



ZSCALER UVM AND TENABLE DEPLOYMENT GUIDE

Contents

Terms and Acronyms	3
About This Document	5
Zscaler Overview	5
Tenable Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and Tenable Introduction	6
Zscaler UVM Overview	6
Tenable Vulnerability Management Overview	7
Tenable Resources	7
Contextualizing Risk Using Tenable Cloud and Zscaler Unified Vulnerability Management	8
Create an API Key in the Tenable Cloud Portal	8
Configure the Zscaler UVM Data Connectors	10
Configure the Tenable Vulnerability Management—Vulnerabilities Data Source	10
Configure the Tenable Vulnerability Management—Issues Data Source	13
Configure the Tenable Vulnerability Management—Assets Data Source	16
Review and Adjust Data Model Mapping	18
Create an API Key in the Zscaler Client Connector Portal	18
Configure the Zscaler Client Connector Devices Data Source	20
Map the Zscaler Client Connector Devices Data Source	23
Map the Tenable Vulnerability Management—Vulnerabilities Data Source	26
Review and Adjust Risk Scoring	28
Appendix A: Requesting Zscaler Support	30

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)
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](#).

Tenable Overview

Tenable (NASDAQ: [TENB](#)) is a leading cybersecurity company specializing in vulnerability management and exposure detection solutions. Founded in 2002 and headquartered in Columbia, Maryland, Tenable empowers organizations worldwide to understand and reduce their cyber risks. Its flagship product, Tenable.io, is a cloud-based platform that provides visibility into an organization's IT environment, helping identify vulnerabilities, misconfigurations, and compliance gaps across assets, networks, and applications. Widely recognized for its innovative solutions like Nessus, one of the most popular vulnerability assessment tools, Tenable serves enterprises, government agencies, and service providers, helping them protect their critical assets and stay resilient against evolving cyber threats. To learn more, refer to [Tenable'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](#)
- [Tenable 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 Tenable Introduction

Overviews of the Zscaler and Tenable 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
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler UVM Help Portal	Zscaler UVM Help Portal.
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	Zscaler UVM Help Portal.
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.

Tenable Vulnerability Management Overview

Tenable Vulnerability Management is a leading-edge solution for modern vulnerability management, designed to help organizations identify, assess, and prioritize risks across their entire attack surface. Built on Tenable’s advanced Cyber Exposure platform, Tenable Vulnerability Management leverages cloud-native architecture to provide unparalleled scalability and flexibility, enabling continuous visibility into vulnerabilities, misconfigurations, and other security risks.

With powerful features such as predictive prioritization, dynamic asset discovery, and seamless integrations, Tenable Vulnerability Management empowers organizations to focus on the vulnerabilities that matter most to their unique environment. By combining real-time insights with automated workflows and comprehensive reporting, Tenable Vulnerability Management streamlines the remediation process and enhances collaboration across security and IT teams, ensuring a proactive and efficient approach to safeguarding critical assets and reducing overall cyber risk.

Tenable Resources

The following table contains links to Tenable support resources.

Name	Definition
Tenable Community	Tenable Community Forum.
Tenable Documentation	Help articles for Tenable.

Contextualizing Risk Using Tenable Cloud and Zscaler Unified Vulnerability Management

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 a preconfigured connectors for Tenable Cloud including:

- Tenable Vulnerability Management—Vulnerabilities
- Tenable Vulnerability Management—Issues
- Tenable Vulnerability Management—Assets

The following steps outline how to start ingesting data from these sources, while also (optionally) combining Tenable Vulnerability Management—Vulnerabilities data with Zscaler Client Connector Device information to provide a more contextualized and personalized risk assessment for your organization.

Create an API Key in the Tenable Cloud Portal

To create an API key:

1. Log in to the Tenable Cloud Portal with an Administrator account.
2. Click **Vulnerability Management**.
3. Click your username icon and click **My Profile**.

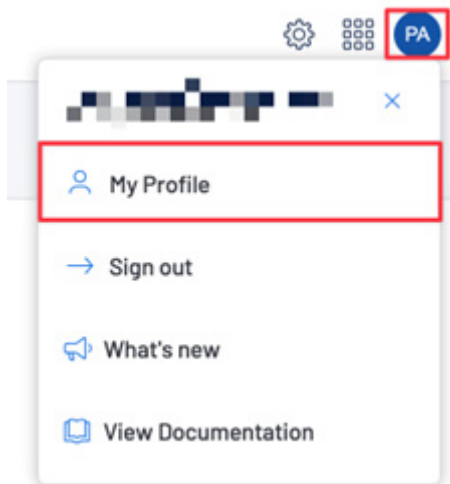


Figure 1. My Profile

- Click **API Keys** and **Generate**.

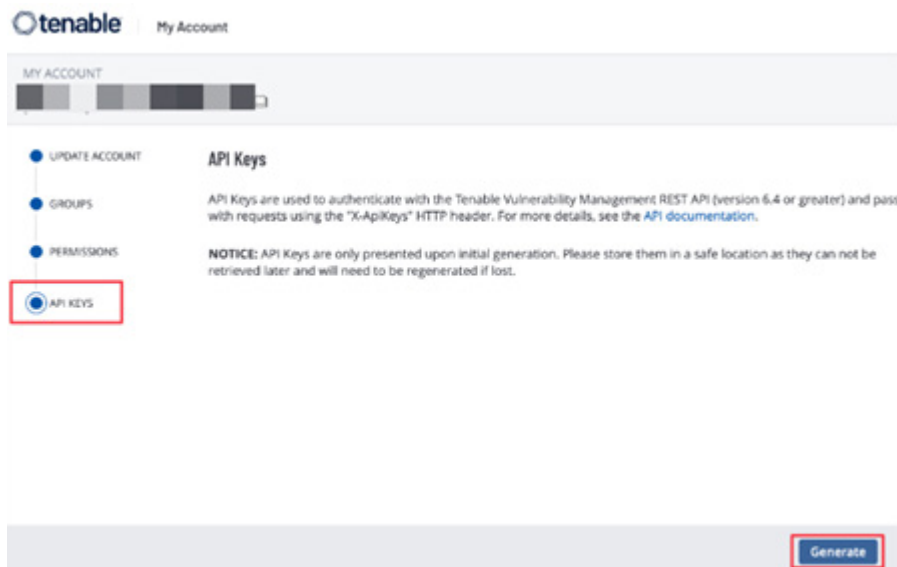


Figure 2. API Keys

- Save the **Access Key** and **Secret Key** for use later.

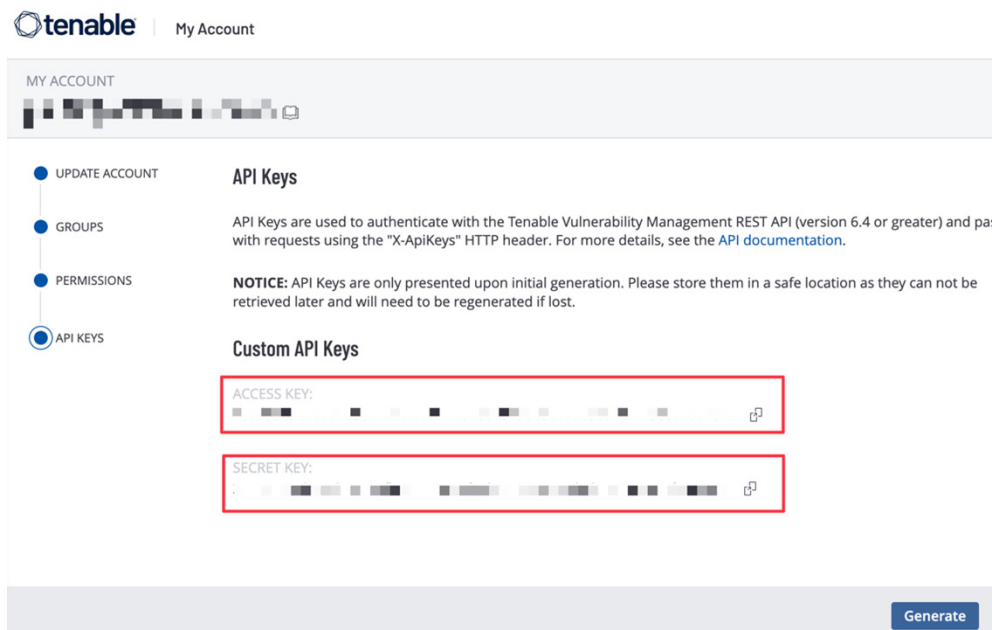


Figure 3. Access Key and Secret Key

Configure the Zscaler UVM Data Connectors

The following sections describe configuring the UVM data connectors.

