ZSCALER AND GITLAB DEPLOYMENT GUIDE

AUGUST 2023, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

©2024 Zscaler, Inc. All rights reserved.

©2024 Zscaler, Inc. All rights reserved.

©2024 Zscaler, Inc. All rights reserved.

Terms and Acronyms

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

Acronym	Definition
API	Application Programming Interface
AWS	Amazon Web Services
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GDRP	General Data Protection Regulation
GRE	Generic Routing Encapsulation (RFC2890)
IaC	Infrastructure as Code
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
NIST	National Institute of Standards and Technology
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

© 2023 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website.

GitLab Overview

GitLab Inc. (NASDAQ: GTLB) is an open-core company that operates GitLab, a DevOps software package which can develop, secure, and operate software. The open-source software project was created by Ukrainian developer Dmytro Zaporozhets and Dutch developer Sytse Sijbrandij.

What started in 2011 as an open-source project to help one team of programmers collaborate is now the platform millions of people use to deliver software faster, more efficiently, while strengthening security and compliance. To learn more, refer to GitLab's website.

Audience

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

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

Software Versions

TThis document was authored using ZPC and GitLab Production 2022 Release. A GitLab free account was used to create and verify the features enabled and used as examples.

Create a free GitLab 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 GitLab Introduction

Overviews of the Zscaler and GitLab applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZPC Overview

Zscaler Posture Control (ZPC) is a multi-tenant software-as-a-service (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 once 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	Definition
ZIA Help Portal	Help articles for ZIA.
ZPC Help Portal	Help articles for ZPC.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
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.
About 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	Definition
ZIA Help Portal	Help articles for ZIA.
ZPC Help Portal	Help articles for ZPC.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
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.
About 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.

GitLab Overview

GitLab is a web-based Git repository that provides free open and private repositories, issue-following capabilities, and wikis. It is a complete DevOps platform that enables professionals to perform all the tasks in a project—from project planning and source code management to monitoring and security. Additionally, it allows teams to collaborate and build better software.

GitLab helps teams reduce product lifecycles and increase productivity, which in turn creates value for customers. The application doesn't require users to manage authorizations for each tool. If permissions are set once, then everyone in the organization has access to every component.

GitLab allows all the team members to collaborate in every phase of the project. GitLab offers tracking from planning to creation to help developers automate the entire DevOps lifecycle and achieve the best possible results. More and more developers have started to use GitLab because of its wide assortment of features and brick blocks of code availability.

- Accelerate your digital transformation: GitLab can help you achieve your digital transformation objectives with the most comprehensive DevSecOps platform. GitLab can help simplify your software delivery toolchain by ditching the plugins, simplifying integration, and helping your teams get back to delivering great software.
- Deliver software faster: Automated software delivery with GitLab helps you adopt cloud native, Kubernetes, and multi-cloud with ease, achieve faster velocity with lower failures and improve developer productivity by eliminating repetitive tasks.
- Ensure compliance: Software compliance is no longer just about checking boxes. Cloud native applications present entirely new attack surfaces via containers, orchestrators, web APIs, and other Infrastructure as Code (IaC). These new attack surfaces, along with complex DevOps toolchains, have resulted in notorious software supply chain attacks and led to new regulatory requirements. Continuous software compliance is becoming a critical way to manage risk inherent in cloud native applications and DevOps automation—beyond merely reducing security flaws within the code itself.
- Improve collaboration and visibility: Give everyone one platform to collaborate and see everything from planning to production.
- Build in security: Integrating security into your DevOps lifecycle is easy with GitLab. Security and compliance are built in, out of the box, giving you the visibility and control necessary to protect the integrity of your software.

GitLab Resources

The following table contains links to GitLab support resources.

Name	Definition
GitLab Documents	GitLab Documentation
GitLab Learn	GitLab Learning Portal
Get Started with GitLab	Get Started with GitLab
GitLab Community	GitLab Community
GitLab Architecture Overview	GitLab Architecture Overview

Version Control and CI/CD Systems

The following sections describe how to configure version control and CI/CD systems for a Zscaler and GitLab integration.

Configuring IaC Scan for GitLab

The Zscaler IaC Scan app scans and identifies security misconfigurations in the IaC Terraform, Helm, Kubernetes, and CloudFormation templates within GitLab. When you add or update the code and make a merge request, the IaC Scan action automatically triggers a scan of the IaC templates, identifies security misconfigurations, and displays the scan results within the code. This allows you to fix the configuration errors before deployment, and ensure your code is secure and compliant with the security policies.

You can configure only one GitLab integration per tenant.

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 GitLab accounts and authorize the IaC Scan app to scan the IaC repositories.

©2024 Zscaler, Inc. All rights reserved.

Configuring the Zscaler IaC Scan Action for GitLab

To configure the Zscaler IaC Scan action for GitLab:

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

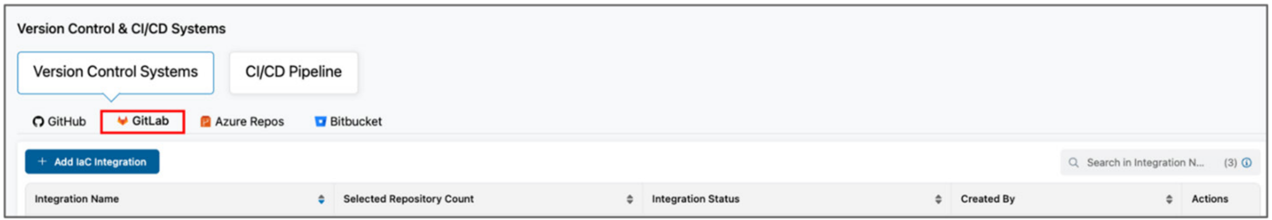


Figure 1. GitLab Version Control and CI/CD Systems

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

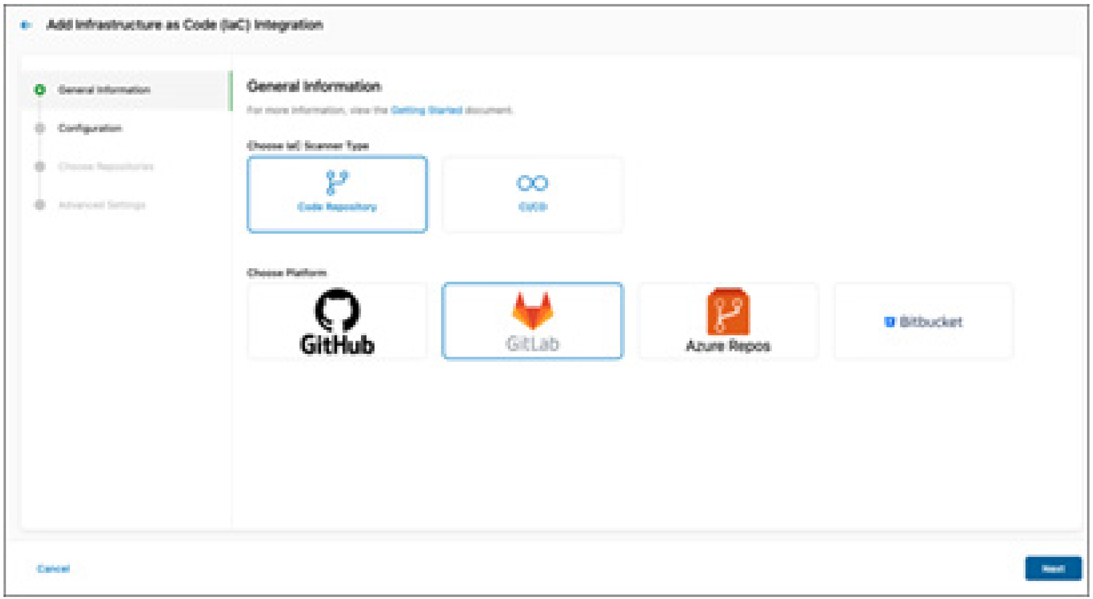
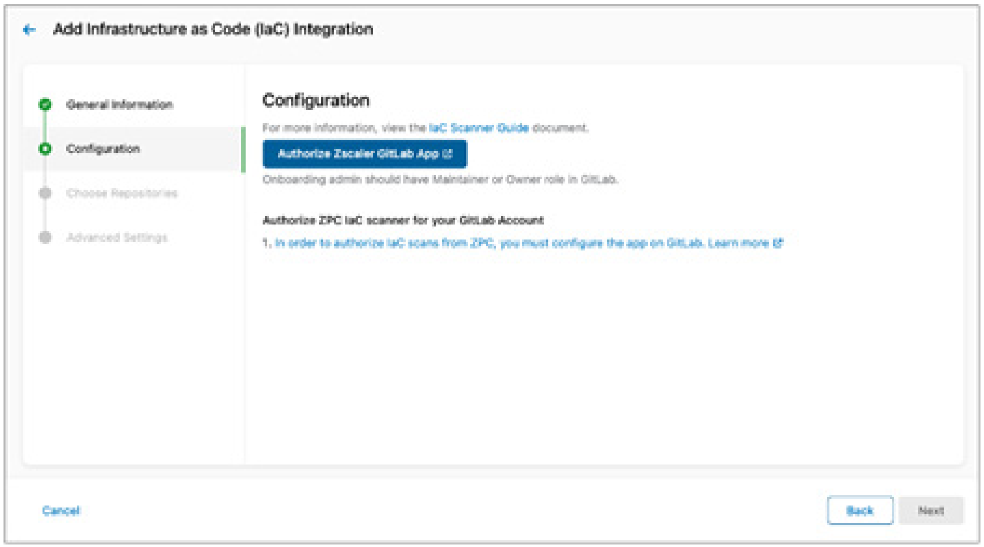


Figure 2. General Information

4. Click **Next**.
5. Click **Authorize Zscaler GitLab App**.



Add Infrastructure as Code (IaC) Integration

Configuration

For more information, view the IaC Scanner Guide document.

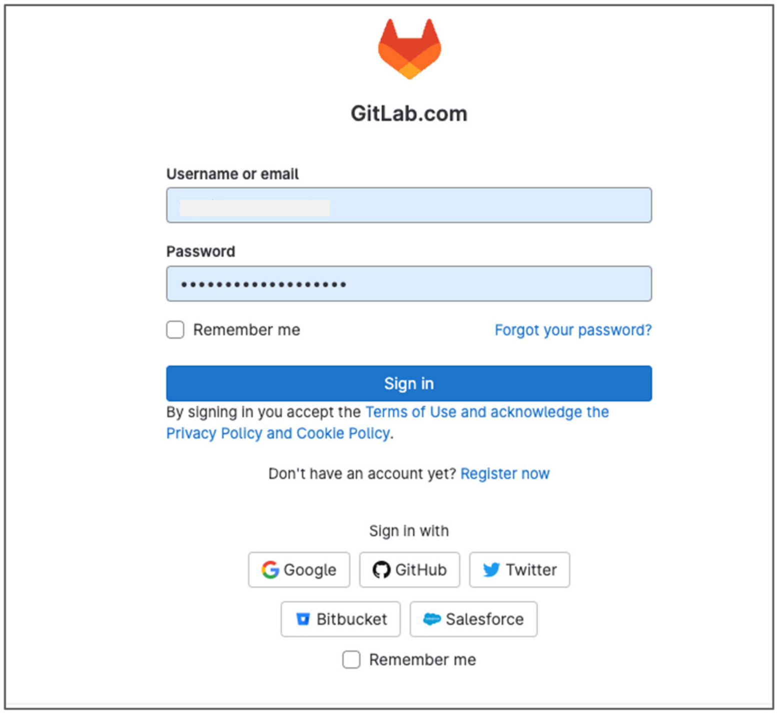
Onboarding admin should have Maintainer or Owner role in GitLab.

Authorize ZPC IaC scanner for your GitLab Account

1. In order to authorize IaC scans from ZPC, you must configure the app on GitLab. Learn more

Figure 3. Authorize Zscaler GitLab App

The GitLab Sign-in page appears. If you are already logged in to your GitLab account, then the GitLab Authorization page appears.



GitLab.com

Username or email

Password

•••••••••••••••••••

By signing in you accept the Terms of Use and acknowledge the Privacy Policy and Cookie Policy.

Don't have an account yet? Register now

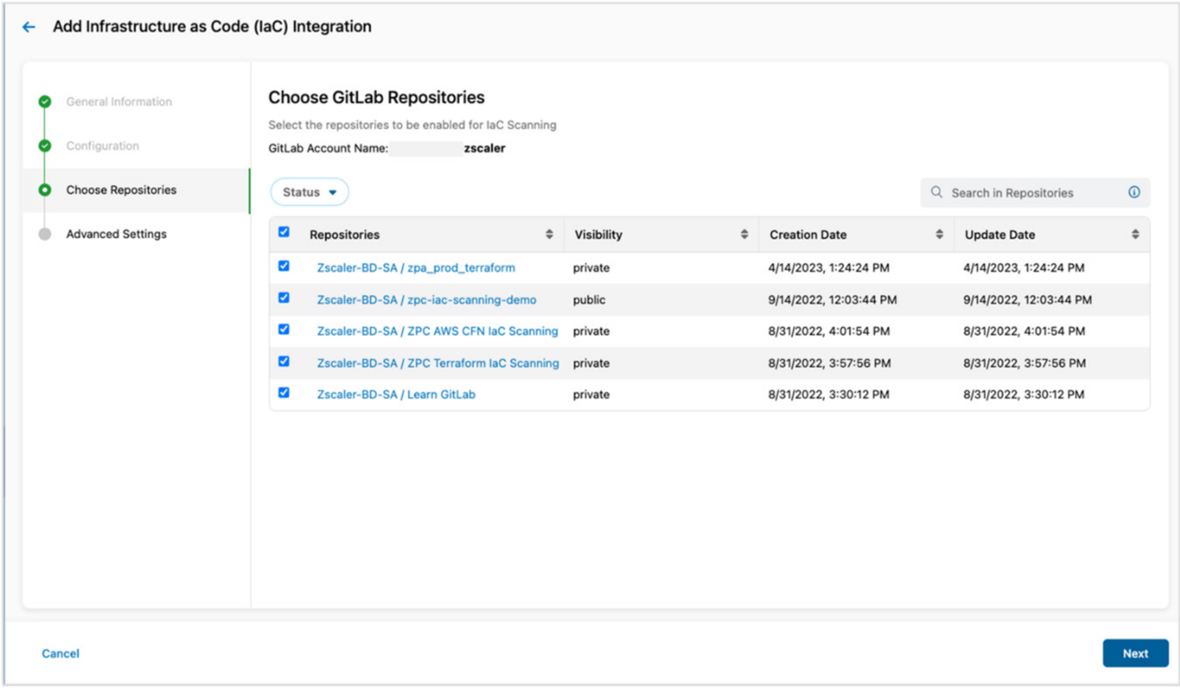
Figure 4. Authorize Zscaler GitLab App

6. Sign in to your GitLab account.
7. On the **GitLab Authorization** page, click **Authorize**. After completing the authorization, you are redirected back to the ZPC Admin Portal.
8. Click **Next**.

Choose GitLab Repositories

Under Choose GitLab Repositories, you can view the onboarded GitLab account and the list of repositories within this account.

1. Select the repositories that must be enabled for scanning.



Choose GitLab Repositories

Select the repositories to be enabled for IaC Scanning

GitLab Account Name: zscaler

☑	Repositories	Visibility	Creation Date	Update Date
☑	Zscaler-BD-SA / zpa_prod_terraform	private	4/14/2023, 1:24:24 PM	4/14/2023, 1:24:24 PM
☑	Zscaler-BD-SA / zpc-iac-scanning-demo	public	9/14/2022, 12:03:44 PM	9/14/2022, 12:03:44 PM
☑	Zscaler-BD-SA / ZPC AWS CFN IaC Scanning	private	8/31/2022, 4:01:54 PM	8/31/2022, 4:01:54 PM
☑	Zscaler-BD-SA / ZPC Terraform IaC Scanning	private	8/31/2022, 3:57:56 PM	8/31/2022, 3:57:56 PM
☑	Zscaler-BD-SA / Learn GitLab	private	8/31/2022, 3:30:12 PM	8/31/2022, 3:30:12 PM

Figure 5. Choose GitLab Repositories

2. Click **Next**.

3. (Optional) Under **Advanced Settings**:

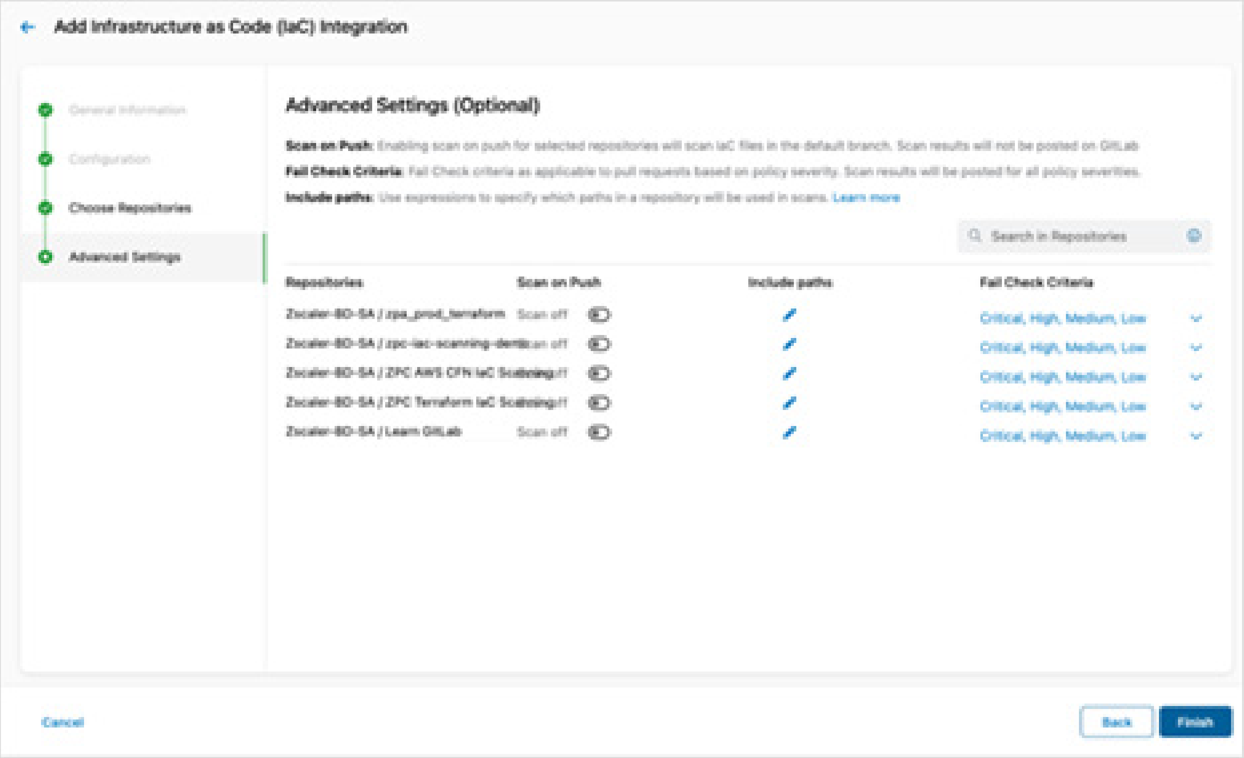
   - **Scan on Push**: Click the toggle to scan the code for a push command. The IaC Scan app performs the scan in the background and triggers alert notifications for any policy violations and displays the alerts in the ZPC Admin Portal. To learn more, see [About Alerts].
   - **Include Paths**: Click **Edit** 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

You can apply a security threshold to each repository. For example, you can fail a merge request that introduces Critical or High issues from a repository that is used to deploy to a production environment. If the same merge request has a Low threshold and the code must be 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.

©2024 Zscaler, Inc. All rights reserved.

