ZSCALER AND ATLASSIAN DEPLOYMENT GUIDE

AUGUST 2023, VERSION 1.1

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines the acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
ASIC	Application-Specific Integrated Circuit
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GCP	Google Cloud Platform
GRE	Generic Routing Encapsulation (RFC2890)
IaC	Infrastructure as Code
ICMP	Internet Control Message Protocol
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)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)
ZPC	Zscaler Posture Control (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. 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 or follow Zscaler on Twitter @zscaler.

Atlassian Overview

Atlassian Corporation (NASDAQ: TEAM) provides software that helps teams organize, discuss, and complete shared work. Teams at more than 144,000 customers, across large and small organizations—including General Motors, Walmart Labs, Bank of America & BofA Securities, Lyft, Verizon, Spotify, and NASA—use Atlassian's project tracking, content creation and sharing, and service management products to work better together and deliver quality results on time. To learn more about Atlassian and Atlassian products such as Jira Software, Confluence, Trello, Bitbucket, Opsgenie, Jira Service Management, and Jira Align, refer to the Atlassian website.

Audience

This guide is for network administrators, endpoint / IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- Zscaler Resources
- Atlassian Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using ZIA v6.2 and Atlassian Production 2022 Release. An Atlassian developer account was used to create and verify the features enabled and used as examples.

Create an Atlassian Developer Account. Click Log in, then select Sign up for an account.

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 Atlassian Introduction

This section provides overviews of the Zscaler and Atlassian applications described in this deployment guide.

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, please 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 on-ramp—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 the 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 Cloud Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or a 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.

ZPC Overview

ZPC is a multi-tenant SaaS platform that detects and responds to cloud security risks and helps businesses adopt the digital transformation journey towards the cloud faster. The service enables your organization to correlate across multiple security engines to prioritize hidden risks caused by misconfigurations, threats, and vulnerabilities, and achieve continuous security, compliance, and governance.

ZPC offers data protection, high availability, and resiliency for all imported, stored, and exported data types. ZPC leverages cloud service provider APIs to connect to your hybrid, multi-cloud environments and collect real-time configuration metadata for your cloud infrastructure, such as web servers, databases, and virtual machines. ZPC evaluates the metadata and offers visibility into your security, compliance, and risk posture.

ZPC helps detect cloud security risks in the development lifecycle, as well as threats like ransomware attacks, account takeover, privilege escalation after the business applications are deployed in the cloud infrastructure across Amazon Web

Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

ZPC is part of Zscaler Cloud Protection, a comprehensive multi-cloud security platform covering misconfigurations, entitlements, exposed attack surfaces, lateral threat movement, and data loss.

ZPC comprises functionality previously covered by several point products, including:

- Cloud Security Posture Management (CSPM): Ensure cloud resources have proper configurations for authentication, data encryption, internet connectivity, and more for compliance and a strong security posture.
- Cloud Infrastructure Entitlement Management (CIEM): Identify and remediate excessive permissions that humans and machines have by using machine learning analysis for increased visibility into access policies, resource policies, actions, and roles.
- Security and Compliance: Benchmark and validate public cloud configurations against best practices standards and compliance frameworks to report misconfigurations, policy violations, and automate remediation.
- Infrastructure as Code (IaC) Security: Monitor your IaC infrastructure and implement security controls to address any misconfigurations or security issues before deployment and thereby ensure the code is secure and compliant with standard security policies.
- Vulnerability Management: Monitor and detect any known vulnerabilities and security weaknesses in the cloud infrastructure and take immediate action to protect networks from potential threats.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZIA.
ZPC Help Portal	Help articles for ZIA.
Adding SaaS Application Tenants	Help articles on using Zscaler API for visibility and security for sanctioned SaaS applications used in your organization.
About SaaS Application Tenants	Help articles on adding SaaS applications to Zscaler.
SaaS Security API DLP Policy	Help articles on creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications.
About Data Loss Prevention	Help article on DLP.
About DLP Dictionaries	Help article on DLP dictionaries.
Adding Custom DLP Engines	Help article on DLP engines.
SaaS Security Insights	Help article providing SaaS security information.
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 and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZIA.
ZPC Help Portal	Help articles for ZIA.

Name and Link	Description
Adding SaaS Application Tenants	Help articles on using Zscaler API for visibility and security for sanctioned SaaS applications used in your organization.
About SaaS Application Tenants	Help articles on adding SaaS applications to Zscaler.
SaaS Security API DLP Policy	Help articles on creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications.
About Data Loss Prevention	Help article on DLP.
About DLP Dictionaries	Help article on DLP dictionaries.
Adding Custom DLP Engines	Help article on DLP engines.
SaaS Security Insights	Help article providing SaaS security information.
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.

Atlassian Platform Overview

All Atlassian products, apps, and integrations are built on a unified cloud technology platform. Whether your teams are in IT, software development, or non-technical functions, their platform powers open and efficient collaboration.

- Analytics: Speed up decision-making at all levels by harnessing data across your Atlassian and non-Atlassian sources. The Atlassian platform provides visibility into how work happens across your entire toolchain so you always stay ahead of the game.
- Automation: Facilitate thoughtful, rule-driven workflows to gain efficiencies and improve quality. The Atlassian platform enables powerful cross-product automation so you can leave the manual work behind.
- Collaboration: Empower open collaboration between your teams to eliminate silos and accelerate impact across your business. The Atlassian platform automatically connects the right context and content with the right people for better ways of working.
- Connection: Amplify productivity across teams by connecting your ecosystem of work. Atlassian's platform provides the connective tissue between all of your apps, projects, and processes with deep integrations.
- Administration: Access a centralized mission control that spans the entirety of the Atlassian product portfolio and empower admins to effectively manage the needs of organizations and teams, regardless of complexity or scale.

Atlassian Resources

The following table contains links to Atlassian support resources.

Name and Link	Description
Atlassian Developer Community	Online developer community to get help with building, deploying, and managing apps.
Atlassian Product Documentation	Online documentation for the Atlassian platform.
Atlassian Support	Online support for the Atlassian platform.
Bitbucket and Jira Integration	Bitbucket and Jira Integration
Atlassian and Open DevOps	Atlassian and Open DevOps
Bitbucket Free Tier	Bitbucket Free Tier.

Zscaler Data Protection for Atlassian

The Atlassian suite of team collaboration software (such as Bitbucket, Confluence, Jira, etc.) helps teams organize, discuss, and complete shared work. Atlassian is an industry leader in SaaS services that assist with team collaboration, whose software is useful and enables global sharing. The downside of quick access and sharing is security risks based on the client's environment.

Ensuring every employee always uses the best SaaS application safety practices is impossible, which leads to costly mistakes for the organization. Risk associated with accidental data exposure, malicious intent, and compliance violations forces companies to restrict or prevent use of these incredible business tools. This is where Zscaler helps Atlassian users.

The following diagram shows a conceptualization of the integration between Zscaler and Atlassian.

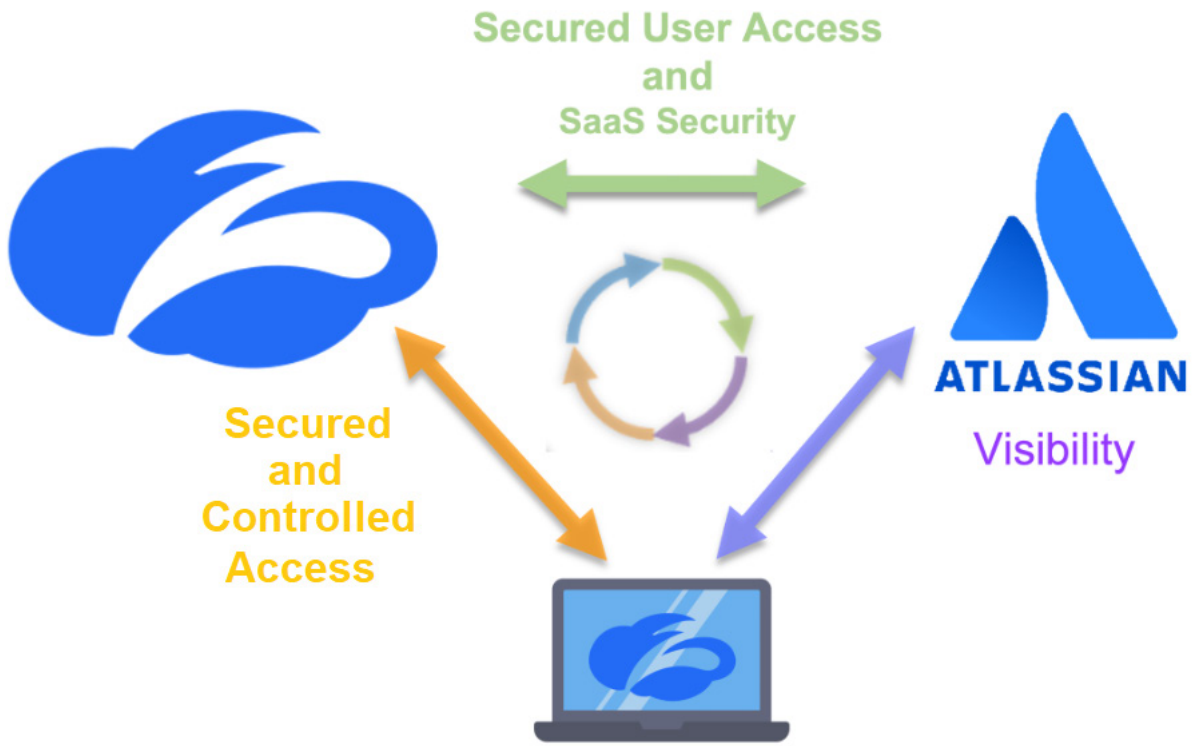

Figure 1. Zscaler solutions for Atlassian

ZIA provides security for Atlassian SaaS products through access control, identity control, SaaS Security Posture Management, an SaaS API to scan the attachments for malicious content, and data loss protection (DLP). ZIA also provides complete security for clients whether they are in the corporate office or their home office.

This guide covers the following ZIA features for Atlassian security:

- Zscaler Overview
- ZIA Data Loss Protection and Malware Detection for Atlassian
- ZIA Cloud Application Control
- ZPC and Jira Incident Creation

ZIA Cloud Browser Isolation

Most new threats that target organizations are browser-based. As a result, organizations are left struggling to keep these threats from reaching endpoint devices and preventing sensitive data from leaking out, while providing unobstructed internet access for users.

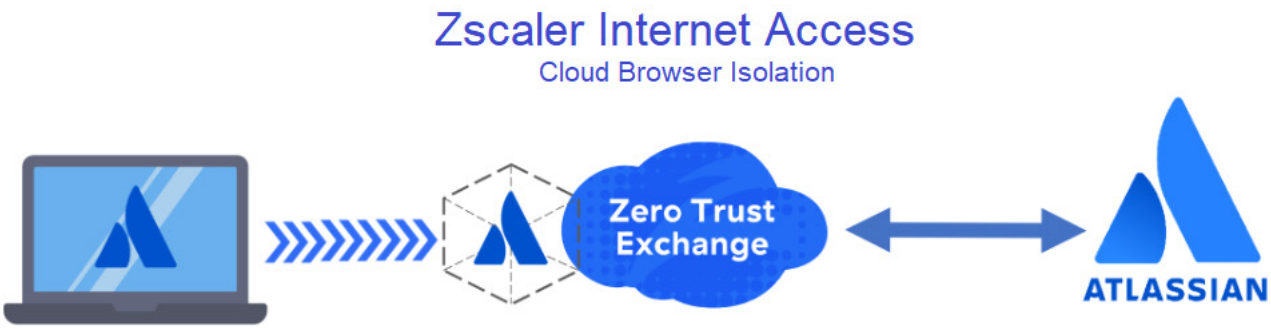

Figure 2. ZIA Cloud Browser Isolation in use with Atlassian products

Zscaler Cloud Browser Isolation provides safe access to active web content for your users by rendering browser content in an isolated environment, and by minimizing the browser attack surface. Sensitive information is protected from web-based malware and data exfiltration.

By defining granular policies based on user group or department, you can effectively protect endpoint devices and prevent confidential data exposure from business-critical applications by managing user activity within the isolation environment enabling viewing actions within Bitbucket, Confluence, and Jira software, while preventing the downloading and copying-and-pasting of confidential business data.

ZIA Data Loss Protection and Malware Detection for Atlassian

The Zscaler SaaS Security API is part of the ZIA security cloud and designed specifically to help manage the risks of our file collaboration SaaS partners, preventing data exposure and ensuring compliance across the SaaS application.

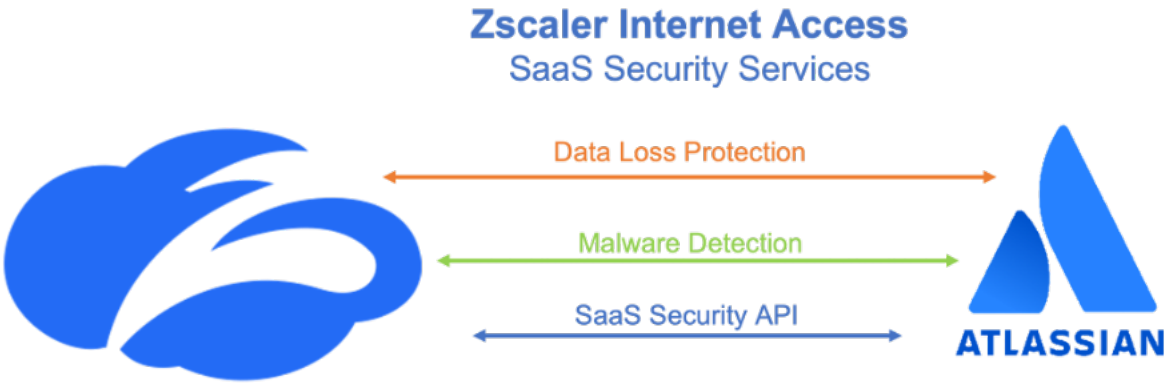

Figure 3. ZIA SaaS security in use with Atlassian products

The Zscaler SaaS Security API enables organizations to securely adopt and govern the use of multiple SaaS applications. It provides real-time visibility, and controls access and user activity across sanctioned and unsanctioned applications. The fully integrated platform eliminates overlay architectures and simplifies policy creation and administration, ensuring data is protected and compliance is maintained.

What makes our SaaS Security unique?

- Data exposure reporting and remediation: Zscaler SaaS Security API checks SaaS applications and cloud providers' configurations and compares them to industry and organizational benchmarks to report on violations and automate remediation.
- Threat identification and remediation: Zscaler SaaS Security API checks SaaS API applications for hidden threats being exchanged and prevents their propagation.
- Compliance assurance: Zscaler SaaS Security API provides compliance visibility across SaaS and cloud providers and can mitigate violations automatically.
- Part of a larger data protection platform: Zscaler Cloud Security provides unified data protection with DLP, and malware scanning capabilities for internet, data center, and SaaS applications, and ensures that public cloud applications are configured to prevent data exposure and maintain compliance. Zscaler also offers Zscaler Private Access (ZPA) for Zero Trust access to internal applications, ZDX for active monitoring of users' experience to SaaS applications, and Zscaler Cloud Protection (ZCP). Zscaler provides end-to-end connectivity, security, and visibility from any location on-premises or remote.

To learn more, see the resources in Zscaler Resources.

ZIA Cloud Application Control

The ZIA security cloud is a fully integrated cloud-based security stack that sits in-line between users and the internet, inspecting all traffic (including SSL) flowing between them. ZIA Cloud App Control delivers full visibility into application usage. Granular policies ensure the proper use of both sanctioned and unsanctioned applications. SaaS tenant security is referred to as out-of-band for data-at-rest. ZIA security cloud is referred to as in-line.

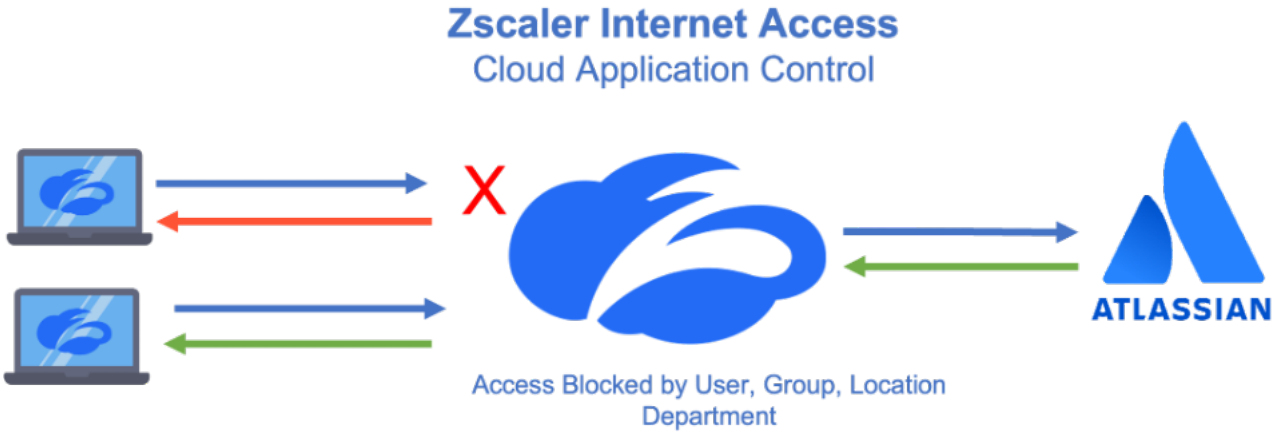

Figure 4. ZIA Cloud App Control

ZIA Cloud App Control provides SaaS application intelligence to consolidate all associated URLs and functions of an application in a single security setting. This allows the control of specific users, groups, locations, or departments, and only allows the authorized users access to the application.

ZPC and Jira Incident Creation

ZPC supports integration with ticketing systems to automatically log incidents when a misconfiguration or compliance violation is discovered by ZPC. These violations and misconfigurations can be related to cloud environments such as AWS, Azure, GCP, and IaC events. ZPC integrates with Incident Management (ticketing) tools such as Jira to automate the incident creation and expedite resolution.

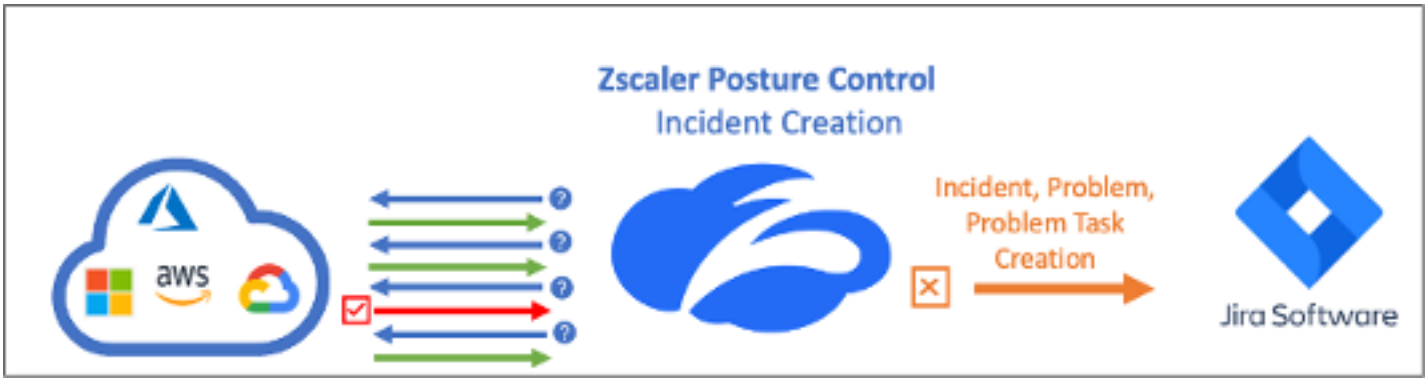

Figure 5. Zscaler automates ticketing in Jira

Configure Cloud Browser Isolation

Zscaler Cloud Browser Isolation provides safe access to active web content for your users by rendering browser content in an isolated environment, and by minimizing the browser attack surface. Sensitive information is protected from web-based malware and data exfiltration.

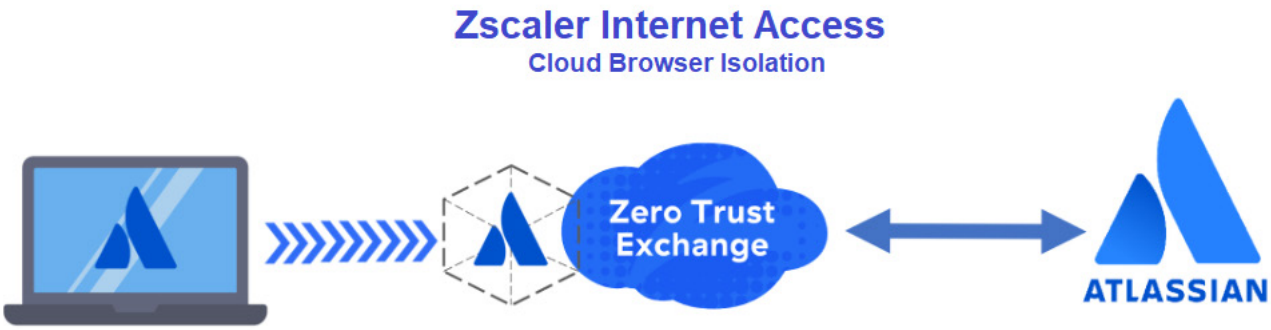

Figure 6. ZIA Cloud Browser Isolation in use with Atlassian

By defining granular policies based on user group or department, you can effectively protect endpoint devices and prevent confidential data exposure from business-critical applications by managing user activity within the isolation environment. In the isolation environment, you can view Atlassian platform products such as Bitbucket, Confluence, and Jira while preventing the downloading and cutting-and-pasting of confidential business data.

Cloud Browser Isolation can be combined with identity proxy to provide extra security to Atlassian users by assuring the identity of the user, guaranteeing the user's traffic is scanned and secured with the ZIA security features. Use with combined identity proxy to provide extra security for identified potentially risky users direct to Cloud Browser Isolation for even greater security measures.

Configure the Cloud Browser Isolation Profile

To begin the Cloud Browser Isolation configuration, log in to your Cloud Browser Isolation Portal with administrator credentials. This is a different portal than your ZIA Admin Portal or ZPA Admin Portal. The link and administrator credentials are supplied to you by Zscaler Support after your organization has subscribed to the feature.

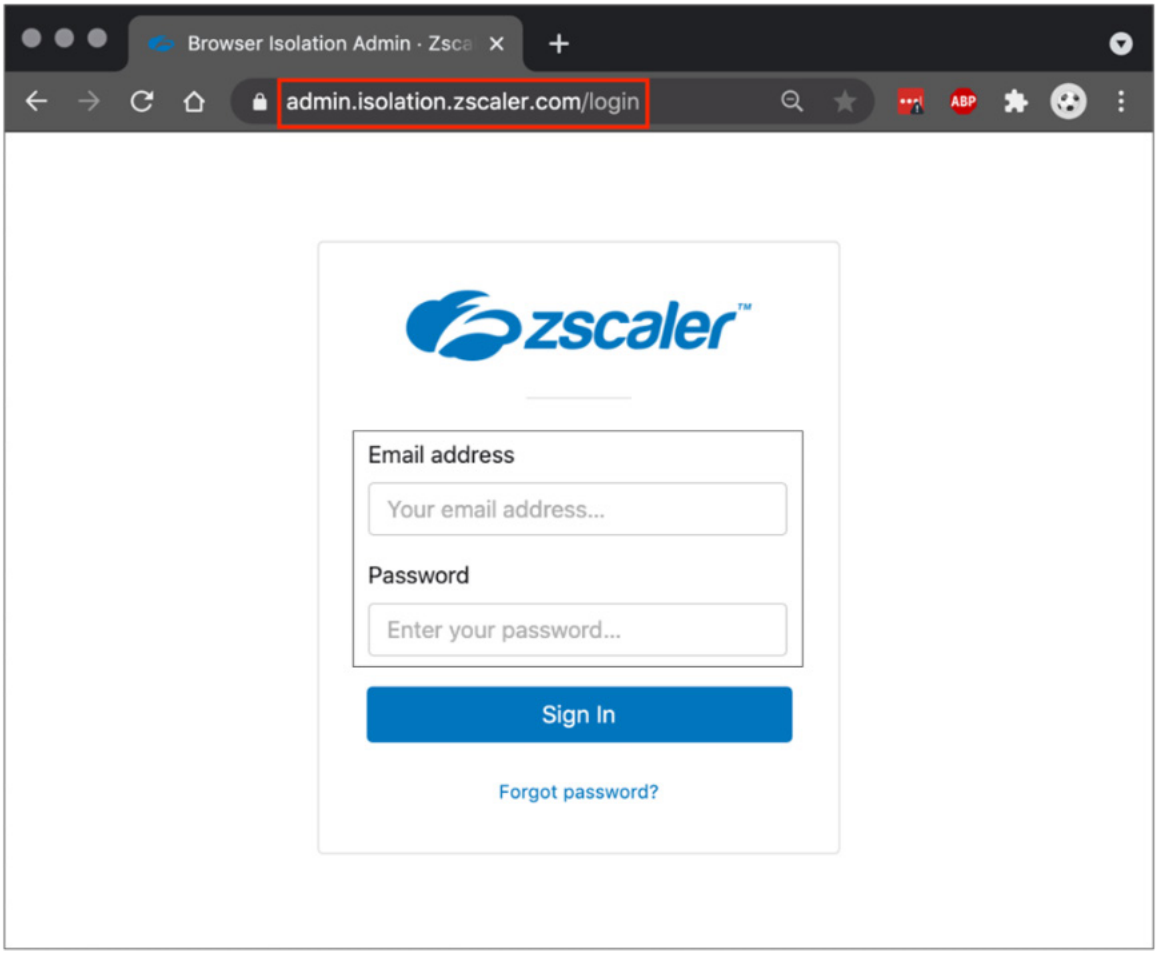

Figure 7. Cloud Browser Isolation login

You must configure a Cloud Browser Isolation profile (or multiple profiles) to use Cloud Browser Isolation features specifically for Atlassian products, along with an individual user profile for the user using Cloud Browser Isolation. This could be a generic profile for all SaaS applications, or it could be multiple policies for individual Atlassian products depending on your needs and level of isolation.

For example, you could have a policy to control file uploads for one client and copy-and-paste for another.

In Cloud Browser Isolation, to start the wizard:

1. Select **Isolation profiles**.
2. Click the **ZIA** tab.
3. Click **Add New**.

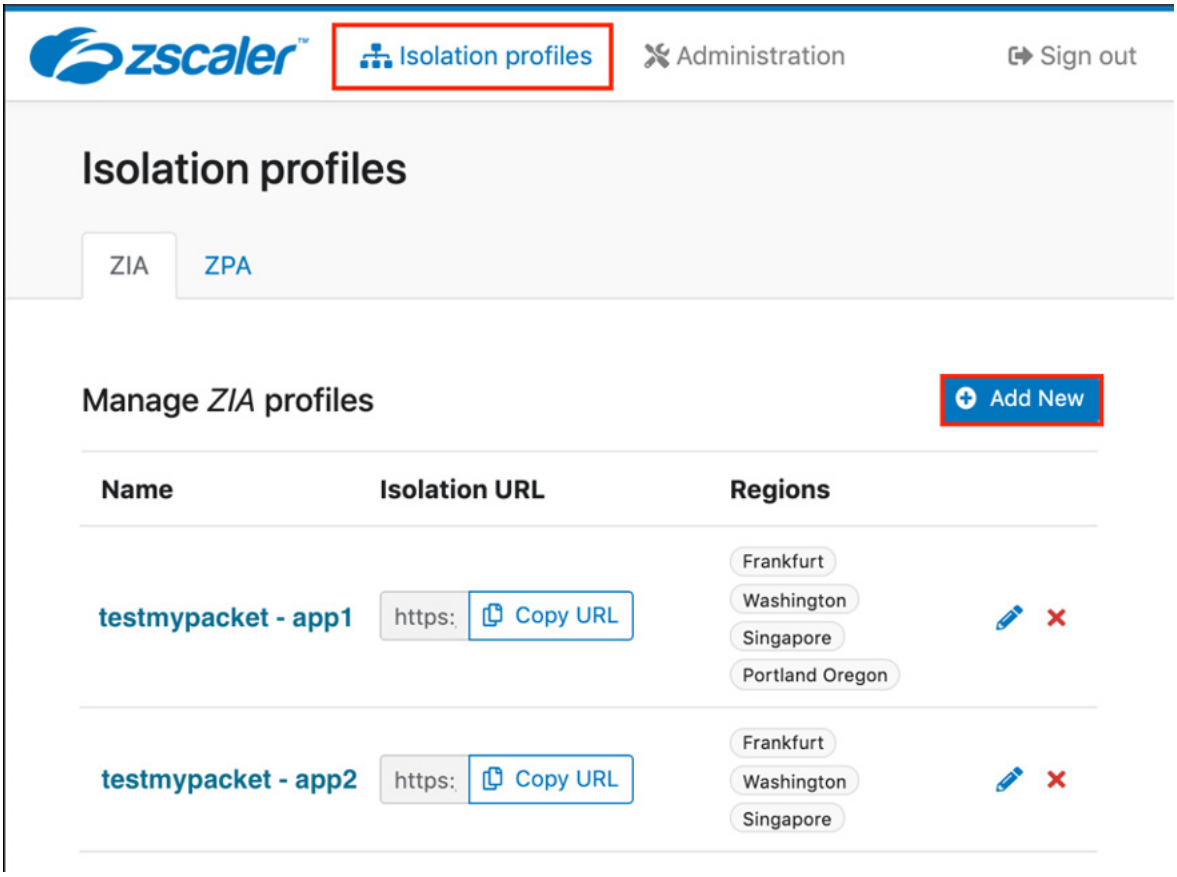

Figure 8. Configure Cloud Browser Isolation profile

This starts the Cloud Browser Isolation wizard and steps you through enabling General Information, Company Settings, Security Controls, Regional Connectivity, and the End User Notification.

For **General Information**, give the profile an intuitive name and description. It is selected in the Isolation Policy on the ZIA Admin Portal and should be clear to the use case:

1. **Name** the profile.
2. Give the profile a detailed **Description**.
3. Click **Next**.

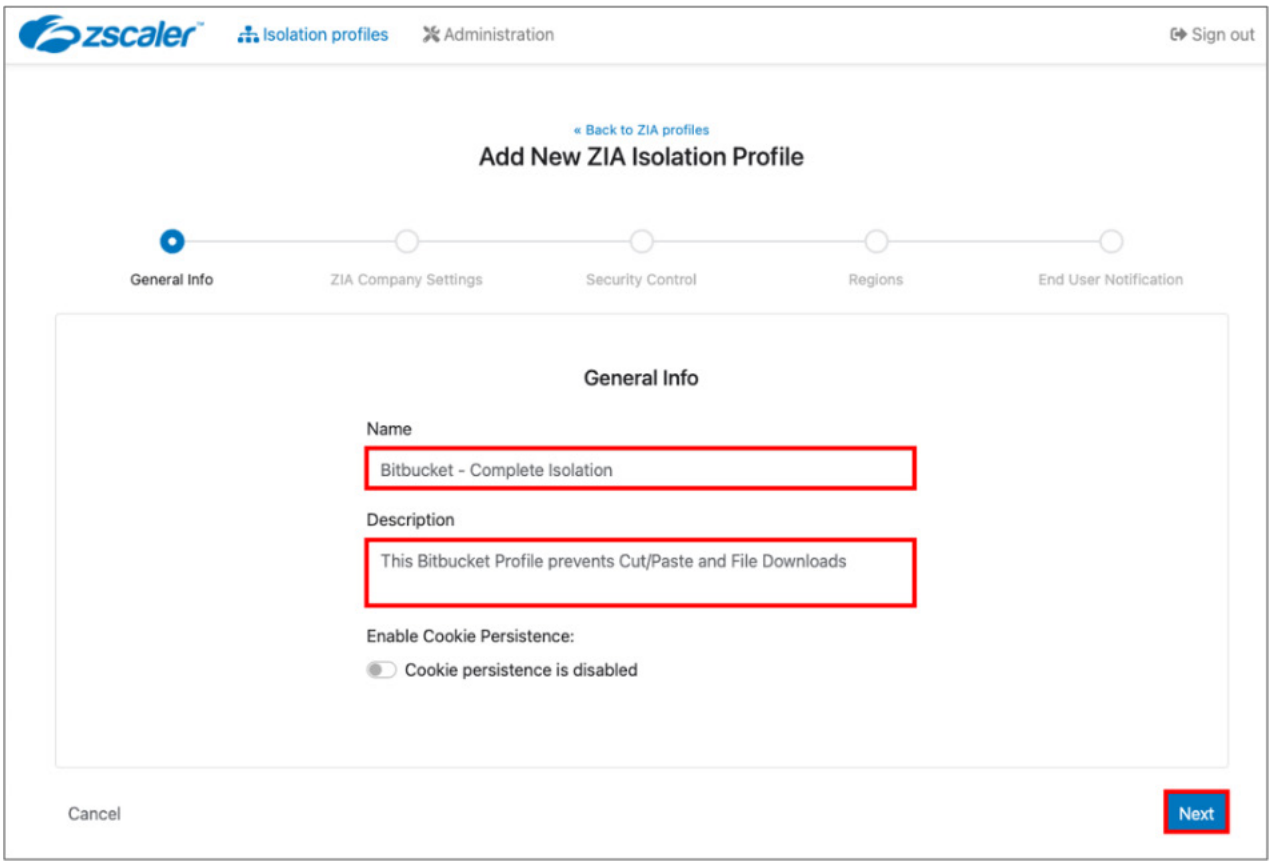

Figure 9. Cloud Browser Isolation general information

For the **ZIA Company Settings**, you must select your **Company ID and Cloud** if your information is not populated automatically. Obtain this information from your ZIA Admin Portal under Administration > Company:

1. Select your **Company ID** and **Zscaler Cloud**.
2. Leave the **Zscaler Root Certificate** as the **Default Certificate**.
3. Click **Next**.

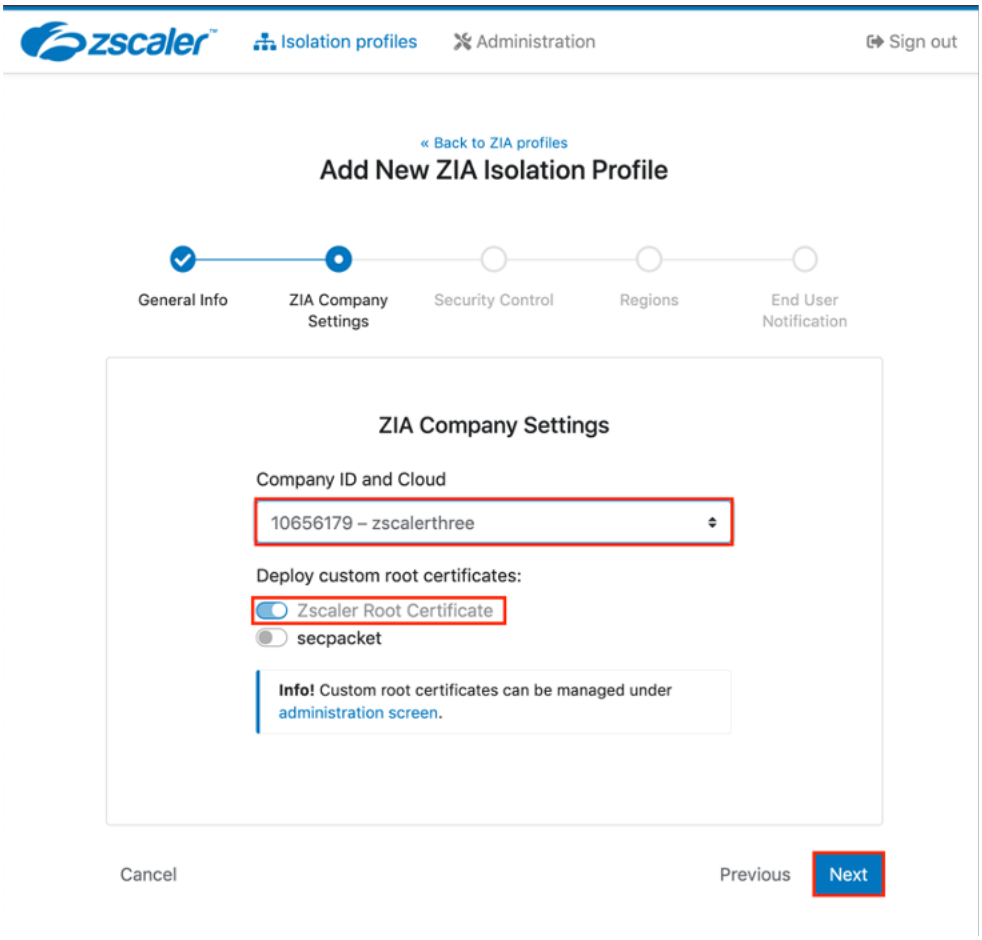

Figure 10. Cloud Browser Isolation ZIA company information

The Security Control of Cloud Browser Isolation allows administrators to maintain a complete air gap between the user and Atlassian, or allow some level of control of the Atlassian applications in the Isolation Session. Settings include allowing copy and paste up to or down from Bitbucket, Confluence and Jira from or to the local computer. You can also control file transfers up to or down from Atlassian products to or from the local computer.

Allowing **Local Browser Rendering** lets the user visit pages outside of the Atlassian domain while in the Isolation Session. This profile maintains the strictest security settings and does not enable any controls.

4. Toggle the security controls you want to allow, then click **Next**.
5. Select two **Regions** for redundancy. (Select the two closest regions to your organization.)
6. Select **Next**.

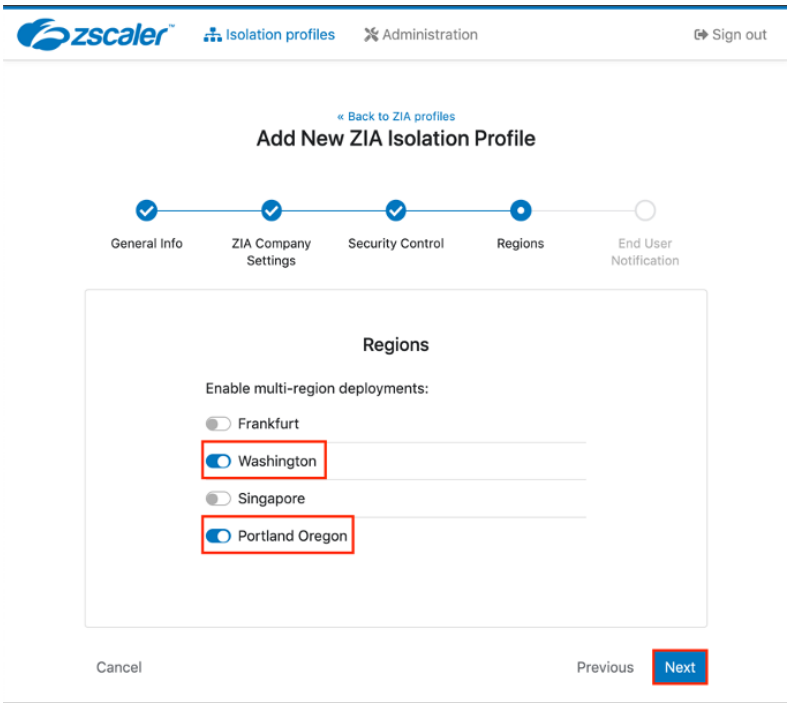

Figure 11. Cloud Browser Isolation regions

7. Use the default **End User Notification**. However, you can create a customized EUN in the **Administration** section of the Cloud Browser Isolation Portal and add it to the profile.

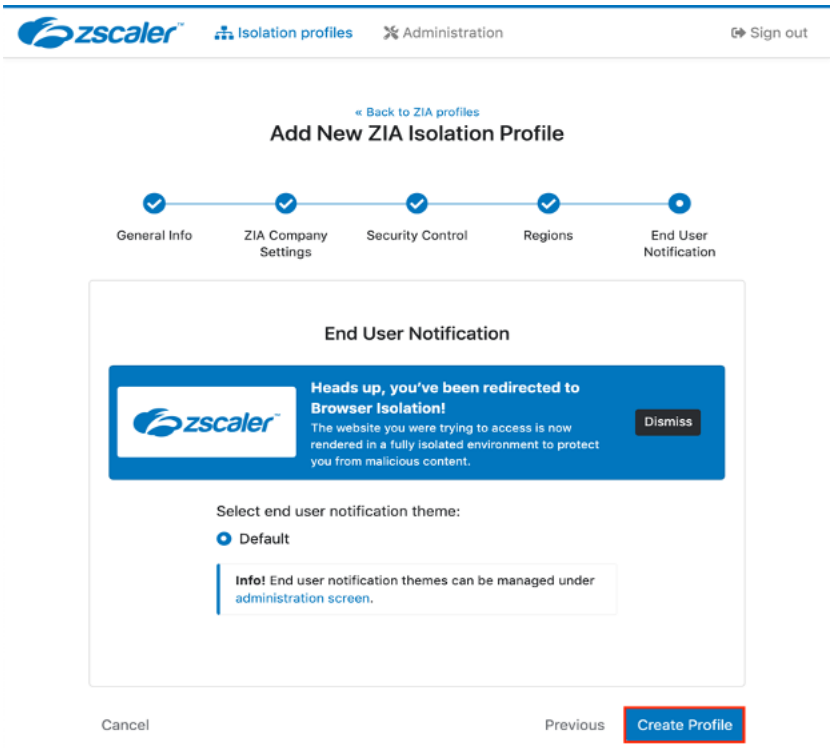

Figure 12. Cloud Browser Isolation EUN

8. To complete the profile, click **Create Profile**.

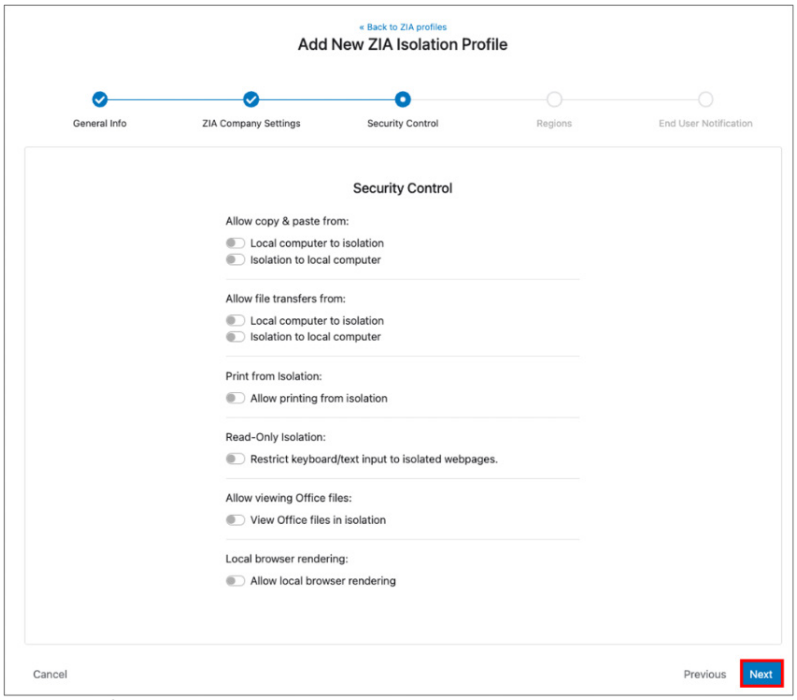

Figure 13. Cloud Browser Isolation security settings

The completed profile appears as a profile option when setting up isolation policies in ZIA.

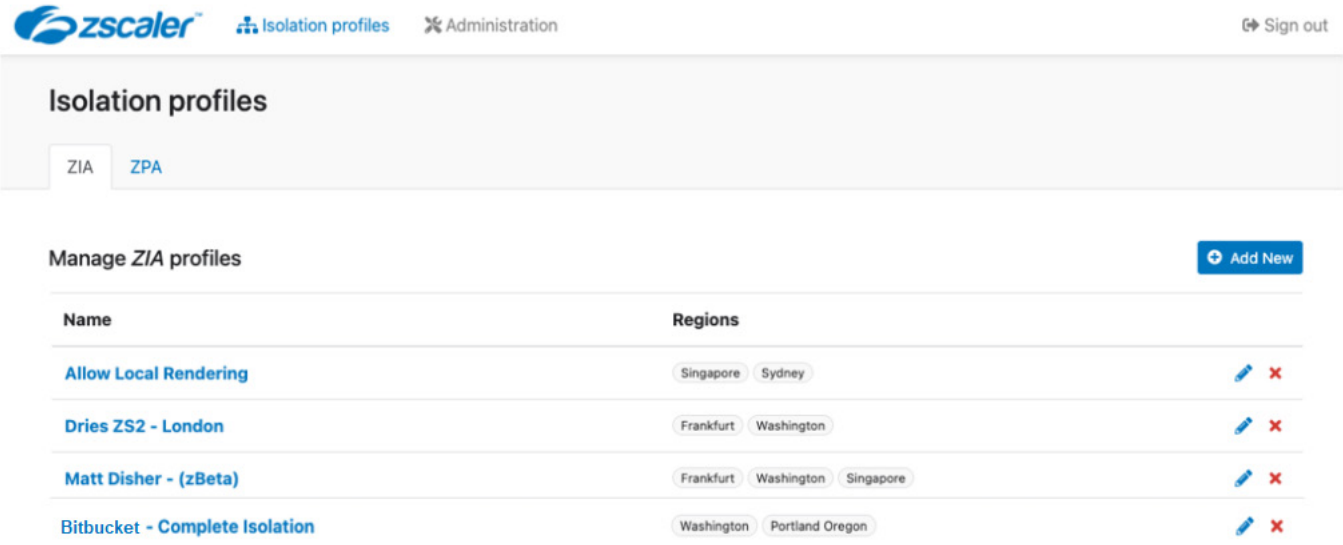

Figure 14. The completed Cloud Browser Isolation profile

Configure Bitbucket SaaS Application Tenant

Next, set up Zscaler Isolation Policies in the ZIA Admin Portal for Atlassian Bitbucket cloud application.

To launch the SaaS Application Tenants wizard for the ZIA Admin Portal:

1. Go to **Administration** > **SaaS Application Tenants**.
2. In the **SaaS Application Tenants** window, click **Add SaaS Application Tenant**.

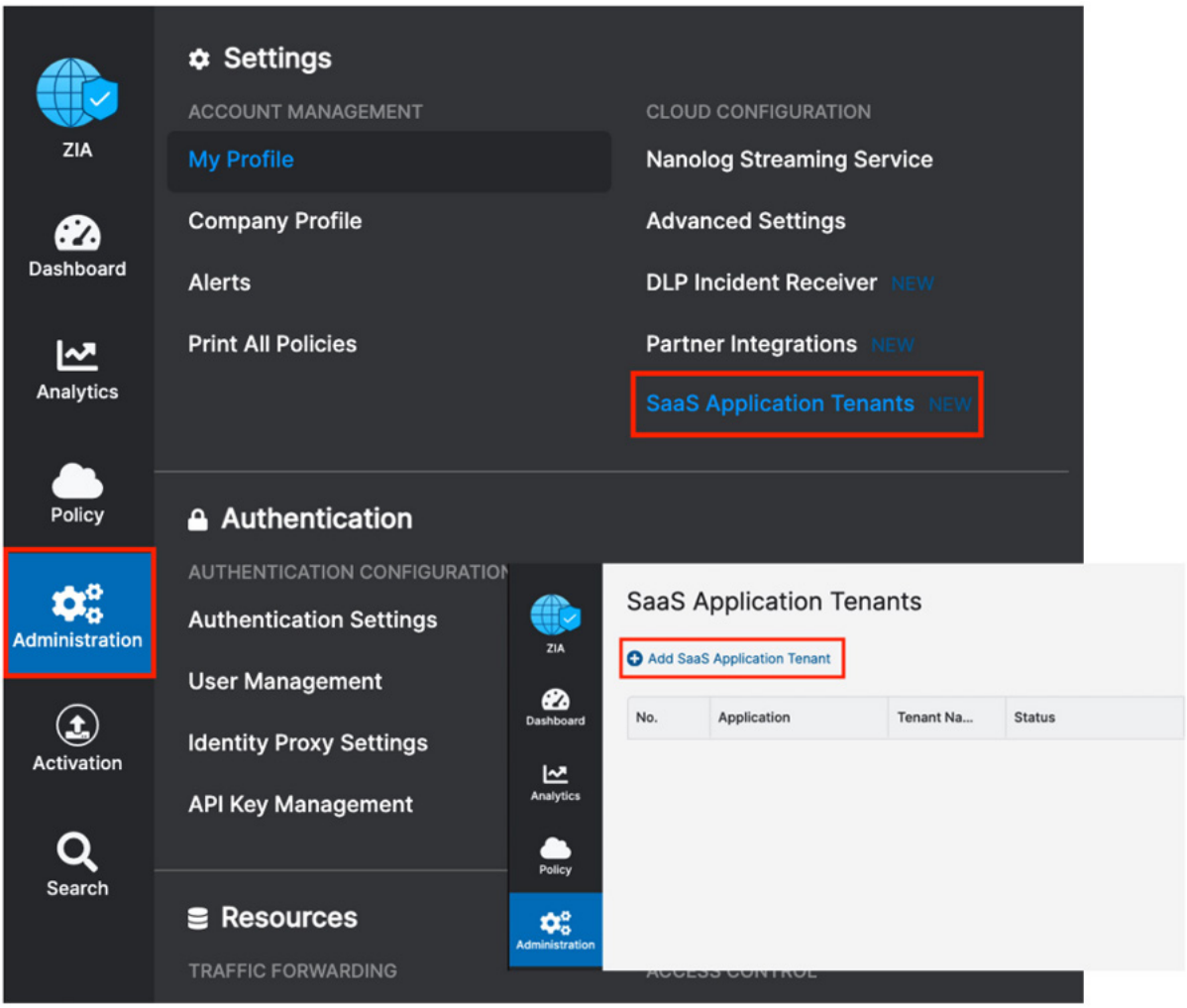

Figure 15. ZIA SaaS application tenant

Bitbucket SaaS Tenant Configuration Wizard

To start the wizard:

1. Click **Add SaaS Application Tenant** on the tenant page.
2. Select the **Bitbucket** tile on the wizard.

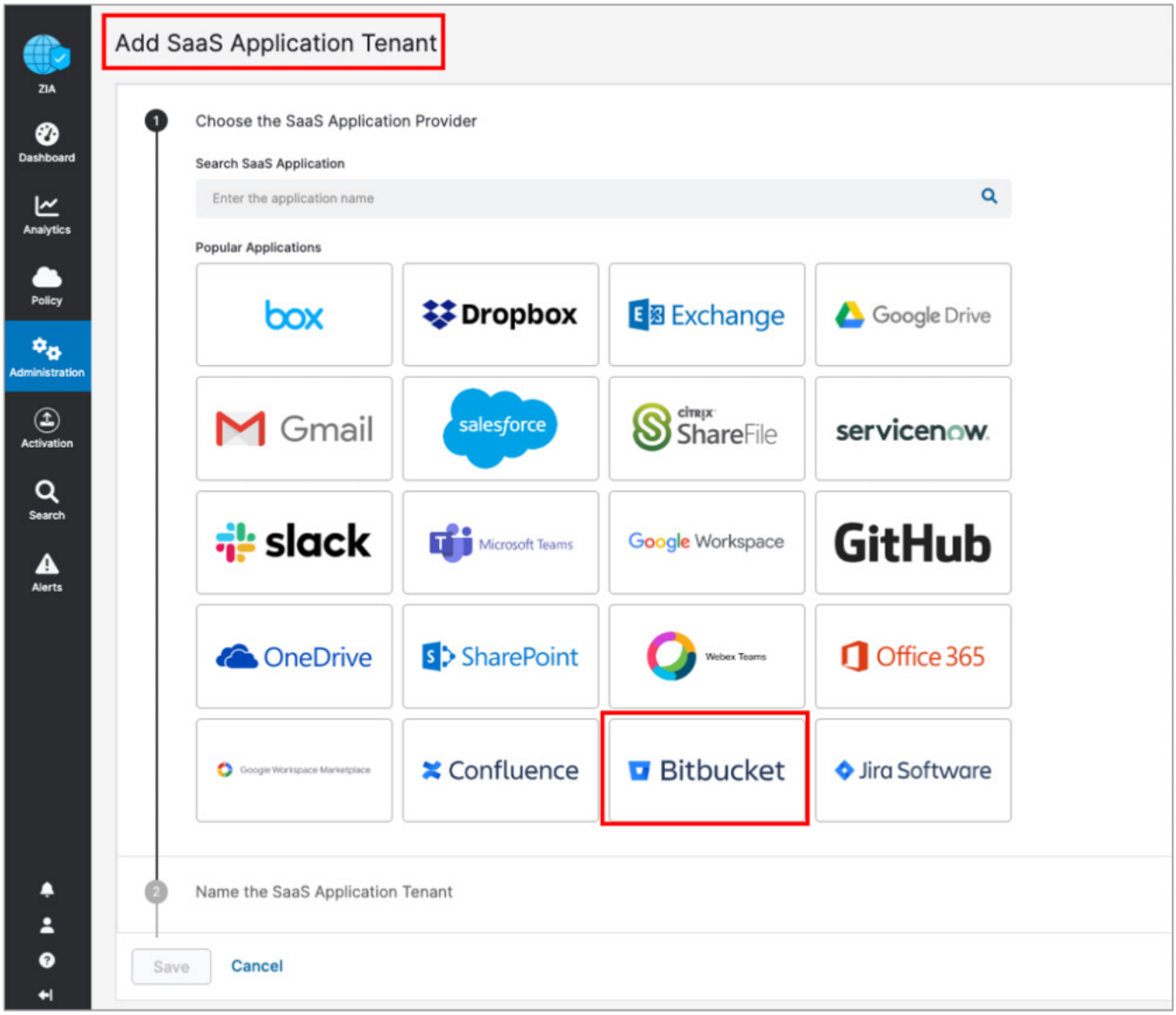

Figure 16. The SaaS application tenant configuration wizard

3. Enter a name in the **Tenant Name**. This is the name that is selected when assigning a policy for the Zscaler security features.
4. Enter the **Bitbucket Admin Email ID**.
5. Click **Provide Admin Credentials**, which redirects you to the Bitbucket login page.

