ZSCALER AND SNYK DEPLOYMENT GUIDE

APRIIL 2025, 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)
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
UVM	Unified Vulnerability Management
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (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.

Snyk Overview

Snyk is a leading developer security platform that helps organizations secure their applications from code to cloud. Founded in 2015 and headquartered in Boston and London, Snyk empowers developers to identify and fix vulnerabilities in open-source libraries, containers, infrastructure as code (IaC), and proprietary code early in the development lifecycle. With its developer-first approach and deep integration into CI/CD pipelines, Snyk provides real-time scanning, automated remediation, and continuous security monitoring, enabling teams to build securely without slowing down innovation. To learn more, refer to Snyk'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
- Snyk Resources
- Appendix A: Requesting Zscaler Support

Software Versions

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

Document Prerequisites

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

Zscaler UVM:

- An active instance of Zscaler UVM.
- Administrator login credentials to Zscaler UVM.

Snyk:

- An active Snyk tenant.
- Administrator login credentials to Snyk.

ZIA (Optional):

- An active instance of Zscaler Internet Access (ZIA).
- 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 Snyk Introduction

Overviews of the Zscaler and Snyk 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.

Zscaler UVM Overview

Zscaler Unified Vulnerability Management (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
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
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.

Snyk Overview

Snyk is an innovative, developer-first security platform designed to help organizations efficiently identify, prioritize, and remediate risks across the software development lifecycle. Leveraging Snyk's seamless integrations and automated scanning capabilities, the platform provides deep visibility into vulnerabilities in open-source dependencies, containers, infrastructure as code, and proprietary code.

With advanced features like real-time feedback in development environments, policy-driven governance, and native integration with CI/CD and DevOps workflows, Snyk empowers developers and security teams to collaborate effectively and address critical risks early and often. By delivering actionable insights, automated fixes, and comprehensive reporting, Snyk simplifies the security lifecycle and helps organizations maintain a secure and scalable cloud-native application stack.

Snyk Resources

The following table contains links to Snyk support resources.

Name	Definition
Snyk Documentation	Snyk help documentation and support.
Snyk Support	Snyk support community.

Contextualizing Risk Using Zscaler Unified Vulnerability Management and Snyk

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 pre-configured Snyk connectors:

- Snyk Connector: Retrieves Software Composition Analysis (SCA) vulnerabilities discovered in your project dependencies.
- Snyk SAST Connector: Static Application Security Testing (SAST) retrieves potential vulnerabilities discovered by analyzing your source code.

Required Parameters

The source authentication configuration requires the following parameters:

- API Token: The API token used for setting up an API source depends on your Snyk plan. If you're on an Enterprise plan, Zscaler recommends using a service account to generate the token. When setting up the service account, ensure it has at least an Org Collaborator role or higher. If you're on a non-Enterprise plan, you can continue using a personal API key.
- Org ID: Your organization ID.

Retrieving the Parameters

The following sections describe retrieving the parameters.

Locate your API Key

To generate an API Key using a Service Account in the Snyk Web UI:

1. In the Snyk Web UI, click your **username**.
2. Go to **Account Settings** > **Service accounts**.
3. Complete the following
   a. **Name**: Enter the Service Account Name.
   b. **Role**: Select **Org Collaborator**.
   c. **Service Account Type**: Select **API Key (no expiry)**.

