ZSCALER AND ORCA SECURITY DEPLOYMENT GUIDE

FEBRUARY 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
CVE	Common Vulnerabilities and Exposures
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)
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.

Orca Security Overview

Orca Security is an agentless cloud security platform that provides comprehensive protection across various cloud environments, including AWS, Azure, Google Cloud, and Kubernetes. Founded in 2019, Orca Security offers a unified solution that identifies, prioritizes, and remediates risks and compliance issues within cloud workloads, configurations, and identities. To learn more, refer to Orca Security'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
- Orca Security Resources
- Appendix A: Requesting Zscaler Support

Software Versions

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

Document Prerequisites

Make sure the following prerequisites are met:

Zscaler UVM:

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

Orca Security Vulnerability Management:

- An active instance of Orca Security.
- Administrator login credentials to Orca Security.

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 Orca Security Introduction

Overviews of the Zscaler and Orca Security 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, Zscaler 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.

Orca Security CNAPP Overview

Orca Security provides an agentless cloud security platform that protects AWS, Azure, Google Cloud, and Kubernetes environments. Their Cloud-Native Application Protection Platform (CNAPP) integrates multiple security functions, including Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), Cloud Infrastructure Entitlement Management (CIEM), Data Security Posture Management (DSPM), and API Security. The platform ensures compliance management with 100+ frameworks and uses AI-driven threat detection. Its patented SideScanning technology enables deep visibility without agents, simplifying deployment, and reducing operational overhead.

Orca Security Resources

The following table contains links to Orca Security support resources.

Name	Definition
Orca Security Documentation	Orca Security Documentation.
Orca Security Support Portal	Support for Orca Security.

Contextualizing Risk Using Zscaler UVM and Orca Security

The Zscaler 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 connectors for Orca Security:

- Orca Alerts
- Orca CVE
- Orca Assets
- Orca Vulnerabilities

The following steps outline how to start ingesting data from these sources, while also (optionally) combining Orca Vulnerabilities data with AWS EC2 tag information to provide a more contextualized and personalized risk assessment for your organization.

Retrieve Your Region and Generate an API Token from the Orca Security Portal

Orca Security uses both an API Token and URL for connectivity. The URL needed for connectivity contains a region identifier. To retrieve your region identifier:

1. Go to the **Orca Security Portal**.
2. Click the login icon and select your region.

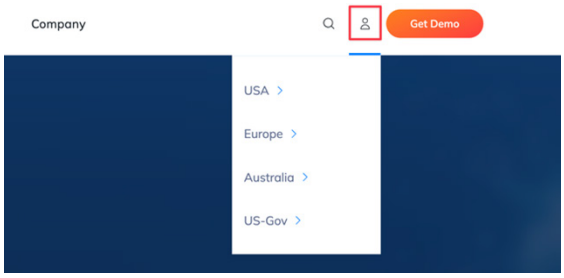

Figure 1. Region

3. Note your region mapping, which you must configure the Orca Security Connectors in Zscaler UVM from the above FQDN. The mappings are:

Region	Mapping
USA	us
Europe	eu
Australia	au
US-Gov	us.gov

4. Click your **Username** and **Manage Profile**.
5. Select **Users & Permissions** > **API**.

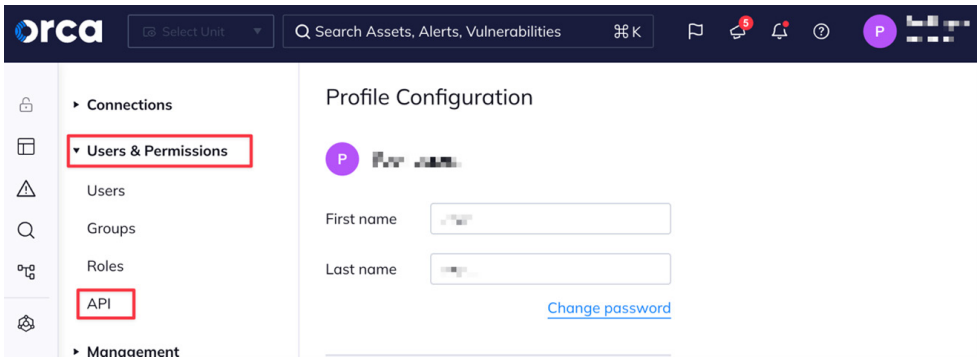

Figure 2. API

6. Click **+ Add API Token**, then fill out the details ensuring the role is **Viewer** or **Administrator**.

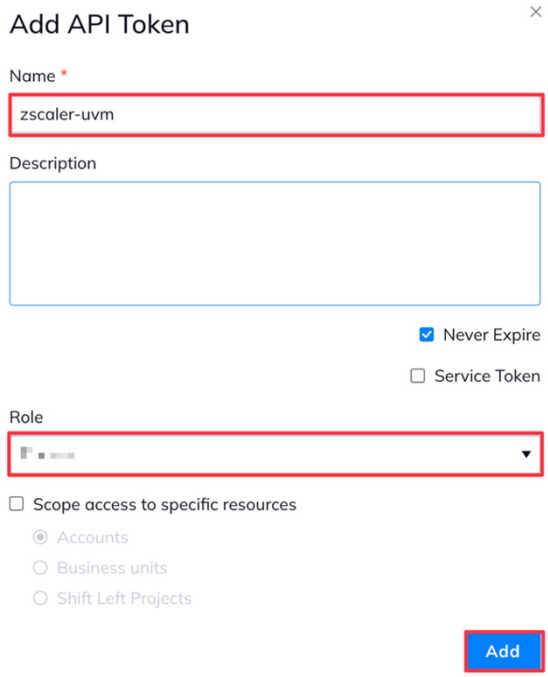

Figure 3. Add API Token

7. Copy the generated **API Token**.

Figure 4. Integration API token

Configure the Zscaler UVM Data Connectors

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

Configure Authentication for the Orca Security Data Sources

To configure the Orca Security data source:

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

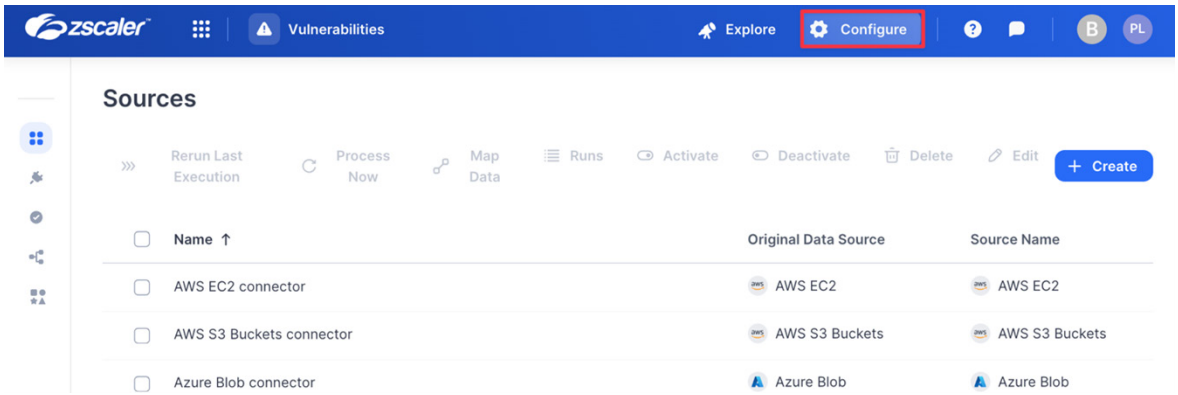

Figure 5. Configure

3. Click **Authentications**.

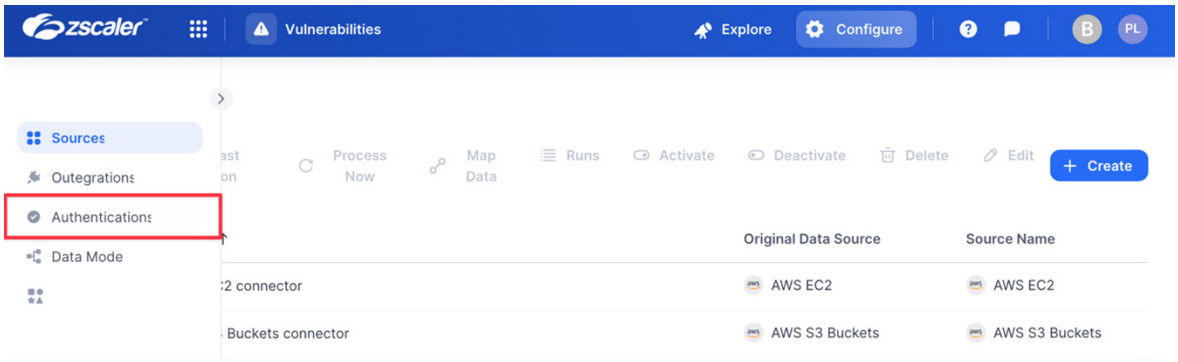

Figure 6. Authentications

4. Click **+ Create**, then click **Orca**.

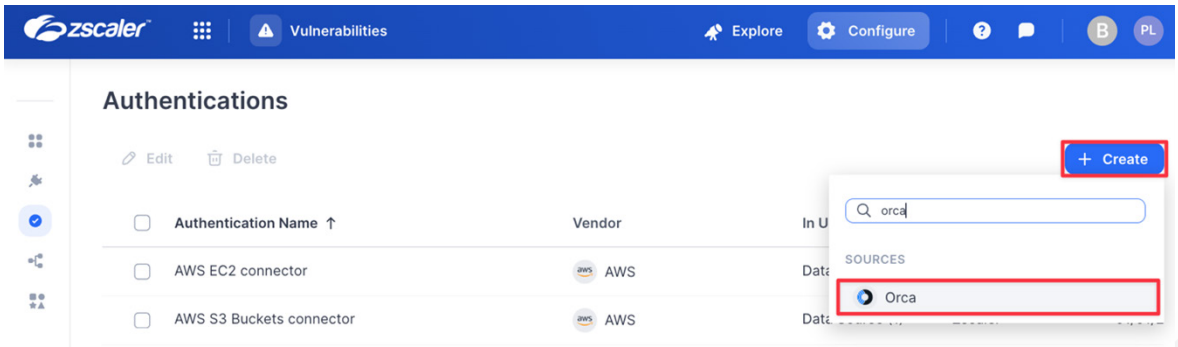

Figure 7. Create Orca

5. Enter the following:
   a. **Name**: Enter your authentication name (e.g., `Orca`).
   b. **Token**: Enter the token you generated in the Orca Security Portal.
   c. **Region**: Enter your Orca Security Region Mapping (e.g., `eu`).
6. Click **Save**.

