Time (UTC) *
Auto: 02:00 AM

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 [+ Add Rule](#)

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

Fallback

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

Advanced Settings

Suppression Rules

Configure suppression rules to exclude specific data before it is ingested into the platform

Type
☒ Exclude Rows ☐ Include Rows

Select Field Contains [+](#)

[+ AND](#) [+ OR](#)

☒ Prevent NULL from overriding existing values

Cancel Test **Save**

Figure 27. Create Armis CVE Source

Review and Adjust Risk Scoring

(Optional) Zscaler UVM automatically maps ingested data to its default Data Model, allowing you to start analysis immediately. However, your data source might contain extra context that can further refine risk prioritization.

After ingested data has been normalized and mapped to the Data Model, Zscaler UVM can evaluate risk.

The following example illustrates how to map the `avmRating` attribute from the Armis CVE data source as a Risk Factor for a Finding when assessing risk.

Map the Armis Data Source

To map the Finding/Key field to the id ingested data field:

1. Select **Configure > Armis CVE connector > Map Data**.

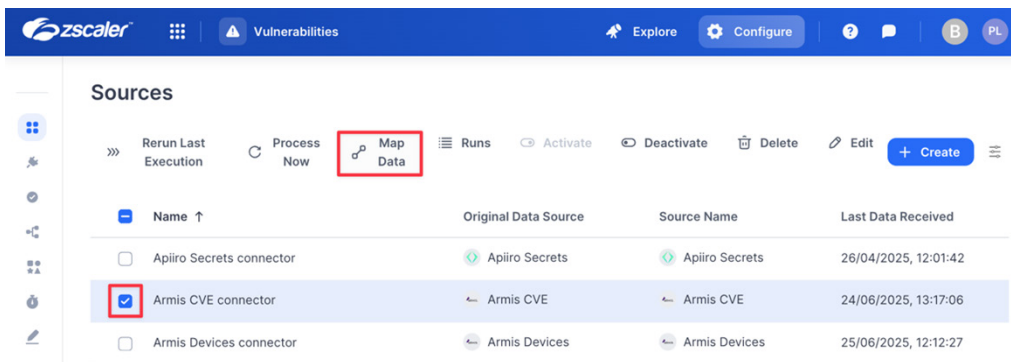


Figure 28. Sources

2. Map the **Finding/Key** entity to the `cveUid` field by:
 - a. On the right side, under **Finding**, drag **Key** to the **Create New Connection** element.
 - b. On the left side, click the `cveUid` field.

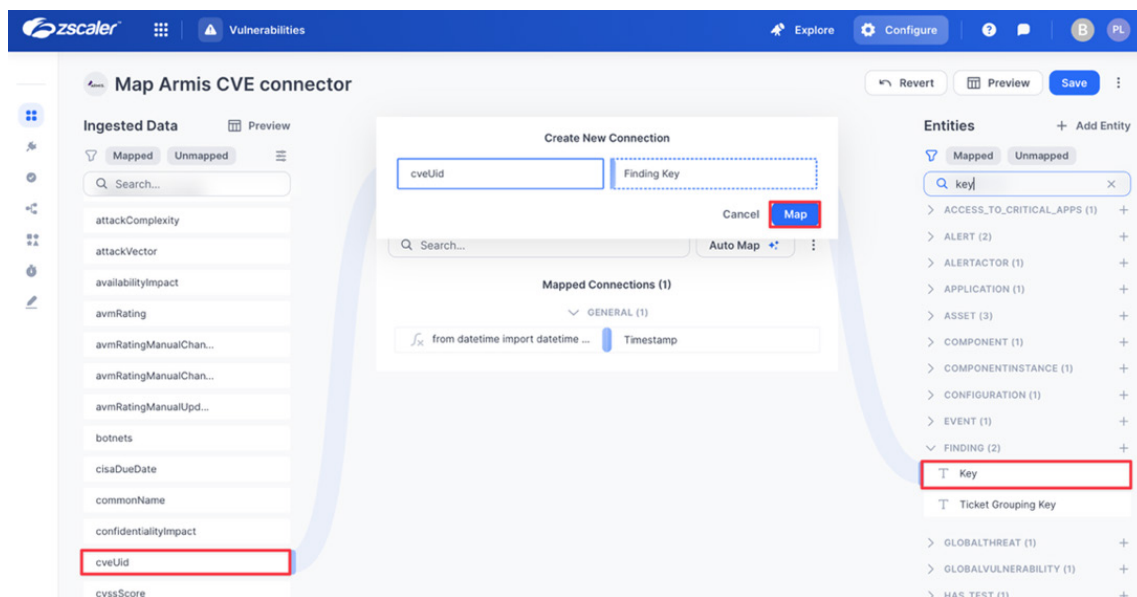


Figure 29. Finding/Key

- c. Click **Map**.
- d. Click the **Key** icon next to the **cveUid** -> **Key** mapping.

