ZSCALER AND TANIUM DEPLOYMENT GUIDE

AUGUST 2025, VERSION 1.1

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
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

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.

Tanium Overview

Tanium is a leading cybersecurity and endpoint management provider, delivering real-time visibility and control across enterprise-scale environments. Founded in 2007 and headquartered in Kirkland, Washington, Tanium's innovative platform offers unparalleled speed, scale, and reliability, empowering organizations to manage and secure millions of endpoints seamlessly. Its unique architecture enables security and IT operations teams to rapidly detect threats, remediate vulnerabilities, and manage endpoints from a single integrated platform.

Tanium's extensive capabilities include threat detection, incident response, vulnerability and patch management, asset discovery, and compliance monitoring. By unifying endpoint management and security through a single console, Tanium significantly reduces complexity, streamlines operations, and provides immediate insights into security posture. Trusted by major enterprises, government agencies, and Fortune 500 companies worldwide, Tanium helps organizations achieve superior endpoint security and operational efficiency. To learn more, refer to Tanium'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
- Tanium 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 following prerequisites are completed:

ZIA

- An active instance of ZIA.
- Administrator login credentials to ZIA.

Zscaler UVM:

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

Tanium:

- An active Tanium tenant.
- Administrator login credentials to your Tanium Tenant.

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 Tanium Introduction

Overviews of the Zscaler and Tanium 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 it as a secure internet onramp - all you do is make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Browser Isolation, allowing you 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 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	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.

Tanium Autonomous Endpoint Management Overview

Tanium is a premier endpoint management provider, offering advanced, real-time visibility and control across extensive enterprise environments.

Tanium's Autonomous Endpoint Management (AEM) suite includes comprehensive capabilities such as asset inventory, configuration management, patch deployment, software distribution, and compliance reporting. Leveraging real-time data collection and automation, Tanium simplifies and accelerates endpoint operations, providing deep visibility and actionable insights that drive productivity and reduce operational risks. Trusted by leading enterprises, governments, and Fortune 500 companies globally, Tanium helps organizations maintain optimal endpoint performance, security, and compliance at scale.

Tanium Resources

The following table contains links to Tanium support resources.

Name	Definition
Tanium Resource Center	Tanium Documentation and Support.
Support Portal	Tanium Support Portal.

Use Case 1: Deploying Zscaler Client Connector Using Tanium

This document describes how to deploy Zscaler Client Connector to Windows devices in your environment using Tanium's **Deploy** module. This enables IT teams to rapidly install, update, or remove software across distributed endpoints with minimal overhead. You can manage the Zscaler Client Connector (packaged and published in the **Tanium Gallery**) using this capability to simplify deployment at enterprise scale.

Deploy Overview

Deploy is a software management module that you can use to rapidly install, update, and remove software across large organizations with minimal infrastructure requirements. You can create deployments to run during a maintenance window that is convenient for your IT operations.

You can deploy applications or a group of applications either **automatically** or **manually** to a flexible set of targets, including computer groups, user groups, departments, locations, individual computers, and individual users. You can also update existing software installation to the latest available versions, and create custom packages to install, update, and remove applications.

Predefined Package Gallery

The Tanium Deploy Predefined Package Gallery is a collection of software packages that you can use to distribute software package templates. These templates include all the required information for you to import and deploy third-party software.

Tanium publishes updates to the Predefined Package Gallery every two to four hours. Each hour, Deploy checks for updates to the Predefined Package Gallery. For a list of packages in the Predefined Package Gallery, refer to **Reference: Predefined Package Gallery**.

For more information, refer to **Import a software package from the Predefined Package Gallery**.

Before you begin, ensure that your Tanium account has the *Deploy Operator* role assigned within your Tanium tenant, as this is required to perform deployment tasks

Deploy Zscaler Client Connector Using Tanium Deploy

To deploy Zscaler Client Connector using Tanium Deploy:

1. Go to the **Deploy** section in your Tanium Console.

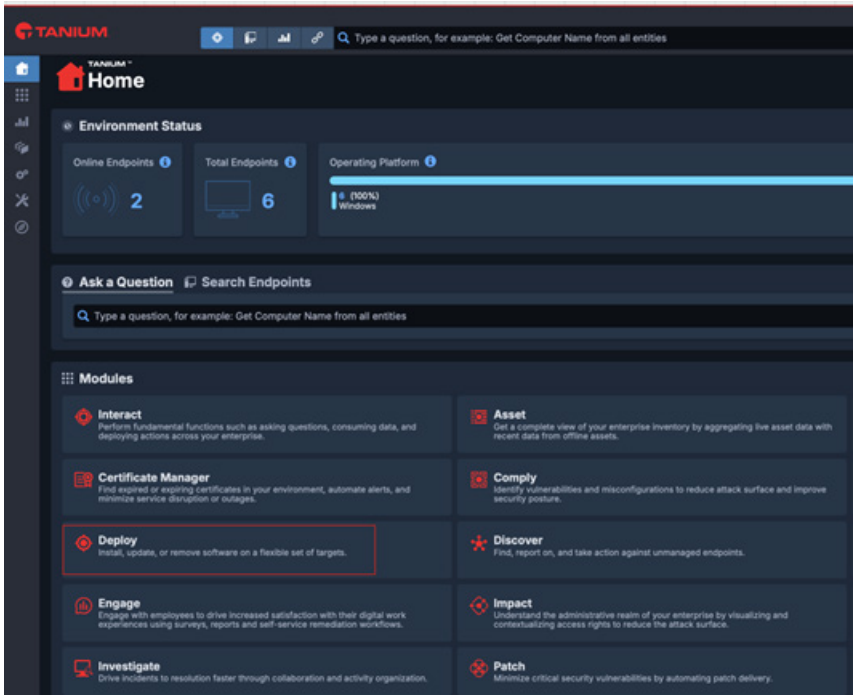

Figure 1. Log in to Tanium Console and navigate to the Deploy section

2. Select the **Package Gallery**.

Figure 2. Go to the Package Gallery

3. Select the **Predefined Package Gallery** tab and select **Zscaler Inc.** from the **Vender** drop-down menu.

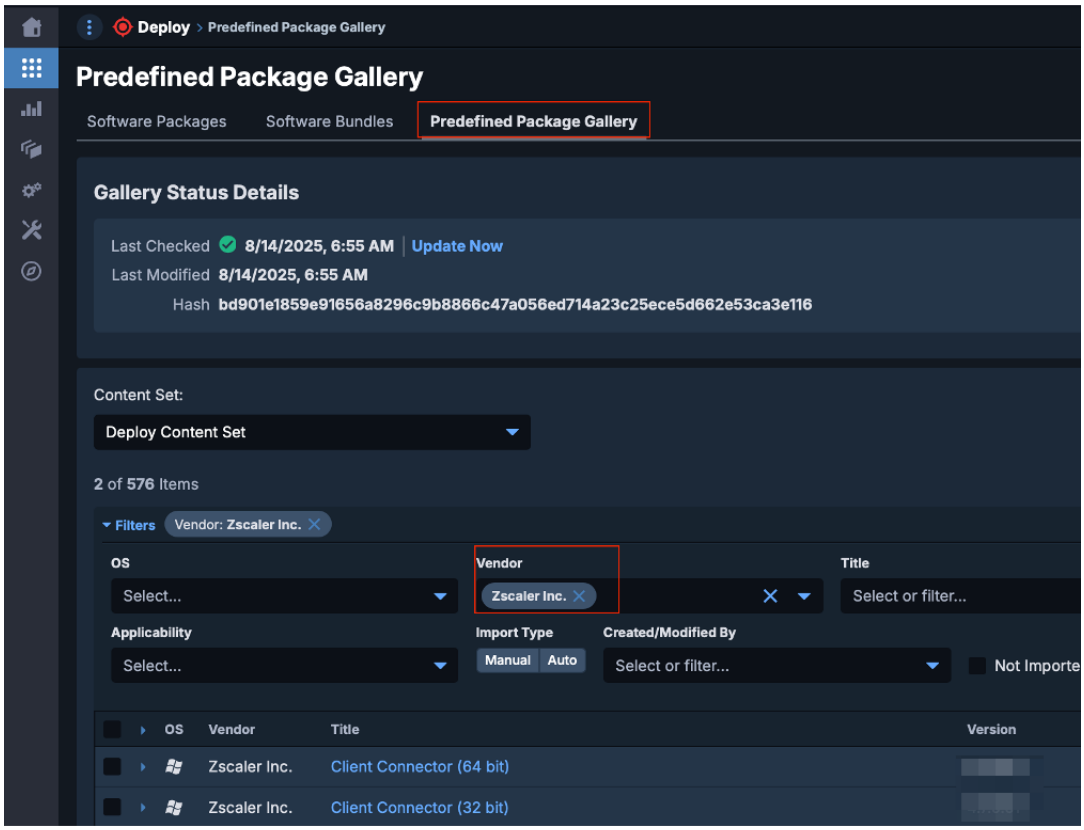

Figure 3. Search for Zscaler

4. In the **Tanium Deploy** module, select **Import Package** to import the **Zscaler Client Connector** package from the **Gallery** into your software management workspace.

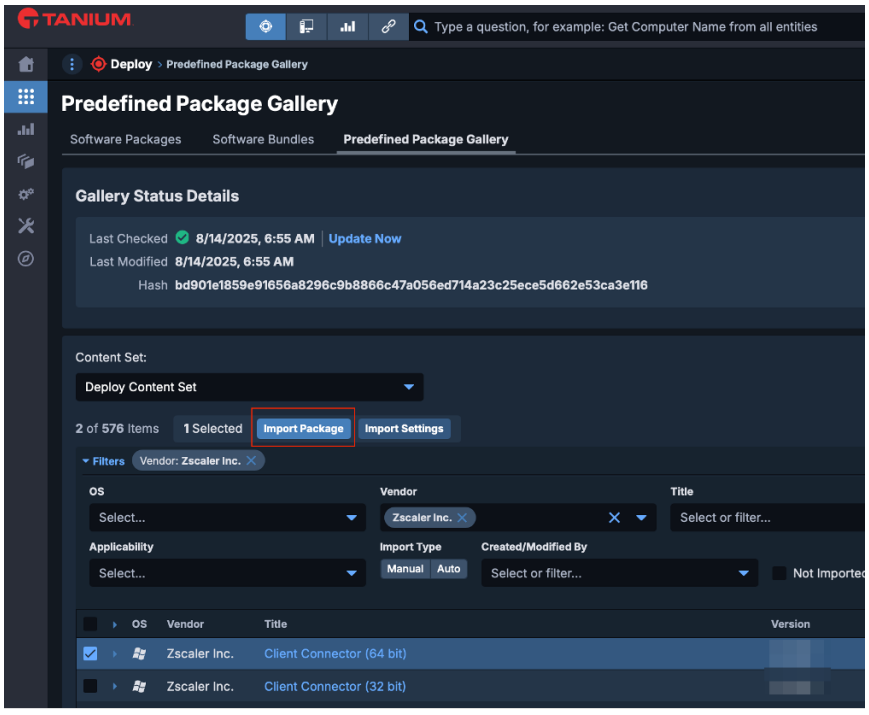

Figure 4. Predefined Package Gallery

5. Click **Yes** to confirm the action.

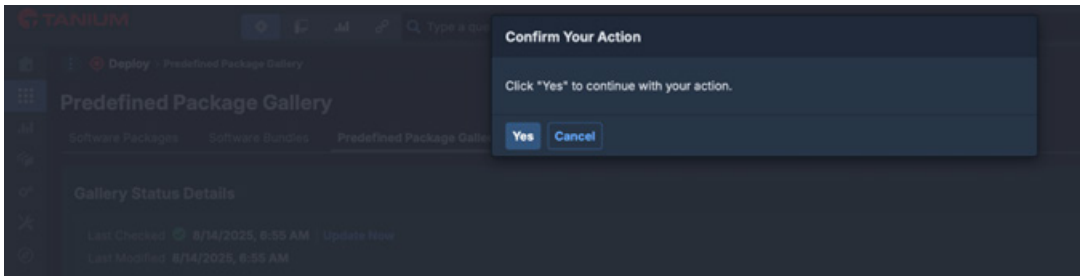

Figure 5. Confirm

6. Click the **Client Connector (64 bit)** or **Client Connector (32 bit)** package title in the list to open it.

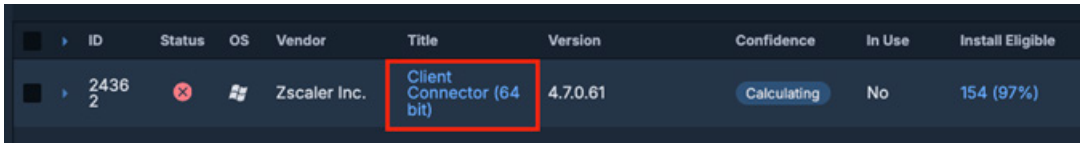

Figure 6. Client Connector (64 bit) package

7. Click **Edit**.

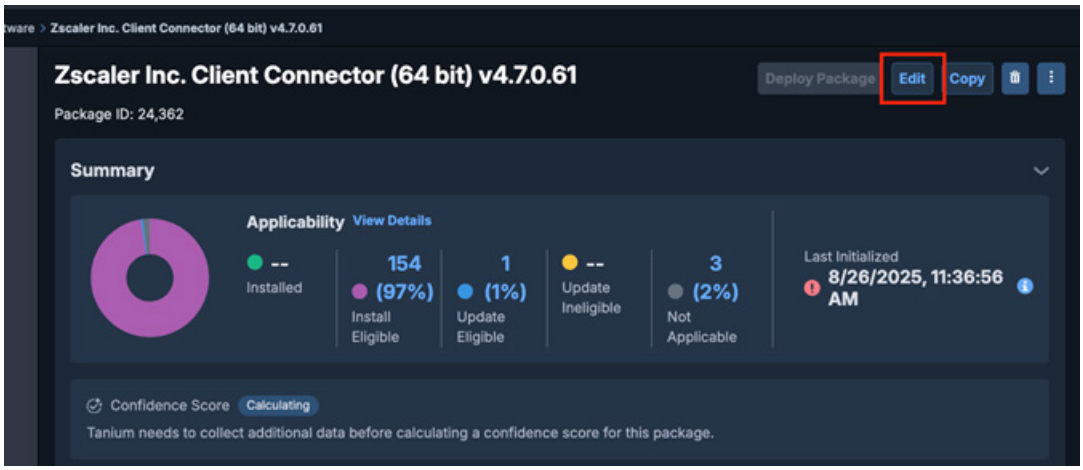

Figure 7. Edit

8. You can customize the command line parameters used for the Zscaler installer for your environment. Review step 2 in the Running the MSI with CLI Options (government agencies, see Running the MSI with CLI Options) of the Zscaler Client Connect help to determine which install options are necessary for your Zscaler deployment.
9. Scroll down to **Deploy Operations** > **Install**. Edit the **Run Command** to include the necessary command line options. Repeat for the **Run Command** under **Deploy Operations** > **Update**.