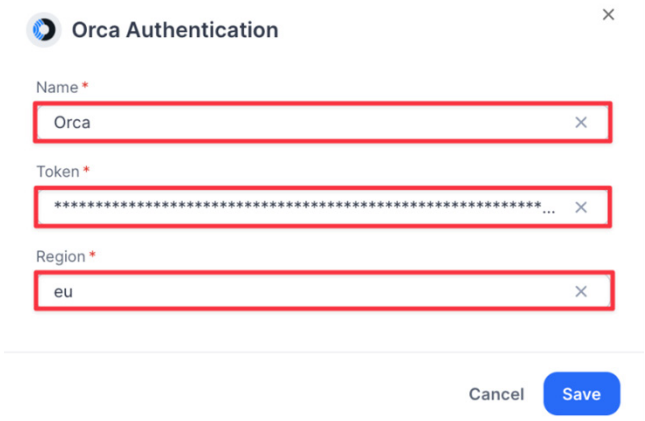

Figure 8. Orca Authentication

Configure the Orca Alerts Data Source

To configure the Orca Alerts data source:

1. Click **Configure**.

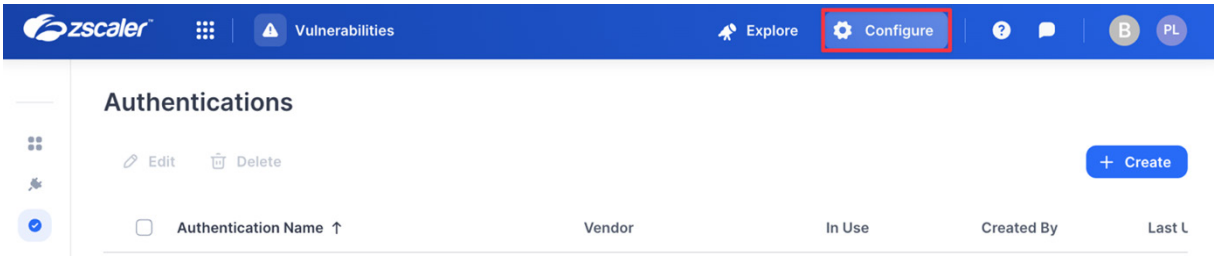

Figure 9. Configure

2. Click **Create**, then search for `Orca Alerts`.

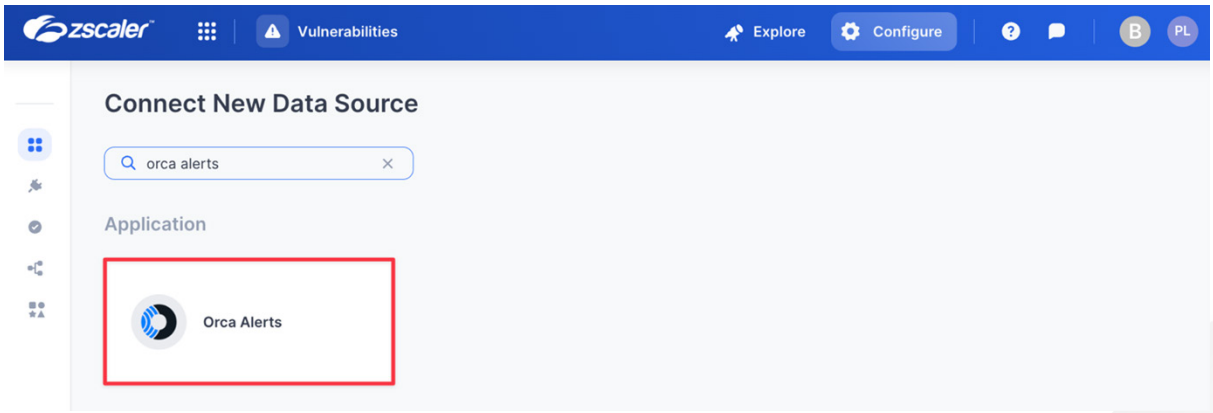

Figure 10. Orca Alerts

3. Click the **Orca Alerts** application.
4. On the **Create Orca Alerts** page, complete the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle to enable the Data Connector.
   c. **Authentication**: Select the Authentication you created previously.
   d. **(Optional) Cloud Vendor IDs**: Enter any Cloud Vendor IDs to which you want to limit this data source.
   e. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   f. **Incremental Refresh Frequency**: Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
   g. **Remediation Detection Settings**: Select your desired option to determine when findings are automatically undetected. To learn more, refer to the Zscaler UVM documentation. Automatic remediation detection only applies when data is refreshed fully, not incrementally.
   h. **Suppression Rules**: Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, refer to the Zscaler UVM documentation.
5. Click **Test**. If the API key and region have been entered correctly, the system responds with `Test Passed`.

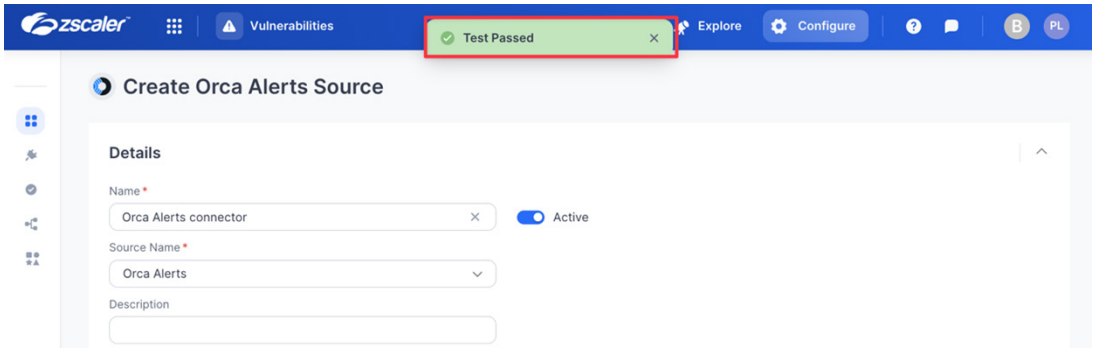

Figure 11. Test Passed

6. Click **Save**.

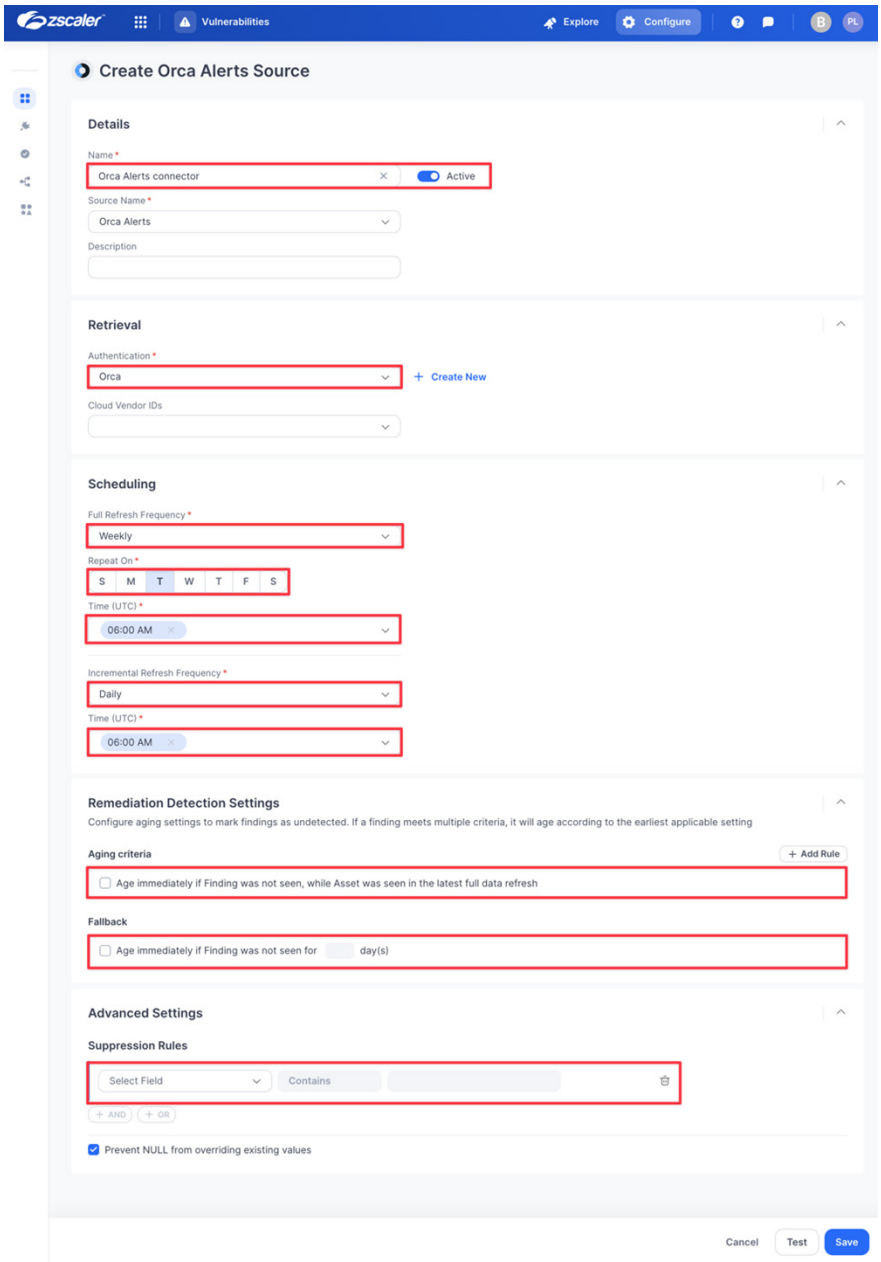

Figure 12. Create Orca Alerts Source

Configure the Orca CVE Data Source

To configure the Orca CVE data source:

1. Click **Configure**.

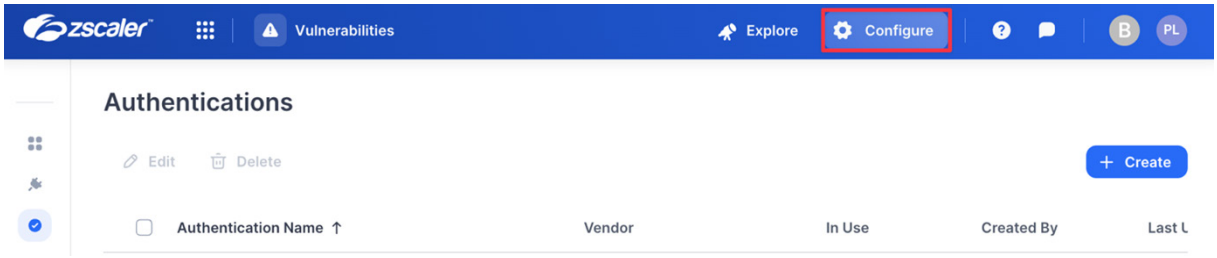

Figure 13. Configure

2. Click **Create**, then search for `Orca CVEs`.

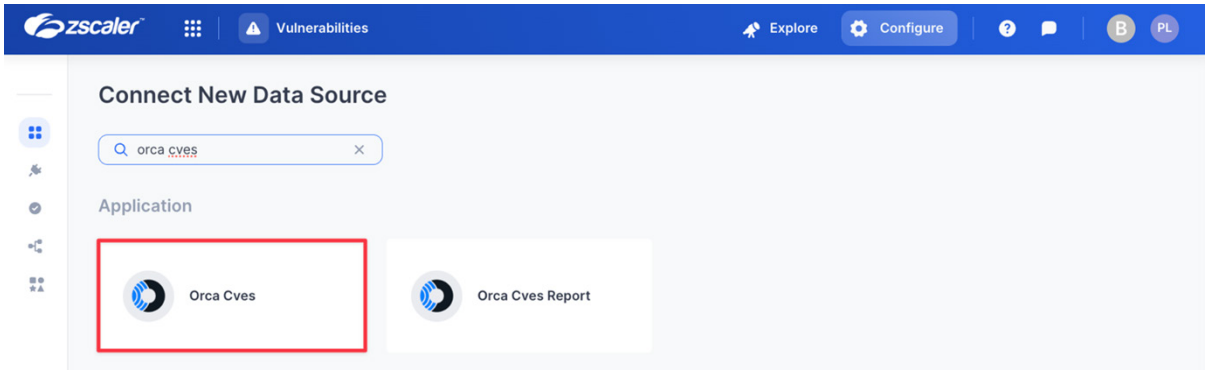

Figure 14. Orca CVEs

3. Click the **Orca Cve Report** application.
4. On the **Create Orca Cve** page, complete the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle to enable the Data Connector.
   c. **Authentication**: Select the Authentication you created previously.
   d. **(Optional) Cloud Vendor IDs**: Enter any Cloud Vendor IDs to which you want to limit this data source.
   e. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   f. **Incremental Refresh Frequency**: Set the schedule for extracting new data only. This option is more efficient because it avoids the need to retrieve all data every time.
   g. **Remediation Detection Settings**: Select your desired option to determine when findings are automatically undetected. To learn more, refer to the Zscaler UVM documentation. Automatic remediation detection only applies when data is refreshed fully, not incrementally.
   h. **Suppression Rules**: Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, refer to the Zscaler UVM documentation.
5. Click **Test**. If the API key and region have been entered correctly, the system responds with `Test Passed`.

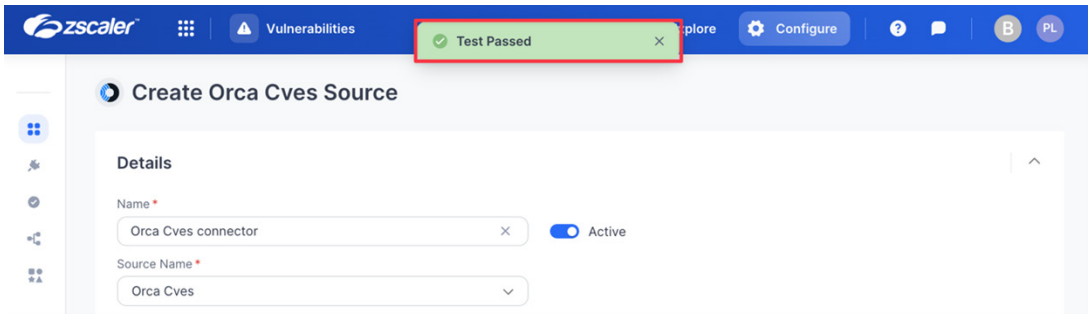

Figure 15. Test Passed

6. Click **Save**.

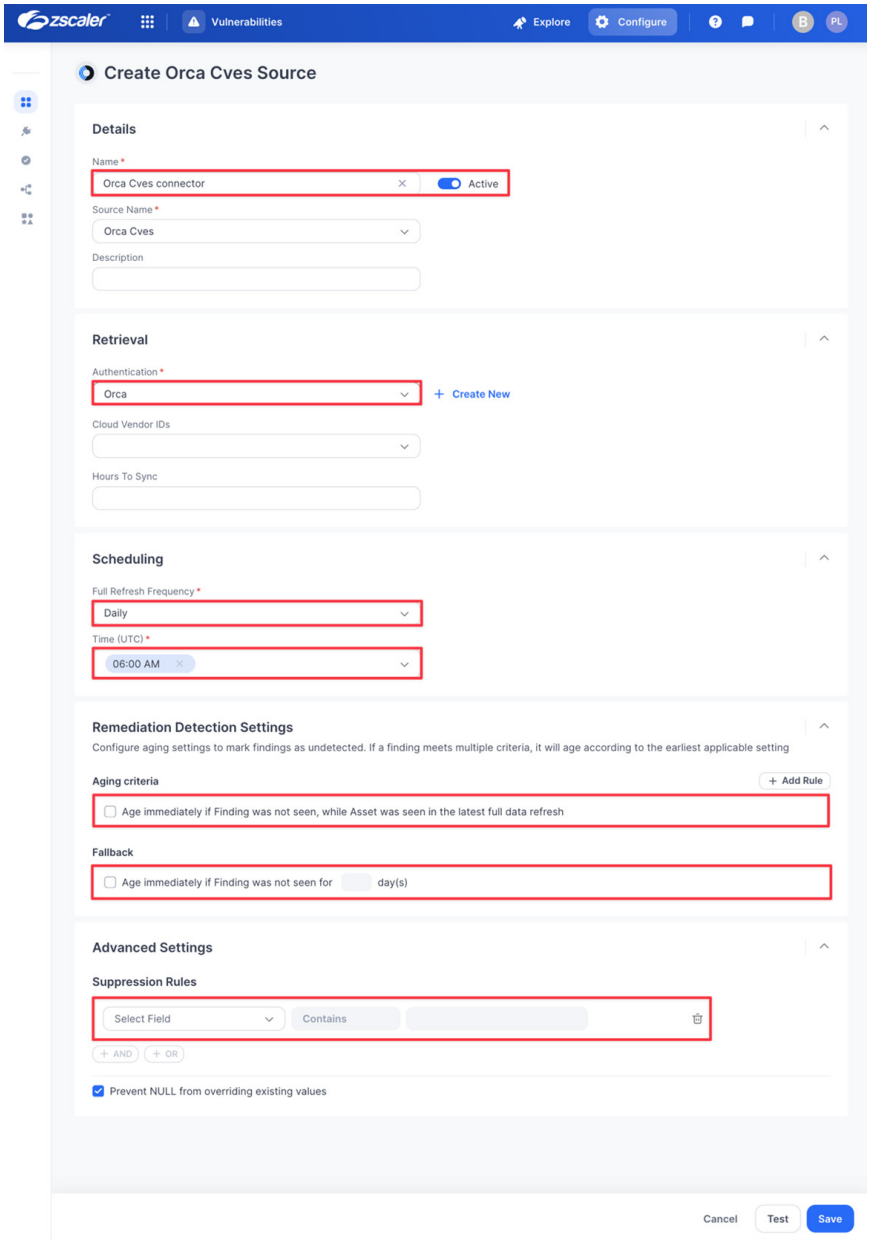

Figure 16. Create Orca Cve Source

Configure the Orca Assets Data Source

To configure the Orca Assets data source:

1. Click **Configure**.

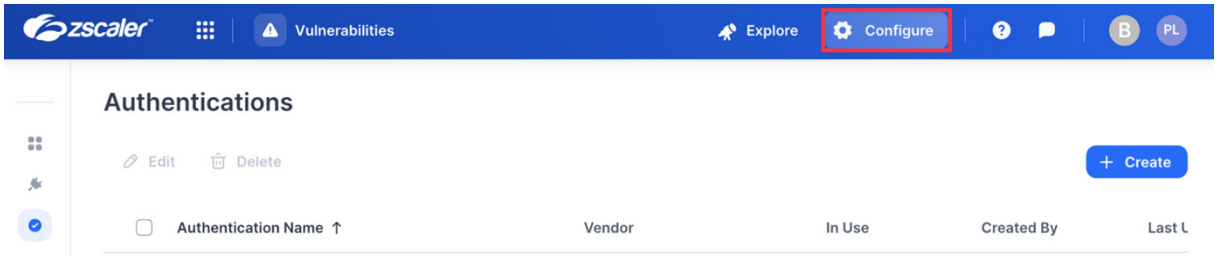

Figure 17. Configure

2. Click **Create**, then search for `Orca Assets`.

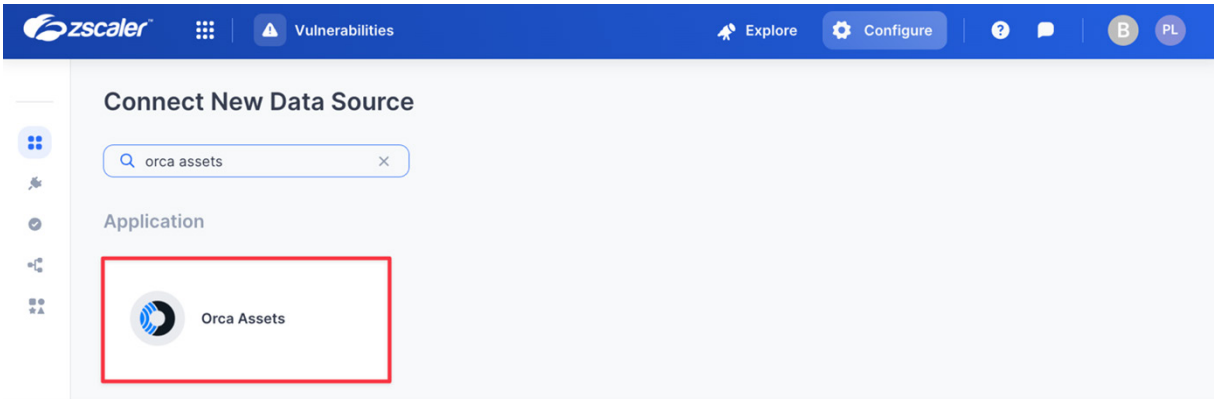

Figure 18. Orca Assets

3. Click the **Orca Assets** application.
4. On the **Create Orca Assets** page, complete the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle to enable the Data Connector.
   c. **Authentication**: Select the Authentication you created previously.
   d. **(Optional) Cloud Vendor IDs**: Enter any Cloud Vendor IDs to which you want to limit this data source.
   e. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   f. **Remediation Detection Settings**: Select your desired option to determine when findings are automatically undetected. To learn more, refer to the Zscaler UVM 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, refer to the Zscaler UVM documentation.