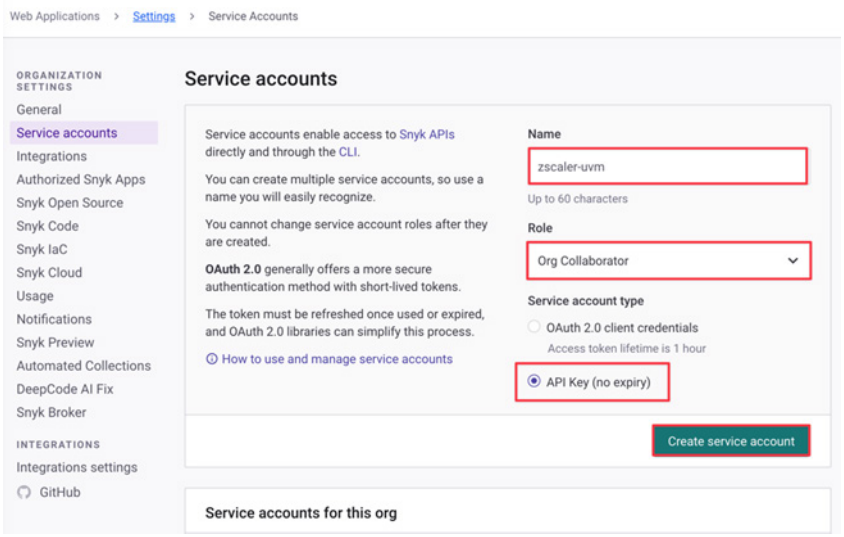

Figure 1. Service accounts

4. Click **Create service account**.
5. Copy the **API Key**.

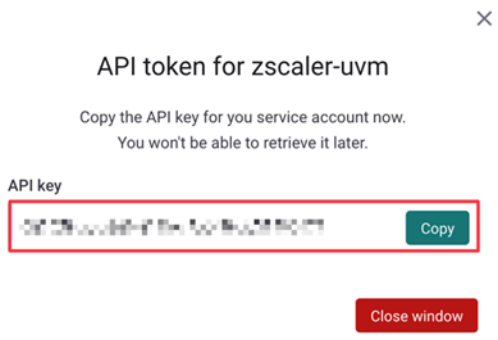

Figure 2. API key

Retrieving the Org ID

To retrieve your Org ID from the Snyk Web UI:

1. In your Snyk Web UI, click your **username**.
2. Under **Organization Settings**, select **General**.
3. Copy your **Organization ID**.