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



Add Infrastructure as Code (IaC) Integration

Advanced Settings (Optional)

Scan on Push: Enabling scan on push for selected repositories will scan IaC files in the default branch. Scan results will not be posted on GitLab

Fail Check Criteria: Fail Check criteria as applicable to pull requests based on policy severity. Scan results will be posted for all policy severities.

Include paths: Use expressions to specify which paths in a repository will be used in scans. Learn more

Repositories	Scan on Push	Include paths	Fail Check Criteria
Zscaler-BD-SA / zpa_prod_terraform	Scan off		Critical, High, Medium, Low
Zscaler-BD-SA / zpc-iac-scanning-dem	Scan off		Critical, High, Medium, Low
Zscaler-BD-SA / ZPC AWS CFN IaC Scanning	Scan off		Critical, High, Medium, Low
Zscaler-BD-SA / ZPC Terraform IaC Scanning	Scan off		Critical, High, Medium, Low
Zscaler-BD-SA / Learn GitLab	Scan off		Critical, High, Medium, Low

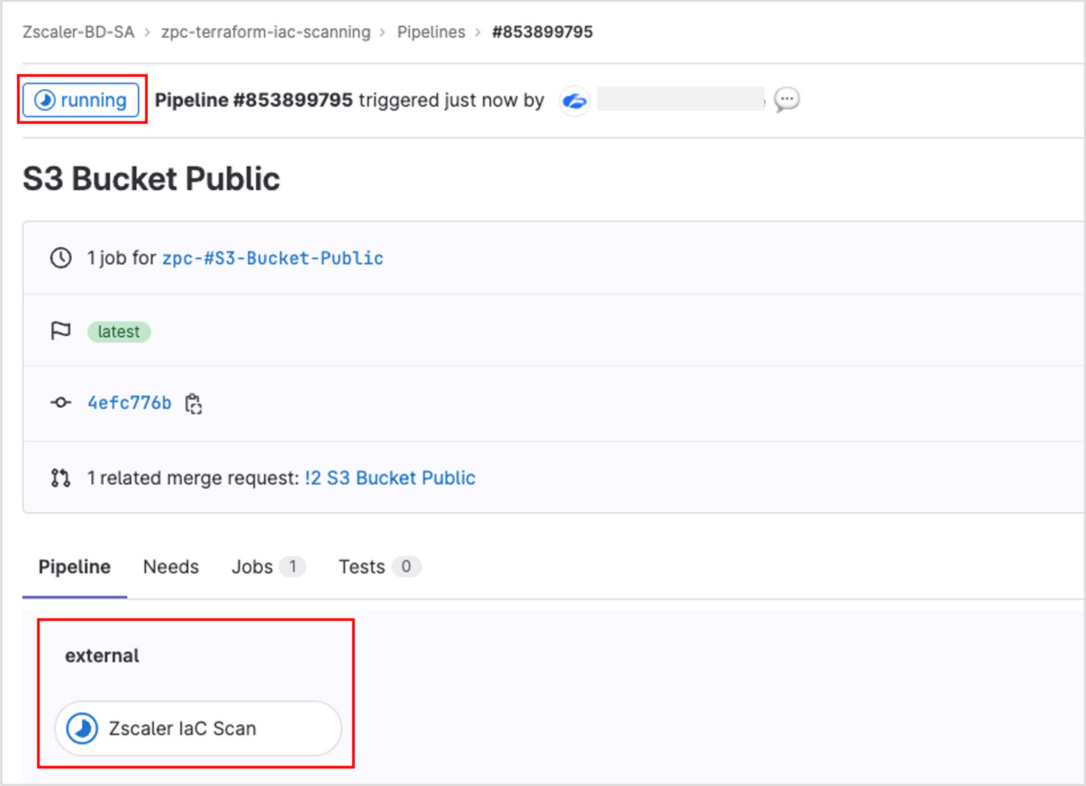
Figure 6. Advanced Settings

4. Click **Finish**.

Viewing the IaC Scan Summary in GitLab

After you enable the selected repositories for scanning, the 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.



Zscaler-BD-SA › zpc-terraform-iac-scanning › Pipelines › #853899795

running **Pipeline #853899795** triggered just now by [redacted]

S3 Bucket Public

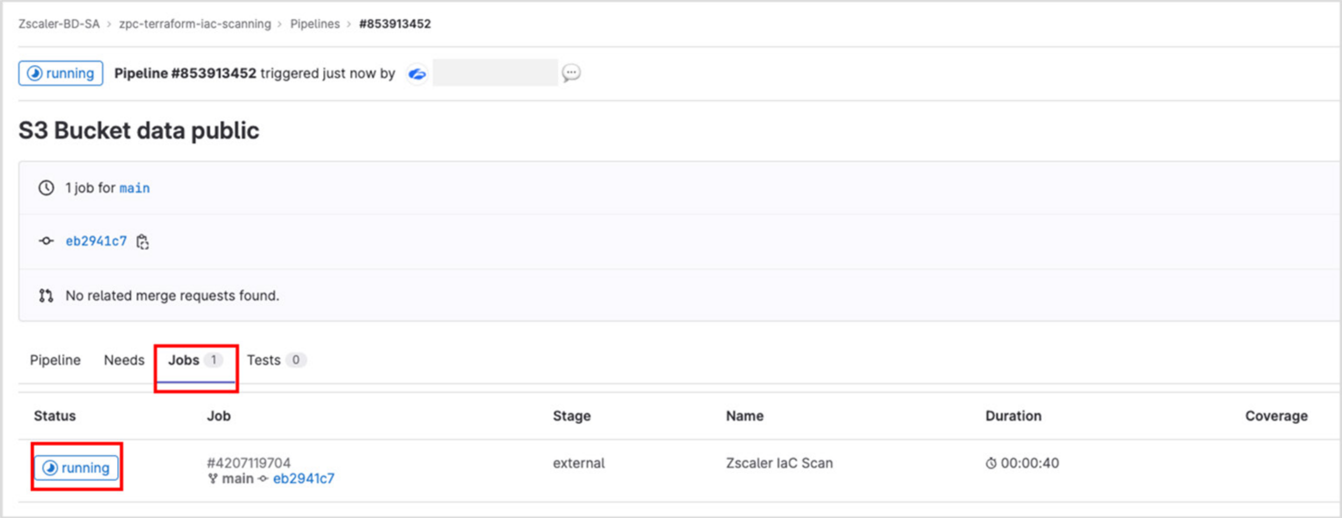
1 job for `zpc-#S3-Bucket-Public`

latest

`4efc776b`

1 related merge request: !2 S3 Bucket Public

Figure 7. GitLab Pipeline execution



Zscaler-BD-SA › zpc-terraform-iac-scanning › Pipelines › #853913452

running **Pipeline #853913452** triggered just now by [redacted]

S3 Bucket data public

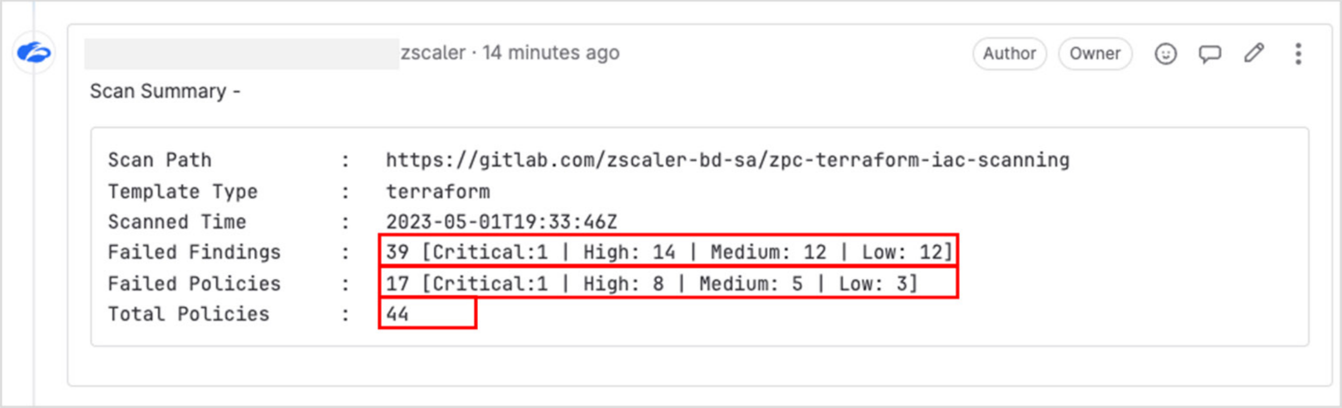
1 job for `main`

`eb2941c7`

No related merge requests found.

Status	Job	Stage	Name	Duration	Coverage
running	#4207119704 main ⊸ eb2941c7	external	Zscaler IaC Scan	00:00:40	

Figure 8. GitLab Job execution



[redacted] zscaler · 14 minutes ago

Scan Summary -

```
Scan Path          :   https://gitlab.com/zscaler-bd-sa/zpc-terraform-iac-scanning
Template Type      :   terraform
Scanned Time       :   2023-05-01T19:33:46Z
Failed Findings    :   39 [Critical:1 | High: 14 | Medium: 12 | Low: 12]
Failed Policies    :   17 [Critical:1 | High: 8 | Medium: 5 | Low: 3]
Total Policies     :   44
```

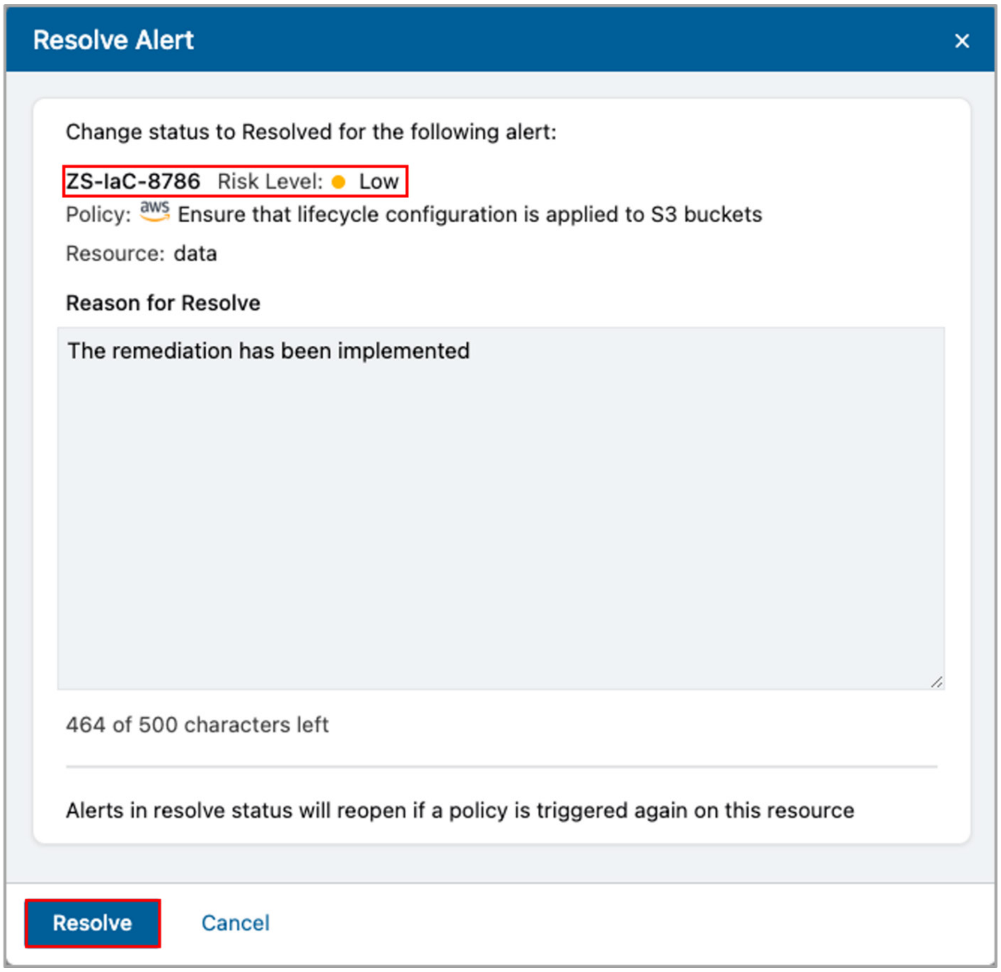
Figure 9. Zscaler IaC Scan results

Viewing Specific IaC Scan Summary in GitLab

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

To resolve a specific alert via the GitLab portal:

1. Select the check mark icon.
2. (Optional) Enter a **Reason to Resolve**.



Resolve Alert

Change status to Resolved for the following alert:

ZS-IaC-8786 Risk Level: ● Low

Policy: aws Ensure that lifecycle configuration is applied to S3 buckets

Resource: data

Reason for Resolve

The remediation has been implemented

464 of 500 characters left

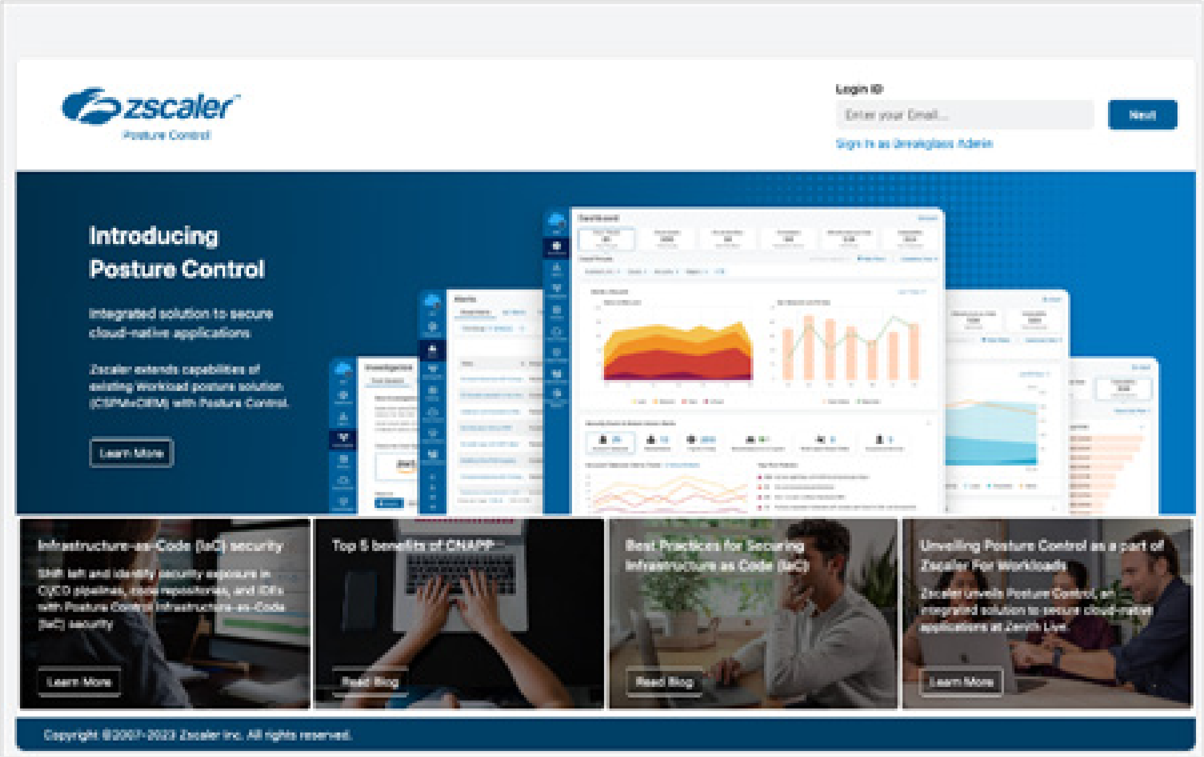
Alerts in resolve status will reopen if a policy is triggered again on this resource

Figure 10. Resolve Alert

Viewing the IaC Scan Summary in the ZPC Admin Portal

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

1. Login to the ZPC Admin Portal.



Introducing Posture Control

Integrated solution to secure cloud-native applications

Zscaler extends capabilities of existing Workload posture solution (CSPM+CIEM) with Posture Control.

Infrastructure-as-Code (IaC) security

Shift left and identify security exposure in CI/CD pipelines, code repositories, and IDEs with Posture Control Infrastructure-as-Code (IaC) security

Top 5 benefits of CNAPP

Best Practices for Securing Infrastructure as Code (IaC)

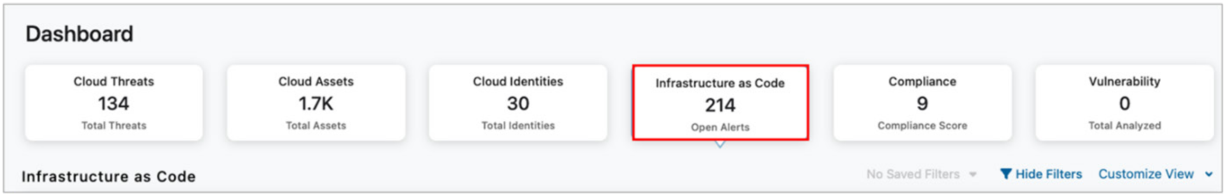
Unveiling Posture Control as a part of Zscaler For Workloads

Zscaler unveils Posture Control, an integrated solution to secure cloud-native applications at Zenith Live.

Copyright ©2007-2023 Zscaler Inc. All rights reserved.

Figure 11. ZPC Admin Portal

2. Select **Infrastructure as Code**.



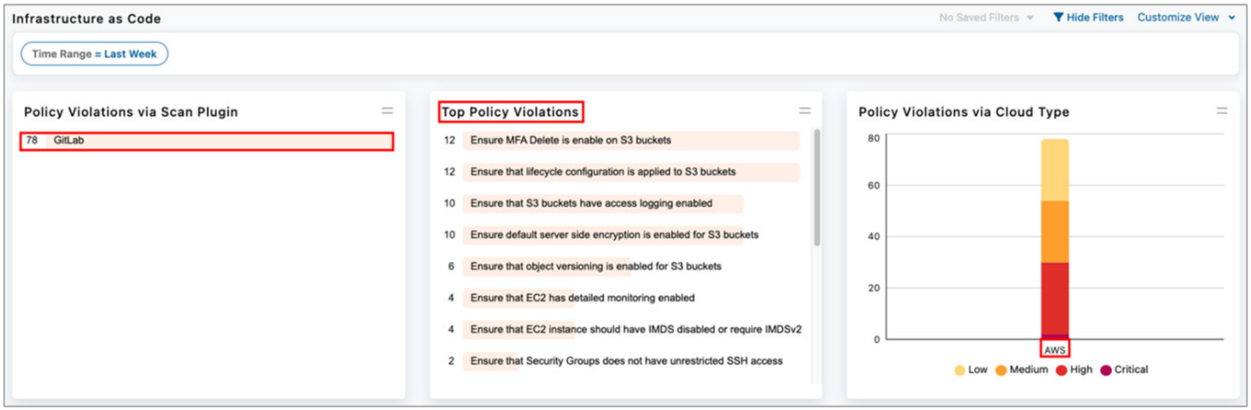
Dashboard

Cloud Threats	Cloud Assets	Cloud Identities	Infrastructure as Code	Compliance	Vulnerability
134	1.7K	30	214	9	0
Total Threats	Total Assets	Total Identities	Open Alerts	Compliance Score	Total Analyzed

Infrastructure as Code

Figure 12. ZPC Infrastructure as Code widget

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

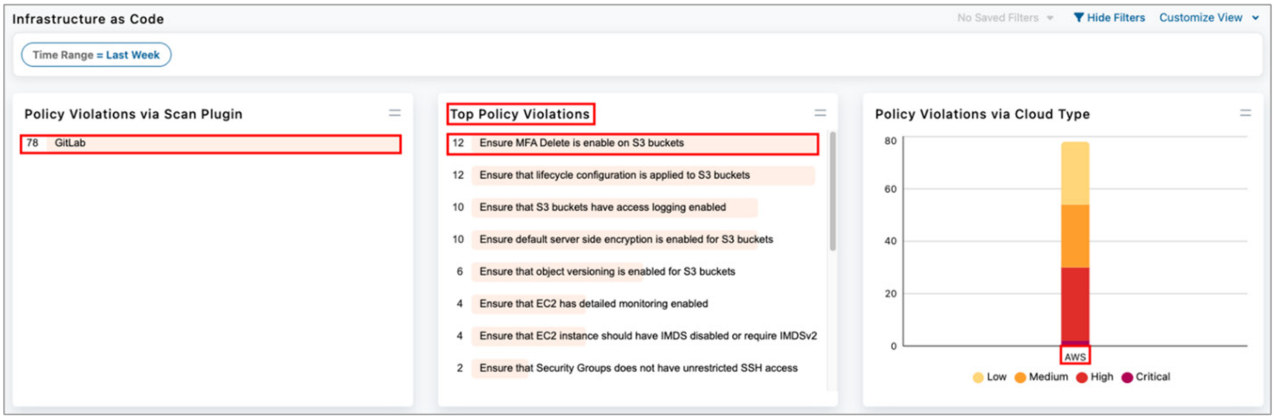


78	GitLab

12	Ensure MFA Delete is enable on S3 buckets
12	Ensure that lifecycle configuration is applied to S3 buckets
10	Ensure that S3 buckets have access logging enabled
10	Ensure default server side encryption is enabled for S3 buckets
6	Ensure that object versioning is enabled for S3 buckets
4	Ensure that EC2 has detailed monitoring enabled
4	Ensure that EC2 instance should have IMDS disabled or require IMDSv2
2	Ensure that Security Groups does not have unrestricted SSH access

Figure 13. 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.