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

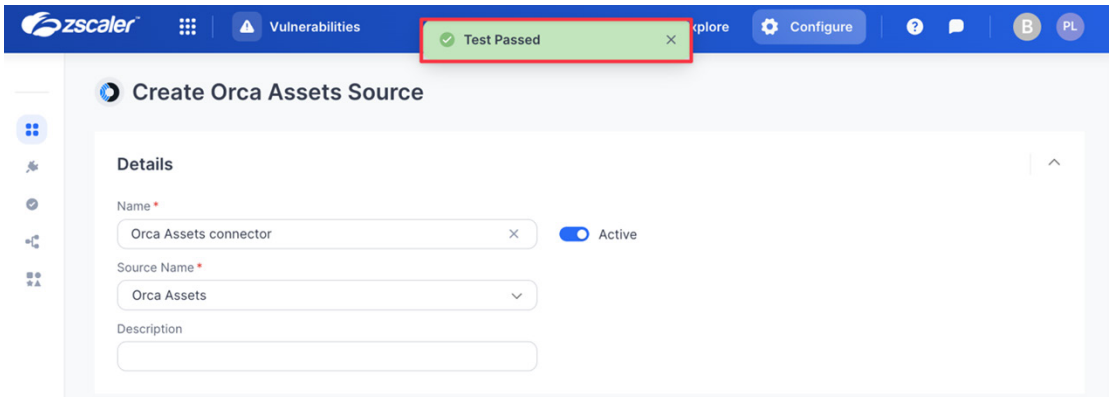

Figure 19. Test Passed

6. Click **Save**.

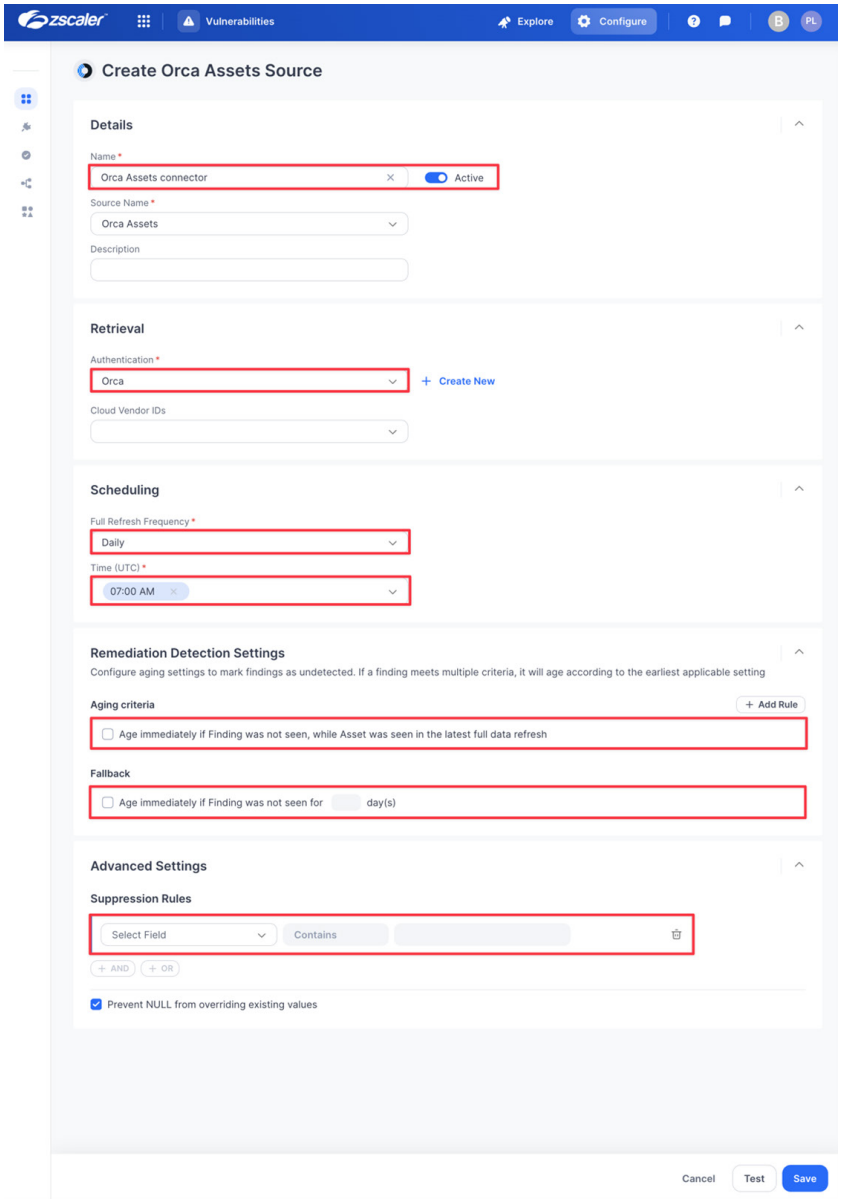

Figure 20. Create Orca Assets Source

Configure the Orca Vulnerabilities Data Source

To configure the Orca Vulnerabilities data source:

1. Click **Configure**.

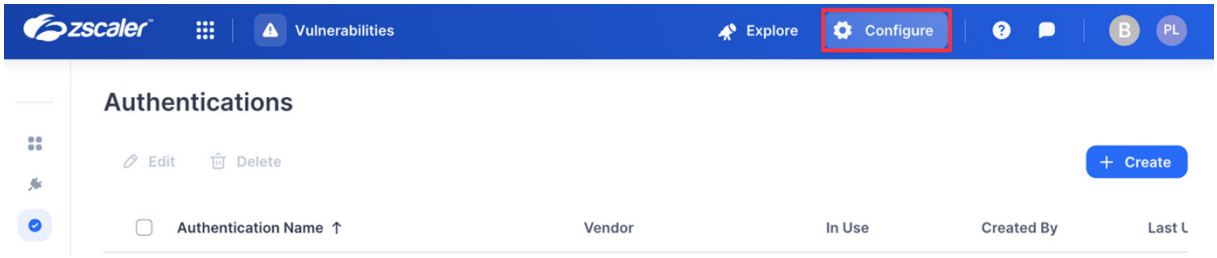

Figure 21. Configure

2. Click **Create**, then search for `Orca Vulnerabilities`.

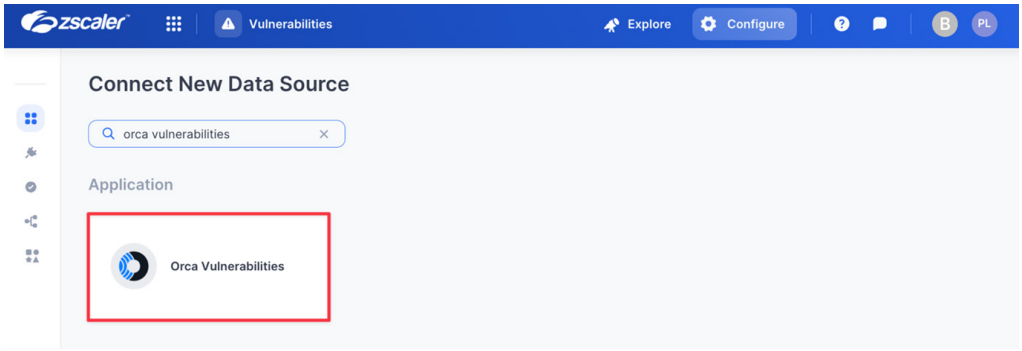

Figure 22. Orca Vulnerabilities

3. Click the **Orca Vulnerabilities** application.
4. On the **Create Orca Vulnerabilities** page, complete the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle to enable the Data Connector.
   c. **Authentication**: Select the Authentication you created previously.
   d. **(Optional) Cloud Vendor IDs**: Enter any Cloud Vendor IDs to which you want to limit this data source.
   e. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   f. **Remediation Detection Settings**: Select your desired option to determine when findings are automatically undetected. To learn more, refer to the Zscaler UVM 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, refer to the Zscaler UVM documentation.