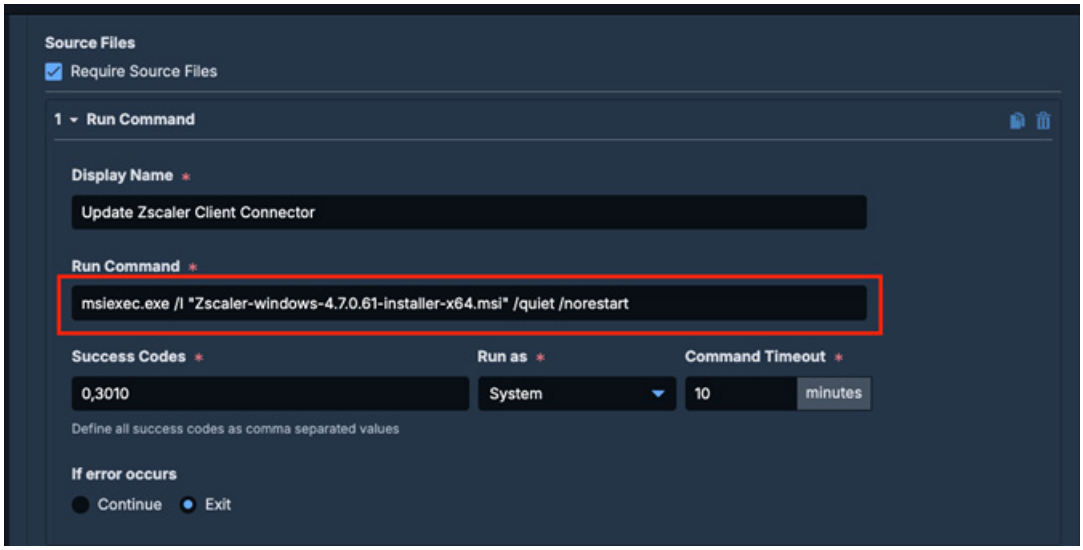

Figure 8. Run Command

10. You might need to customize the command line parameters used for the Zscaler uninstaller. See step 2 of the Uninstall from the Command Line Using the MSI File (government agencies, see Uninstall from the Command Line Using the MSI File) section to determine which install options are necessary for your Zscaler deployment.
11. Scroll down to **Deploy Operations** > **Remove**. Edit the **Run Command** to include the necessary command line options.
12. Scroll to the bottom of the screen and click **Save Package**.

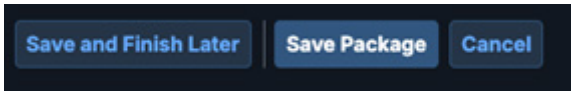

Figure 9. Save Package

13. Define specific endpoints or dynamic groups as deployment targets.

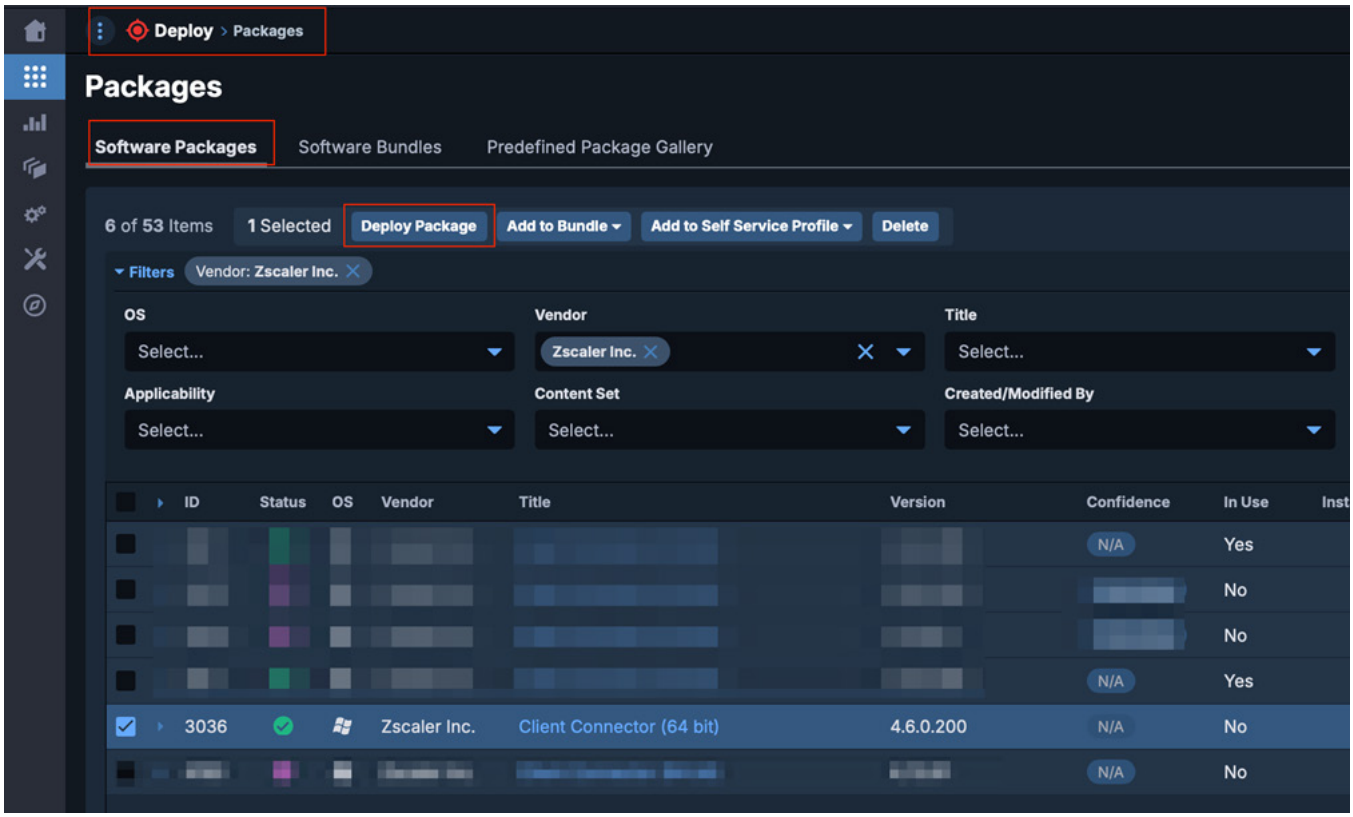

Figure 10. Deploy Zscaler package

14. Select the **Endpoints to Target**.

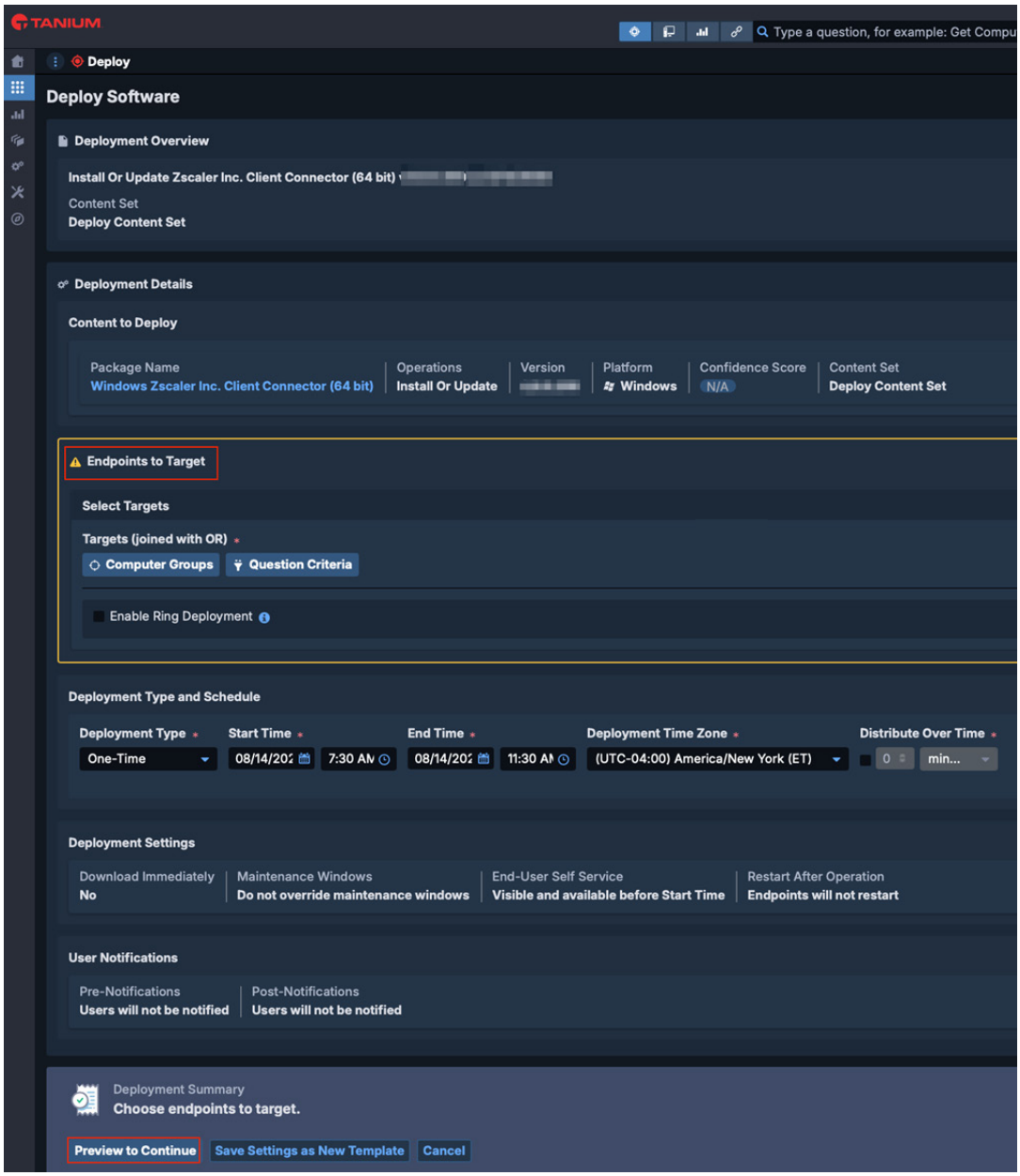

Figure 11. Decide which endpoints to target

15. Initiate the deployment. Tanium distributes and executes the Zscaler Client Connector installation package across your defined targets, while providing centralized visibility into success rates, failure logs, and deployment progress.