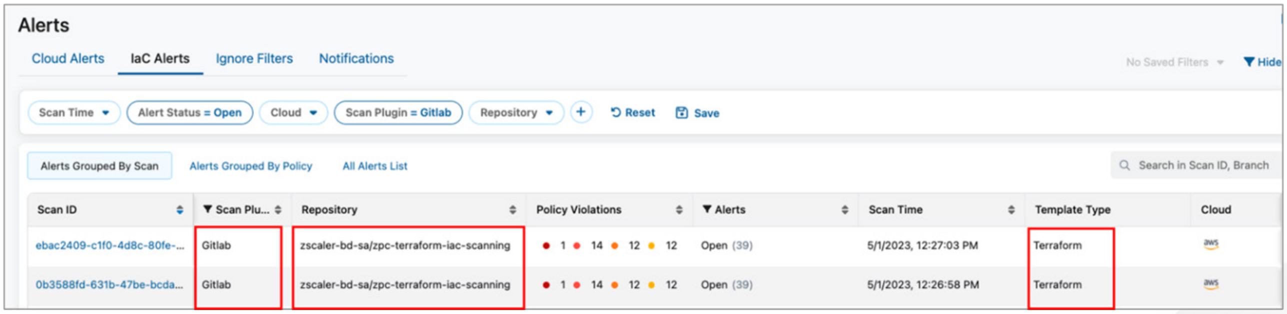


78	GitLab

12	Ensure MFA Delete is enable on S3 buckets
12	Ensure that lifecycle configuration is applied to S3 buckets
10	Ensure that S3 buckets have access logging enabled
10	Ensure default server side encryption is enabled for S3 buckets
6	Ensure that object versioning is enabled for S3 buckets
4	Ensure that EC2 has detailed monitoring enabled
4	Ensure that EC2 instance should have IMDS disabled or require IMDSv2
2	Ensure that Security Groups does not have unrestricted SSH access

Figure 14. ZPC Infrastructure as Code Top Policy Violations

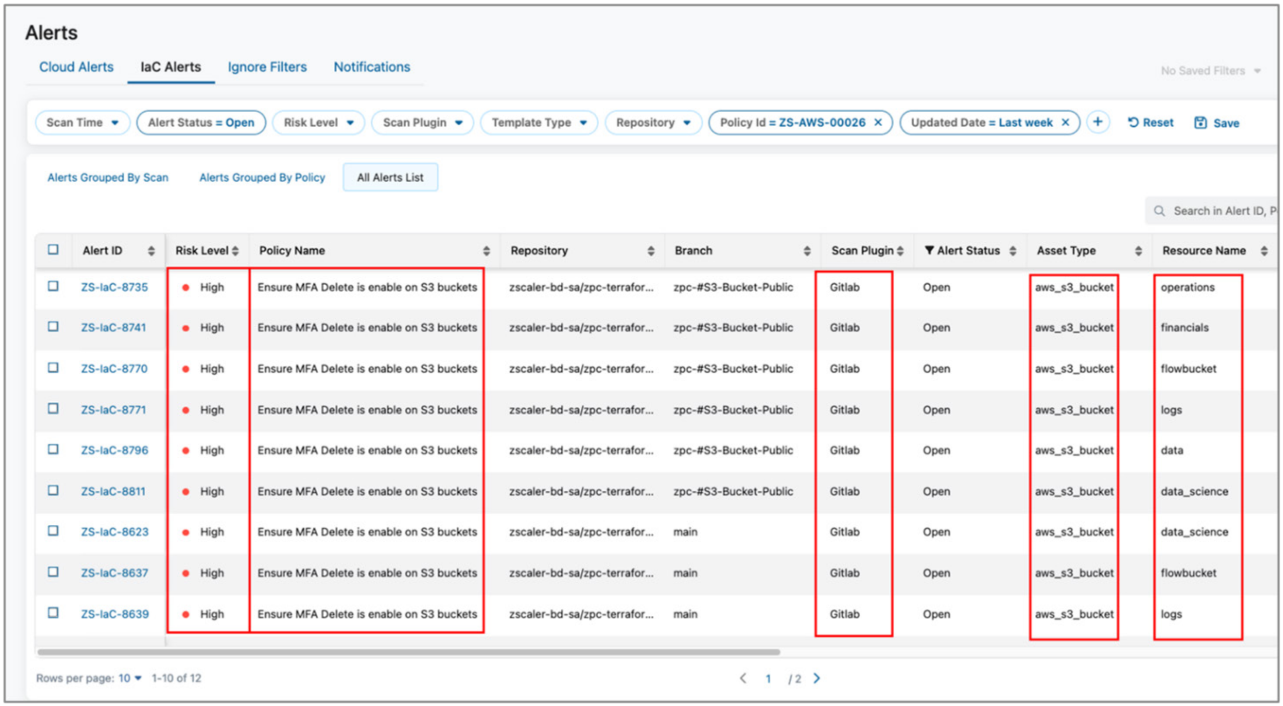
5. The administrator can also group the IaC alerts by scan type. In the following example, the filter only displays **Scan Plugin = GitLab**.
   a. Other filters are also available (e.g., **Scan Time**, **Alert Status**, **Cloud**, and **Repository**).
   b. You can add other filters by selecting the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



Scan ID	Scan Plu...	Repository	Policy Violations	Alerts	Scan Time	Template Type	Cloud
ebac2409-c1f0-4d8c-80fe-...	Gitlab	zscaler-bd-sa/zpc-terraform-iac-scanning	● 1 ● 14 ● 12 ● 12	Open (39)	5/1/2023, 12:27:03 PM	Terraform	aws
0b3588fd-631b-47be-bcda...	Gitlab	zscaler-bd-sa/zpc-terraform-iac-scanning	● 1 ● 14 ● 12 ● 12	Open (39)	5/1/2023, 12:26:58 PM	Terraform	aws

Figure 15. ZPC IaC Alerts by Scan Plugin

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



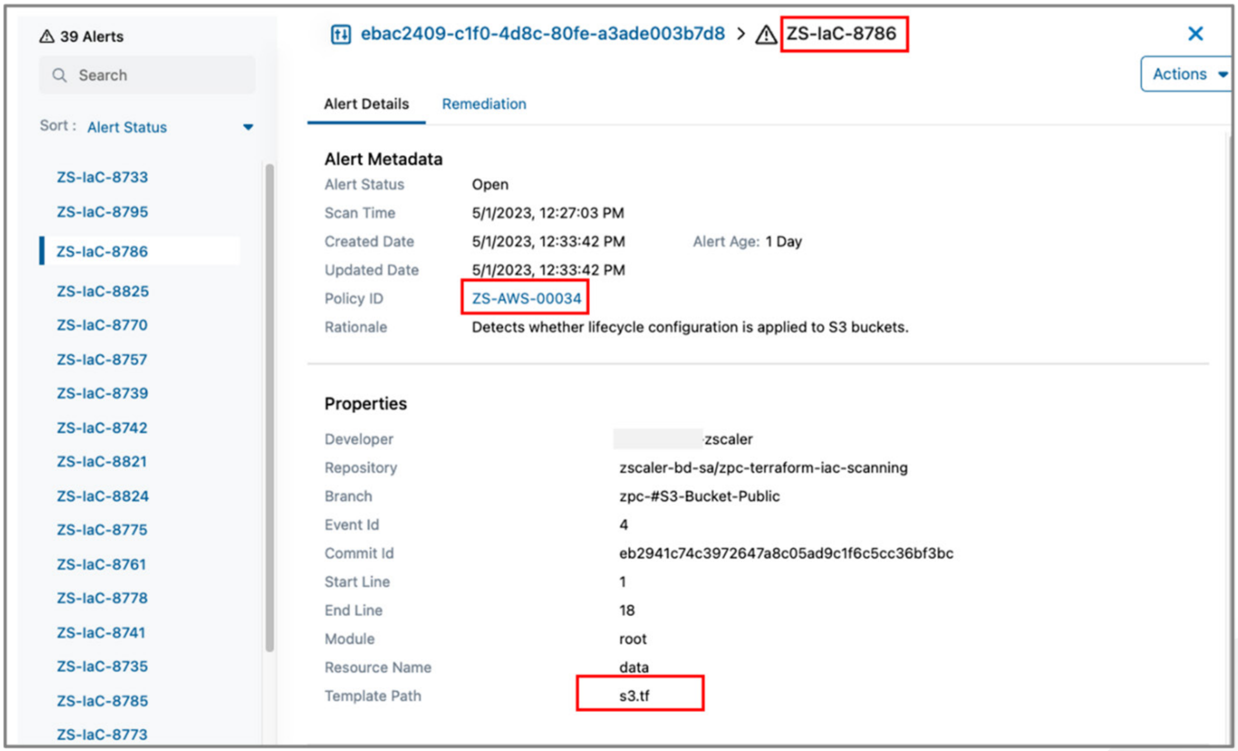
Alerts

☐	Alert ID	Risk Level	Policy Name	Repository	Branch	Scan Plugin	Alert Status	Asset Type	Resource Name
☐	ZS-IaC-8735	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	zpc-#S3-Bucket-Public	Gitlab	Open	aws_s3_bucket	operations
☐	ZS-IaC-8741	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	zpc-#S3-Bucket-Public	Gitlab	Open	aws_s3_bucket	financials
☐	ZS-IaC-8770	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	zpc-#S3-Bucket-Public	Gitlab	Open	aws_s3_bucket	flowbucket
☐	ZS-IaC-8771	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	zpc-#S3-Bucket-Public	Gitlab	Open	aws_s3_bucket	logs
☐	ZS-IaC-8796	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	zpc-#S3-Bucket-Public	Gitlab	Open	aws_s3_bucket	data
☐	ZS-IaC-8811	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	zpc-#S3-Bucket-Public	Gitlab	Open	aws_s3_bucket	data_science
☐	ZS-IaC-8623	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	main	Gitlab	Open	aws_s3_bucket	data_science
☐	ZS-IaC-8637	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	main	Gitlab	Open	aws_s3_bucket	flowbucket
☐	ZS-IaC-8639	● High	Ensure MFA Delete is enable on S3 buckets	zscaler-bd-sa/zpc-terrafor...	main	Gitlab	Open	aws_s3_bucket	logs

Rows per page: 10 1-10 of 12 1 /2

Figure 16. ZPC IaC Alerts

7. Select one of the alerts listed in the **Alert ID** column. This example selects the alert **ID ZS-IaC-8786,** which indicates that ZPC has detected a violation associated with a **Policy ID: ZS-AWS-00034**. This policy detects whether the lifecycle configuration is applied to the S3 bucket.



ebac2409-c1f0-4d8c-80fe-a3ade003b7d8 > ZS-IaC-8786

Alert Metadata

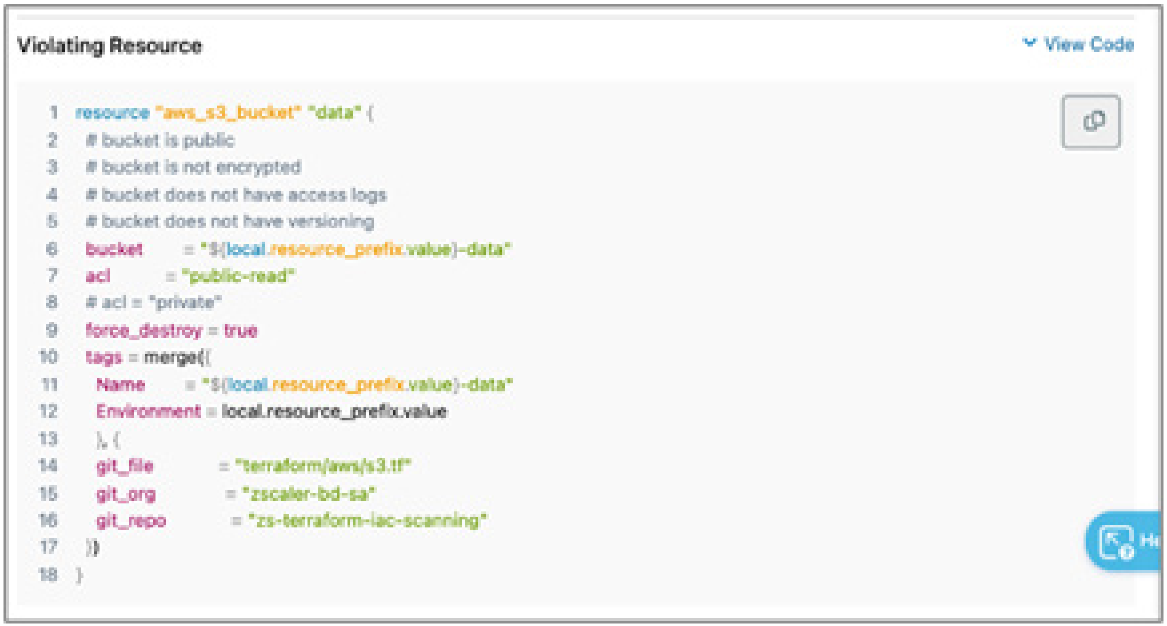
Alert Status Open
Scan Time 5/1/2023, 12:27:03 PM
Created Date 5/1/2023, 12:33:42 PM Alert Age: 1 Day
Updated Date 5/1/2023, 12:33:42 PM
Policy ID ZS-AWS-00034
Rationale Detects whether lifecycle configuration is applied to S3 buckets.

Properties

Developer [redacted]zscaler
Repository zscaler-bd-sa/zpc-terraform-iac-scanning
Branch zpc-#S3-Bucket-Public
Event Id 4
Commit Id eb2941c74c3972647a8c05ad9c1f6c5cc36bf3bc
Start Line 1
End Line 18
Module root
Resource Name data
Template Path s3.tf

Figure 17. ZPC Alert Details

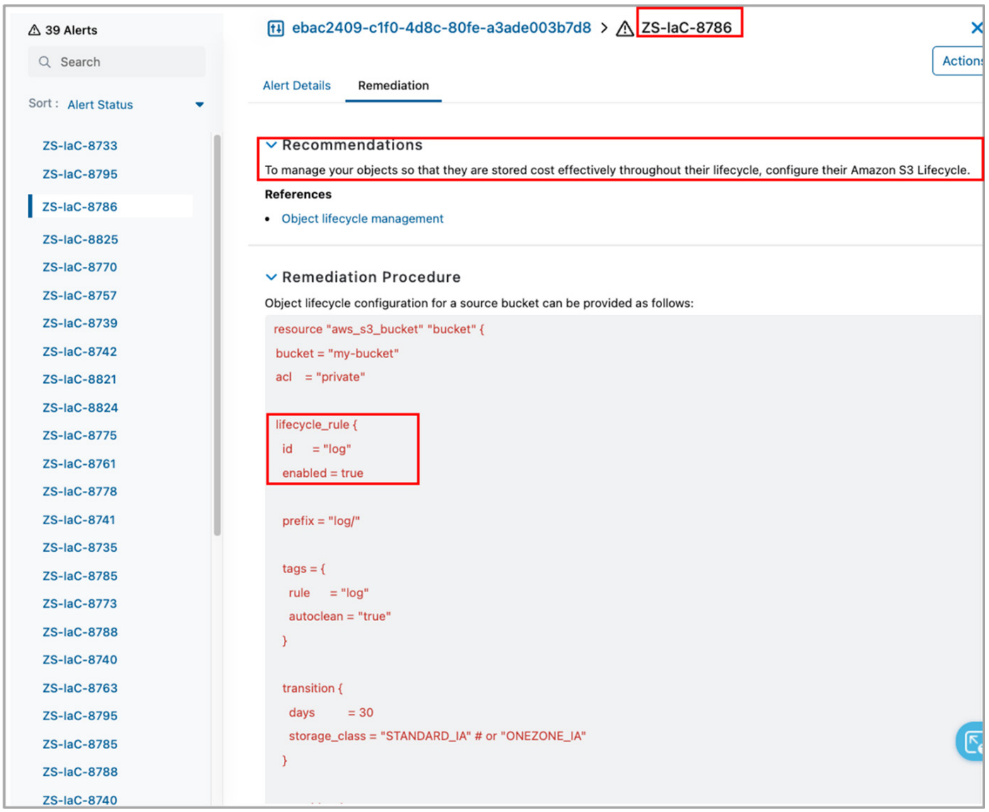
8. See the code snippet with information about the **Violating Resource**.



```
resource "aws_s3_bucket" "data" {
  # bucket is public
  # bucket is not encrypted
  # bucket does not have access logs
  # bucket does not have versioning
  bucket        = "${local.resource_prefix.value}-data"
  acl        = "public-read"
  # acl = "private"
  force_destroy = true
  tags = merge({
    Name        = "${local.resource_prefix.value}-data"
    Environment = local.resource_prefix.value
    }, {
    git_file           = "terraform/aws/s3.tf"
    git_org            = "zscaler-bd-sa"
    git_repo           = "zs-terraform-iac-scanning"
  })
}
```

Figure 18. ZPC Violating Resource

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



Recommendations

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle.