Configure the Tenable Vulnerability Management—Vulnerabilities Data Source

To configure the Tenable Vulnerability Management data source:

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

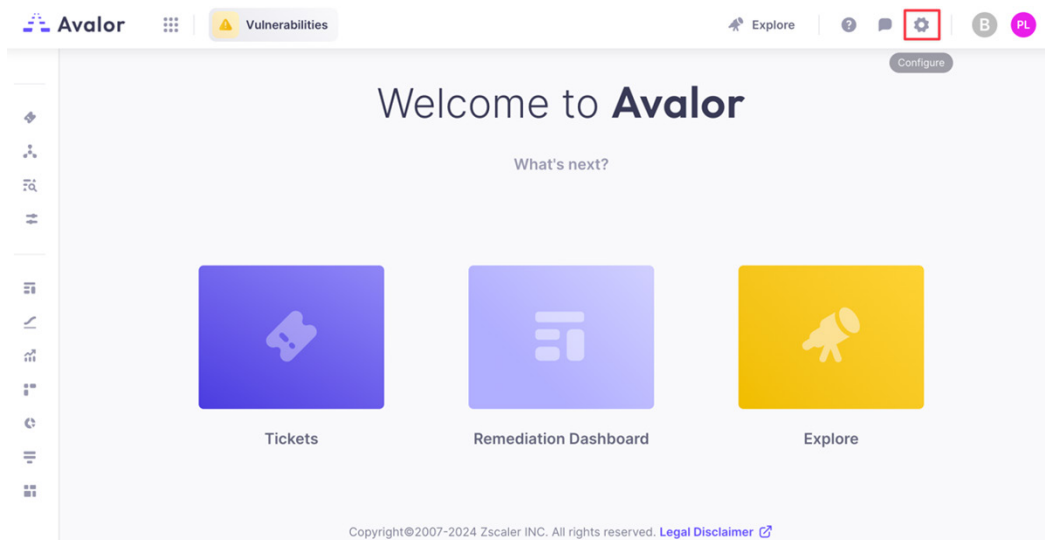


Figure 4. Configure

3. Click **Create**, then search for Tenable Vulnerability Management—Vulnerabilities.

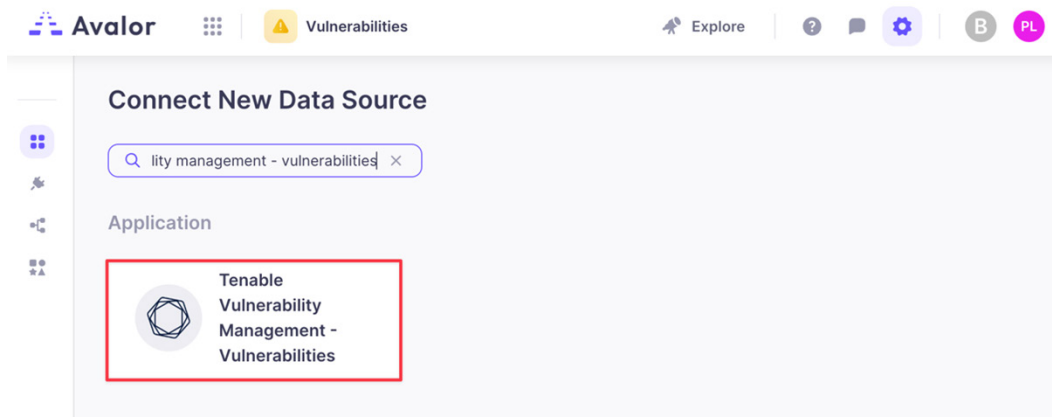


Figure 5. Tenable Vulnerability Management—Vulnerability

4. Click the **Tenable Vulnerability Management—Vulnerabilities** application.

5. On the **Create Tenable Vulnerability Management—Vulnerabilities Source** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Access key:** Enter the Access you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - d. **Secret Key:** Enter the Secret Key you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - e. **Split findings by Output:** Select the checkbox to split findings by output.
 - f. **Include Info-Level Severity Data:** Select the checkbox to include info-level severity data.
 - g. **Full Refresh Frequency:** Set your desired schedule for extracting all data.
 - h. **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.
 - i. **Suppression Rules:** Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, refer to the [Avalor documentation](#).
 - j. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
6. Click **Test**. If the API key and region have been entered correctly, the system responds with **Test Passed**.

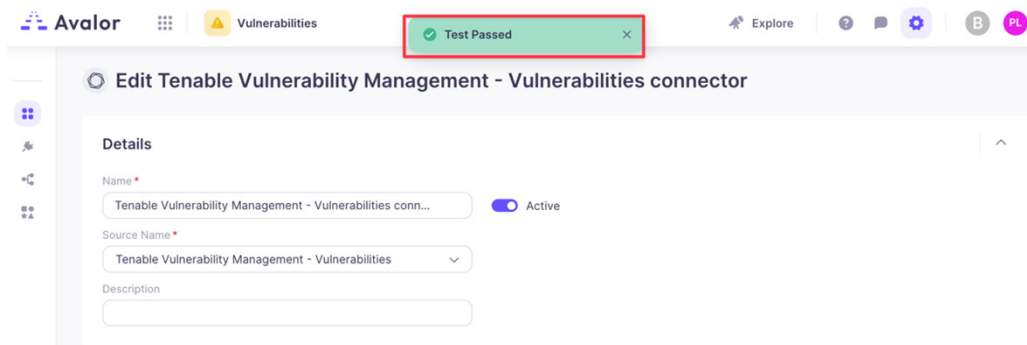


Figure 6. Test Passed

7. Click **Save**.

Edit Tenable Vulnerability Management - Vulnerabilities connector

Details

Name *
Tenable Vulnerability Management - Vulnerabilities conn... Active

Source Name *
Tenable Vulnerability Management - Vulnerabilities

Description

Retrieval

Access Key *

Secret Key *

☐ Split findings by Output

☐ Include Info-Level Severity Data

Scheduling

Full Refresh Frequency *
Daily

Time (UTC) *
10:00 PM

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 Finding Immediately 0

OR

☐ 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

Select Field Contains Type Value

+ AND + OR

☒ Prevent NULL from overriding existing values

Cancel Test Save

Figure 7. Create Tenable Vulnerability Management—Vulnerabilities Connector

Configure the Tenable Vulnerability Management—Issues Data Source

To configure the Tenable Vulnerability Management issues data source:

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

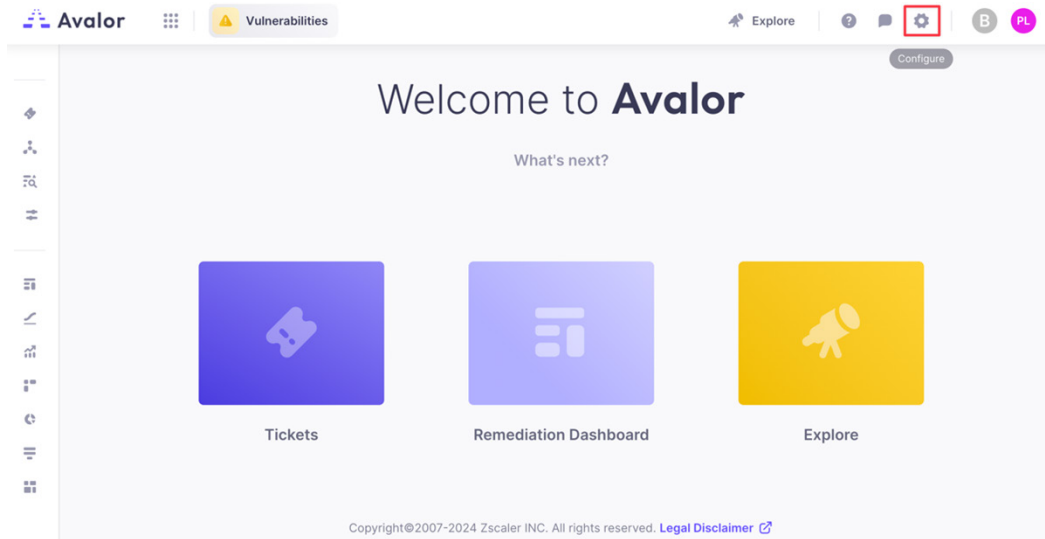


Figure 8. Configure

3. Click **Create**, then search for **Tenable Vulnerability Management—Issues**.
4. Click the Tenable Vulnerability Management—Issues application.

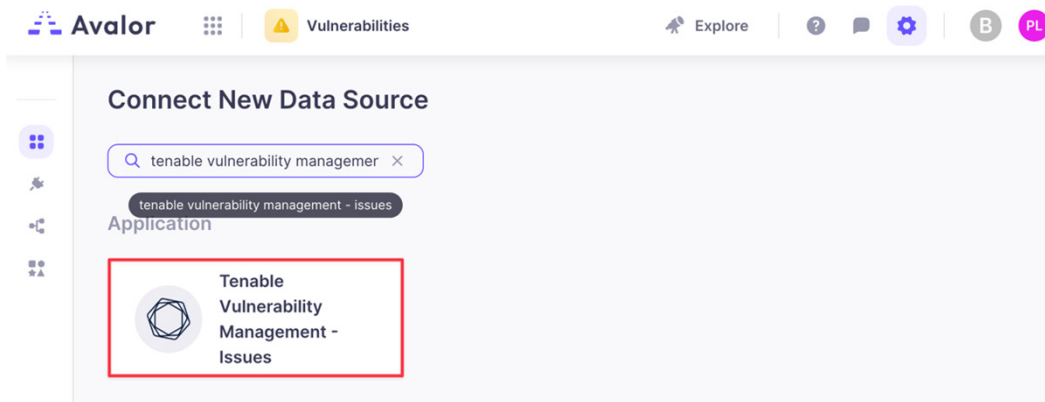


Figure 9. Tenable Vulnerability Management—Issues

5. On the **Create Tenable Vulnerability Management—Issues Source** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Access key:** Enter the Access you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - d. **Secret Key:** Enter the Secret Key you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - e. **Split findings by Output:** Select the checkbox to split findings by output.
 - f. **Include Info-Level Severity Data:** Select the checkbox to include info-level severity data.
 - g. **Full Refresh Frequency:** Set your desired schedule for extracting all data.
 - h. **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.
 - i. **Suppression Rules:** Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, refer to the [Avalor documentations](#).
 - j. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
6. Click **Test**. If the API key and region have been entered correctly, the system responds with Test Passed.

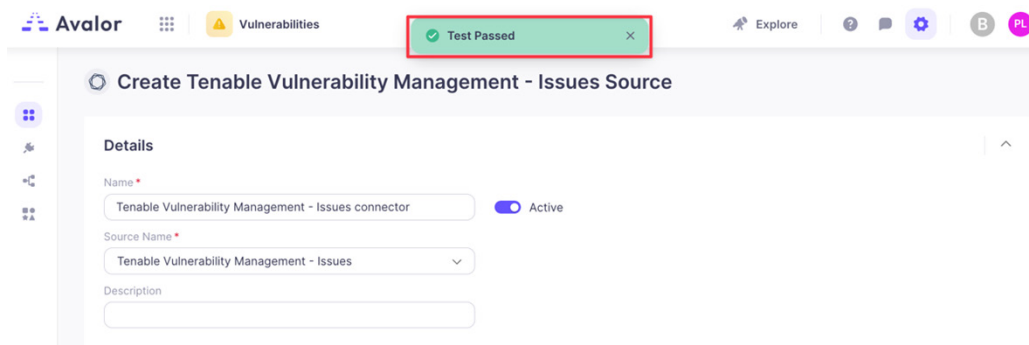


Figure 10. Test Passed

7. Click **Save**.

Create Tenable Vulnerability Management - Issues Source

Details

Name *

Tenable Vulnerability Management - Issues connector

Active

Source Name *

Tenable Vulnerability Management - Issues

Description

Retrieval

Access Key *

Secret Key *

☐ Split findings by Output

☐ Include Info-Level Severity Data

Scheduling

Full Refresh Frequency *

Daily

Time (UTC) *

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 Finding

Immediately

0

OR

☐ 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

Select Field

Contains

Type Value

+ AND

+ OR

☒ Prevent NULL from overriding existing values

Cancel

Test

Save

Figure 11. Create Tenable Vulnerability Management—Issues Source

©2024 Zscaler, Inc. All rights reserved. 15

Configure the Tenable Vulnerability Management—Assets Data Source

To configure the Tenable Vulnerability Management assets data source:

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

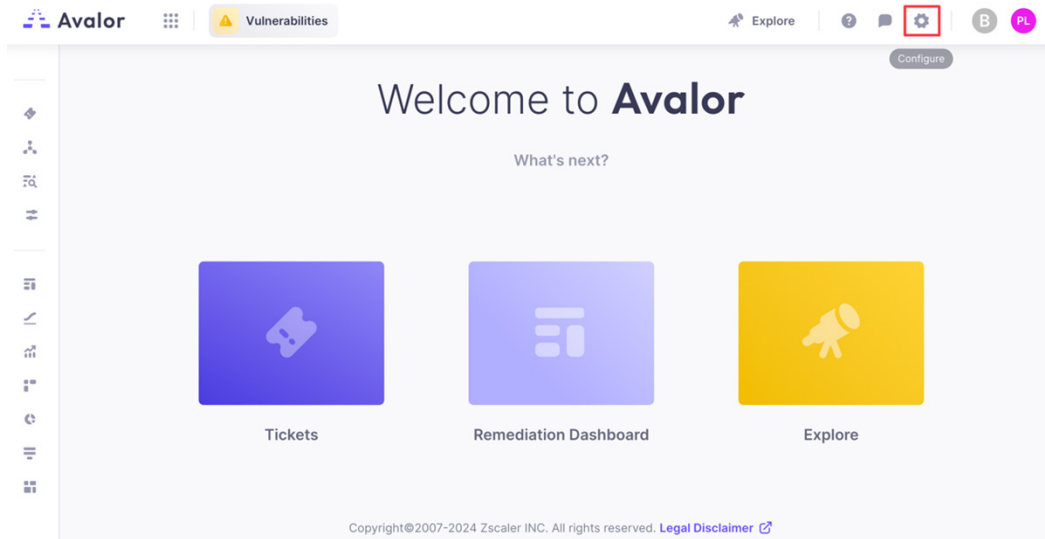


Figure 12. Configure

3. Click Create, then search for Tenable Vulnerability Management—Assets.

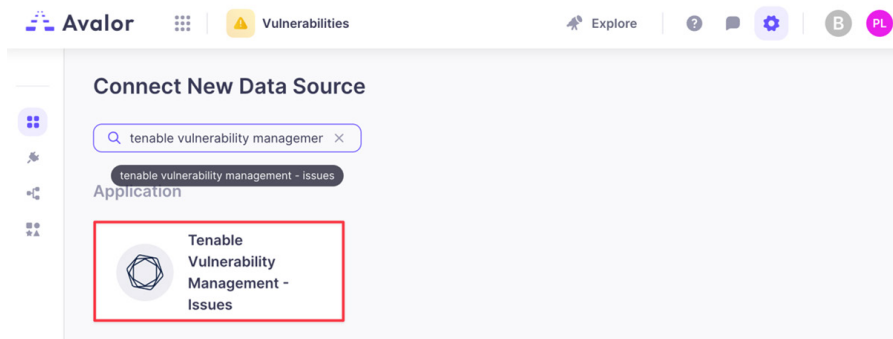


Figure 13. Tenable Vulnerability Management—Assets

4. Click the **Tenable Vulnerability Management—Assets** application.
5. On the **Create Tenable Vulnerability Management—Assets Source** page, complete the following:
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Access key:** Enter the Access you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - d. **Secret Key:** Enter the Secret Key you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - e. **Split findings by Output:** Select the checkbox to split findings by output.
 - f. **Include Info-Level Severity Data:** Select the checkbox to include info-level severity data.
 - g. **Full Refresh Frequency:** Set your desired schedule for extracting all data.
 - h. **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.

- i. **Suppression Rules:** Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, refer to the [Avalor documentation](#).
 - j. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally.
6. Click **Test**. If the API key and region have been entered correctly, the system responds with Test Passed.

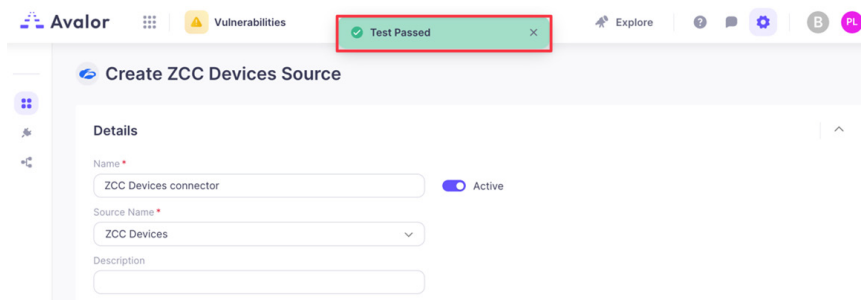


Figure 14. Create Tenable Vulnerability Management—Issues Source

7. Click **Save**.

Figure 15. Create Tenable Vulnerability Management—Issues 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 map a Has ZCC Data Model Entity using the Zscaler Client Connector Source to the ingested Tenable Vulnerability Management—Vulnerabilities data source so that this field can be used as a mitigating score factor when calculating risk for an asset.

Create an API Key in the Zscaler Client Connector Portal

To enable the Zscaler Client Connector API for your organization, contact Zscaler Support.

1. Log in to your ZIA Admin Portal.
2. Select **Policy > Zscaler Client Connector Portal**.

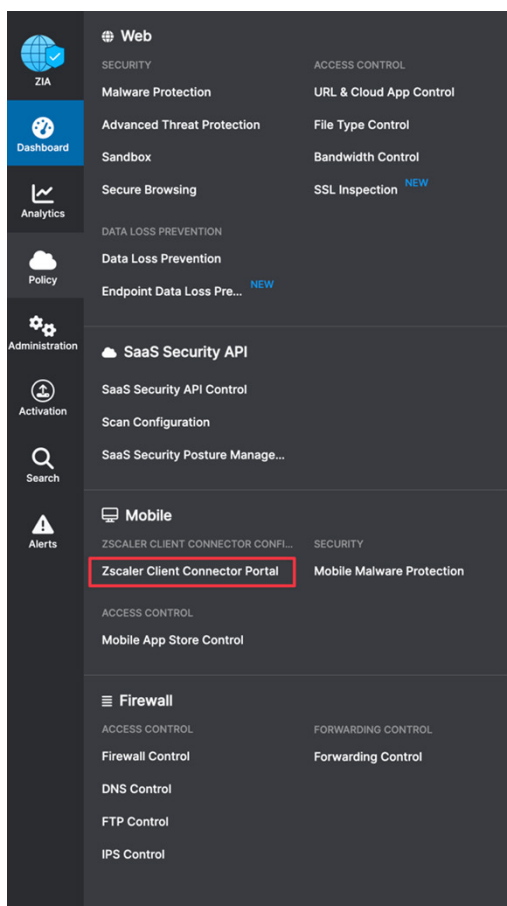


Figure 16. Zscaler Client Connector Portal

3. Click **Administration > Public API**.

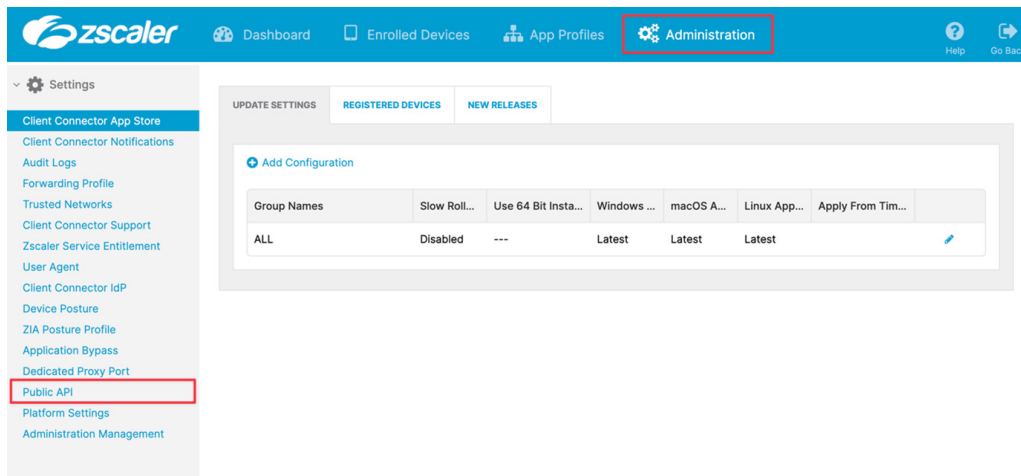


Figure 17. Public API

4. Click **Add API Key**.

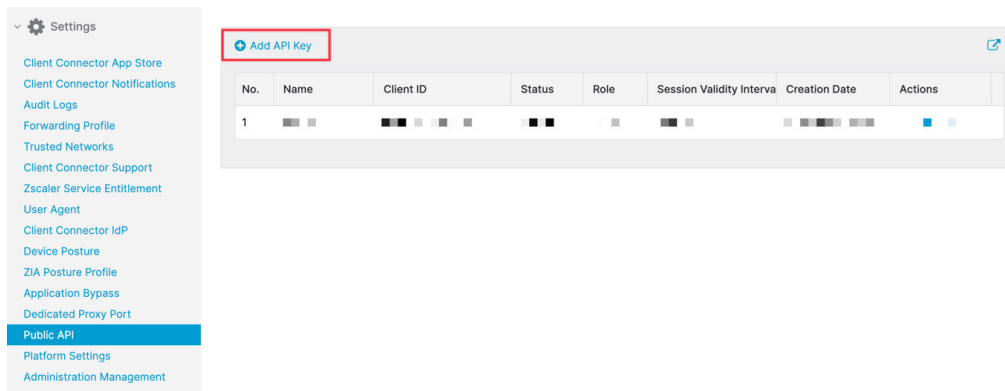


Figure 18. Add API Key

5. Complete the following

- Name:** Enter a name for the API key.
- Session Validity Interval (In Seconds):** Enter the number of seconds for which a session is valid (i.e., 86400 for 24 hours).