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

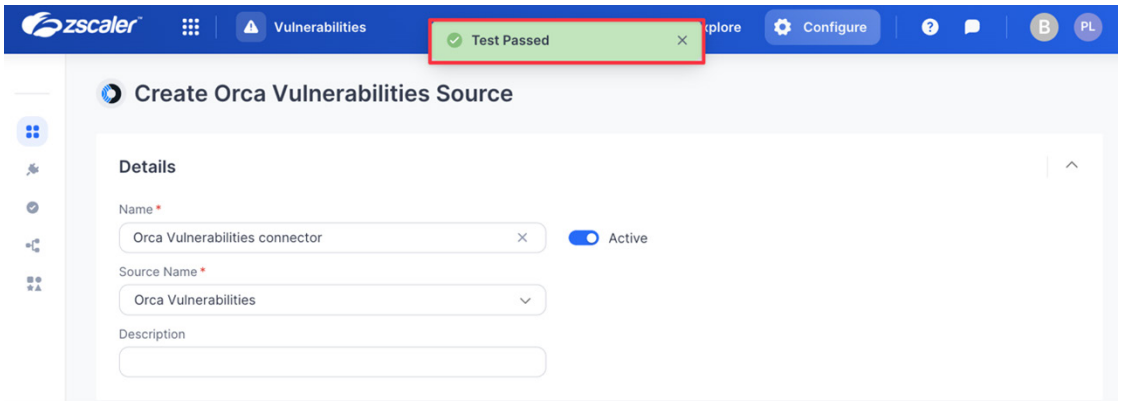

Figure 23. Test Passed

6. Click **Save**.

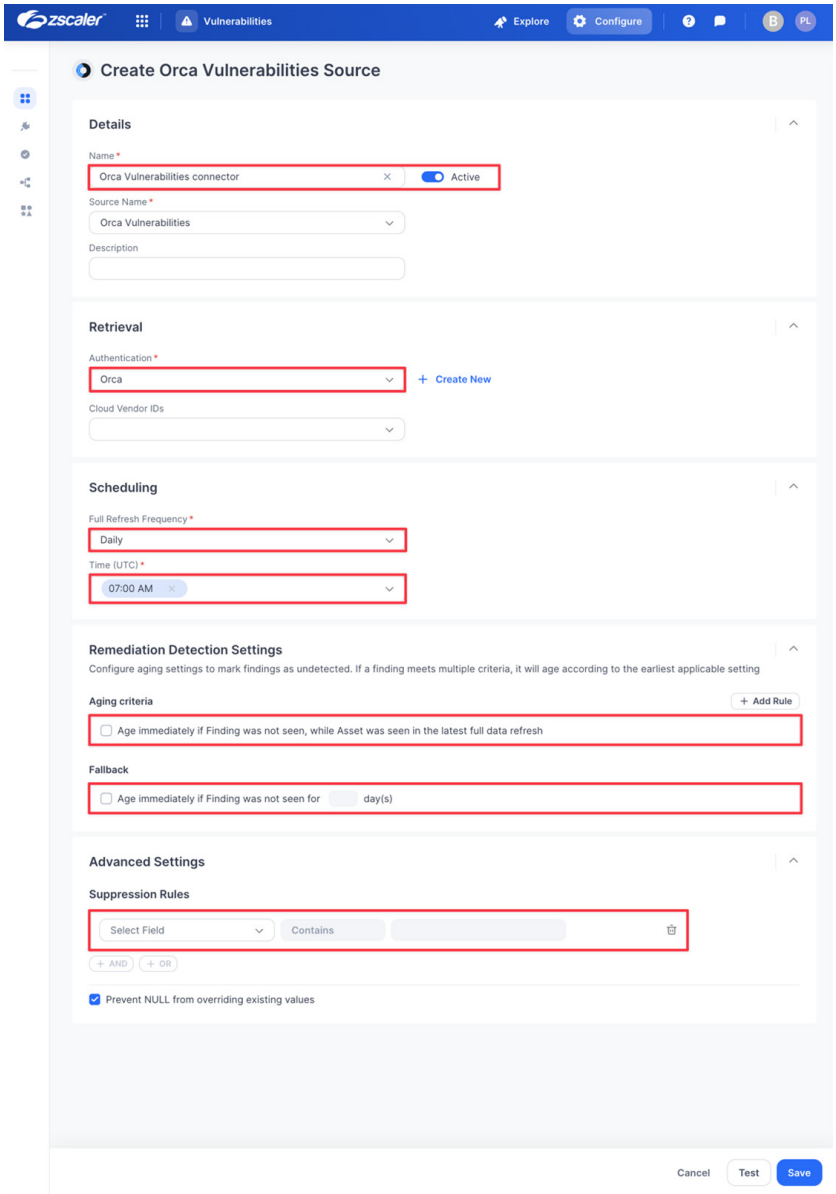

Figure 24. Create Orca Vulnerabilities Source

Review and Adjust Data Model Mapping

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

The following example shows how to leverage the Crown Jewel Data Model Entity based on an AWS EC2 instance tag so that you can use that field as a Risk Factor when calculating risk for an Asset.

Create a Crown Jewel Tag for an EC2 Instance

To create a Crown Jewel tag for an EC2 Instance:

1. Log in to your AWS Console.
2. Select **Services** > **EC2**.

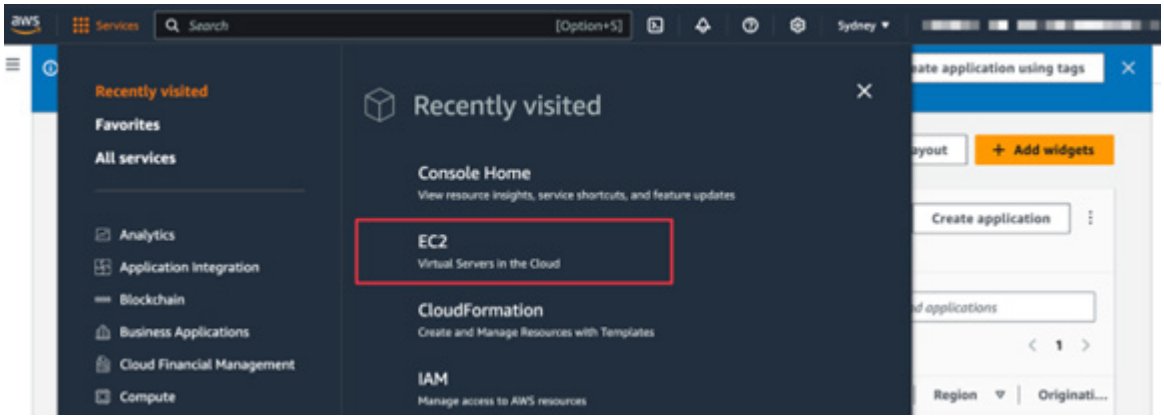

Figure 25. EC2

3. Click **Instances**.

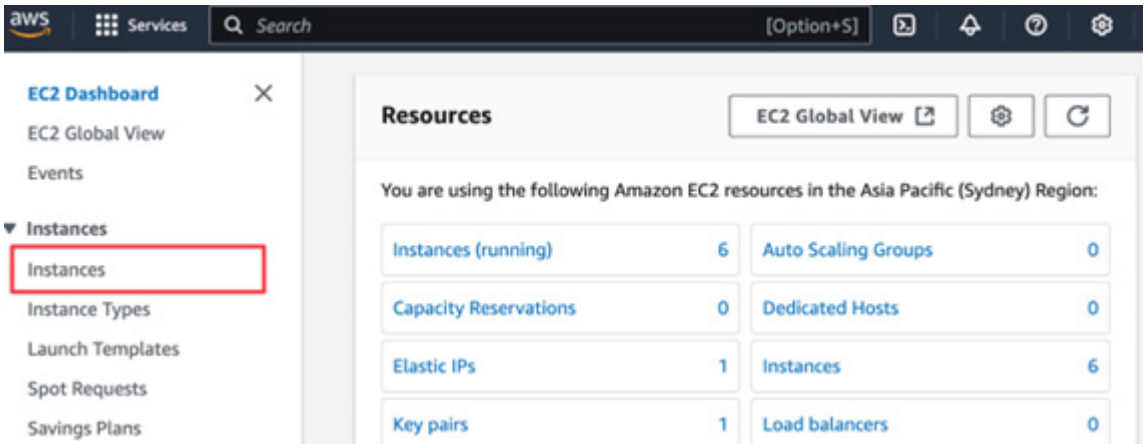

Figure 26. Instances

4. Select the instance you want to add the **Crown Jewel** tag to and click **Tags**.

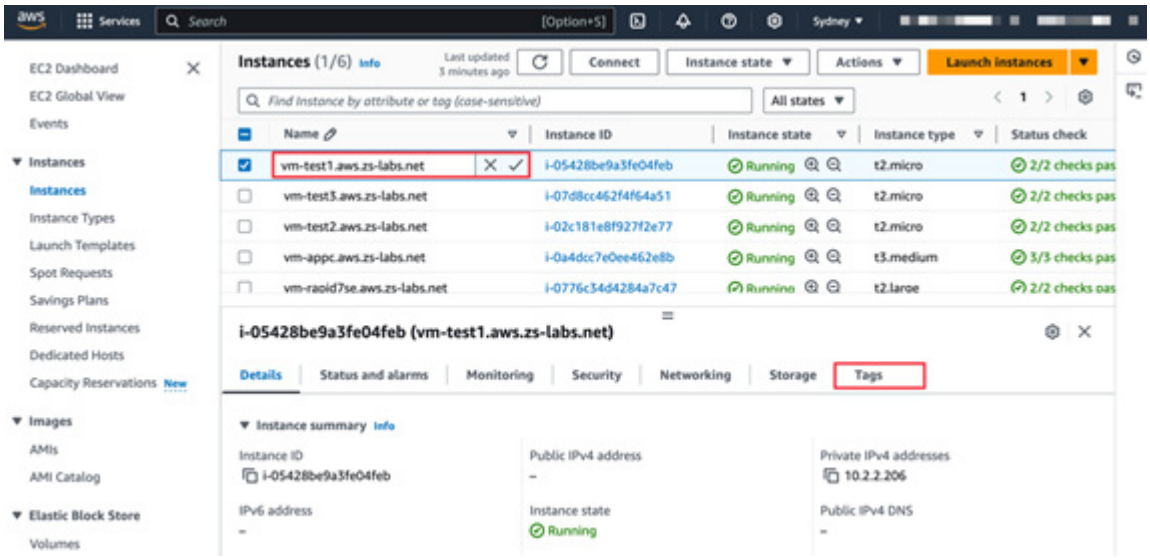

Figure 27. Tags

5. Click **Manage tags**.

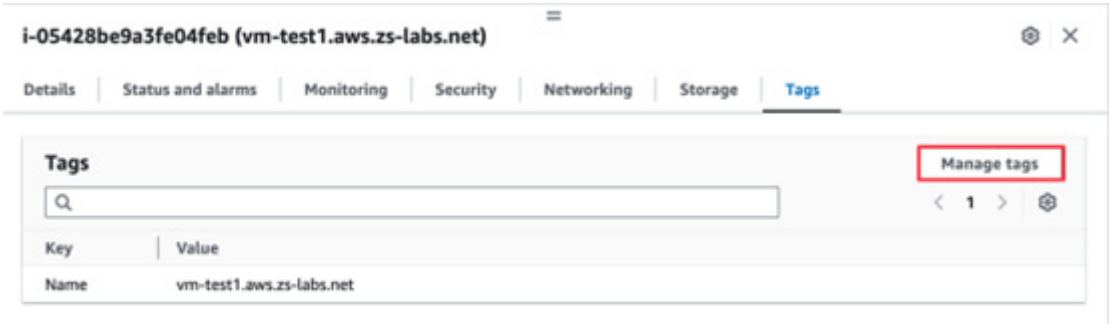

Figure 28. Manage tags

6. Click **Add new tag** and enter:
   a. Key: `Classification`.
   b. Value: `Crown Jewel`.

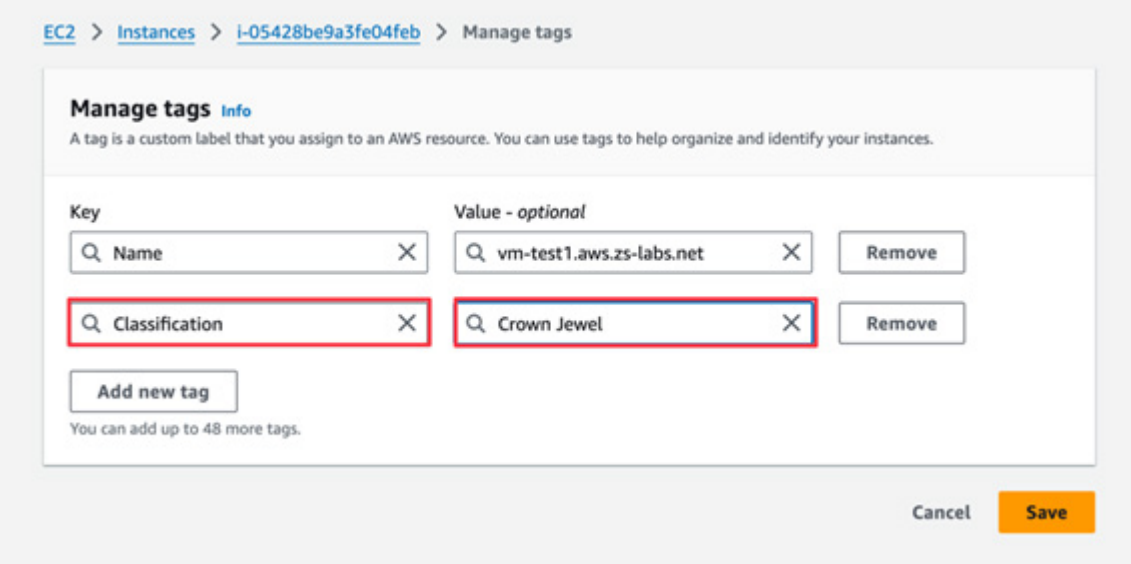

Figure 29. Add new tag

7. Click **Save**.

Map the AWS EC2 Data Source

To map the AWS EC2 data source:

1. Refer to the [Zscaler and AWS Deployment Guide] for instructions on adding the EC2 Data Source.
2. After you have added the EC2 Data Source, select **Configure**, then go to **AWS EC2 connector** > **Map Data**.