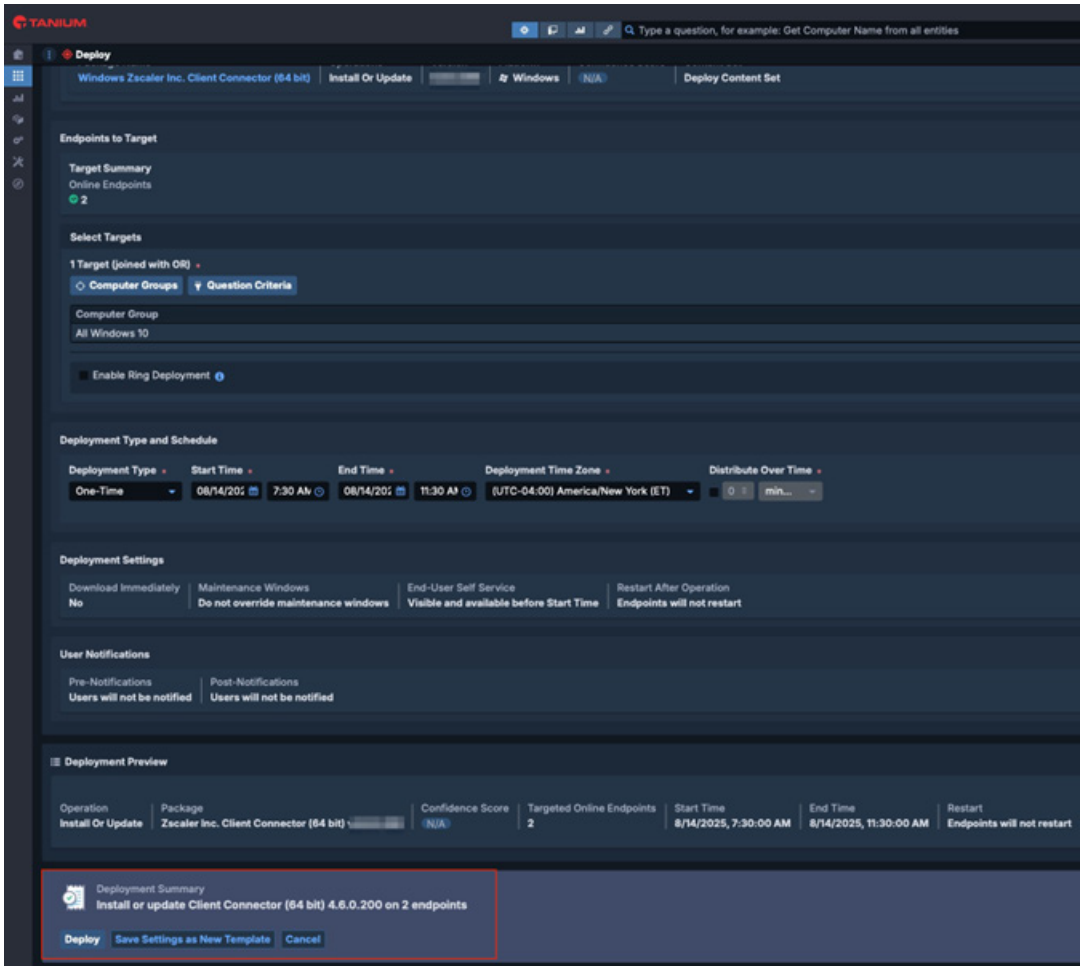

Figure 12. Deploy your changes

Create TLS Exemptions

The following sections describe creating TLS exemptions.

Select the Tanium Domains ZIA TLS Inspection Skips

To prevent any potential communication issues between Tanium agents running on the endpoints and the Tanium cloud, you must exempt certain Tanium specific domains ZIA SSL/TLS inspection policies. You can obtain the customer-specific list of domains by performing the following procedure.

1. In the home section of your Tanium Console, run the query `Get Computer Name` and `Tanium Server Name List from all machines` to get a list of Tanium specific domains pertinent to your deployment. The query returns all the domains that are recommended to be exempted from SSL/TLS inspection in your ZIA tenant.

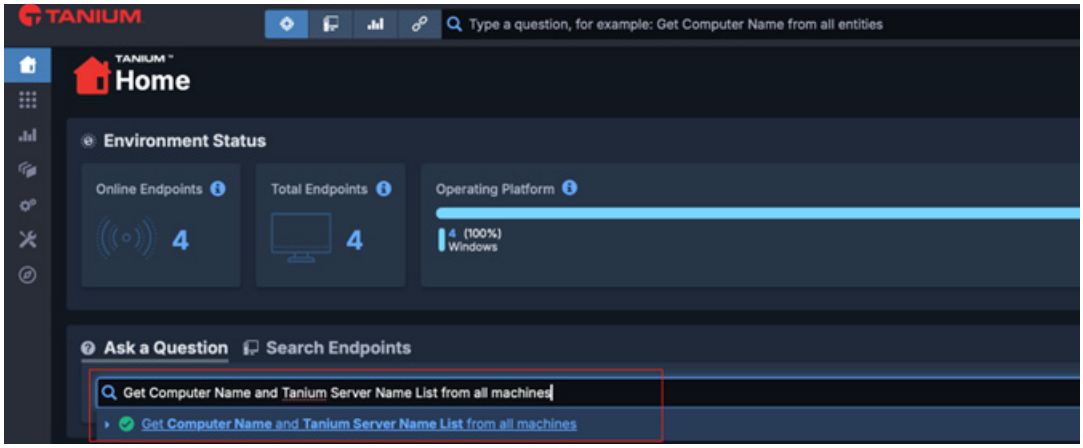

Figure 13. Run the query

2. Make a note of the recommended domains.

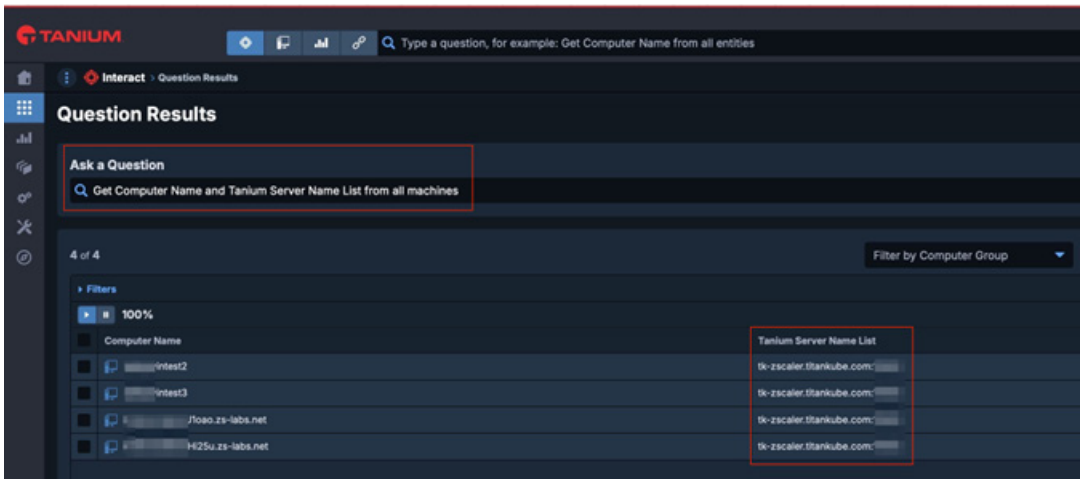

Figure 14. Note the Tanium domains

3. Create a custom URL category in your ZIA tenant by going to **Administration** > **URL Categories** and adding the top-level Tanium domains to this category. In this case, you are adding `.customername.cloud`, which was returned by the Tanium query in the previous step. The "." preceding the domain acts as a wildcard (*) in ZIA (government agencies, see wildcard (*) in ZIA).

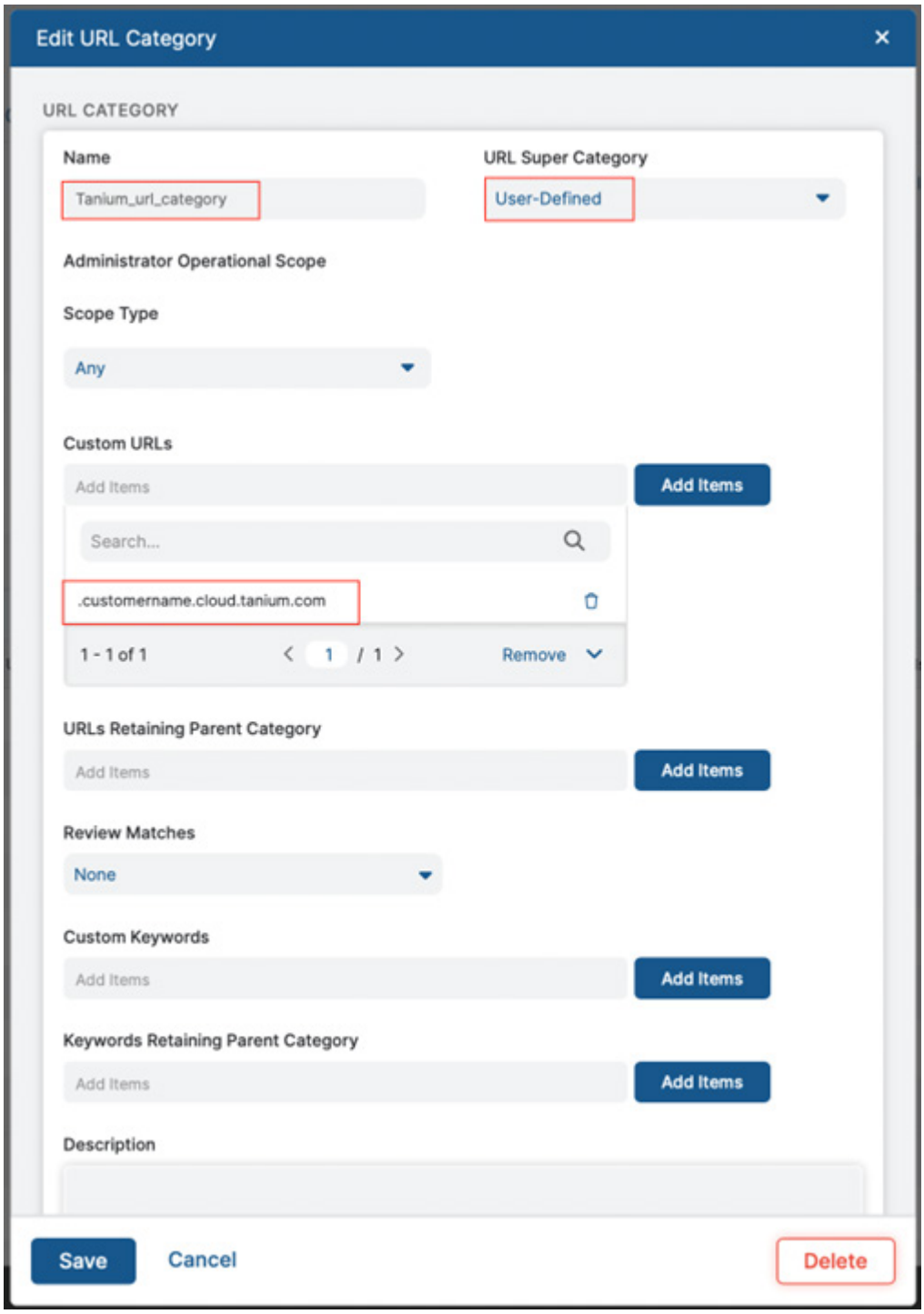

Figure 15. Create a custom URL category for Tanium

4. Update the SSL/TLS exemption policy under **Policy** > **SSL Inspection** in your ZIA tenant to skip inspection of the traffic going to this newly created URL category. Since the policies are evaluated top-down, insert this exemption rule at the appropriate sequence based on your setup.

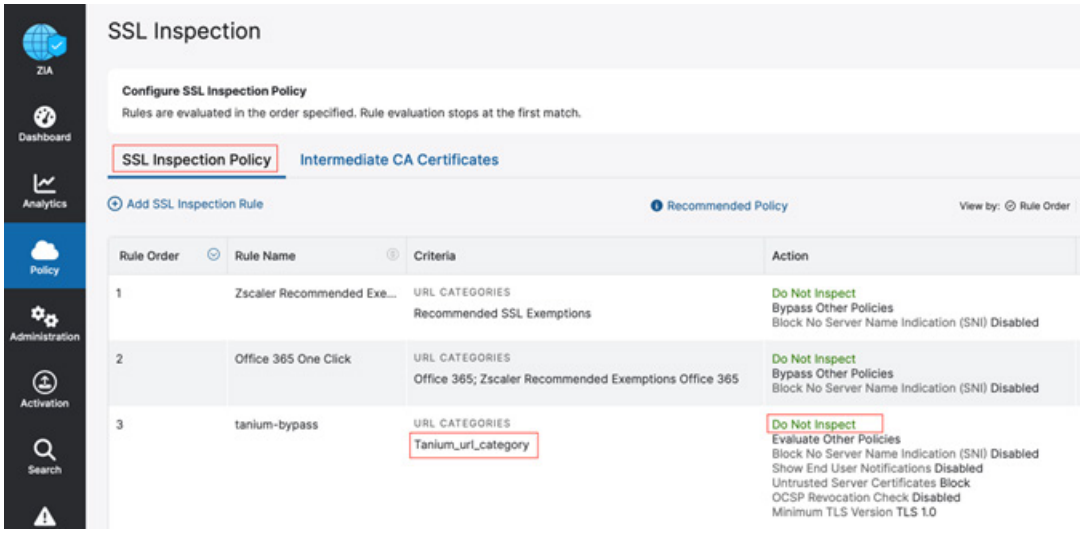

Figure 16. Create ZIA SSL exemption rule

Use Case 2: Contextualizing Risk using Zscaler UVM and Tanium AEM Platform

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 Tanium AEM connectors:

- Tanium Assets: Retrieves essential asset data, such as serial number, computer ID, operating system, IP address.
- Tanium Compliance: Retrieves a detailed list of all compliance findings on the endpoint, including ID, state, category, rule, first found date, last scan date.
- Tanium CVE: Retrieves vulnerability data, including CVE ID, score, summary, last scan date, severity.

Required Parameters

The source authentication configuration requires the following parameters:

- API Key: Your generated API token.
- Domain: Your domain from the API URL.

Roles and Permissions

To issue API URL and Token from the Tanium AEM platform and enable the integration, you must use a user with an Admin Reserved role.