The screenshot shows the 'Add API Key' form. It has a blue header bar with the title 'Add API Key' and a close button. The form contains the following fields:

- Name:** A text input field with the value 'avalor'.
- Status:** A toggle switch with 'Enabled' selected.
- Role:** A dropdown menu with 'Read' selected.
- Session Validity Interval (In Seconds):** A text input field with the value '86400'.

At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 19. Configure the API Key

6. Click **Save**. The client secret is displayed.
7. Copy the client secret for use later.

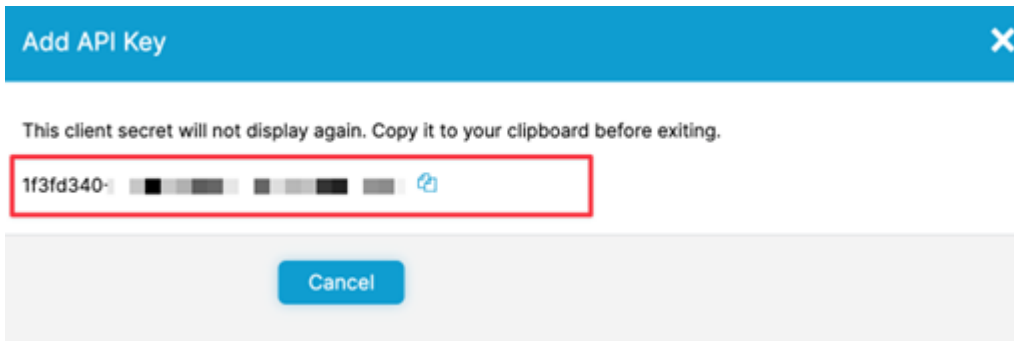


Figure 20. Copy the Client Secret

Configure the Zscaler Client Connector Devices Data Source

To configure the Zscaler Client Connector devices data source:

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

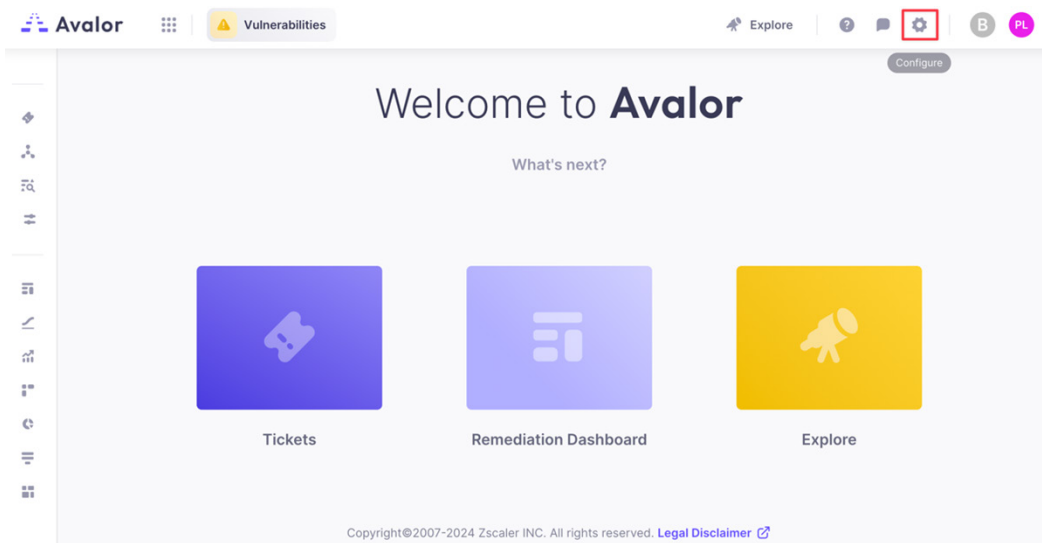


Figure 21. Configure

3. Click **Create**, then search for ZCC.

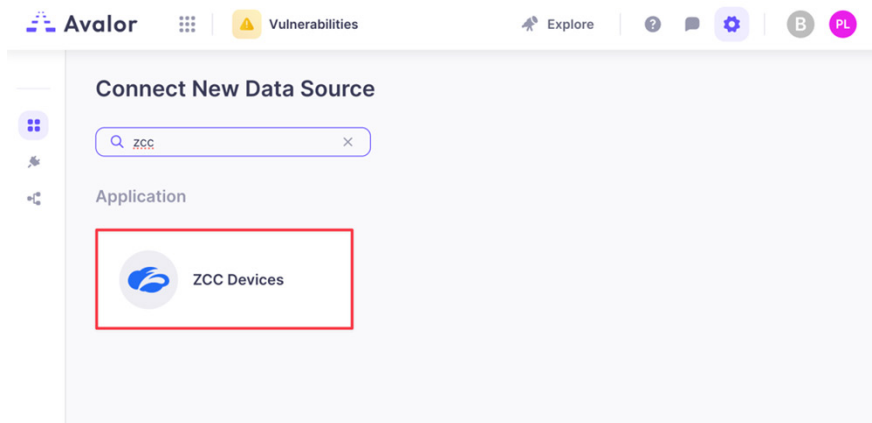


Figure 22. ZCC Devices

4. Click the **ZCC Devices** application.
5. On the **Create ZCC Devices Source** page, complete the following
 - a. **Name:** Enter a name for the Data Connector.
 - b. **Active:** Toggle to enable the Data Connector.
 - c. **Access key:** Enter the Access you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - d. **Secret Key:** Enter the Secret Key you noted in [Create an API Key in the Tenable Cloud Portal](#).
 - e. **Split findings by Output:** Select the checkbox to split findings by output.
 - f. **Full Refresh Frequency:** Set your desired schedule for extracting all data.
 - g. **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.
 - h. **Suppression Rules:** Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, refer to the [Avalor documentation](#).
 - i. **Remediation Detection Settings:** Select your desired option to determine when findings automatically turn undetected. To learn more, refer to the [Avalor documentation](#). Automatic remediation detection only applies when data is refreshed fully, not incrementally..
6. Click **Test**. If the API key and region have been entered correctly, the system responds with Test Passed.

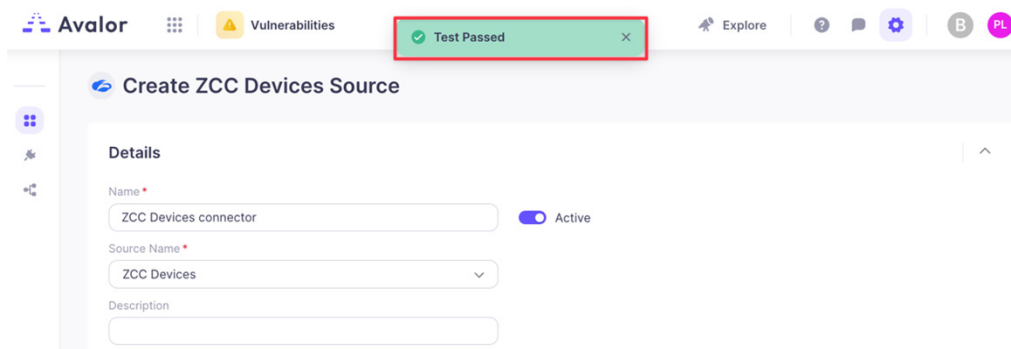


Figure 23. Test Passed

7. Click **Save**.

Create ZCC Devices Source

Details

Name *

ZCC Devices connector

Active

Source Name *

ZCC Devices

Description

Retrieval

Api Key *

Secret Key *

Cloud Name *

zscaler2wo

Scheduling

Full Refresh Frequency *

Daily

Time (UTC) *

06:00 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

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

Fallback

Age immediately if Finding was not seen for

day(s)

Advanced Settings

Suppression Rules

Select Field

Contains

Type Value

+ AND

+ OR

☒ Prevent NULL from overriding existing values

Cancel

Test

Save

Figure 24. Create ZCC Devices Source

Map the Zscaler Client Connector Devices Data Source

To map the Zscaler Client Connector devices data source:

1. Select **Configure** > <newly created ZCC Devices Connector> .
2. Click **Map Data**.

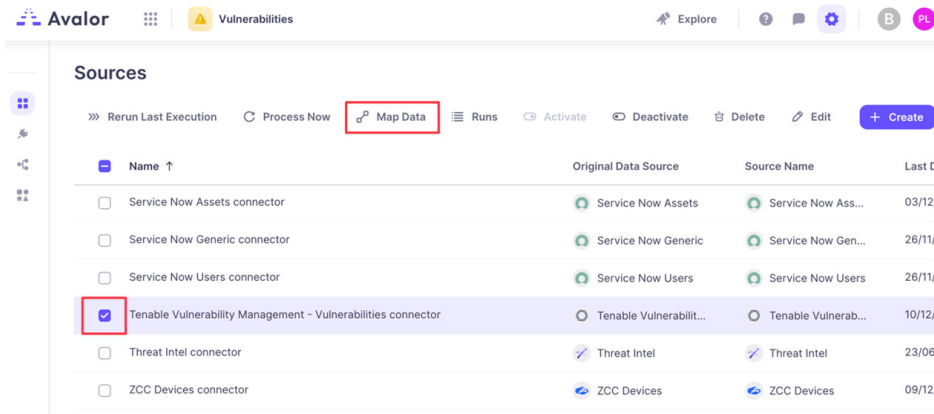


Figure 25. Map Data

3. In the **Map connector** window:
 - a. Create a new connection between the **Asset Key** and the **machineHostname** by:
 - i. On the right side, under **Asset**, drag **Key** to the **Create New Connection** element.
 - ii. On the left side, drag **machineHostname** to the **Create New Connection** element.
 - iii. Click **Map**.

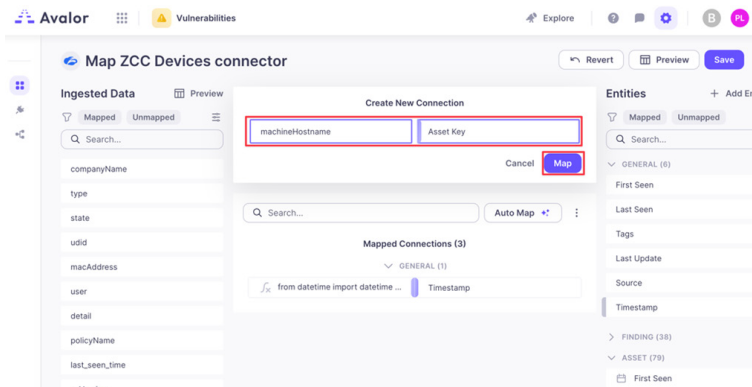


Figure 26. Map

iv. Click the **Key** icon on the **Key** field.

asset.fqdn	FQDN
asset.hostname	Hostname
asset.hostname	Name
asset.device_type	Type
asset.mac_address	MAC Address
asset.hostname	Key

Figure 27. Key field

b. Select **Entities > Asset > +**.

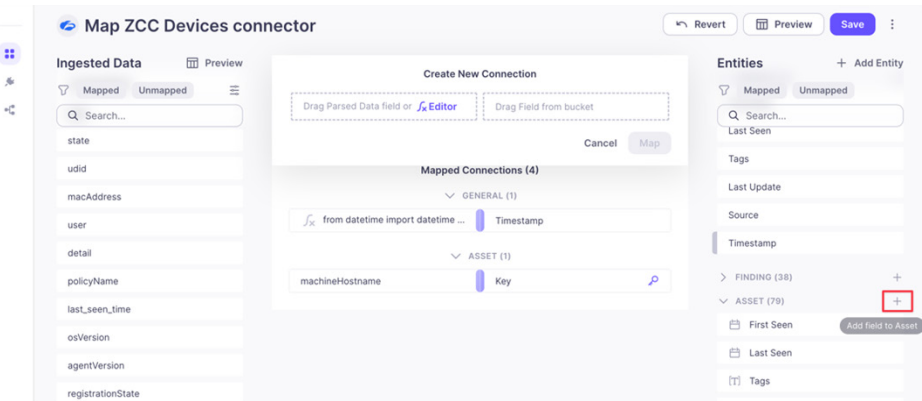


Figure 28. Click +

c. Create a new field called **Has ZCC** of type **Boolean** and click **Add**.

Field Name *

Has ZCC

Field Type

☒ Boolean

Add

Figure 29. New field

- d. Drag the **Has ZCC** field to the **Create New Connection** element, then click **Editor**, select **Value**, enter **True** in the **Value Editor**.
- e. Click **Map**.

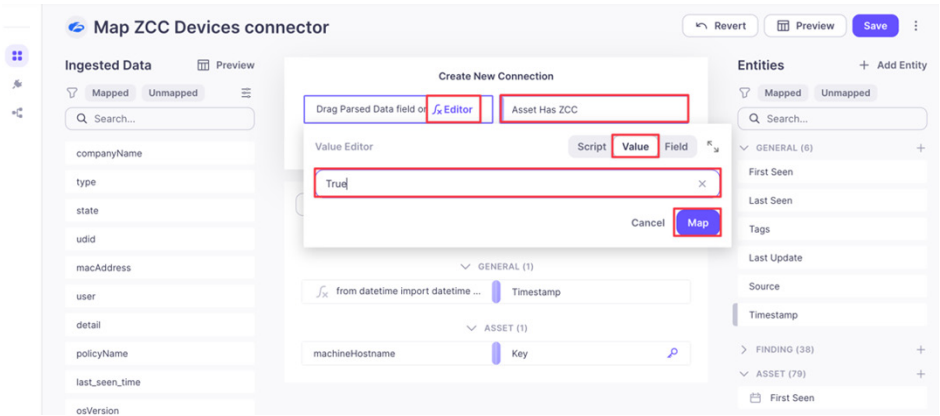


Figure 30. Has ZCC

- 4. Click **Save**.
- 5. Select the **ZCC Devices Connector**, and click **Process Now**.

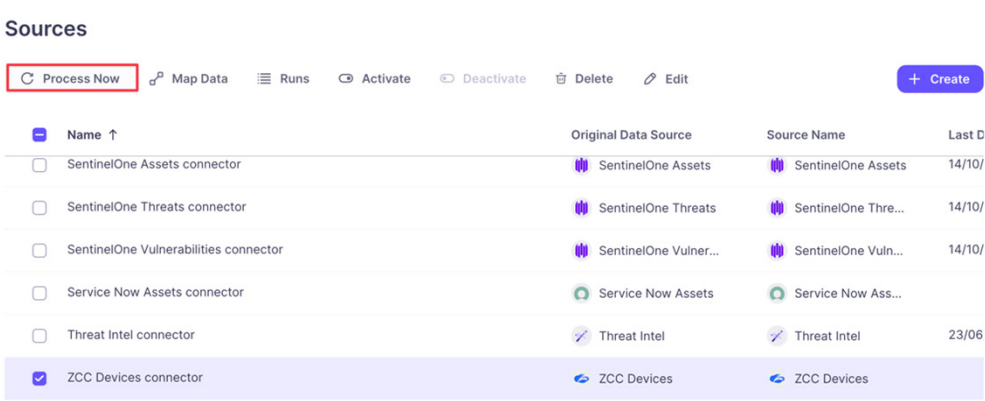


Figure 31. ZCC Devices Connector

Map the Tenable Vulnerability Management—Vulnerabilities Data Source

To map the Tenable Vulnerability Management vulnerabilities data source:

1. Select **Configure** > <newly created Tenable Vulnerability Management - Vulnerabilities Connector>.
2. Click **Map Data**.