References

- Object lifecycle management

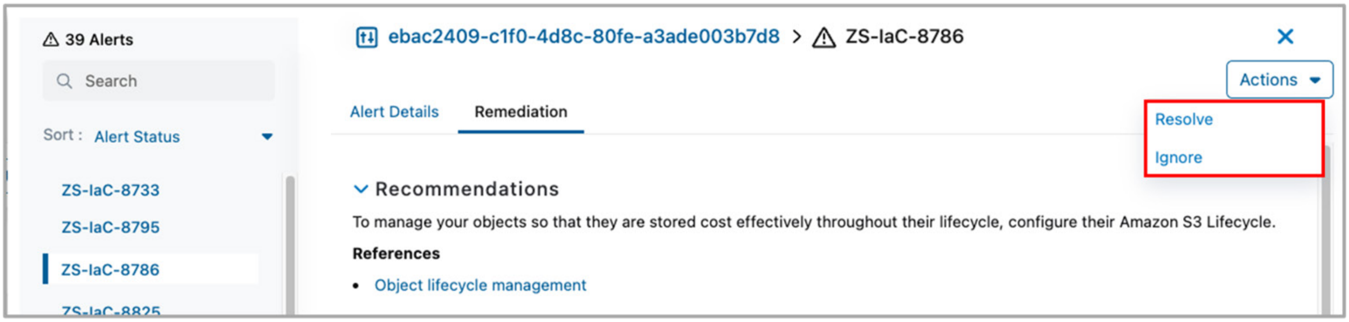
Remediation Procedure

Object lifecycle configuration for a source bucket can be provided as follows:

```
resource "aws_s3_bucket" "bucket" {
 bucket = "my-bucket"
 acl   = "private"

 lifecycle_rule {
  id     = "log"
  enabled = true

  prefix = "log/"

  tags = {
   rule     = "log"
   autoclean = "true"
  }

  transition {
   days        = 30
   storage_class = "STANDARD_IA" # or "ONEZONE_IA"
  }
```

Figure 19. ZPC Remediation

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



Recommendations

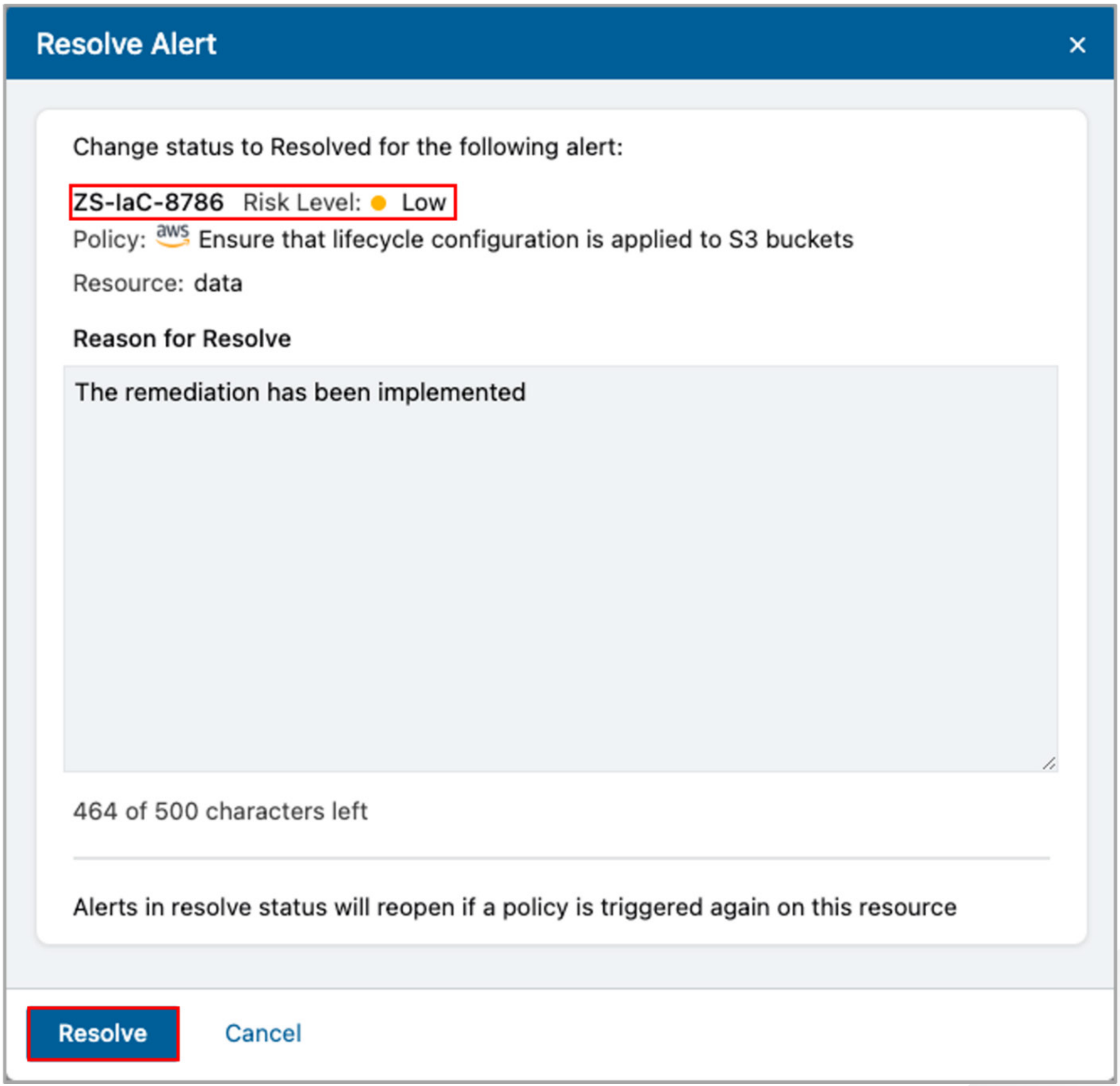
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle.

References

- Object lifecycle management

Figure 20. Alert Actions

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



Change status to Resolved for the following alert:

ZS-IaC-8786 Risk Level: ● Low

Policy: aws Ensure that lifecycle configuration is applied to S3 buckets

Resource: data

Reason for Resolve

The remediation has been implemented

464 of 500 characters left

Alerts in resolve status will reopen if a policy is triggered again on this resource

Figure 21. Resolve Alert

Resolving Failed Integrations

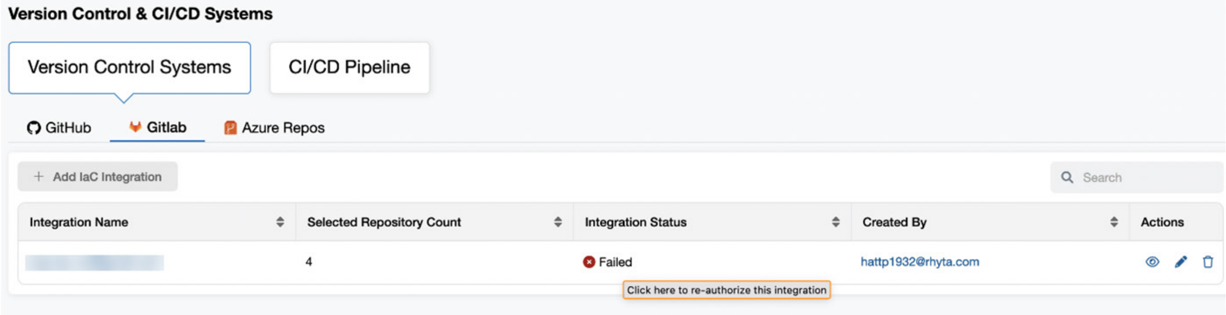
Use Case 1

GitLab integration that worked previously can be disrupted (e.g., if a user accidentally unauthorizes the Zscaler IaC Scan in GitLab or if the authorization token is corrupted in the ZPC Admin Portal). Instead of deleting the GitLab account and repeating the configuration steps again, you can reauthorize the existing integration.

When an integration fails, the Integration Status is displayed as Failed in the ZPC Admin Portal.

To reauthorize a GitLab integration:

1. Go to **Version Control & CI/CD Systems**.
2. Under **Version Control Systems**, click the **GitLab** tab.
3. Search for the integration that failed.
4. Hover the mouse over the **Failed** status to see the following tooltip: **Click here to reauthorize this integration**.



Integration Name	Selected Repository Count	Integration Status	Created By	Actions
[redacted]	4	Failed	hattp1932@rhyta.com	

Click here to re-authorize this integration

Figure 22. Failed GitLab integration

5. Click the tooltip to go to the **GitLab Authorization** page.
6. Click **Authorize Zscaler GitLab App** to re-establish the connection between GitLab and the ZPC Admin Portal and enable IaC scanning of the GitLab repositories.

A confirmation message appears indicating that the reauthorization is successful, and you are redirected to the Version Control & CI/CD Systems page. The Integration Status is displayed as Success for that integration.

Use Case 2

For failed integrations, the Integration Status is displayed as Failed in the ZPC Admin Portal. In this case, if you offboard the tenant or unsubscribe from the IaC service entitlement, then the integration is deleted from ZPC, but the webhooks are not deleted from the GitLab repository. You need to manually delete the webhooks.

If you don't delete the webhooks, then you can't integrate the GitLab account whenever you subscribe for the IaC entitlement again.

Zscaler Data Protection for GitLab

Gitlab is a service that provides remote access to Git repositories. In addition to hosting your code, the services provide additional features for managing the software development lifecycle.

There are two software distributions of GitLab:

- The open source Community Edition (CE).
- The open core Enterprise Edition (EE).

GitLab is available under different subscriptions. New versions of GitLab are released from stable branches, and the main branch is used for bleeding-edge development. To learn more, refer to the **GitLab release process**.

Both distributions require additional components. These components are described in the Component details section, and all have their own repositories. New versions of each dependent component are usually tags, but staying on the main branch of the GitLab codebase gives you the latest stable version of those components. New versions are generally released around the same time as GitLab releases, with the exception of informal security updates deemed critical.

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 GitLab users.

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

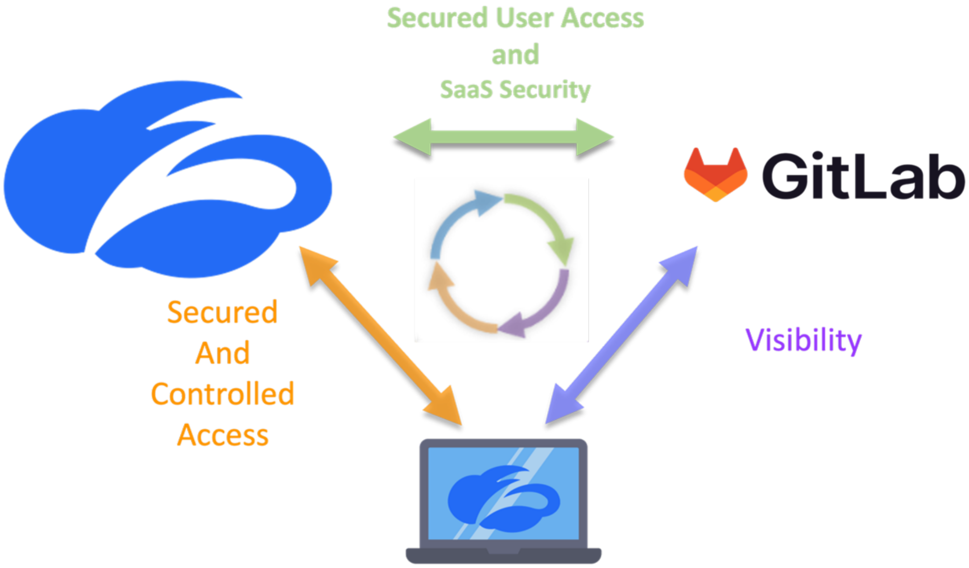


Figure 23. Zscaler solutions for GitLab

ZIA provides security for GitLab SaaS platform through access control, identity control, SaaS Security Posture Management, a SaaS API to scan the attachments for malicious content, and 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 GitLab security:

- ZIA Cloud Browser Isolation
- SaaS Security Data Loss Protection and Malware Detection
- ZIA Cloud Application Control
- ZPC and GitLab Integration

©2024 Zscaler, Inc. All rights reserved.

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 concurrently providing unobstructed internet access for users.

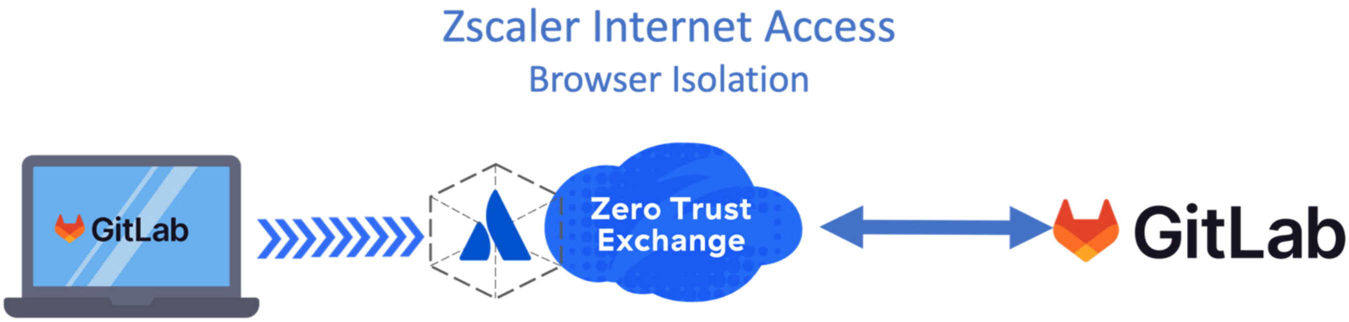


Figure 24. ZIA Cloud Browser isolation in use with GitLab product

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 GitLab platform, while preventing the downloading and copying-and-pasting of confidential business data.

ZIA Data Loss Protection and Malware Detection for GitLab

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.

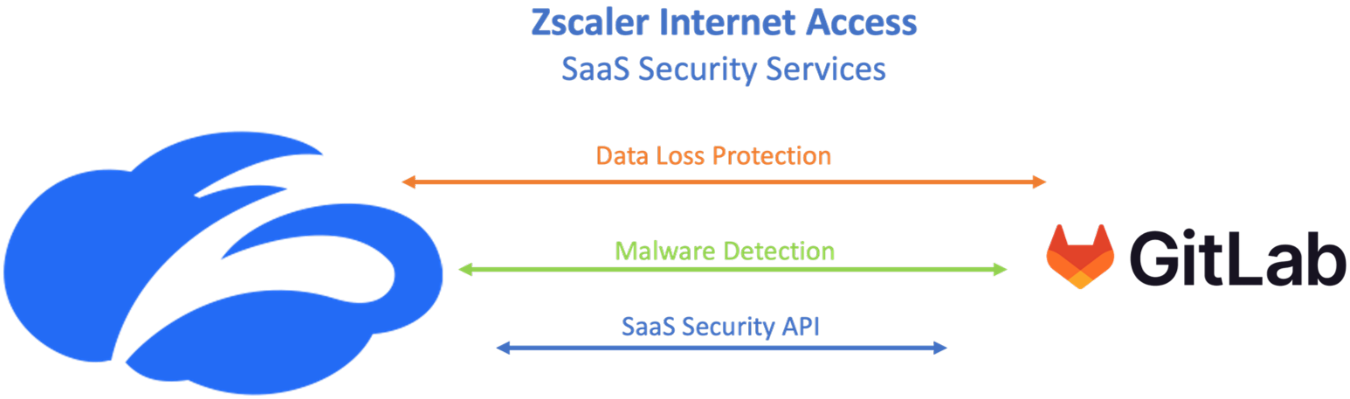


Figure 25. ZIA SaaS Security in use with GitLab Product

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.

©2024 Zscaler, Inc. All rights reserved.

What Makes Zscaler 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 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: The Zscaler Cloud Security Platform 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-prem 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. Zscaler Cloud Application Visibility and 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. Zscaler cloud application security is referred to as in-line.

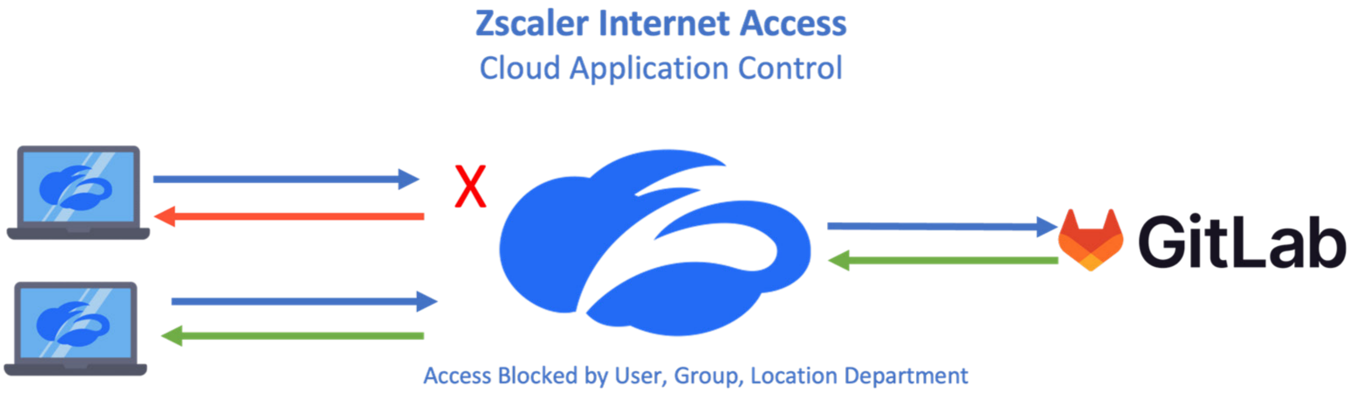

Zscaler Internet Access
Cloud Application Control
X
GitLab
Access Blocked by User, Group, Location Department

Figure 26. Cloud App Control

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 required users access to the application.

©2024 Zscaler, Inc. All rights reserved.

ZPC and GitLab Integration

The ZPC IaC Scan app scans and identifies security misconfigurations in the IaC Terraform, Helm, Kubernetes, and CloudFormation templates within GitLab. When you add or update the code and make a merge request, the IaC Scan action automatically triggers a scan of the IaC templates, identifies security misconfigurations, and displays the scan results within the code. This allows you to fix the configuration errors before deployment, and ensure your code is secure and compliant with the security policies.

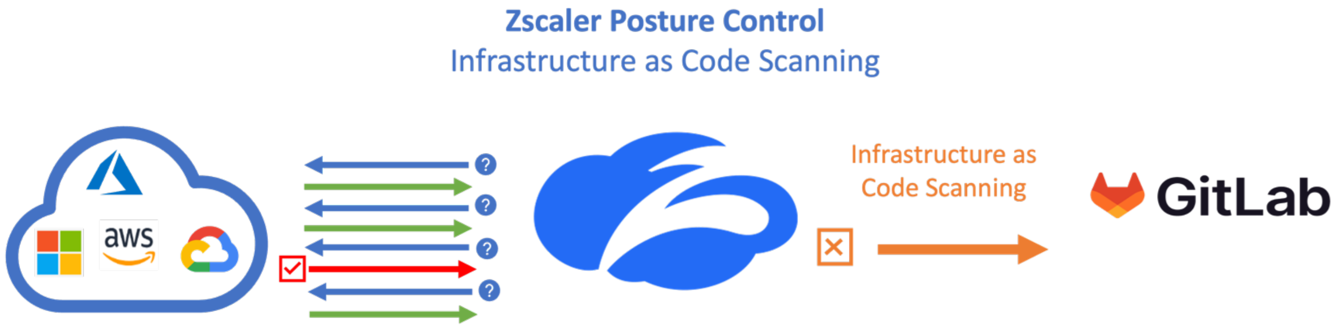

Zscaler Posture Control
Infrastructure as Code Scanning
aws
Infrastructure as Code Scanning
GitLab

Figure 27. ZPC and GitLab integration

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.

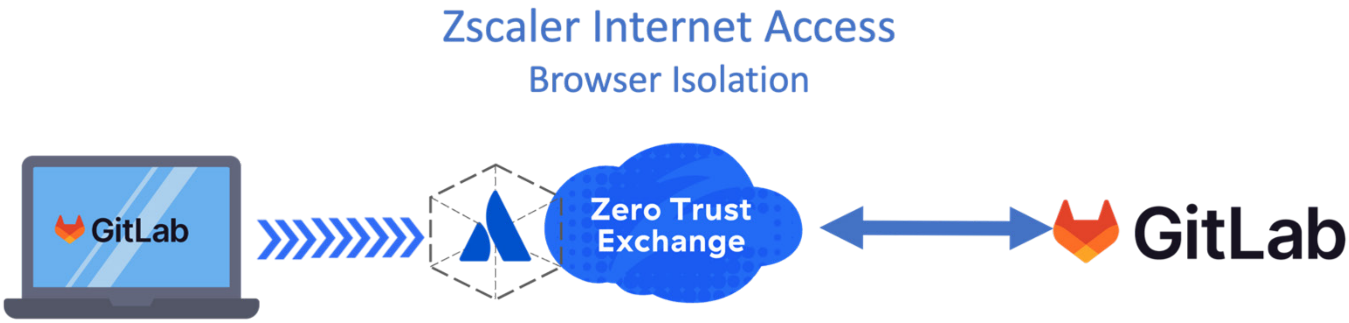


Figure 28. ZIA Cloud Browser Isolation in use with GitLab

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 in GitLab platform while preventing the downloading and cutting-and-pasting of confidential business data.