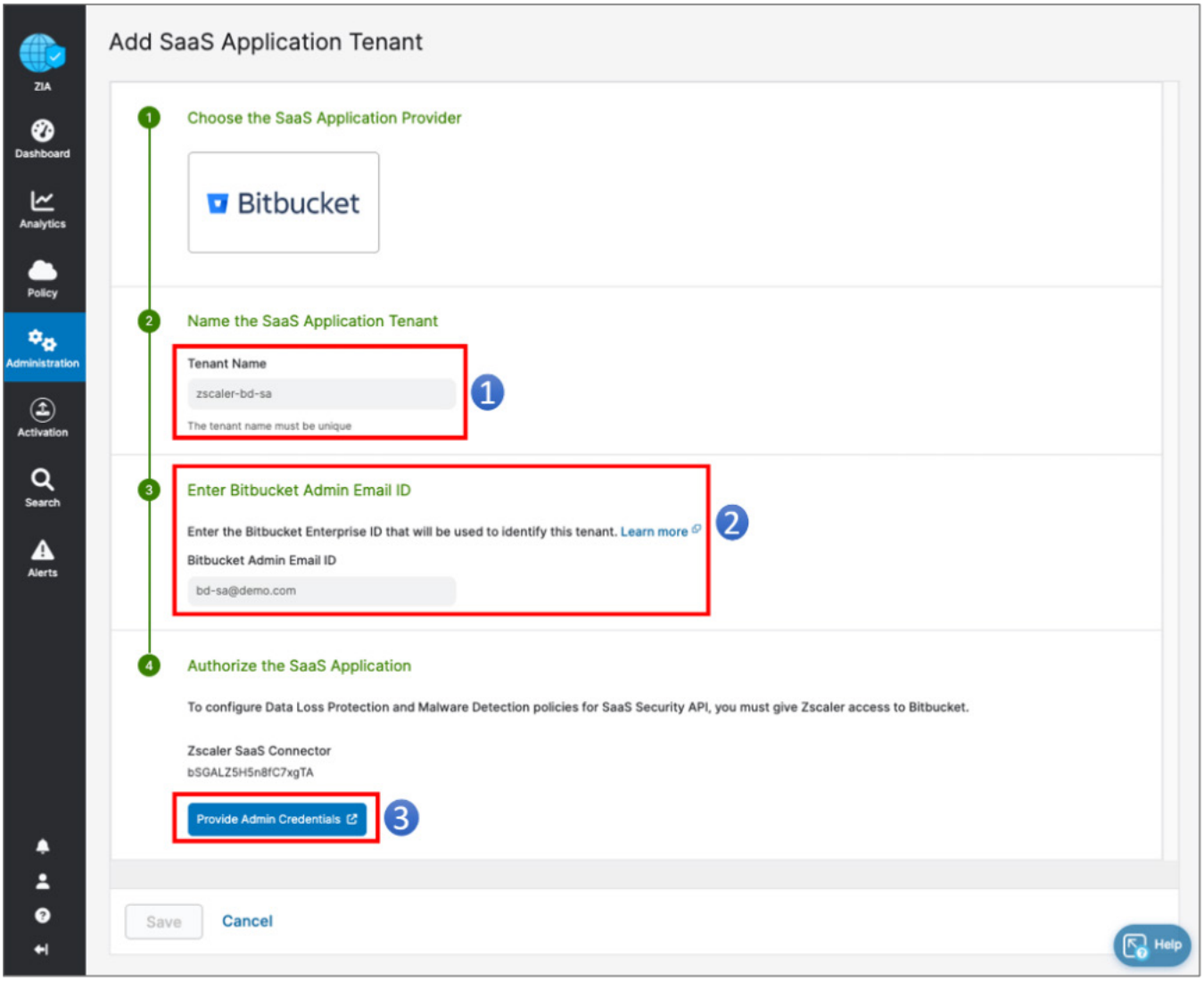

Figure 17. Authorize Zscaler SaaS Connector

6. Enter the same **Bitbucket Admin Email ID** that you entered earlier.

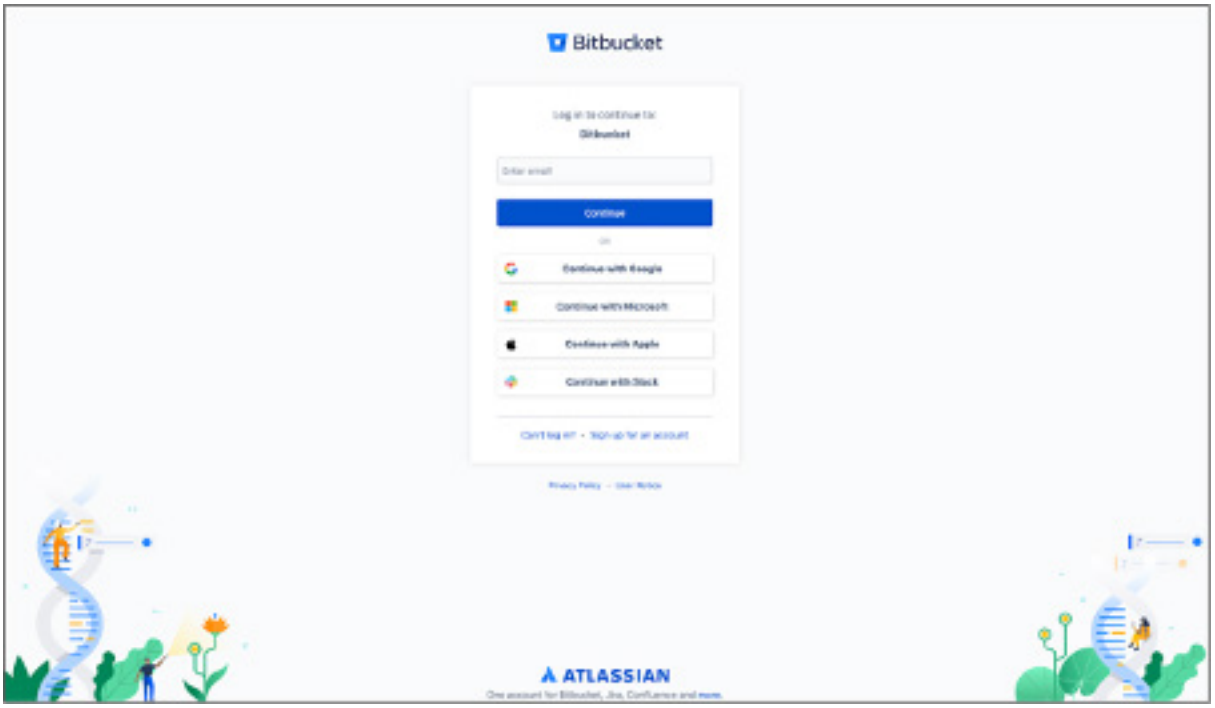

Figure 18. Authenticate to the Bitbucket tenant

7. Click **Grant access** to give permission to Zscaler Client Connector.

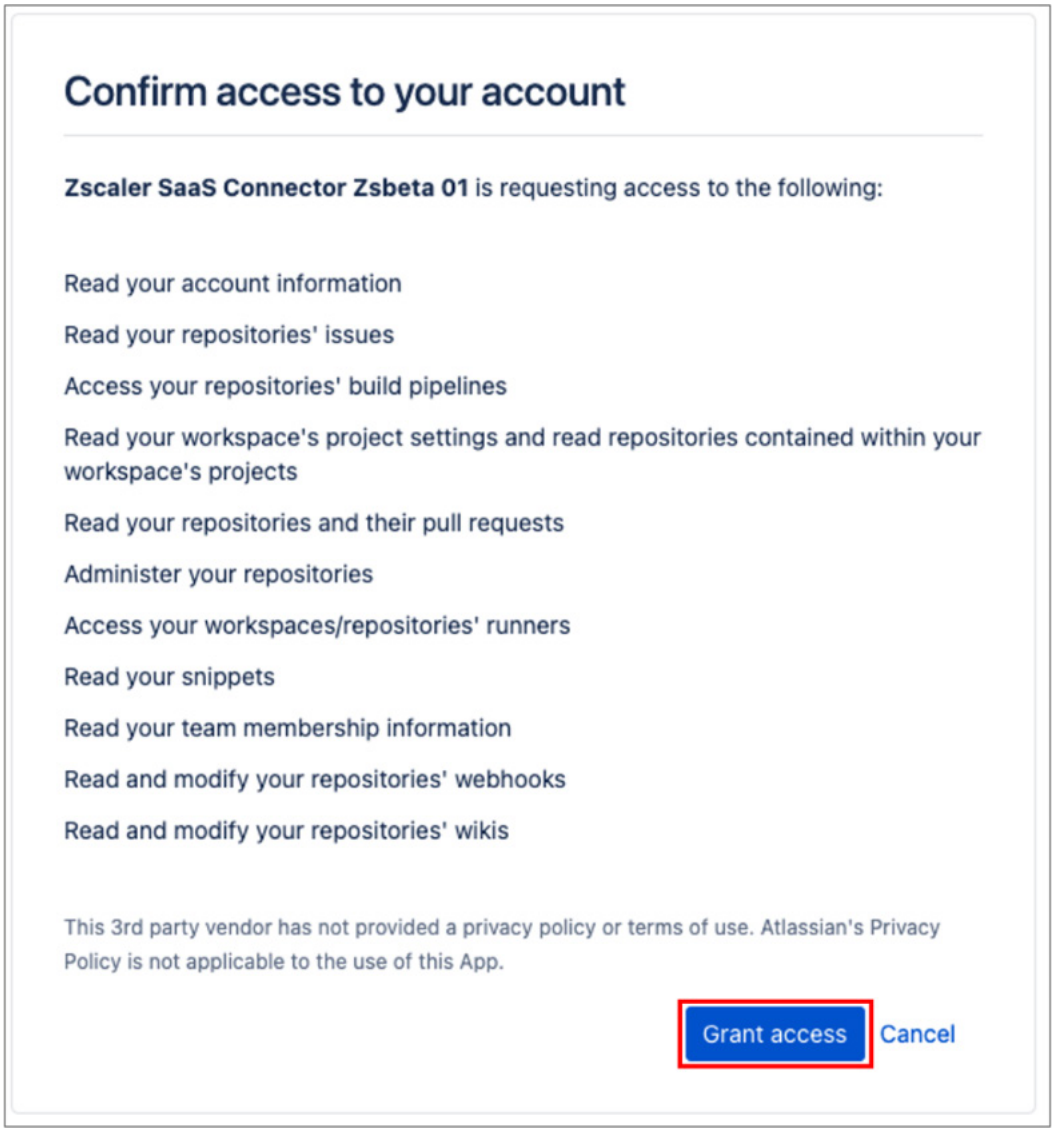

Figure 19. Grant access to Zscaler SaaS Connector

8. Click **Save**.

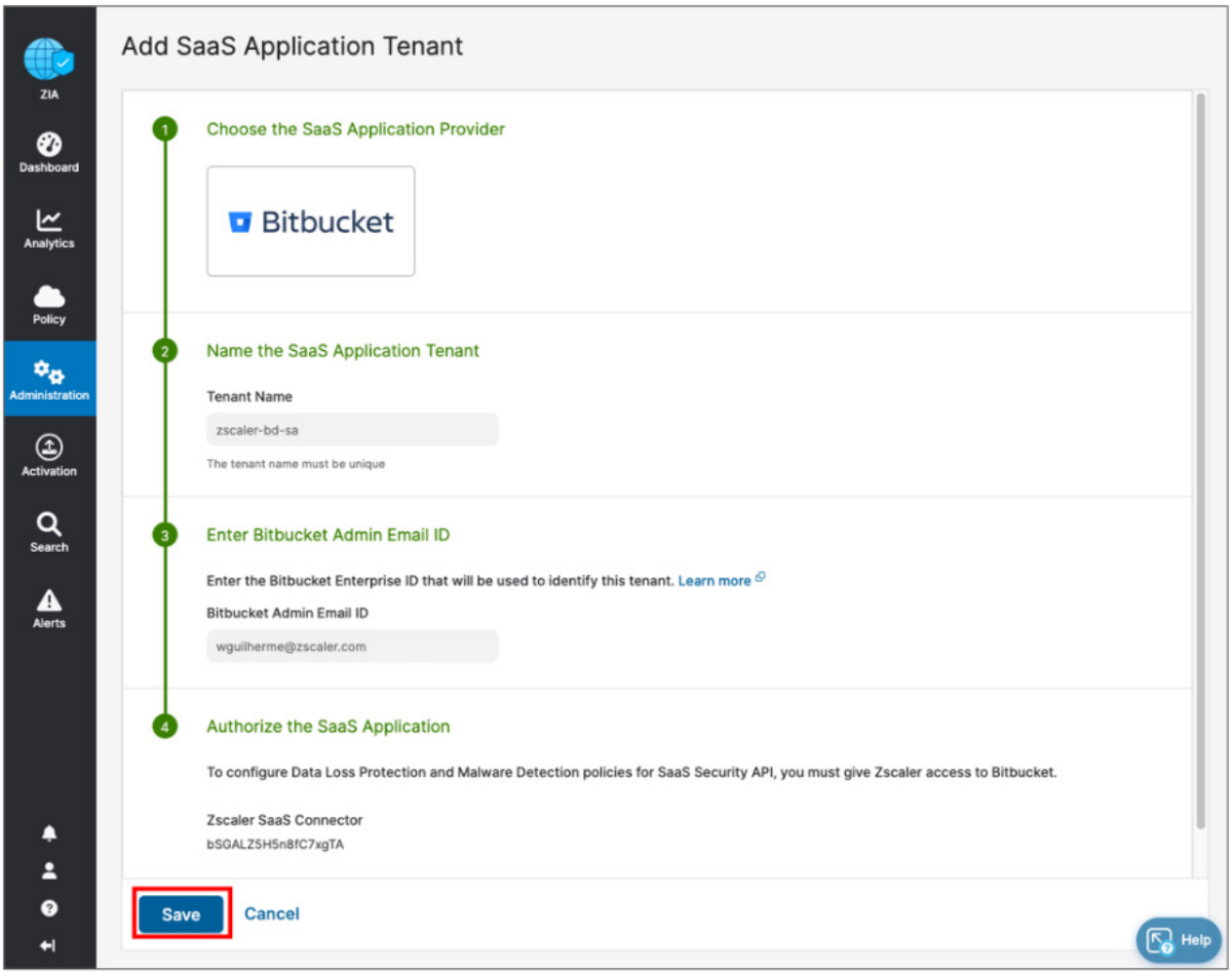

Figure 20. Zscaler SaaS Connector

The completed and active Bitbucket API connector is displayed.

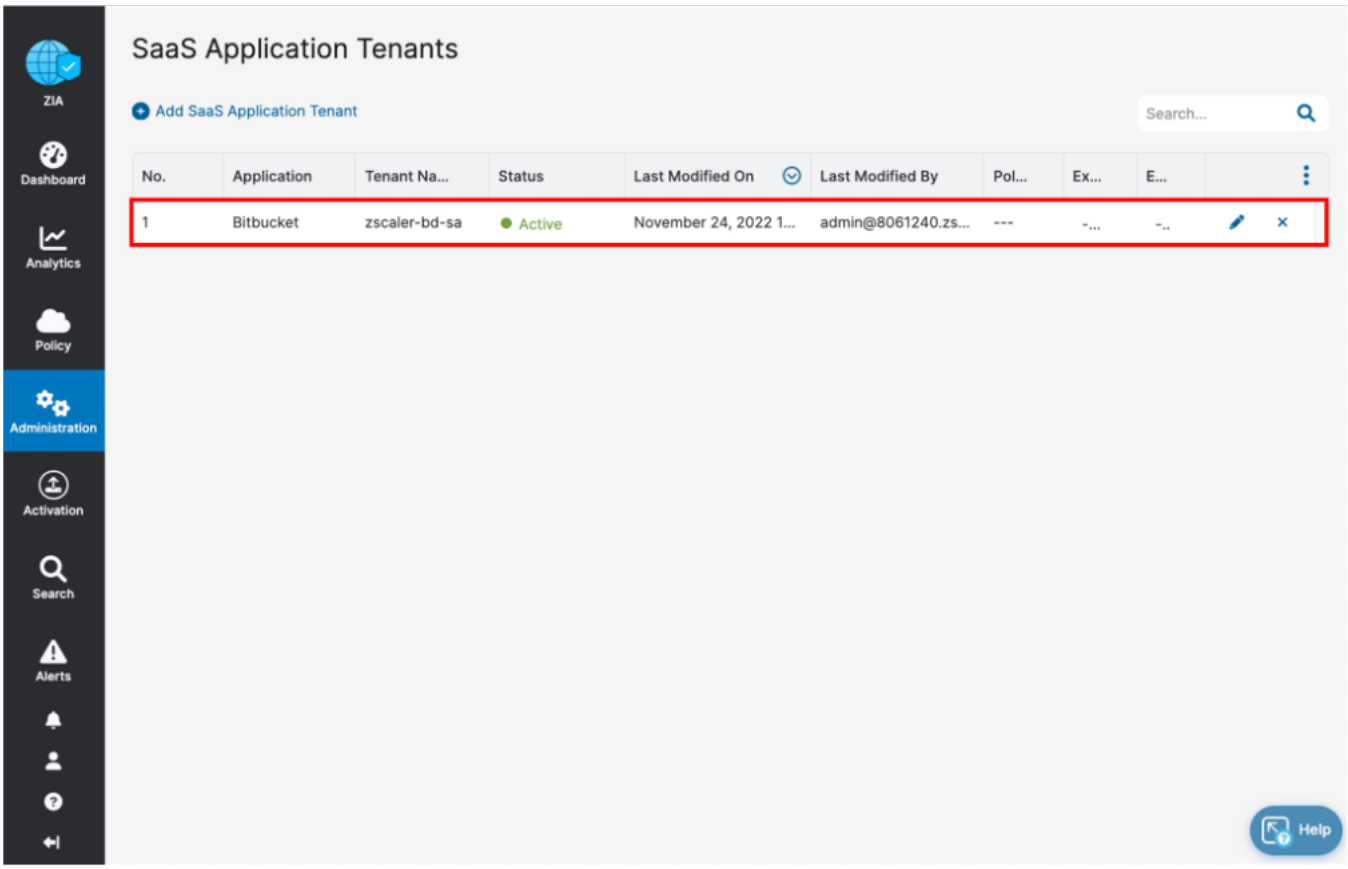

Figure 21. Completed Bitbucket API connector

Configure Bitbucket Policies and Scan Configuration

After adding and configuring the Bitbucket tenant, configure the SaaS Security API to control DLP, malware policies, and scan the configuration for the policies. You can also view reports and data for Bitbucket in analytics, SaaS security insights, and logs.

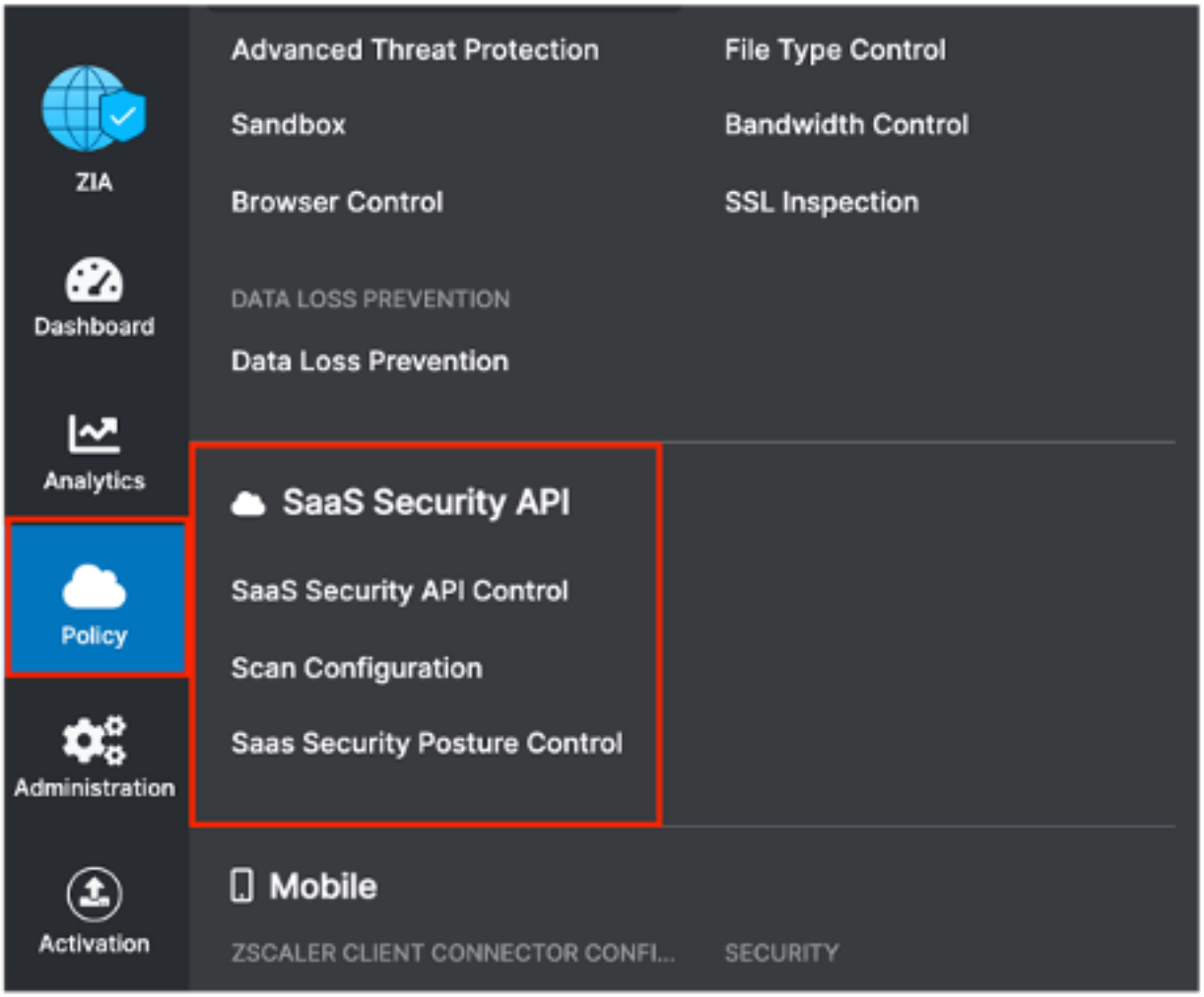

Figure 22. Configure SaaS Security API in ZIA Admin Portal

Scoping the Policies and Remediation

Zscaler SaaS Security API scans file attachments. This deployment guide configures a basic DLP policy and a malware policy. The policies scan the Bitbucket files for matching content of the DLP policy and known malware for the malware policy. A Bitbucket repository is created with malicious attachments and DLP violations to test the policies.

Zscaler SaaS Security API out-of-band data protection capabilities look inside the SaaS applications themselves through API integrations to identify accidental or intentional data exposure and compliance violations that would otherwise go unnoticed.

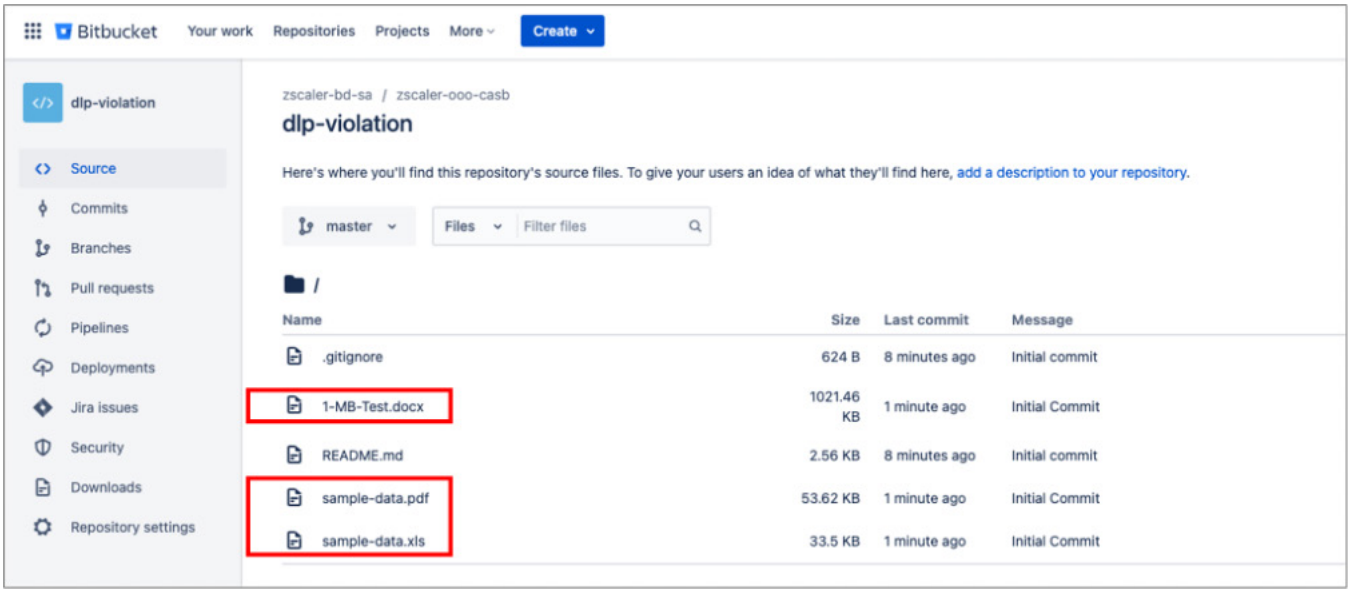

Figure 23. Bitbucket repository

The DLP policy creates a spreadsheet with a list of US Social Security numbers. DLP is a subject of its own, and this policy is only used for demonstration purposes. Conduct a true DLP policy review to minimize false positives and false negatives.

It is also important to note that SaaS DLP protection is only part of the Zscaler DLP solution and is used to scan data-at-rest (like the Bitbucket files). This deployment guide doesn't cover in-line data protection, exact data match, or indexed document matching (document template fingerprinting), although they are integral pieces of a complete data protection solution.

For next steps to test the DLP SaaS functionality, create a basic policy and apply it to the Bitbucket tenant. If you already have DLP policies created, skip to Configure a SaaS Malware Policy for Bitbucket.

Creating a DLP Policy

Create a custom dictionary (or use the available dictionaries) to identify the data the scan is going to look for.

Then create an engine that is the logical template for adding expressions and additional data. This is where you would specify Social Security numbers and any other criteria for the policy. The engine provides the means to precisely add or remove data to match violations and eliminate false positives.

A SaaS security DLP policy is created that allows you to specify the details about where, when, the action taken, and whom to inform about violations.

Notice that you can create a custom DLP dictionary that contains your own patterns and phrases, or use one of the predefined dictionaries. This deployment guide focuses on predefined dictionaries.

Creating a DLP Engine

To create a DLP engine:

1. Click the **DLP Engines** tab.
2. Click **Add DLP Engine**.

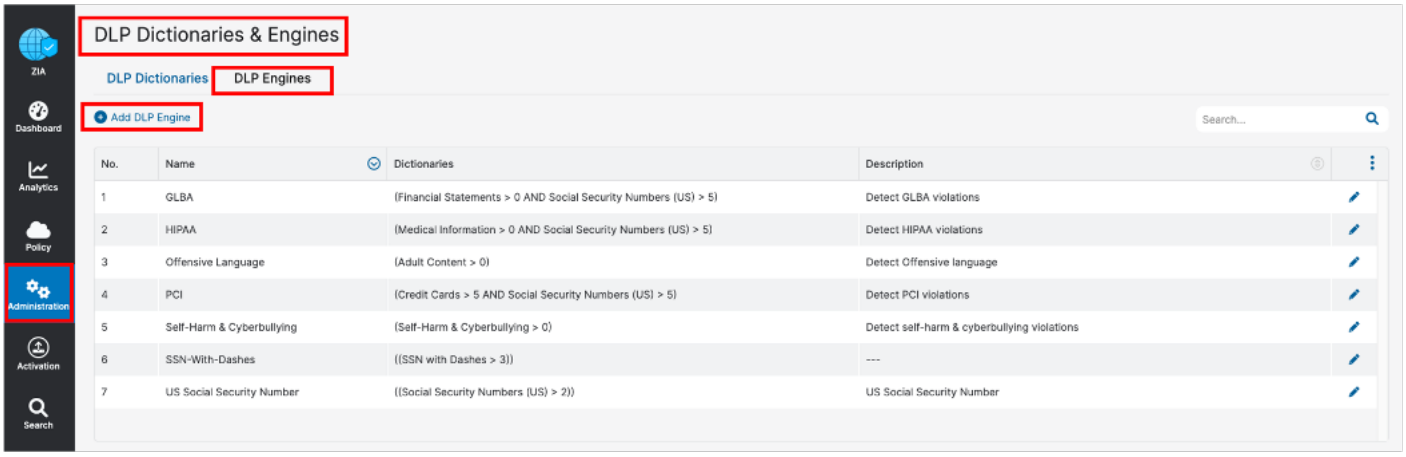

Figure 24. Creating a DLP engine

3. Give the DLP engine a **Name**.
4. In the **Engine Builder** under **Expression**, select the desired dictionary. In the following example, **Social Security Numbers (US)** is selected.
5. Specify the **Match Count**, which is the minimum number of instances the data must occur in the file.
6. (Optional) Click **Add** to add the next dictionary and repeat the process of naming and defining the dictionary.
7. Click **Save**, then **Activate** the configuration.

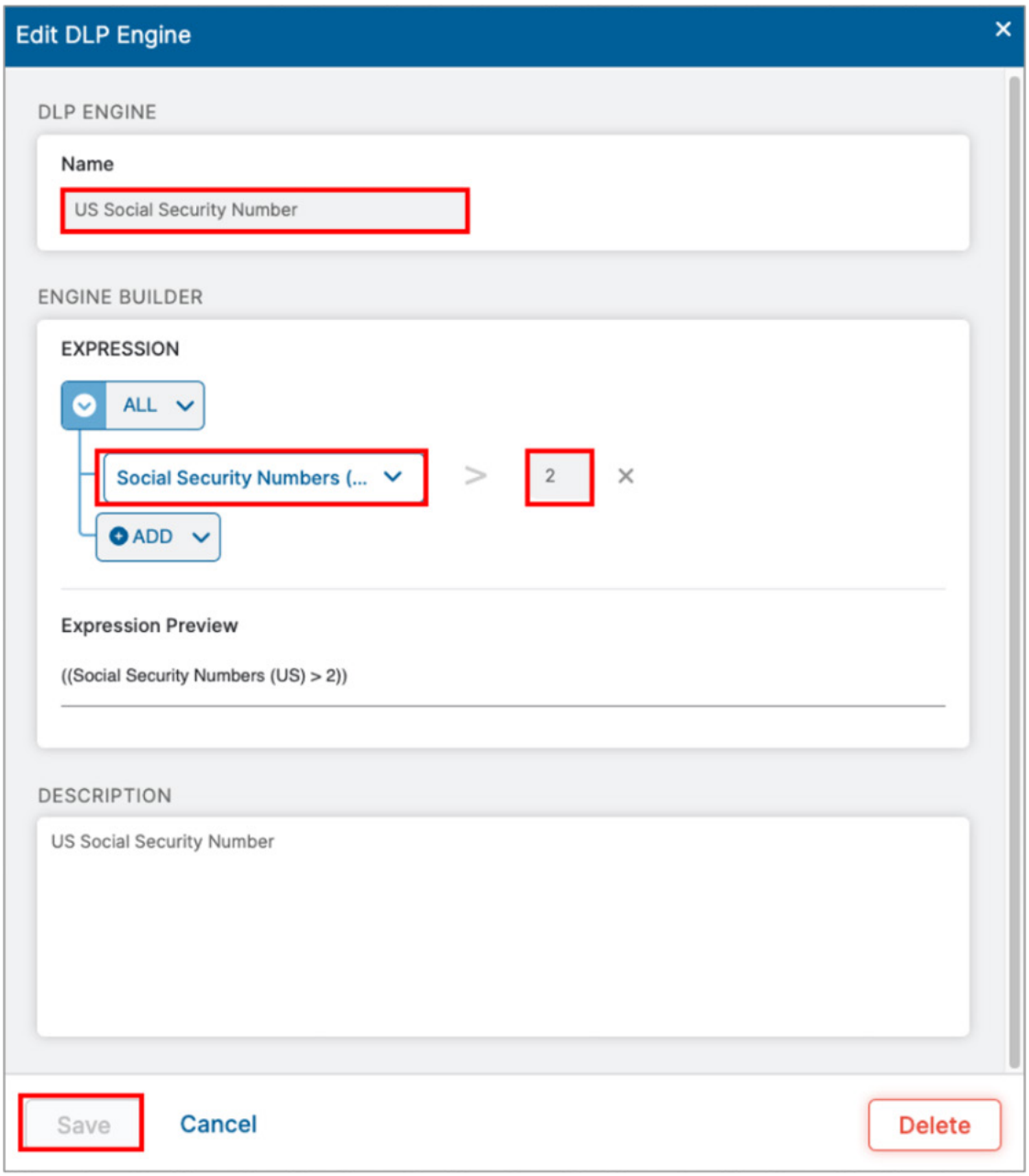

Figure 25. The DLP engine wizard

This policy triggers when you see the third Social Security number. Again, this is a demonstration and the criteria is too general to be a production DLP rule.

Configure a SaaS DLP Policy for Bitbucket

Apply the engine to a DLP policy used for the Bitbucket instance. Launch the Add DLP Rule wizard to start the process:

1. Go to **Policy** > **SaaS Security API Control** > **Data Loss Prevention**.
2. Select **Source Code Repository**.
3. Click **Add DLP Rule**.
4. Select **Bitbucket** as the **SaaS Application Tenant**.
5. Select the **DLP Engine** created in [Bitbucket SaaS Tenant Configuration Wizard](#).
6. Select **Any-Any** for **Collaboration Scope**.
7. Select **Report Incident Only** as the **Action**.
8. Select **High** as **Severity** to allow for identification, searches, and tracking.
9. Click **Save**, and then **Activate** your configuration.

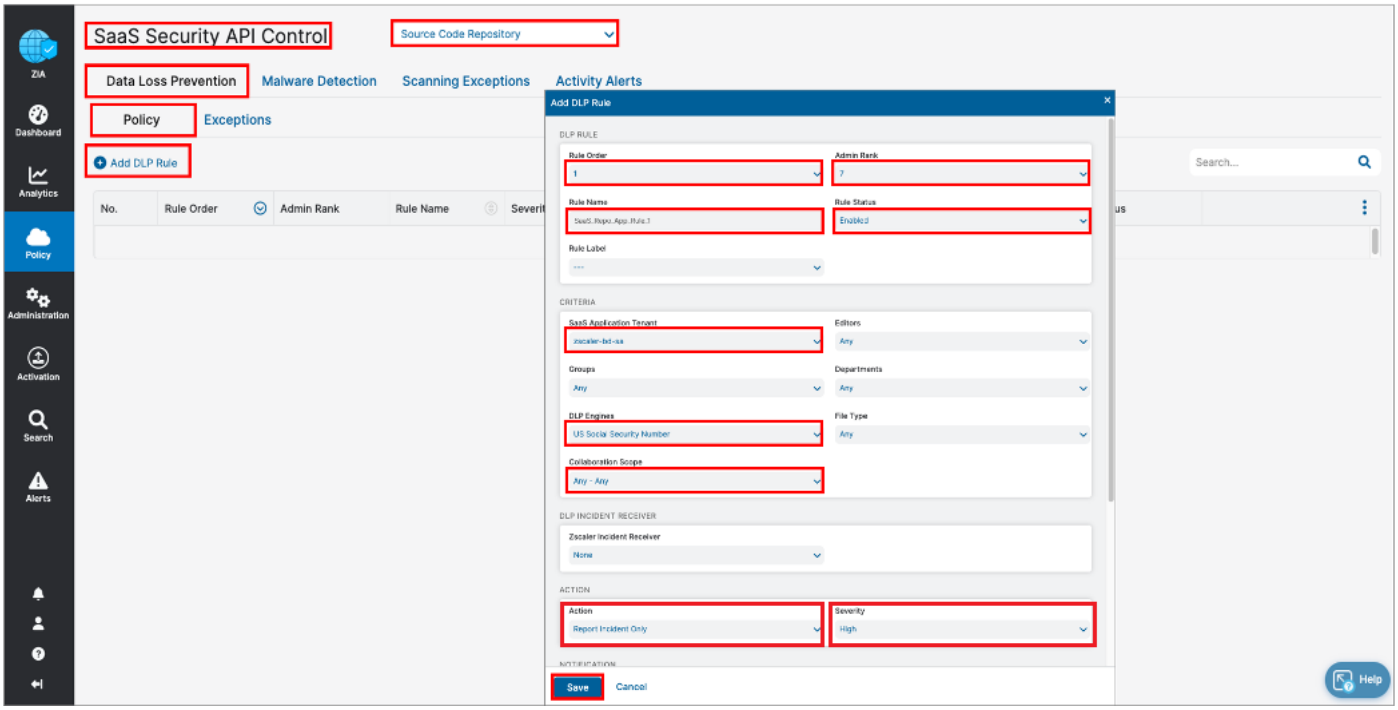

Figure 26. Launch the SaaS DLP Policy Configuration Wizard

Apply a scanning schedule to the Bitbucket DLP rule.

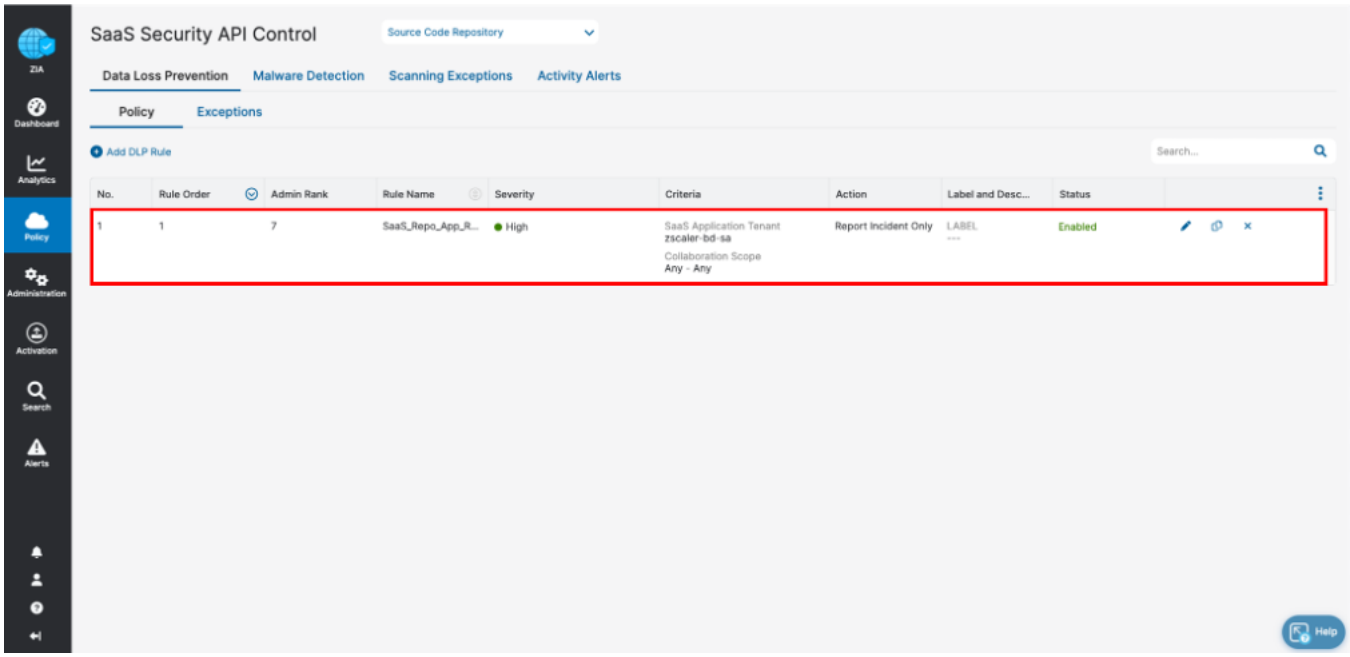

Figure 27. The configured DLP policy

SaaS DLP Policy Details

The SaaS DLP policy specifies the details on whom and what data this policy applies. You specify the rule order if you have multiple DLP policies, which are processed in an ascending manner. The first rule that matches is the applied rule. Specify the DLP engine you defined, any file owners, groups or departments, and the file types to inspect. The collaboration scope and the action are unique to the SaaS DLP. Select Any Collaboration, and an Action of Remove Sharing.

The Collaboration Scope includes the collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select Any to apply the rule to files with all collaboration levels, or select one or more of the following collaboration scopes and specify the permissions for each scope:

- External Collaborators: Files that are shared with specific collaborators outside of your organization.
- External Link: Files with shareable links that allow anyone outside your organization to find the files and have access.
- Internal Collaborators: Files that are shared with specific collaborators or are discoverable within your organization.
- Internal Link: Files with shareable links that allow anyone within your organization to find the files and have access.
- Private: Files that are only accessible to the owner.
- The Action: The rule acts after detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant. For Bitbucket, the action is Report Incident Only. This means that any violations are reported in the Zscaler SaaS Analytics and alerts are sent to auditors if defined.
- Report Incident Only: The rule reports only the incident and makes no changes to the file's collaboration scope.

Configure a SaaS Malware Policy for Bitbucket

To launch the Malware Rule wizard:

1. Go to **Policy** > **SaaS Security API Control** > **Malware Detection**.
2. Select **Source Code Repository**.
3. Click **Add Malware Detection Rule**. The SaaS Security API Malware Detection policy is an all-encompassing policy and all files in the tenant are scanned. You can remove files from the scope by selecting the **Exceptions** tab under **Malware Detection**. To add a malware policy, specify the application, the SaaS tenant, and the status.

The action for Bitbucket is limited to only Report Malware.

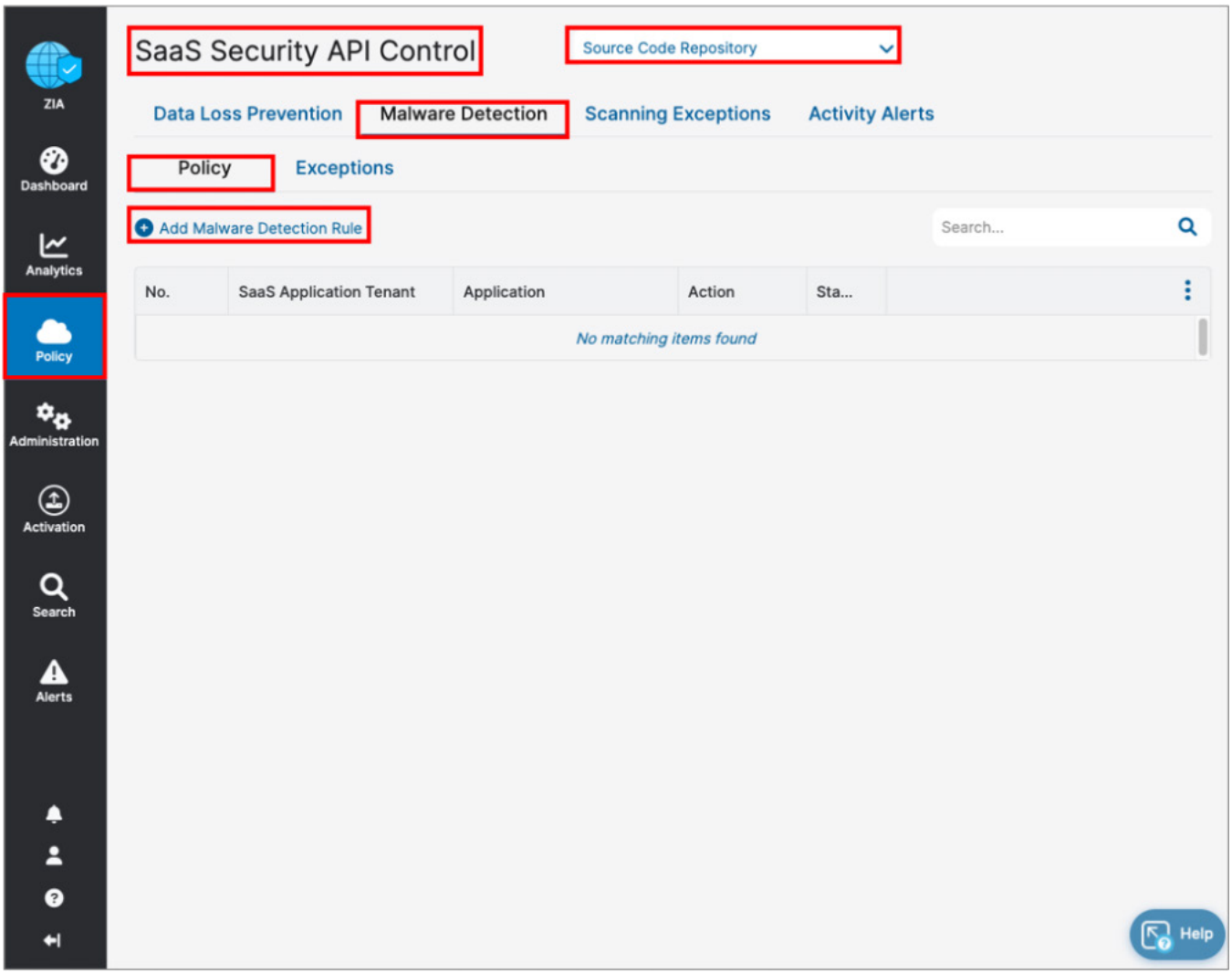

Figure 28. Launch the malware Policy Configuration wizard

Bitbucket SaaS Malware Policy

Configure the Malware Detection Rule:

1. Go to **Policy** > **SaaS Security API Control** > **Malware Detection**.
2. Select **Source Code Repository**.
3. Click **Add Malware Detection Rule**.
4. Under **Application**, select **Bitbucket** as the application.
5. Select **Bitbucket** as the **SaaS Application Tenant**.
6. Select **Enabled** for **Status**.
7. Click **Save**.