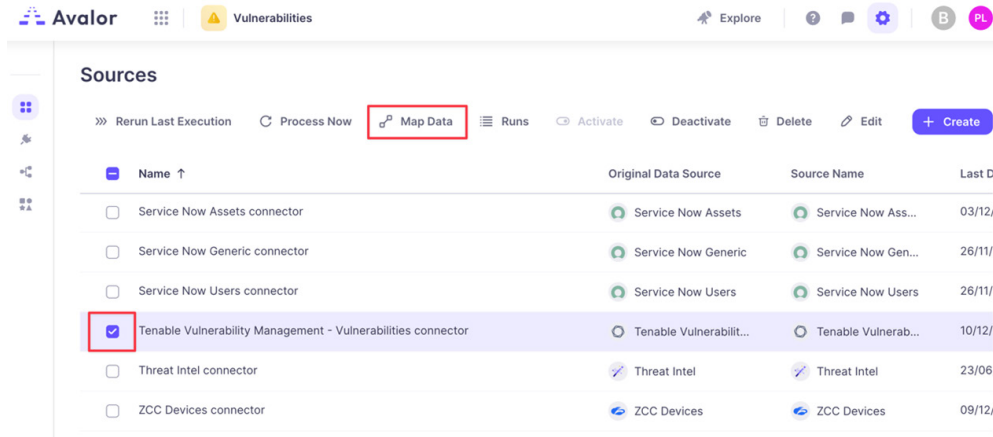


Figure 32. Map Data

3. In the **Map connector** window:
 - a. Create a new connection between the **Asset Key** and the **asset.hostname**:
 - i. Under **Asset**, click the **Purple Bar** element to **Unmap the Key** entity.

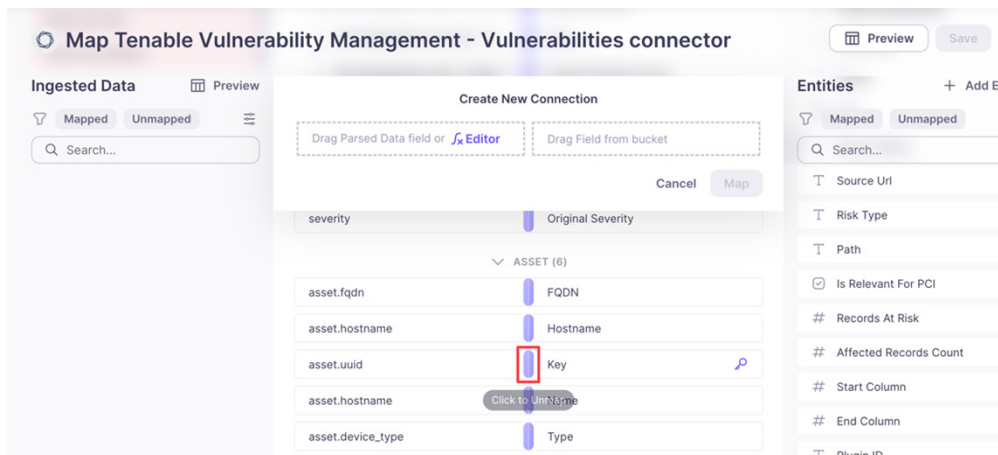


Figure 33. Unmap the Key

- ii. Double-click the **hostname** data entity under asset to update the **Asset Key** connection, then click **Map**.

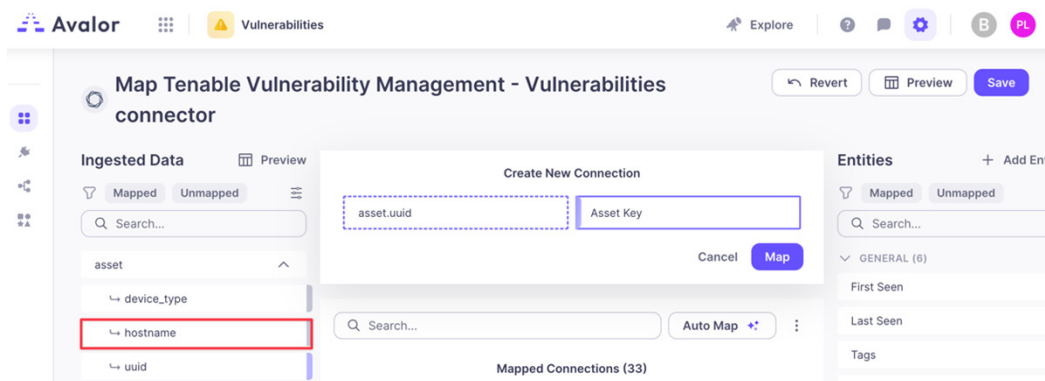


Figure 34. Asset Key

- iii. Click the **Key** icon on the **Key** field.



Figure 35. Key field

4. Click **Save**.
5. Select the **Tenable Vulnerability Management—Vulnerabilities** connector, and click **Process Now**.

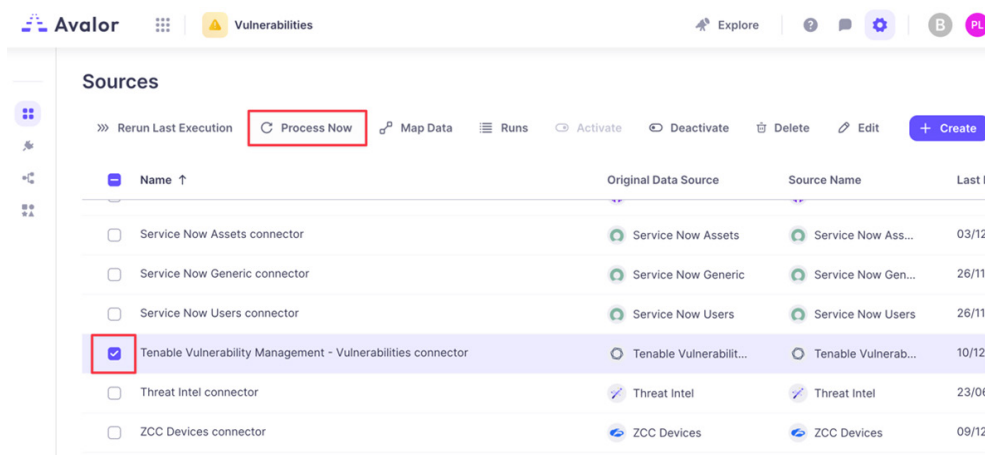


Figure 36. Process Now

6. Click **Full Processing (Complete update of all data)** and then **Process Now**.



Figure 37. Full Processing

Review and Adjust Risk Scoring

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

The following example shows how the Asset has ZCC field is added as a mitigating factor for risk scoring. A value of True reduces the risk calculation (since the asset has mitigating software installed).

- From the **Vulnerabilities** tab in the **Zscaler UVM dashboard (Remediation Hub)**.
 - In the left pane, select **Settings > Score**.
 - Click **Add Factor** in the **Risk & Mitigating Factors** section.
- In the **Add new factor** modal:
 - Select **Mitigating Factors** for **Factor Type** (Mitigating Factors generally lower risk scoring, while **Risk Factors** generally increases risk scoring).
 - Enter a **Factor Name**.
 - Select **Asset Has ZCC** for **Field**.
 - In the **Boolean** login section, under **True**, enter a percentage by which the risk is reduced.