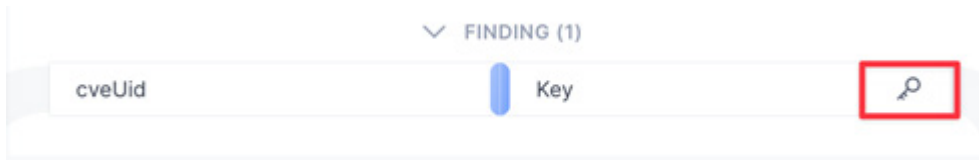


Figure 30. cveUid

3. Map the **Finding/Original Severity** entity to the **avmRating** field by:
 - a. On the right side, under **Finding**, drag **Original Severity** to the **Create New Connection** element.
 - b. On the left side, click the **avmRating** field.

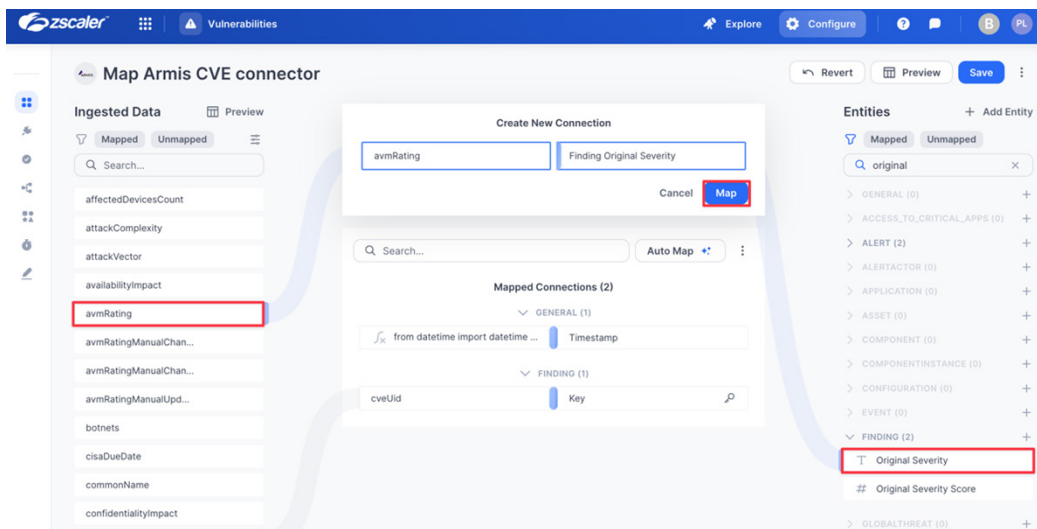


Figure 31. avmRating field

- c. Click **Map**.
4. Map the **Asset/Key** entity to **match_device/deviceId** by:
 - a. On the right side, under **Finding**, drag **Key** to the **Create New Connection** element.
 - b. On the left side, click the **match_device** item, then click on **deviceId**:

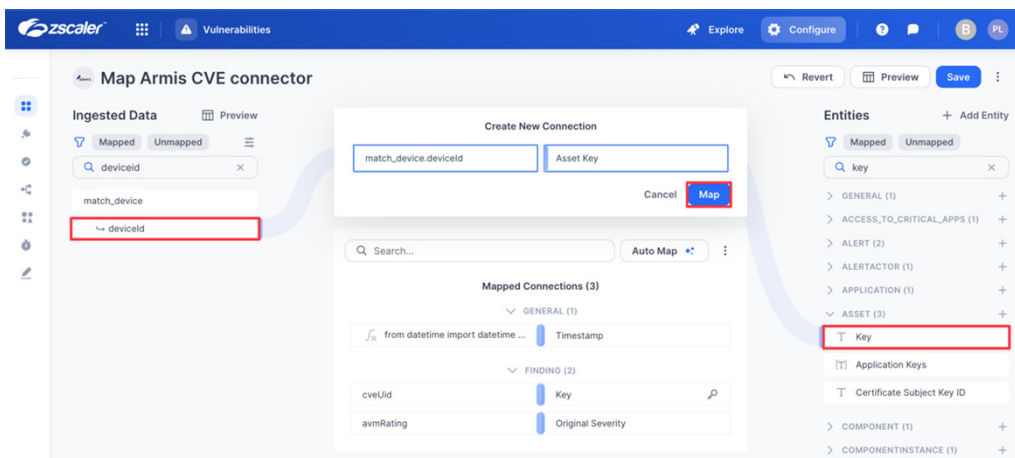


Figure 32. match_device/deviceId

- c. Click **Map**.
- d. Click the **Key** icon next to the `match_device.deviceId` -> **Key** mapping.