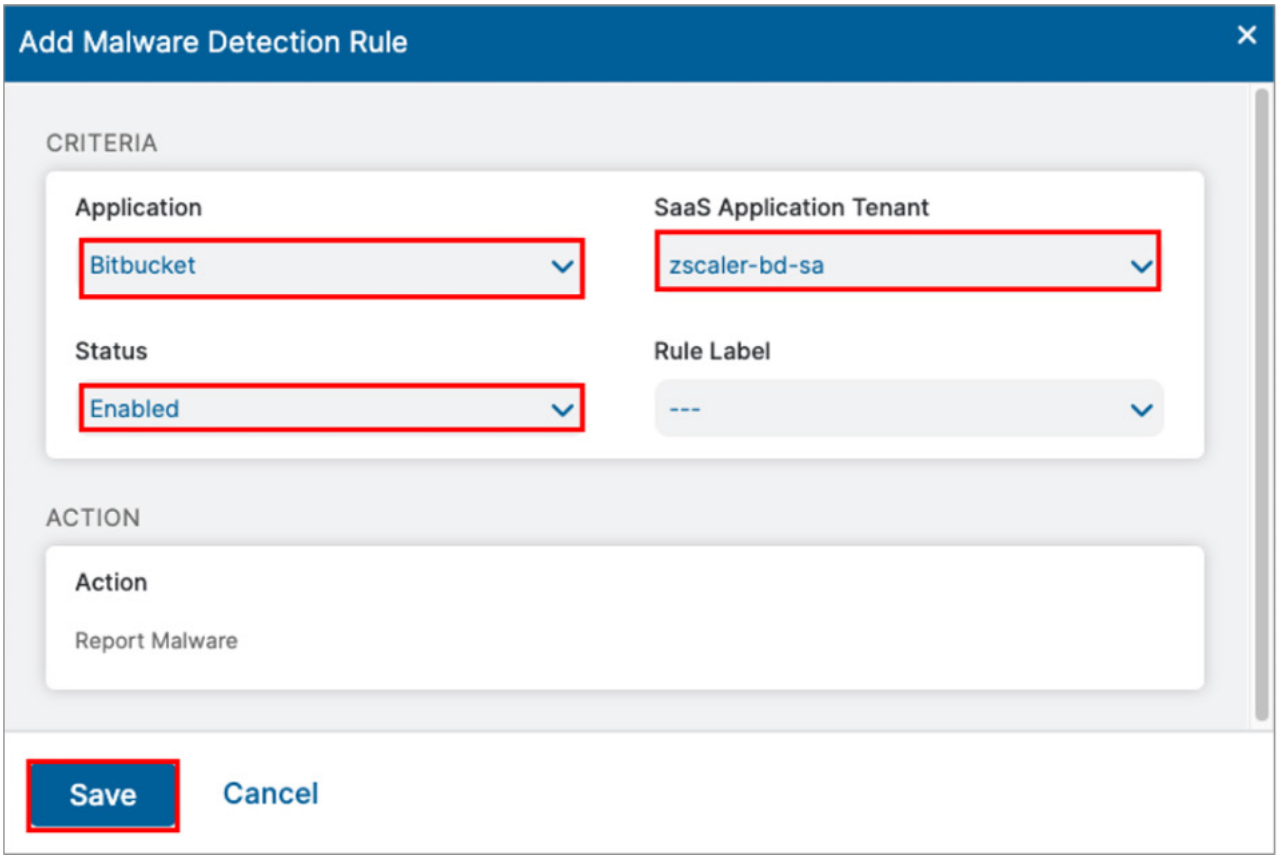

Figure 29. The Malware Policy Configuration wizard

Bitbucket SaaS Malware Policy

Apply the completed SaaS Security API Malware Detection policy for the Bitbucket SaaS Application Tenant to the Bitbucket instance with a scanning schedule. Activate your configuration.

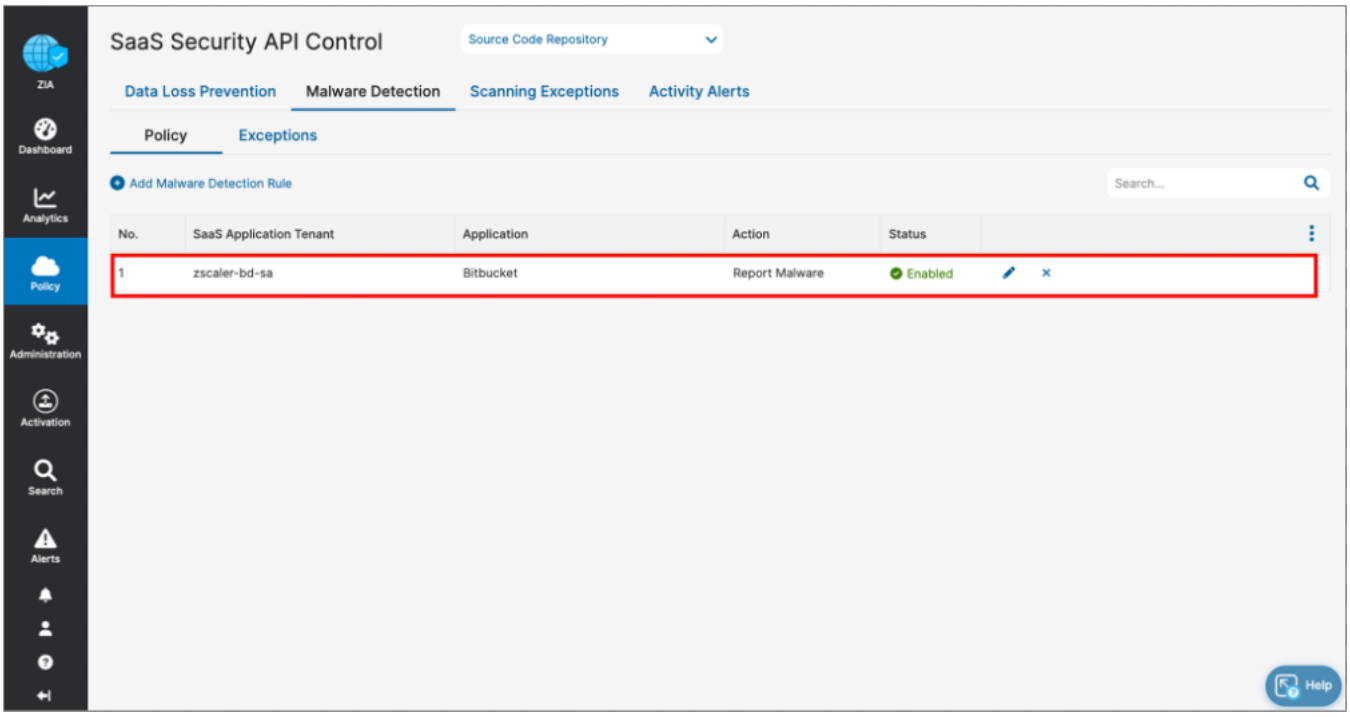

Figure 30. The complete Bitbucket Malware Policy Configuration wizard

Configure a Scan Schedule Configuration for Bitbucket

The final configuration step is to create a Scan Configuration. Specify the tenant to which Scan Configuration applies, any policies that are to be included in the scan, and what data to scan relative to a date. The options for Data to Scan are All Data, Date Created or Modified After, or New Data Only. For this deployment guide, select All Data.

However, if this is a Proof of Value (POV) or a Trial, the only option available is New Data Only.

To add a Scan Schedule:

1. Go to **Policy** > **SaaS Security API Control** > **Scan Configuration** > **Add Scan Schedule**.
2. Select the **Bitbucket** as the **SaaS Application Tenant**.
3. In the **Policy** field, select the Data Loss Prevention policy and Malware policy created in prior procedures.
4. Select **All Data**. (Or, for a POV or Trial, select **New Data Only**.)
5. Click **Save**, and then **Activate** the configuration.

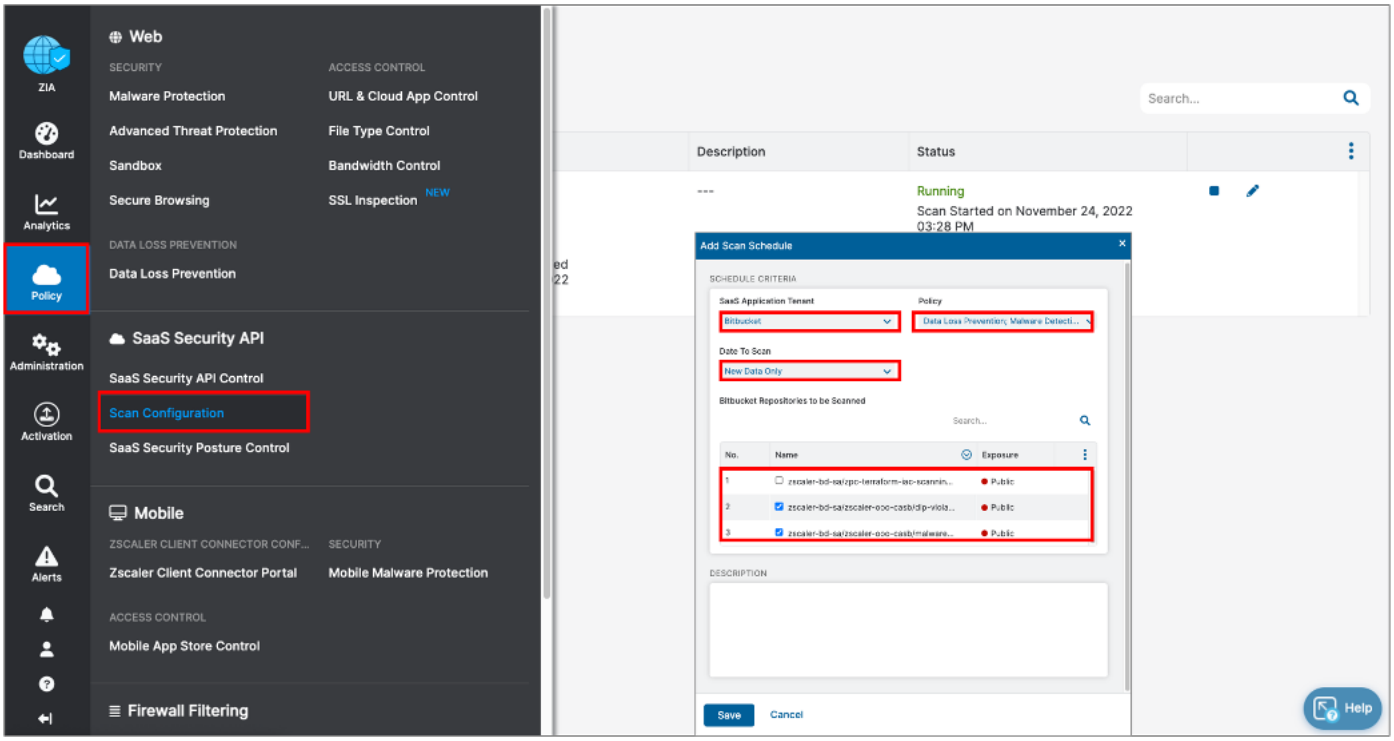

Figure 31. Create and enable a scan for the Bitbucket SaaS tenant

Start the Scan Schedule

After the schedule has been configured and saved, start the scan for the DLP policy and malware policy to be applied.

1. Click the **Start** icon on the Scan Configuration window to start the SaaS Security API on the Bitbucket tenant. When the scan is running, the icon changes from a run symbol to a stop symbol.
2. Review the **Status** column and ensure it is **Running** with a start date and a latest scan date.

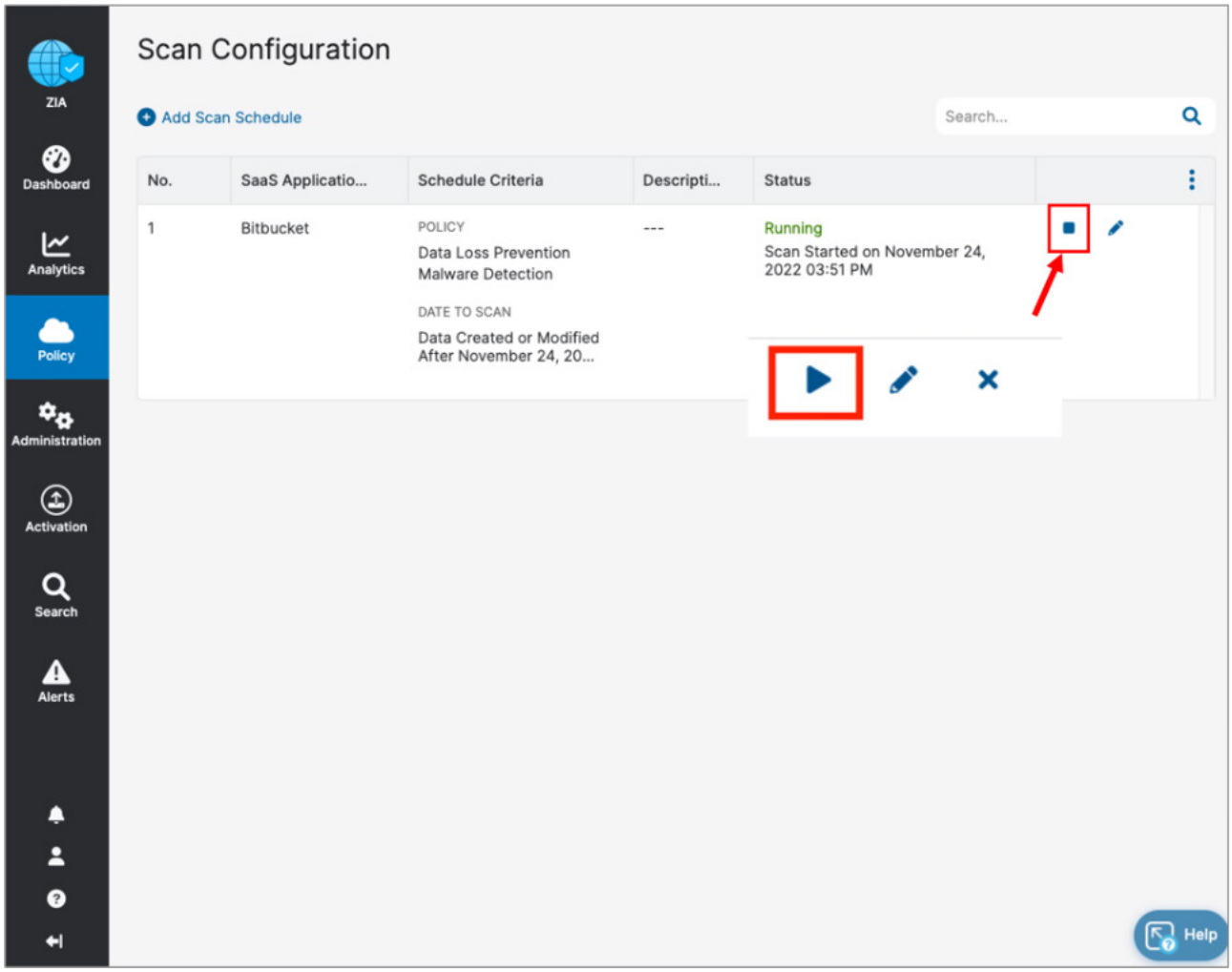

Figure 32. Starting the Bitbucket Scan Schedule

Bitbucket Reporting and Visibility

Zscaler analytics provide detailed reporting of all user activity down to each session created by the user when visiting a destination. Zscaler extends that visibility to include reporting of activity, malware incidents, and DLP violations of data at-rest associated with the user. Zscaler has reports and SaaS security insights, which provide visibility from a high-level overview to management of the individual logs and violations.

To learn more, see [SaaS Security Insights].

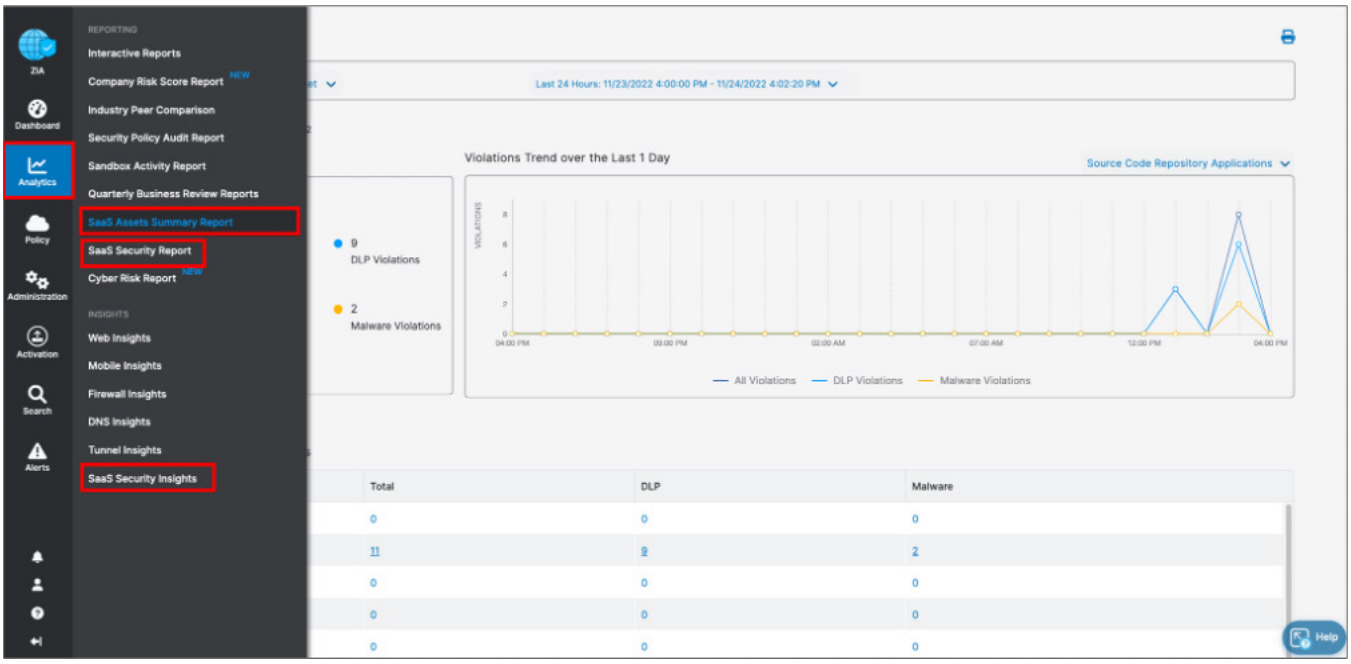

Figure 33. SaaS security visibility

SaaS Assets Summary Report

A SaaS Assets Summary Report provides all activity and violations at a quick glance. The report identifies all SaaS tenant information from a single page. Although your Bitbucket activity over the creation of this deployment guide is shown, any configured tenant is displayed on this summary report. The data is hyperlinked, and you can easily pivot from a summary to individual logs and activities provided by SaaS security insights.

Select the Total violations number next to the Bitbucket icon to pivot to SaaS security insights.

On the Security Logs window, review the log data for each violation containing over 30 metadata points of information.

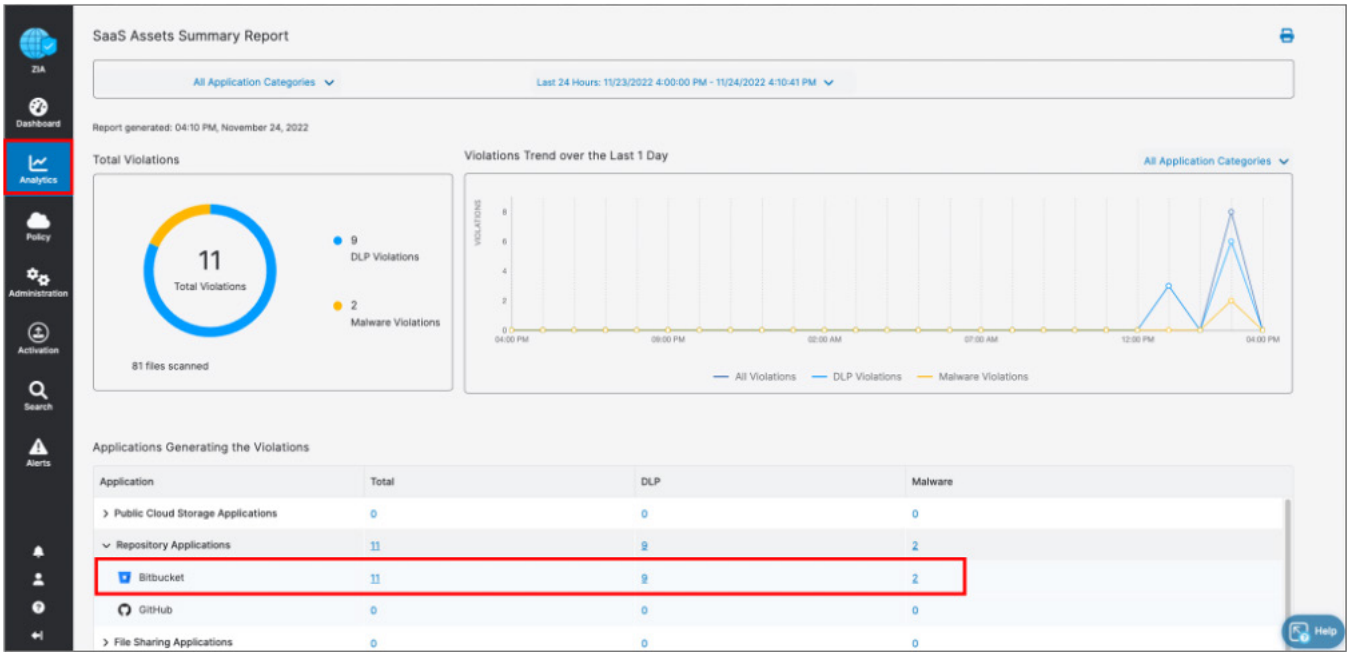

Figure 34. Bitbucket SaaS Assets Summary reports

SaaS Security Insights

The SaaS Security Insights Logs window allows you to select information fields for closer viewing when analyzing files scanned through charts. These logs provide the detail of the policy that found the violation, the threat name, the owner, and over 30 metadata points for identification and threat hunting.

The following are the SaaS Security data types.

- Application
- Application Category
- Department
- DLP Dictionary
- DLP Engine
- Incident Type
- Owner Name
- Severity
- Tenant
- Threat Category
- Threat Super Category
- User

Figure 35. Bitbucket SaaS security insights

Configure the Cloud Browser Isolation Policies for Bitbucket

To move to next steps, launch your ZIA Admin Portal and sign in with administrator credentials:

This configuration focuses on how to isolate Bitbucket applications. However, the process is applicable to any of the Atlassian applications described in this deployment guide.

1. Launch your ZIA Admin Portal.
2. Log in to the ZIA Admin Portal with administrator credentials.

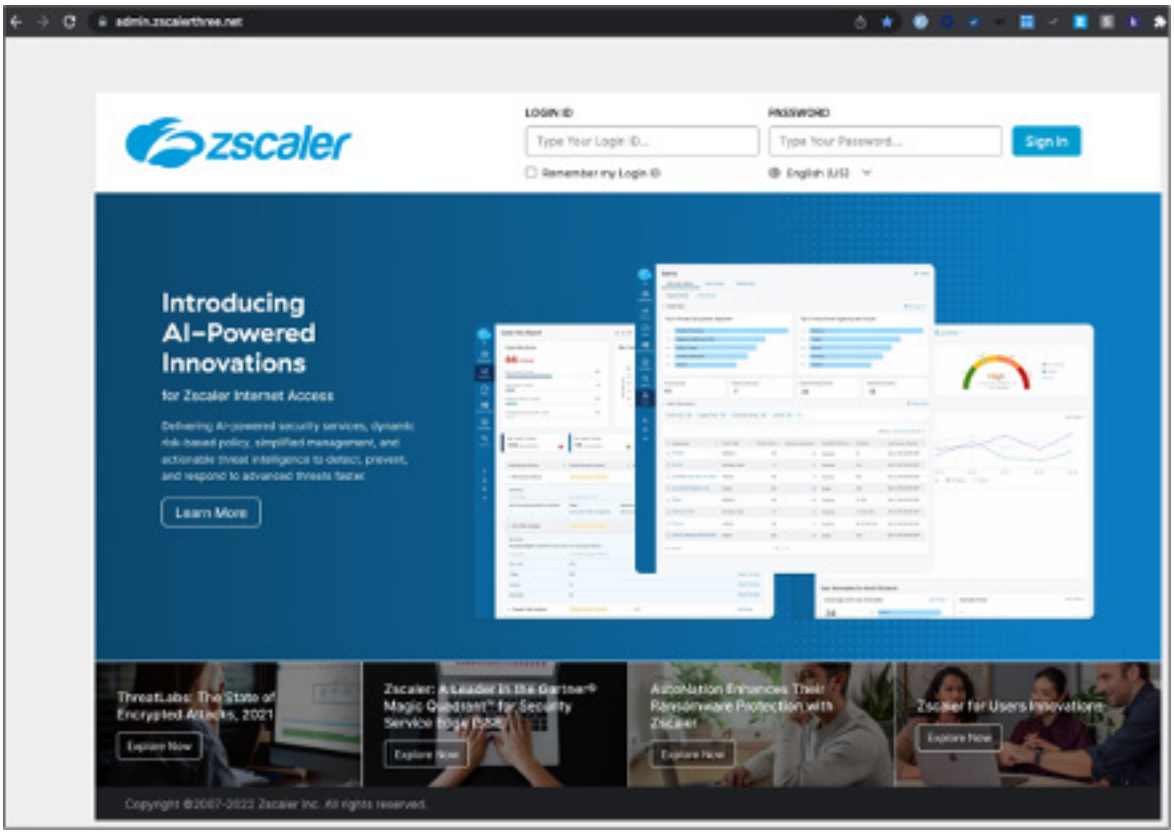

Figure 36. Configure Cloud Browser Isolation

3. To configure policies that redirect Bitbucket traffic to Cloud Browser Isolation, launch the **URL Filtering** wizard:
   a. Go to **Policy** > **URL & Cloud App Control**.
   b. Click **Add URL Filtering Rule**.

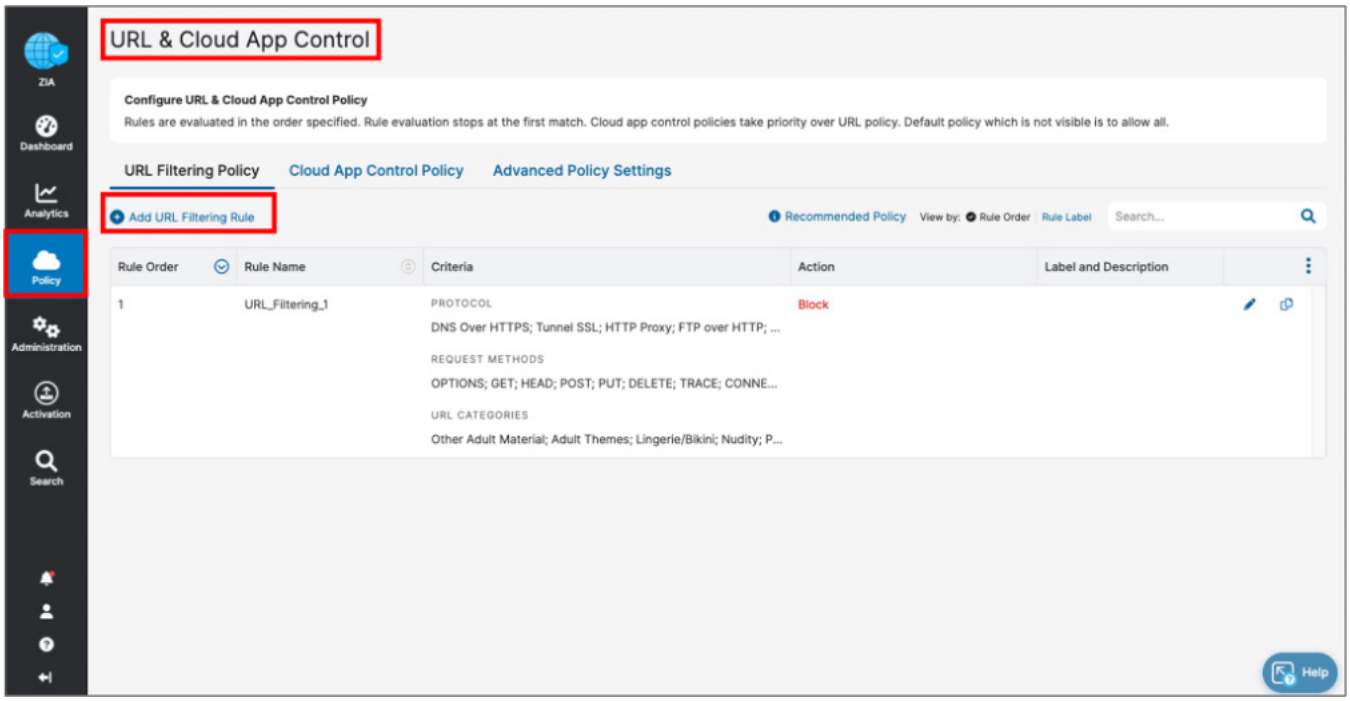

Figure 37. Configure Cloud Browser Isolation policies

4. In the **URL Filtering Rule** wizard:
   a. Select the **Rule Order**.
   b. Name the rule in the **Rule Name** field.
   c. Select **Enabled** in the **Rule Status** field.
   d. Select the drop-down arrow in the **URL Categories** field.
   e. Click the **Add** icon (+) next to the **Search** field on the **URL Selection** dialog.

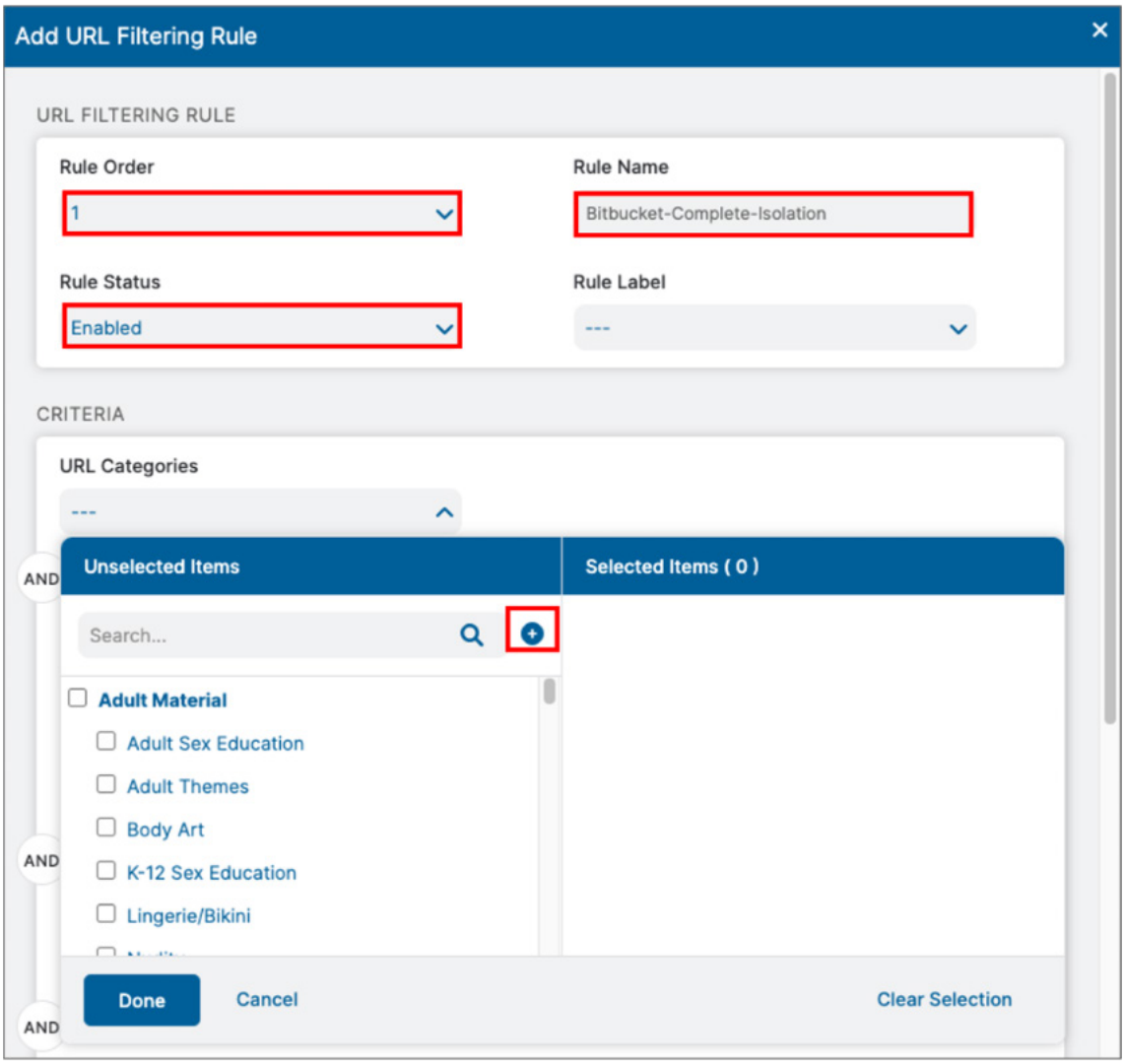

Figure 38. Configure Cloud Browser Isolation policy

5. This displays the **Add URL Category** dialog. You must add Bitbucket as a **Custom URL**:
   a. Name the **URL Category**.
   b. Enter `.bitbucket.org` as the domain in the **Add Items** field and click **Add Items**. Include the period preceding the URL to indicate a wildcard for the domain.
   c. Click **Save**.

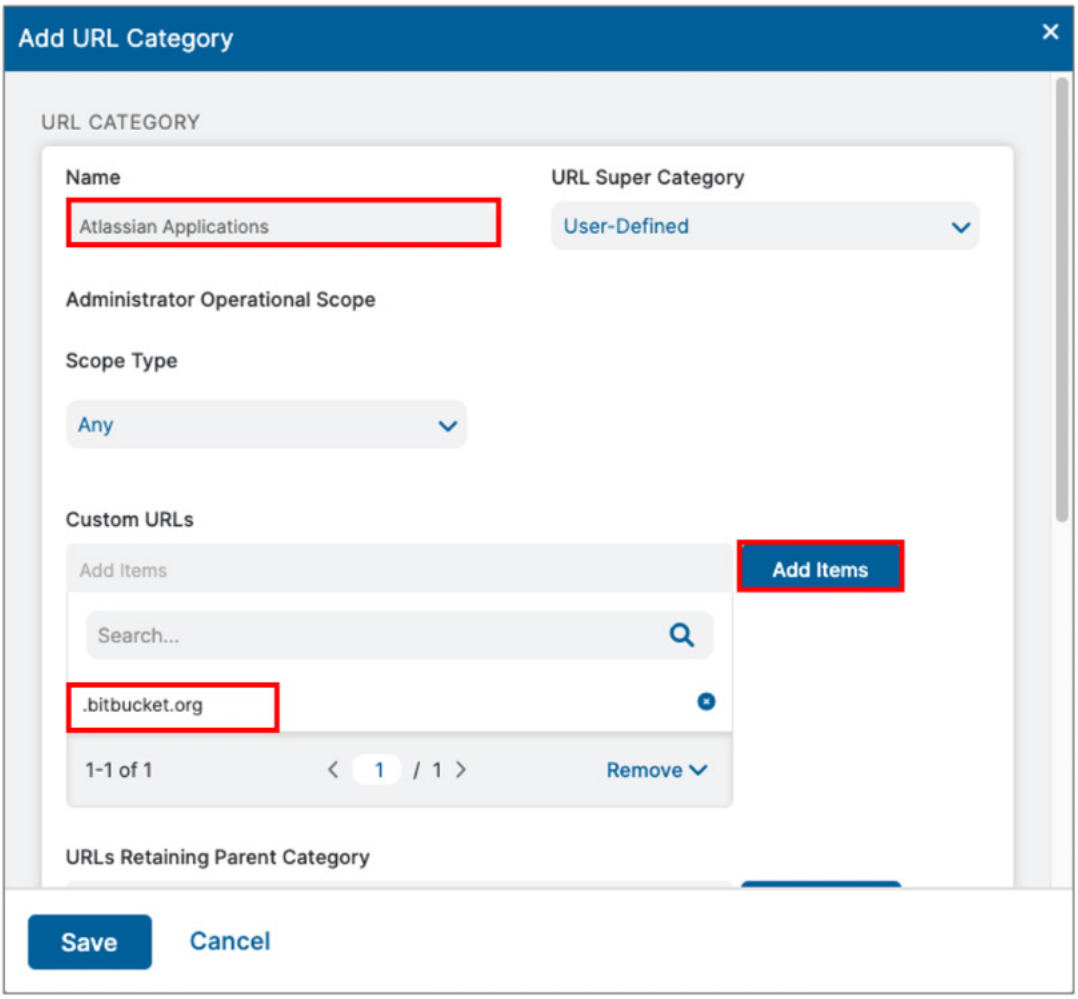

Figure 39. Configure Cloud Browser Isolation

6. Scroll down the dialog to fill in the remaining fields:
    a. For **Request Methods**, select **CONNECT**, **GET**, **HEAD**, and **TRACE**.
    b. For **Protocols**, select **HTTP** and **HTTPS**.
    c. For **User Agent**, select your organization's specific browsers for use with Cloud Browser Isolation.
    d. Click **Save** to complete the configuration.

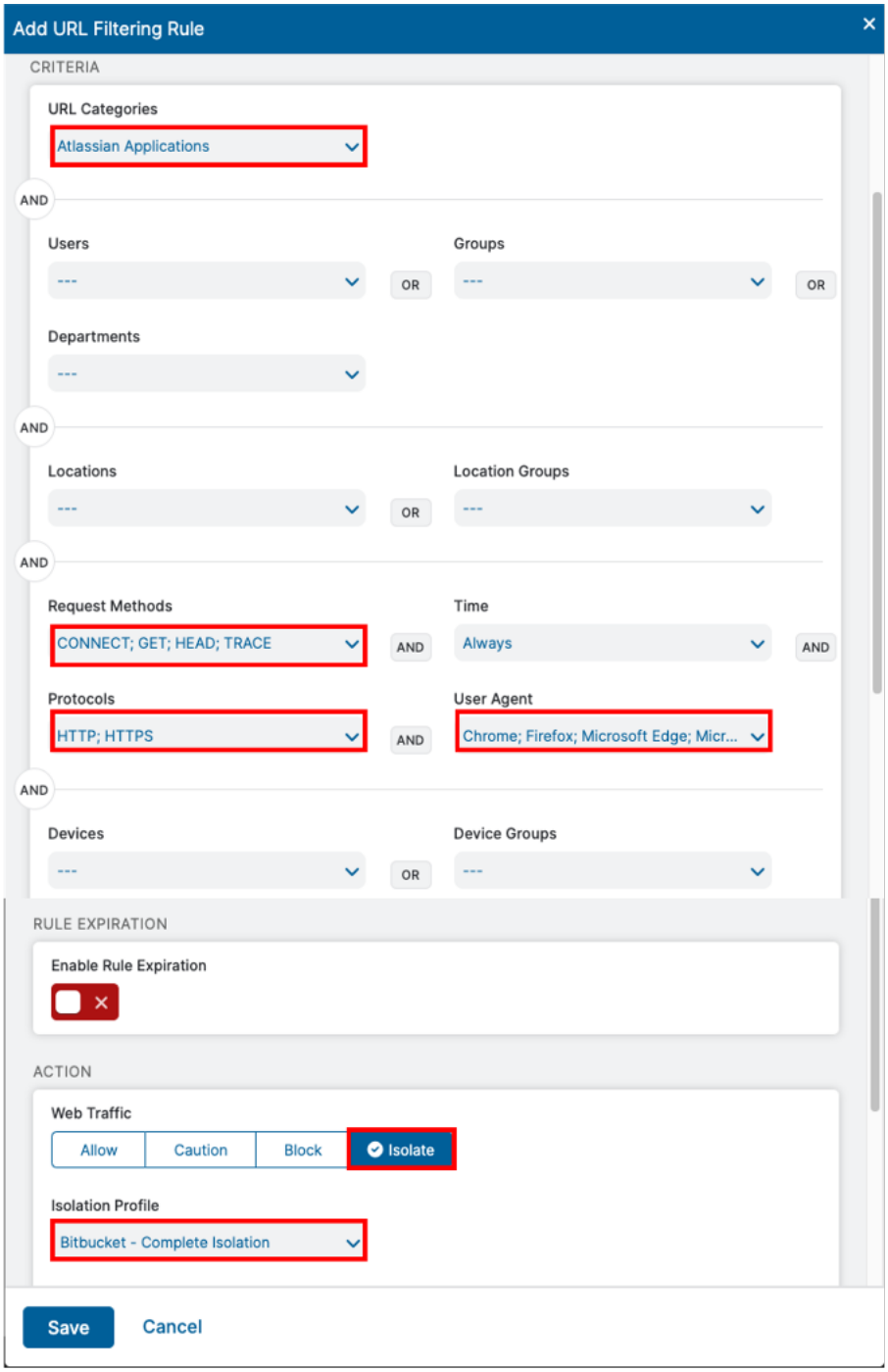

Figure 40. Configure Cloud Browser Isolation

7. Review the completed Cloud Browser Isolation profile.

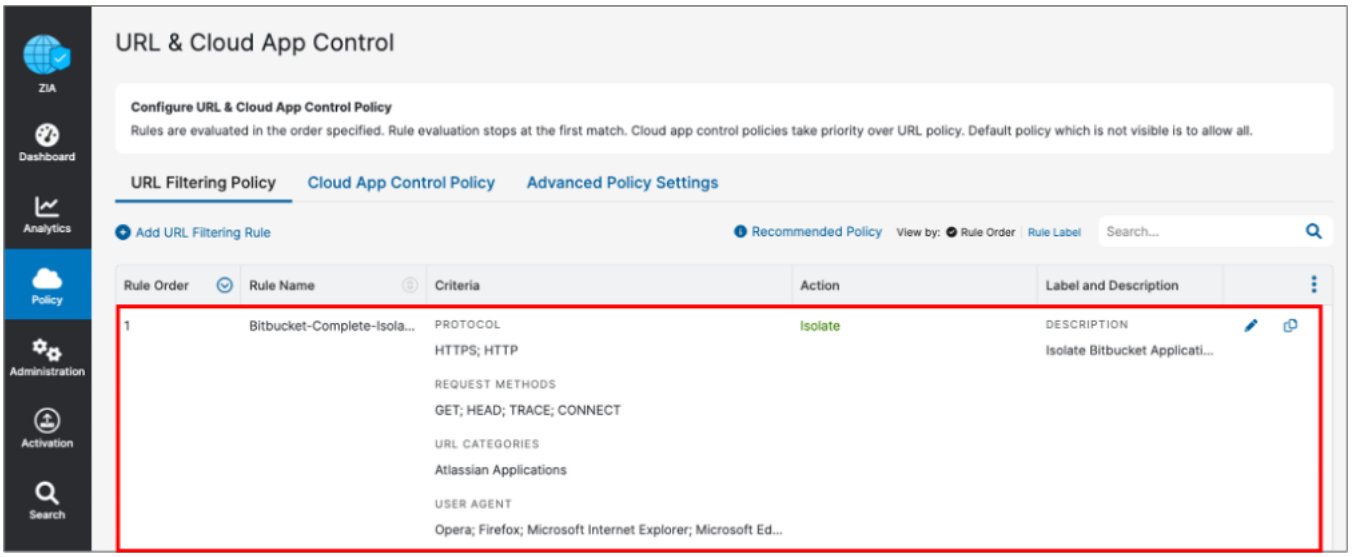

Figure 41. Configure Cloud Browser Isolation

Configure Confluence SaaS Application Tenant

The following sections describe configuring an Atlassian Confluence SaaS application tenant.

Create Confluence Organization API Key

Before starting with the Confluence configuration as a SaaS application tenant in the ZIA Admin Portal, you must create an organization API key.

API keys allow you to manage your organization via the cloud admin REST APIs. You can update organization settings with the Organizations REST API and manage user accounts with the User management REST API.

To create an organization API key:

1. Go to admin.atlassian.com. Select your organization if you have more than one.
2. Click **Settings** > **API Keys**.
3. Click **Create API Key**.

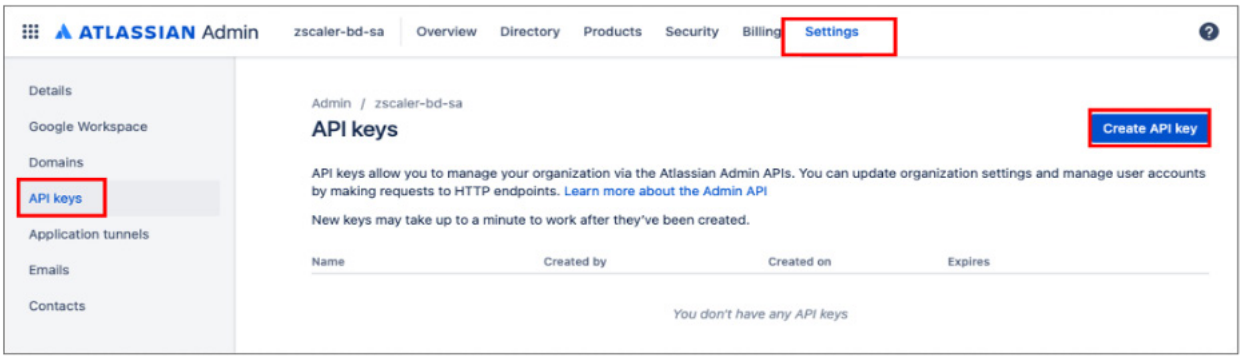

Figure 42. Create organization API key in Atlassian Admin

4. Enter a name to identify the API key.
5. By default, the key expires one week from the current date. If you'd like to change the expiration date, select a new date under **Expires on**.

You're unable to select a date longer than a year from the date of creation.

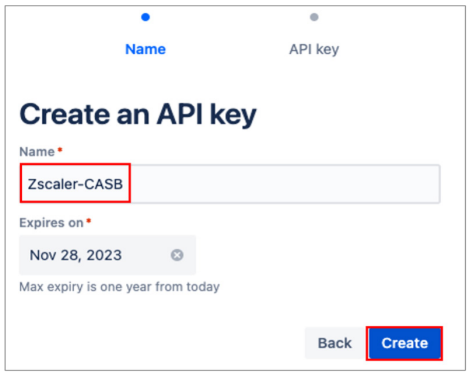

Figure 43. Create organization API key in Atlassian Admin

6. Click **Create** to save the API key.
7. Copy the values for your **Organization ID** and **API key**. These values are required to configure the Confluence SaaS Application Tenant in the ZIA Admin Portal.

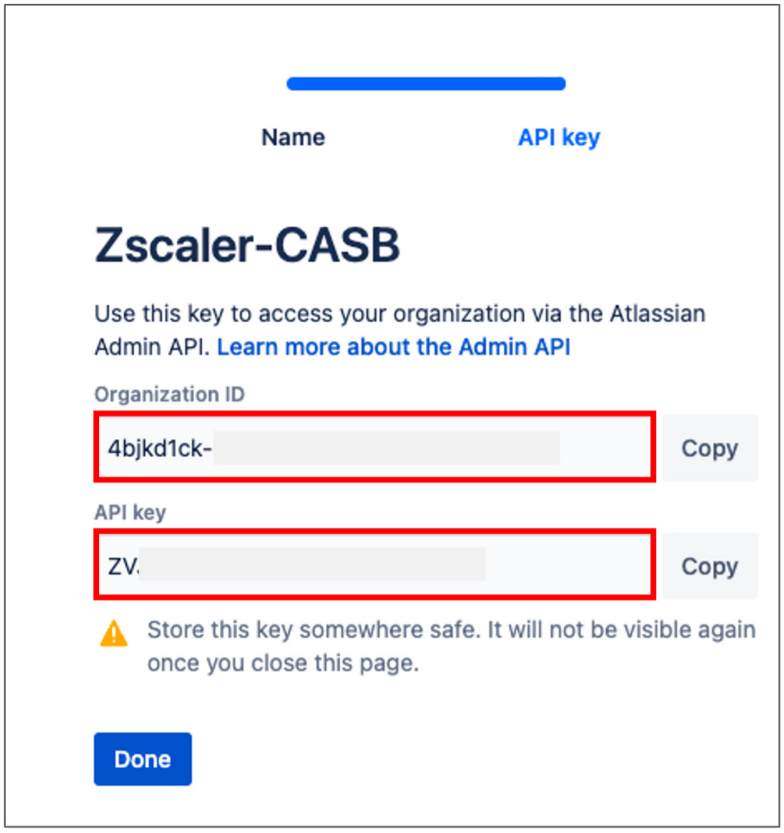

Figure 44. Complete organization API key in Atlassian Admin

Make sure you store these values in a safe place, as they won't be displayed again. Zscaler requires only the API key value.

8. Click **Done**. The key appears in the list of API keys.

Configure Confluence SaaS Application Tenant

To launch the SaaS Application Tenants wizard for the ZIA Admin Portal:

1. Go to **Administration** > **SaaS Application Tenants**.
2. In the **SaaS Application Tenants** window, click **Add SaaS Application Tenant**.