The following lists the necessary permissions and content sets to which the generated API token must be bound:

Streams	Permissions	Content Sets
Tanium Assets Tanium CVE Tanium Compliance	Administration > Token – Use Administration > Token – View Gateway > Gateway API (Execute) Administration > Computer Group (Read) Unrestricted Management Rights (recommended to ensure all endpoint data is accessible) Platform Content Permissions > Sensor (Read)	Base Reserved Default Core Content Performance
Tanium Assets	Assets > Asset API User (Read)	Asset
Tanium CVE Tanium Compliance		Comply Reporting

Retrieving the Parameters

The following sections describe retrieving the parameters.

Retrieving the API Token

To retrieve your API Token in the Tanium AEM Portal, perform the following:

1. Go to **Administration** > **API Tokens**.

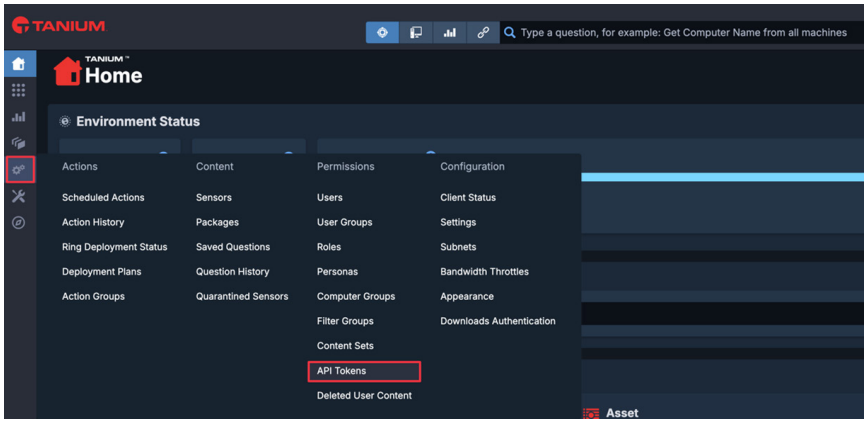

Figure 17. API Tokens

2. Click **New API Token**:
   a. **Notes**: Enter a description for the token.
   b. **Expiration**: Enter the expiration interval in days (default is 7 days, maximum is 365 days).
   c. **Persona:** Select the user account (Default persona) or an **alternative persona** you created for this purpose, with the permissions and content sets listed earlier. The default option is the currently selected persona for your Tanium Console session.
   d. **Trusted IP addresses:** Enter 0.0.0.0/0 or the list of IPs provided in our **IP allowlist article**. Use commas or new lines to separate multiple entries. If you choose to restrict the allowed IPs, follow the IP allowlist article to guarantee you are updated when changes are made to this list.
   e. Click **Create** and **Review** the token details.

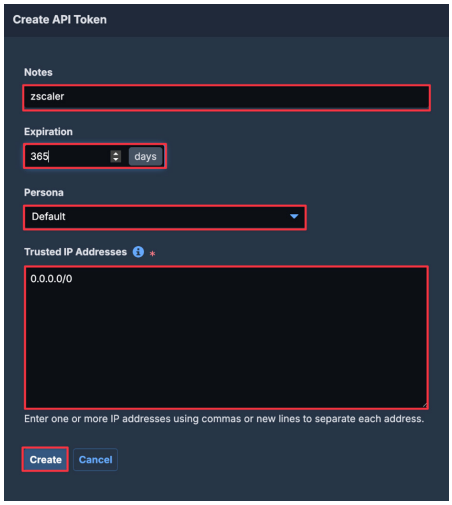

Figure 18. Create API Token

3. Copy the token and **Save** it securely, then click **Close**.

Retrieving the Tanium AEM Domain

The domain is your tenant name as it appears in the API URL:

```
<TENANT_NAME>.cloud.tanium.com
```

For example, if your API URL is: acme.cloud.tanium.com, enter `acme.cloud.tanium.com` in the **Domain** field as shown in the following image:

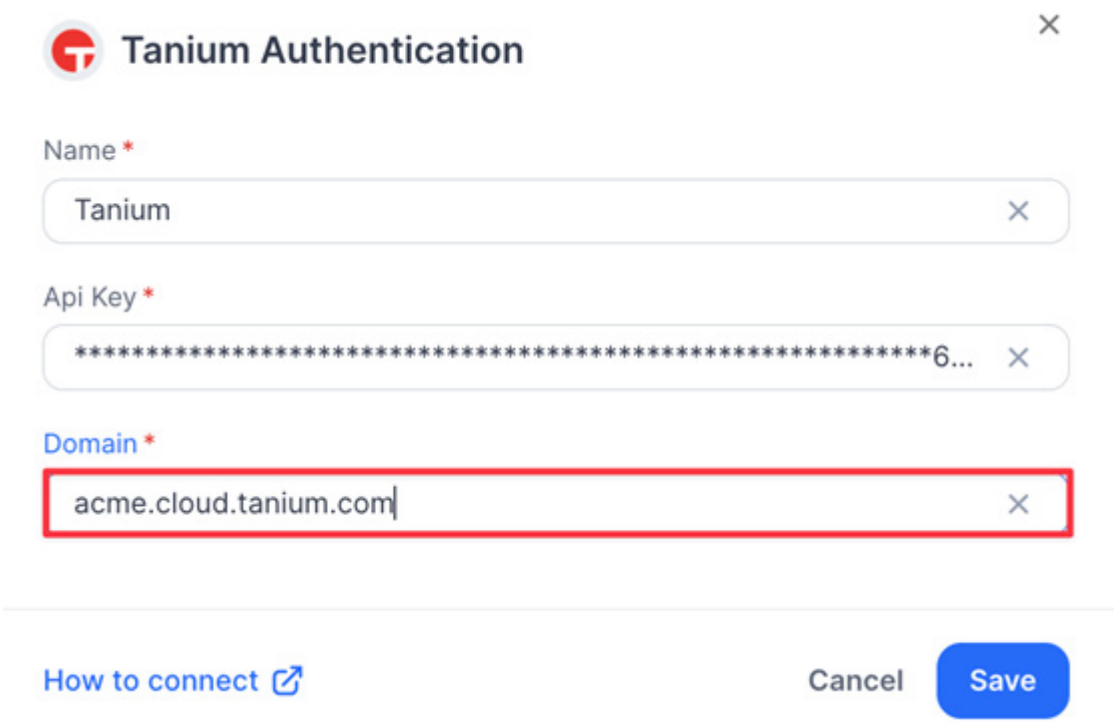

Figure 19. Domain

Configure the Zscaler UVM Data Connectors

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

Configure Authentication for the Tanium AEM Data Source

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

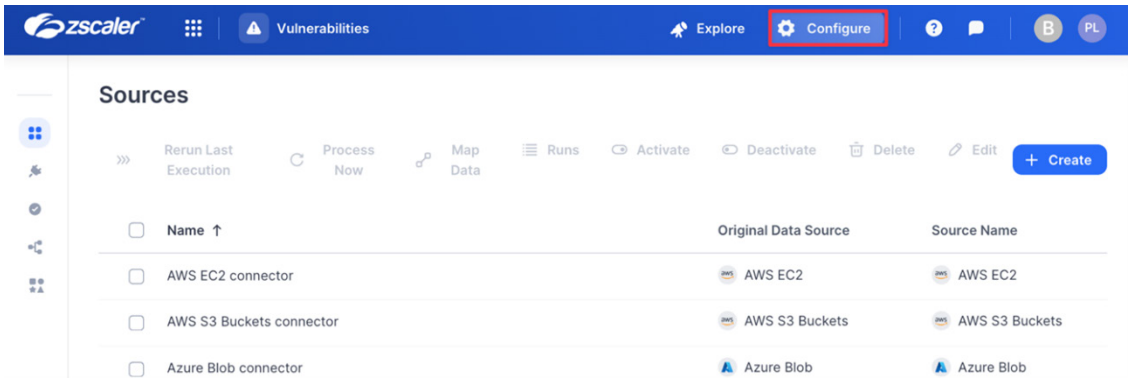

Figure 20. Configure

3. Click **Authentications**.

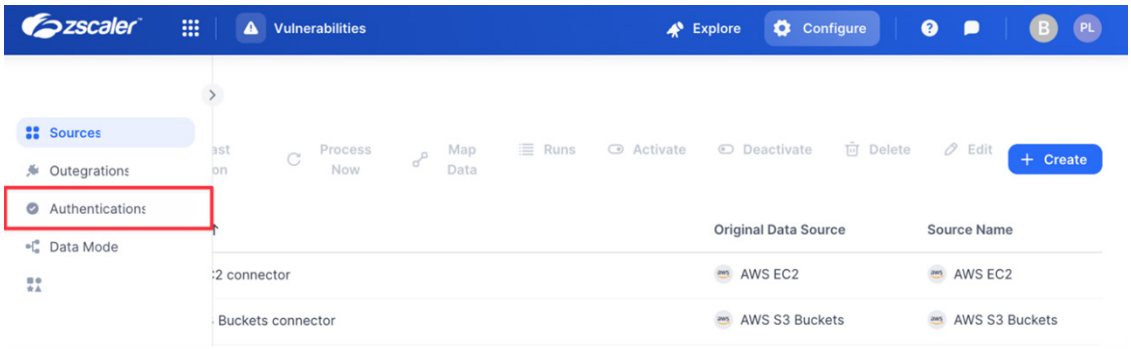

Figure 21. Authentications

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

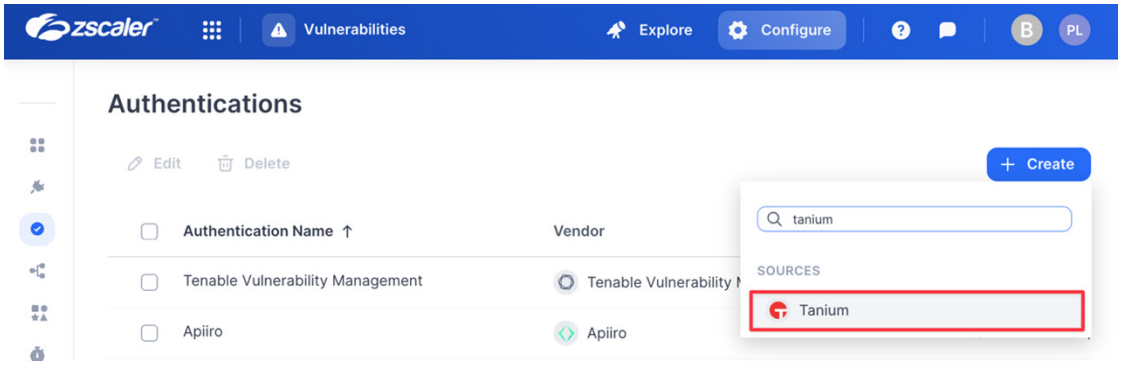

Figure 22. Add Tanium authentication

5. Enter the following:
   a. **Name**: Enter a name for your authentication (e.g., `Tanium`).
   b. **API Key**: Enter the API Key (see Retrieving the API Token).
   c. **Domain**: Enter in the domain (see Retrieving the Tanium AEM Domain).