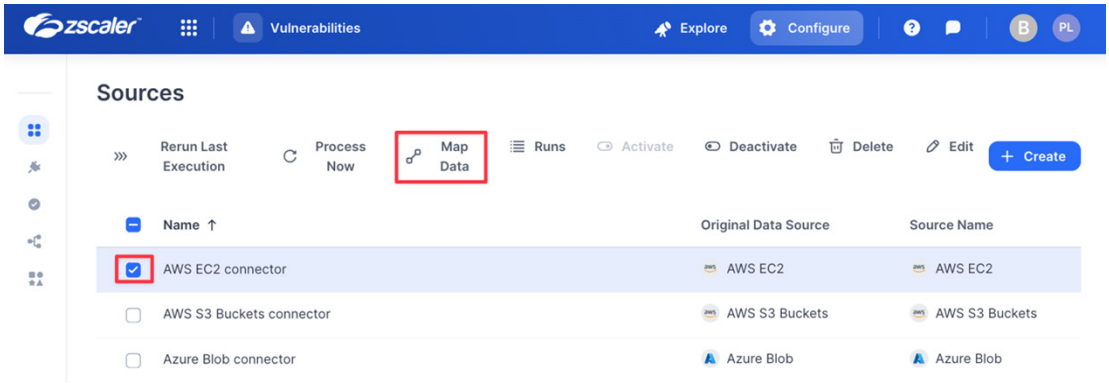

Figure 30. Map Data

3. In the **Map AWS EC2 connector** window, create a new **Asset Key** using **InstanceId**:
   a. On the right side, under **Asset**, drag **Key** to the **Create New Connection** element.
   b. On the left side, under **Ingested Data**, drag **InstanceId** to the **Create New Connection** element.

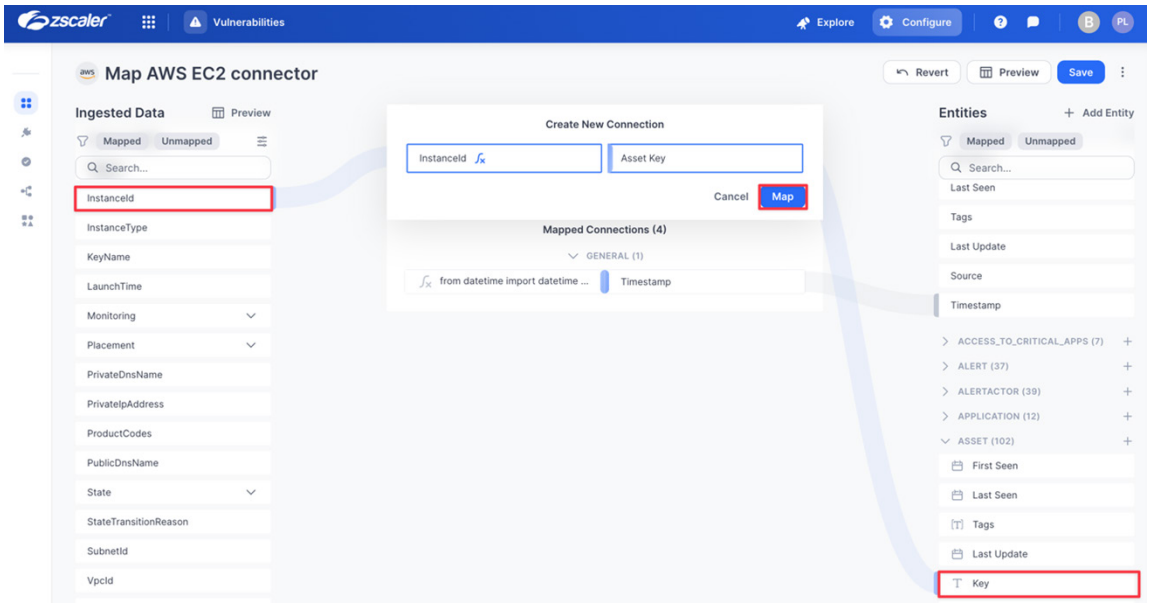

Figure 31. Map AWS EC2 connector

   c. Click **Map**, then click the **Key** icon next to the **Asset Key** to set as a key.

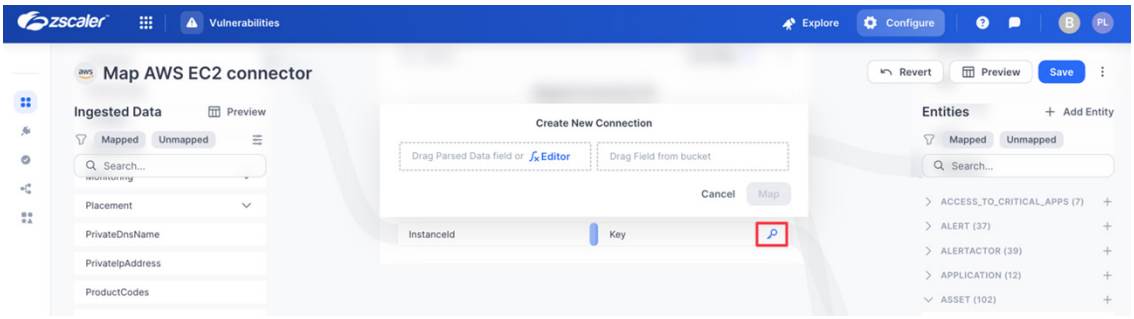

Figure 32. Create New Connection

   d. Map the **Is Crown Jewel Asset** entity to the **Crown Jewel EC2** tag created earlier by:
      - On the right side, under **Asset**, drag Is **Crown Jewel** to the Create New Connection element.
      - On the left side, click the **Editor** element.

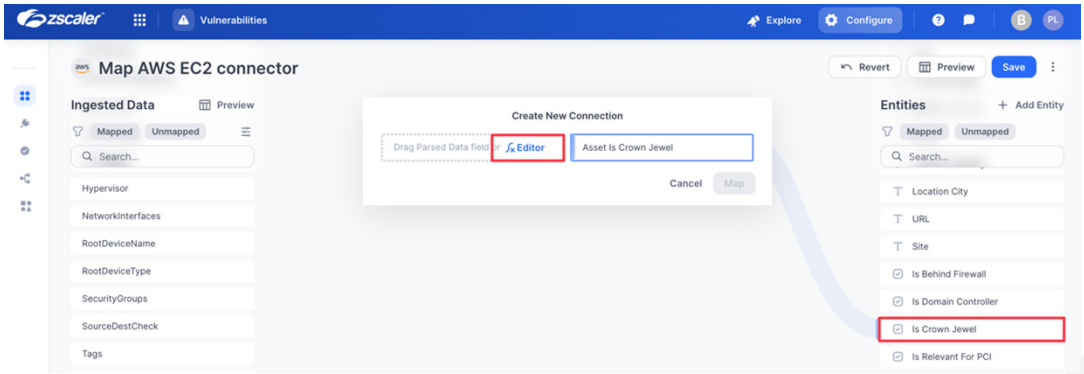

Figure 33. Editor

- Replace the text in the script field with:

```
def evaluate(row: dict) -> bool:
    tags = row.get("Tags")
    for item in tags:
    if item.get("Key") == "Classification" and item.get("Value") == "Crown Jewel":
                            return True
        else:
        return False
```

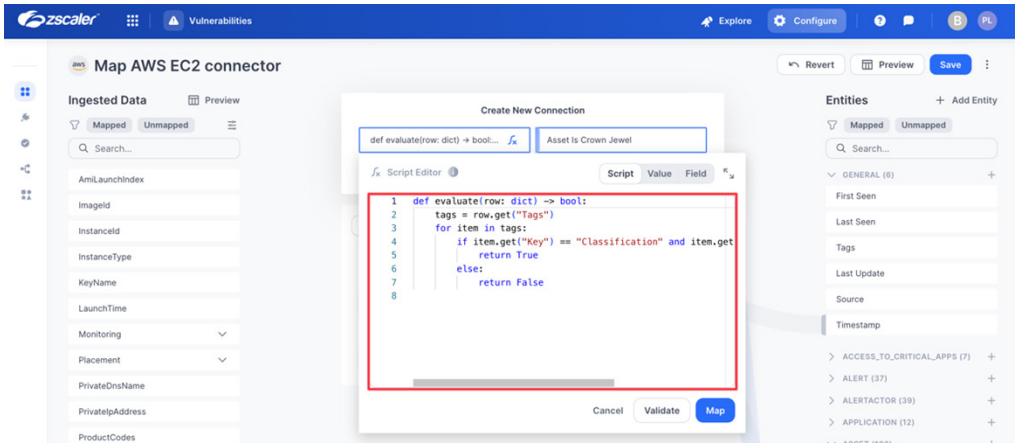

Figure 34. Script

- Click **Map**.

e. Click **Preview** to see the if an **Asset** is marked as a **Crown Jewel** based on its **EC2 tag** and its **Asset Key** is its Instance ID.