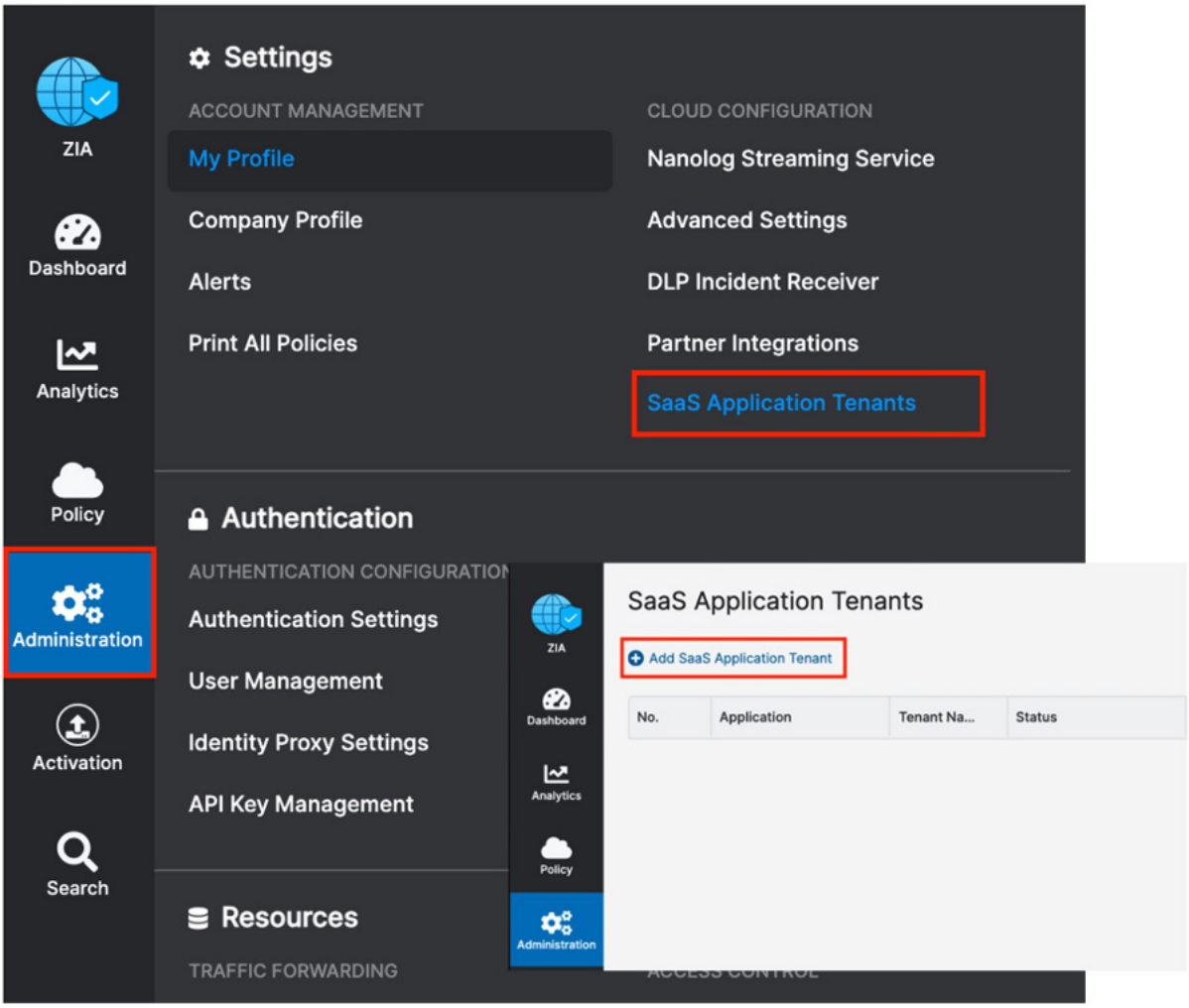

Figure 45. ZIA SaaS application tenant

Confluence SaaS Tenant Configuration Wizard

To start the wizard:

1. Click **Add SaaS Application Tenant** on the tenant page.
2. Select the **Confluence** tile.

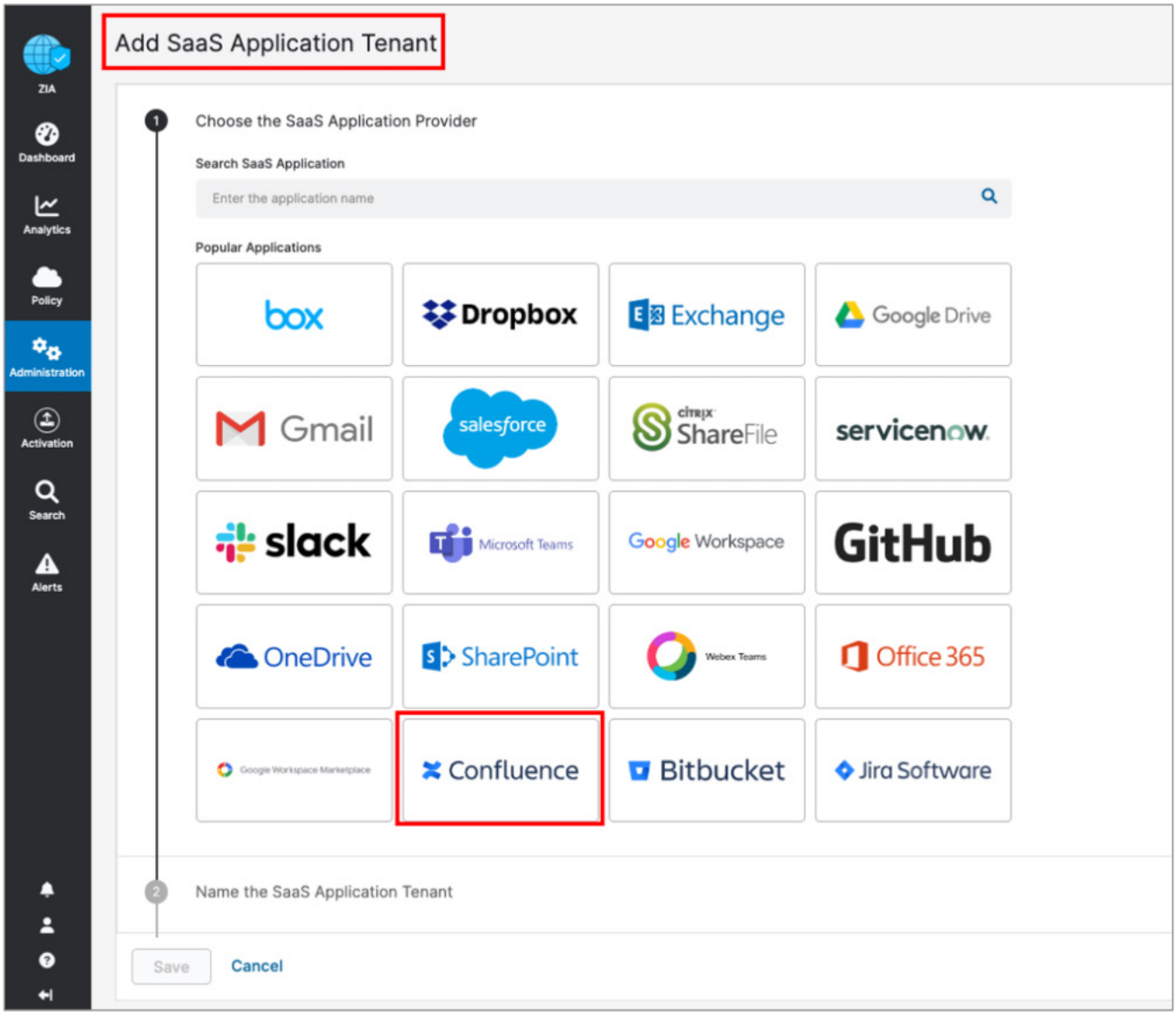

Figure 46. The Confluent SaaS tenant configuration wizard

3. Give the Confluence tenant a name. This is the name you select when assigning a policy for the Zscaler security features:
   a. Enter a name in the **Tenant Name**.
   b. Enter the **Confluence Site Name**.
   c. Enter the **Confluence Organization API Key** created in [Create Confluence Organization API Key](#).

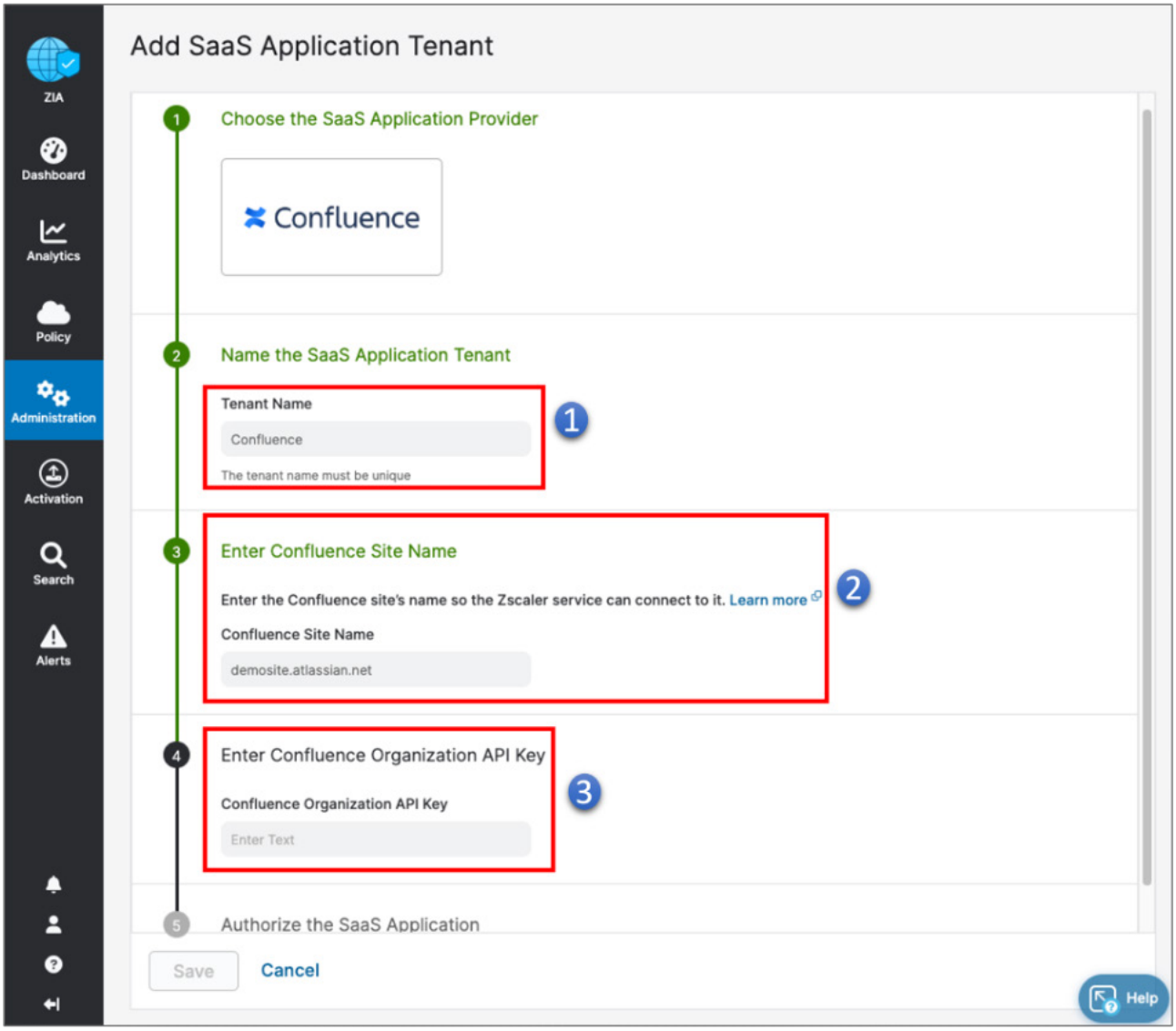

Figure 47. The Confluent SaaS tenant configuration wizard

4. Click **Provider Admin Credentials**, which redirects you to the Confluence login page.

Figure 48. Authenticate with your Confluence administrator credentials

5. Authenticate with your Jira administrator credentials.

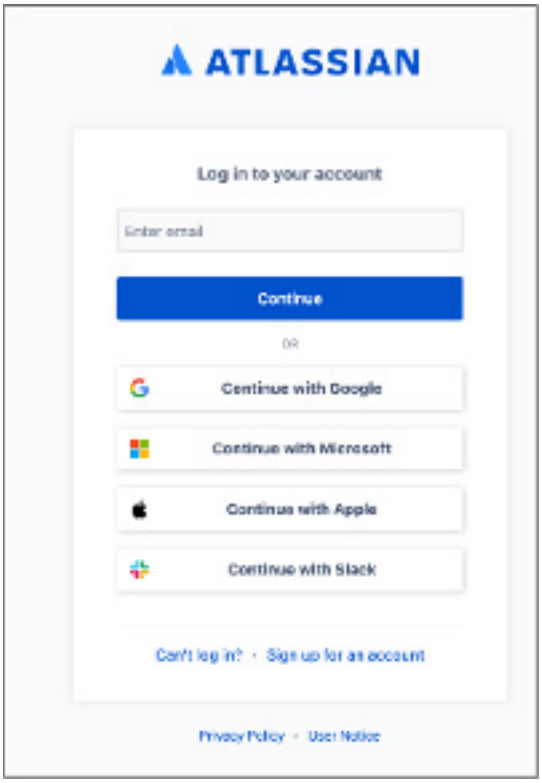

Figure 49. Authenticate to the Confluence tenant

6. Give permission to Zscaler SaaS Connector by clicking **Accept**.

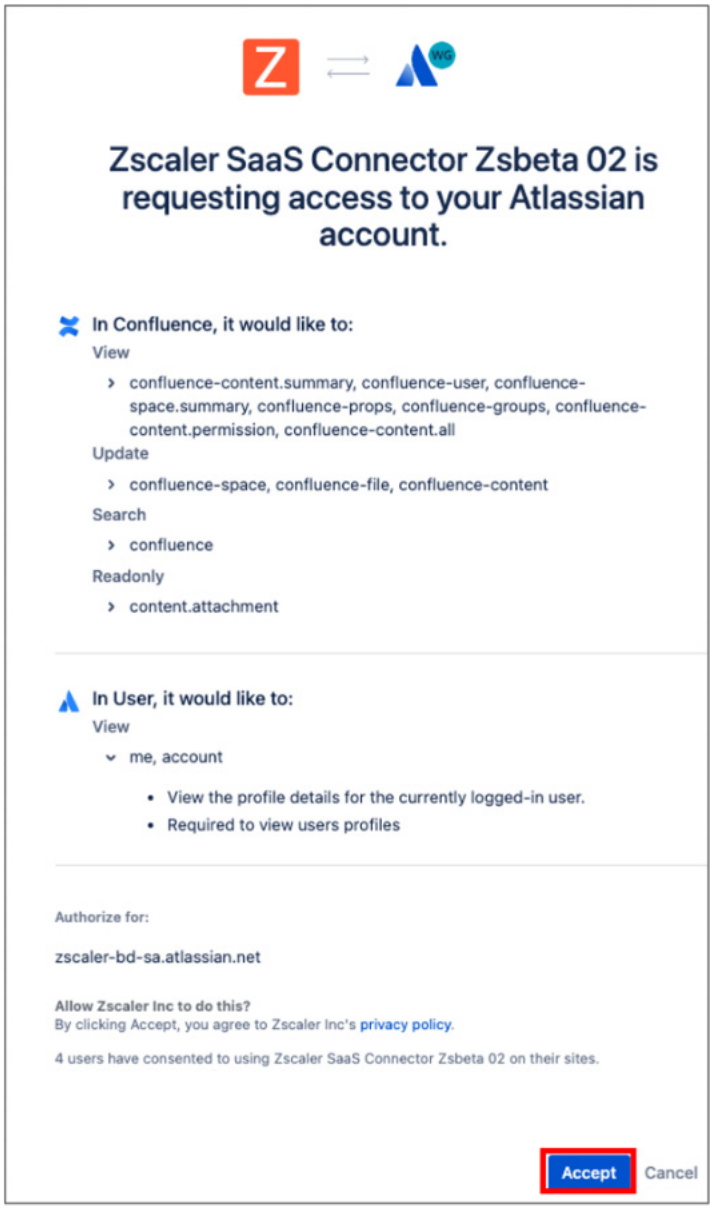

Figure 50. Grant access to Zscaler SaaS Connector in Atlassian Admin

7. Click **Save**.

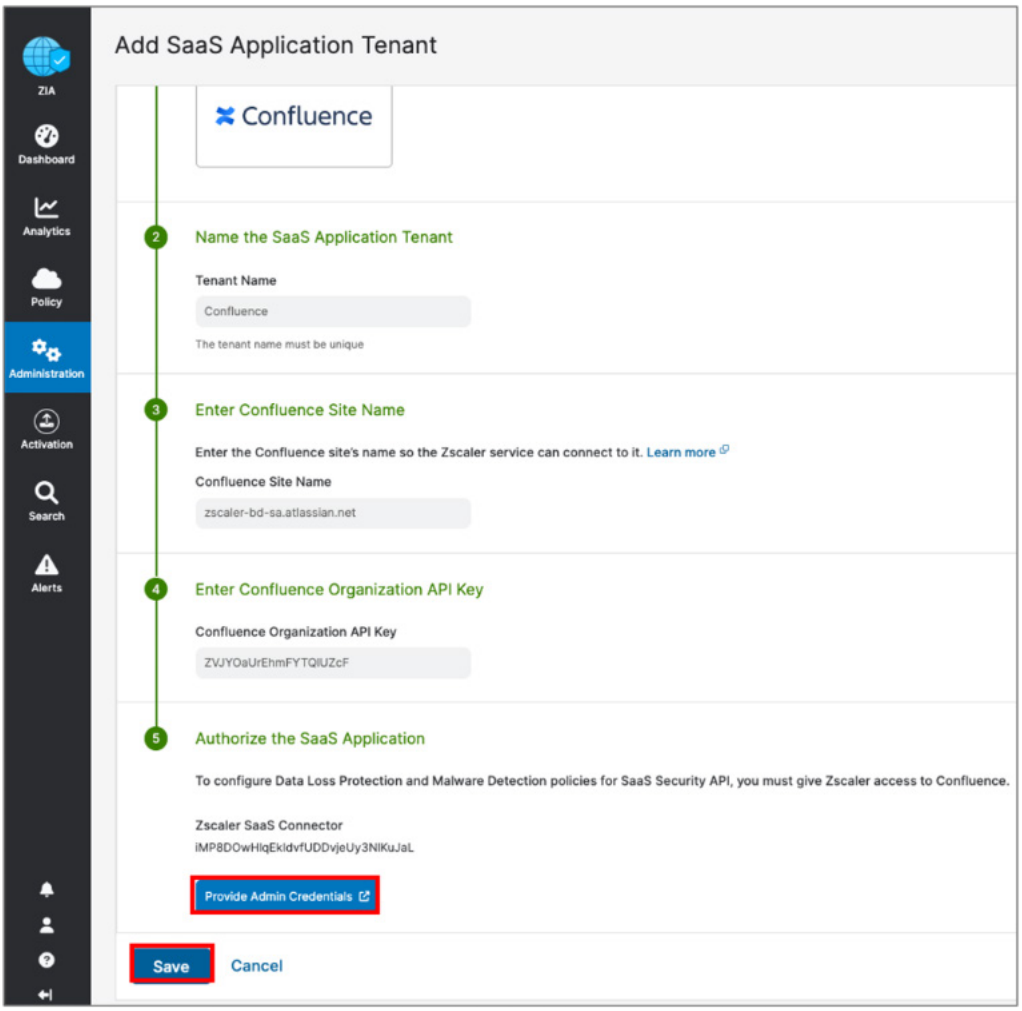

Figure 51. Save Zscaler SaaS Connector configuration

The completed and active Confluence API connector is displayed.

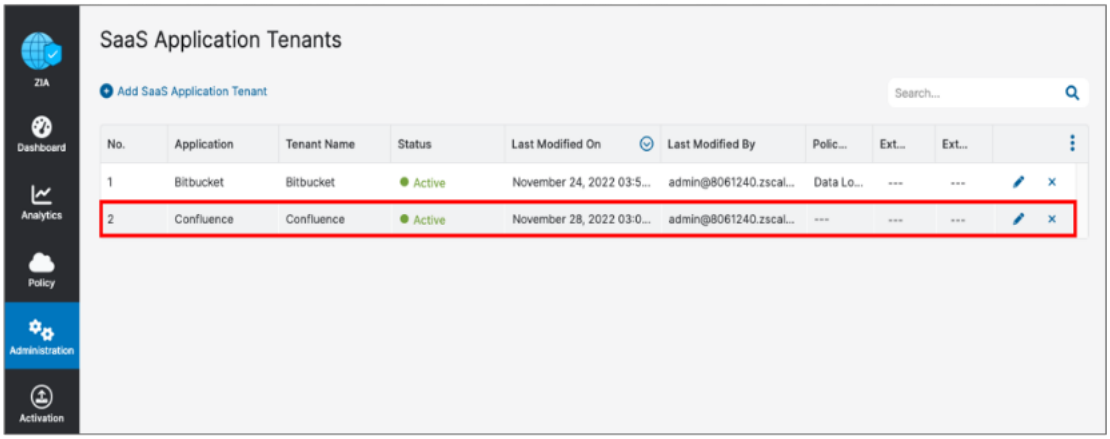

Figure 52. SaaS Application Tenant

Configure Confluence Policies and Scan Configuration

After adding and configuring the Confluence tenant, you must configure the SaaS Security API to control DLP and malware policies, and then scan the configuration for the policies. You can also view reports and data for Confluence in analytics, SaaS security insights, and logs.

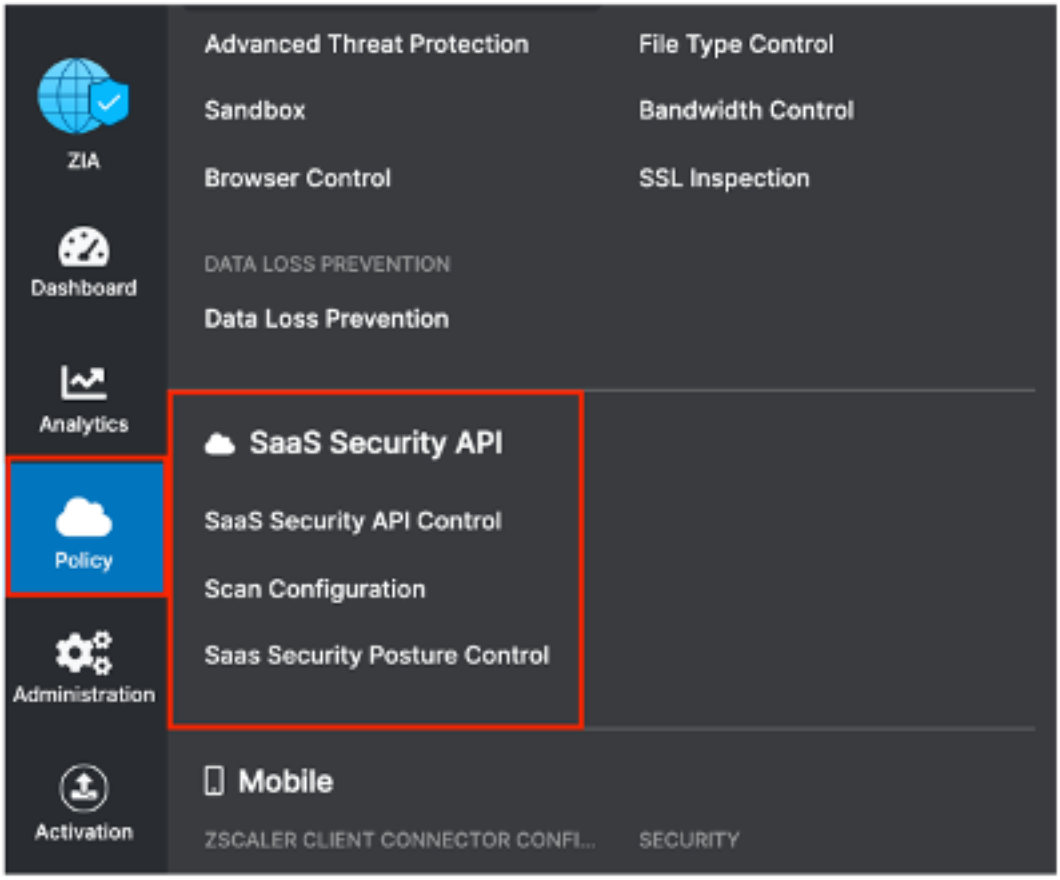

Figure 53. Configure and Scan Configuration in the ZIA Admin Portal

Scoping the Policies and Remediation

This deployment guide configures a basic DLP policy and a malware policy. Zscaler SaaS security out-of-band data protection capabilities look inside the SaaS applications themselves through API integrations to identify accidental or intentional data exposure and compliance violations that otherwise would go unnoticed.

For Confluence, the Zscaler SaaS Security API DLP rule scans all the blogs, pages, and attachments within a space. The DLP rule does not scan the overview page for any space.

The DLP policy broadly identifies a spreadsheet with a list of US Social Security numbers, and the policy is only used for demonstration purposes. A true DLP policy review minimizes false positives and false negatives.

SaaS DLP protection is only part of the Zscaler DLP solution and scans data-at-rest (like the Confluence files). This deployment doesn't cover in-line data protection, exact data match, or indexed document matching (document template fingerprinting), although they are integral pieces of a complete data protection solution.

For next steps to test the DLP SaaS functionality, create a basic policy and apply it to the Confluence tenant. If you already have DLP policies created, skip ahead to Configure a SaaS Malware Policy for Confluence.

Creating a DLP Policy

To create a DLP policy, you must:

- Create a custom dictionary (or use the available dictionaries) to identify the data the scan is going to look for.
- Create an engine that is the logical template for adding expressions and additional data. This is where you would specify Social Security numbers and any other criteria for the policy. The engine provides the means to precisely add or remove data to match violations and eliminate false positives.
- Create a SaaS security DLP policy that allows you to specify the details about where, when, the action taken, and whom to inform about violations.

Notice that you can create a custom DLP dictionary that contains your own patterns and phrases, or use one of the predefined dictionaries. This deployment guide focuses on predefined dictionaries.

Creating a DLP Engine

To create a DLP engine, from the ZIA Admin Portal:

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. Click the **DLP Engines** tab, then click **Add DLP Engine**.

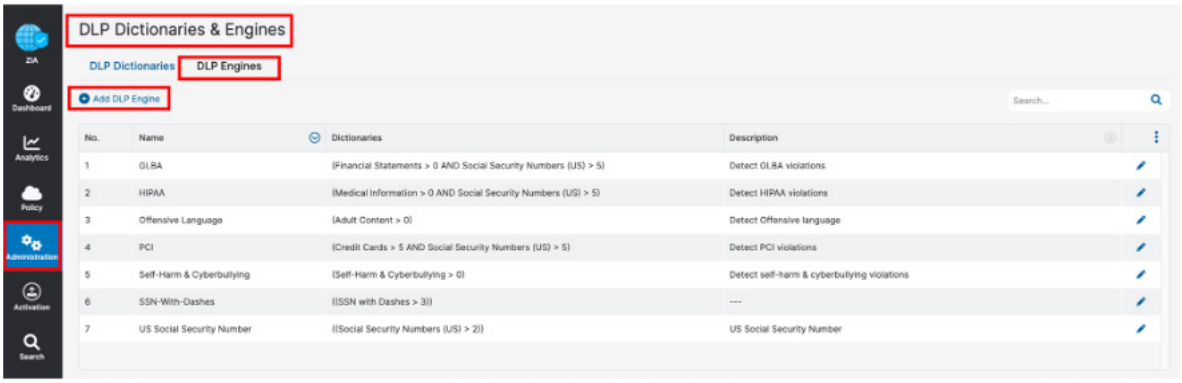

Figure 54. Creating a DLP engine

3. Give the DLP engine a **Name**.
4. In the **Engine Builder** under **Expression**, select the desired dictionary. In the following example, **Social Security Numbers (US)** is selected.
5. Specify the **Match Count**, which is the minimum number of instances the data must occur in the file.
6. (Optional) Click **Add** to add the next dictionary and repeat the process of naming and defining the dictionary.
7. Click **Save**, then **Activate** the configuration.

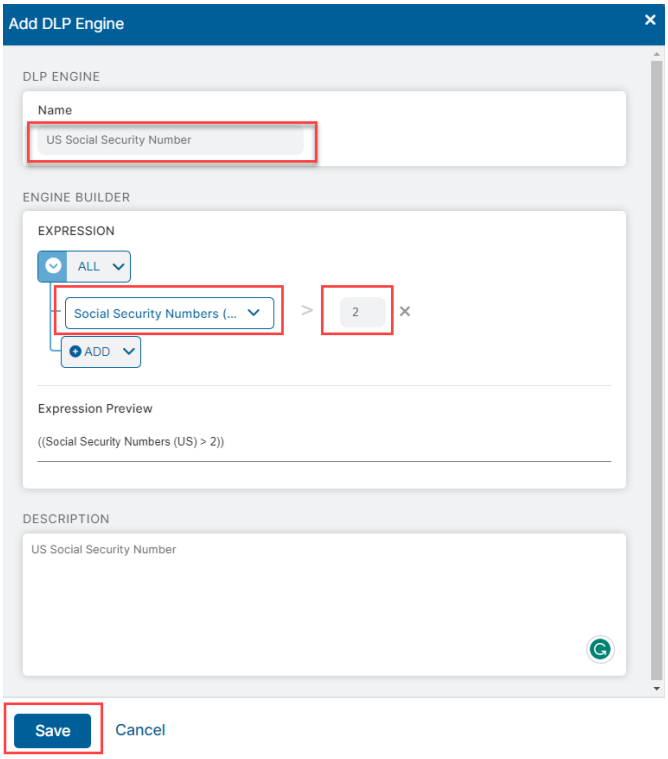

Figure 55. The DLP engine wizard

This policy triggers when you see the third Social Security number. Again, this is a demonstration and the criteria is too general to be a production DLP rule.

Configure a SaaS DLP Policy for Confluence

Apply the engine to a DLP policy used for the Confluence instance. Launch the Add DLP Rule wizard to start the process:

1. Go to **Policy** > **SaaS Security API Control** > **Data Loss Prevention**.
2. Select **File Sharing**.
3. Click **Add DLP Rule**.
4. Select **Confluence** as the **SaaS Application Tenant**.
5. Select the **DLP Engine** created in [Confluence SaaS Tenant Configuration Wizard](#).
6. Select **Any-Any** for the **Collaboration Scope**.
7. Select **Report Incident Only** as the **Action**.
8. Select **High** as **Severity** to allow for identification, searches, and tracking.
9. Click **Save** and then **Activate** your configuration.

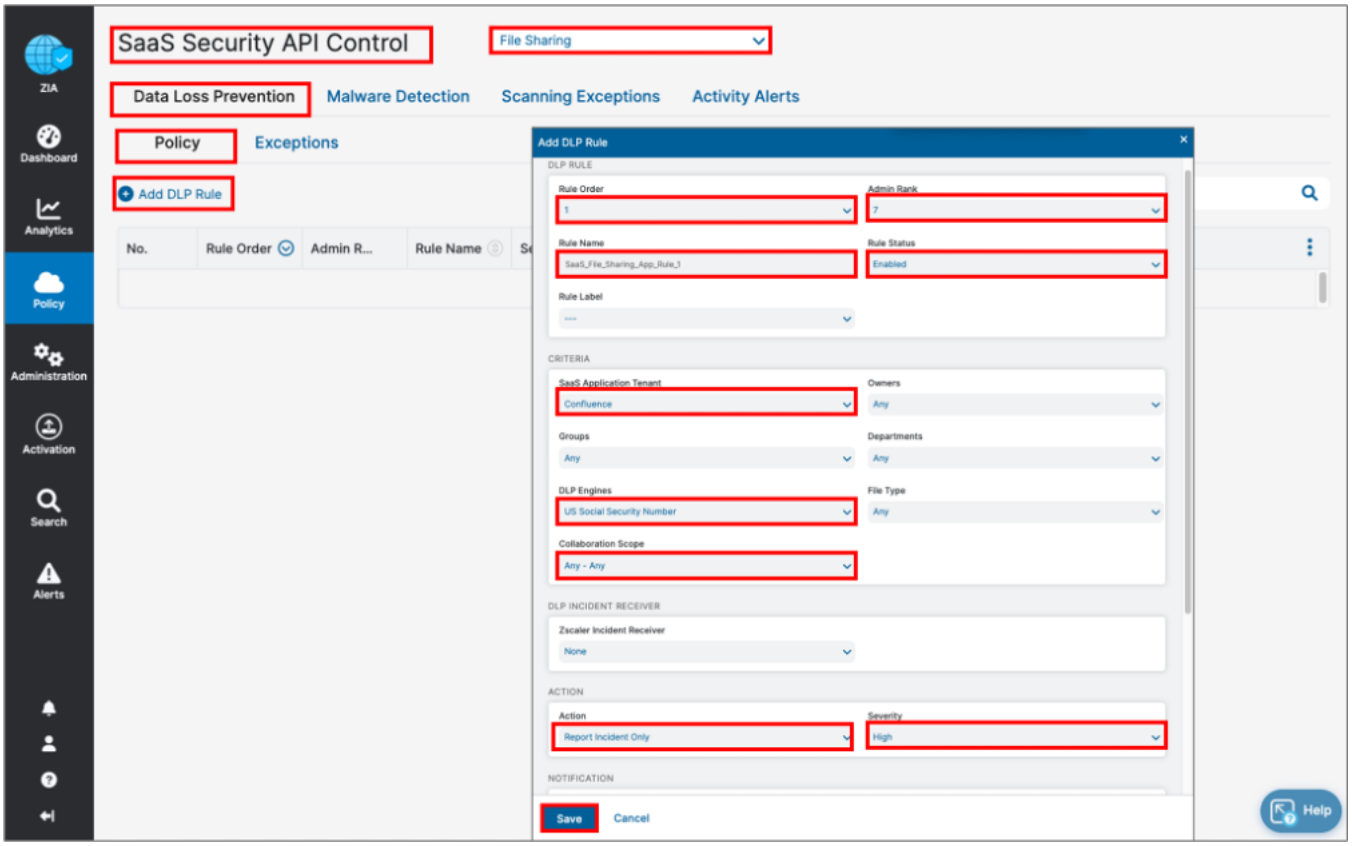

Figure 56. Launch the SaaS DLP Policy Configuration wizard

Apply a scanning schedule to the Confluence DLP rule.

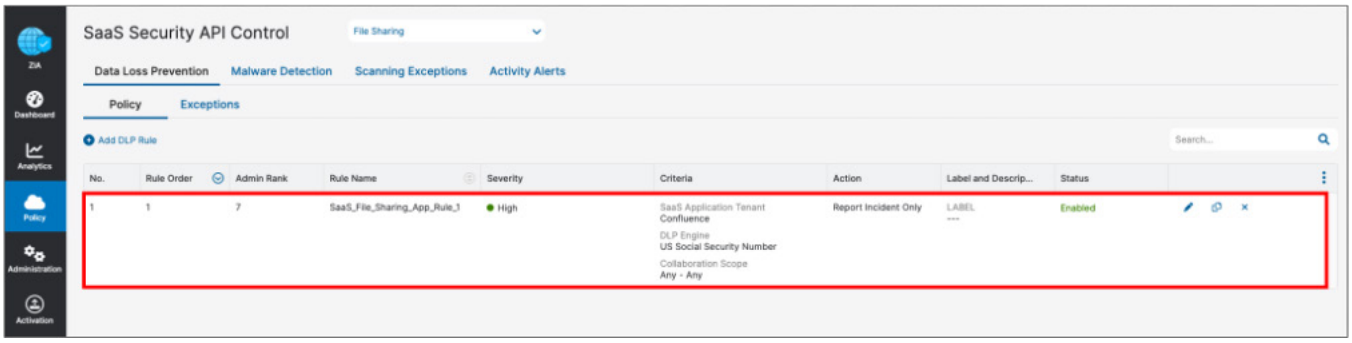

Figure 57. The configured DLP policy

SaaS DLP Policy Details

The SaaS DLP policy specifies the details for whom and for what data this policy applies. You specify the rule order if you have multiple DLP policies, which are processed in an ascending manner. The first rule that matches is the applied rule. Specify the DLP engine you defined, any file owners, groups or departments, and the file types to inspect. The collaboration scope and the action are unique to the SaaS DLP.

Select a collaboration and an action to remove sharing.

The Collaboration Scope includes the collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select Any to apply the rule to files with all collaboration levels, or select one or more of the following collaboration scopes and specify the permissions for each scope:

- External Collaborators: Files that are shared with specific collaborators outside of your organization.
- External Link: Files with shareable links that allow anyone outside your organization to find the files and have access.
- Internal Collaborators: Files that are shared with specific collaborators or are discoverable within your organization.
- Internal Link: Files with shareable links that allow anyone within your organization to find the files and have access.
- Private: Files that are only accessible to the owner.
- The Action: The rule acts after detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant. For Confluence, the actions are:
    - Move to Restricted Folder
    - Remove
    - Report Incident Only
- Report Incident Only: The rule reports the incident only and makes no changes to the file's collaboration scope.

Configure a SaaS Malware Policy for Confluence

To launch the Malware Detection Rule wizard:

1. Go to **Policy** > **SaaS Security API Control** > **Malware Detection**.
2. Click **File Sharing**.
3. Click **Add Malware Detection Rule**.

The SaaS Security API Malware Detection policy is an all-encompassing policy and all files in the tenant are scanned unless you remove the tenant from the scope by specifying exemptions on the Exceptions tab that is located under Malware Detection. To add a malware policy, specify the application, the SaaS tenant, and the status.

The actions available for Confluence are: "Quarantine Malware," "Remove Malware," "Report Malware."

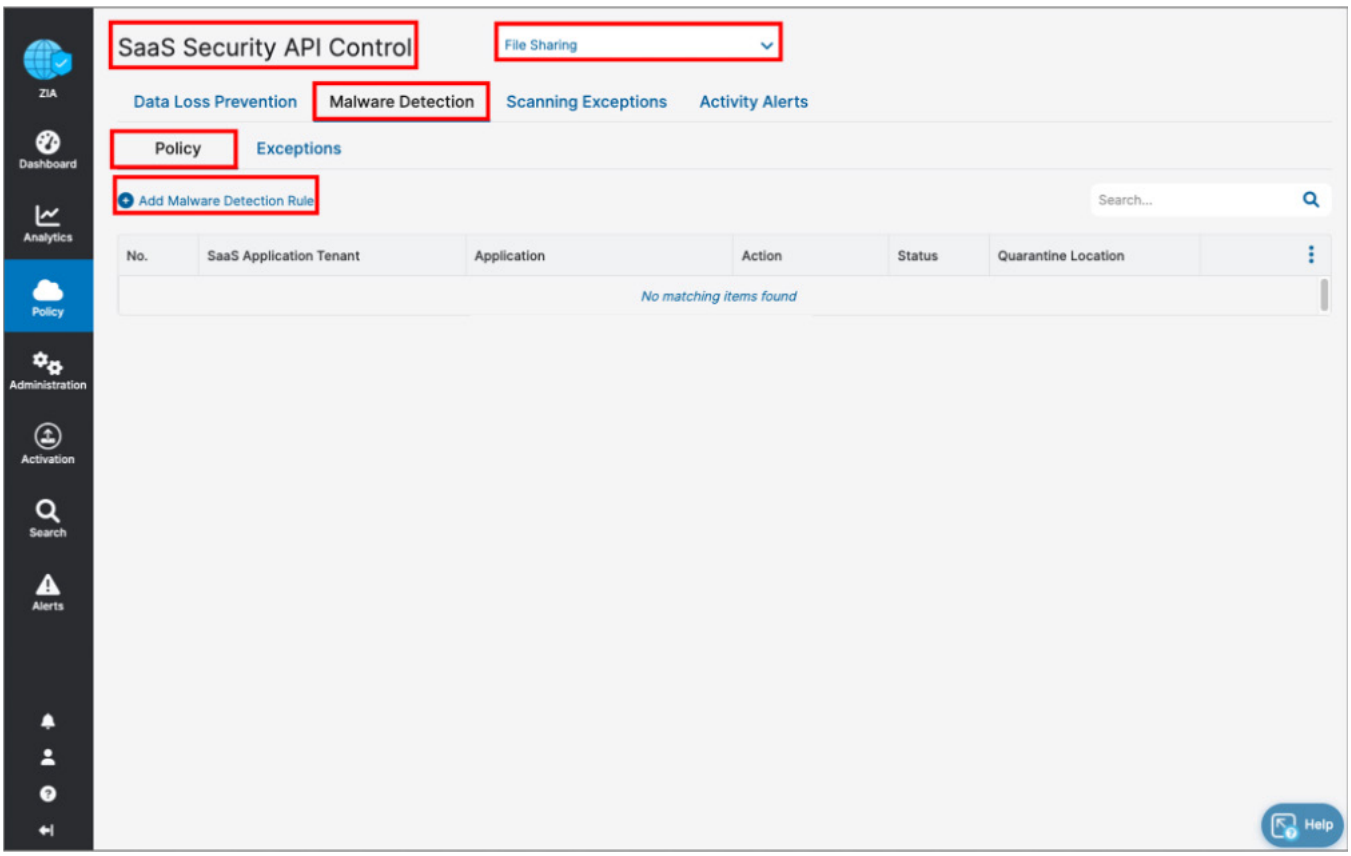

Figure 58. Launch the Malware Policy Configuration wizard

Confluence SaaS Malware Policy Wizard

Configure the Malware Detection Rule wizard:

1. Go to **Policy** > **SaaS Security API Control** > **Malware Detection**.
2. Select **File Sharing**.
3. Click **Add Malware Detection Rule**.
4. Under **Application**, select **Confluence** as the application.
5. Select **Confluence** as the **SaaS Application Tenant** to apply the policy.
6. Select **Enabled** for **Status**.
7. Select the desired **Action**. In the following example, **Report Malware** is selected.
8. Click **Save**.

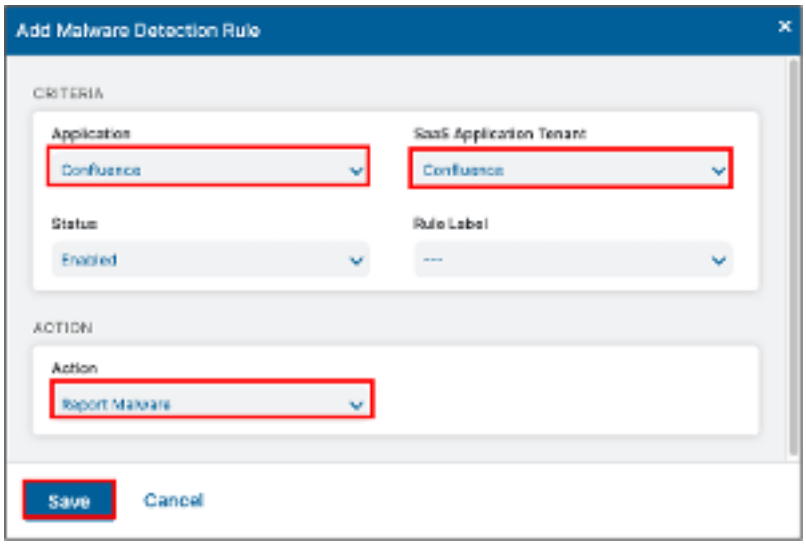

Figure 59. The Malware Policy Configuration wizard

Confluence SaaS Malware Policy

Apply the completed SaaS Security API Malware Detection policy for the Confluence SaaS tenant to the Confluence instance with a scanning schedule. Activate your configuration.

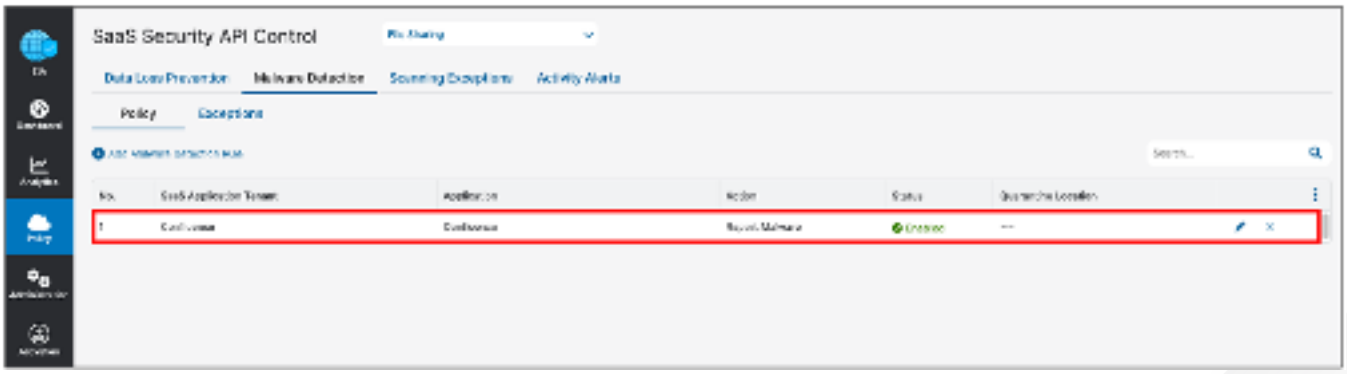

Figure 60. The complete Confluence Malware Policy Configuration wizard

Configure a Scan Schedule Configuration for Confluence

The final step is to create a Scan Configuration. Specify the tenant that the Scan Configuration applies to, any policies that are to be included in the scan, and the data to scan relative to a date. The options for Data to Scan are: All Data, Date Created or Modified After, or New Data Only. For this deployment guide, select All Data.

However, if this is a Proof of Value (POV) or a Trial, the only option available is New Data Only.

To add a Scan Schedule:

1. Select **Policy** > **SaaS Security API** > **Scan Configuration** > **Add Scan Schedule**.
2. Select **Confluence** as the **SaaS Application Tenant**.
3. In the **Policy** field, select **Data Loss Prevention** policy and the **Malware** policy created in prior procedures.
4. Select **All Data**. (Or, for a POV or Trial, select **New Data Only**.)
5. Click **Save**, and then **Activate** the configuration.

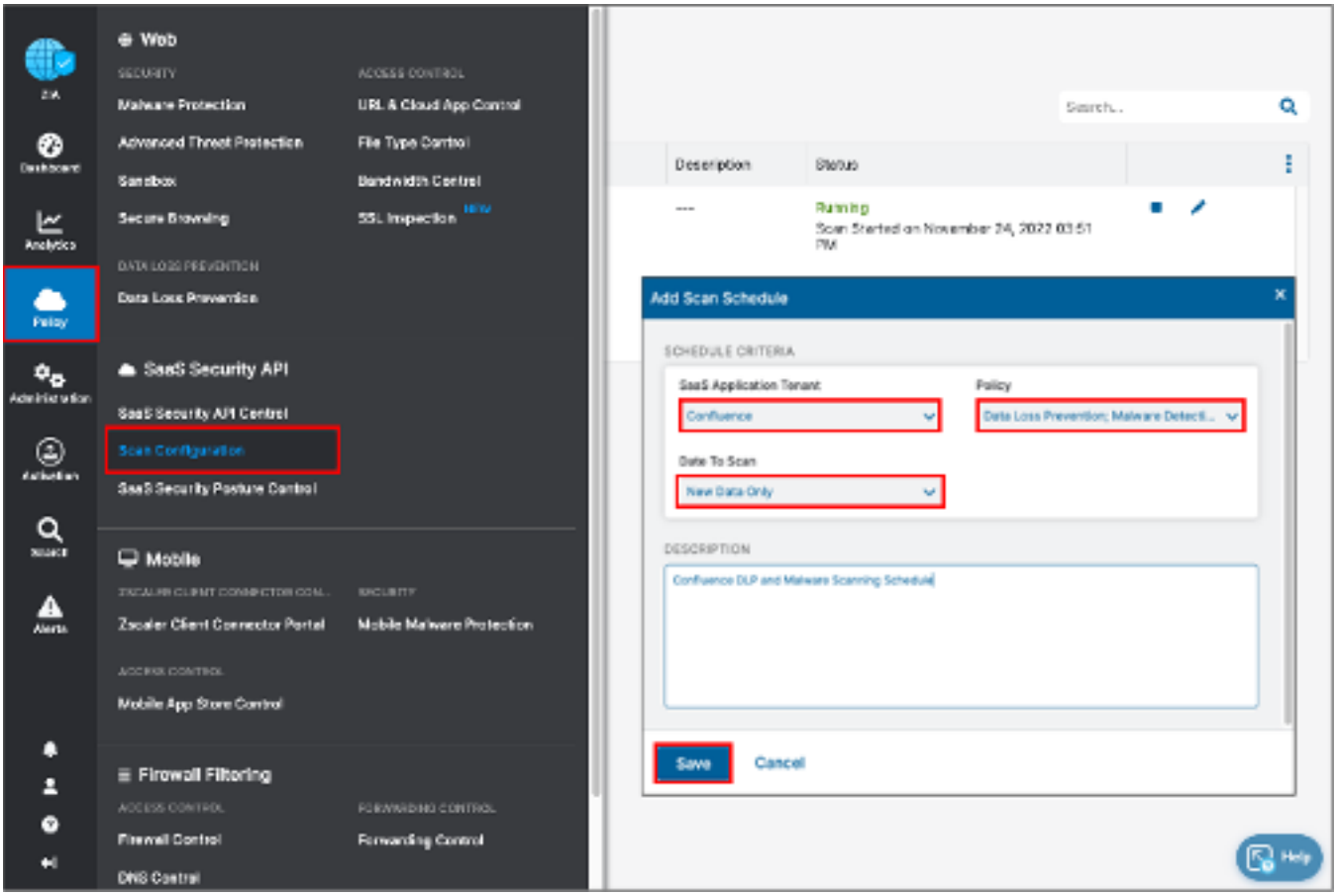

Figure 61. Create and enable a scan for the Confluence SaaS tenant

Start the Scan Schedule for Confluence

After the schedule is configured and saved, start the scan for the applied DLP and malware policies.

1. Click the **Start** icon on the **Scan Configuration** window to start the SaaS Security API on the Confluence tenant. When the scan is running, the icon changes from a run to a stop symbol.
2. Review the **Status** column and ensure it is **Running** with a start date and a latest scan date.