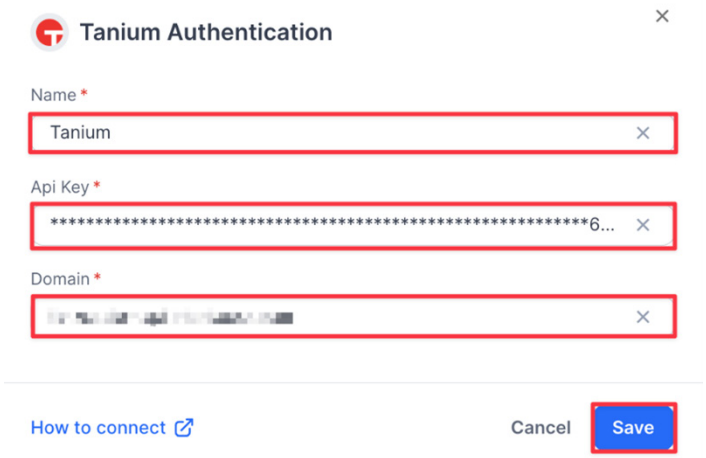

Figure 23. Tanium Authentication

6. Click **Save**.

Configure the Tanium Assets Data Source

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

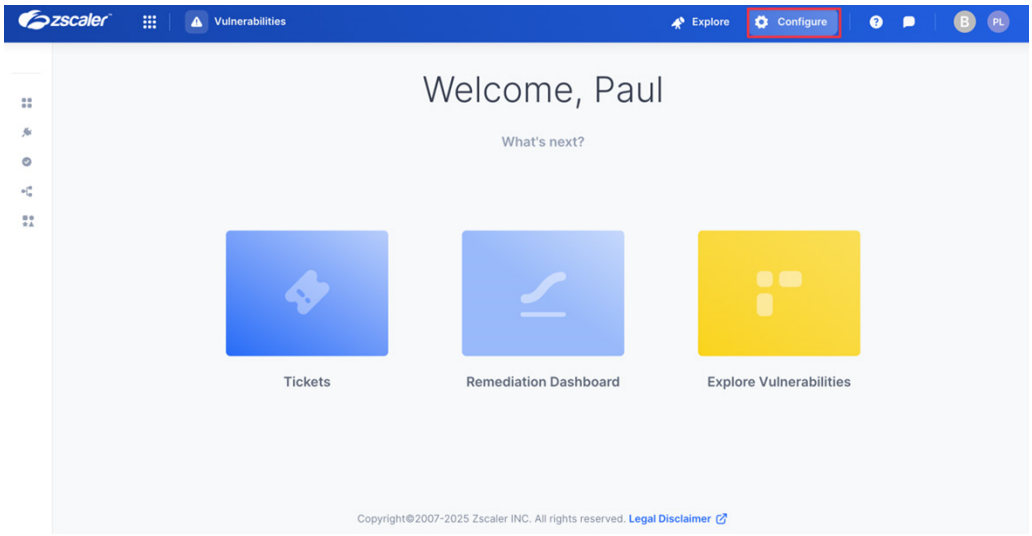

Figure 24. Configure

3. Click **Create**, then search for `Tanium Assets`.

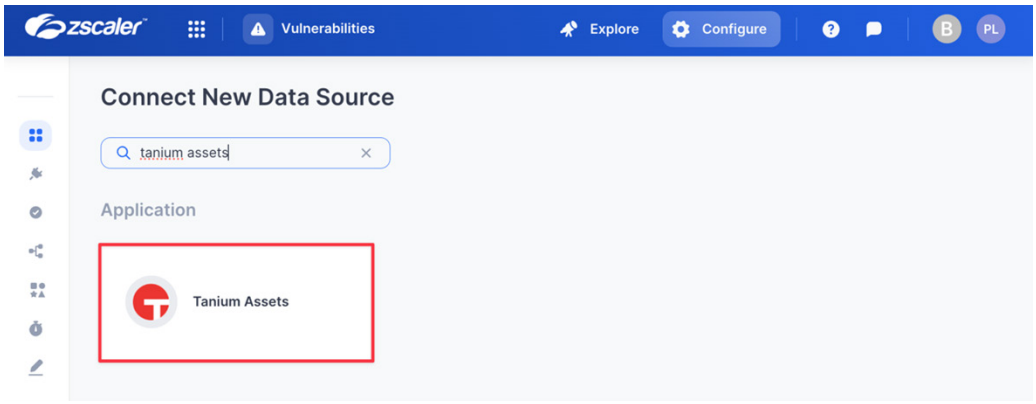

Figure 25. Connect New Data Source

4. Click the **Tanium Assets** application.
5. On the **Create Tanium Assets 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 created previously.
   d. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   e. **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.
   f. **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**.

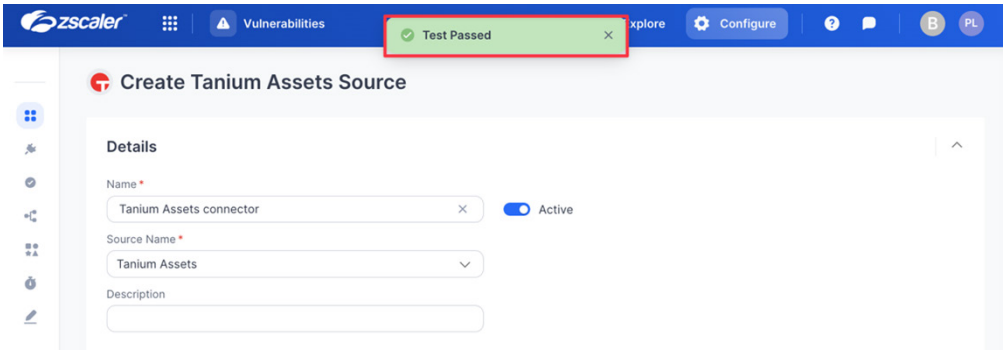

Figure 26. Test Passed

7. Click **Save**.

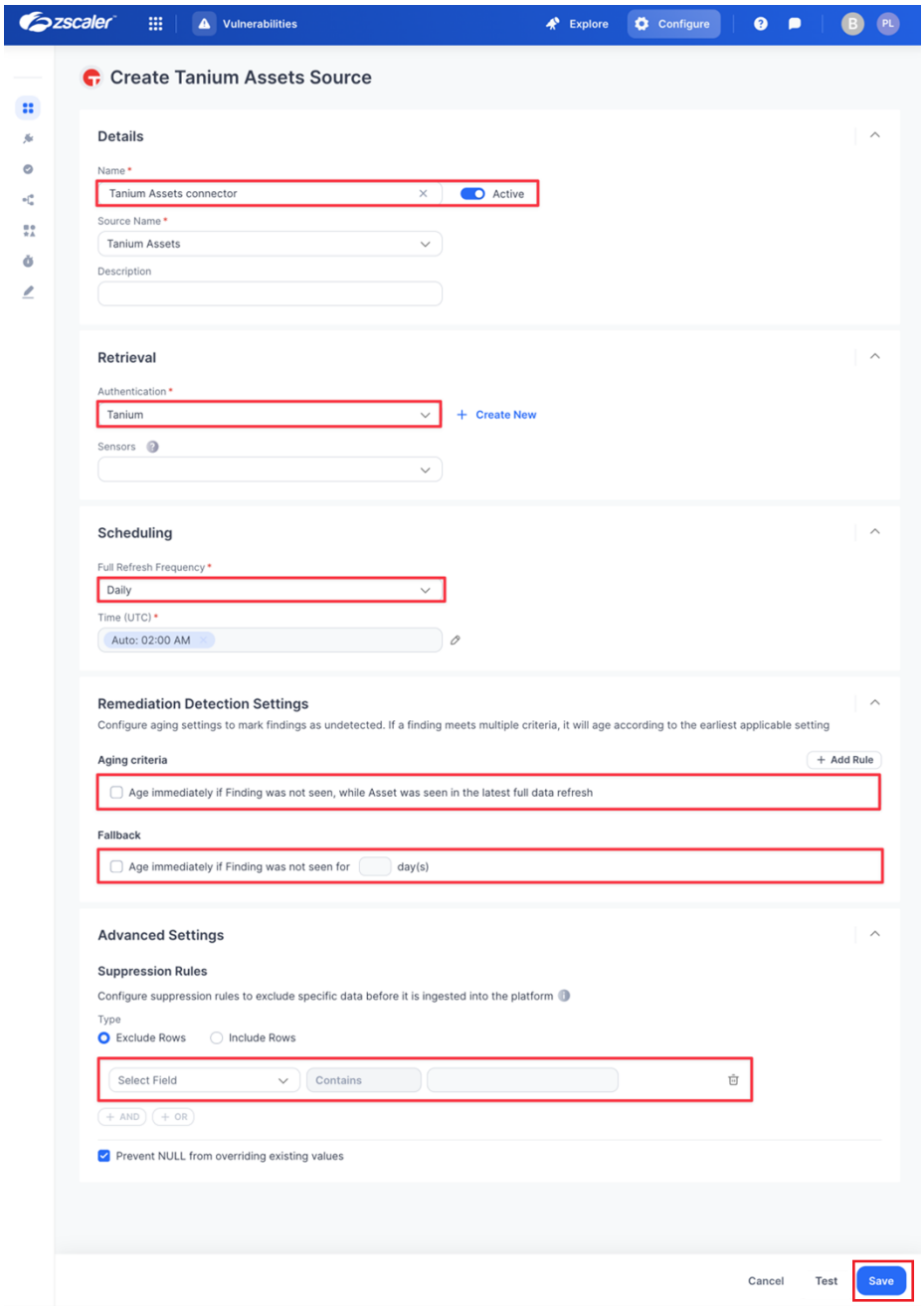

Figure 27. Create Tanium Assets Source

Configure the Tanium Compliance Data Source

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

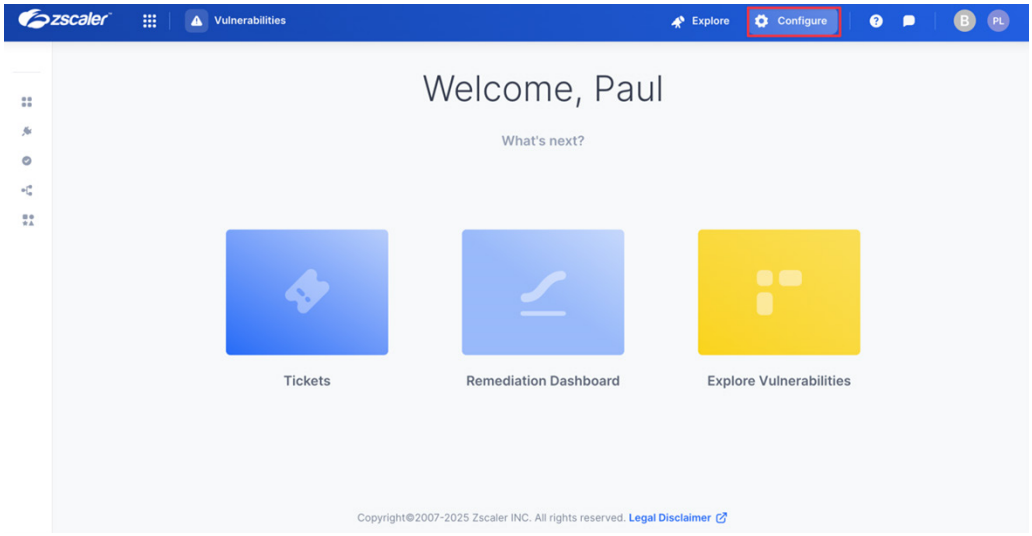

Figure 28. Configure

3. Click **Create**, then search for `Tanium Compliance`.

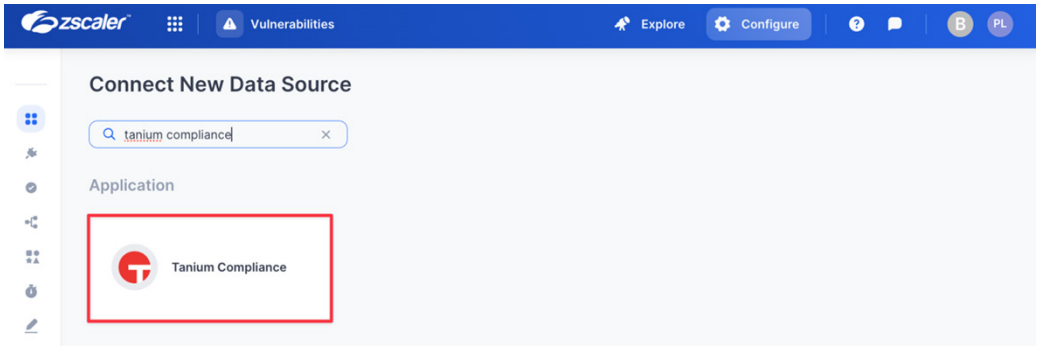

Figure 29. Connect New Data Source

4. Click the **Tanium Compliance** application.
5. On the **Create Tanium Compliance Datat 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 created previously.
   d. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   e. **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.
   f. **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**.