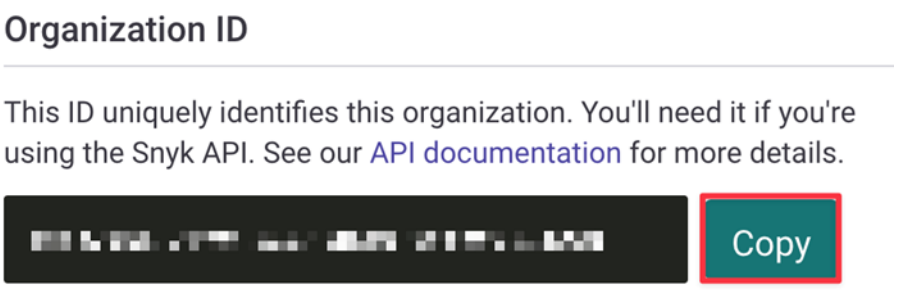

Figure 3. Organization ID

Configure the Zscaler UVM Data Connectors

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

Configure Authentication for the Snyk Data Sources

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

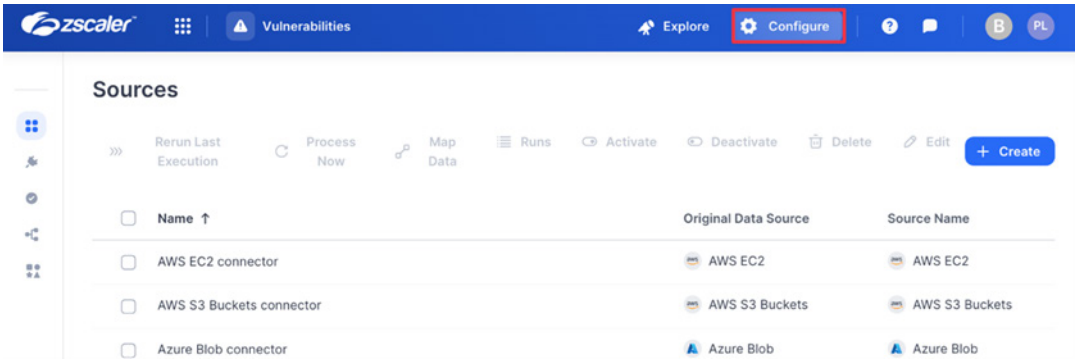

Figure 4. Configure

3. Click **Authentications**.

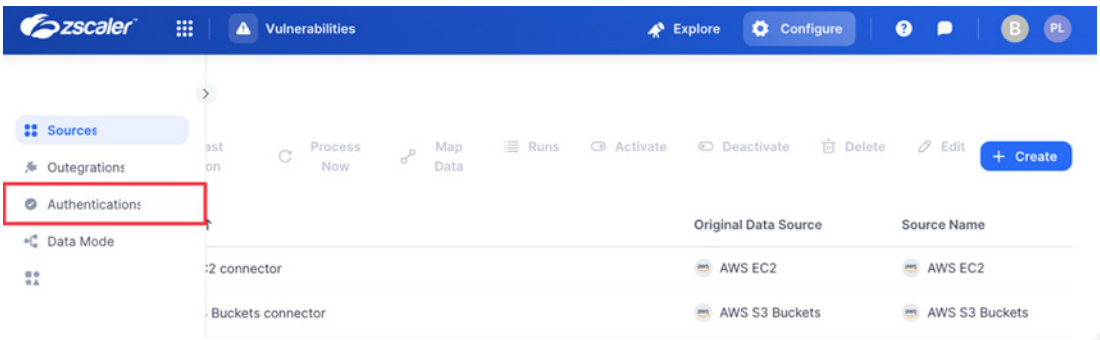

Figure 5. Authentications

4. Click **Create**, enter `Snyk`, then click **Snyk**.

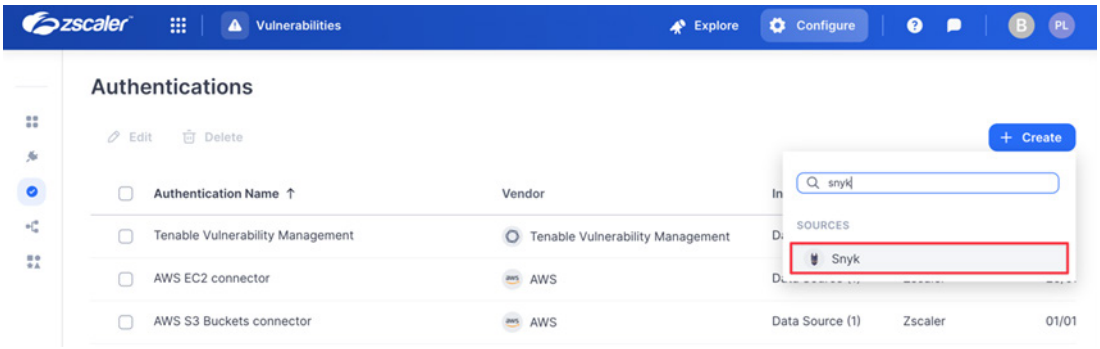

Figure 6. Add Snyk authentication

5. Enter the following:
   a. **Name**: Enter an authentication name (e.g., `Snyk`).
   b. **Token**: Enter the API Token from the previous step.
   c. **Org Id**: Enter the Org ID from the previous step.
6. Click **Create**.