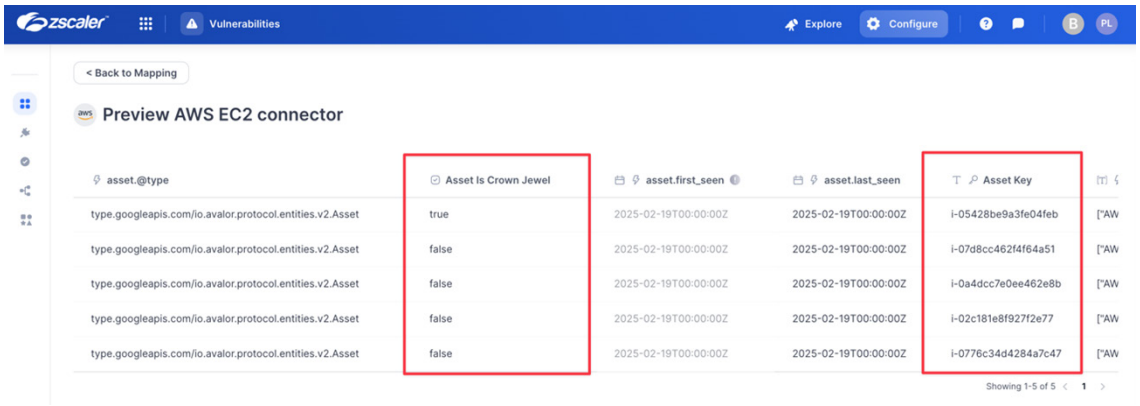

Figure 35. Preview

f. Click **Back to Mapping**, then click **Save**.

g. On the **Sources** page, click **Process Now** > **Process Now** under your **AWS EC2 Data Source**.

Map the Orca Vulnerabilities Data Source

To map the Orca Vulnerabilities data source:

1. Click **Configure** > your **Orca Vulnerabilities Connector** > **Map Data**.

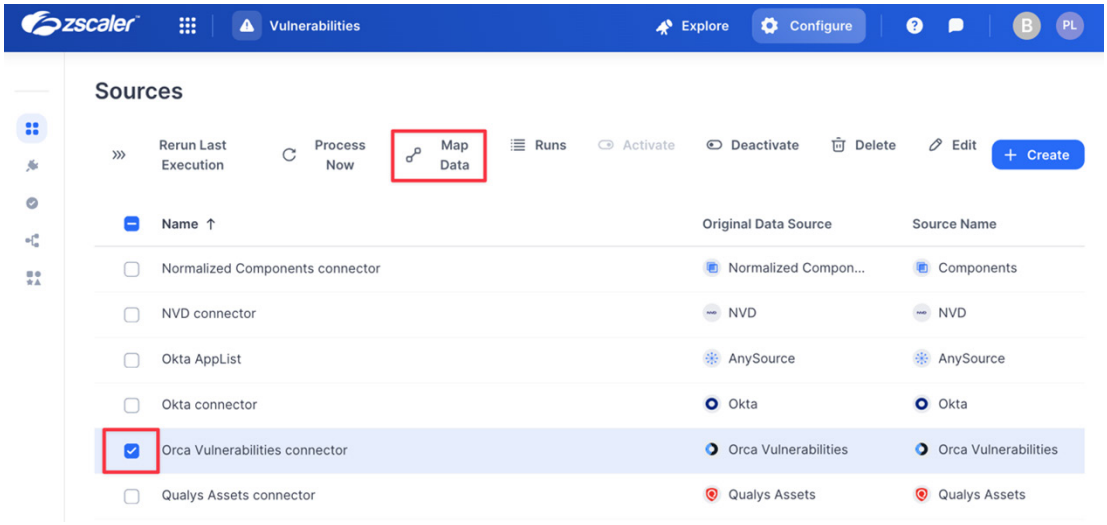

Figure 36. Map Data

2. In the **Map Orca Vulnerabilities connector** window, create a new **Global Vulnerability CVE** using the **cve_id**:
   a. On the right side, under **Global Vulnerability**, drag **CVE** to the **Create New Connection** element.
   b. On the left side, under **Ingested Data**, drag **cve_id** to the **Create New Connection** element.

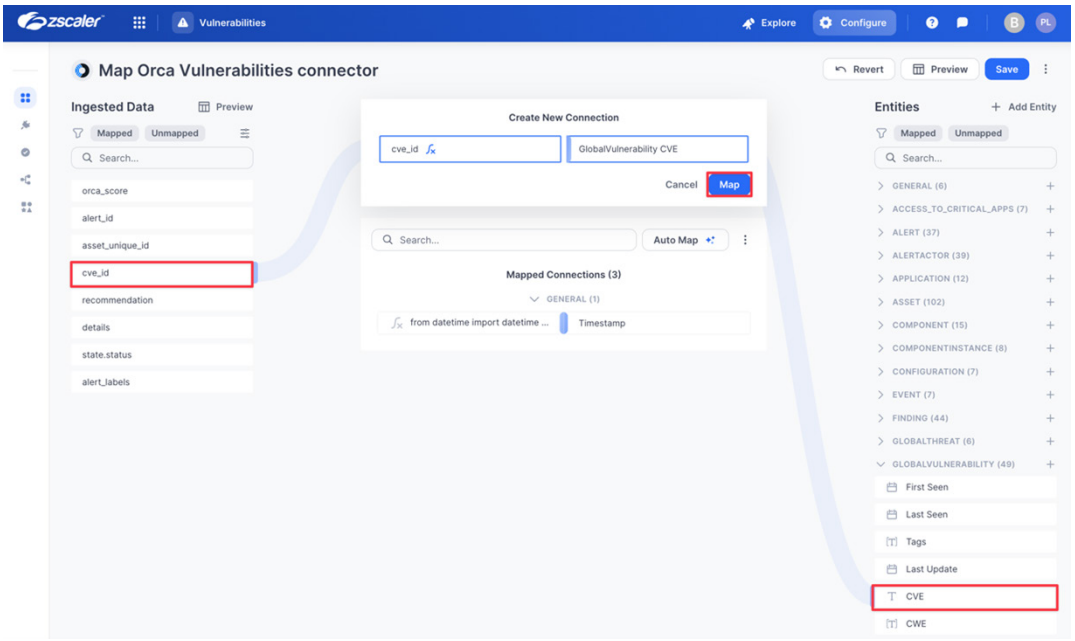

Figure 37. Map Orca Vulnerabilities connector

   c. Click **Map**.

3. Create a new **Asset Key** using a custom function:
   a. On the right side, under **Asset**, drag **Key** to the **Create New Connection** element.
   b. Click the **Editor** button on the left-hand side.

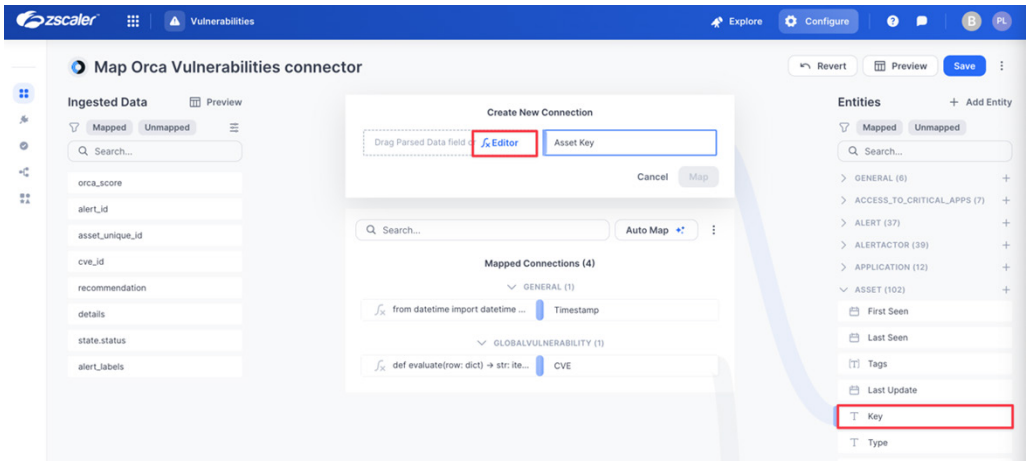

Figure 38. Editor

   c. Replace the text with the following:

```
def evaluate(row: dict) -> str:

    item = row.get("asset_unique_id")

    parts = item.rsplit("_", 1)

    return parts[1] if len(parts) > 1 else ""
```

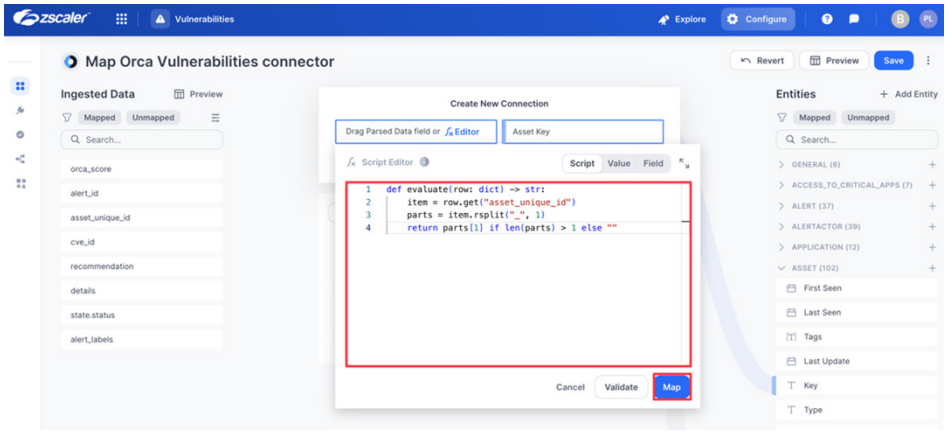

Figure 39. Script

d. Click **Map**.

e. Click the **Key** icon under **Asset (Key) connection** and under **Global Vulnerability (CVE)**.

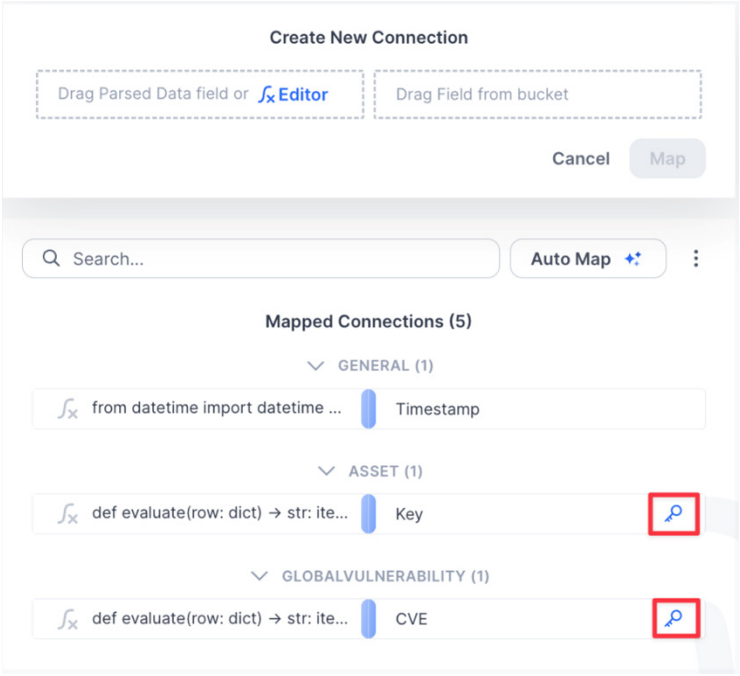

Figure 40. Create New Connection

f. Click **Save**.

g. On the **Sources** page, click **Process Now** > **Process Now** under your **Orca Vulnerabilities Data Source**.