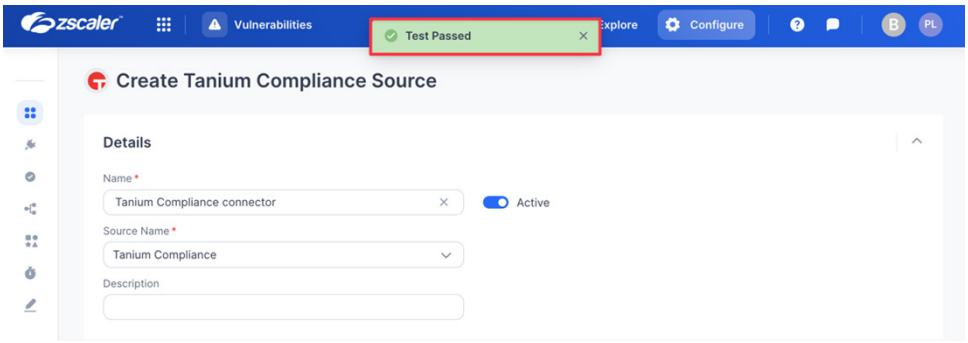

Figure 30. Test Passed

7. Click **Save**.

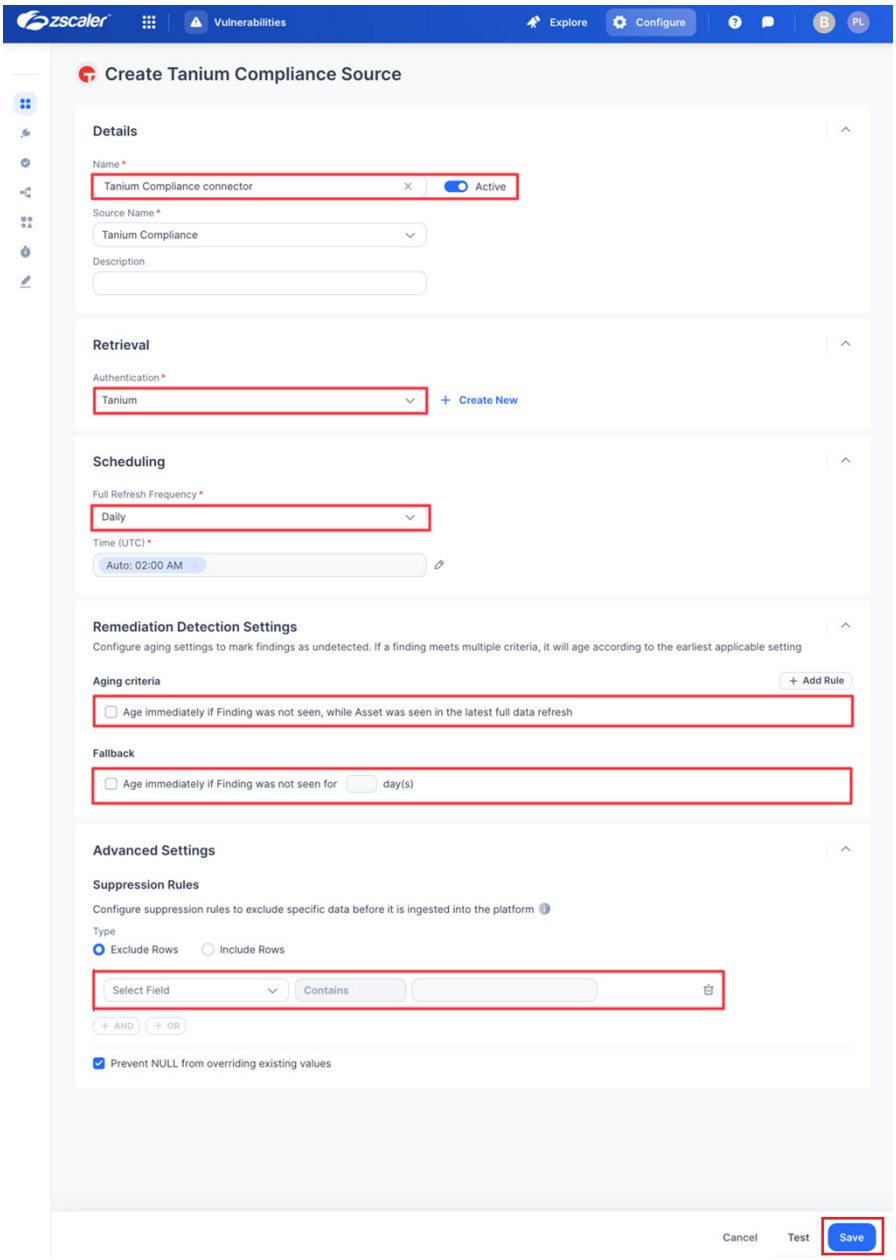

Figure 31. Create Tanium Compliance Source

Configure the Tanium CVE Data Source

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

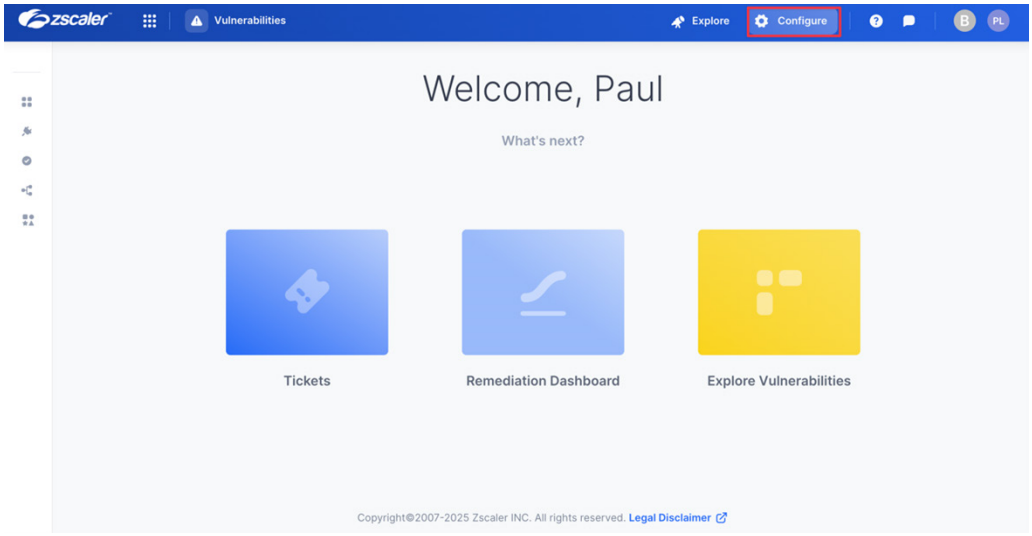

Figure 32. Configure

3. Click **Create**, then search for `Tanium CVE`.

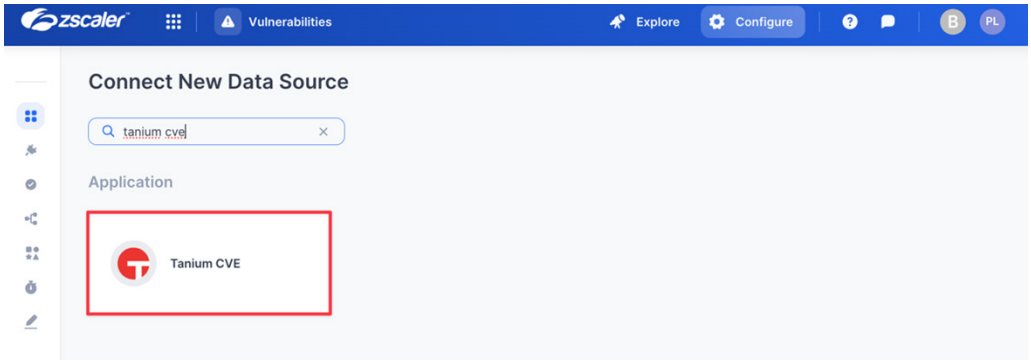

Figure 33. Connect New Data Source

4. Click the **Tanium CVE** application.
5. On the **Create Tanium CVE 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 created previously.
   d. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   e. **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.
   f. **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**.

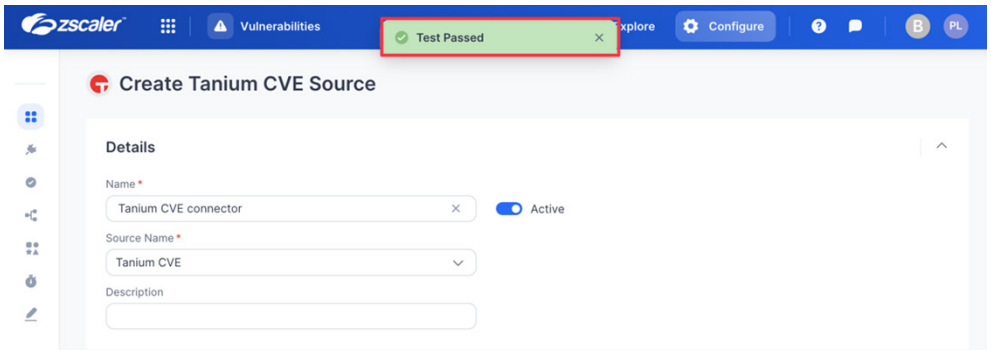

Figure 34. Test Passed

7. Click **Save**.

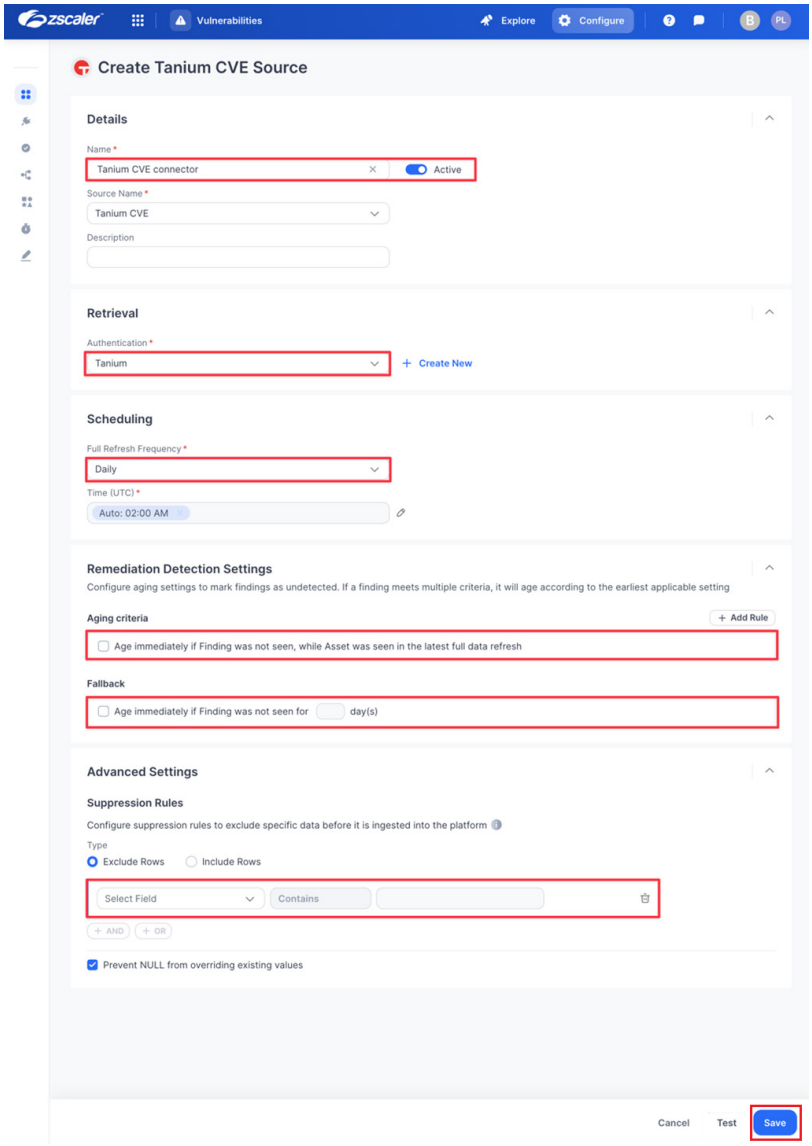

Figure 35. Create Tanium CVE Source

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 it is ingested, data is normalized and mapped to the Data Model. Zscaler UVM then evaluates risk.

The following example illustrates how to map the severityV3 attribute from the Tanium CVE data source and then use the Service Pack attribute from the Tanium Assets data source as a Risk Factor for a finding when assessing risk.

Map the Tanium CVE Data Source

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

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

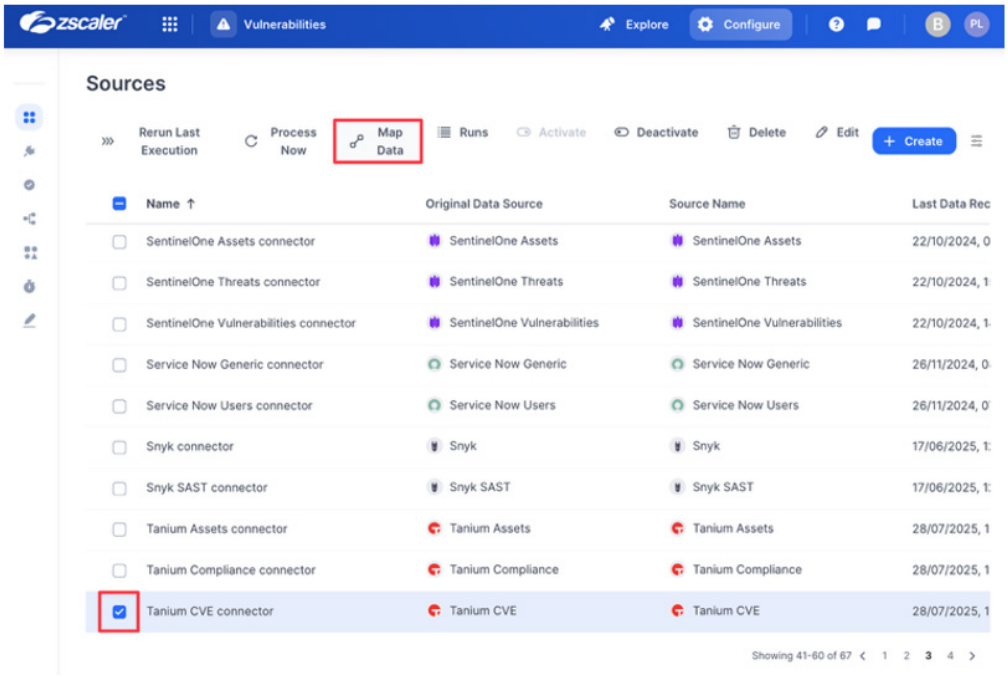

Figure 36. Map Data

2. Map the **Finding/Original Severity** entity to the **severityV3** field:
   a. On the right side, under **Finding**, drag **Original Severity** to the **Create New Connection** element.
   b. On the left side, click the **severityV3** field.