Configure the Cloud Browser Isolation Profile

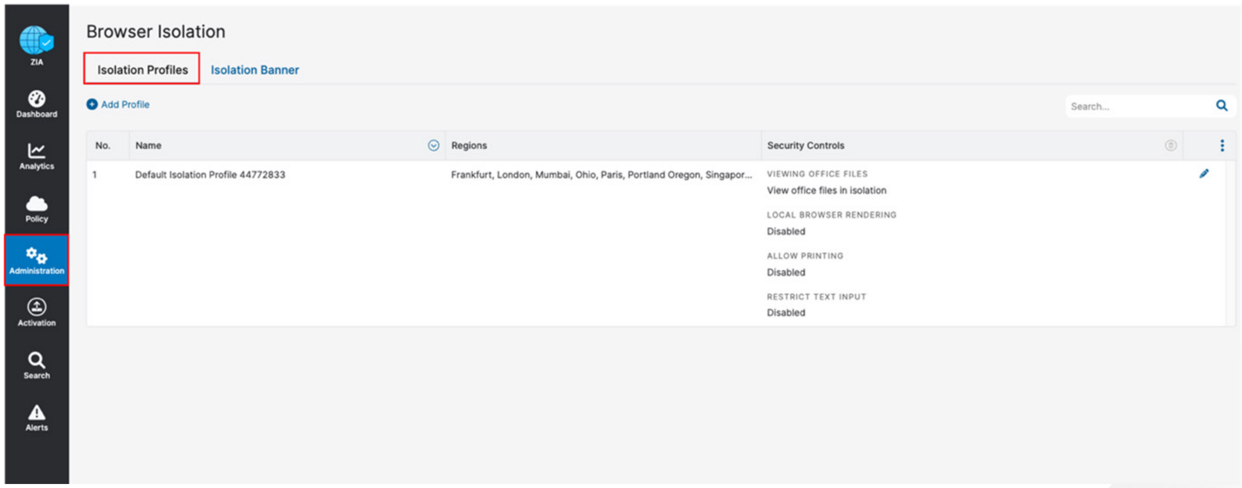
To begin the Cloud Browser Isolation configuration, log into the ZIA Admin Portal with administrator credentials.

You must configure a Browser Isolation Profile (or multiple profiles) to use Zscaler Cloud Browser Isolation features specifically for GitLab products, along with an individual user profile for the user using Browser Isolation.

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

To start the Policy Wizard:

1. Go to **Administration** > **Secure Browsing** > **Browser Isolation**.
2. Select the **Isolation Profiles** tab.
3. Click **Add Profile**.



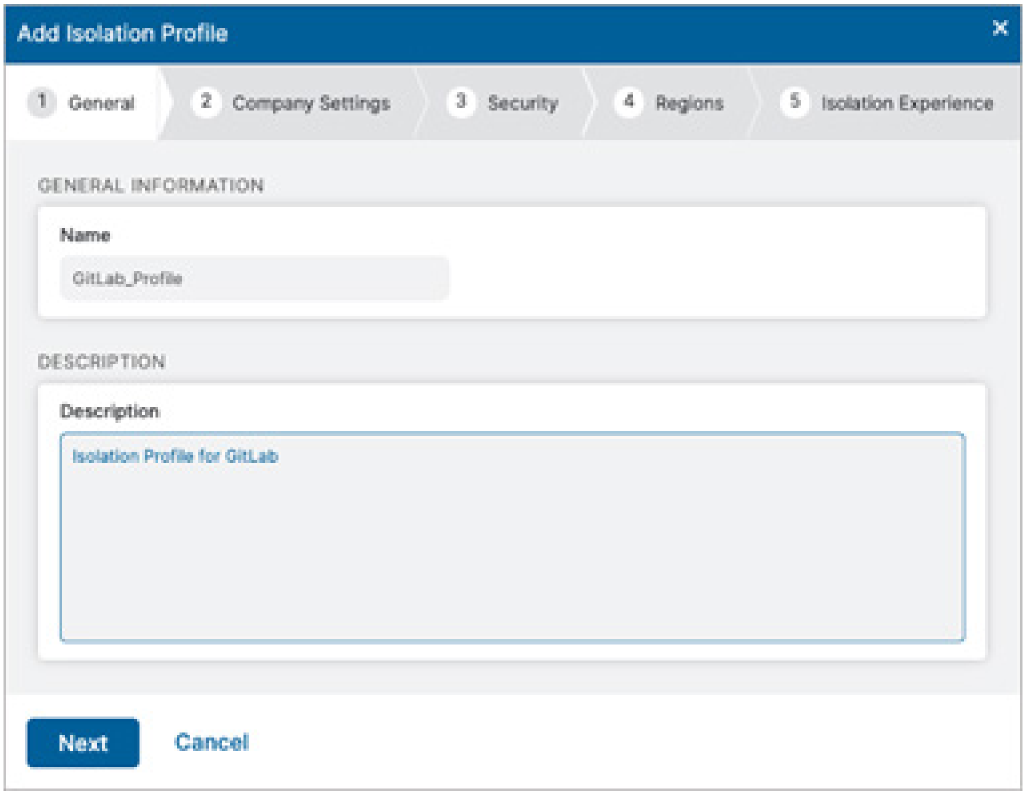
No.	Name	Regions	Security Controls
1	Default Isolation Profile 44772833	Frankfurt, London, Mumbai, Ohio, Paris, Portland Oregon, Singapor...	VIEWING OFFICE FILES View office files in isolation LOCAL BROWSER RENDERING Disabled ALLOW PRINTING Disabled RESTRICT TEXT INPUT Disabled

Figure 29. Cloud Browser Isolation Profile

This starts the 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 portal and should be clear to the use case:

1. **Name** the profile.
2. Give the profile a detailed **Description**.



Name
GitLab_Profile

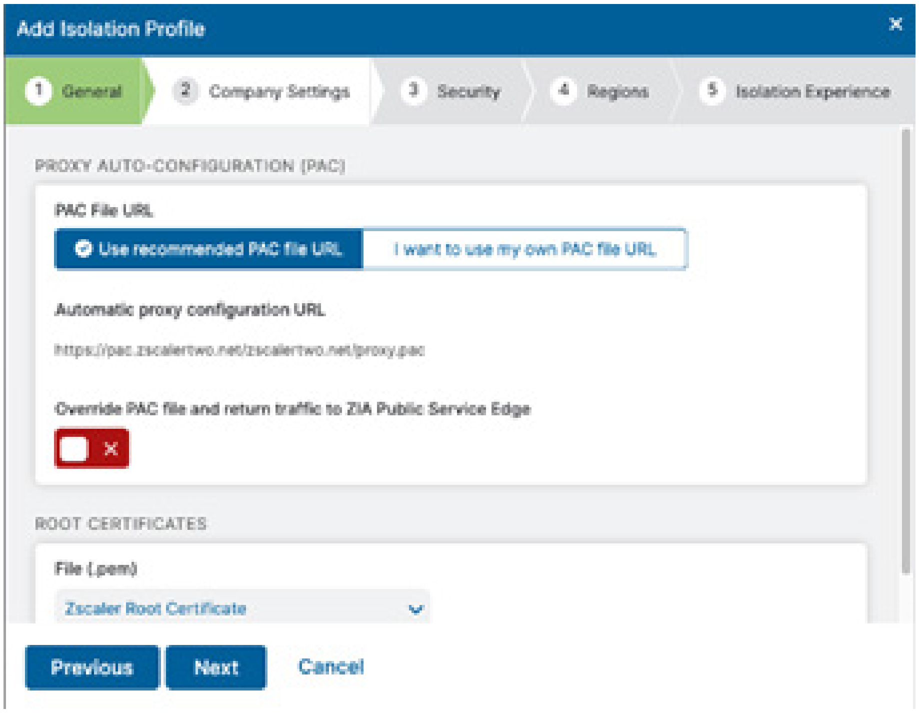
Description
Isolation Profile for GitLab

Figure 30. Cloud Browser General Information

Make your selections in the **Company Settings** section:

a. Choose to either use the recommended PAC file URL or to use your own manually configured PAC file URL:

- If you choose to use the recommended PAC file URL, the **Automatic proxy configuration URL** field is populated by default with the recommended PAC file from your Hosted PAC Files list in ZIA. This PAC file is configured onto the isolation browser within the endpoint experience containers, and any traffic to the internet from the isolated browser is also forwarded through the ZIA cloud.
- Enable or disable the option to **Override the PAC File** and return traffic to the ZIA Public Service Edge. The ZIA Public Service Edges use auto-geo proximity, meaning that the traffic is returned to the service edge closest to the location of the user, not the location of the isolation browser. To see the full list of ZIA Public Service Edges, see the Cloud Enforcement Node Ranges (government agencies, see Cloud Enforcement Node Ranges).



PROXY AUTO-CONFIGURATION (PAC)

PAC File URL

● Use recommended PAC file URL | I want to use my own PAC file URL

Automatic proxy configuration URL

https://pac.zscalertwo.net/zscalertwo.net/proxy.pac

Override PAC file and return traffic to ZIA Public Service Edge

☒

ROOT CERTIFICATES

File (.pem)

Zscaler Root Certificate

Figure 31. Proxy Auto-Configuration (PAC)

b. Select from the drop-down menu at least one Root Certificate. The Zscaler Root Certificate used for SSL inspection by ZIA is listed by default in the drop-down menu. If your organization uses custom root certificates for SSL inspection, you can add (government agencies, see add) them before creating isolation profiles. You can add up to ten root certificates for your organization. To learn more, see About ZIA Root Certificates for Isolation (government agencies, see About ZIA Root Certificates for Isolation).

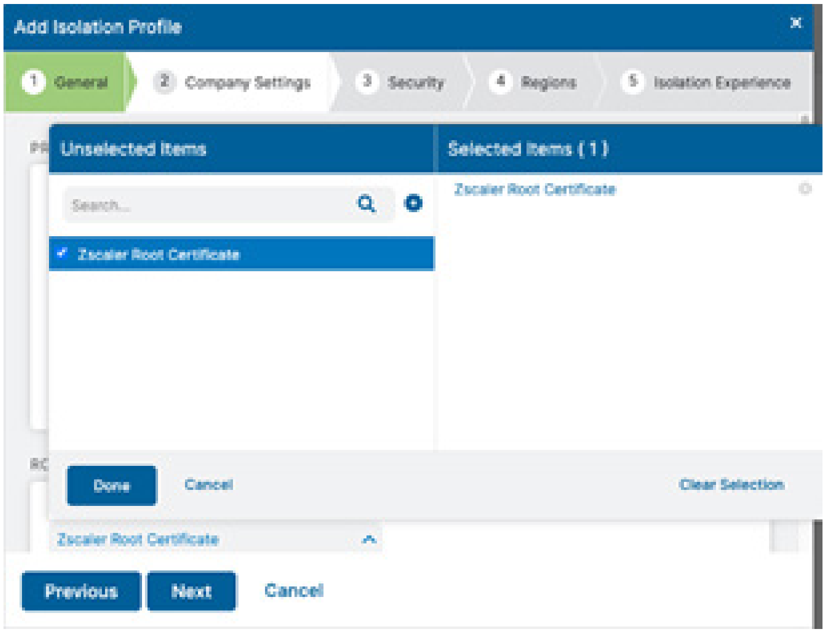
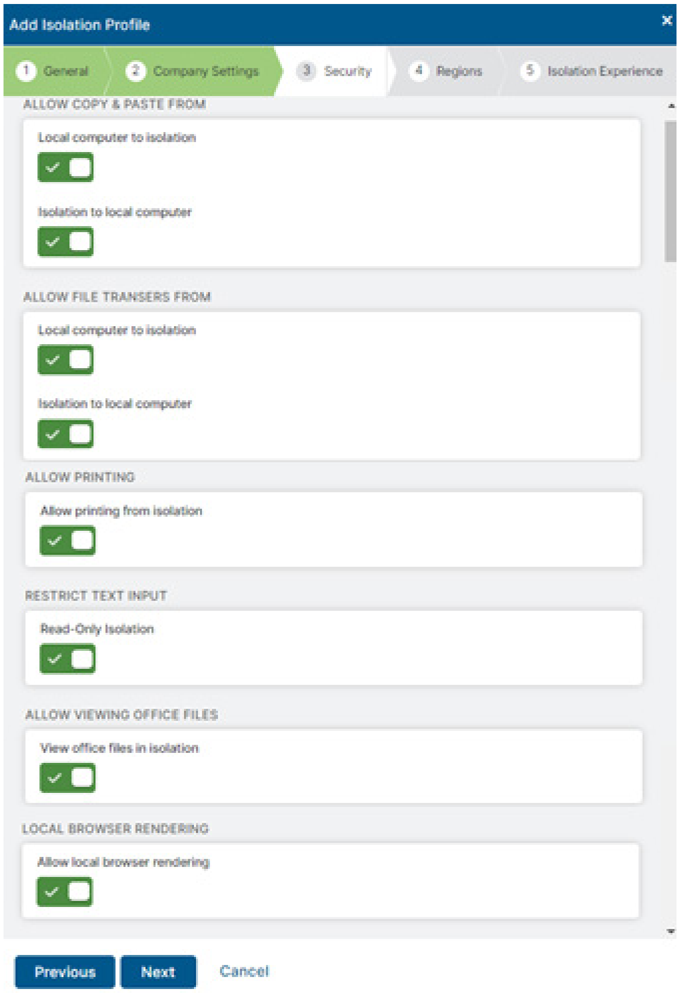


Figure 32. Zscaler Root Certificate

3. Click **Done**.
4. Click **Next**.

5. The Security Control of Browser Isolation allows administrators to maintain a complete air gap between the user and GitLab or allow some level of control of the GitLab application in the Isolation Session. Enable or disable the different settings in the Security section:
   - Allow copying and pasting to and from your computer and the isolation browser.
   - Allow file transfers to and from your computer and the isolation browser.
   - Allow printing of web pages and inline content from isolation.
   - Restrict keyboard/text input to isolated web pages.
   - Allow viewing office files while in isolation.
   - Allow local browser rendering while in isolation.



ALLOW COPY & PASTE FROM

Local computer to isolation ✓

Isolation to local computer ✓

ALLOW FILE TRANSFERS FROM

Local computer to isolation ✓

Isolation to local computer ✓

ALLOW PRINTING

Allow printing from isolation ✓

RESTRICT TEXT INPUT

Read-Only Isolation ✓

ALLOW VIEWING OFFICE FILES

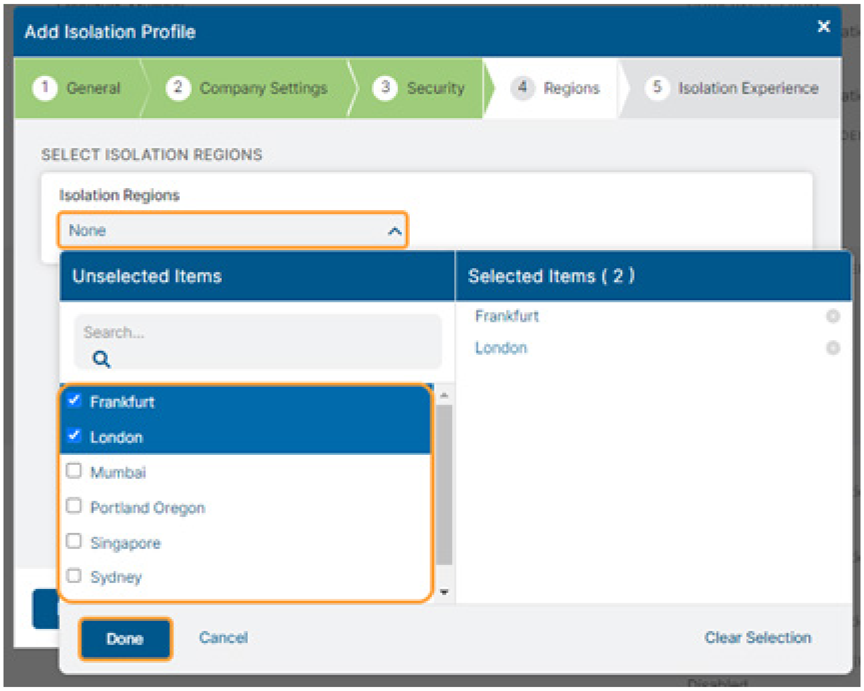
View office files in isolation ✓

LOCAL BROWSER RENDERING

Allow local browser rendering ✓

Figure 33. Security settings

6. Enable at least two Regions for the isolation profile by selecting from the drop-down menu. The isolation containers are leased to the user only from the selected regions based on the least network latency.
7. Click **Done**.
8. Click **Next**.


Add Isolation Profile

1 General · 2 Company Settings · 3 Security · 4 Regions · 5 Isolation Experience

SELECT ISOLATION REGIONS

Isolation Regions: None

Unselected Items	Selected Items (2)
Search...	Frankfurt
☑ Frankfurt	London
☑ London	
□ Mumbai	
□ Portland Oregon	
□ Singapore	
□ Sydney	

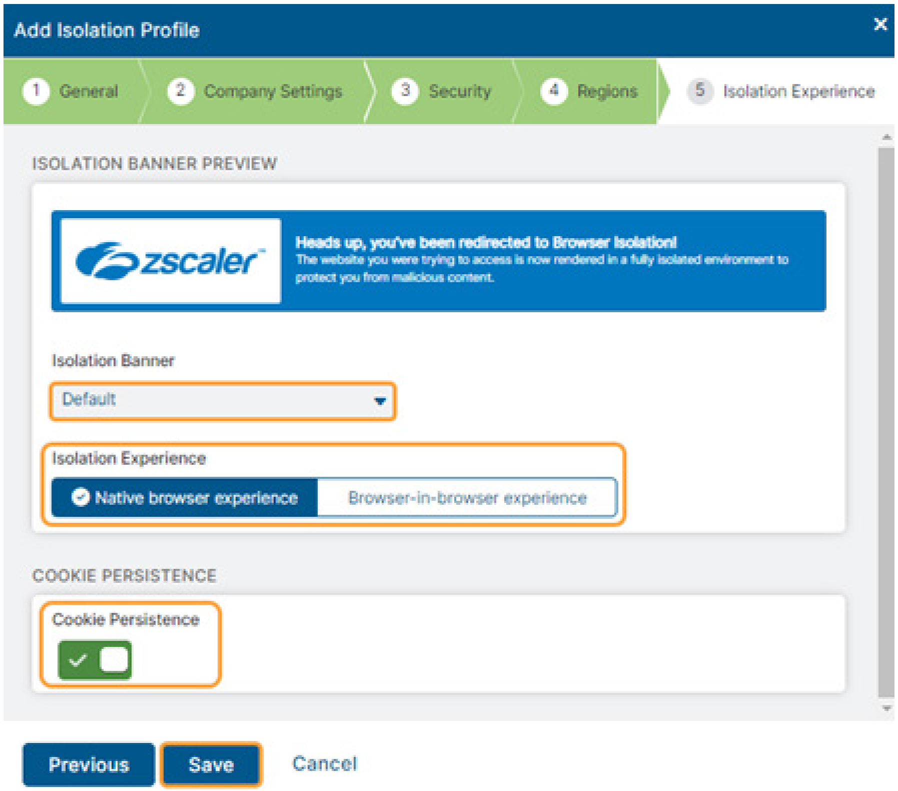
Figure 34. Select Isolation Regions

9. Make your selections for the user's Isolation Experience:

   a. Select an **Isolation Banner** from the drop-down menu. The option you choose shows a preview banner in the window. You choose from existing banners or create custom isolation banners to use for your isolation profiles. To learn more, see Adding a Banner Theme for the Isolation End User Notification in ZIA (government agencies, see Adding a Banner Theme for the Isolation End User Notification in ZIA).

   b. Select the **Isolation Experience** mode:

      - **Native browser experience**: This mode provides the user with a browsing experience similar to accessing the native web page natively typical browser. You can also customize this view.
      - **Browser-in-browser experience**: This mode provides the user with the complete look and feel of an isolated session experience. To learn more, see User Experience Modes in Isolation (government agencies, see User Experience Modes in Isolation).