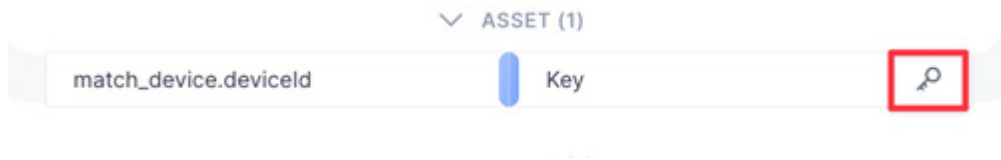


Figure 33. `match_device.deviceId`

5. Click **Back to Mapping**, then click **Save**.
6. On the **Sources** page, click **Process Now** > **Process Now** under your **Armris Data Source**.

Review and Adjust Risk Scoring

1. From the **Vulnerabilities** tab in the **Zscaler UVM dashboard (Remediation Hub)**:
 - a. In the left-side navigation, select **Settings** > **Score**.
 - b. Click **Add Factor** in the **Risk & Mitigating Factors** section.
2. In the **Add new factor** modal:
 - a. **Factor Type**: Select **Risk Factors** (Mitigating Factors generally lower risk scoring, while Risk Factors generally increase risk scoring).
 - b. **Factor Name**: Enter a name (e.g., `Finding Original Severity`).
 - c. **Field**: Choose **Finding Original Severity**.
 - d. **When Finding Original Servery Equals**: Enter `Critical` and enter a percentage by which the risk is increased. This example uses 10%.

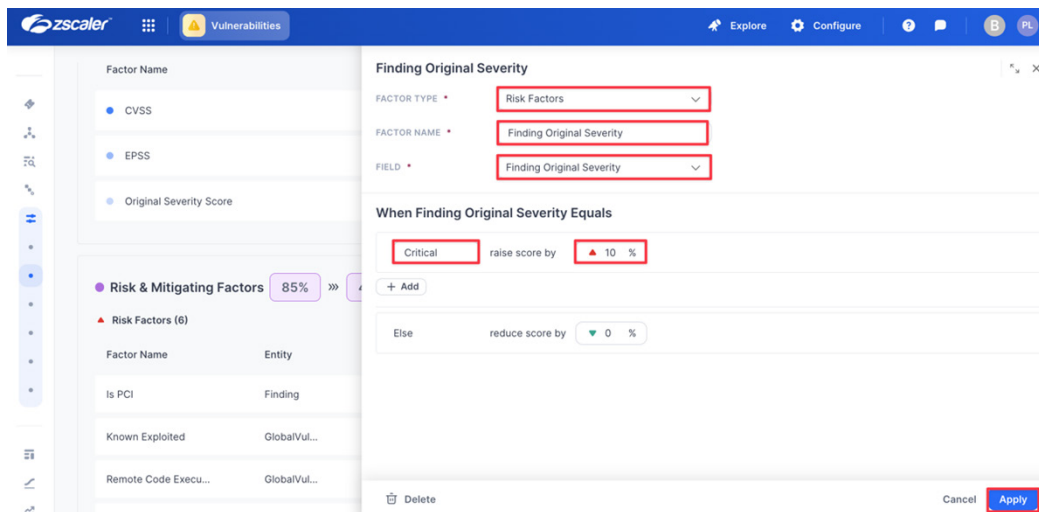


Figure 34. Add new factor

- e. Click **Apply**, then **Save & Run**.

3. In the left-hand pane, select the **Findings** dashboard. From the **Findings** dashboard:
 - a. Click **Source = Armis CVE**.
 - b. Click **Severity = Critical**.