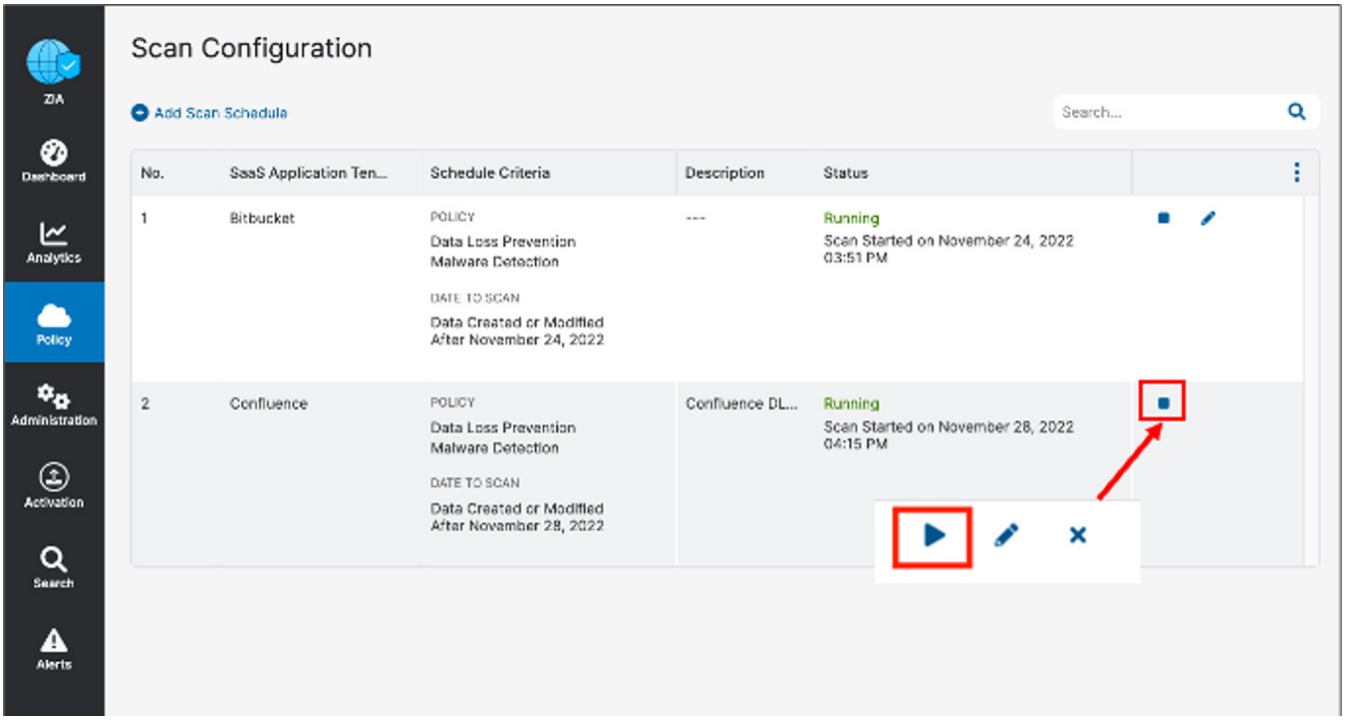

Figure 62. Starting the Confluence Scan Schedule

Confluence Reporting and Visibility

Zscaler analytics provide detailed reporting of all user activity down to each session created by the user when visiting a destination. Zscaler extends that visibility to include reporting of activity, malware incidents, and DLP violations of data at-rest associated with the user. Zscaler has reports and SaaS security insights, which provide visibility from a high-level overview to management of the individual logs and violations.

To learn more, see SaaS Security Insights.

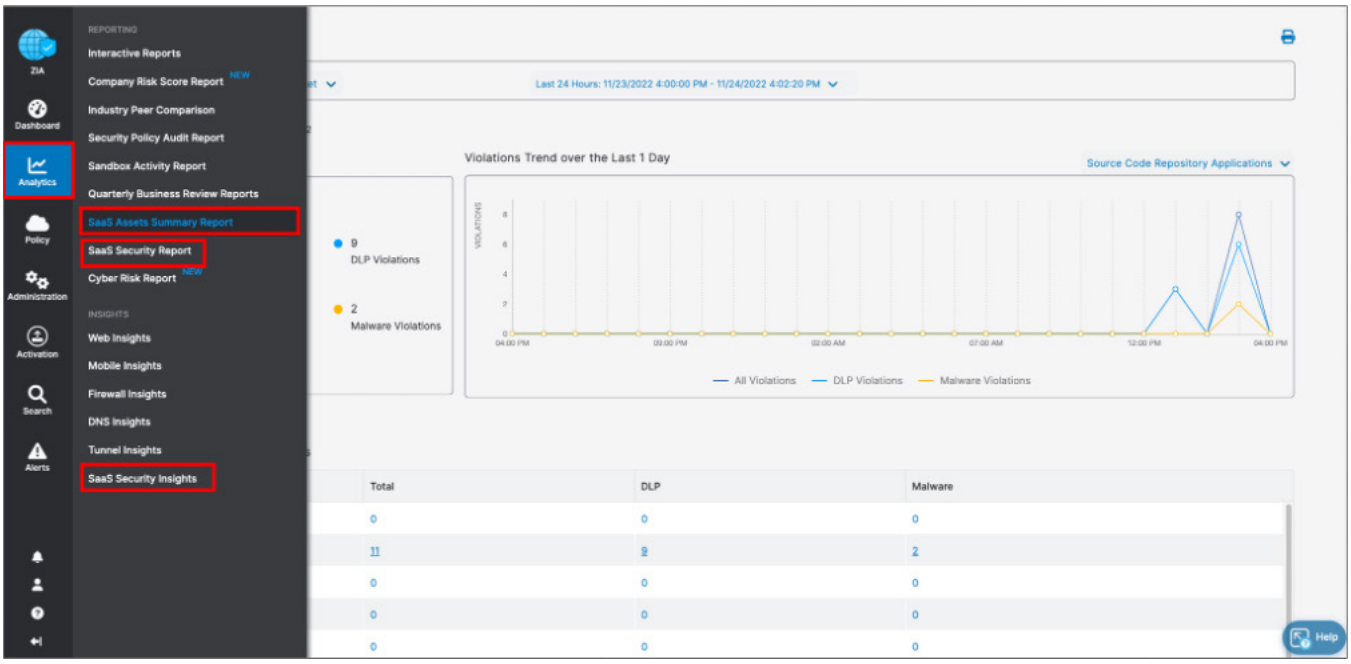

Figure 63. SaaS security visibility

SaaS Assets Summary Report

A SaaS Assets Summary Report provides all activity and violations at a quick glance. The report identifies all SaaS tenant information from a single page. Although the Confluence activity over the creation of this deployment guide is shown, any configured tenant is displayed on this summary report. The data is hyperlinked, allowing you to pivot from a summary to individual logs and activities provided by SaaS security insights.

1. Select the **Total** violations number next to the **Confluence** application to pivot to SaaS security insights.
2. On the **Security Logs** window, review the log data for each violation containing over 30 metadata points of information.

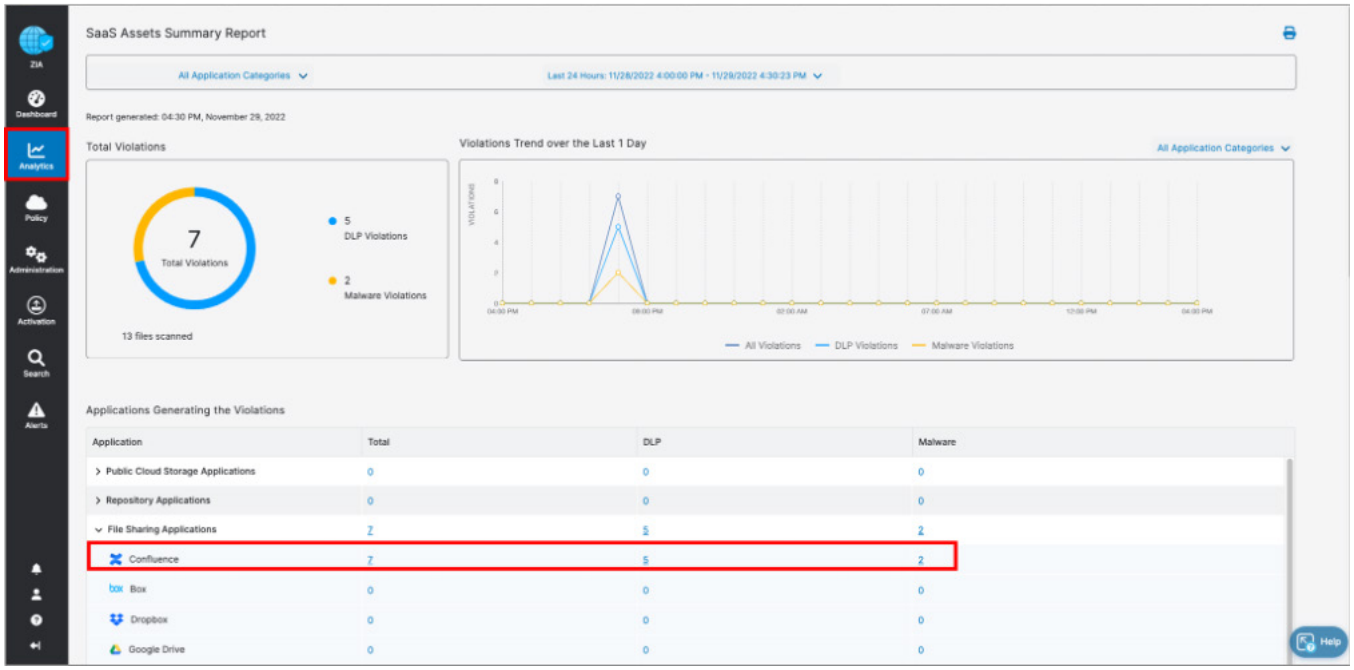

Figure 64. Confluence SaaS Assets Summary reports

SaaS Security Insights

The SaaS Security Insights Logs window allows you to select information fields for closer viewing when analyzing files scanned through charts. These logs provide the detail of the policy that found the violation, the threat name, the owner, and over 30 metadata points for identification and threat hunting.

The following are the SaaS Security data types.

- Application
- Application Category
- Department
- DLP Dictionary
- DLP Engine
- Incident Type
- Owner Name
- Severity
- Tenant
- Threat Category
- Threat Super Category
- User

Figure 65. Confluence SaaS security insight

Configure Jira SaaS Application Tenant

The following sections detail how to configure a Zscaler SaaS application tenant for Jira.

Create Jira Organization API Key

Before starting with the Jira configuration as a SaaS application tenant in the ZIA Admin Portal, you must create an organization API key.

API keys allow you to manage your organization via the cloud admin REST APIs. You can update organization settings with the Organizations REST API and manage user accounts with the User management REST API.

To create an organization API key:

1. Go to the Atlassian login portal.
2. Select your organization if you have more than one.
3. Click **Settings** > **API keys**.
4. Click **Create API Key**.

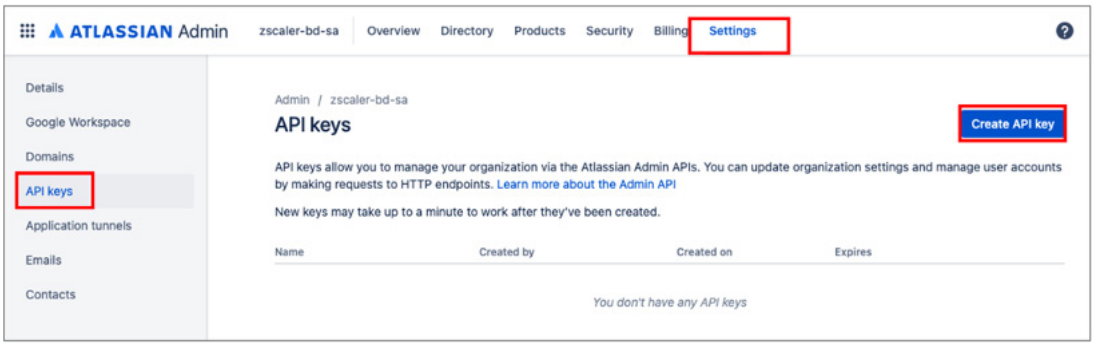

Figure 66. Create organization API key in Atlassian Admin

5. Enter a name to identify the **API key**.
6. By default, the key expires one week from the current date. If you want to change the expiration date, select a new date under **Expires on**.

You're unable to select a date longer than a year from the date of creation.

7. Select **Create** to save the API key.

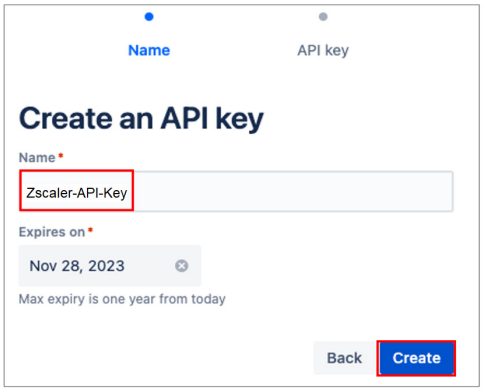

Figure 67. Create organization API key

8. Copy the values for your **Organization ID** and **API key**. These values are required to configure the Confluence SaaS Application Tenant in the ZIA Admin Portal.

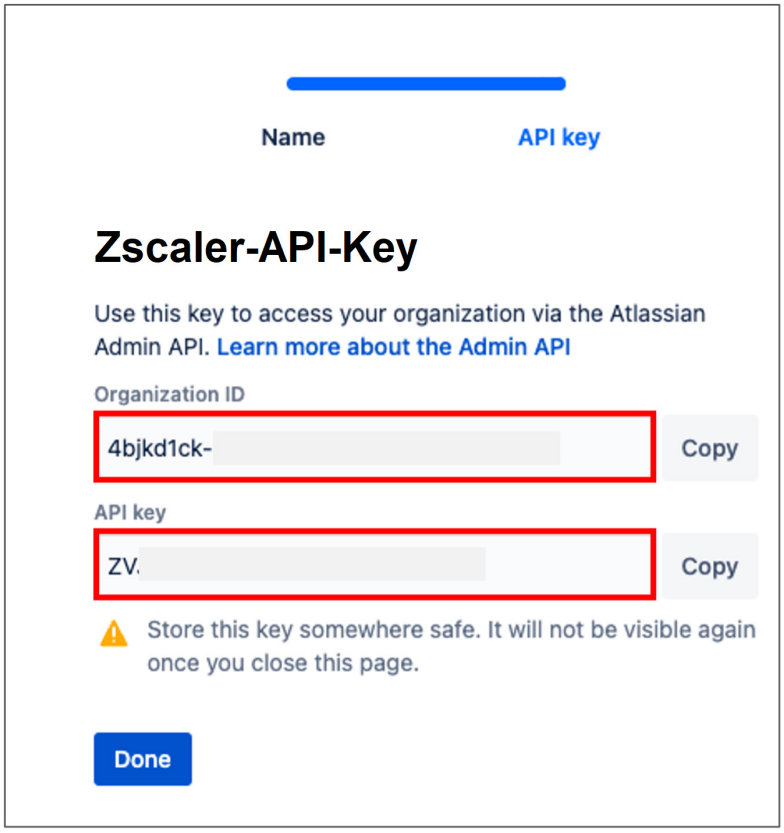

Figure 68. Complete organization API key

Make sure you store these values in a safe place, as they won't be displayed again. Zscaler only requires the API key value.

9. Click **Done**. The key appears in the list of API keys.

Configure Jira SaaS Application Tenant

To launch the SaaS Application Tenants wizard for the ZIA Admin Portal:

1. Go to **Administration** > **SaaS Application Tenants**.
2. In the **SaaS Application Tenants** dialog, click **Add SaaS Application Tenant**.

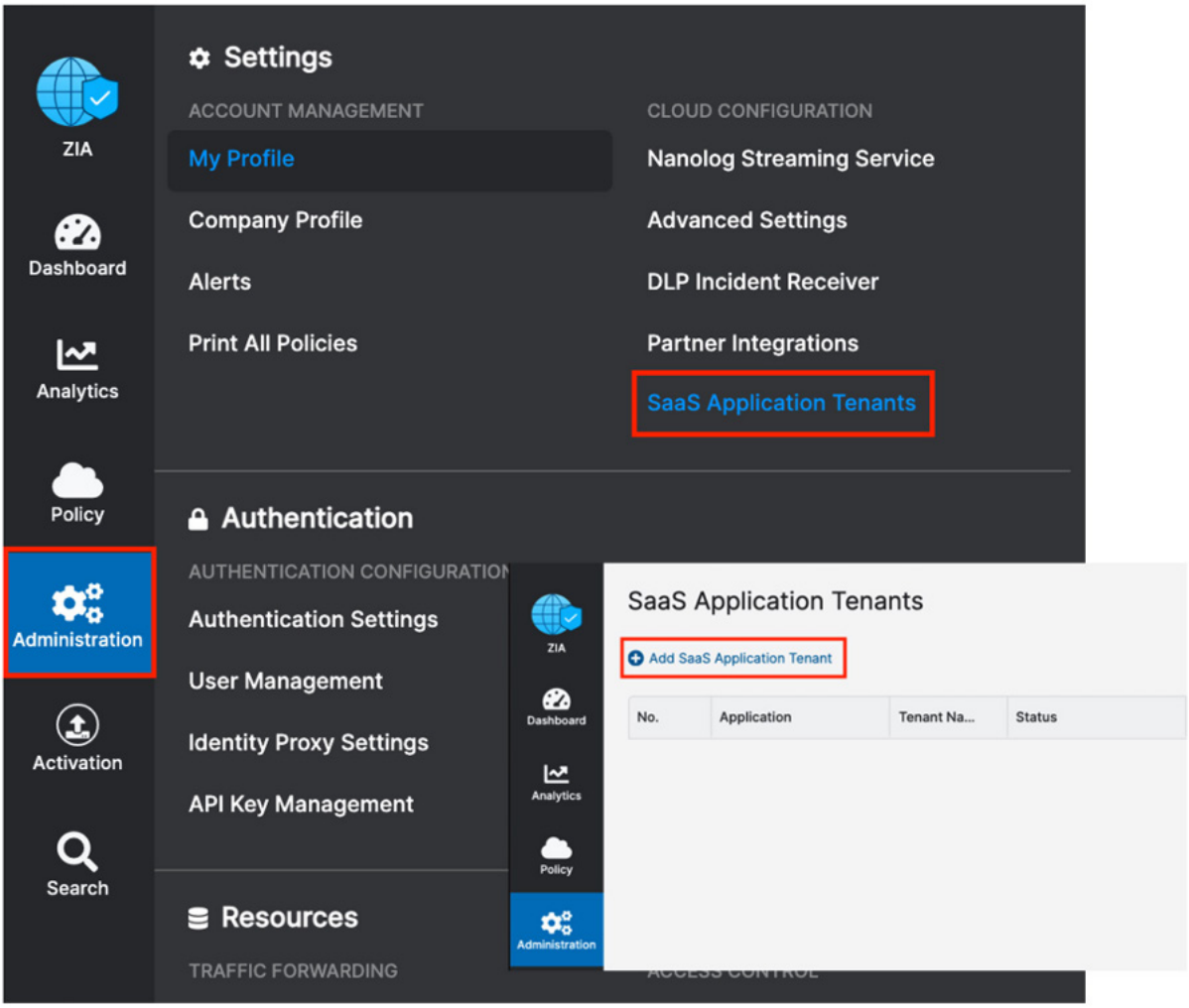

Figure 69. ZIA SaaS Application Tenants

Jira SaaS Tenant Configuration Wizard

To start the wizard:

1. Select **Add SaaS Application Tenant**.
2. Select the **Jira Software** tile.

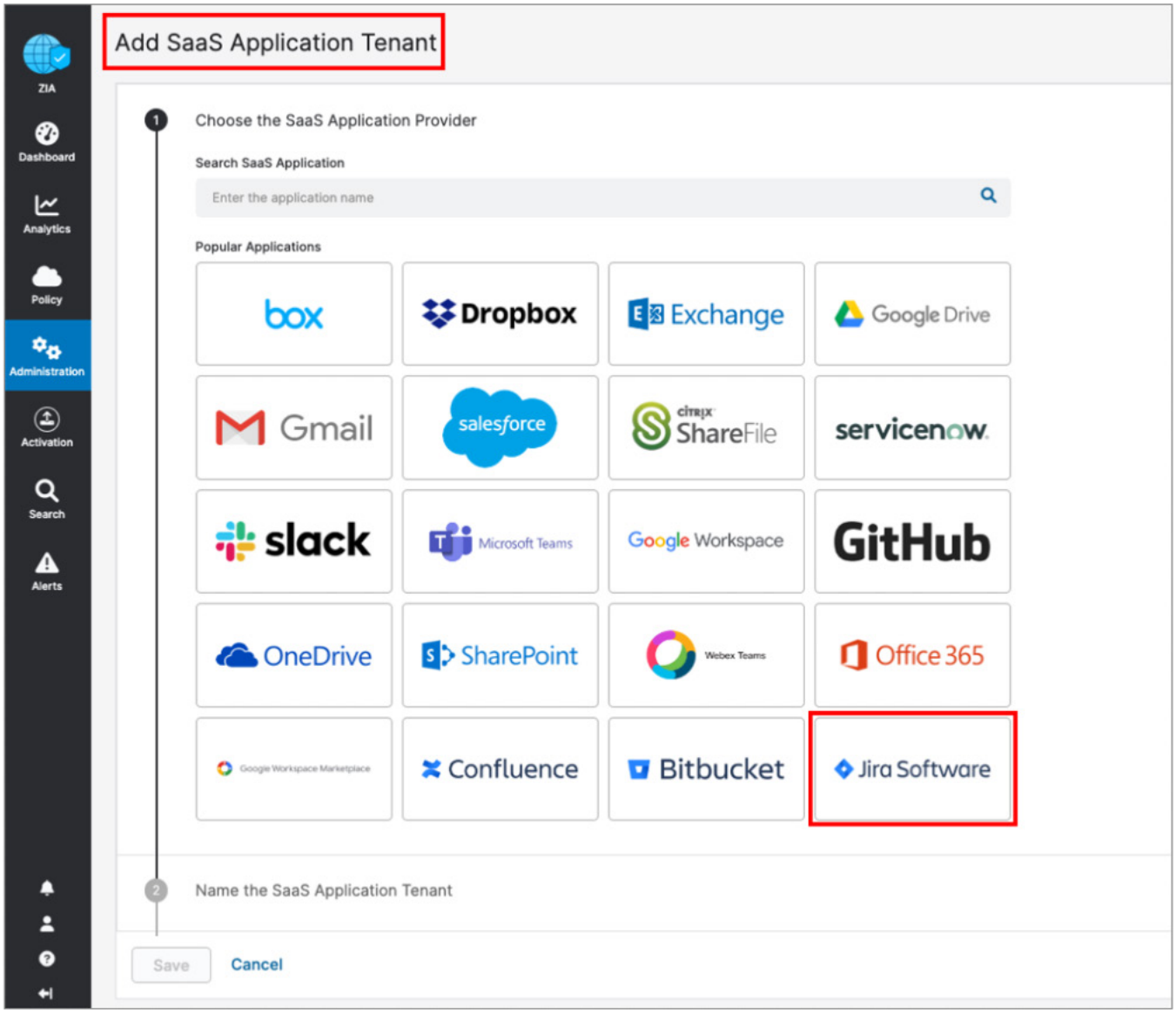

Figure 70. The Confluent SaaS tenant configuration wizard

3. Give the Jira tenant a name. This is the name that is selected when assigning a policy for the Zscaler security features:
   a. Enter a name in the **Tenant Name**.
   b. Enter the **Jira Site Name**.
   c. Enter the **Jira Organization API Key** created in [Create Jira Organization API Key].

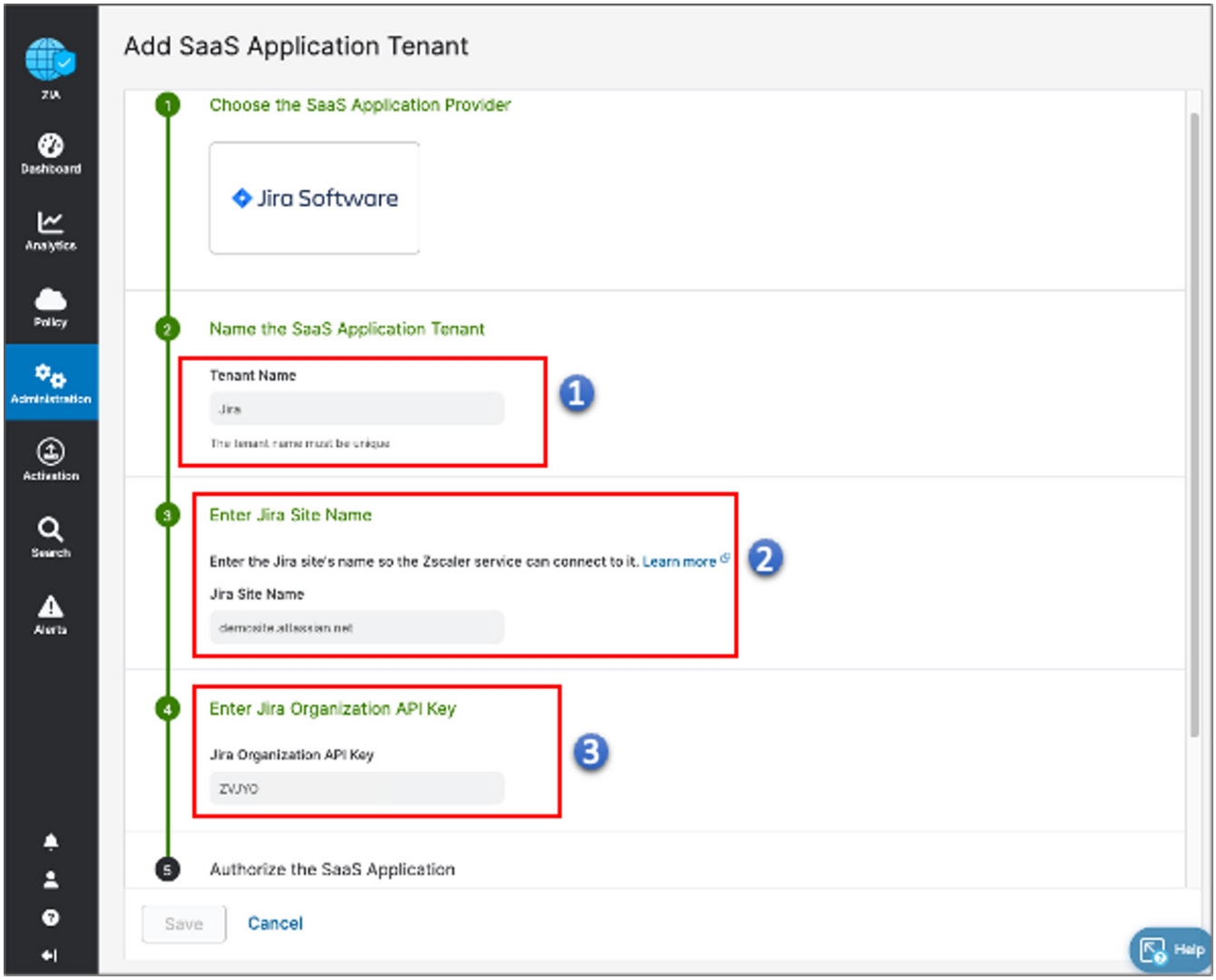

Figure 71. The Jira SaaS tenant configuration wizard

4. Click **Provide Admin Credentials**, which redirects you to the Atlassian login portal.

Figure 72. Atlassian login portal

5. Authenticate with your Jira administrator credentials.

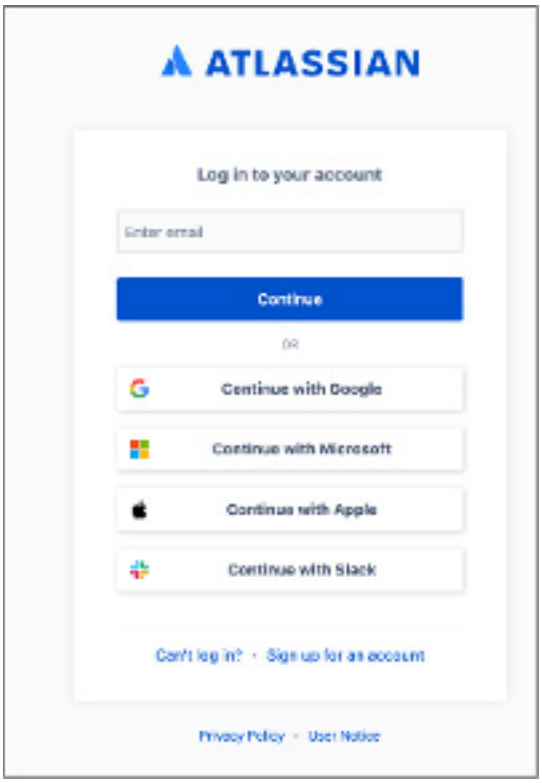

Figure 73. Authenticate to the Jira tenant

6. Give permission to Zscaler SaaS Connector by clicking **Accept**.

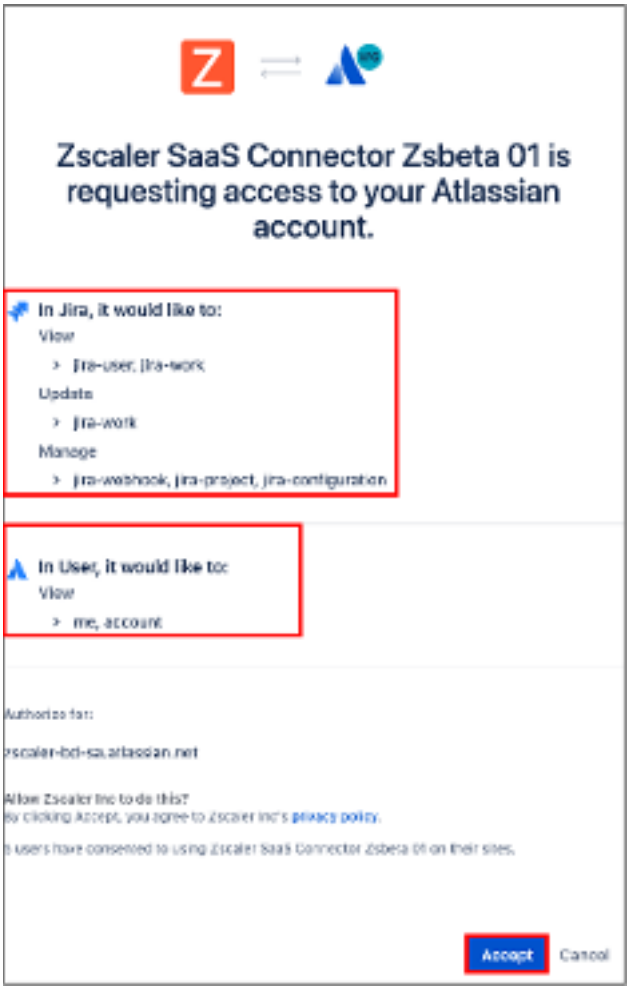

Figure 74. Grant access to Zscaler SaaS Connector

7. Click **Save**.

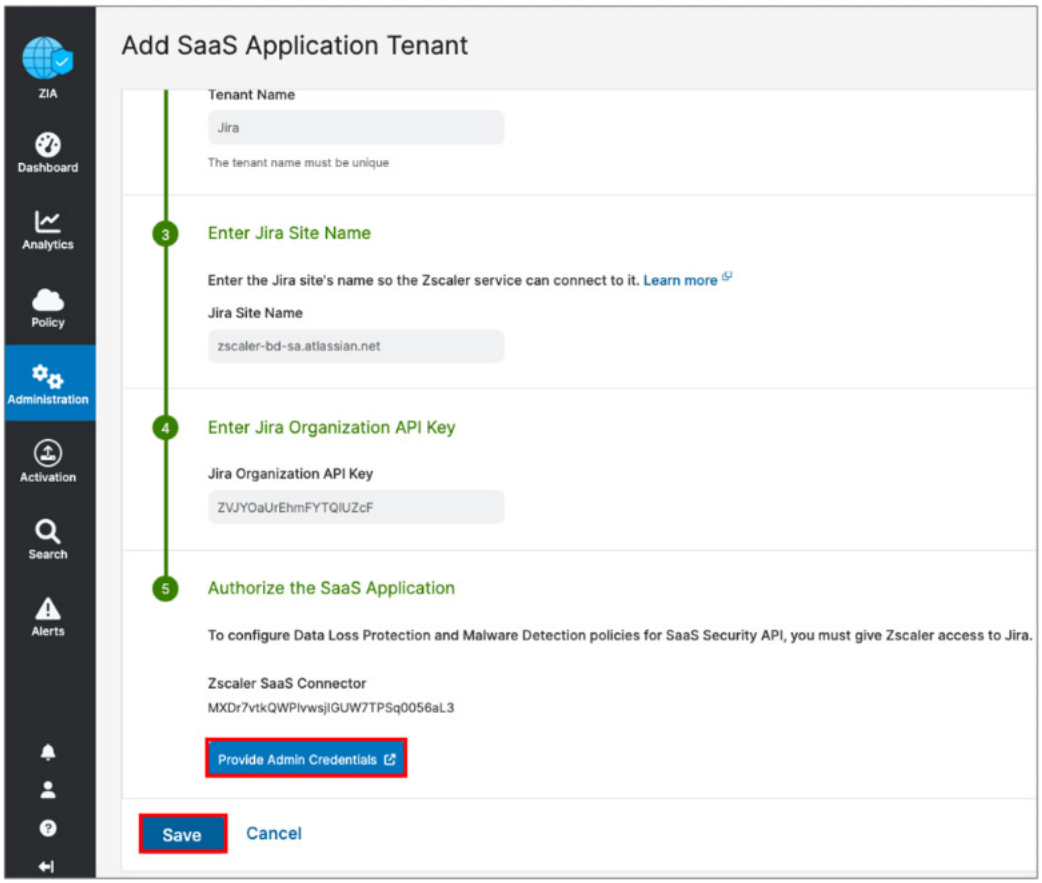

Figure 75. Save Zscaler SaaS Connector configuration

The completed and active Jira API connector is displayed.

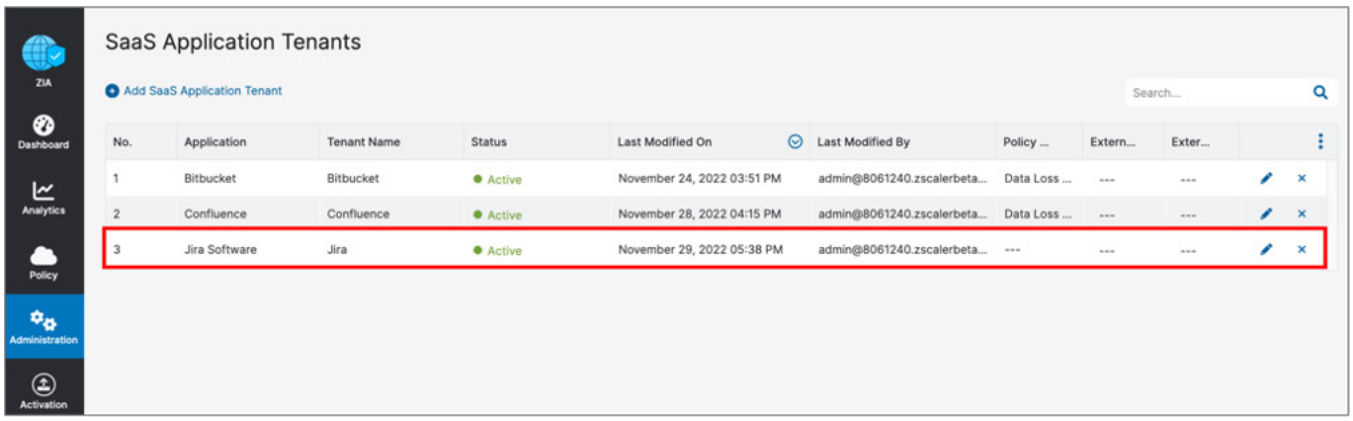

Figure 76. Completed Jira API Connector

Configure Jira Policies and Scan Configuration

After adding and configuring the Jira tenant, you can configure the SaaS Security API to control DLP, malware policies, and then scan the configuration for the policies. You can also view reports and data for Jira in analytics, SaaS security insights, and logs.

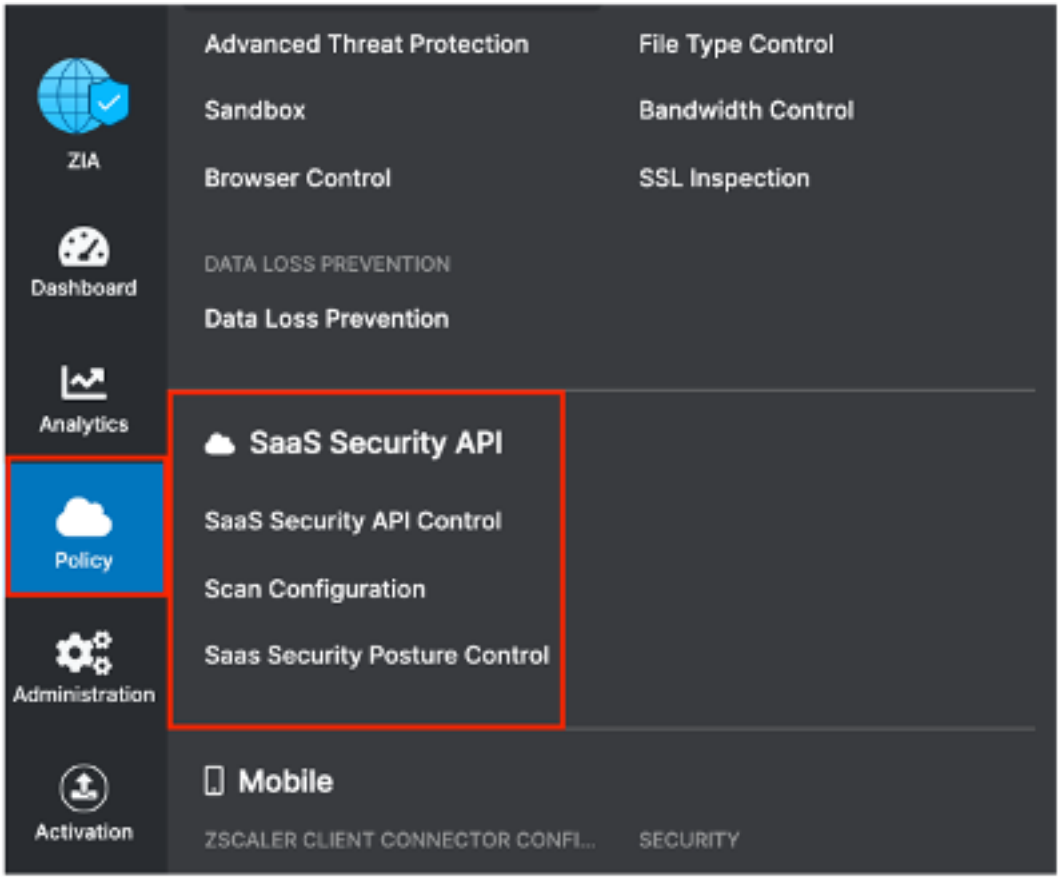

Figure 77. SaaS Security API in ZIA Admin Portal

Scoping the Policies and Remediation

This deployment guide configures a basic DLP policy and a malware policy. Zscaler SaaS Security API out-of-band data protection capabilities look inside the SaaS applications themselves through API integrations to identify accidental or intentional data exposure and compliance violations that would otherwise go unnoticed.

For Jira, the Zscaler SaaS Security API DLP rule scans all the blogs, pages, and attachments within a space. The DLP rule does not scan the overview page for any space.

The DLP policy broadly identifies a spreadsheet with a list of US Social Security numbers. DLP is a subject of its own, and this policy is only used for demonstration purposes. Conduct a true DLP policy review to minimize false positives and false negatives.

It is also important to note that SaaS DLP protection is only part of the Zscaler DLP solution and scans data-at-rest (like the Jira files). This deployment doesn't cover in-line data protection, exact data match, or indexed document matching (document template fingerprinting), although they are integral pieces of a complete data protection solution.

For next steps to test the DLP SaaS functionality, create a basic policy, and apply it to the Jira tenant. If you already have DLP policies created, skip ahead to Configure a SaaS Malware Policy for Jira.

Creating a DLP Policy

To create a DLP policy:

- Create a custom dictionary (or use the available dictionaries) to identify the data the scan is going to look for.
- Create an engine that is the logical template for adding expressions and additional data. This is where you would specify Social Security numbers and any other criteria for the policy. The engine provides the means to precisely add or remove data to match violations and eliminate false positives.
- Create an SaaS security DLP policy that specifies the details about where, when, the action taken, and whom to inform about violations.

Notice that you can create a custom DLP dictionary that contains your own patterns and phrases, or use one of the predefined dictionaries. This deployment guide focuses on predefined dictionaries.

Creating a DLP Engine

To create a DLP engine, from the ZIA Admin Portal:

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. Click the **DLP Engines** tab, and then click **Add DLP Engine**.

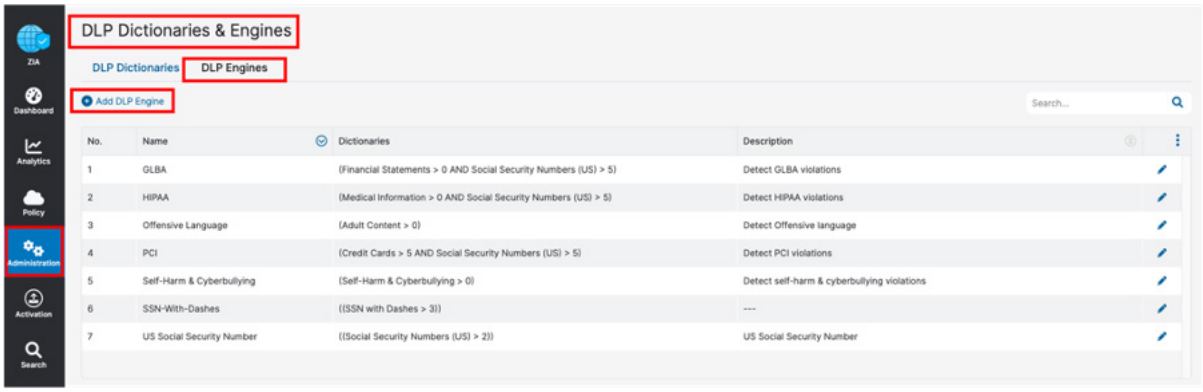

Figure 78. Creating a DLP engine

3. Give the DLP engine a **Name**.
4. In the **Engine Builder** under **Expression**, select the desired dictionary. In the following example, **Social Security Numbers (US)** is selected.
5. Specify the **Match Count**, which is the minimum number of instances the data must occur in the file.
6. (Optional) Click **Add** to add the next dictionary and repeat the process of naming and defining the dictionary.
7. Click **Save**, then **Activate** the configuration.

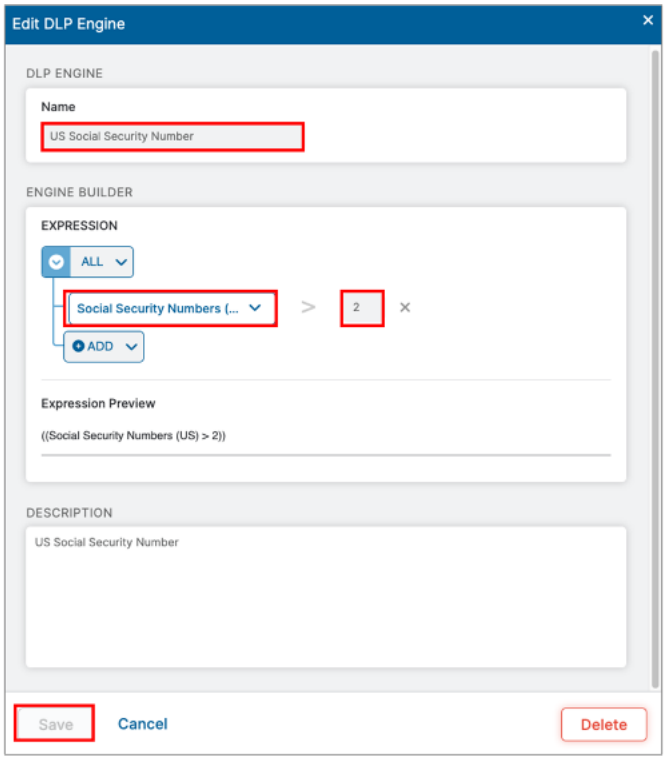

Figure 79. The DLP Engine wizard

This policy triggers when you see the third Social Security number. Again, this is a demonstration and the criteria is too general to be a production DLP rule.

Configure a SaaS DLP Policy for Jira

Apply the engine to a DLP policy used for the Jira instance. Launch the Add DLP Rule wizard to start the process:

1. Go to **Policy** > **SaaS Security API Control** > **Data Loss Prevention**.
2. Click **File Sharing**.
3. Click **Add DLP Rule**.
4. Select **Jira** as the **SaaS Application Tenant**.
5. Select the **DLP Engine** created in [Jira SaaS Tenant Configuration Wizard].
6. Select **Any-Any** for the **Collaboration Scope**.
7. Select **Report Incident Only** as the **Action**.
8. Select **High** as **Severity** to allow for identification, searches, and tracking.
9. Click **Save**, then **Activate** your configuration.

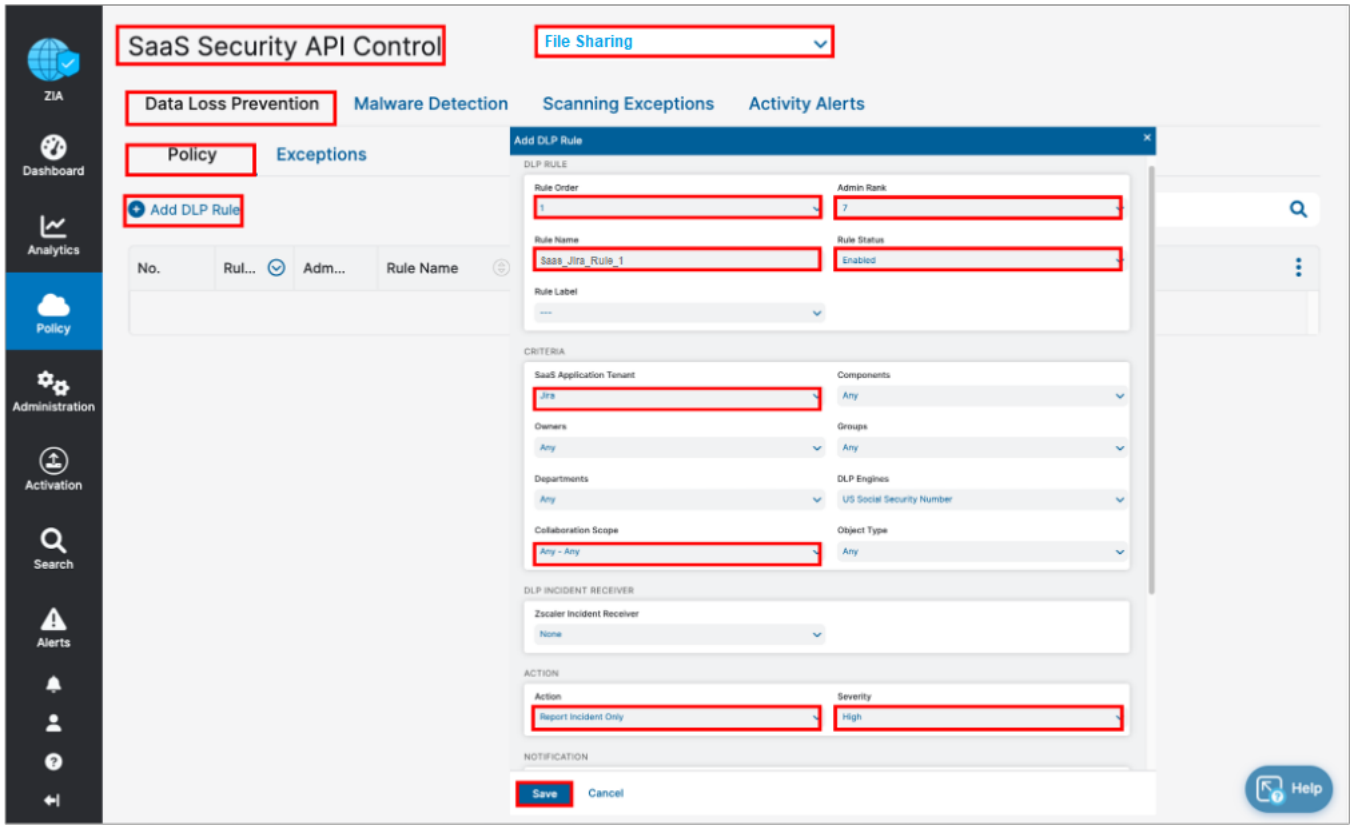

Figure 80. Launch the SaaS DLP Policy Configuration wizard

Apply a scanning schedule to the Jira DLP rule.

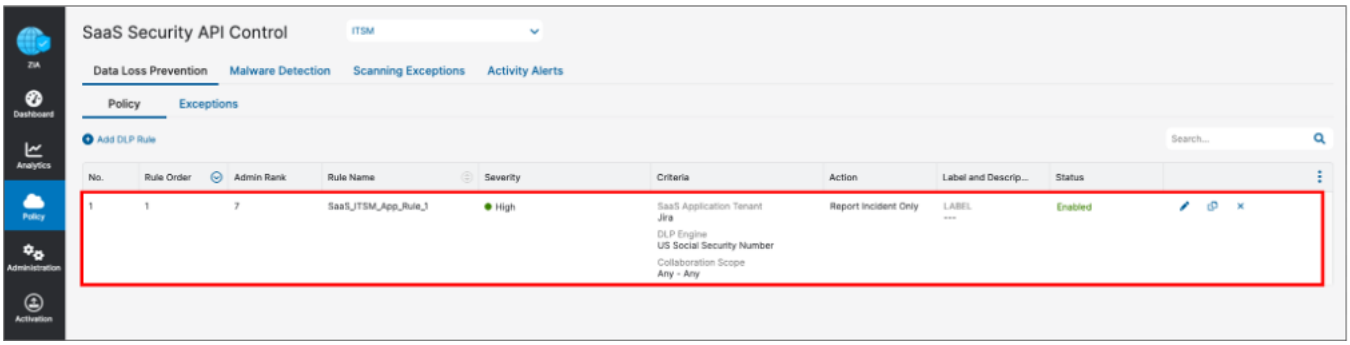

Figure 81. The configured DLP policy

SaaS DLP Policy Details

The SaaS DLP policy specifies the detail on whom this policy and for what data this policy applies. You specify the rule order if you have multiple DLP policies, which are processed in an ascending manner. The first rule that matches is the applied rule. Specify the DLP engine you defined, any file owners, groups or departments, and the file types to inspect. The collaboration scope and the action are unique to the SaaS DLP. Select a collaboration and an action to remove sharing.

The Collaboration Scope includes the collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select Any to apply the rule to files with all collaboration levels, or select one or more of the following collaboration scopes and specify the permissions for each scope:

- External Collaborators: Files that are shared with specific collaborators outside of your organization.
- External Link: Files with shareable links that allow anyone outside your organization to find the files and have access.
- Internal Collaborators: Files that are shared with specific collaborators or are discoverable within your organization.
- Internal Link: Files with shareable links that allow anyone within your organization to find the files and have access.
- Private: Files that are only accessible to the owner.
- The Action: The rule acts after detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant. For Jira, the actions are Quarantine, Remove, Report Incident Only.
- Report Incident Only: The rule reports the incident only and makes no changes to the file's collaboration scope.