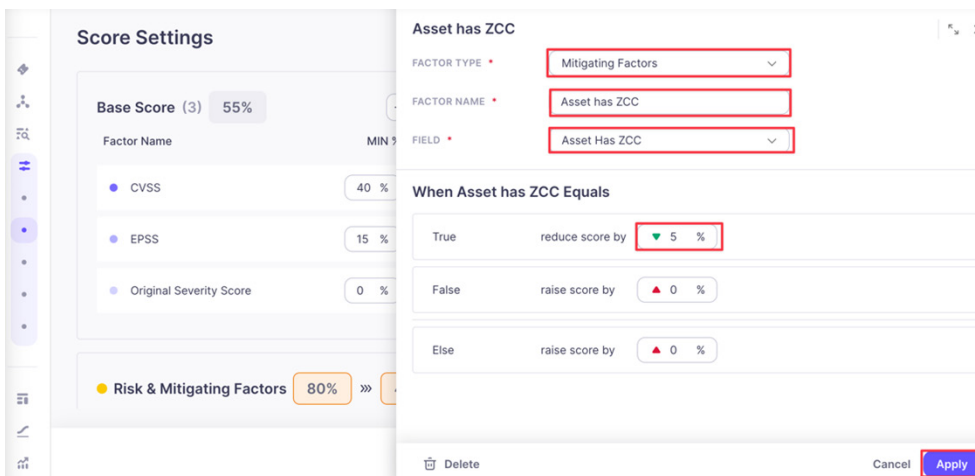


Figure 38. Asset Has ZCC

- Click **Apply**, then **Save**.
- In the left-hand navigation, select the **Assets** dashboard. From the **Assets** dashboard:
 - Set a filter by clicking the **More** button and adding the **Has ZCC = True Entity**.

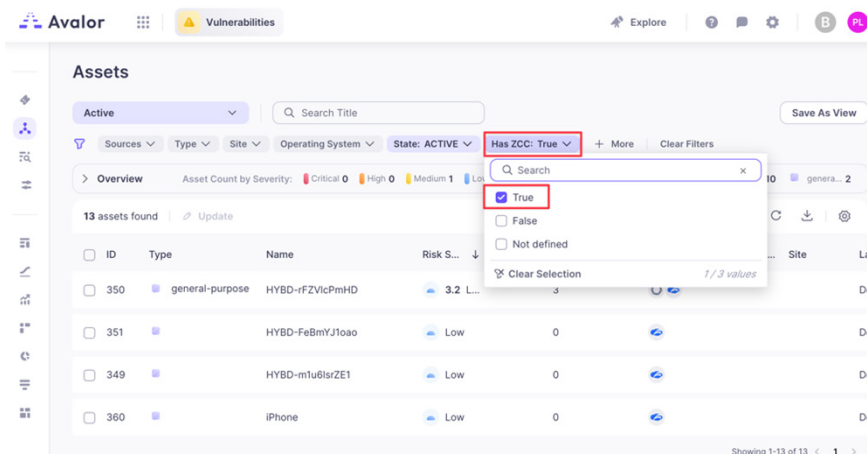


Figure 39. Has ZCC = True Entity

- b. Click one of your **Assets** in the filtered list that also has **Tenable Vulnerability Management - Vulnerabilities**.
- c. In the **Asset** modal that appears, click the **Findings** tab.
- d. Click one of the **Findings**.
- e. Review the output (notice the **Score Adjustment** section and whether **Asset has ZCC** has modified the risk scoring).

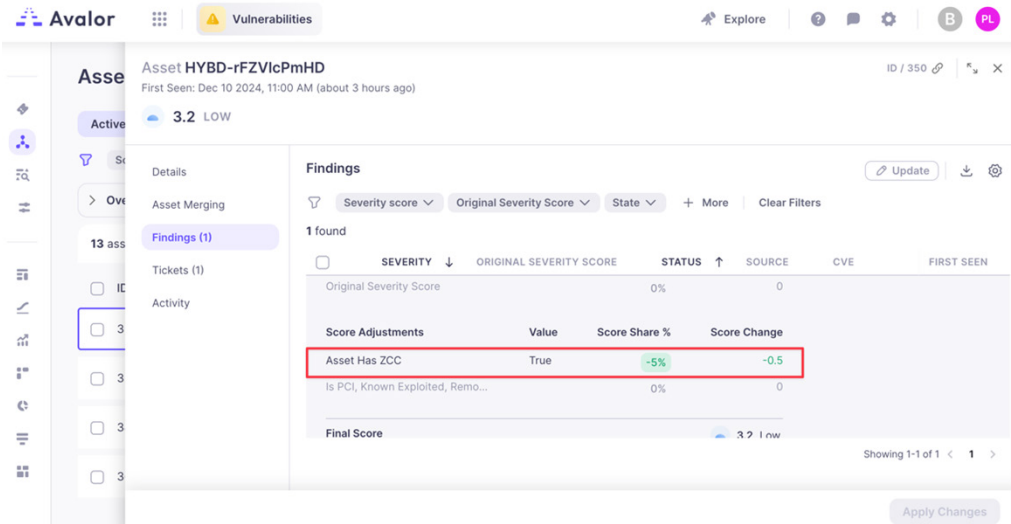


Figure 40. Risk Scoring

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.

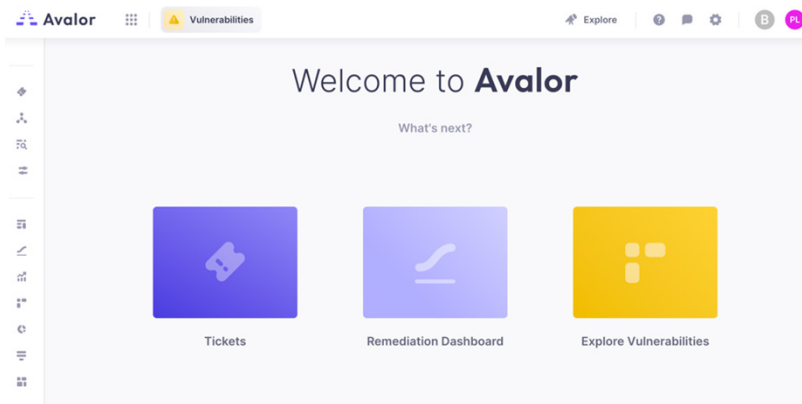


Figure 41. Zscaler UVM Platform

2. Click **Contact Support**.

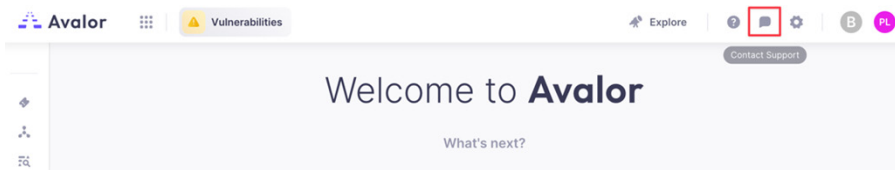


Figure 42. Contact Support

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

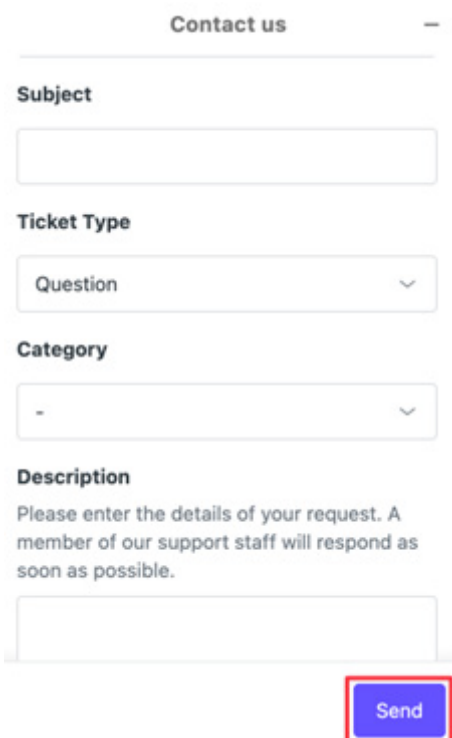
The screenshot shows the 'Contact us' form. It has a title 'Contact us' at the top. Below the title are four input fields: 'Subject' (a text box), 'Ticket Type' (a dropdown menu with 'Question' selected), 'Category' (a dropdown menu with '-' selected), and 'Description' (a larger text box with placeholder text: 'Please enter the details of your request. A member of our support staff will respond as soon as possible.'). At the bottom right of the form is a blue 'Send' button, which is highlighted with a red rectangular box.

Figure 43. Contact us