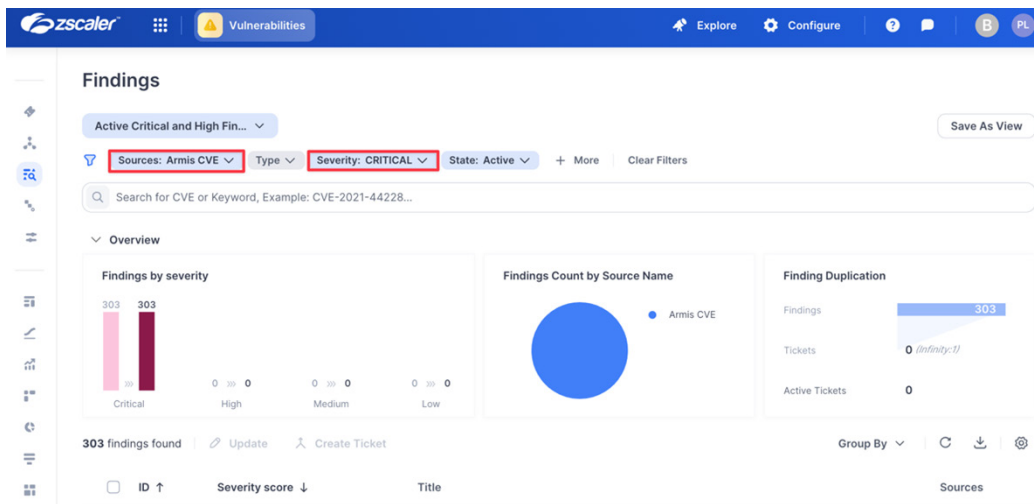


Figure 35. Findings

- c. Click one of your **Armis Findings** in the filtered list.
- d. In the **Finding** modal that appears, click the **Details** tab.
- e. Click the **Finding**.
- f. Review the output (notice the Score Adjustment section and how Finding Original Severity has modified the risk scoring).

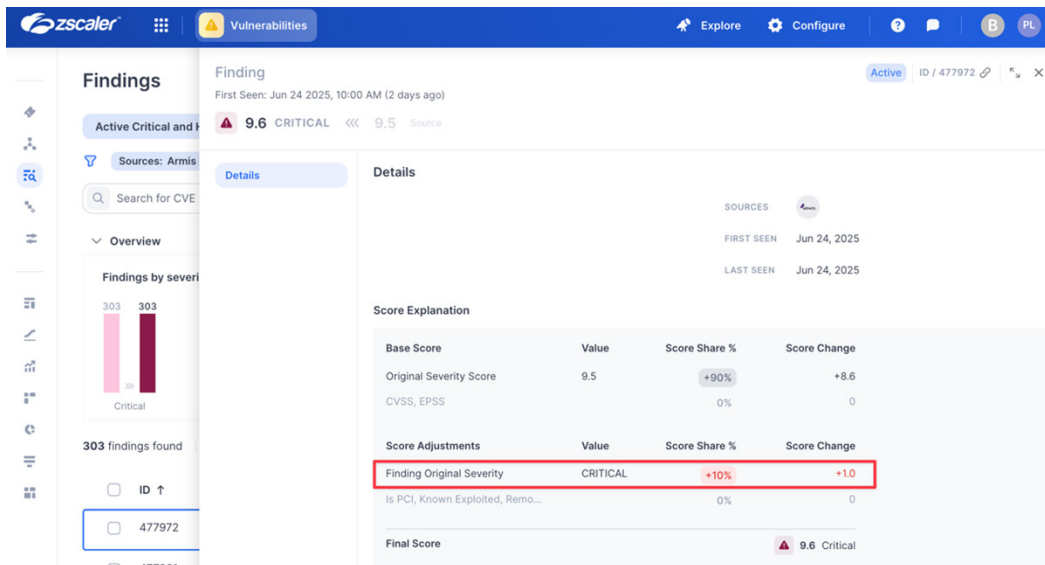


Figure 36. Details

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**.