Configure a SaaS Malware Policy for Jira

To launch the Malware Detection Rule wizard:

1. Go to **Policy** > **SaaS Security API Control** > **Malware Detection**.
2. Click **File Sharing**.
3. Click **Add Malware Detection Rule**.

The SaaS Security API Malware Detection policy is an all-encompassing policy and all files in the tenant are scanned unless removed from the scope specifying exemptions by selecting the Exceptions tab under Malware Detection. To add a malware policy, specify the application, the SaaS tenant, and the status.

The actions available for Jira are Quarantine Malware, Remove Malware, and Report Malware.

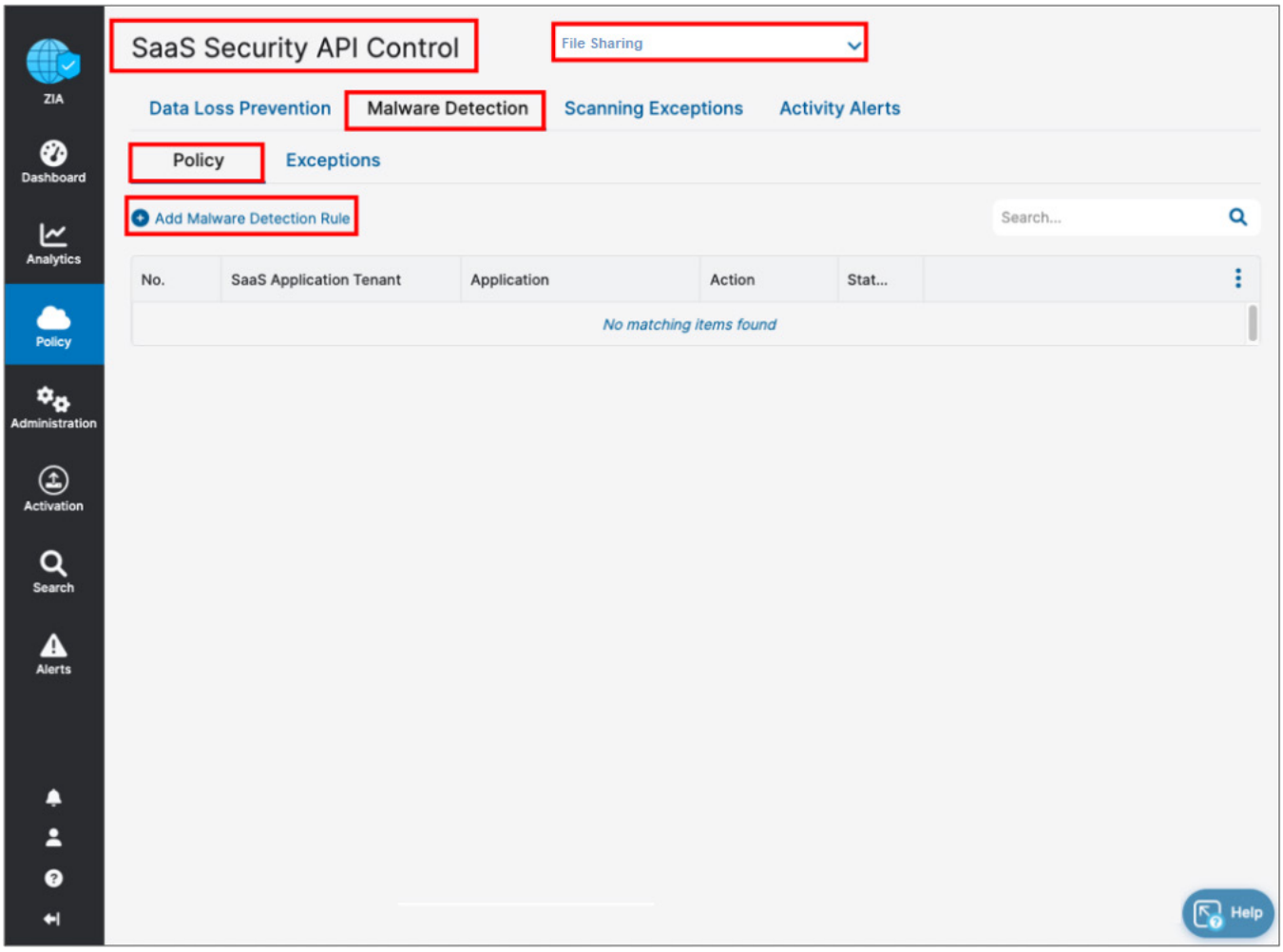

Figure 82. Launch the malware Policy Configuration wizard

Jira SaaS Malware Policy Wizard

Configure the Malware Detection Rule wizard:

1. In **Application**, select **Jira Software** as the application.
2. Select **Jira** as the **SaaS Application Tenant** to apply the policy.
3. Select **Enabled** for **Status**.
4. Select the desired **Action**. In the following example, **Report Malware** is selected.
5. Click **Save**.

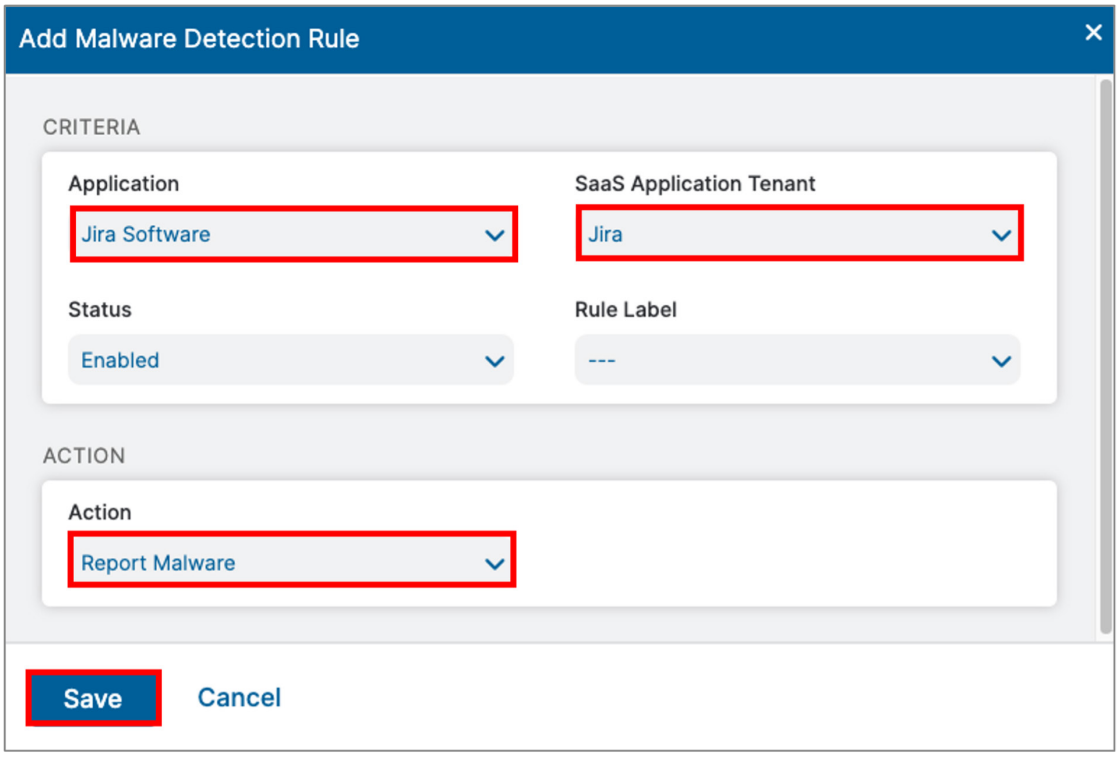

Figure 83. The Malware Policy Configuration wizard

Jira SaaS Malware Policy

Apply the completed SaaS Security API Malware Detection policy for the Jira SaaS tenant to the Jira instance with a scanning schedule. Activate your configuration.

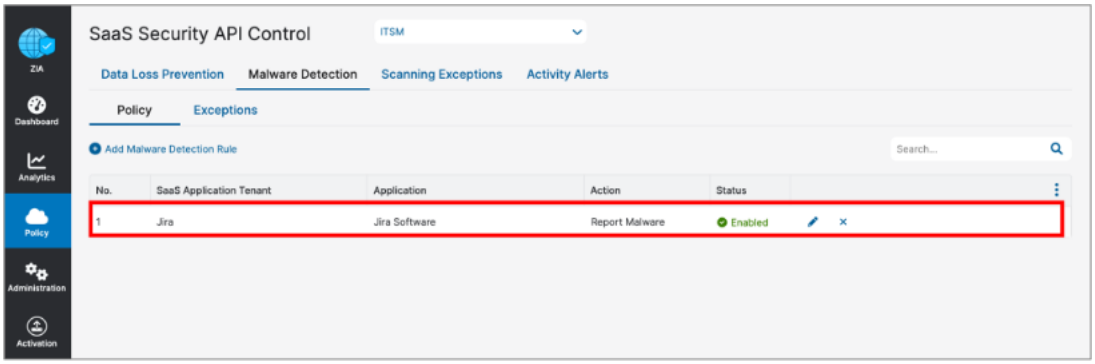

Figure 84. The complete Jira Malware Policy Configuration wizard

Configure a Scan Schedule Configuration for Jira

The final configuration step is to create a Scan Configuration. Specify the tenant the Scan Configuration applies to, any policies that are to be included in the scan, and what data to scan relative to a date. The options for Data to Scan are All Data, Date Created or Modified After, or New Data Only. For this deployment guide, select All Data.

However, if this is a Proof of Value (POV) or a Trial, the only option available is New Data Only.

To add a Scan Schedule:

1. Go to **Policy** > **SaaS Security API** > **Scan Configuration** > **Add Scan Schedule**.
2. Select **Jira** SaaS as the **SaaS Application Tenant**.
3. In the **Policy** field, select the **Data Loss Prevention** policy and **Malware** policy created in prior procedures.
4. Select **All Data**. (Or, for a POV or a Trial, select **New Data Only**.)
5. Click **Save**, and then **Activate** the configuration.

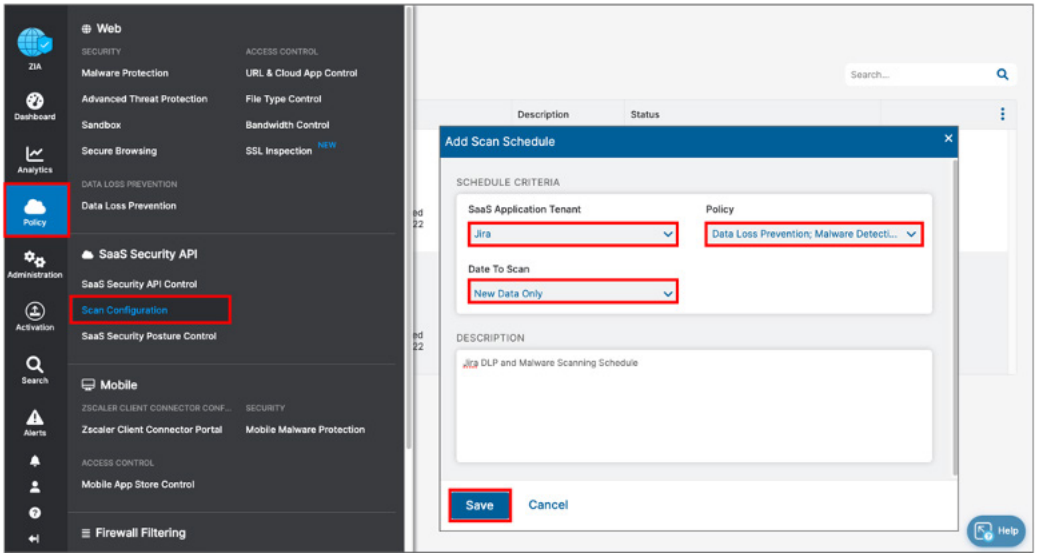

Figure 85. Create and enable a scan for the Jira SaaS tenant

Start the Scan Schedule for Jira

After the schedule has been configured and saved, start the scan for the DLP policy and malware policy to be applied.

1. Click the **Start** icon on the Scan Configuration window to start SaaS API security on the Jira tenant. If the scan is running, the icon changes from a start to a stop symbol.
2. Review the **Status** column and ensure it is **Running** with a start date and a latest scan date.

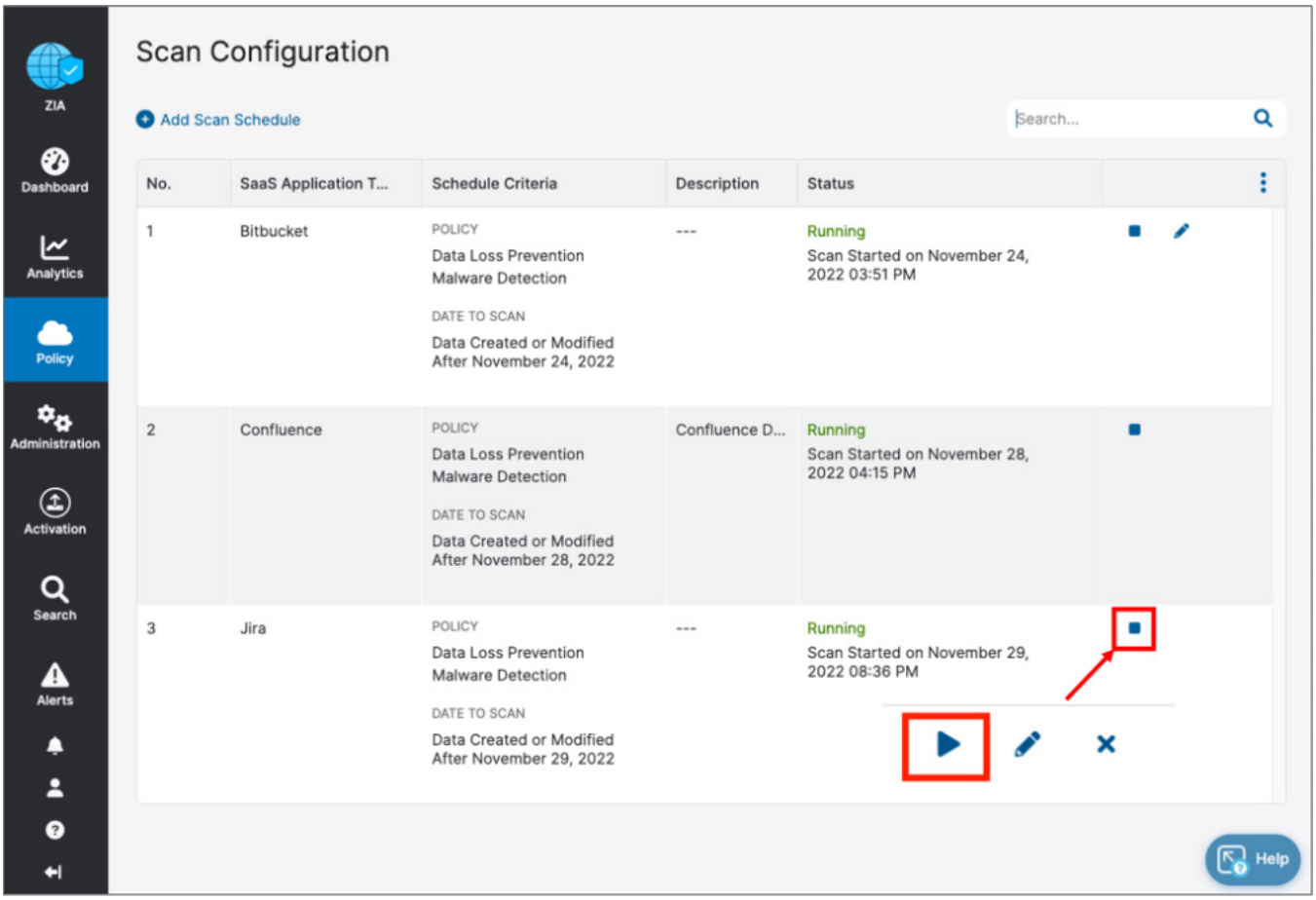

Figure 86. Starting the Jira Scan Schedule

Jira Reporting and Visibility

Zscaler analytics provide detailed reporting of all user activity down to each session created by the user when visiting a destination. Zscaler extends that visibility to include reporting of activity, malware incidents, and DLP violations of data at-rest associated with the user. Zscaler has reports and SaaS security insights that provide visibility from a high-level overview to management of the individual logs and violations.

To learn more, see [SaaS Security Insights](#).

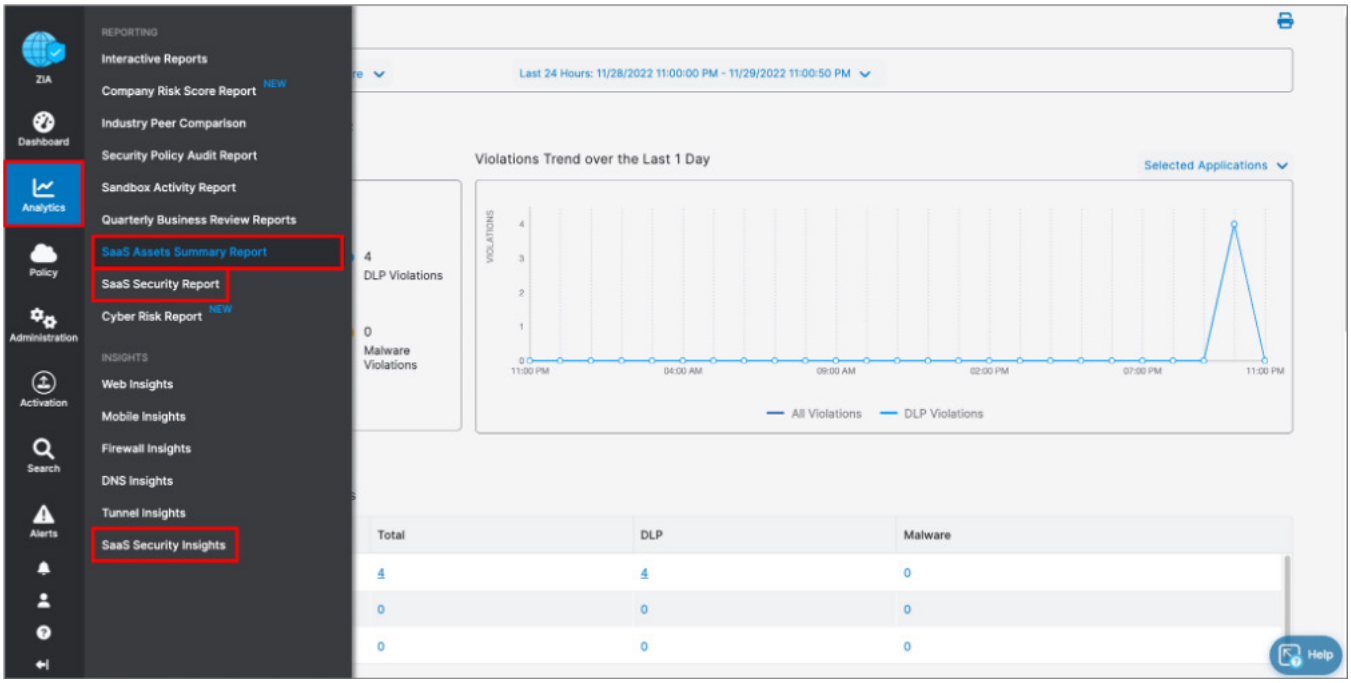

Figure 87. SaaS security visibility

SaaS Assets Summary Report

The SaaS asset reports provide a summary or customizable reporting to have a quick view of your files and emails. A SaaS Assets Summary Report provides all activity and violations in a quick glance. The report identifies all SaaS tenant information from a single page. Although your Jira activity over the creation of this deployment guide is shown, any configured tenant is displayed on this summary report. The data is hyperlinked, and you can easily pivot from a summary to individual logs and activities provided by SaaS security insights.

1. Select the **Total** violations number next to the **Jira** icon to pivot to SaaS security insights.
2. On the **Security Logs** window, review the log data for each violation containing over 30 metadata points of information.

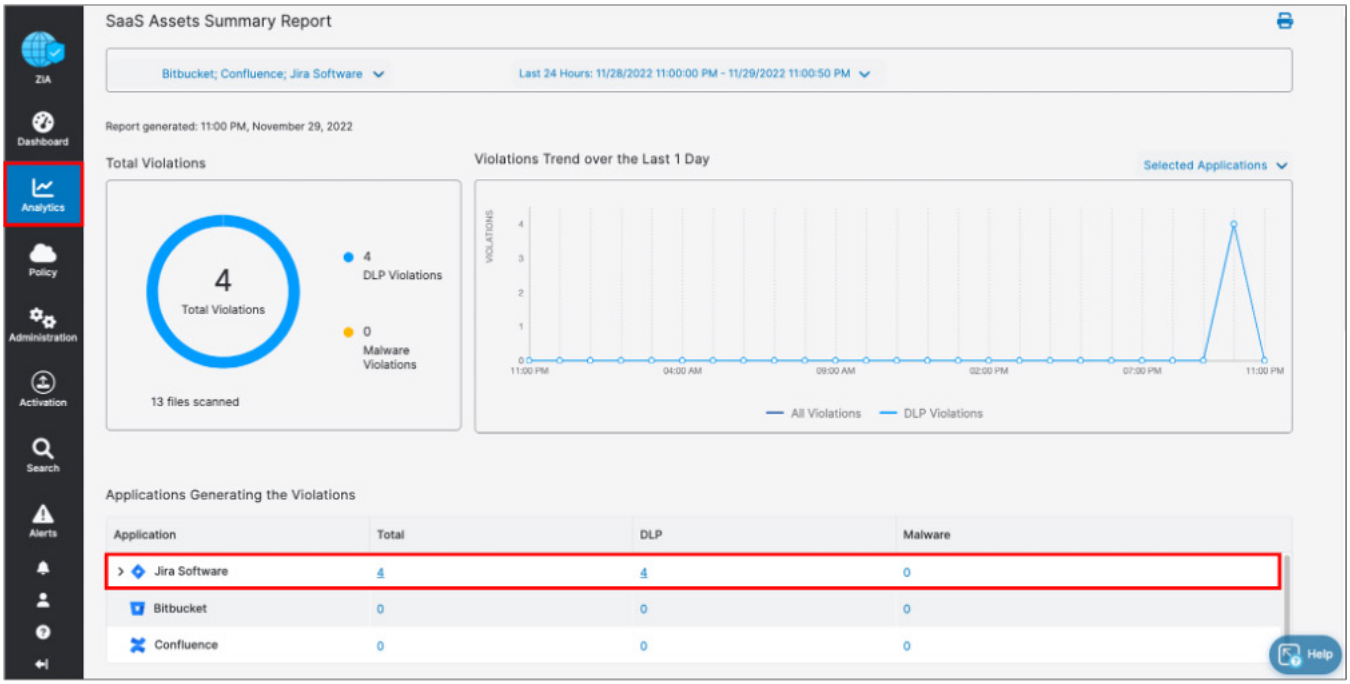

Figure 88. Jira SaaS Assets Summary reports

SaaS Security Insights

The SaaS Security Insights Logs window allows you to select information fields for closer viewing when analyzing files scanned through charts. These logs provide the detail of the policy that found the violation, the threat name, the owner, and over 30 metadata points for identification and threat hunting.

The following are the SaaS Security data types.

- Application
- Application Category
- Department
- DLP Dictionary
- DLP Engine
- Incident Type
- Owner Name
- Severity
- Tenant
- Threat Category
- Threat Super Category
- User

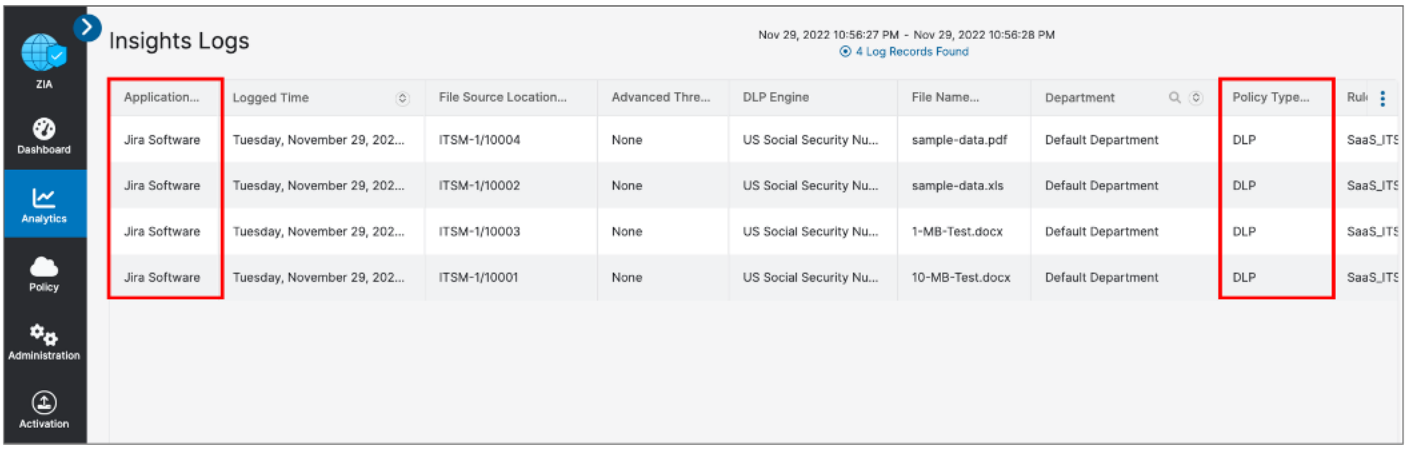

Figure 89. Jira SaaS security insight

ZPC: Jira Integration for Ticket Creation

The process to configure the integration includes the following steps:

- Configure ZPC Jira Integration for ServiceNow License Admin.
- ZPC: Jira Incident Management Integration for the subscription owner.
- ZPC: Jira Incident Management detail tickets for ServiceNow admins.

Create a New Jira OAuth 2.0 (3LO) Integration

Before starting the ZPC integration with Jira, you must first complete the OAuth configuration.

To configure the OAuth app:

1. Log in to the Jira Developer console.
2. Click **Create** to add a new OAuth 2.0 integration.
3. Under **Create a New OAuth 2.0 (3LO) integration**, enter a name for the application.
4. Accept the terms and conditions, then click **Create**.

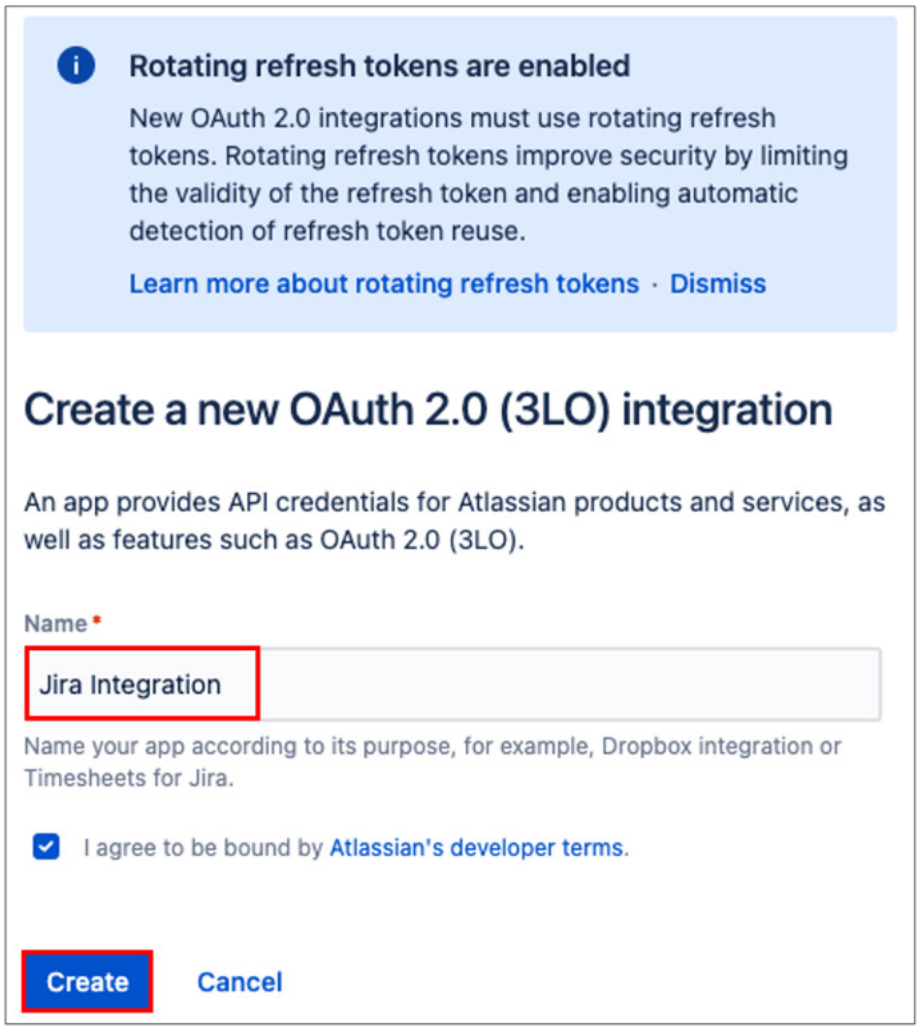

Figure 90. Create OAuth 2.0 integration in Atlassian Admin

The application is created and displayed under **Console** > **My Apps**.

5. Click **Permissions**.
6. Click **Add** for the Jira API. The button name changes to **Configure**.
7. Click **Configure** to view the list of Jira APIs.

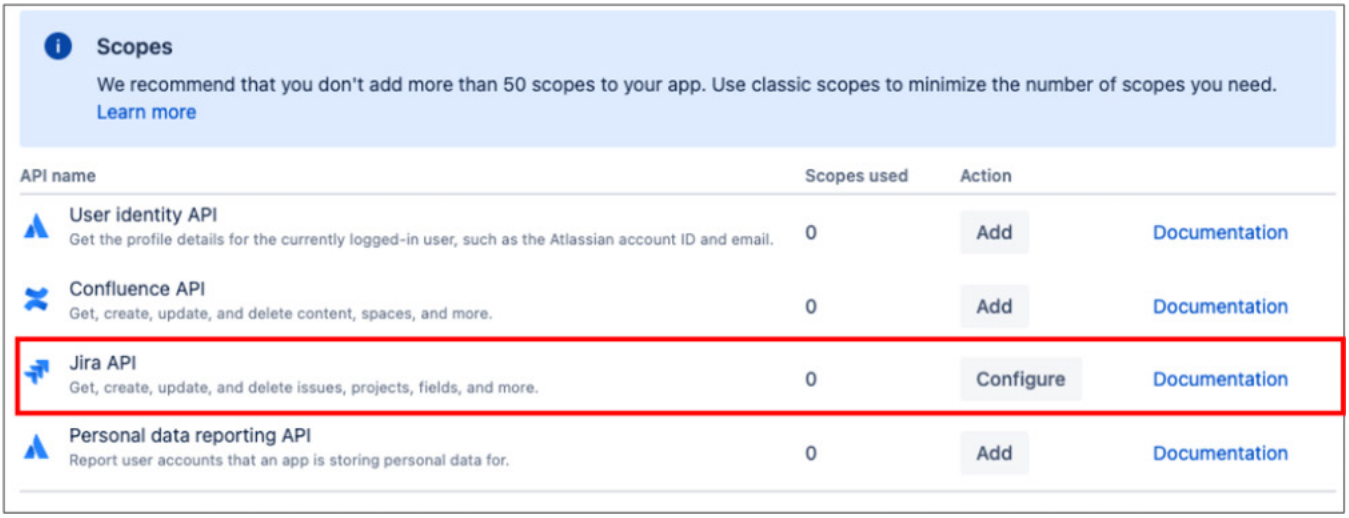

Figure 91. Configure Jira API Permissions in Atlassian Admin

8. Click **Edit Scope** to select the required Jira features that you want to use for this integration.
9. Select the following checkboxes:
   a. **read:jira-work**: To read the Jira project and issue data.
   b. **read:jira-user**: To view user information in Jira to which the user has access.
   c. **write:jira-work**: To create and edit issues in Jira.

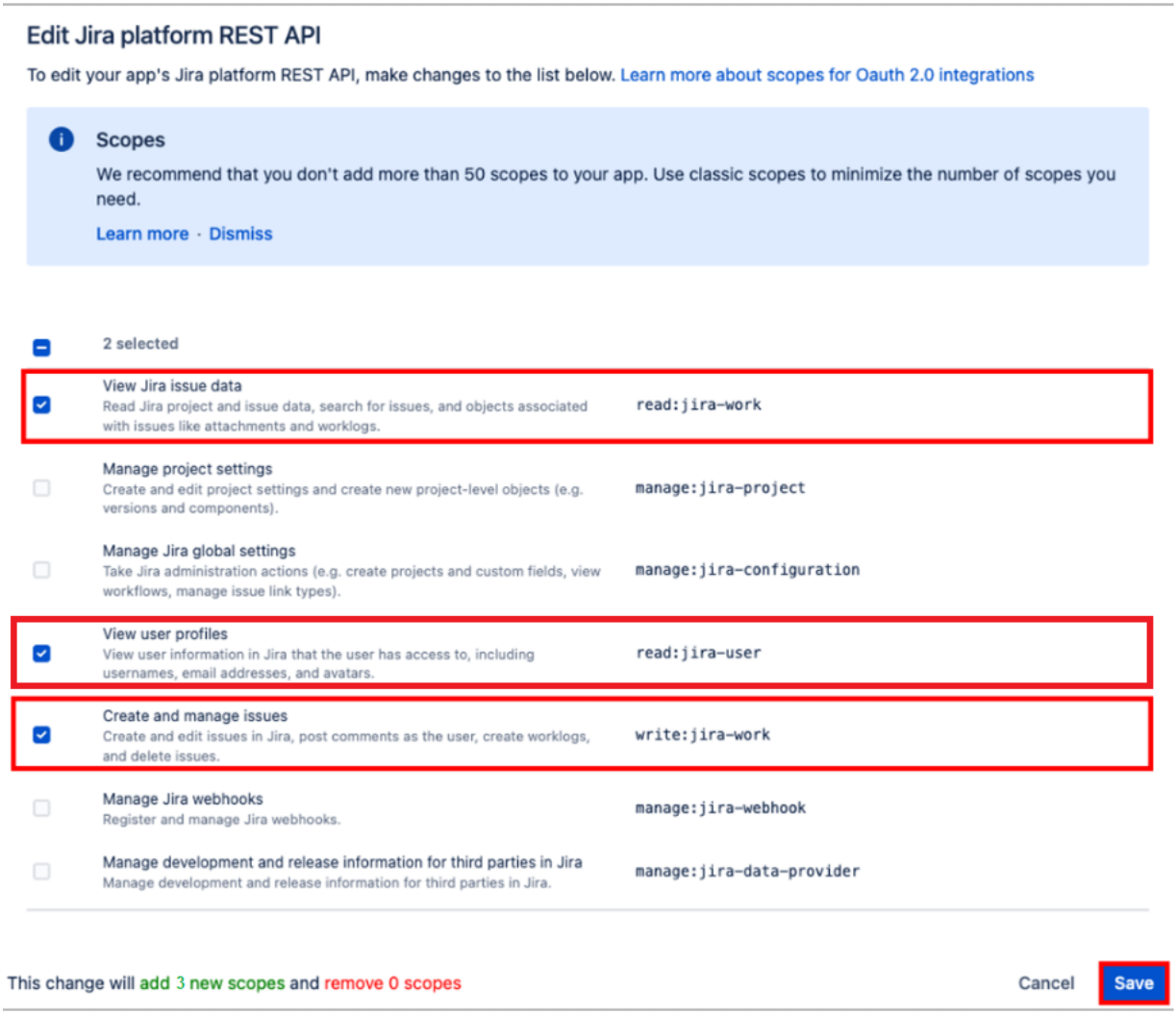

Figure 92. Select Jira API Scope in Atlassian Admin

10. Click **Save**.
11. In the left-side navigation, click **Authorization**.
12. Click **Add** to add the ZPC URL and authorize ZPC to access the Jira APIs.
13. For **Callback URL**, copy and paste the application URL that is specified under **ITSM Details** in the ZPC Admin Portal.

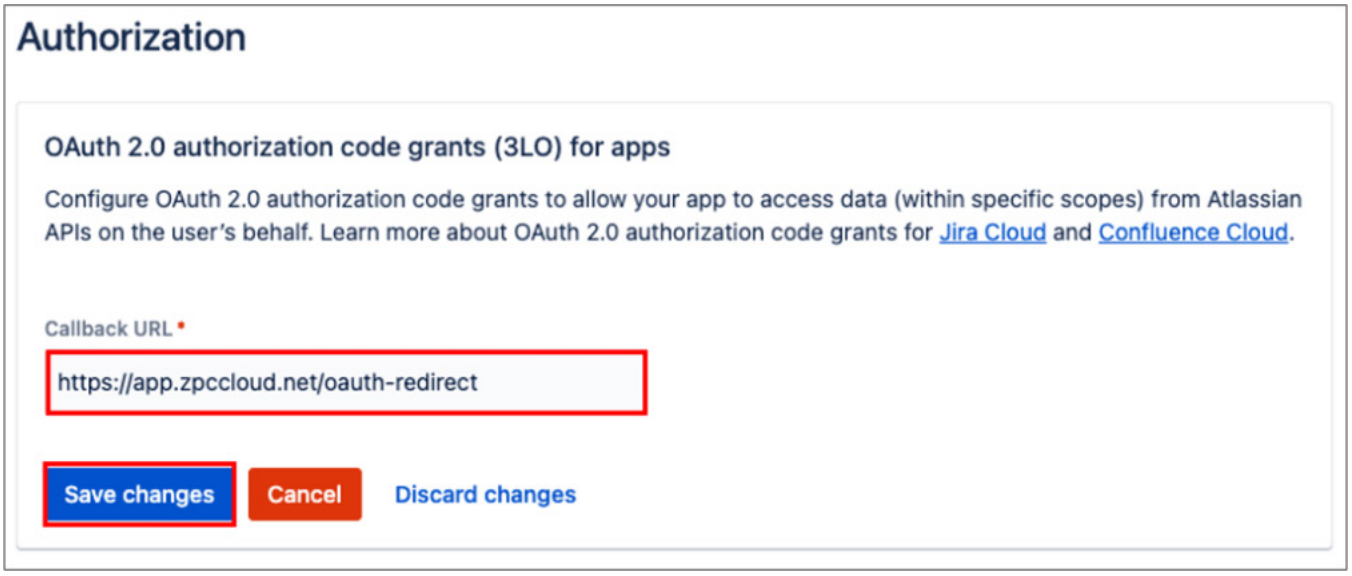

Figure 93. Jira Callback URL in Atlassian Admin

14. Click **Save changes**.
15. Next, click **Settings** in the left-side navigation.
16. Copy the **Client ID** and **Secret**. You use these values while adding the Jira integration on the ZPC Admin Portal.

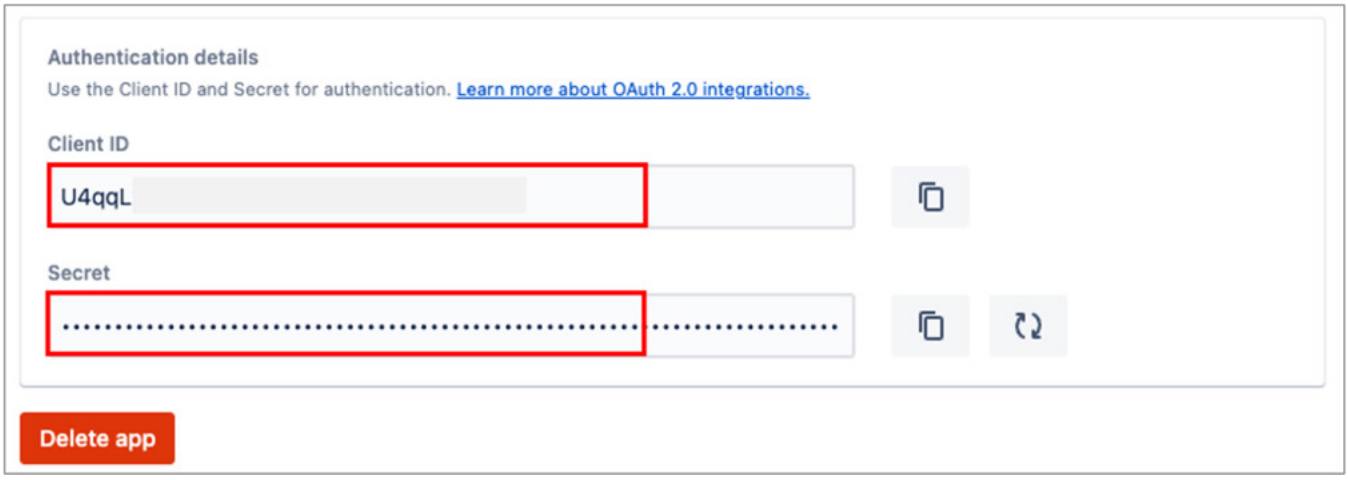

Figure 94. Jira Authentication Details in Atlassian Admin

Configure ZPC Jira Integration

To configure the Jira ticketing system integration:

1. Log in to the ZPC Admin Portal as an administrator.
2. Go to **Administration** > **Integrations**.

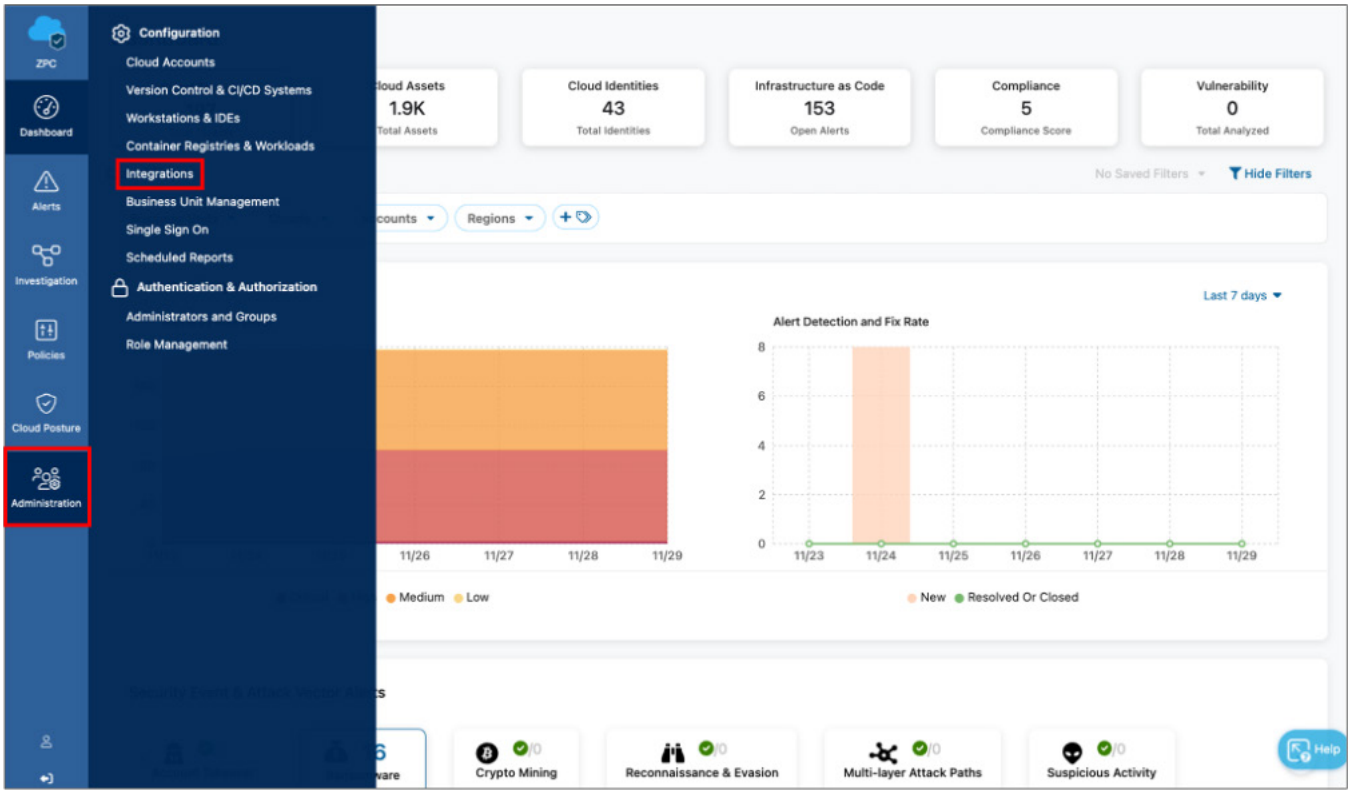

Figure 95. Integrations in ZPC Admin Portal

3. On the **Integrations** page, in the **ITSM** section, click **Add**.

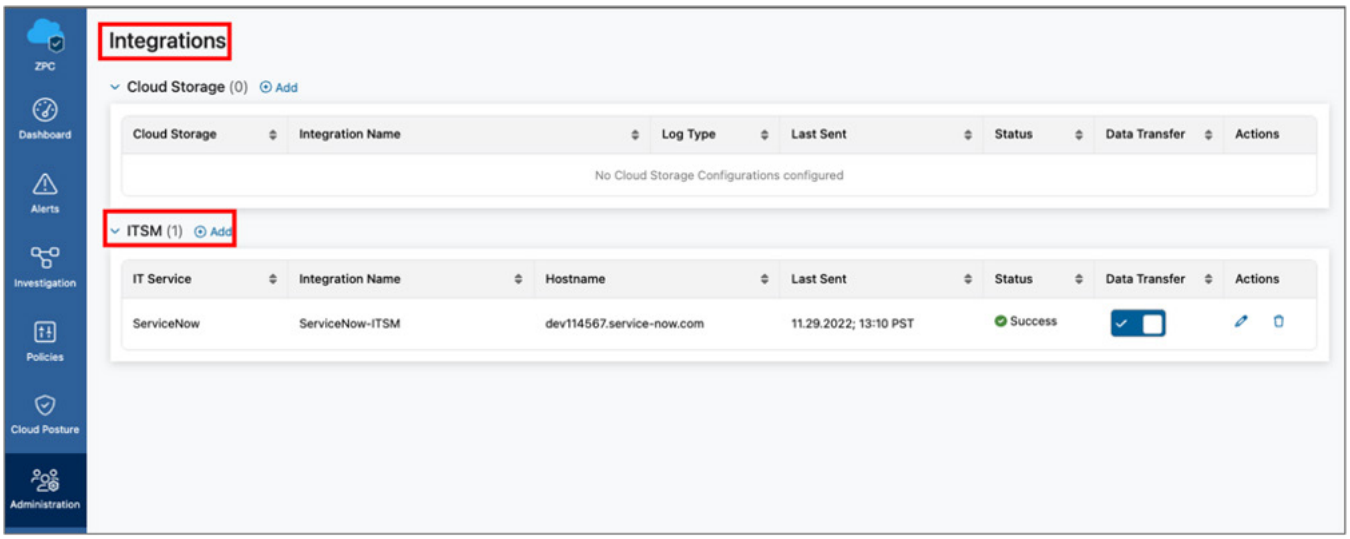

Figure 96. Add ITSM integration in ZPC Admin Portal

ZPC: Jira Incident Management Integration

On the **Add ITSM Integration** page:

1. For **Integration Name**, enter a unique name for the integration.
2. For **IT Service**, select **Jira**.
3. Click **Next**.

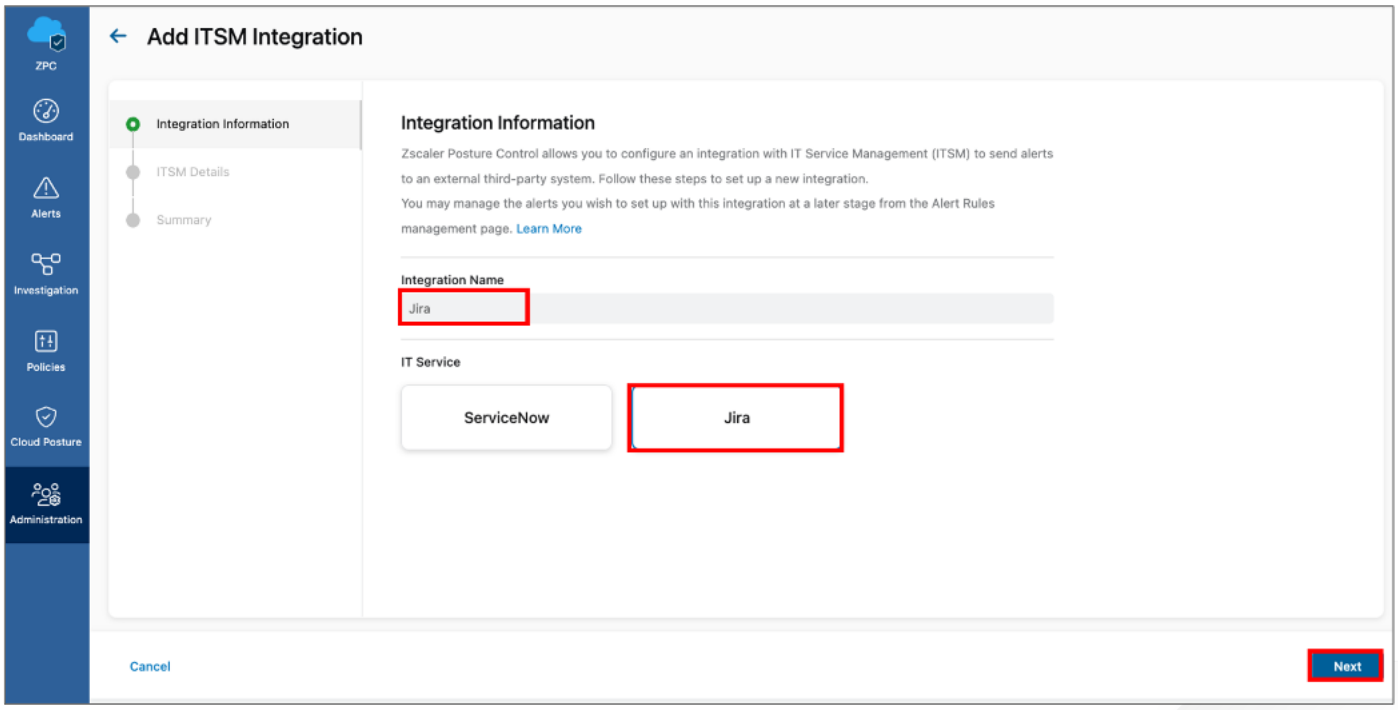

Figure 97. Select Jira in integration information page in ZPC Admin Portal

4. Under **ITSM Details**:
    a. **Jira Client ID**: Paste the Client ID that you copied while configuring the OAuth app.
    b. **Jira Client Secret**: Paste the Client Secret that you copied while configuring the OAuth app.
    c. Click **Authorize** to validate the Jira connection.