Add Isolation Profile

1 General · 2 Company Settings · 3 Security · 4 Regions · 5 Isolation Experience

ISOLATION BANNER PREVIEW

Heads up, you've been redirected to Browser Isolation!
The website you were trying to access is now rendered in a fully isolated environment to protect you from malicious content.

Isolation Banner: Default

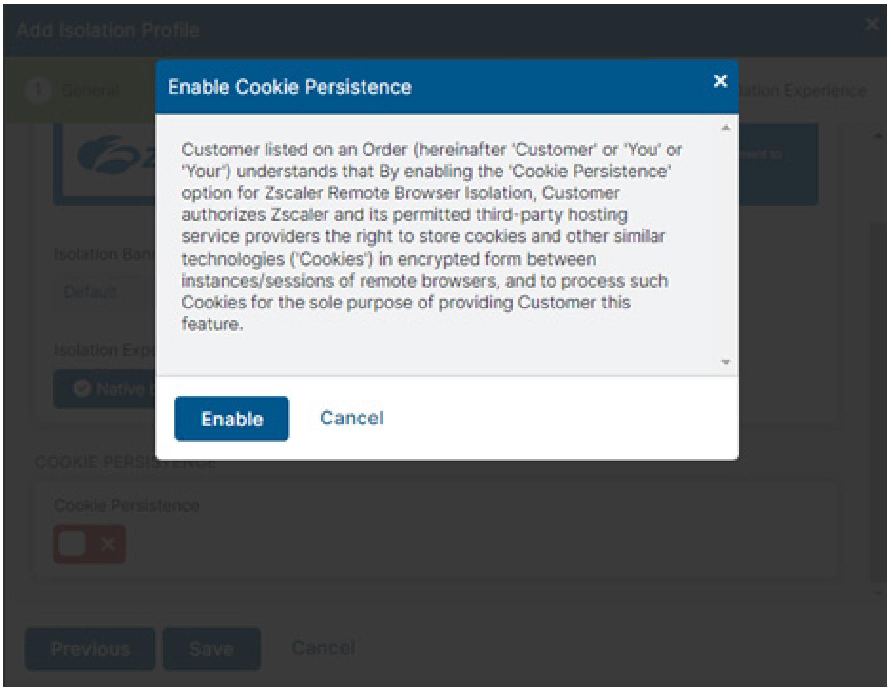
Isolation Experience: Native browser experience (selected) | Browser-in-browser experience

COOKIE PERSISTENCE

Cookie Persistence: ✓ (on)

Figure 35. Isolation Experience

c. (Optional) Enable **Cookie Persistence**. Upon enabling, the **Enable Cookie Persistence** window displays the consent message for the admin to read before enabling. This action means the cookies set by the websites and accessed by a user through isolation persist across browsing sessions. If this option is enabled, the cookies are stored in an encrypted storage. If not enabled, no cookies persist, meaning they are destroyed with the container upon the user's logout or upon exceeding the session timeout.



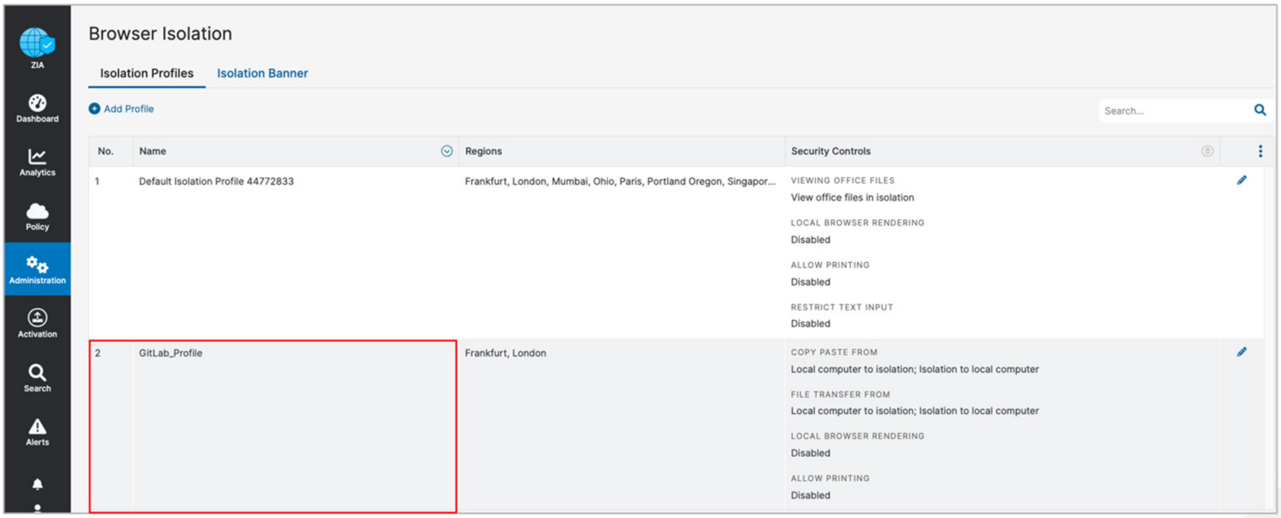
Enable Cookie Persistence

Customer listed on an Order (hereinafter 'Customer' or 'You' or 'Your') understands that By enabling the 'Cookie Persistence' option for Zscaler Remote Browser Isolation, Customer authorizes Zscaler and its permitted third-party hosting service providers the right to store cookies and other similar technologies ('Cookies') in encrypted form between instances/sessions of remote browsers, and to process such Cookies for the sole purpose of providing Customer this feature.

Figure 36. Enable cookie persistence

d. Click **Save**.

When saved, your new isolation profile appears in the list of ZIA **Isolation Profiles**. You can edit a profile directly from the list. To learn more, see [Editing Your ZIA Isolation Profile]() and [Deleting Your ZIA Isolation Profile]() (government agencies, see [Editing Your ZIA Isolation Profile]() and [Deleting Your ZIA Isolation Profile]()).



Browser Isolation

No.	Name	Regions	Security Controls
1	Default Isolation Profile 44772833	Frankfurt, London, Mumbai, Ohio, Paris, Portland Oregon, Singapor...	VIEWING OFFICE FILES View office files in isolation LOCAL BROWSER RENDERING Disabled ALLOW PRINTING Disabled RESTRICT TEXT INPUT Disabled
2	GitLab_Profile	Frankfurt, London	COPY PASTE FROM Local computer to isolation; Isolation to local computer FILE TRANSFER FROM Local computer to isolation; Isolation to local computer LOCAL BROWSER RENDERING Disabled ALLOW PRINTING Disabled

Figure 37. Isolation Profile

You can use this isolation profile to create a policy in ZIA to allow traffic forwarding through browser isolation. To learn more, see [Configuring ZIA for Isolation]() (government agencies, see [Configuring ZIA for Isolation]()).

Configure GitLab 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, select **Add SaaS Application Tenant**.

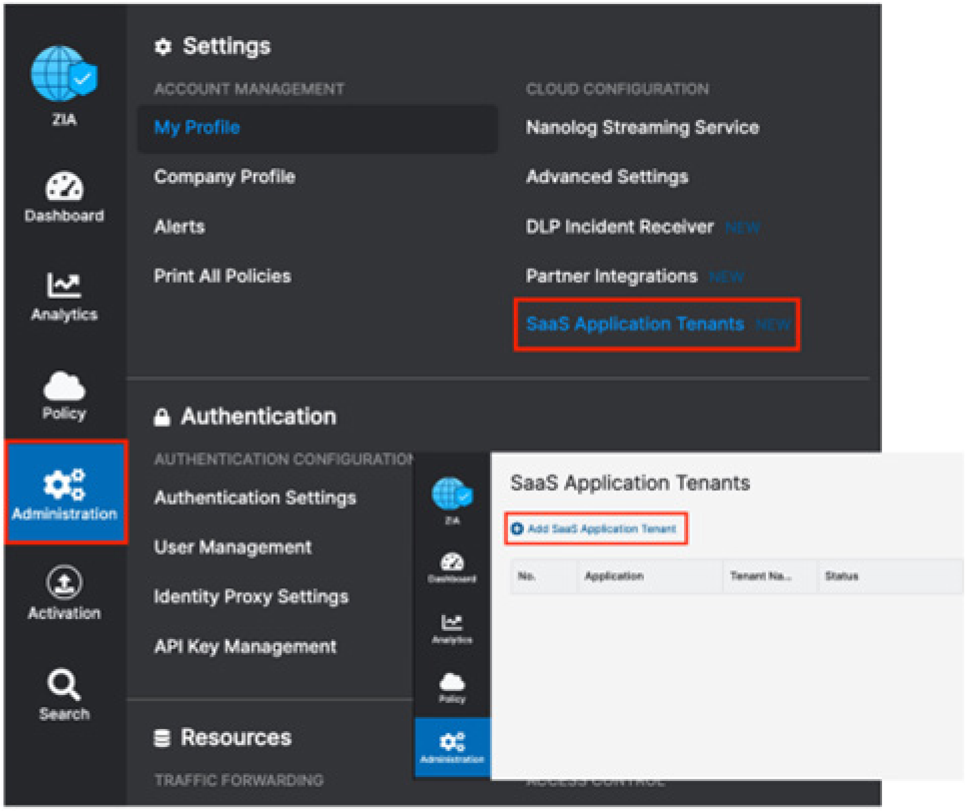


Figure 38. ZIA SaaS Application Tenant

GitLab SaaS Tenant Configuration Wizard

To start the wizard:

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

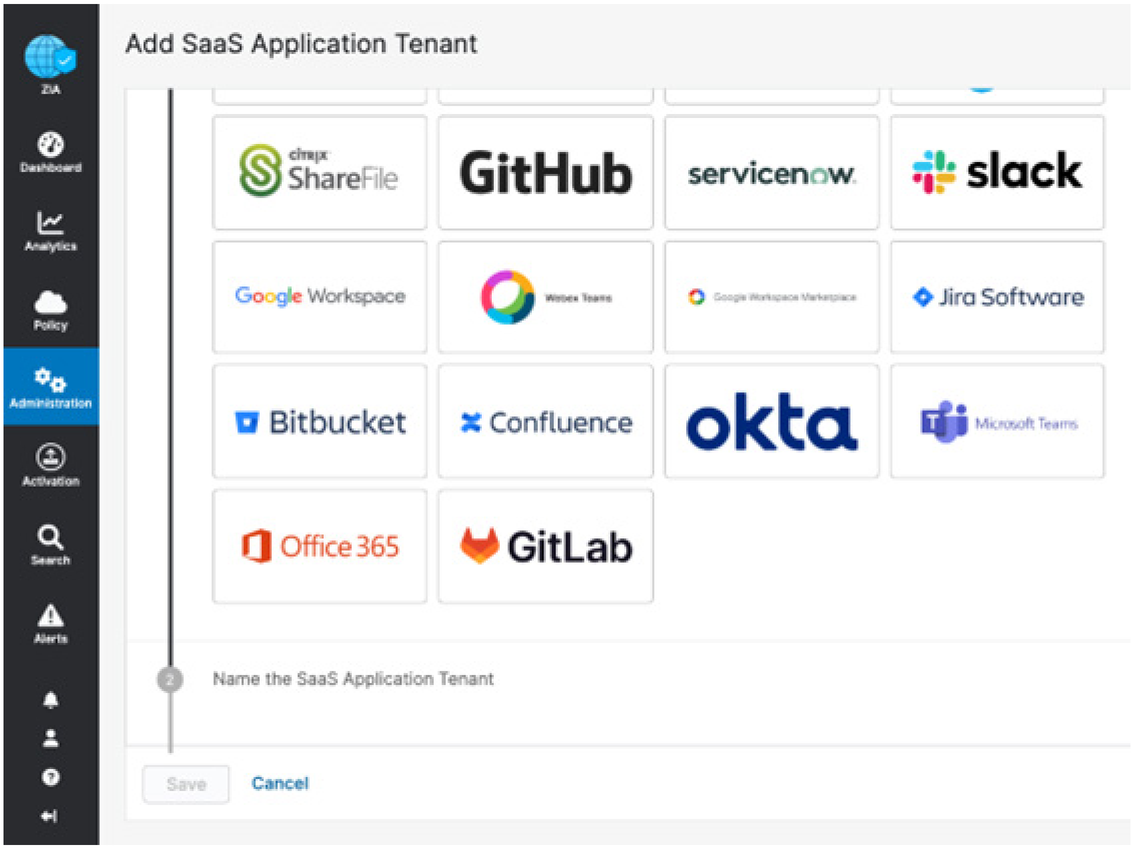
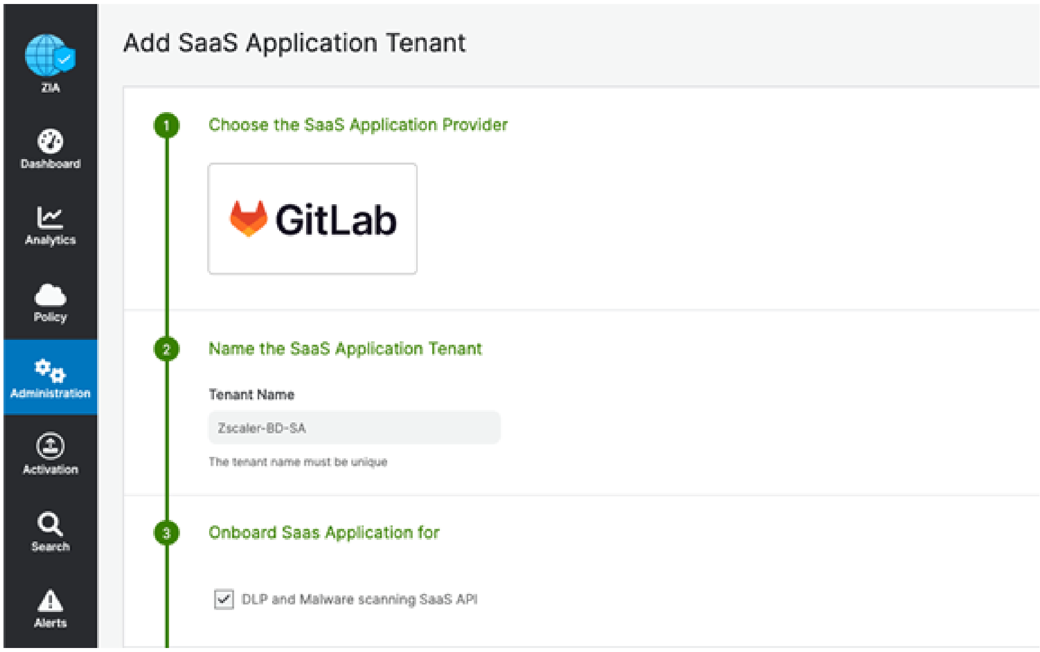


Figure 39. GitLab SaaS Application Tenant

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. Select the **DLP and Malware Scanning SaaS API** checkbox.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

GitLab

2 Name the SaaS Application Tenant

Tenant Name

Zscaler-BD-SA

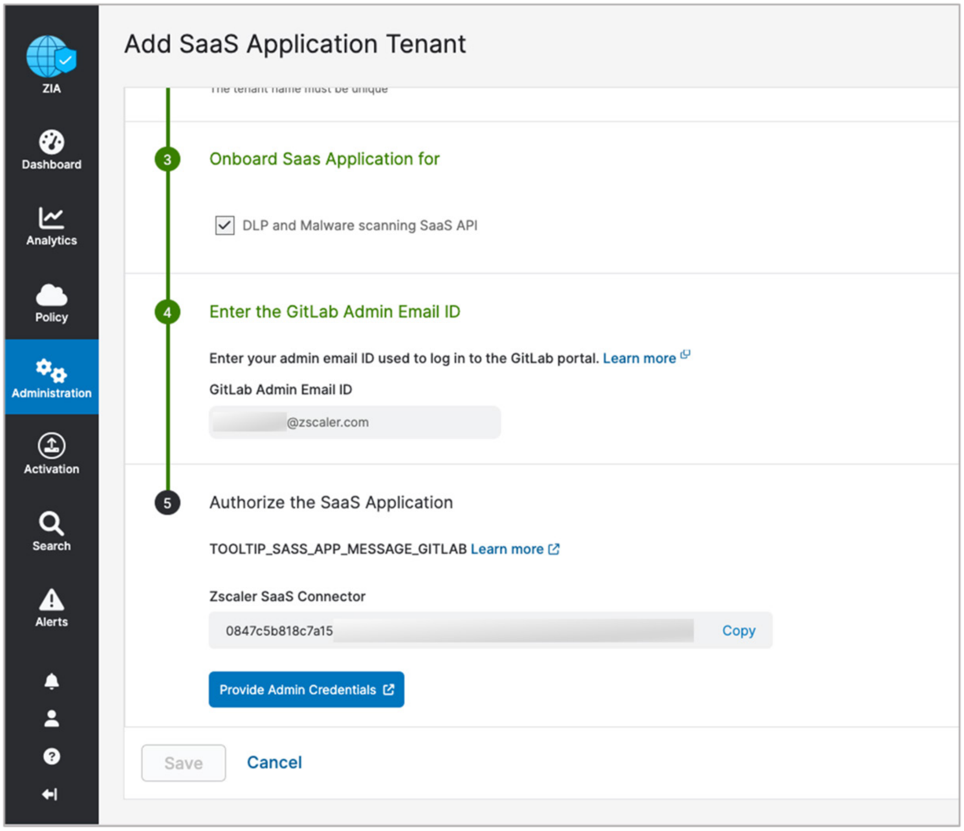
The tenant name must be unique

3 Onboard Saas Application for

☑ DLP and Malware scanning SaaS API

Figure 40. SaaS Application Tenant configuration

5. Enter the **GitLab Admin Email ID**.
6. Click **Provide Admin Credentials**, which redirects you to the **GitLab login** page.



Add SaaS Application Tenant

The tenant name must be unique

3 Onboard Saas Application for

☑ DLP and Malware scanning SaaS API

4 Enter the GitLab Admin Email ID

Enter your admin email ID used to log in to the GitLab portal. Learn more

GitLab Admin Email ID

[redacted]@zscaler.com

5 Authorize the SaaS Application

TOOLTIP_SASS_APP_MESSAGE_GITLAB Learn more

Zscaler SaaS Connector

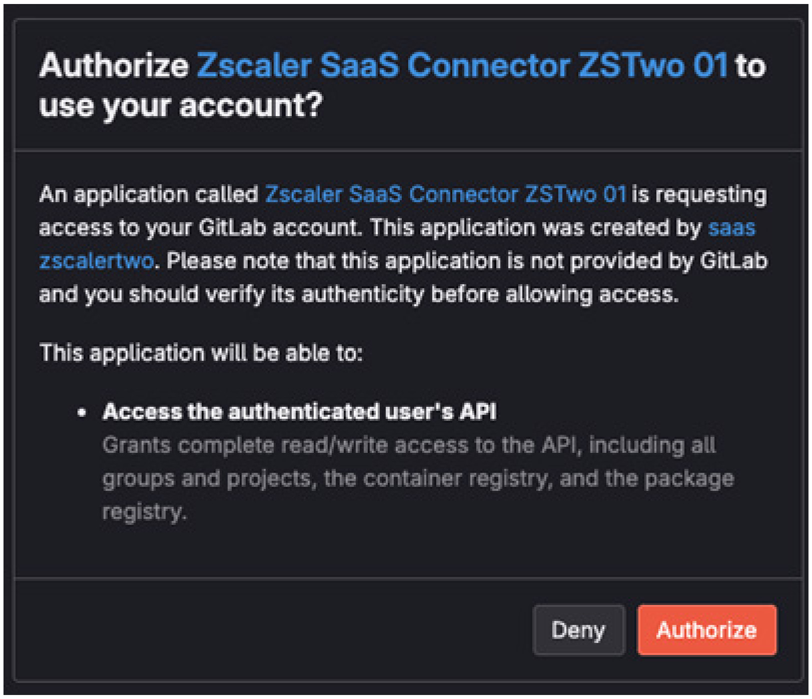
0847c5b818c7a15[redacted] Copy

Provide Admin Credentials

Save Cancel

Figure 41. SaaS Application Tenant configuration

7. Click **Authorize** to give permission to Zscaler SaaS Connector.



Authorize Zscaler SaaS Connector ZSTwo 01 to use your account?