Review and Adjust Risk Scoring

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

The following example shows how the Is Crown Jewel field is added as a Risk Factor for risk scoring. A value of True increases the risk calculation (since the asset is a Crown Jewel application).

1. From the **Vulnerabilities** tab in the **Zscaler UVM dashboard (Remediation Hub)**:
   a. In the left pane, select **Settings** > **Score**.
   b. Click **Add Factor** in the **Risk & Mitigating Factors** section.

2. If **Crown Jewel** is not already a **Risk Factor**, in the **Add new factor** modal:
   a. Select **Risk Factors** for **Factor Type** (where Mitigating Factors generally lower risk scoring, while Risk Factors generally increase risk scoring).
   b. Enter a **Factor Name**.
   c. Select **Asset is Crown Jewel** for **Field**.
   d. In the **Boolean** login section, under **True**, enter a percentage by which the risk is increased.

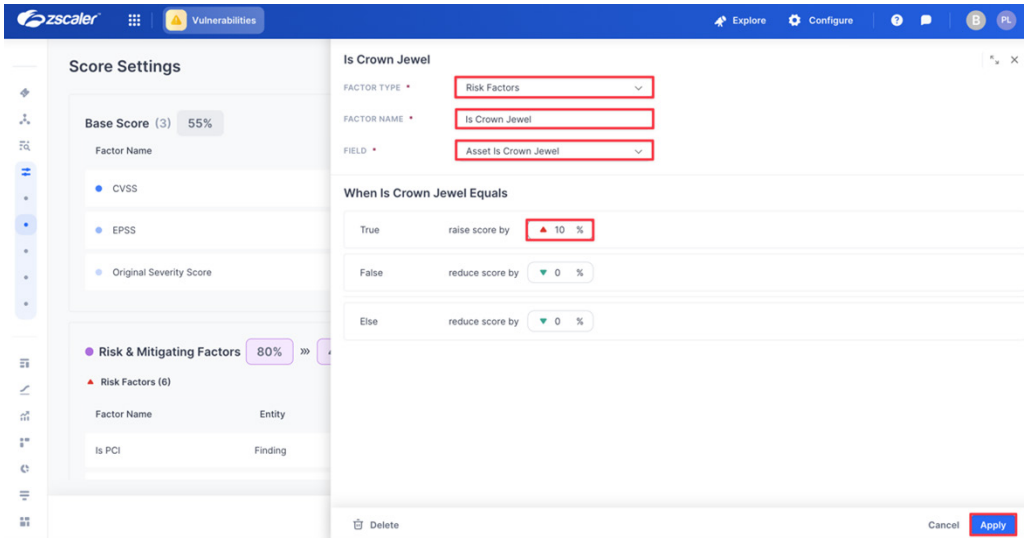

Figure 41. Score Settings

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

3. In the left-side pane, select the **Assets** dashboard. From the **Assets** dashboard:
   a. Under **Sources**, select **AWS EC2** and **Orca Vulnerabilities**.
   b. Set a filter by clicking **More** and selecting **True** for **Is Crown Jewel True**.

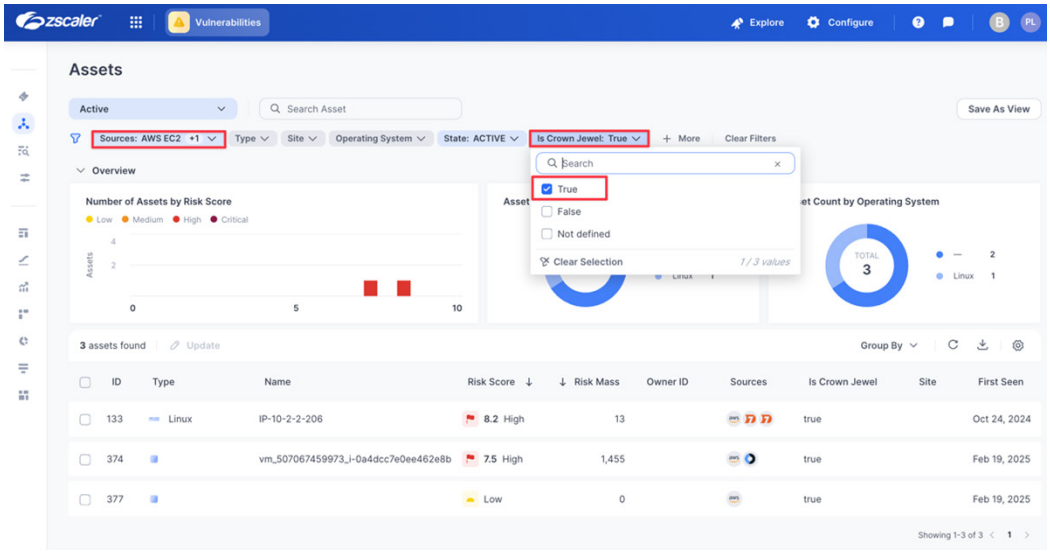

Figure 42. Assets

c. Click one of your **Assets** in the filtered list.

d. In the **Asset** modal that appears, click the **Findings** tab.

e. Click one of the **Findings**.

f. Review the output (notice in the **Score Adjustment** section and how **Is Crown Jewel** has modified the risk scoring).

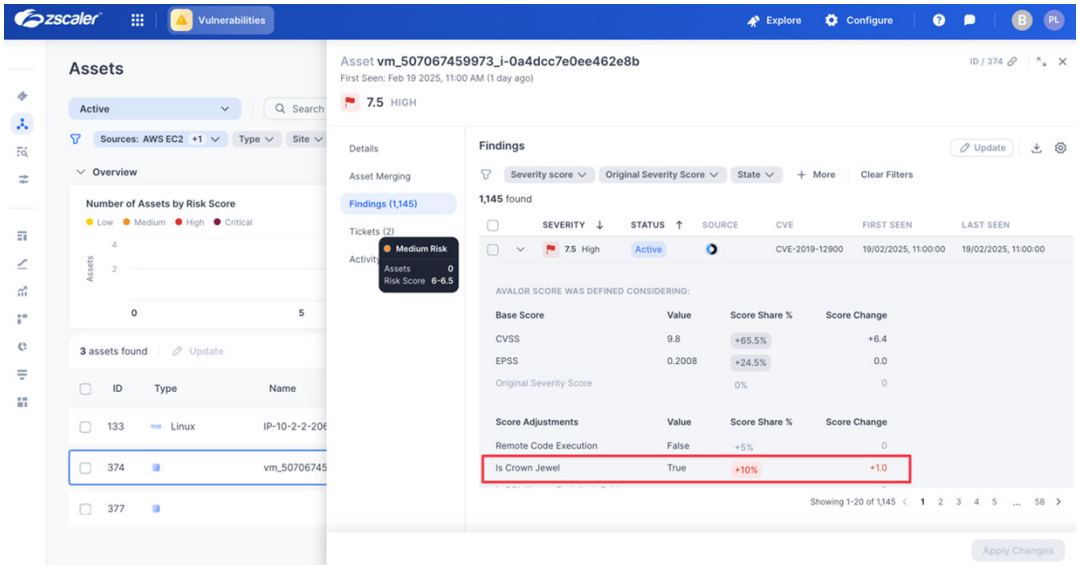

Figure 43. Findings

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. Log in to the Zscaler UVM Platform.

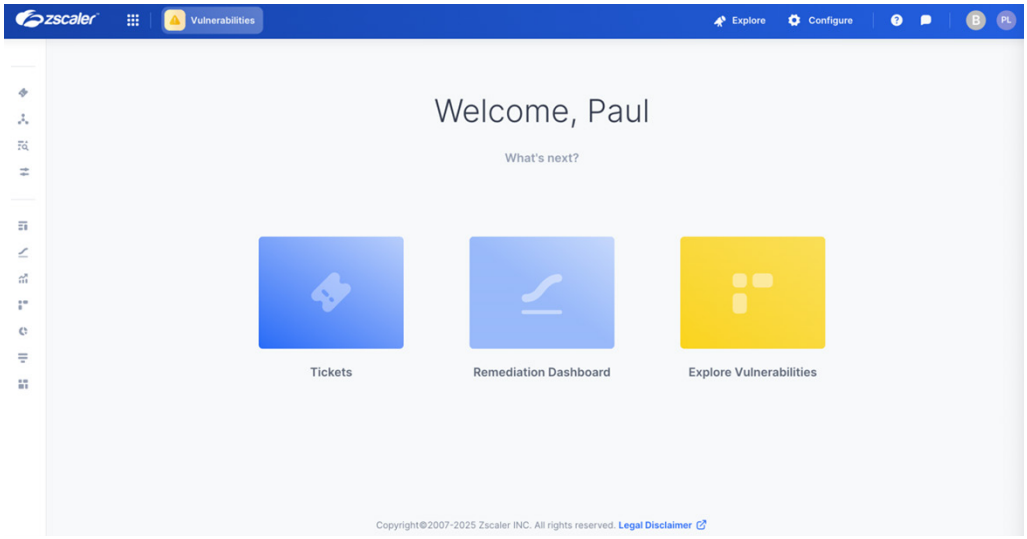

Figure 44. Zscaler UVM Platform

2. Click **Contact Support**.

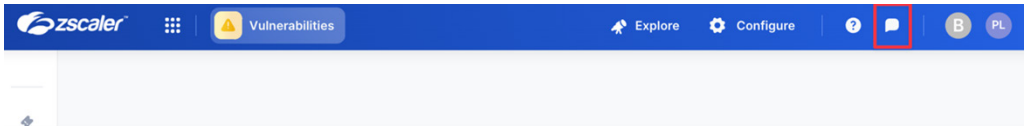

Figure 45. Contact Support

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

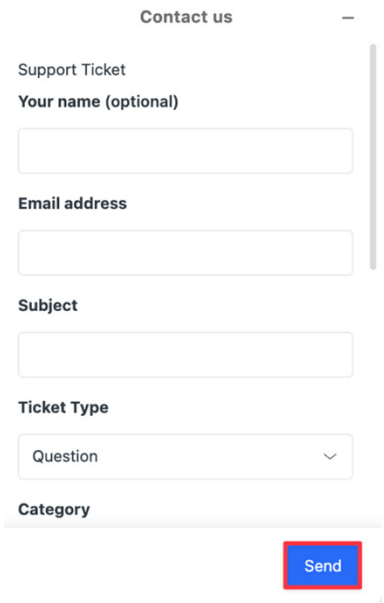

Figure 46. Contact us