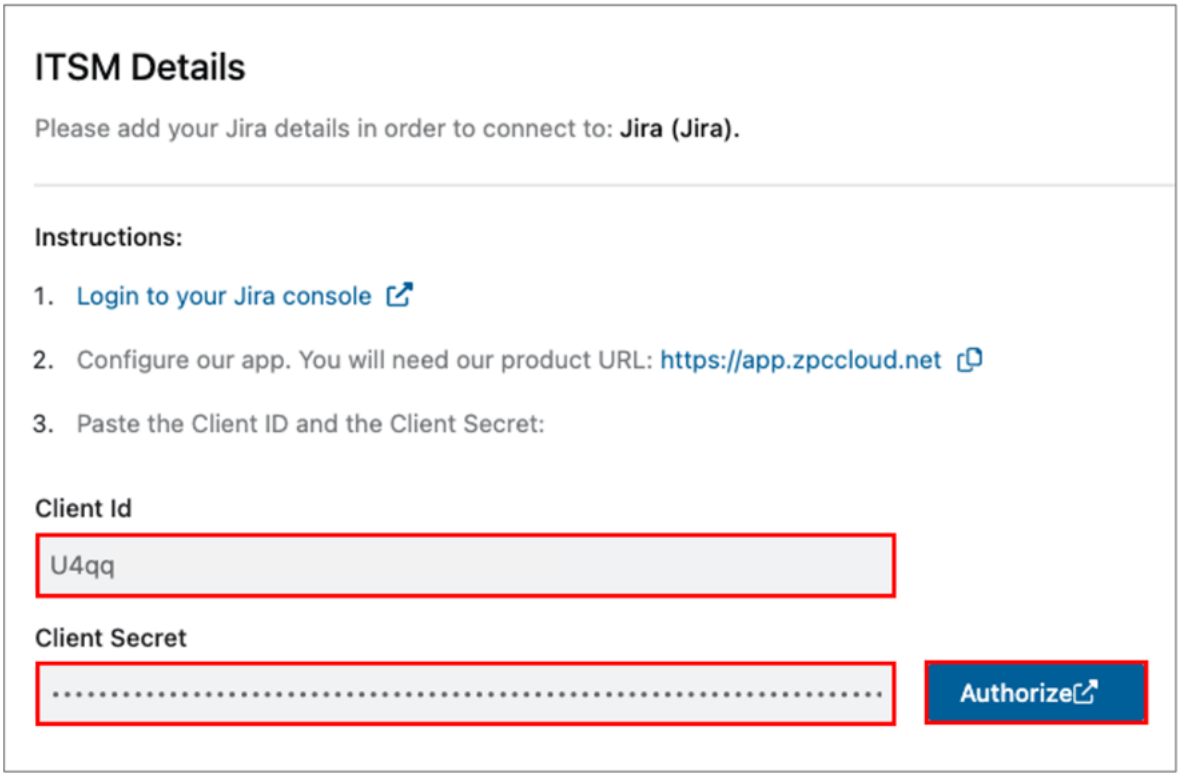

Figure 98. Authorize ZPC to Jira in Atlassian Admin

You are redirected to the Jira Login page.

If you're unable to log in to Jira, then the authorization process is displayed as In Process on the ZPC Admin Portal, and an error message is displayed. Check the Jira Client ID and Client Secret, and use the correct values for a successful authorization.

5. On the Jira Administration console, click **Accept** to grant the required permissions to the OAuth app to perform API operations in Jira.

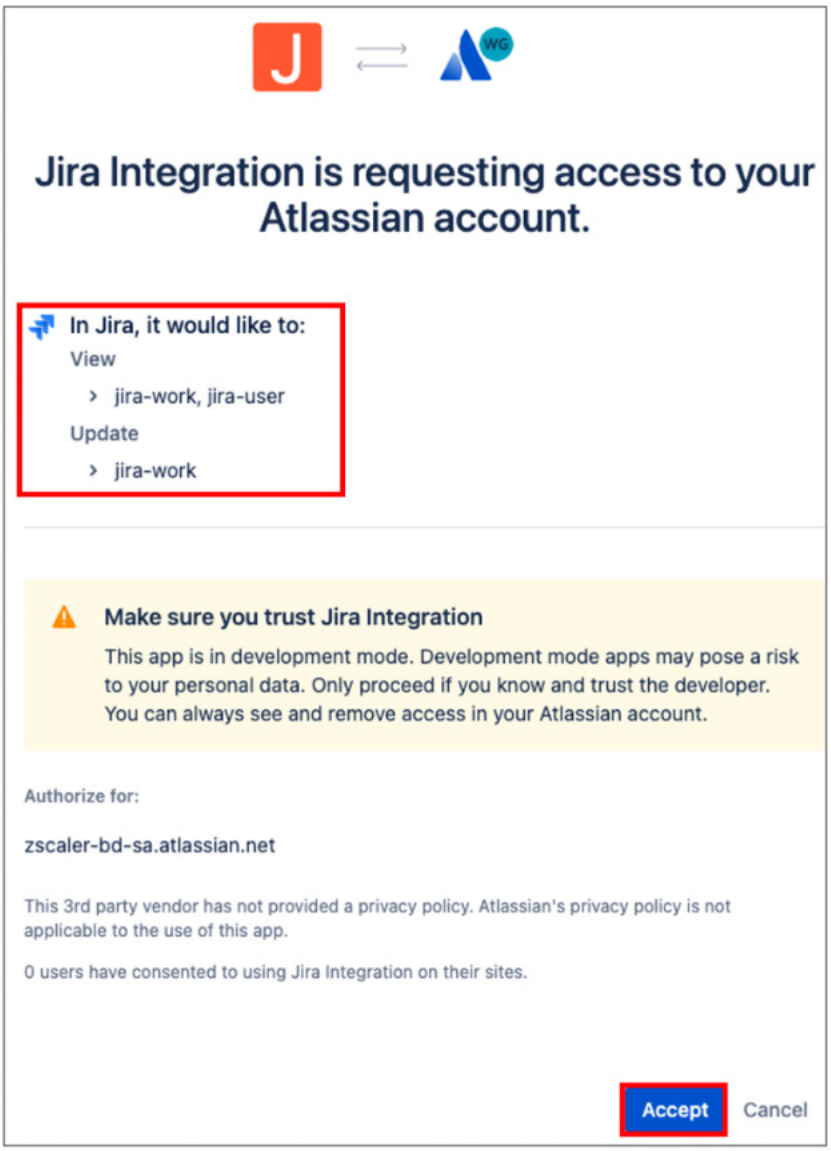

Figure 99. Authorize ZPC to access Jira in Atlassian Admin

6. Ensure that you see the Authorized successfully message.

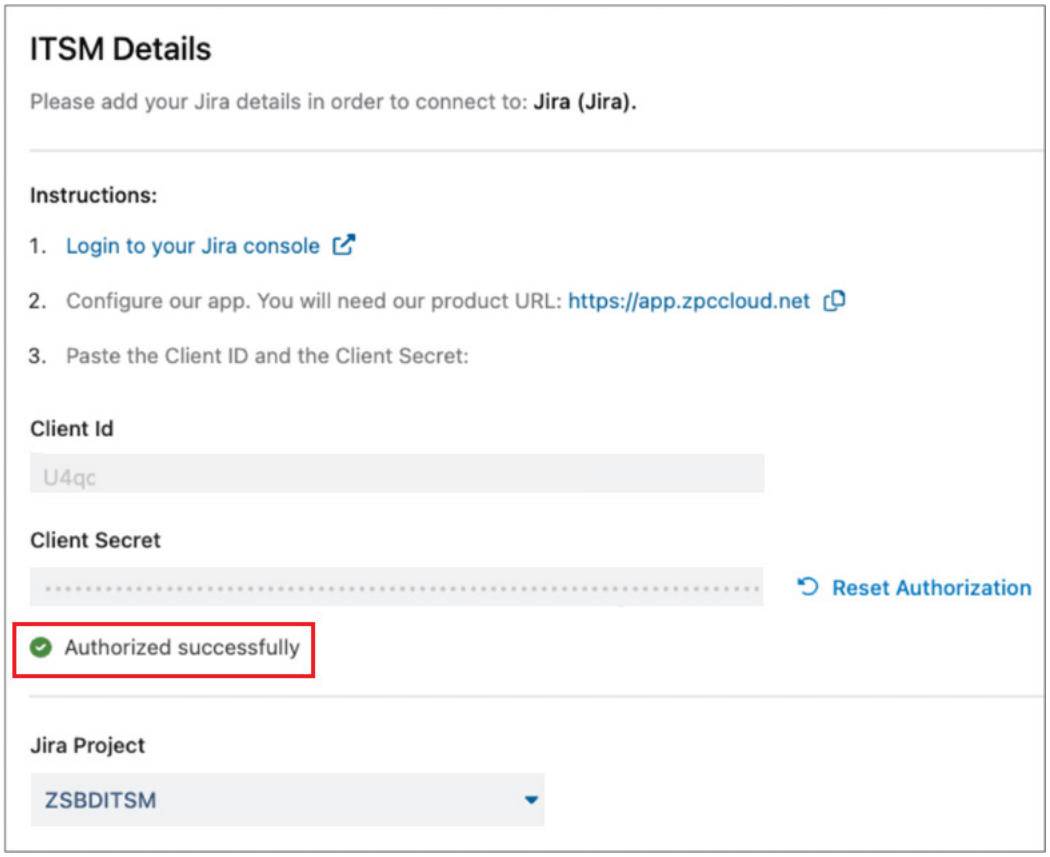

Figure 100. Authorize ZPC to access Jira in Atlassian Admin

7. Select the required **Jira Project** from the drop-down menu.
8. Click **Next**.
9. Review the integration details on the **Summary** page.

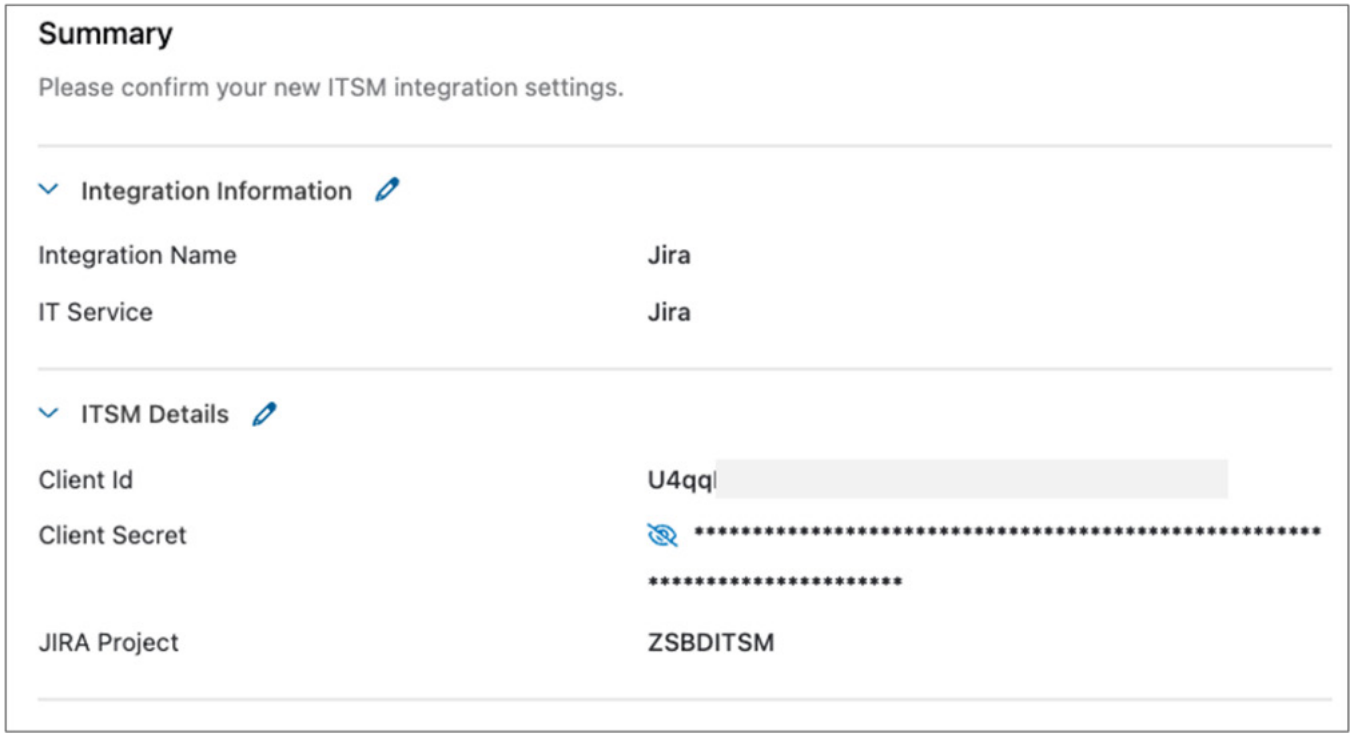

Figure 101. Configuration Summary in Atlassian Admin

10. Click the respective **Edit** icon if you need to make changes.
11. Click **Finish**.

ZPC: Create Jira Notification Rules

ZPC can send notifications to Jira ITSM based on alerts generated due to security and compliance violations in cloud workloads, and IaC.

From the ZPC Admin Portal:

1. Click **Alerts**.
2. Click **Notifications**.
3. Click **Create Rule**.

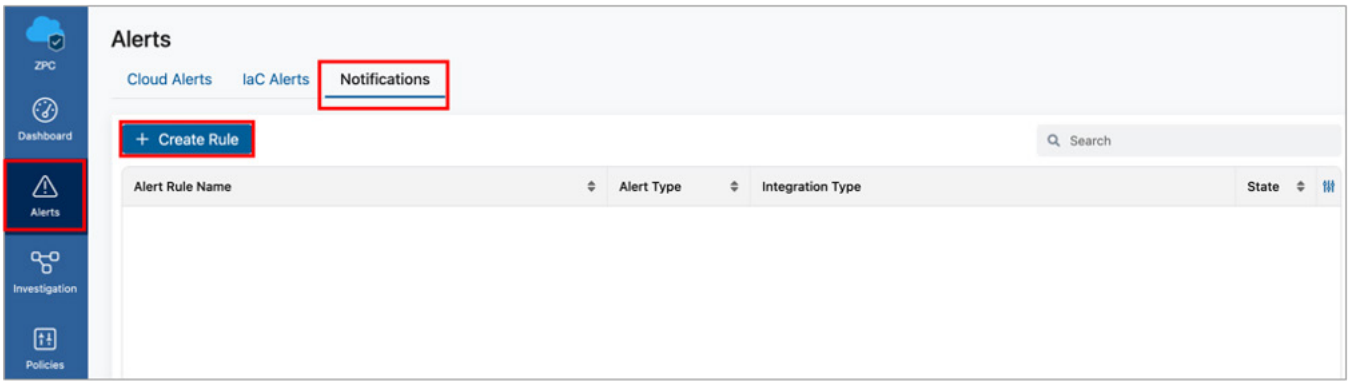

Figure 102. Create alert notification rule

ZPC: Create A Cloud Notification Rule

To create a cloud notification rule:

1. Provide an **Alert Rule Name** to the notification rule.
2. Select **Cloud** in **Alert Type**.
3. Select **Alert Rule Status**.
4. Click **Next**.

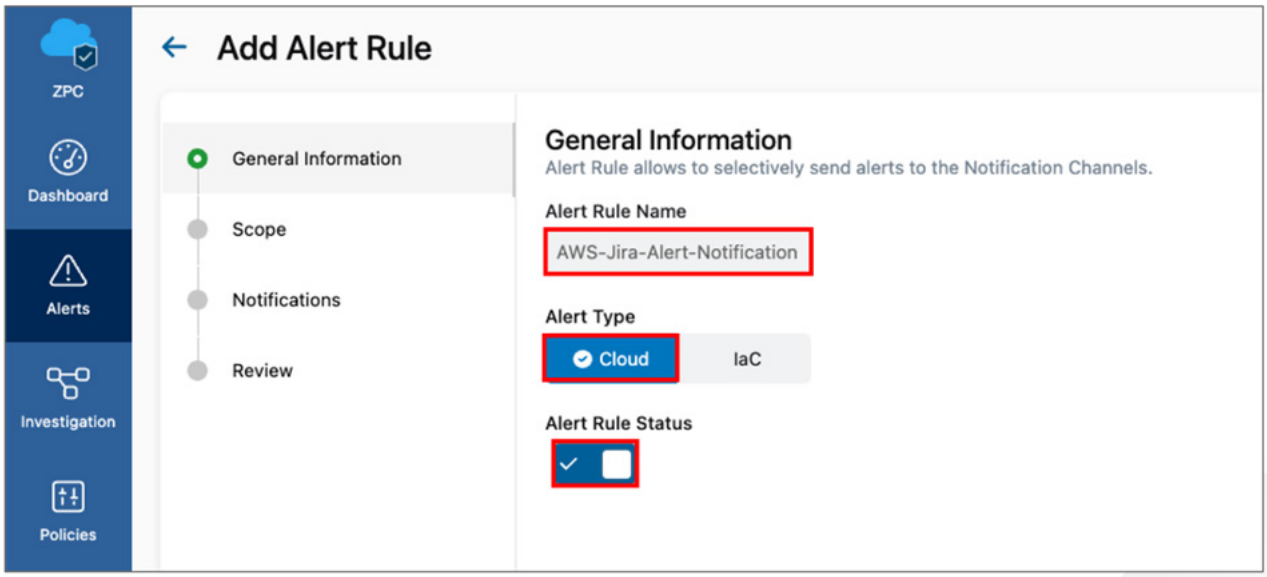

Figure 103. ZPC alert rule general information

5. On the **Scope** page, select the scope you want to receive notifications for. Filter the scope for **Business Units, Clouds, Accounts, and Regions.**
6. In the **Select Policy** section, select the policies whose alerts you want sent to Jira.
7. Click **Next**.

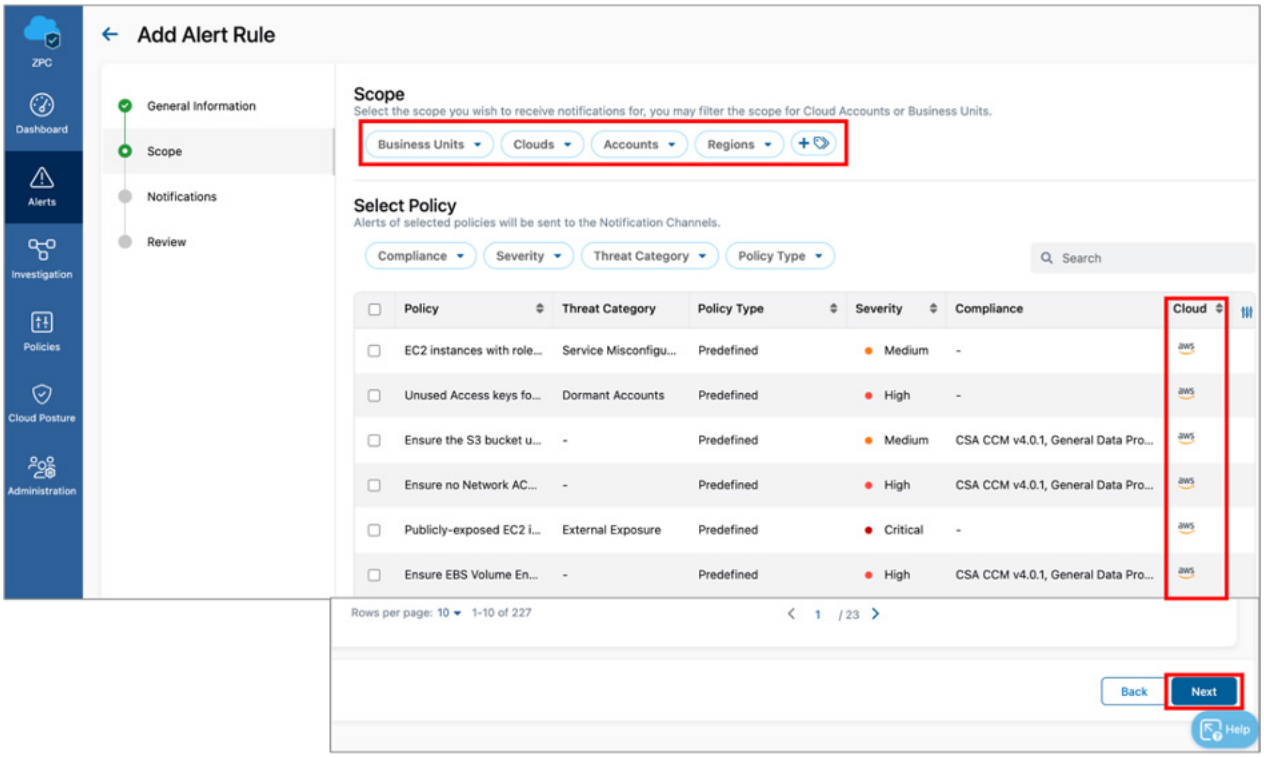

Figure 104. ZPC policy scope

8. In the **Notifications** page:
   a. Select **Jira** in the **ITSM/Ticketing** section.
   b. Select the integration configured in the drop-down menu.
   c. In the **Assignee** field, provide the email address you'd like notifications sent to when an incident is closed or resolved in Jira. Select **Send Notifications for closed Alerts** and/or **Send Notifications for resolved Alerts**.
   d. Click **Next**.

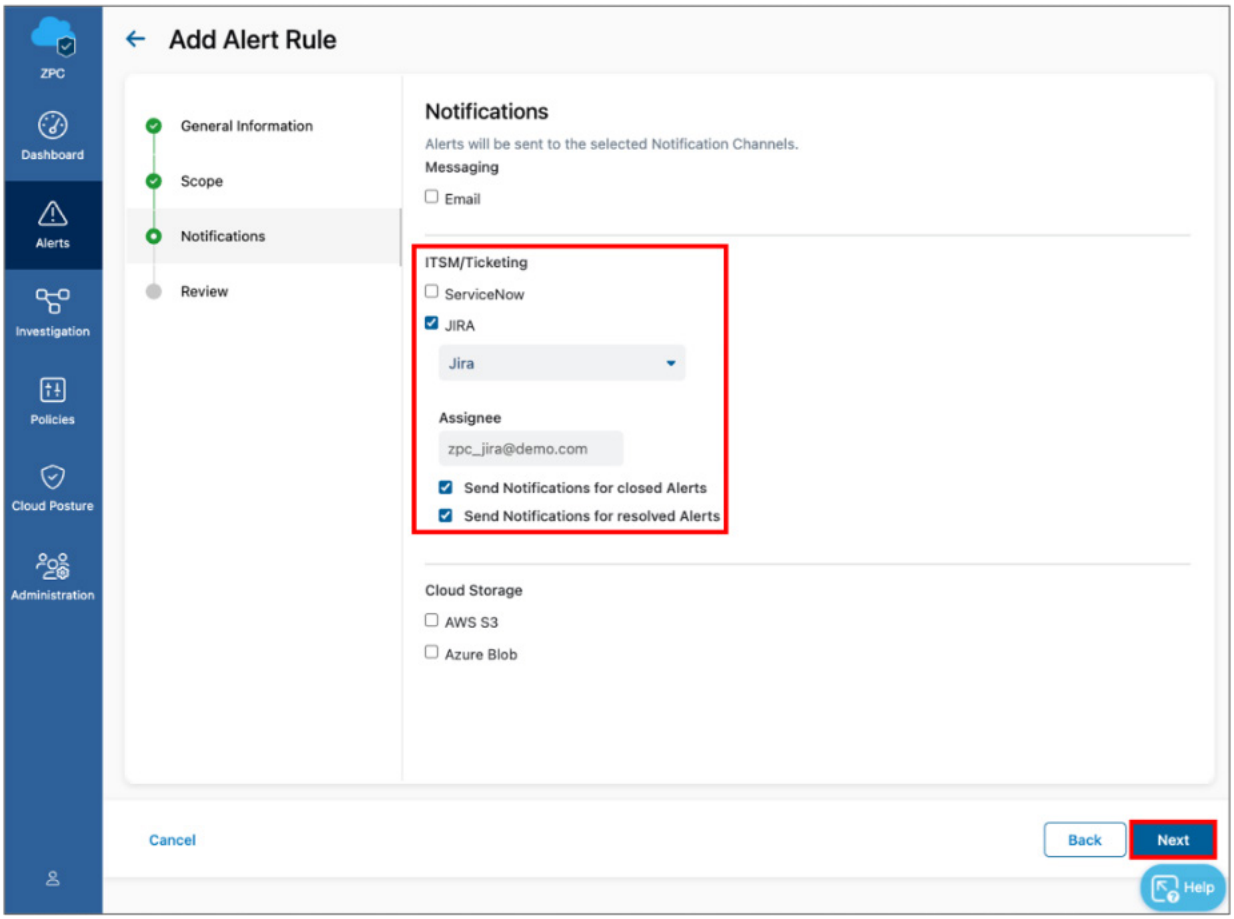

Figure 105. ZPC alert rule notification

ZPC: Create IaC Notification Rule

To create an IaC notification rule:

1. Provide an **Alert Rule Name** to the notification rule.
2. Select **IaC** in **Alert Type**.
3. Select **Alert Rule Status**.
4. Click **Next**.

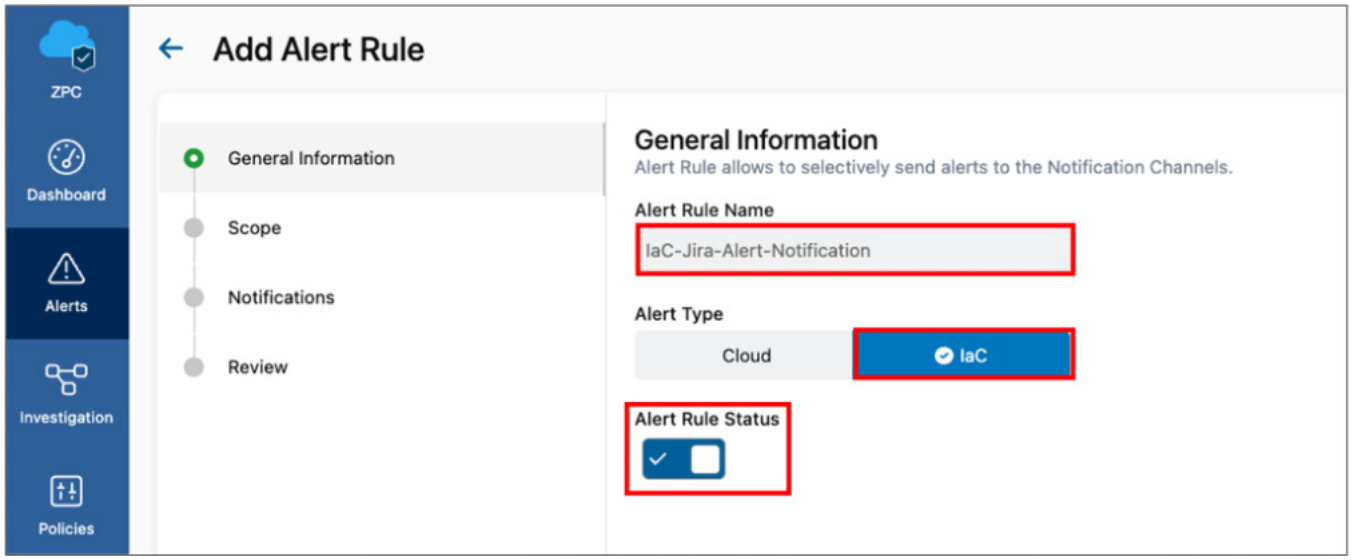

Figure 106. ZPC alert rule general information

5. On the **Scope** Page, select **Scan Plugin**, **Repository,** or both. Alerts associated with Scan Plugins and Repositories are sent to the Jira notification channel:
   - **Scan Plugin**: Provides the following options:
     - GitHub Actions
     - Jenkins
     - GitLab
     - Azure Pipelines
     - Azure Repos
   - **Repository**: Lists all the repositories currently being scanned by Zscaler Posture Control. Select repositories that are to send notifications to Jira via the notification rule.

6. In **Select Policy**, ZPC allows the selection of several different compliance policy values, such as:
    a. CIS (Center for Internet Security)
    b. CSA CCM (CSA Cloud Controls Matrix)
    c. HIPAA
    d. ISO/IEC 27001
    e. NIST SP 800
    f. PCI DSS v3.2.1
    g. SOC 2
    h. Zscaler Best Practices

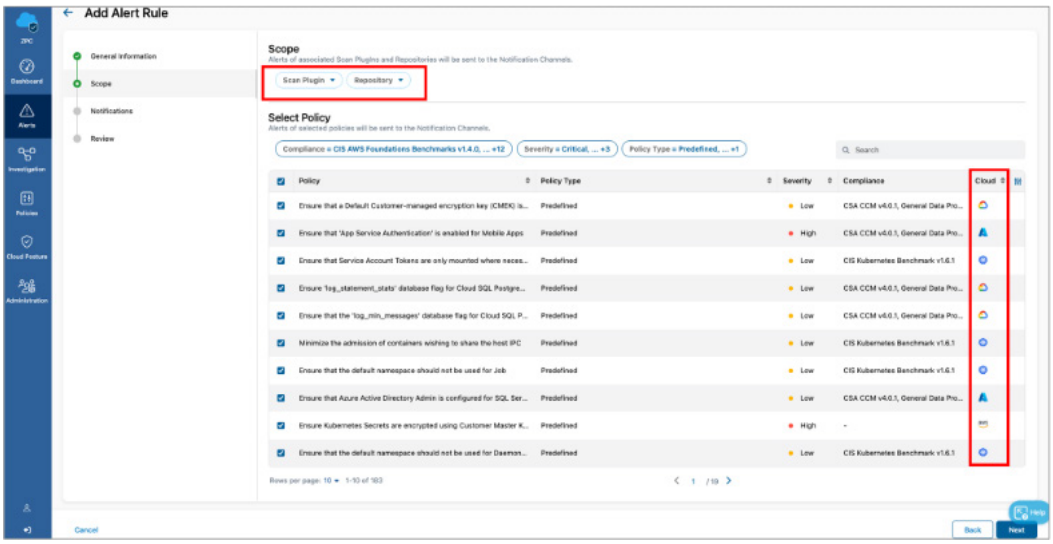

Figure 107. ZPC policy scope

7. In the **Notifications** page:
    a. Select **Jira** in the **ITSM/Ticketing** section.
    b. Select the integration configured in the drop-down menu.
    c. In the **Assignee** field, provide the email address where you'd like notifications sent to when an incident is closed or resolved in Jira. Choose either **Send Notifications for closed Alerts** or **Send Notifications for resolved Alerts**.

8. Click **Next** and then **Finish**.

The alert is displayed in the Notifications page.

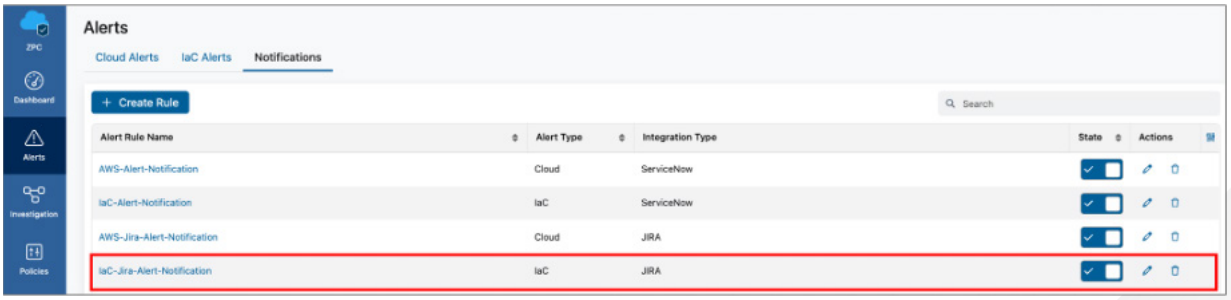

Figure 108. List of alert notifications

ZPC: Jira Incident Management

ZPC creates problem tasks for workflow management of security and compliance violations found in your monitored cloud services and IaC. Jira entries contain the following fields by default (you can apply additional customization).

The Problem task includes:

- Summary: Incident title.
- Description: Detailed description.
- Assignee: The incident is automatically assigned depending on customization.
- Reporter: The system or individual that reported the incident.
- Status: By default, open incidents are in To Do status.
- Resolution: By default, new incidents are Unresolved.
- Created: The date the incident was created.
- Updated: The date the incident was last updated.

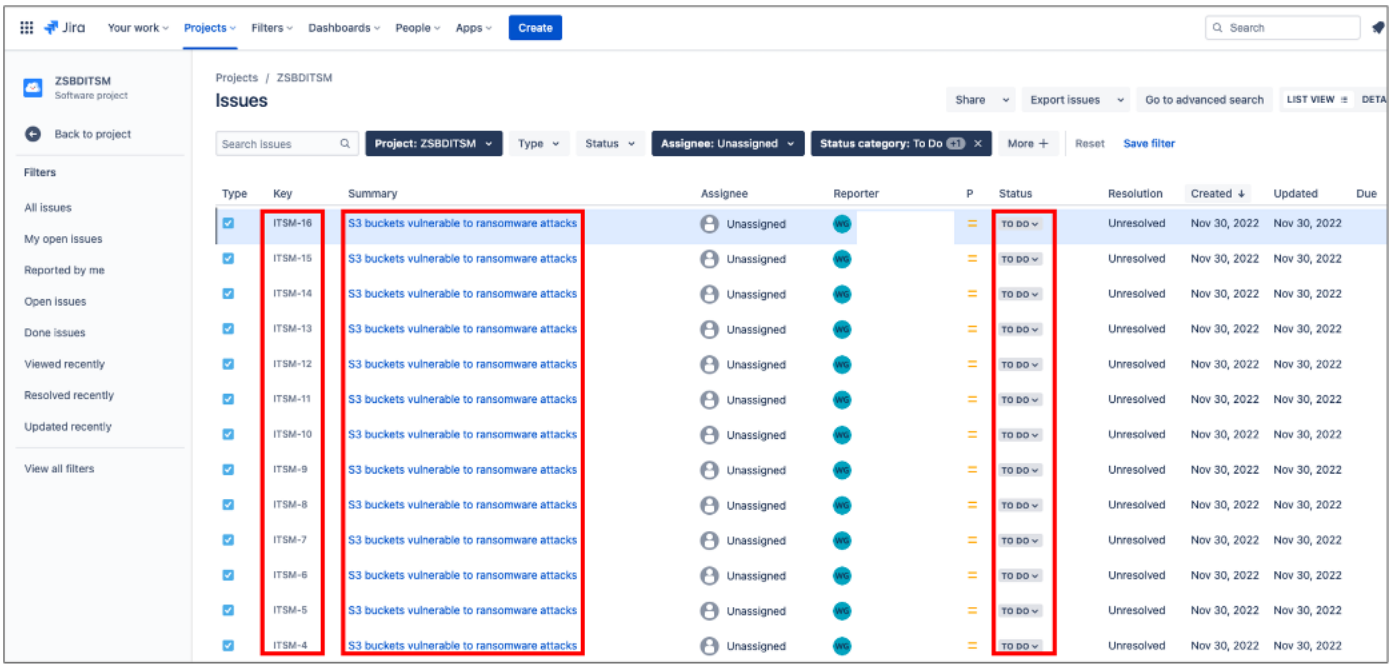

Figure 109. ZPC incidents in Jira

ZPC: Jira Incident Detail

ZPC sends detailed alert description information to Jira. In the following example, the incident is related to AWS S3 buckets being vulnerable to potential ransomware attacks.

Notice that the severity level of the incident in this case matches the **Priority** field in Jira.

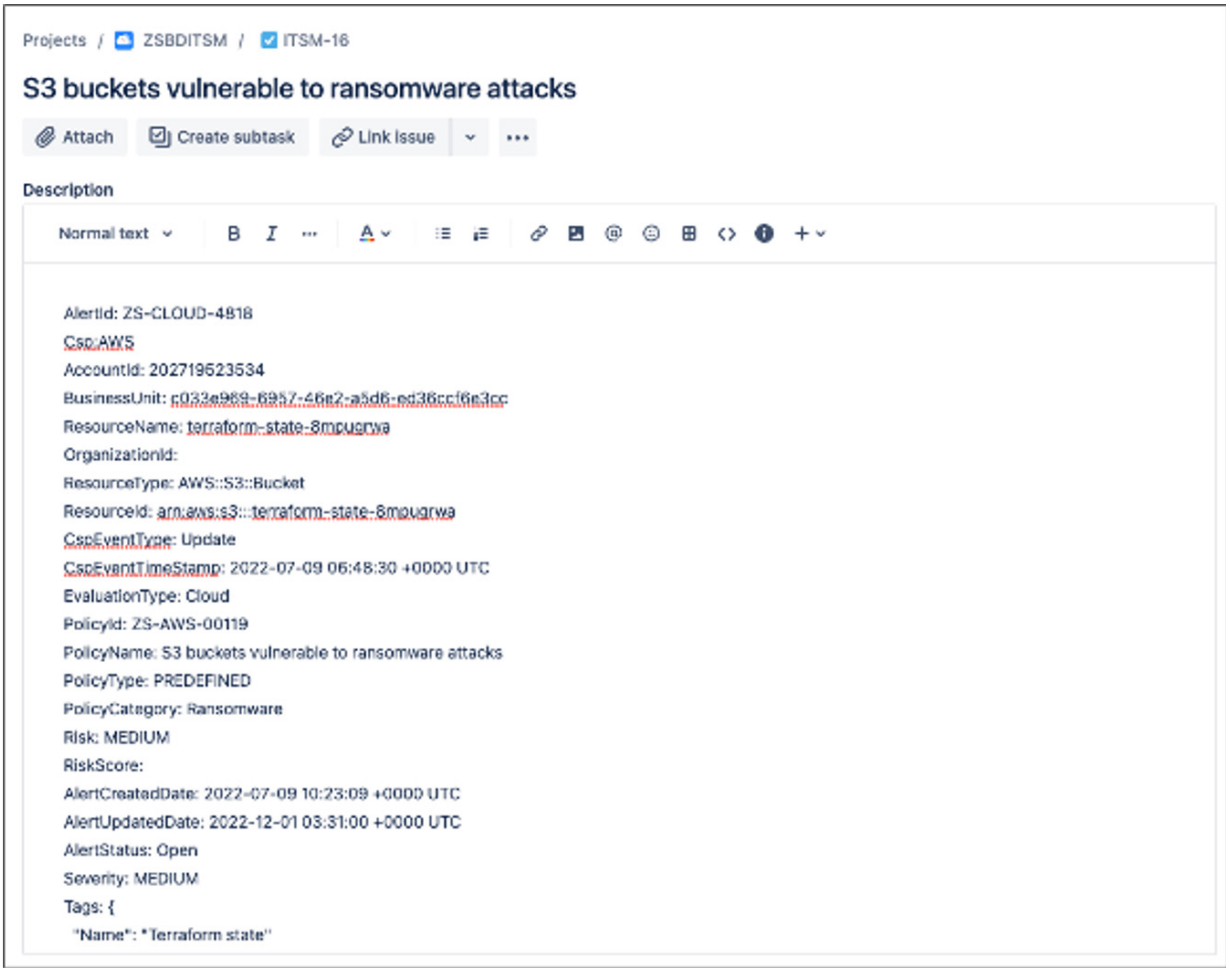

Figure 110. Detailed ZPC incident in Jira

ZPC for Bitbucket

The following sections are an overview of the ZPC and Bitbucket described in this deployment guide.

Version Control and CI/CD Systems

ZPC offers the Zscaler IaC Scan security feature that enables you to apply security controls on your IaC infrastructure before deployment. The IaC Scan tool scans the IaC templates for misconfigurations and known vulnerabilities that are a potential risk for attacks. The IaC Scan tool leverages more than 100 security policies to check for configuration errors in your code (e.g., missing database encryption, publicly exposed services, etc.) so you can remediate these errors and ensure your code is secure and compliant with the security policies. To learn more, see About Security Policies.

You can integrate the IaC Scan with various code repositories, continuous integration (CI) and continuous deployment/delivery (CD) tools, and integrated development environments (IDEs). The IaC Scan is also available as a command line interface tool.

Software entitlements are products that you are allowed to use. You can subscribe to the Zscaler IaC Scan service. If the software entitlement expires, or if you've removed or downgraded the subscription (e.g., reverted from ZPC-Advanced to the ZPC-Essential version), then you cannot perform the IaC scan.

About Security Policies

Security policies protect your cloud deployment from asset misconfigurations and excessive permissions by defining a condition or parameter for how a particular cloud asset must be configured. ZPC offers over 400 security policies across multiple cloud service providers (CSPs), including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. ZPC has created security policies to protect both your runtime and build time environments. You cannot modify the security policies, but you can create new custom security policies tailored for your cloud deployment.

ZPC also bundles security policies to emulate cybersecurity benchmarks (e.g., NIST) or compliance benchmarks (e.g., GDPR).

The Policies page provides the following benefits and enables you to:

- View all cloud and IaC policies offered by ZPC.
- Gain cloud posture overview based on whether the policies are passing or failing for your cloud deployment.
- Create custom security policies to cater to your cloud deployment's compliance requirements.

Prerequisites

The administrator with an owner role can onboard the Bitbucket accounts and authorize the IaC Scan app to scan the IaC repositories.

Configuring IaC Scan for Bitbucket

ZPC provides support for integrating the Zscaler IaC Scan with Bitbucket to scan your IaC templates in Bitbucket repositories. It continuously verifies security misconfigurations against ZPC security controls and displays the failed checks.

The Bitbucket integration allows you to perform IaC scans of the Bitbucket repositories on pull and push requests. You can perform an IaC scan on the entire repository of a branch or templates that were newly added to the branch. The scan results are displayed within Bitbucket, providing visibility into the IaC policy violations.

You can configure only one Bitbucket integration per tenant.

1. Go to **Administration** > **Version Control & CI/CD Systems**.
2. On the **Version Control & CI/CD Systems** page, click **Add IaC Integration**.

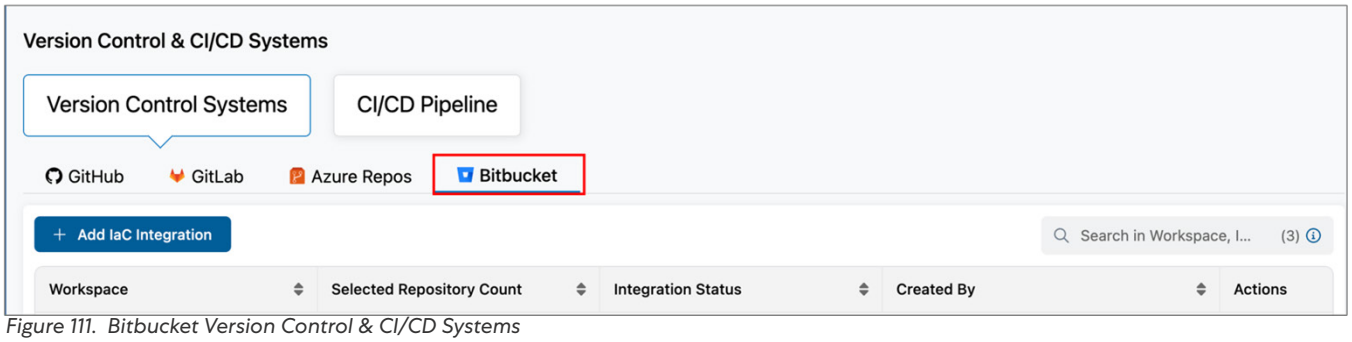

Figure 111. Bitbucket Version Control & CI/CD Systems

3. Under **General Information**:
   a. For **IaC Scanner Type**, select **Code Repository**.
   b. For **Platform**, select **Bitbucket**.

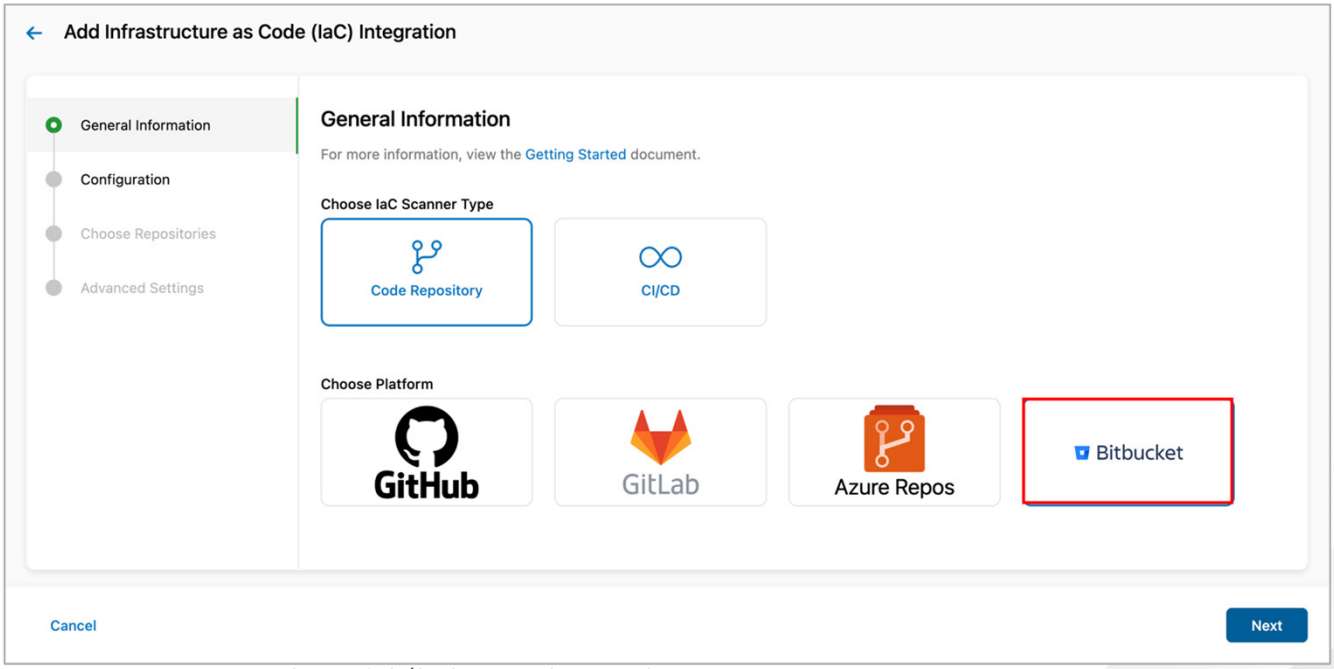

Figure 112. Bitbucket Version Control & CI/CD Systems—General Information

4. Click **Next**.

5. Under **Configuration**, click **Authorize app from Bitbucket**.

   The **Bitbucket Sign-in** page appears. If you are already logged in to Bitbucket, then install the **Zscaler IaC Scan** in the required workspace.

6. Otherwise, sign in to your Bitbucket account.
7. Install the **Zscaler IaC Scan**.

> Only an administrator can install and authorize the IaC Scan. Zscaler recommends that you select All repositories so you can later onboard subsequent repositories directly from the ZPC Admin Portal.

8. Click **Install & Authorize**. After completing the installation, you are returned to the ZPC Admin Portal.

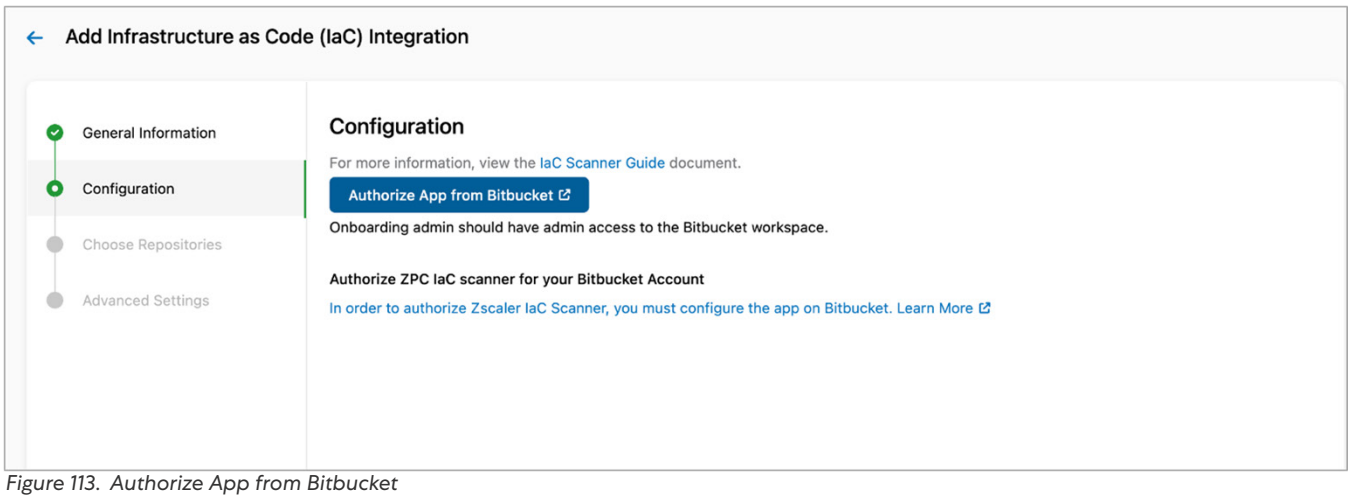

Figure 113. Authorize App from Bitbucket

9. In the Bitbucket authorization portal:
    a. Select the workspace to be authorized.
    b. Click in **Grant Access**.