An application called Zscaler SaaS Connector ZSTwo 01 is requesting access to your GitLab account. This application was created by saas zscalertwo. Please note that this application is not provided by GitLab and you should verify its authenticity before allowing access.

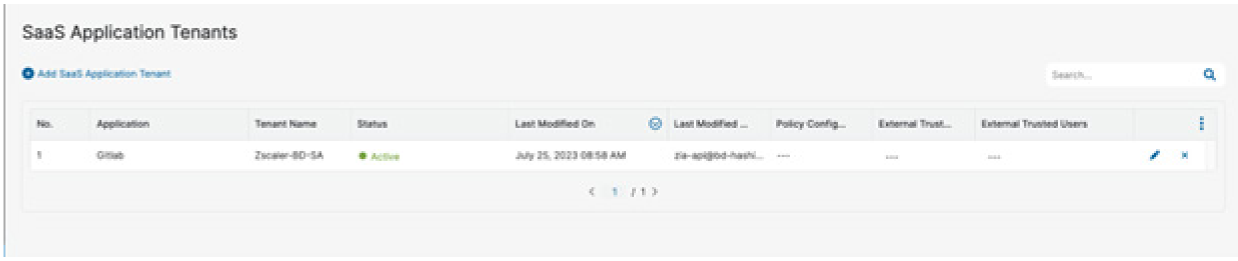
This application will be able to:

- **Access the authenticated user's API**
  Grants complete read/write access to the API, including all groups and projects, the container registry, and the package registry.

Figure 42. Authorize Zscaler SaaS Connector

8. The Z**scaler Onboard window** is displayed. Click **Save**.

The completed and active GitLab API connector is displayed.



SaaS Application Tenants

No.	Application	Tenant Name	Status	Last Modified On	Last Modified ...	Policy Config...	External Trust...	External Trusted Users
1	Gitlab	Zscaler-BD-SA	Active	July 25, 2023 08:58 AM	zia-api@bd-hashi...	---	---	---

Figure 43. GitLab SaaS Tenant Activation Complete

Configure GitLab Policies and Scan Configuration

After adding and configuring the GitLab 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 GitLab in analytics, SaaS security insights, and logs.

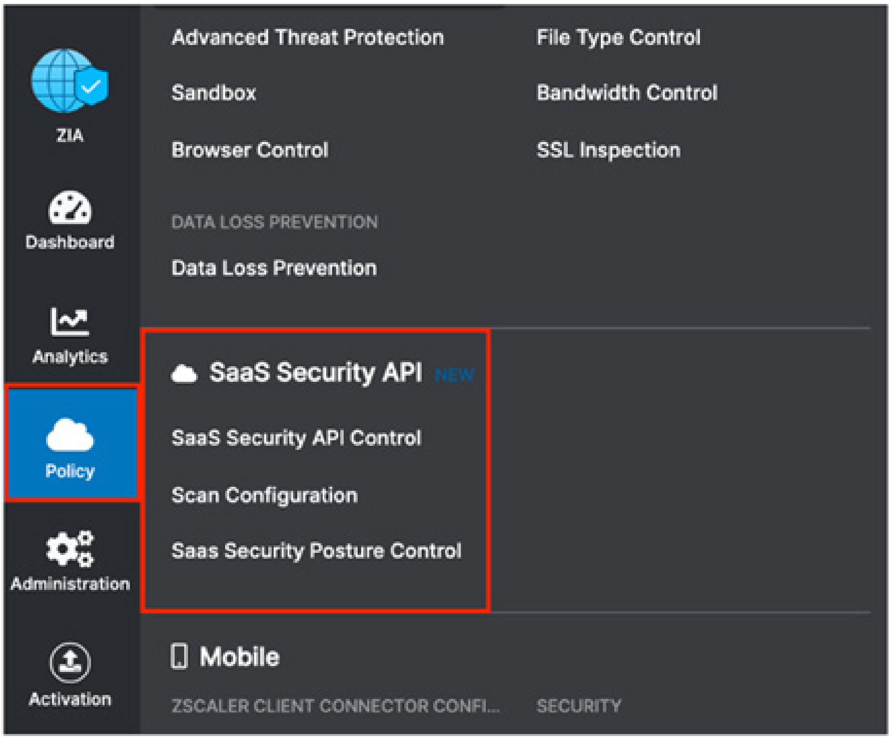


Figure 44. SaaS Security API configuration

Scoping the Policies and Remediation

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

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 would otherwise go unnoticed.

The DLP policy creates 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. A true DLP policy review would need to be conducted 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 GitLab 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 GitLab tenant. If you already have DLP policies created, skip ahead to **Configure a SaaS Malware Policy for GitLab**.

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.

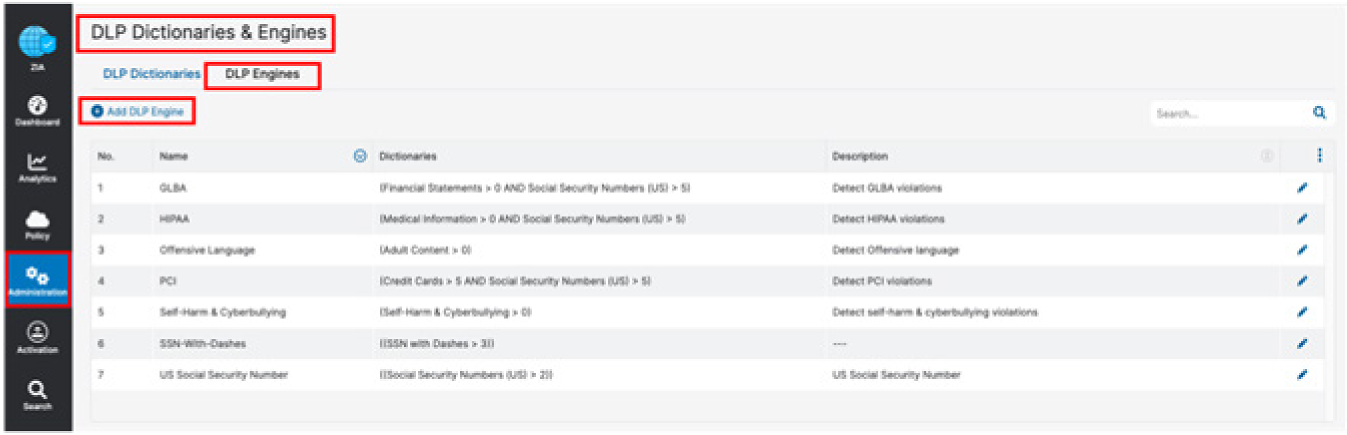
A SaaS security DLP policy is created that allows you to specify the details about where, when, the action taken, and whom to inform about violations.

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. Select the **DLP Engines** tab.
2. Select **Add DLP Engine**.

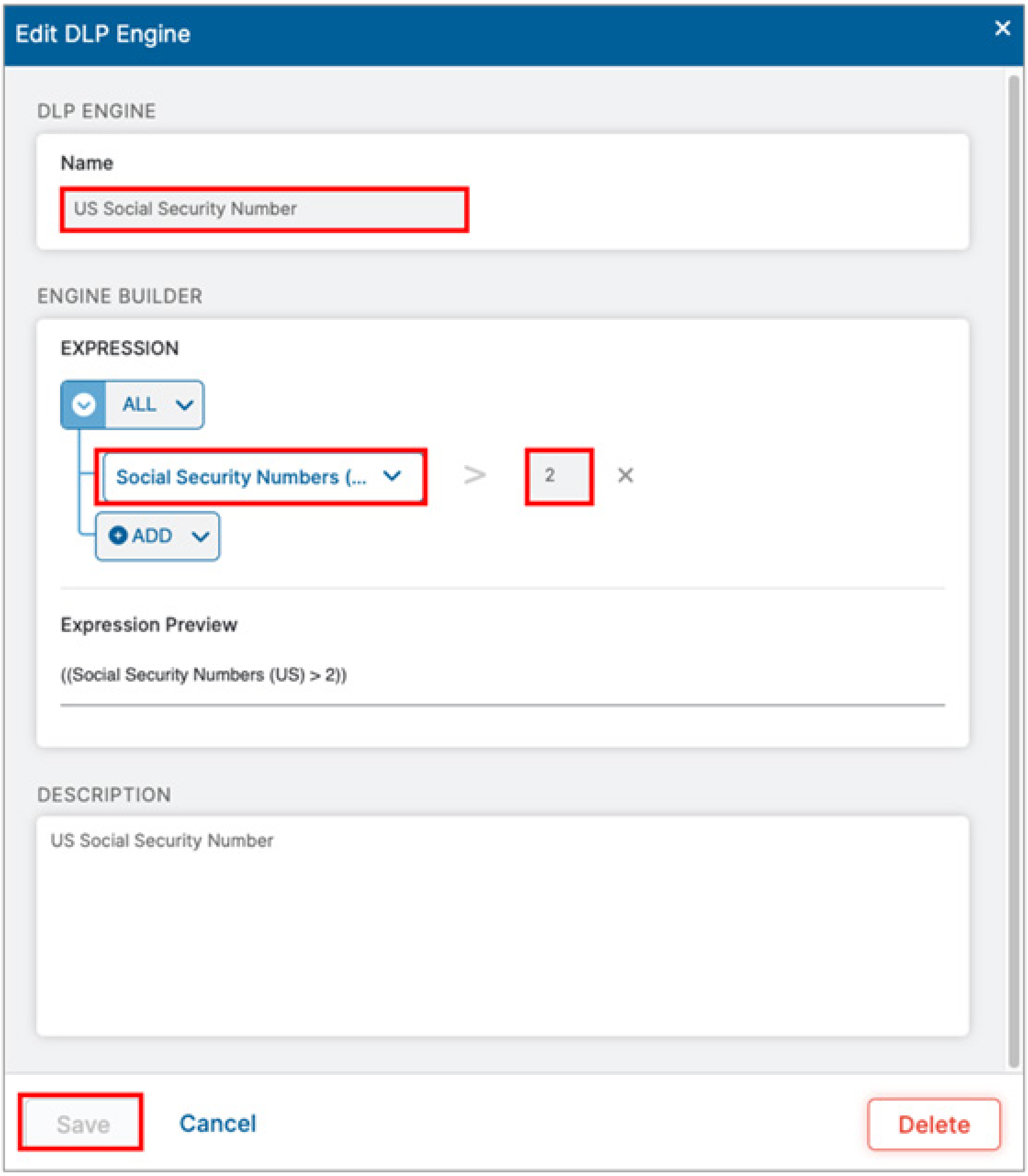


DLP Dictionaries & Engines

No.	Name	Dictionaries	Description
1	GLBA	((Financial Statements > 0 AND Social Security Numbers (US) > 5))	Detect GLBA violations
2	HIPAA	((Medical Information > 0 AND Social Security Numbers (US) > 5))	Detect HIPAA violations
3	Offensive Language	((Adult Content > 0))	Detect Offensive language
4	PCI	((Credit Cards > 5 AND Social Security Numbers (US) > 5))	Detect PCI violations
5	Self-Harm & Cyberbullying	((Self-Harm & Cyberbullying > 0))	Detect self-harm & cyberbullying violations
6	SSN-With-Dashes	((SSN with Dashes > 3))	---
7	US Social Security Number	((Social Security Numbers (US) > 2))	US Social Security Number

Figure 45. 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.
7. Click **Save**, then **Activate** the configuration.



Edit DLP Engine

DLP ENGINE

Name: US Social Security Number

ENGINE BUILDER

EXPRESSION

Expression Preview

((Social Security Numbers (US) > 2))

DESCRIPTION

US Social Security Number

Figure 46. The DLP engine wizard

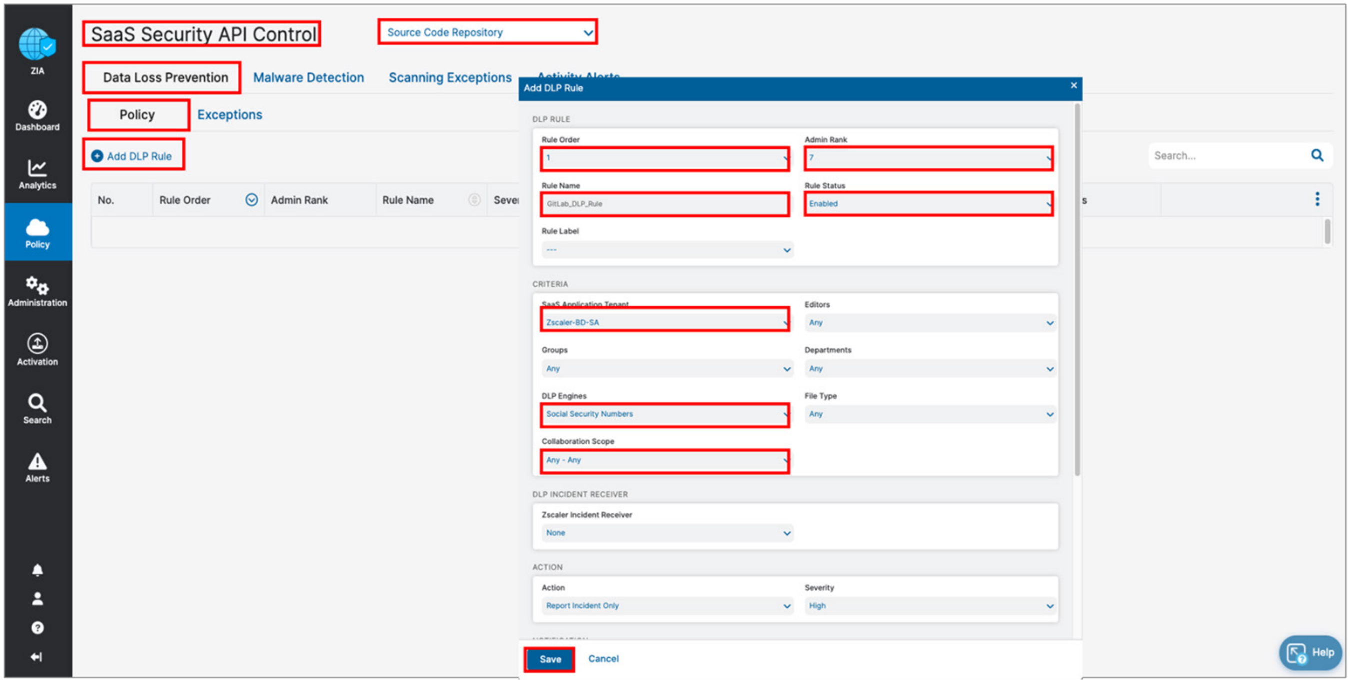
This policy triggers when you see the third Social Security number. Again, this is a demonstration, and the criteria is too general to be a production DLP rule.

©2024 Zscaler, Inc. All rights reserved.

Configure a SaaS DLP Policy for GitLab

Apply the engine to a DLP policy used for the GitLab 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. Select **Add DLP Rule**.
4. Select the **GitLab SaaS Tenant**.
5. Select the DLP Engine created in **GitLab 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.



Add DLP Rule

DLP RULE

Rule Order: 1
Admin Rank: 7
Rule Name: GitLab_DLP_Rule
Rule Status: Enabled
Rule Label: ---

CRITERIA

SaaS Application Tenant: Zscaler-BD-SA
Editors: Any
Groups: Any
Departments: Any
DLP Engines: Social Security Numbers
File Type: Any
Collaboration Scope: Any - Any

DLP INCIDENT RECEIVER

Zscaler Incident Receiver: None

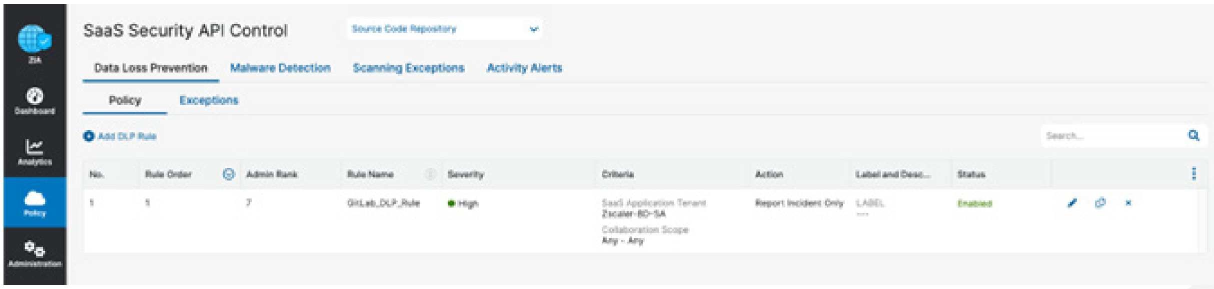
ACTION

Action: Report Incident Only
Severity: High

Save Cancel

Figure 47. Launch the SaaS DLP Policy configuration wizard

The complete GitLab DLP rule is ready to be applied with a scanning schedule.