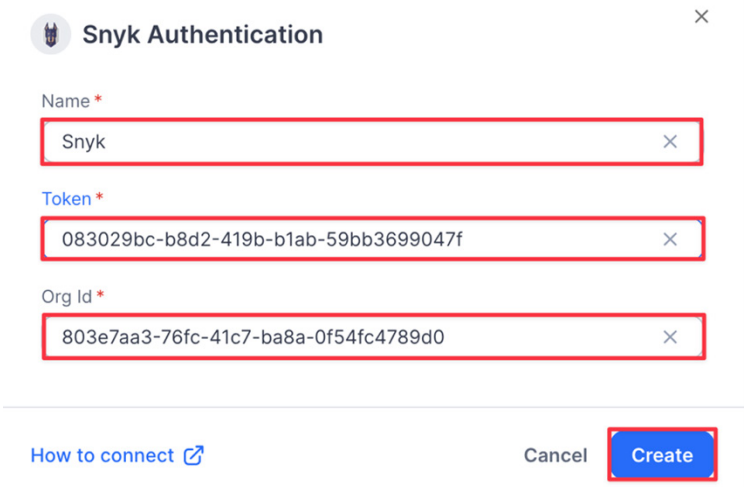

Figure 7. Configure Snyk authentication

Configure the Snyk Data Source

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

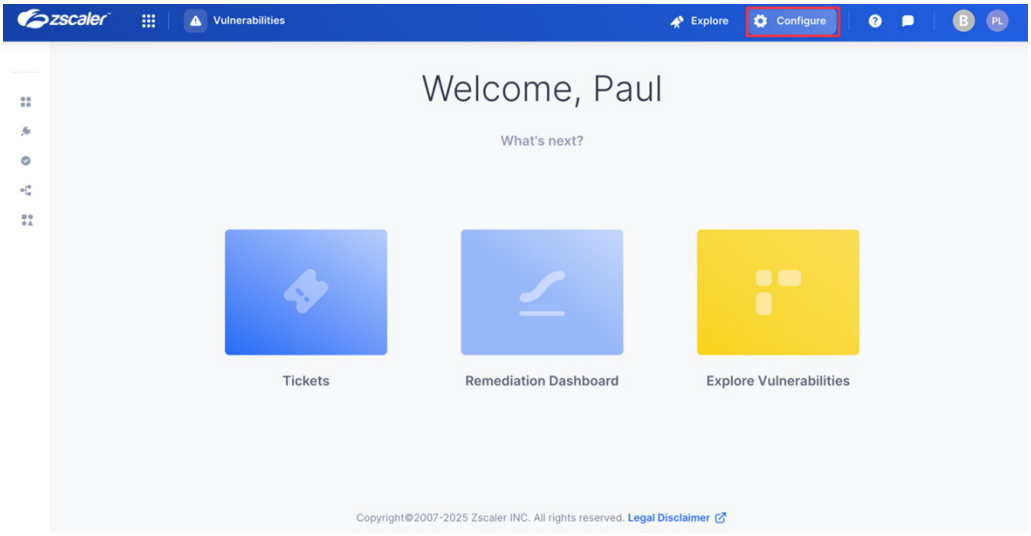

Figure 8. Configure

3. Click **Create**, then search for `Snyk`.

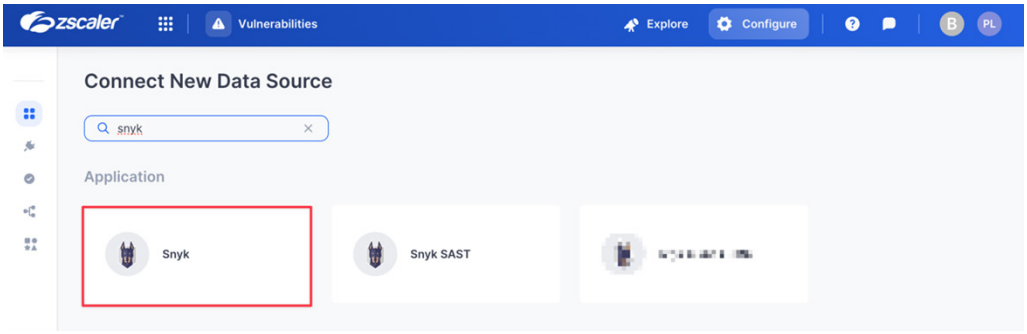

Figure 9. Connect New Data Source

4. Click the **Snyk** application.

5. On the **Create Snyk 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 sources created previously.
   d. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   e. **Aging Criteria/Fallback**: Select your desired option to determine when findings automatically turn to undetected. For more information, refer to the **UVM documentation**. Automatic remediation detection only applies when data is refreshed fully, not incrementally.
   f. **Suppression Rules**: Define rules and conditions to remove specific data before it enters the Zscaler UVM system. For more on suppression rules, refer to the **UVM documentation**.
   g. **Click Test**. If the API key and region have been entered correctly, the system responds with `Test Passed`.