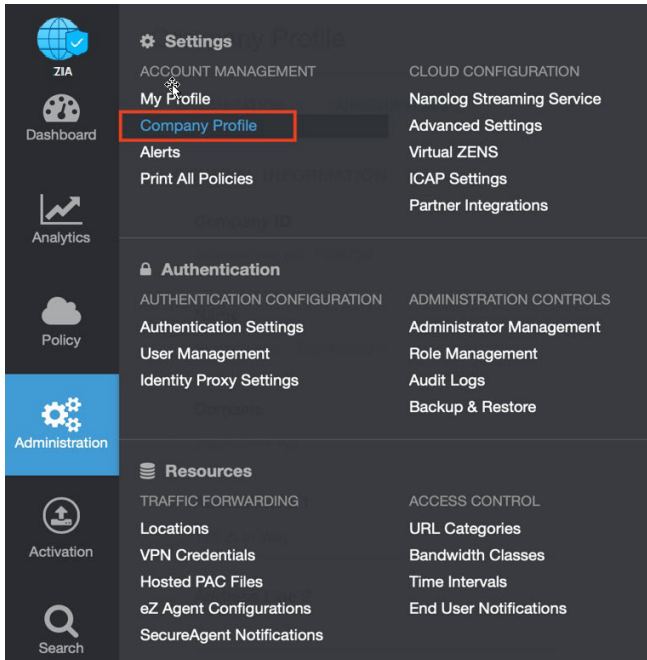


Figure 37. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

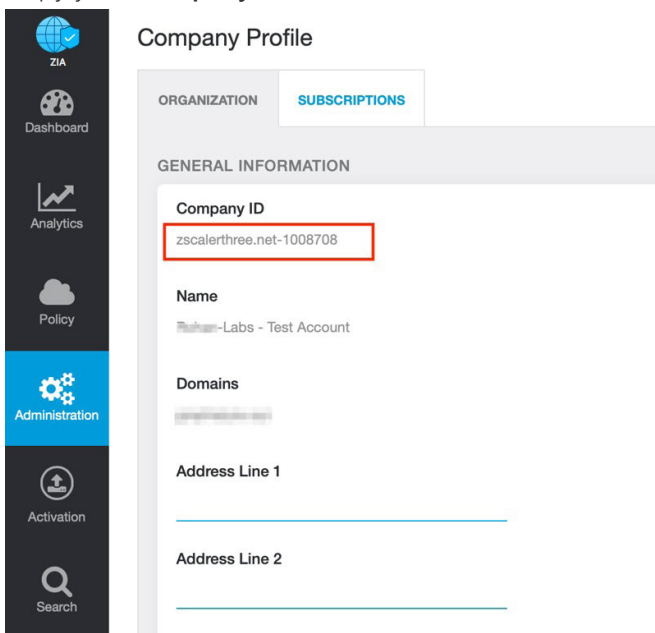


Figure 38. Company ID

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

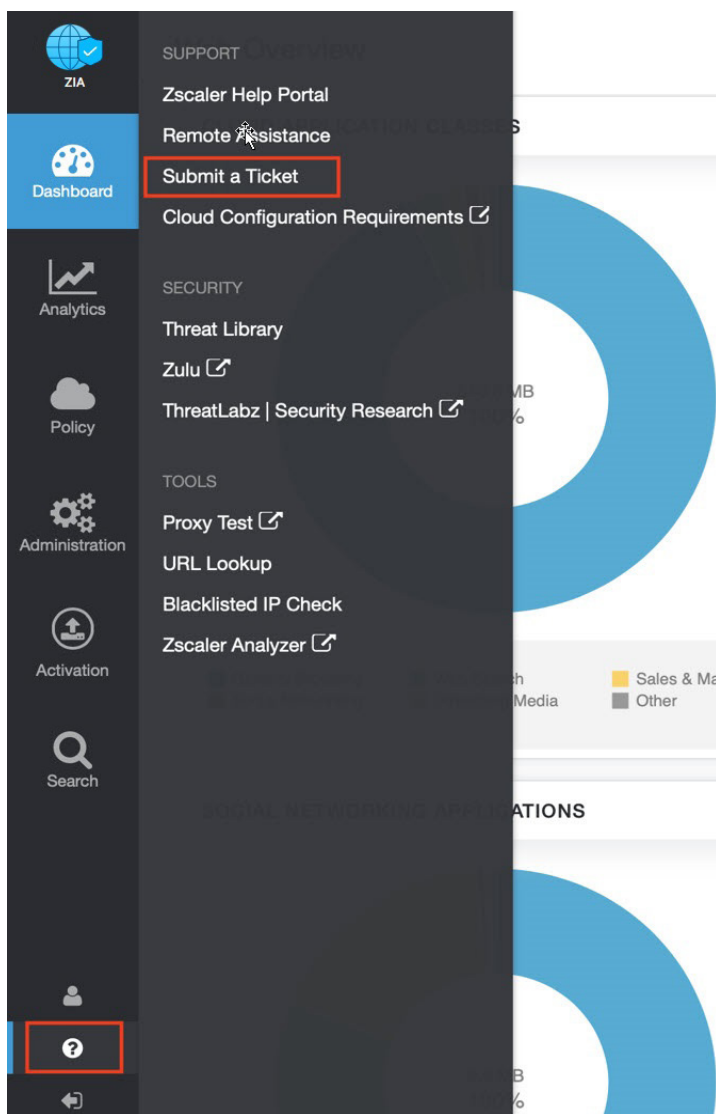


Figure 39. Submit a ticket