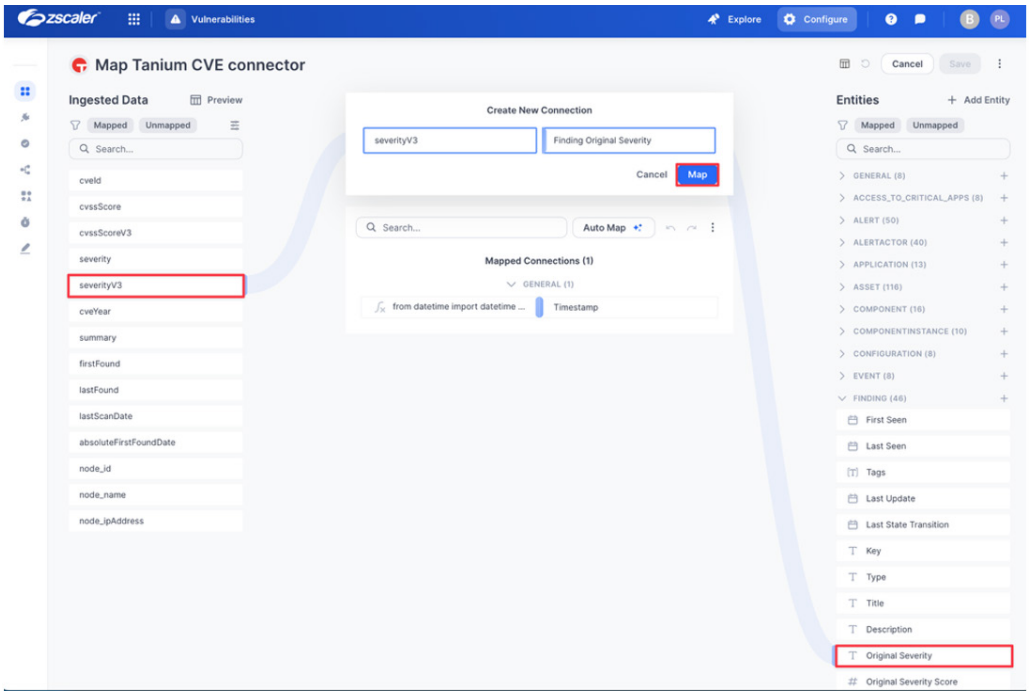

Figure 37. Map Tanium CVE connector

3. Click **Map**.
4. Map the **Finding/Key** entity to the **node_id** field by:
   a. On the right side, under **Finding**, drag **Key** to the **Create New Connection** element.
   b. On the left side, click the **node_id** field.

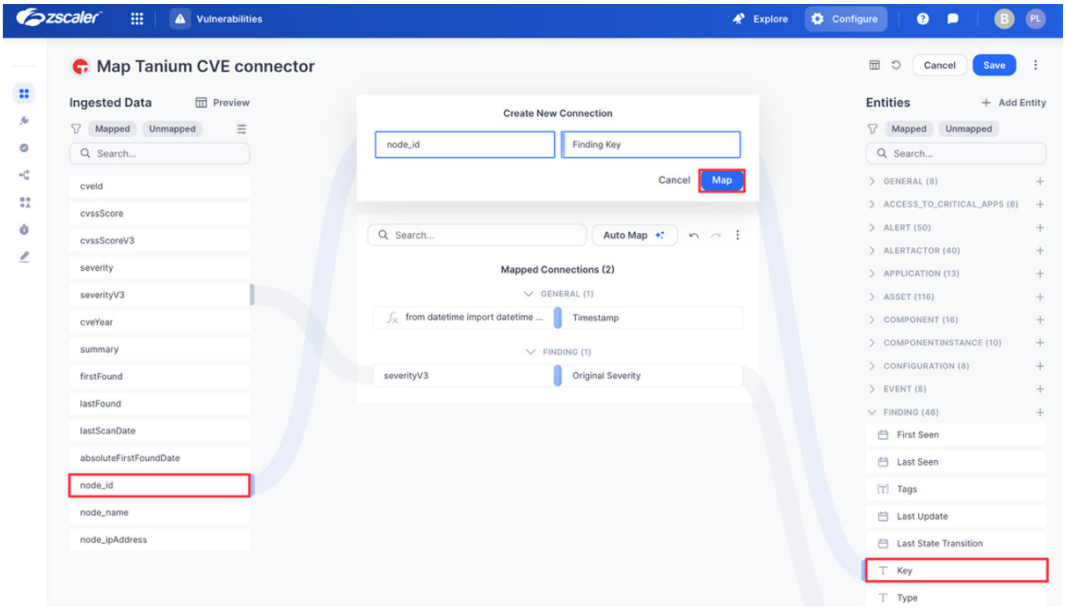

Figure 38. Finding/Key

5. Click **Map**.
6. Map the **Finding/Description** entity to the summary by:
   a. On the right side, under **Finding**, drag **Description** to the **Create New Connection** element.
   b. On the left side, click **summary**.

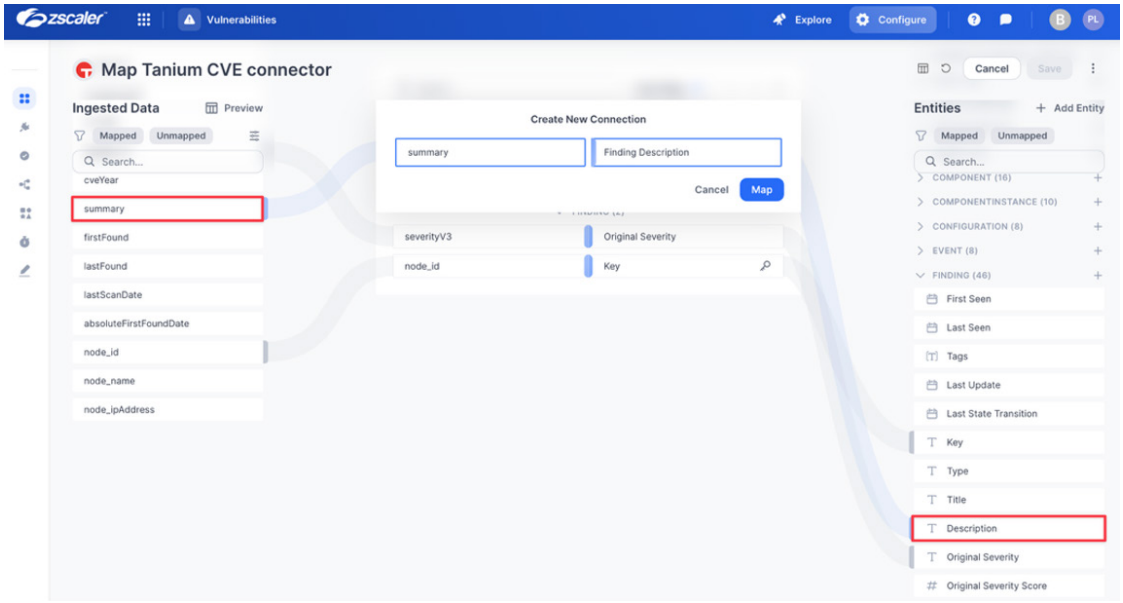

Figure 39. Summary

7. Click **Map**.
8. Map the **Asset/Key** entity to the **node_id**:
   a. On the right side, under **Asset**, drag **Key** to the **Create New Connection** element.
   b. On the left side, click the **node_id**.

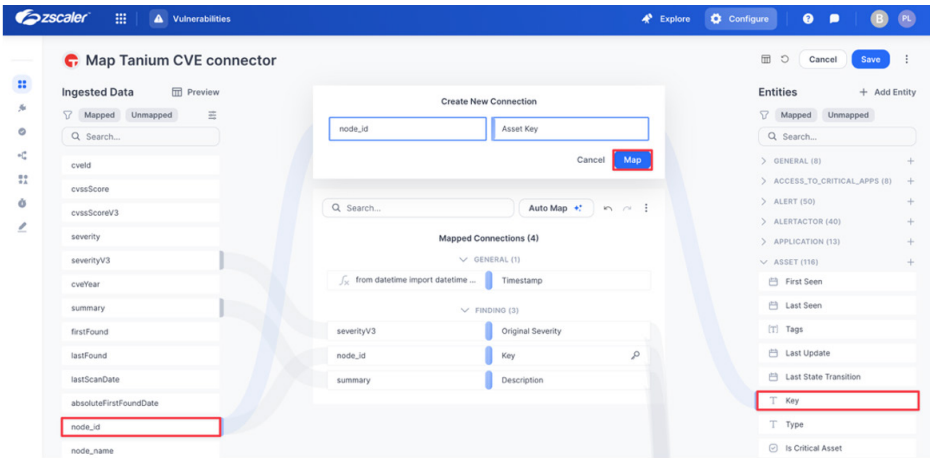

Figure 40. node_id

9. Click **Map**.
10. Click **Back to Mapping**, then click **Save**, **Continue Anyway**.
11. On the **Sources** page, click **Process Now** > **Process Now** under your **Tanium CVE Data Source.**

Map the Tanium Assets Data Source

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

1. Select **Configure** > **Tanium Assets connector** > **Map Data**.

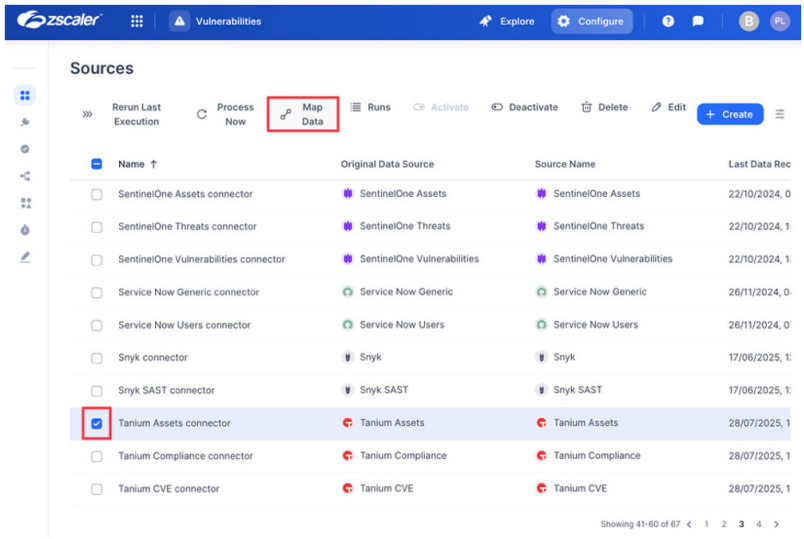

Figure 41. Map Data

2. Create a new field called **Service Pack** under **Assets** by clicking **+** next to **Asset**.

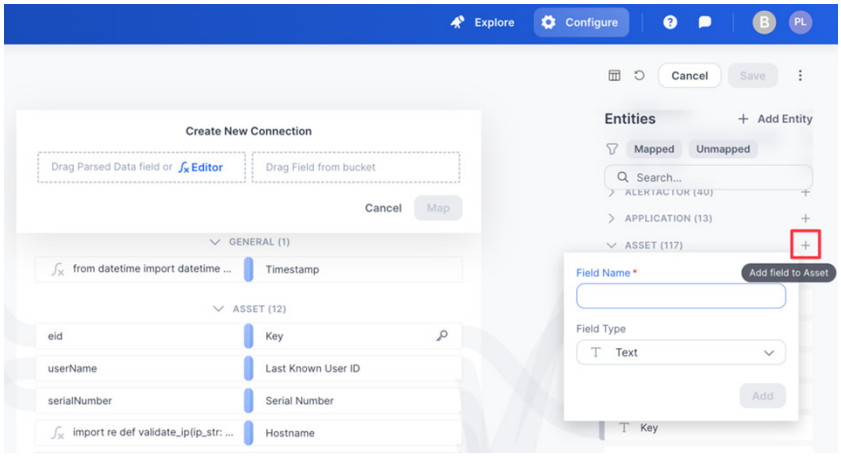

Figure 42. Service Pack

3. Enter `Service Pack` for the **Field Name**, `Text` for **Field Type**, and click **Add**:

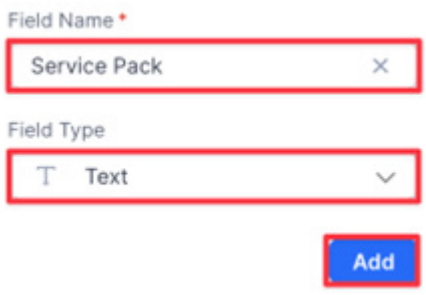

Figure 43. Field Name, Field Type

4. Map the new **Asset/Service Pack** entity to the **servicePack** field:
   a. On the right side, under **Asset**, drag **Service Pack** to the **Create New Connection** element.
   b. On the left side, click the **servicePack** field.

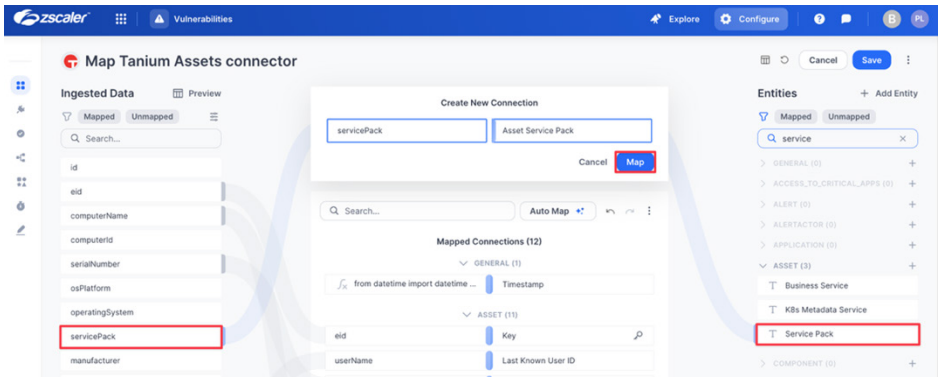

Figure 44. Map Tanium Assets connector

5. Click **Map.**
6. Click **Save**.
7. On the **Sources** page, click **Process Now** > **Process Now** under your T**anium Assets Data Source**.