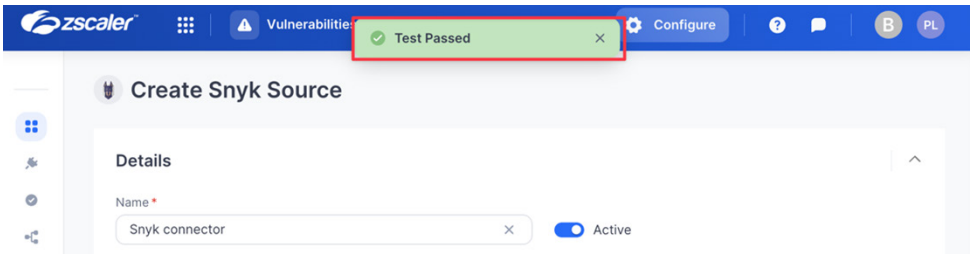

Figure 10. Test Passed

6. Click **Save**.

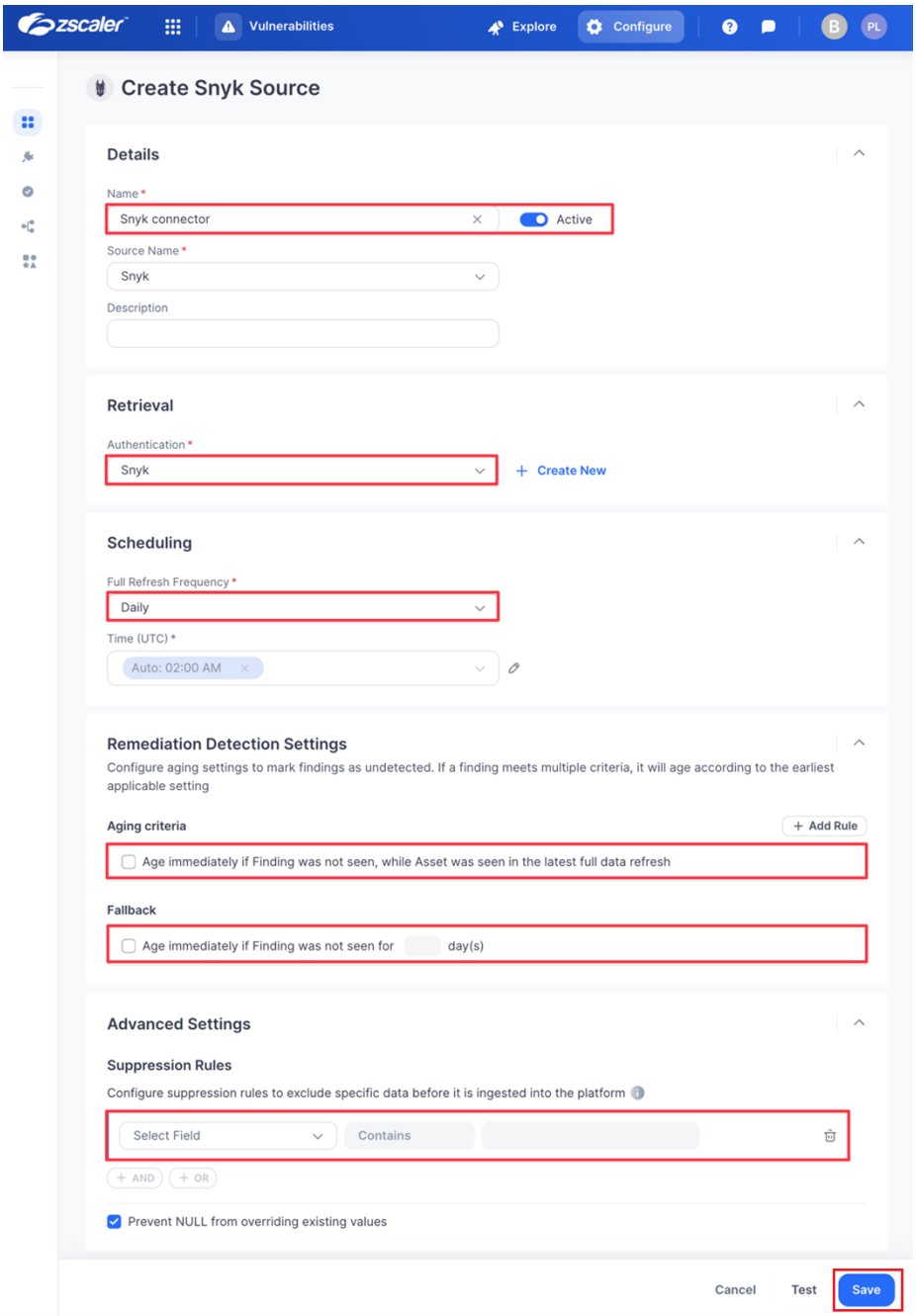

Figure 11. Create Snyk Source

Configure the Snyk SAST Data Source

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

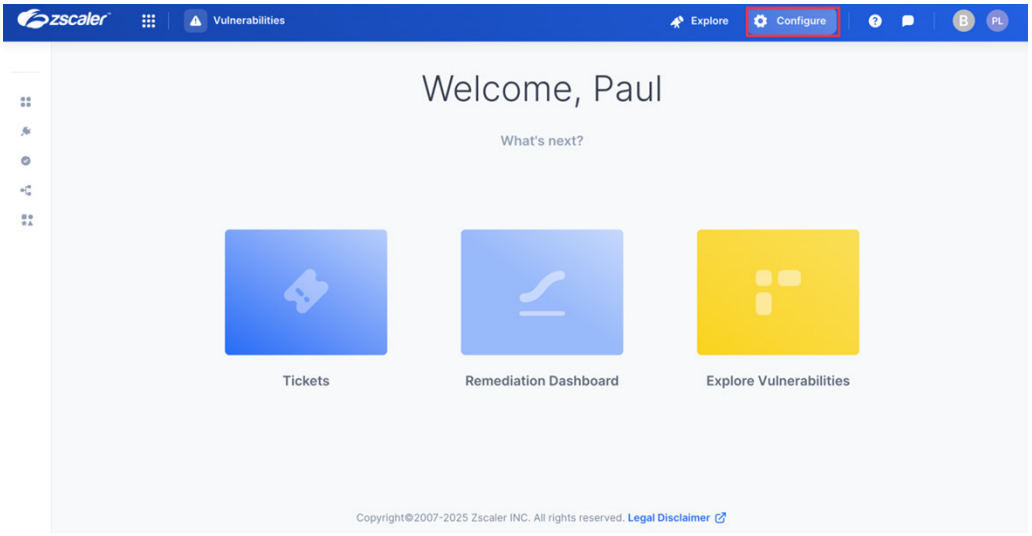

Figure 12. Configure

3. Click **Create**, then search for `Snyk SAST`.

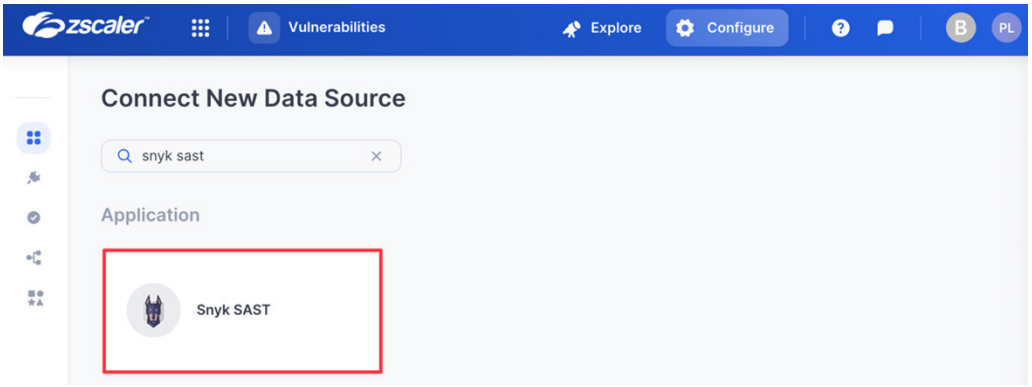

Figure 13. Connect New Data Source

4. Click the **Snyk SAST** application.

5. On the **Create Snyk SAST 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 sources created previously.
   d. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   e. **Aging Criteria/Fallback**: Select your desired option to determine when findings automatically turn to undetected. For more information, refer to the **UVM documentation**. Automatic remediation detection only applies when data is refreshed fully, not incrementally.
   f. **Suppression Rules**: Define rules and conditions to remove specific data before it enters the Zscaler UVM system. For more on suppression rules, refer to the **UVM documentation**.
   g. **Click Test**. If the API key and region have been entered correctly, the system responds with `Test Passed`.