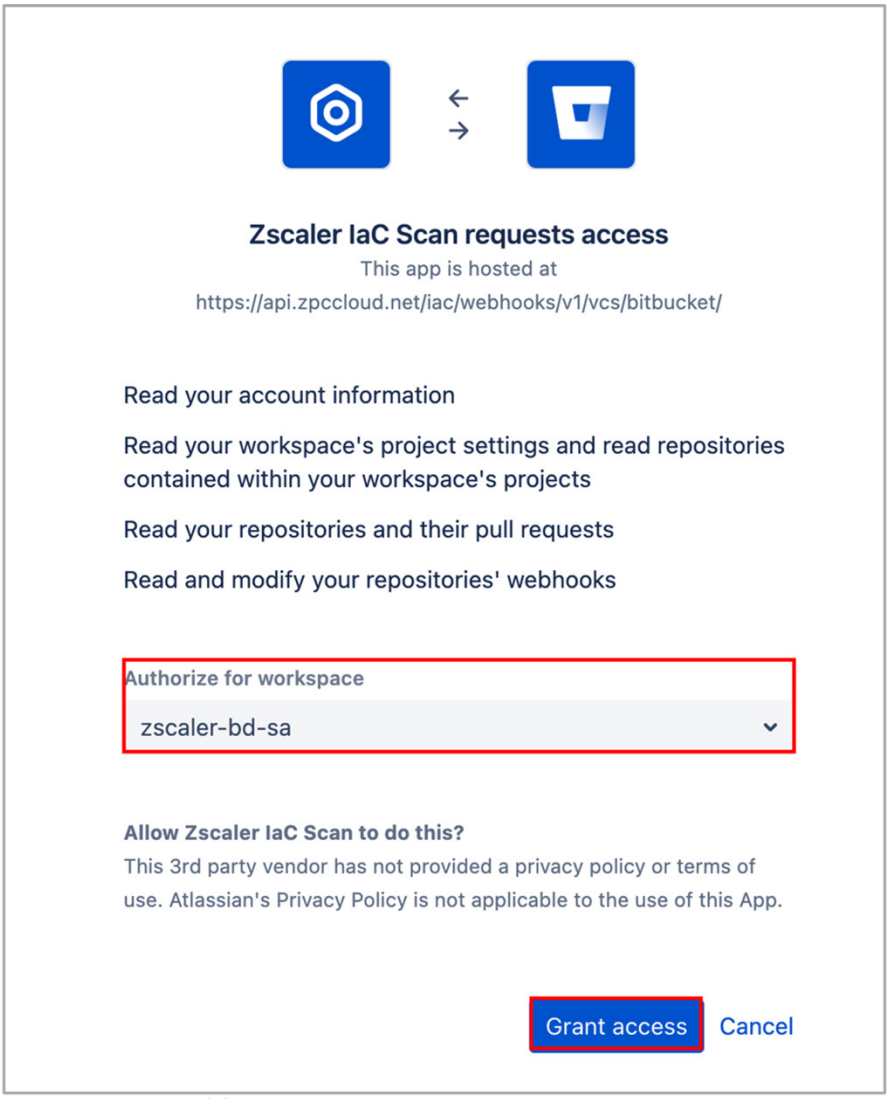

Figure 114. Zscaler IaC Scan access request

10. Under **Choose Bitbucket Repositories**, select the checkbox for the repositories that must be enabled for scanning.

> The date and time format displayed is based on the browser locale.

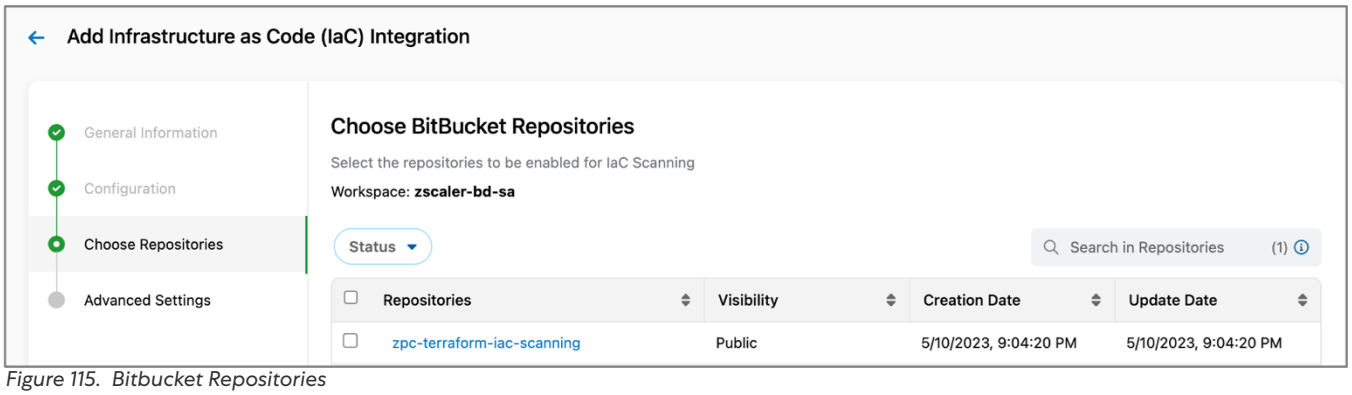

Figure 115. Bitbucket Repositories

11. Click **Next**.

12. (Optional) Under **Advanced Settings**:
    - **Scan on Push**: Click the toggle to scan the code for a push command. The IaC Scan app performs the scan in the background and triggers alert notifications for any policy violations and displays the alerts in the ZPC Admin Portal. To learn more, see About Alerts.
    - **Include Paths**: Click **Edit** to include the path of the specific folder within the repository that must be scanned. For example, if you define an *include* path for a single file, then only that file is scanned and all other files and folders within the repository are ignored. You can also use regular expressions (regex) to search for and include files or folders that must be scanned.

Regex Pattern	Description	Example
/**/	Match zero or more directories	If you type charts/**/, then the following files are included: • charts / docker.yml • charts / stub • charts / stub / config.yml • charts / server / config / app1 / app.yml
**/	Match any directory/ directories, start of pattern only	If you type **/internal/test/**, then the following files are included: • root/internal/test/stub.txt • internal/test/stub.txt • /internal/test/server • root/internal/test
/**	Match any directory/ directories, end of pattern only	If you type monorepo/**/terraform/**, then the following files are included: • monorepo/terraform/doc.tf • monorepo/app1/terraform • monorepo/app1/terraform/stub.yml • monorepo/app1/app2/terraform
*	Match any non-separator character	If you type *repo/**/terraform/**, then the following files are included: • monorepo/terraform/doc.tf • monorepo/app1/terraform • publicrepo/app1/terraform/stub.yml • newrepo/app1/app2/terraform
!	Excludes all matches from the result set, start of pattern only	If you type !**/internal/test/**, then the following files are excluded: • root/internal/test/stub.txt • internal/test/stub.txt • /internal/test/server • root/internal/test

- **Fail Check Criteria**: Fail check criteria is applicable to only pull requests based on policy severity. Select the security threshold (Critical, High, Medium, or Low) for the policy from the drop-down menu.

You can apply a security threshold to each repository. For example, you can fail a pull request that introduces Critical or High issues from a repository that is used to deploy to a production environment. If the same pull request has a Low threshold and the code is merged to a repository that is used to deploy in a development environment, then you can pass the request. However, the alert notification is generated in both scenarios.

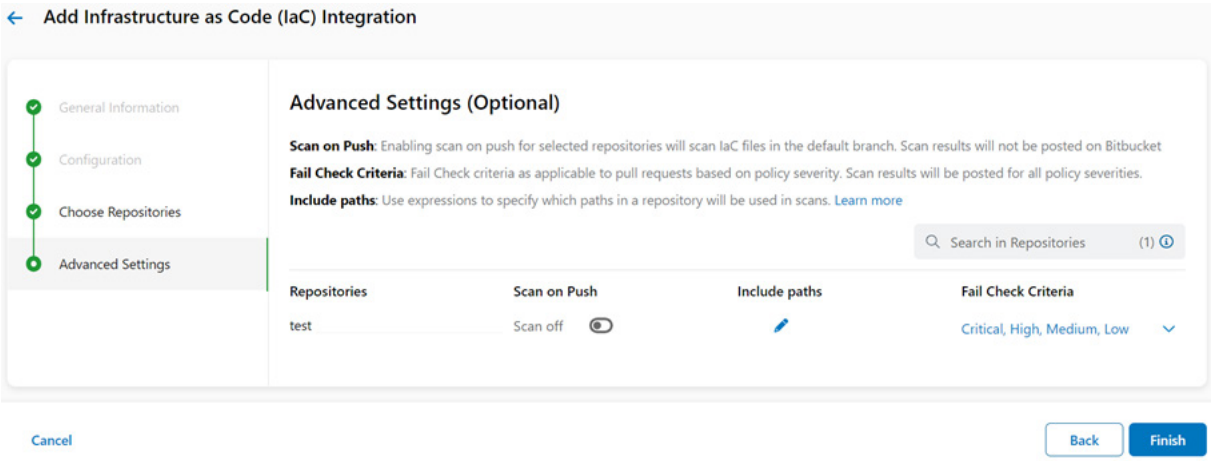

Figure 116. Bitbucket Advanced Settings

13. Click **Finish**.

Viewing the IaC Scan Summary in Bitbucket

After you enable the selected repositories for scanning, the Zscaler IaC Scan app performs a scan every time you add or update a code and make a merge request. The IaC Scan app identifies security misconfigurations and displays policy violations and remediation steps within the code. You can fix the issues and then merge the code.

You can see the total policies along with passed and failed findings. This information indicates if the code is violation-free for the policies evaluated or if none of the policies were evaluated for this resource. You can see the policy title and ID, severity, and resource details after the line of code that has issues.

To view the scan summary report in the Bitbucket pull request:

1. Select the repository where the new pull request was created.
2. Go to **Pull requests**.
3. Select the new pull request.

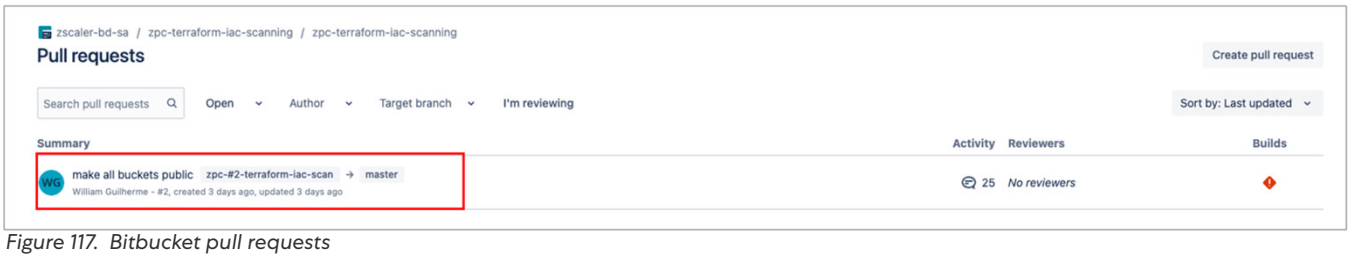

Figure 117. Bitbucket pull requests

4. Review the **Scan Summary Report**.

Figure 118. Zscaler IaC Scan results

Viewing Specific IaC Scan Summary in Bitbucket

In addition to the scan summary, the Bitbucket integration with ZPC provides visibility and details on specific alerts.

Bitbucket allows you to take the following actions in an alert:

- Resolve. The alert has been resolved
- Create Task. Create a task related to the alert
- Create Jira Issue. Bitbucket integrates with Jira so an incident can be created for further investigation

To resolve a specific alert via the Bitbucket portal:

1. Select **Resolve**.
2. Enter a comment to the thread.

Figure 119. Zscaler IaC Scan Results

Viewing the IaC Scan Summary in the ZPC Admin Portal

To visualize the Bitbucket alerts generated by the Zscaler IaC Scan tool:

1. Login to the ZPC Admin Portal.

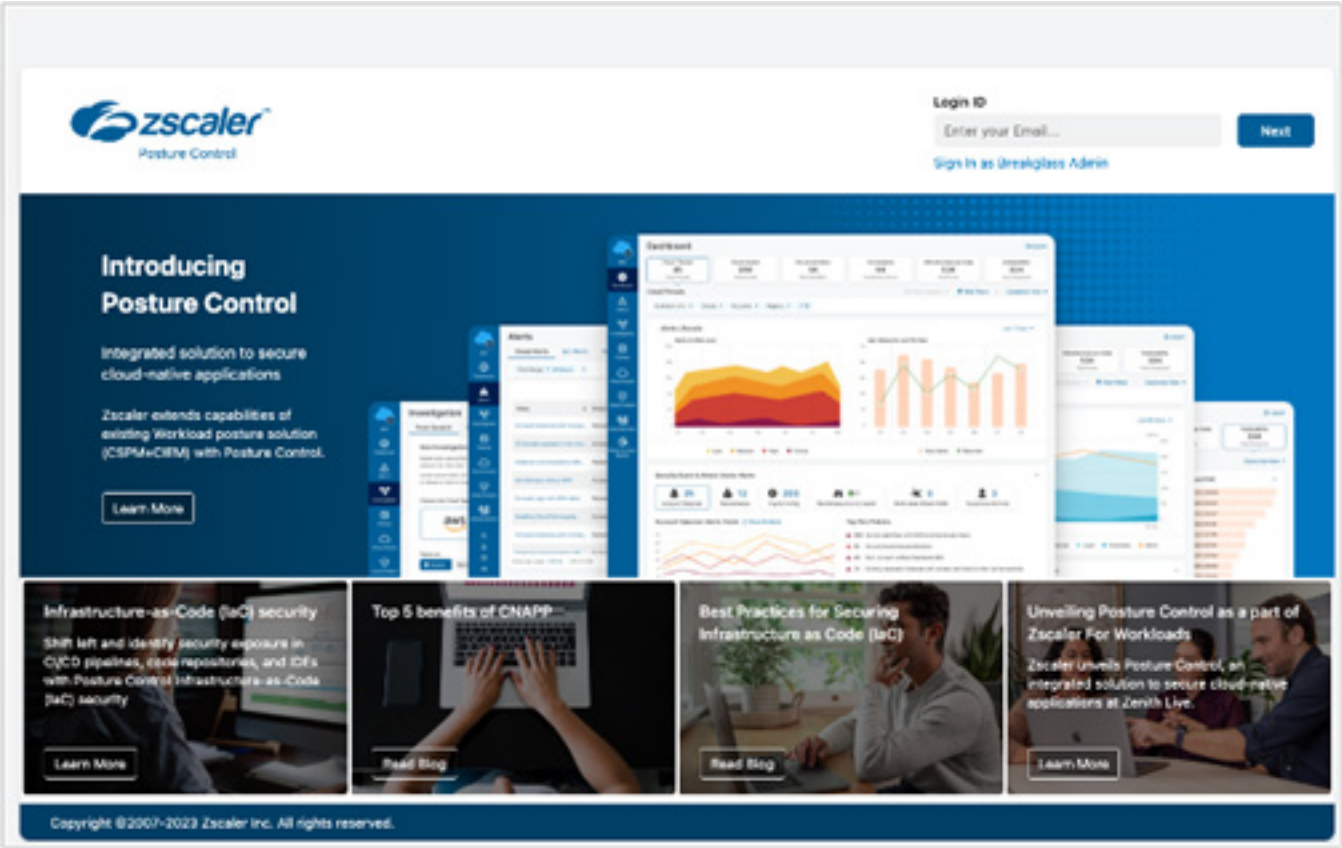

Figure 120. ZPC Administrator portal

2. Select **Infrastructure as Code**.

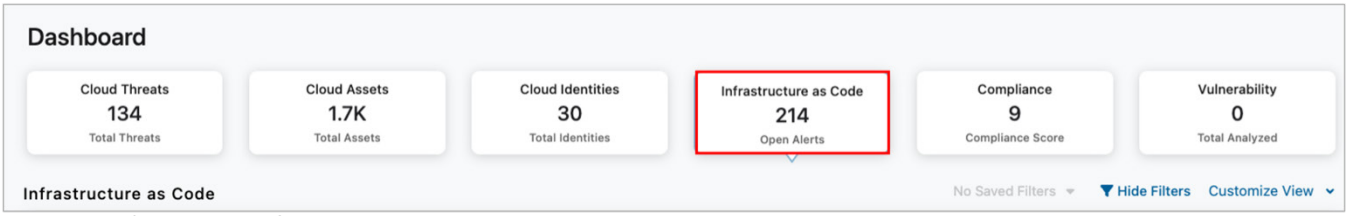

Figure 121. Infrastructure as Code widget

3. In the main **Infrastructure as Code** dashboard, Zscaler provides a summary of the following:
   a. **Policy Violations identified via Scan Plugin**.
   b. **Top Policy Violations**.
   c. **Policy Violations via Cloud Type**.

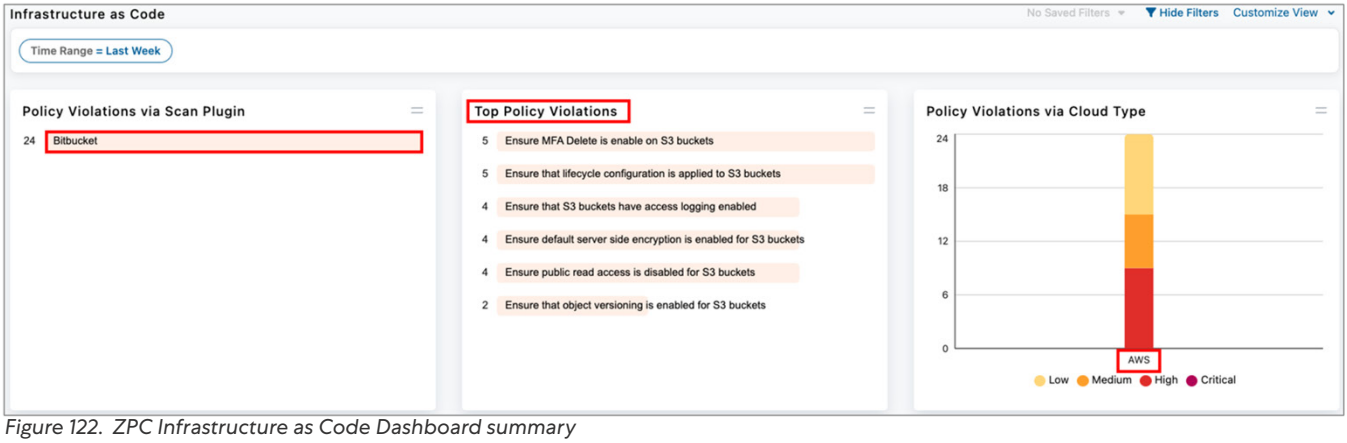

Figure 122. ZPC Infrastructure as Code Dashboard summary

4. Select one of the **Top Policy Violations**. In this example, **Ensure MFA Delete is enabled on S3 buckets** is selected.

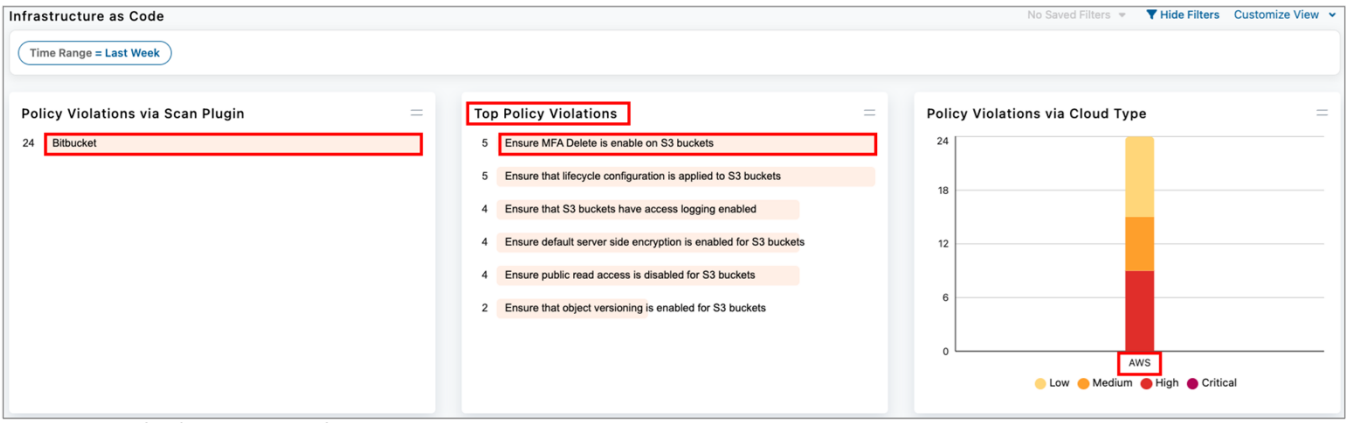

Figure 123. ZPC Infrastructure as Code Top Violations

5. The administrator can also group the IaC alerts by scan type. In the following example, the filter only displays **Scan Plugin = Bitbucket**.
   a. Other filters are also available (e.g., **Scan Time**, **Alert Status**, **Cloud**, and **Repository**).
   b. You can add other filters by selecting the Add icon (+) in the filter area.

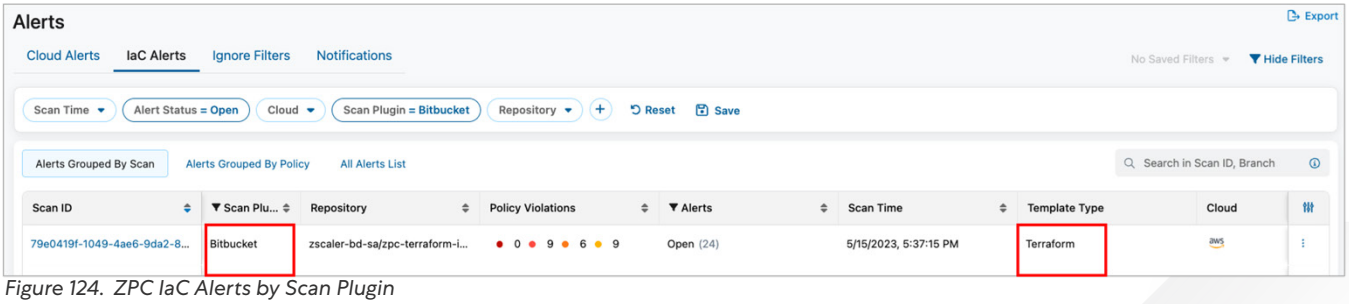

Figure 124. ZPC IaC Alerts by Scan Plugin

6. (Optional) Select the top violations and ZPC automatically creates an IaC alerts filter containing all violations originated by the Bitbucket scan plugin.

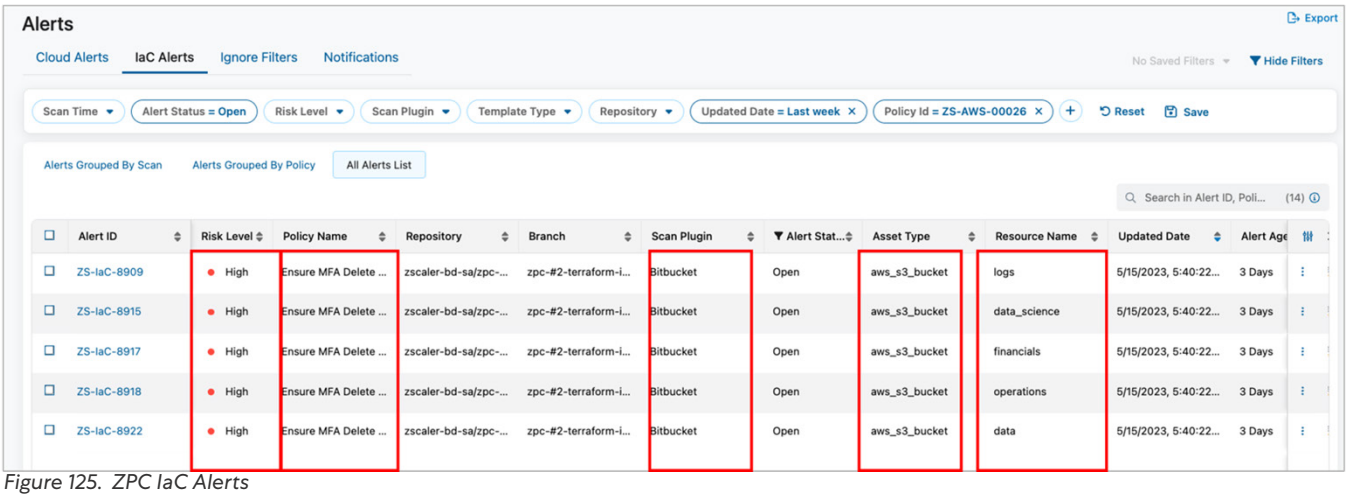

Figure 125. ZPC IaC Alerts

7. Select one of the alerts listed in the left-side **Alerts** column. This example selects the alert ID **ZS-IaC-8909**, which indicates that ZPC have detected violation associated with a **Policy ID: ZS-AWS-00026**. This policy detects whether the S1 bucket has the MFA Delete feature enabled.

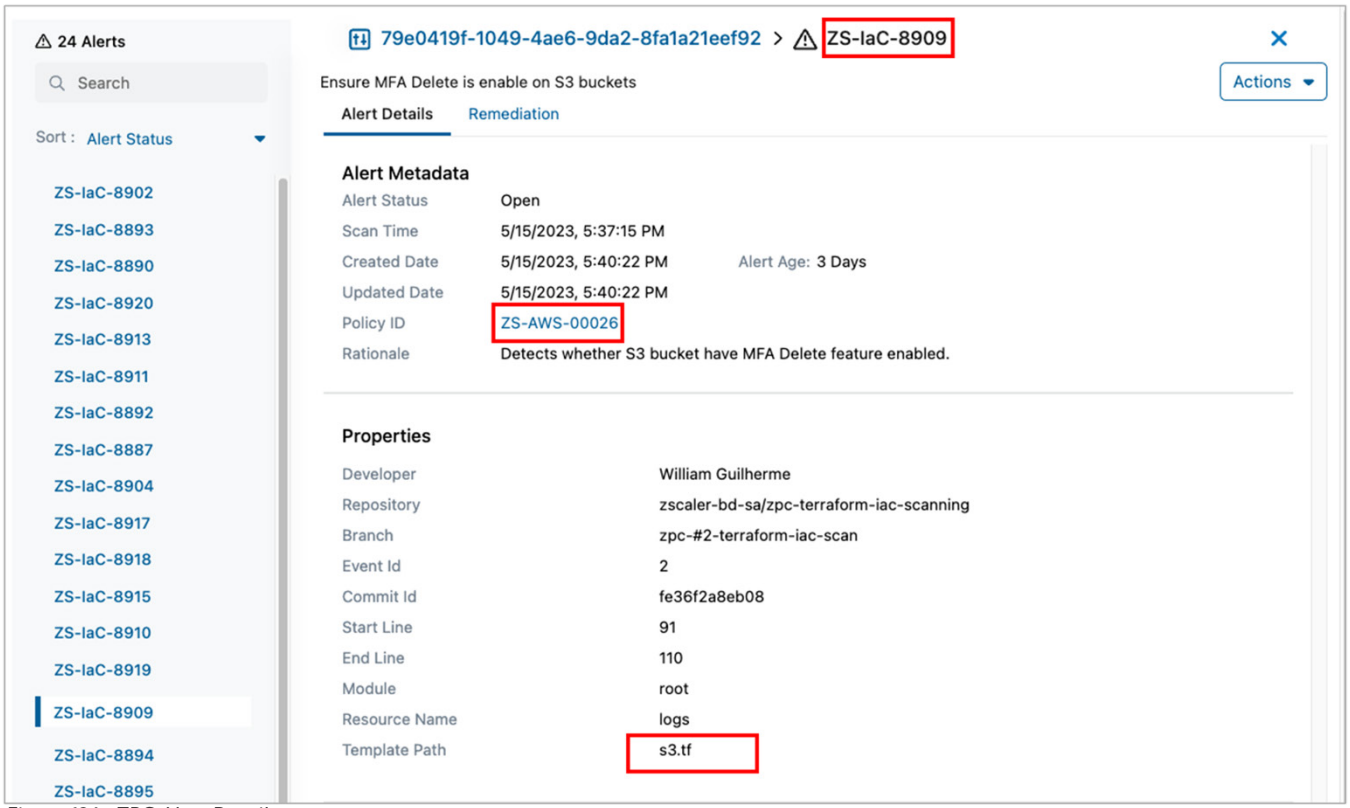

Figure 126. ZPC Alert Details

8. See the code snippet with information about the **Violating resource**.

Figure 127. ZPC Violating Resource

9. To remediation recommendation procedures, select the **Remediation** tab.

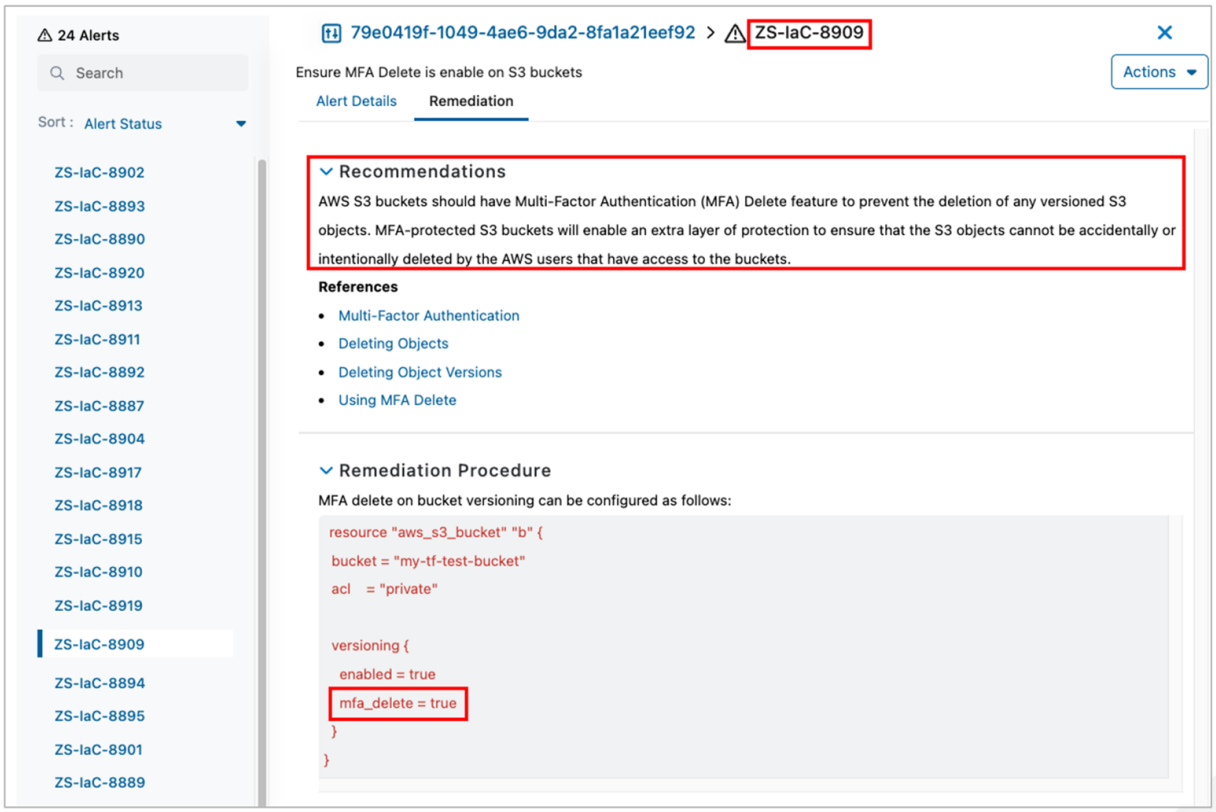

Figure 128. ZPC Remediation

10. To resolve or ignore the alert, select **Actions**, and then select **Resolve** or **Ignore**. This example uses **Resolve**. The **Resolve Alert** screen is displayed.

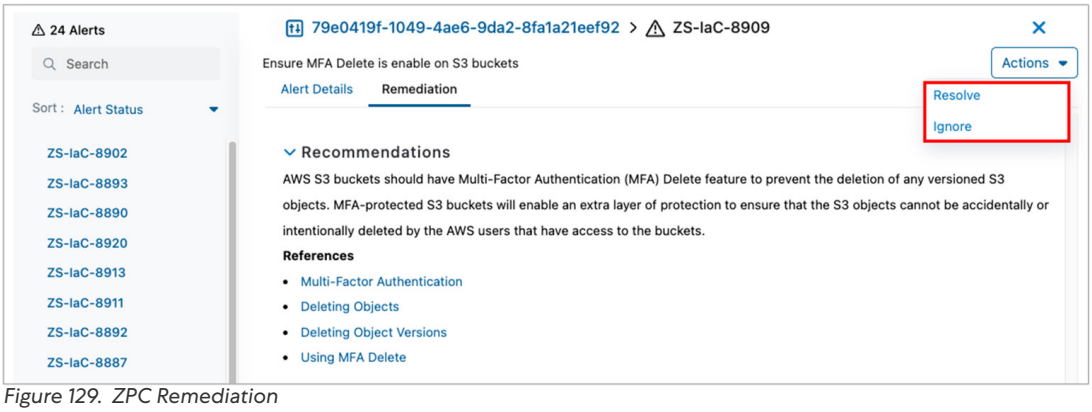

Figure 129. ZPC Remediation

11. Enter a reason to resolve the alert.
12. Click **Resolve**.

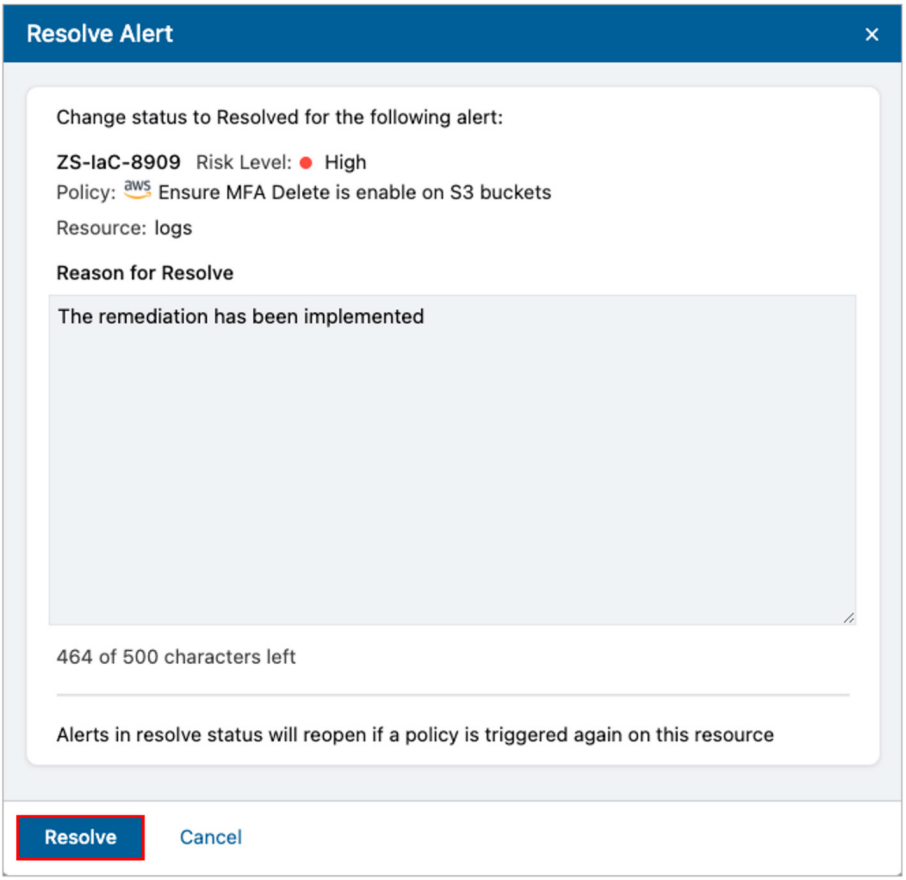

Figure 130. ZPC Resolve Alert

Resolved alerts reopen if a policy is triggered again on this resource.

To learn more, see the Zscaler Posture Control IaC Scanning and Bitbucket Integration demonstration and Zscaler IaC Scan – Atlassian Marketplace.

Appendix A: Requesting Zscaler Support

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

Depending on the Zscaler application, there are different methods of contacting Zscaler Support.

Requesting Zscaler Support via ZIA

To contact Zscaler Support

1. Go to **Administration** > **Settings** > and then click **Company Profile**.

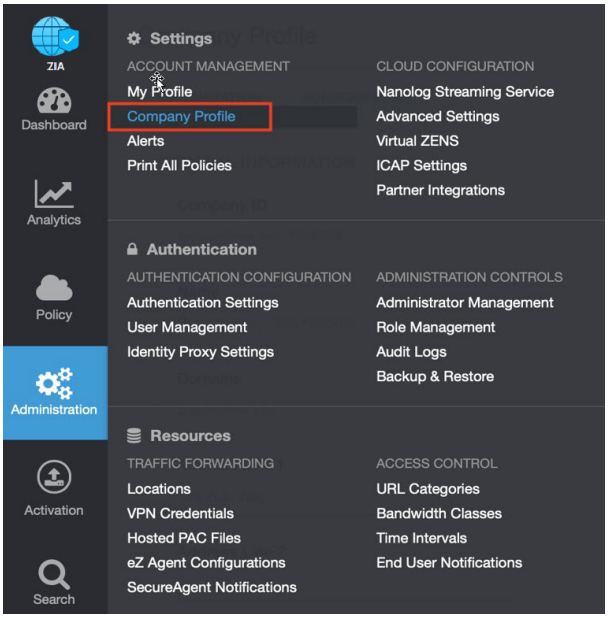

Figure 131. Collecting details to open support case with Zscaler TAC

2. Copy the Company ID.

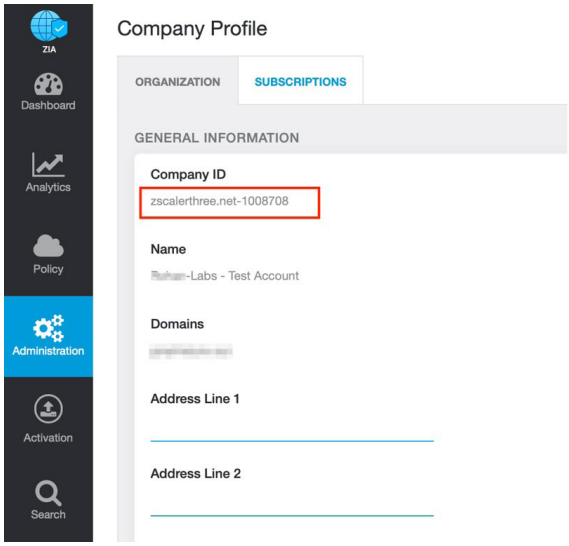

Figure 132. Company ID

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

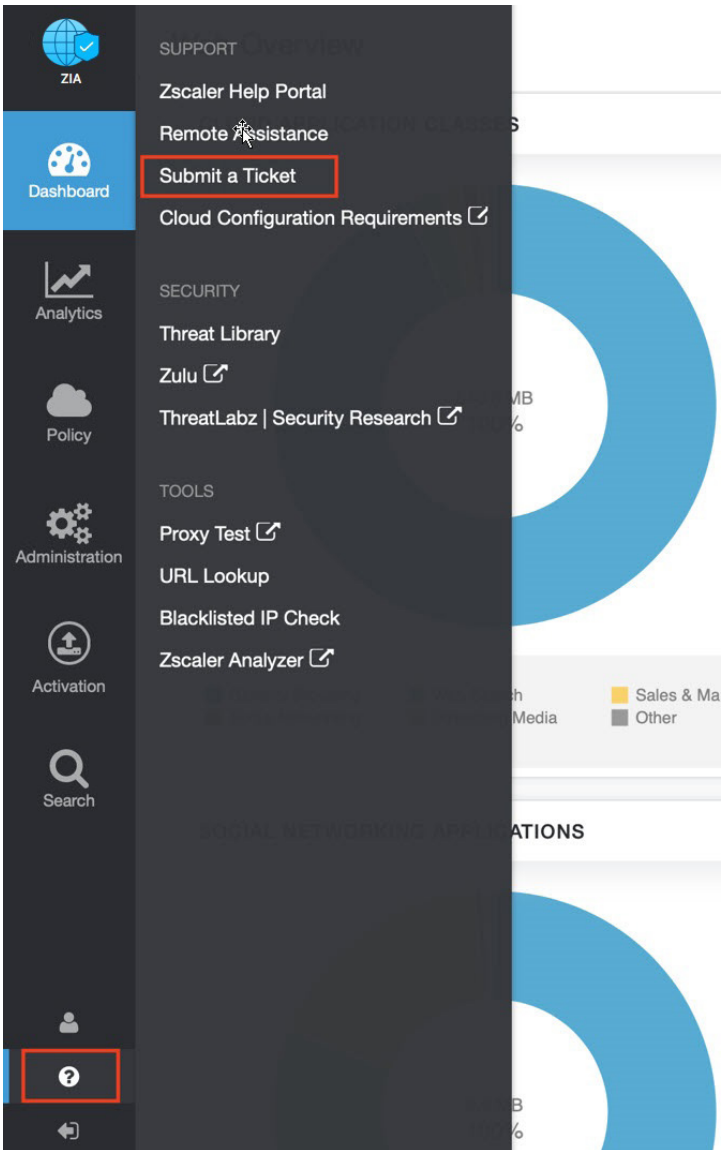

Figure 133. Submit a ticket

Requesting Zscaler Support via ZPC

If you need Zscaler Support for provisioning certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to the ZPC help and select **Support** from the left-side navigation.
2. Select **Submit Ticket**.

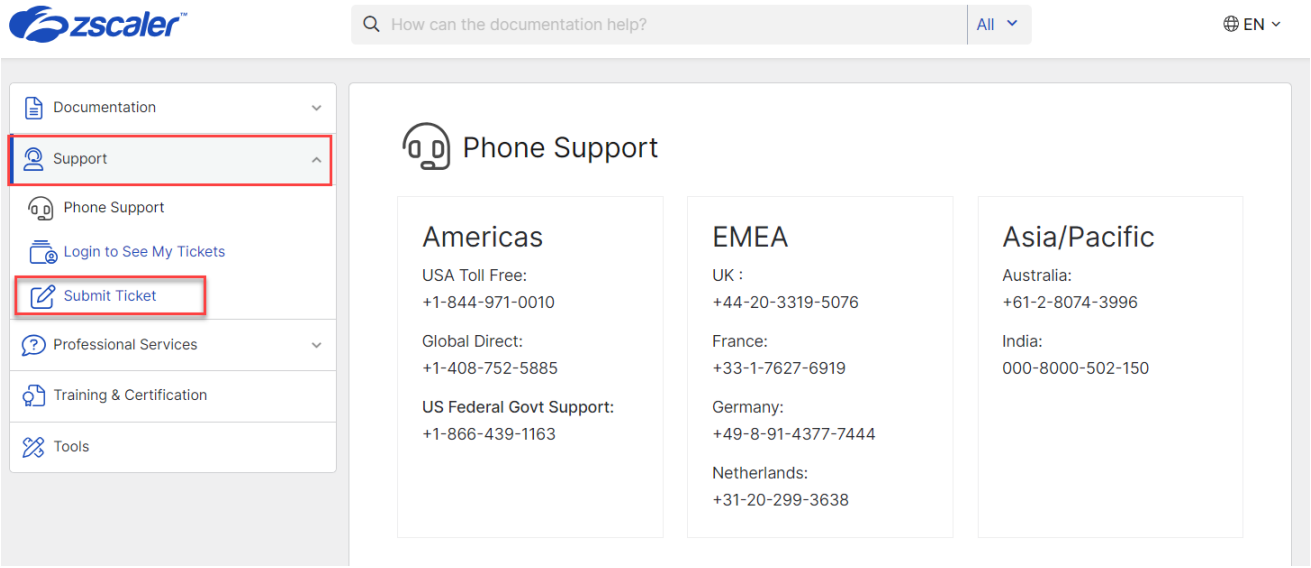

Figure 134. ZPC Help

3. In the **Submit Ticket** window, select **Submit Ticket for Posture Control (ZPC)**.

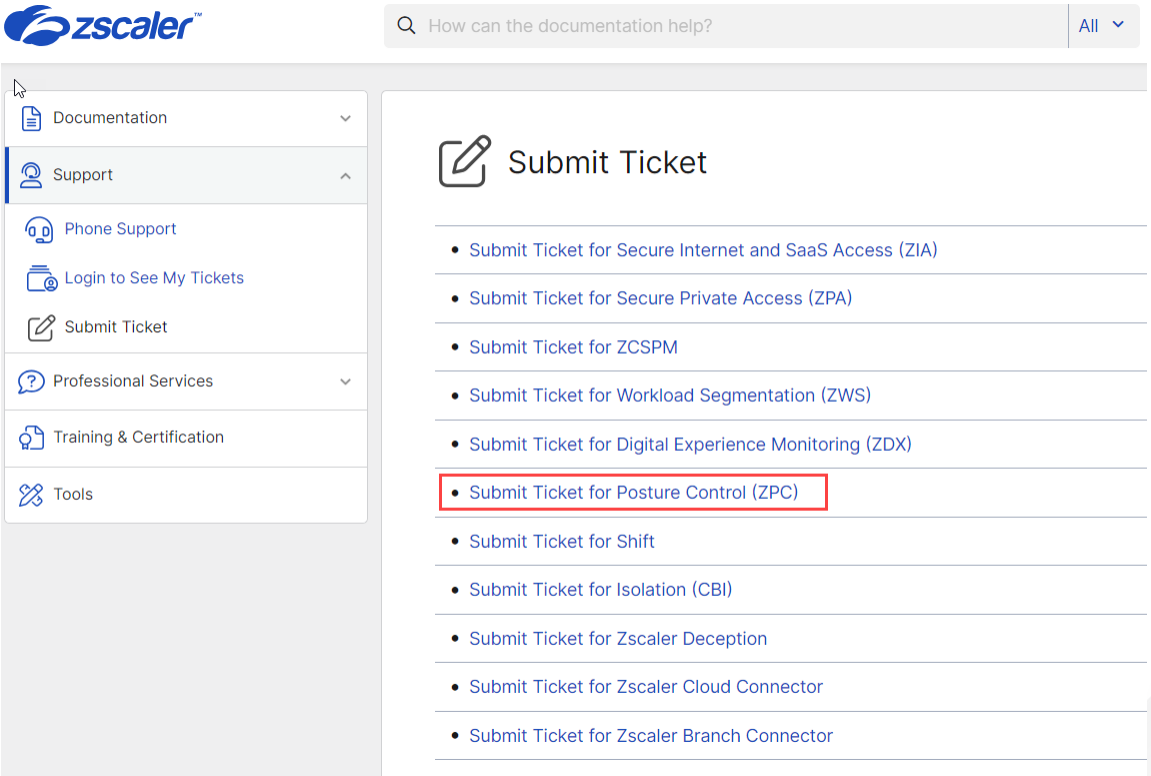

Figure 135. ZPC Support

4. In the **ZPC - Submit Ticket** window, fill in the required fields.

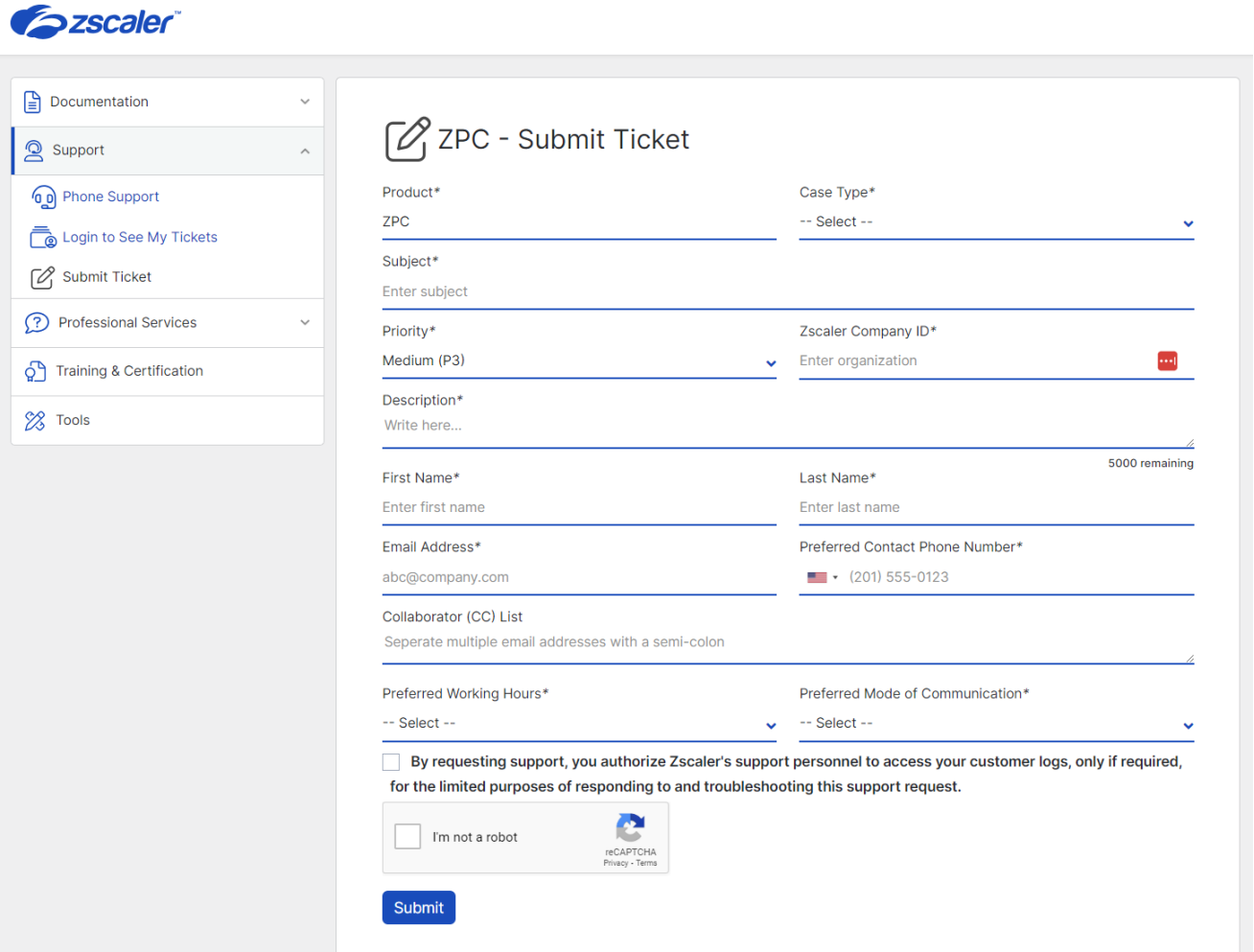

Figure 136. Submit ZPC ticket

5. Select the reCAPCHA checkbox, and click **Submit**. A Zscaler Support representative contacts you via the submitted contact information within 24 hours.