Review and Adjust Risk Scoring

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. 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., `Service Pack`).
   c. **Field**: Choose Asset Service Pack.
   d. **When Service Pack Equals**: Enter `No Service Pack` and enter a percentage by which the risk is increased. This example uses `10`%.

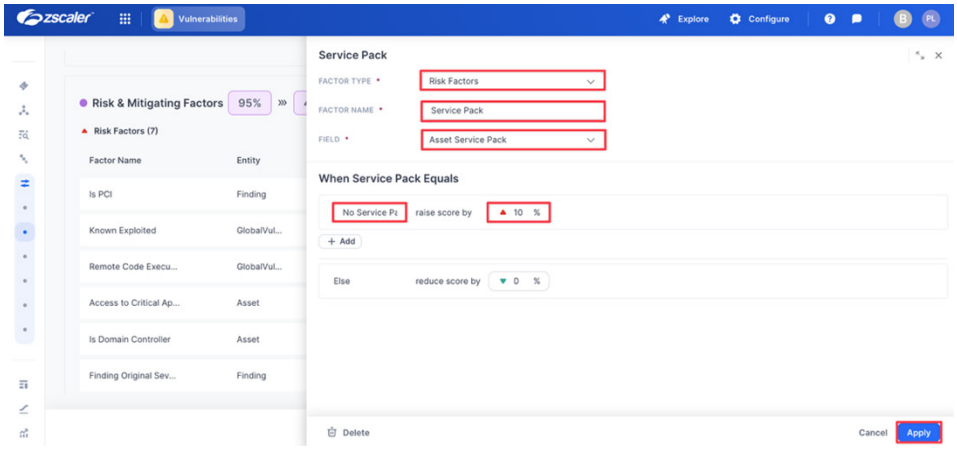

Figure 45. Service Pack

3. Click **Apply**, then **Save & Run**.
4. In the left-side pane, select the **Findings** dashboard. From the **Findings** dashboard:
   a. **Set Sources**: Select **Tanium CVE**.

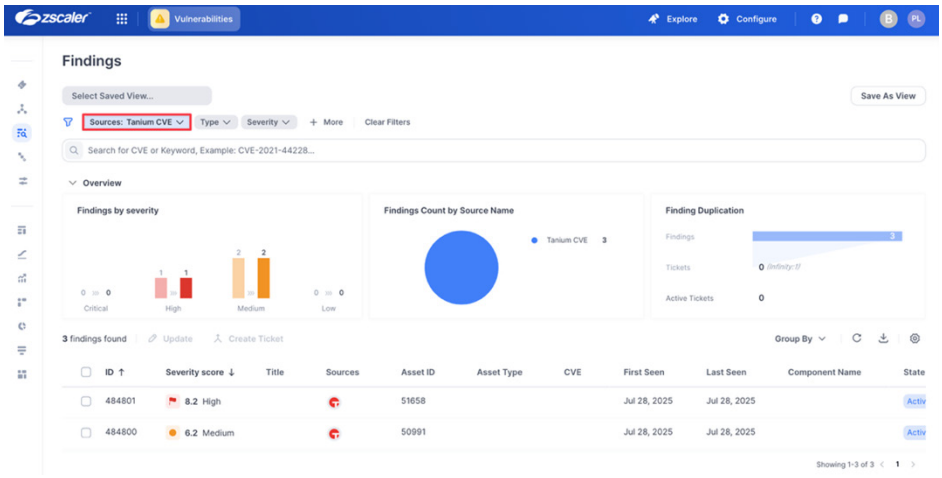

Figure 46. Set Sources

   b. Click one of your **Tanium CVE 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 Original Severity** has modified the risk scoring).

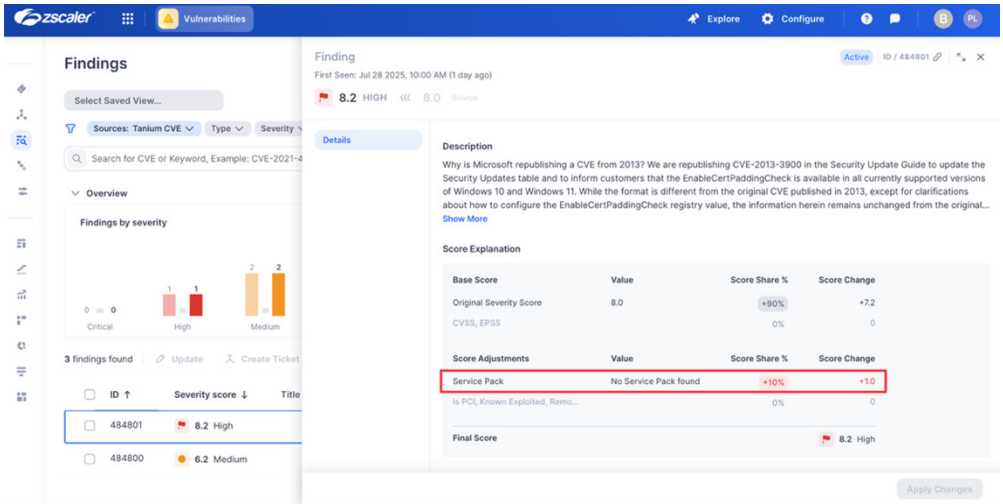

Figure 47. Score Adjustment

Appendix A: Requesting Zscaler Support

You might sometimes need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

Contact Support in ZIA

To contact Zscaler Support:

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

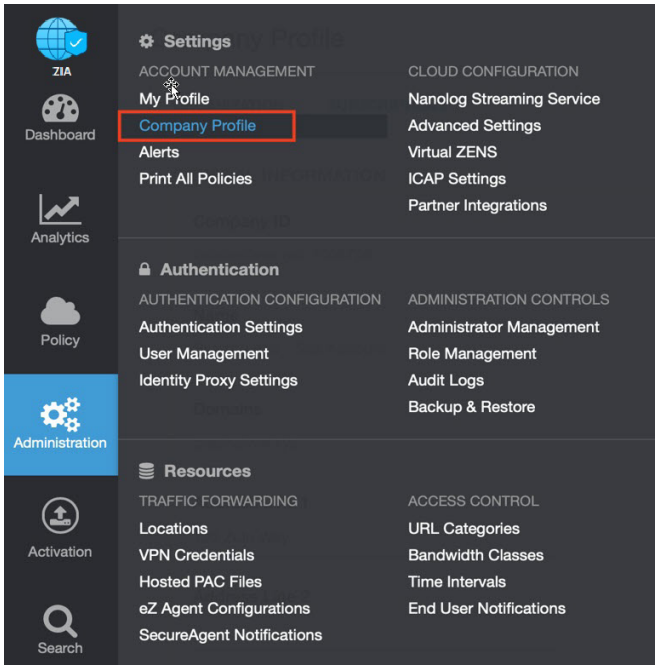

Figure 48. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

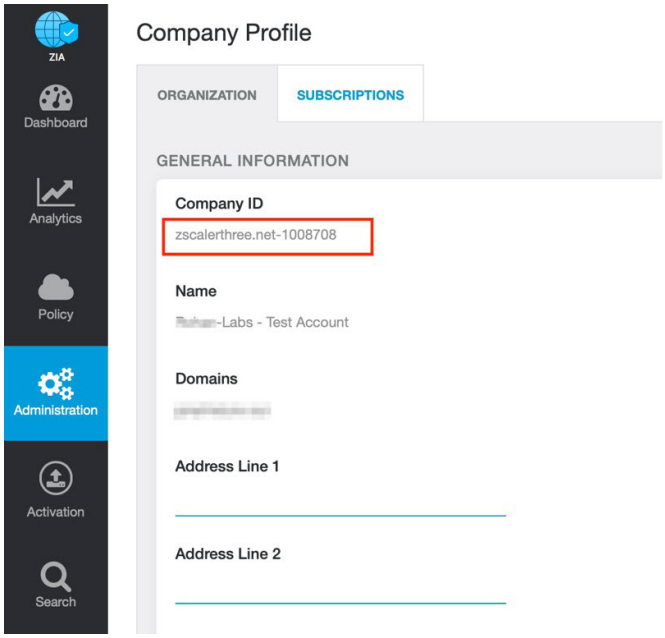

Figure 49. Company ID

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

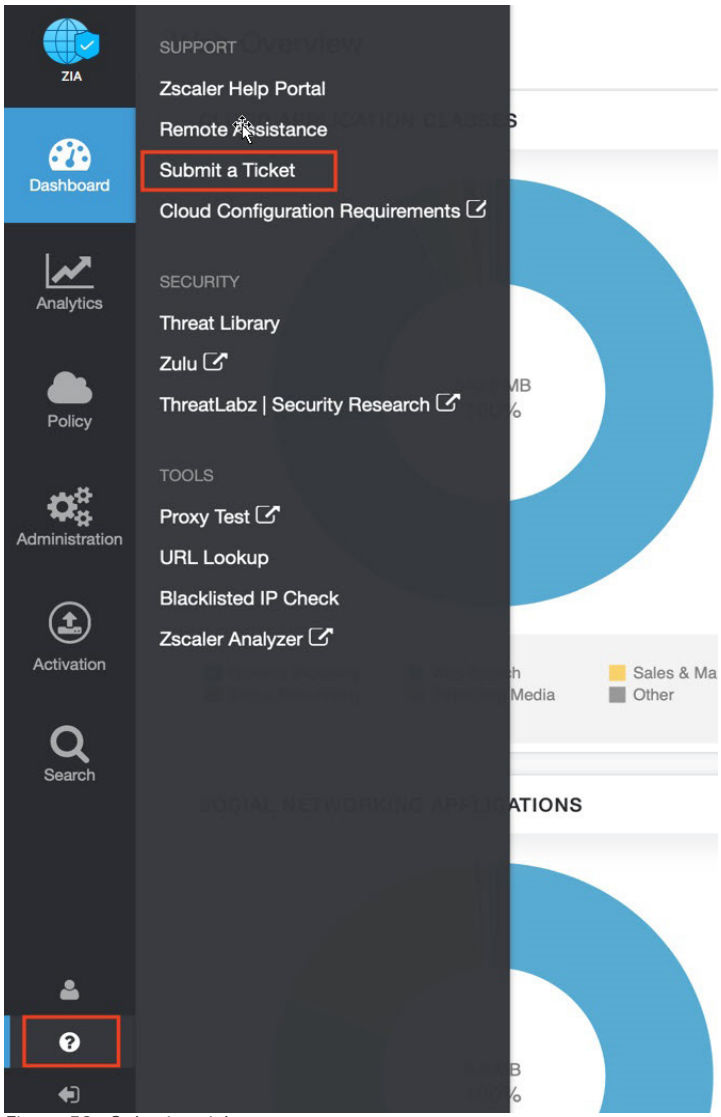

Figure 50. Submit a ticket

Contact Support in Zscaler UVM

To contact Zscaler Support:

1. Log in to the Zscaler UVM Platform,

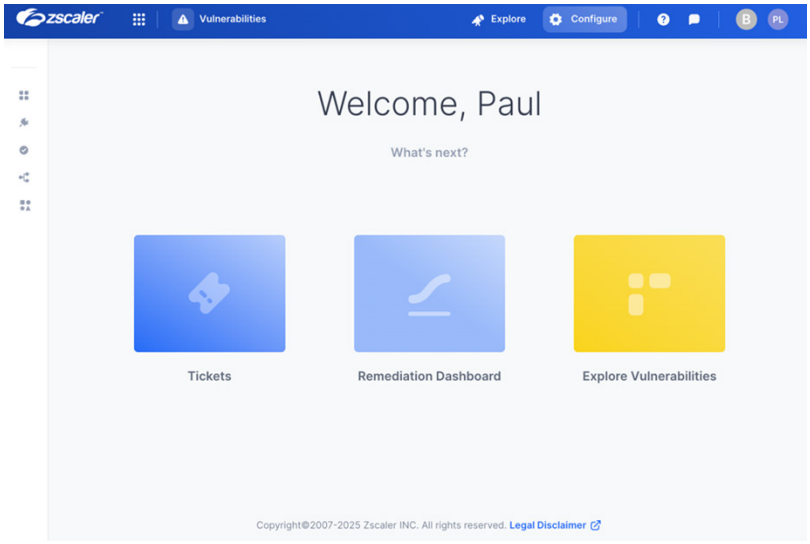

Figure 51. Zscaler UVM

2. Click **Contact Support**.

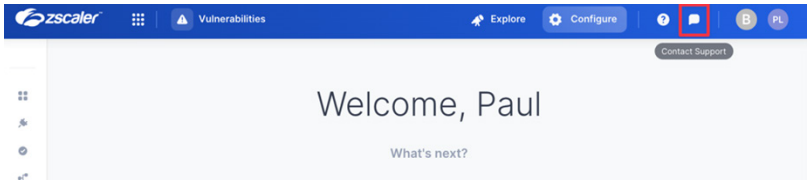

Figure 52. Contact Support

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

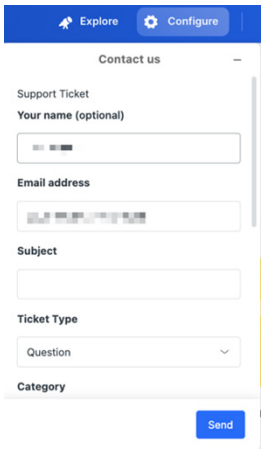

Figure 53. Send