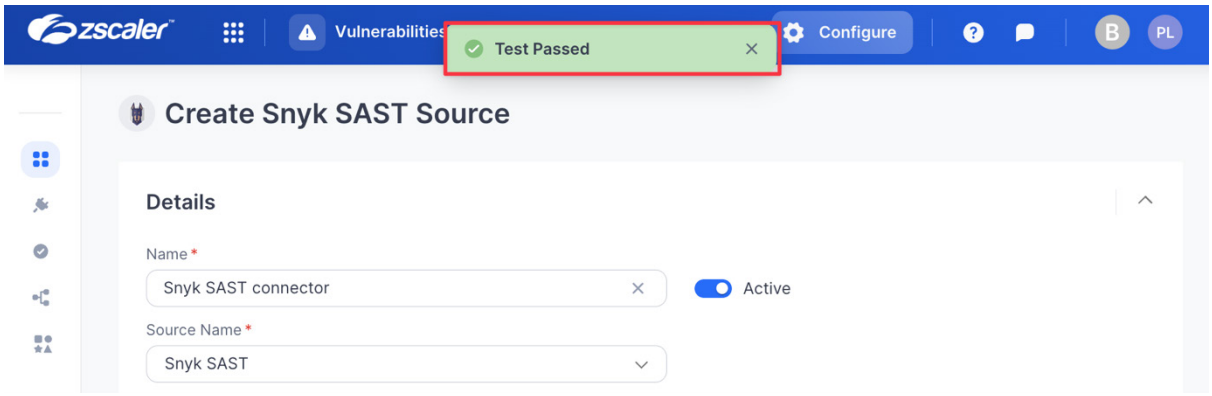

Figure 14. Test Passed

6. Click **Save**.

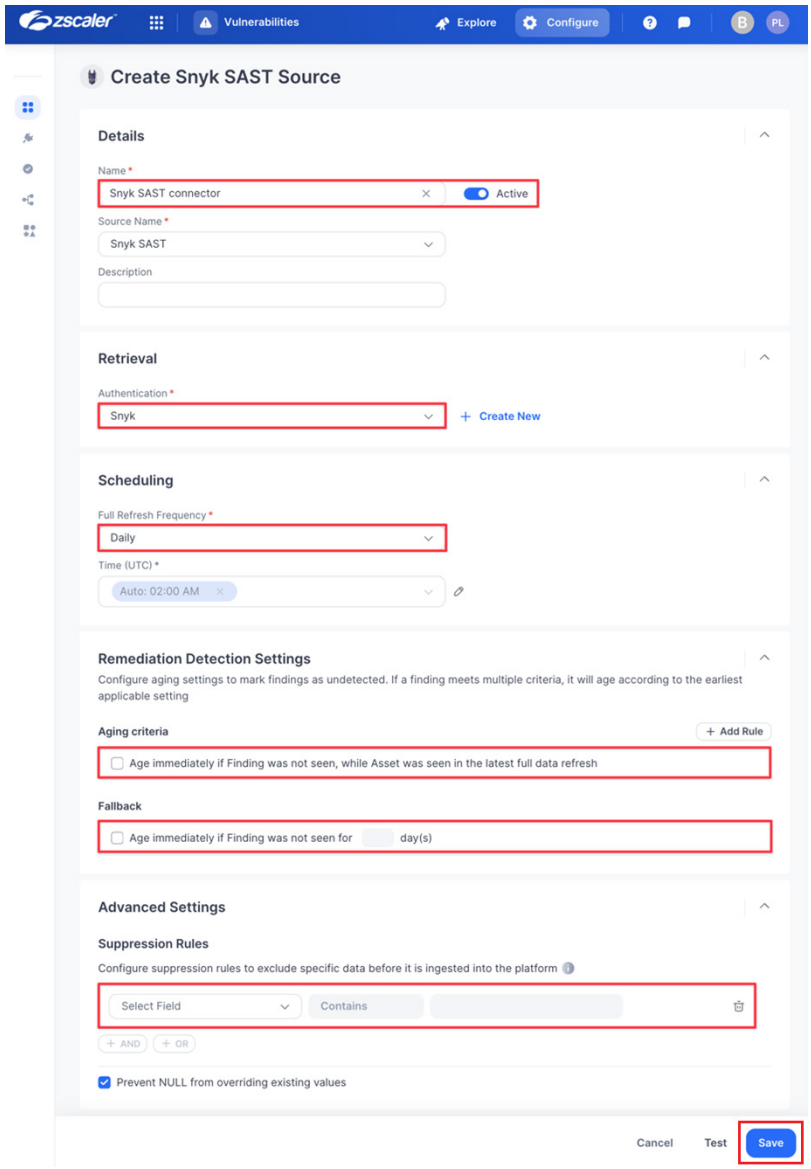

Figure 15. Create Snyk SAST Source

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 evaluates risk.

The following example illustrates how to map the is_fixable attribute from the Snyk data source as a mitigating factor for a Finding when assessing risk.

1. From the **Vulnerabilities** tab in the **Zscaler UVM dashboard (Remediation Hub)**:
   a. In the left-side navigation, go to **Settings** > **Score**.
   b. Click **Add Factor** in the **Risk & Mitigating Factors** section.
2. In the **Add new factor** modal:
   a. **Factor Type**: Select **Mitigating Factors** (Mitigating Factors generally lower risk scoring, while Risk Factors generally increase risk scoring).
   b. **Factor Name**: Enter a name.
   c. **Field**: Choose **Finding Is Fixable**.
   d. **When Finding is Fixable Equals**: Under **True**, enter a percentage by which the risk is reduced. This example uses 10%.

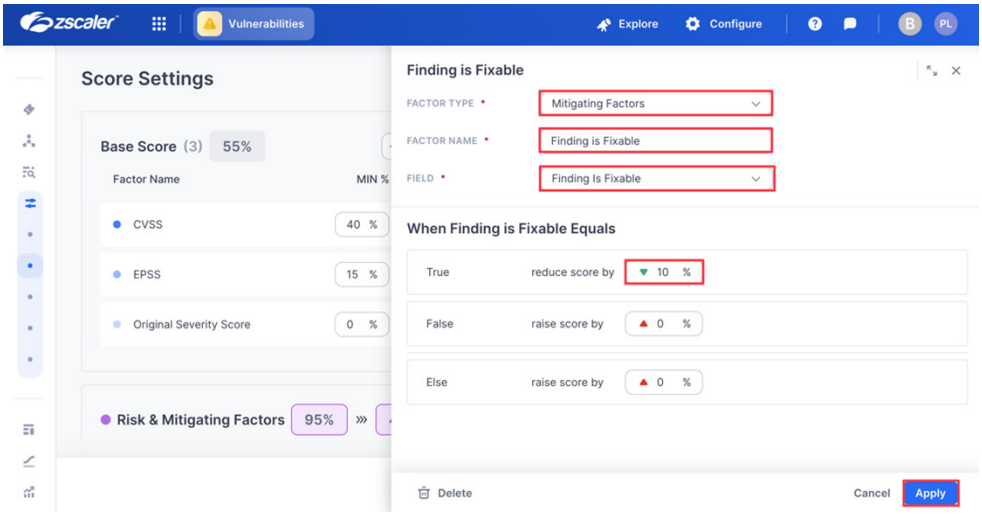

Figure 16. Score Settings

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

3. In the left-side navigation, select the **Findings** dashboard.
4. From the **Findings** dashboard:
   a. Set a filter by clicking **More** and adding the **Finding Is Fixable = True Entity**.

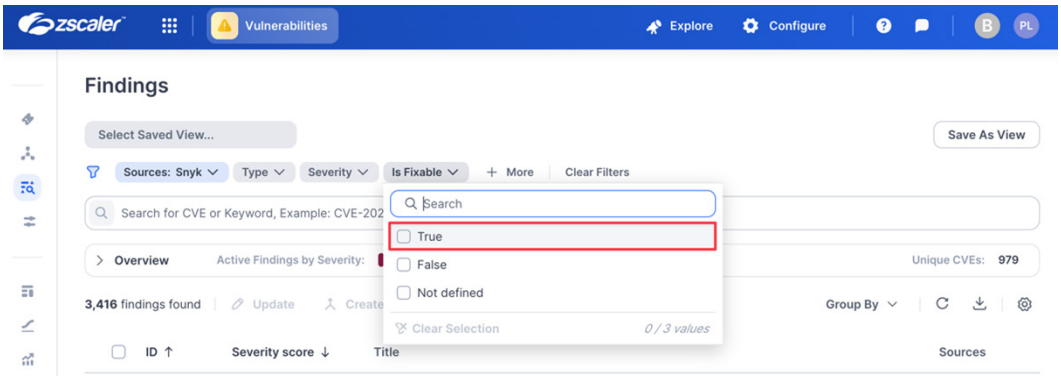

Figure 17. Findings

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

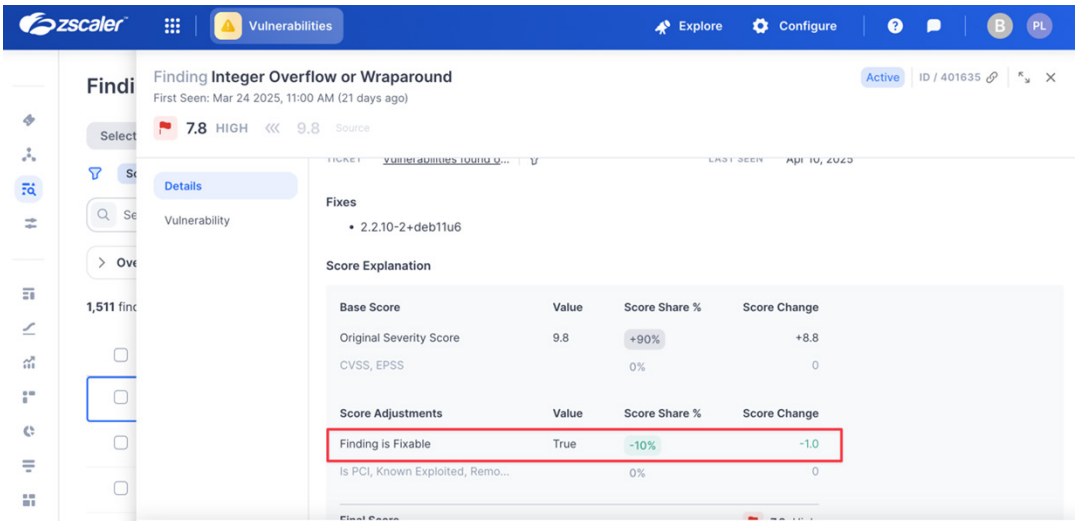

Figure 18. Details

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 UVM Support:

1. Log in to the Zscaler UVM Platform.

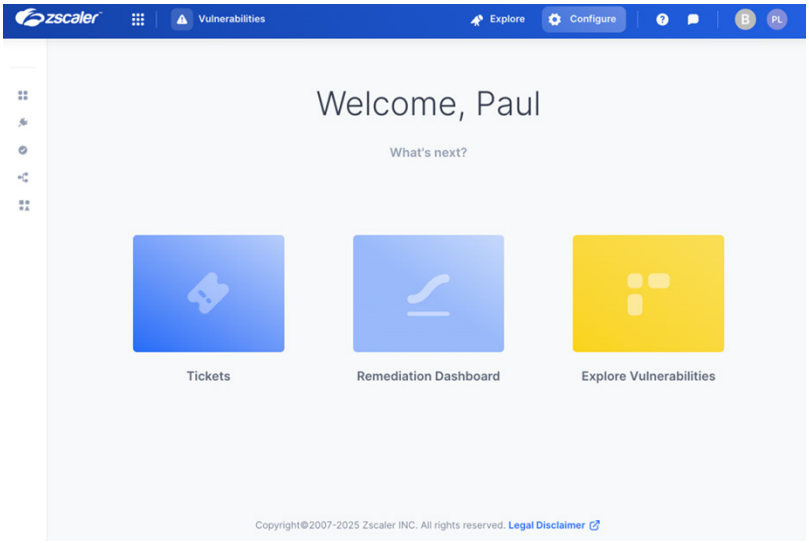

Figure 19. Zscaler UVM Platform

2. Click **Contact Support**.

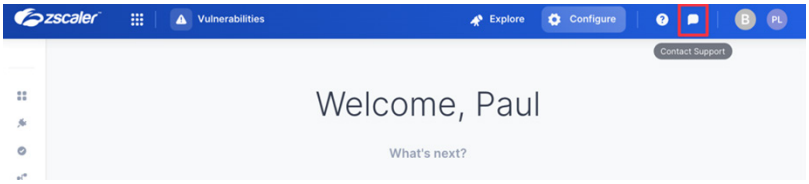

Figure 20. Contact Support

3. Complete the details in the **Contact us** form and click **Send**.

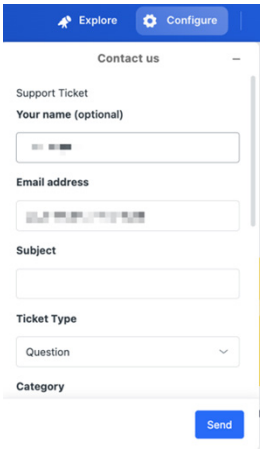

Figure 21. Contact us