No.	Rule Order	Admin Rank	Rule Name	Severity	Criteria	Action	Label and Desc...	Status
1	1	7	GitLab_DLP_Rule	● High	SaaS Application Tenant Zscaler-BD-SA Collaboration Scope Any - Any	Report Incident Only	LABEL ---	Enabled

Figure 48. Launch the SaaS DLP Policy configuration wizard

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:

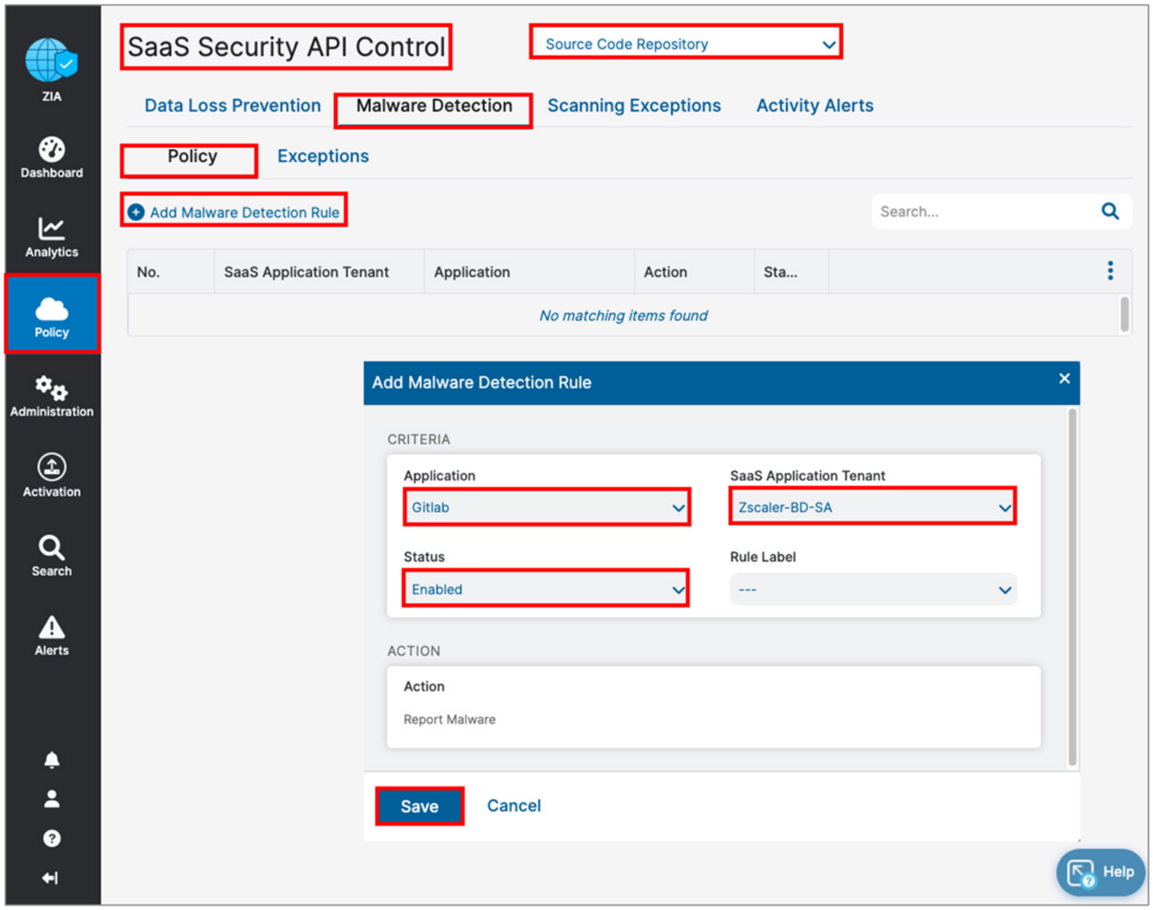
- External Collaborators: Files that are shared with specific collaborators outside of your organization.
- External Link: Files with shareable links that allow anyone outside your organization to find the files and have access.
- Internal Collaborators: Files that are shared with specific collaborators 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 takes upon detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant. For GitLab, the action is Report 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 the incident only and makes no changes to the file's collaboration scope.

Configure a SaaS Malware Policy for GitLab

To launch the Malware Rule wizard:

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

The action for GitLab is limited to reporting malware only.



Source Code Repository

No.	SaaS Application Tenant	Application	Action	Sta...

No matching items found

Add Malware Detection Rule

CRITERIA

Application: Gitlab

SaaS Application Tenant: Zscaler-BD-SA

Status: Enabled

Rule Label: ---

ACTION

Action: Report Malware

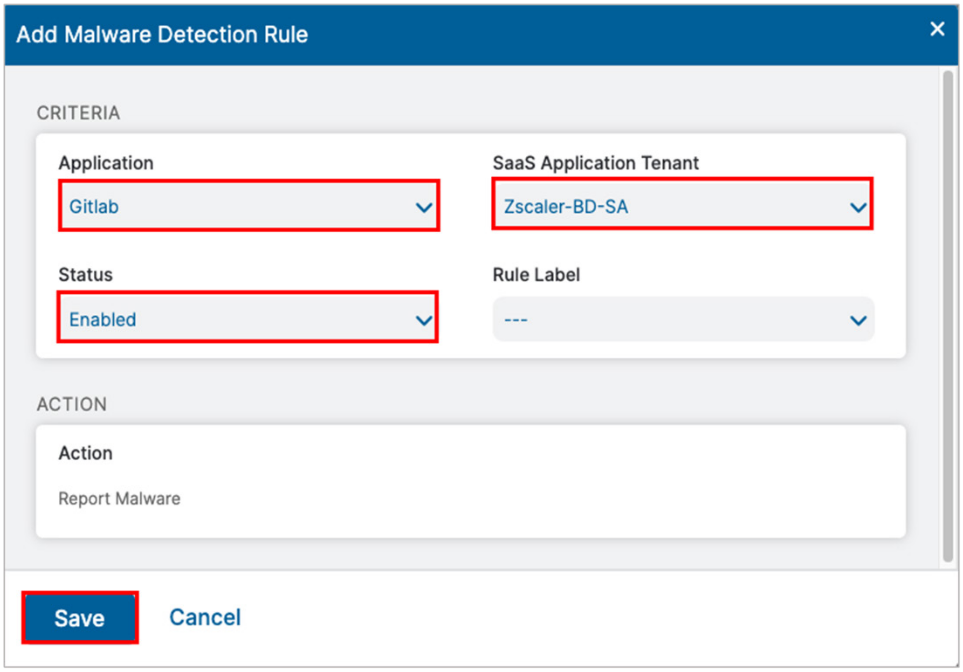
Save   Cancel

Figure 49. Launch the Malware Policy configuration Wizard

GitLab SaaS Malware Policy Wizard

Configure the malware Rule wizard:

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



Add Malware Detection Rule

CRITERIA

Application: Gitlab

SaaS Application Tenant: Zscaler-BD-SA

Status: Enabled

Rule Label: ---

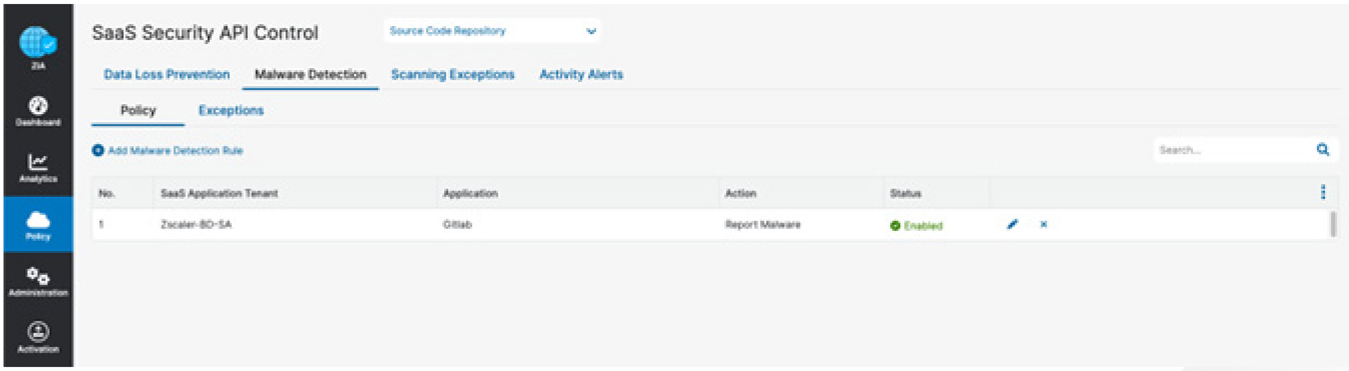
ACTION

Action: Report Malware

Figure 50. The Malware Policy configuration wizard

GitLab SaaS Malware Policy

Apply the completed SaaS security malware policy for the GitLab SaaS tenant to the GitLab instance with a scanning schedule. Activate your configuration.



SaaS Security API Control — Source Code Repository

No.	SaaS Application Tenant	Application	Action	Status
1	Zscaler-BD-SA	Gitlab	Report Malware	Enabled

Figure 51. The complete GitLab Malware Policy configuration

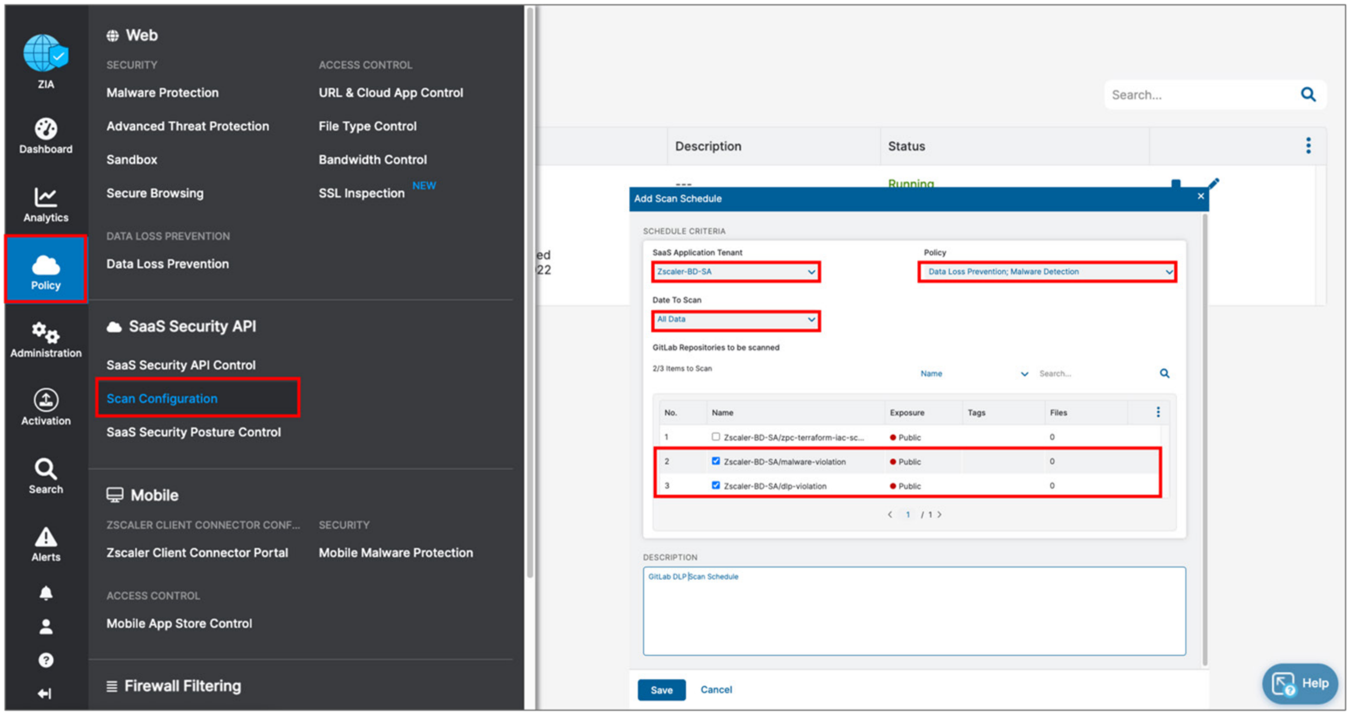
Configure a Scan Schedule Configuration for GitLab

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 Control** > **Scan Configuration** > **Add Scan Schedule**.
2. Select the GitLab SaaS tenant for the **SaaS Application Tenant**.
3. Select the data loss 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.



Add Scan Schedule

SCHEDULE CRITERIA

SaaS Application Tenant: Zscaler-BD-SA

Policy: Data Loss Prevention; Malware Detection

Date To Scan: All Data

GitLab Repositories to be scanned

2/3 Items to Scan

No.	Name	Exposure	Tags	Files
1	□ Zscaler-BD-SA/zpc-terraform-iac-sc...	● Public		0
2	☑ Zscaler-BD-SA/malware-violation	● Public		0
3	☑ Zscaler-BD-SA/dlp-violation	● Public		0

DESCRIPTION

GitLab DLP Scan Schedule

Save Cancel

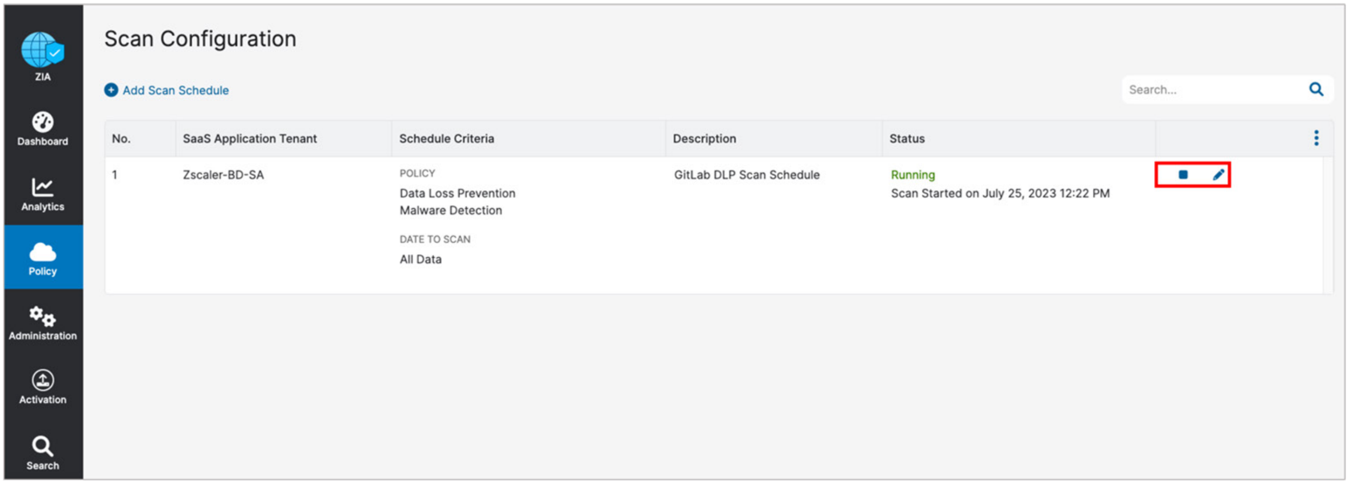
Figure 52. Create and enable a scan for the GitLab SaaS tenant

©2024 Zscaler, Inc. All rights reserved.

Start the Scan Schedule for GitLab

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

1. Select the **Start** icon on the scan configuration to start SaaS Security API on the GitLab tenant.
2. Review the **Status** column and ensure it is **Running** with a start date and a latest scan date.



Scan Configuration

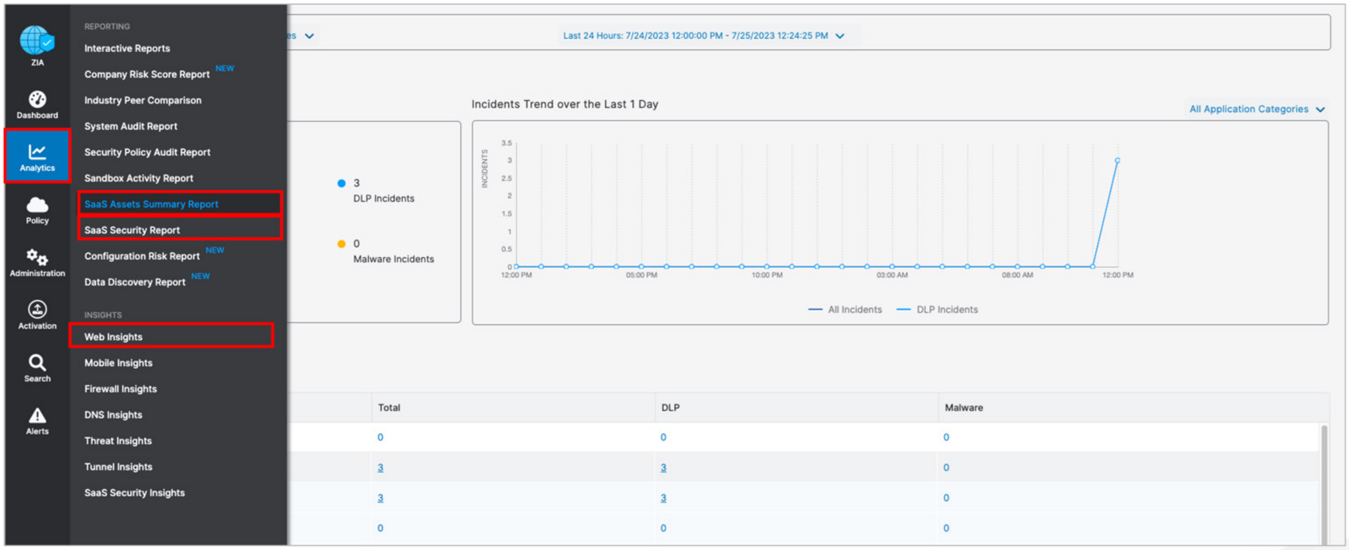
No.	SaaS Application Tenant	Schedule Criteria	Description	Status
1	Zscaler-BD-SA	POLICY Data Loss Prevention Malware Detection DATE TO SCAN All Data	GitLab DLP Scan Schedule	Running Scan Started on July 25, 2023 12:22 PM

Figure 53. Starting the GitLab Scan Schedule

GitLab 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**.



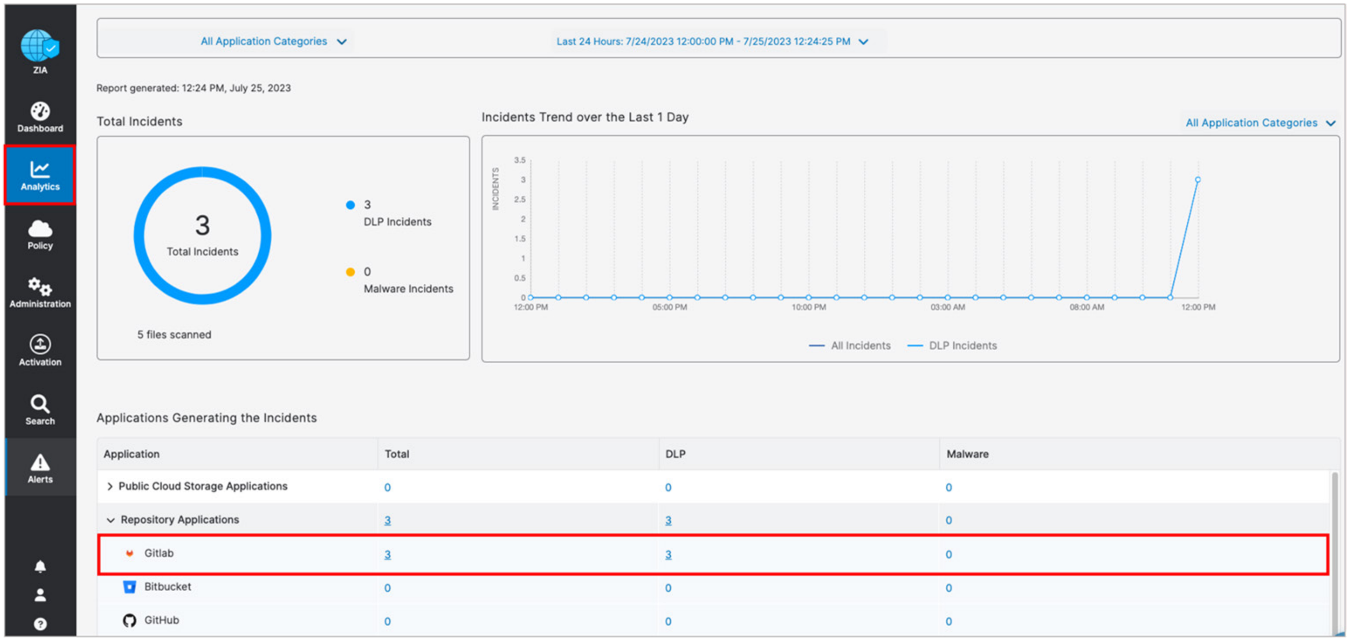
Total	DLP	Malware
0	0	0
3	3	0
3	3	0
0	0	0

Figure 54. SaaS security visibility

SaaS Assets Summary Report

A SaaS Assets Summary Report provides all activity and violations in a quick glance. The report identifies all SaaS tenant information from a single screen. Although your GitLab activity over the creation of this deployment guide is shown, any tenant configured is displayed on this summary screen. 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** incidents number next to the GitLab 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.



Report generated: 12:24 PM, July 25, 2023

Total Incidents

3 Total Incidents

● 3 DLP Incidents

● 0 Malware Incidents

5 files scanned

Applications Generating the Incidents

Application	Total	DLP	Malware
› Public Cloud Storage Applications	0	0	0
⌄ Repository Applications	3	3	0
Gitlab	3	3	0
Bitbucket	0	0	0
GitHub	0	0	0

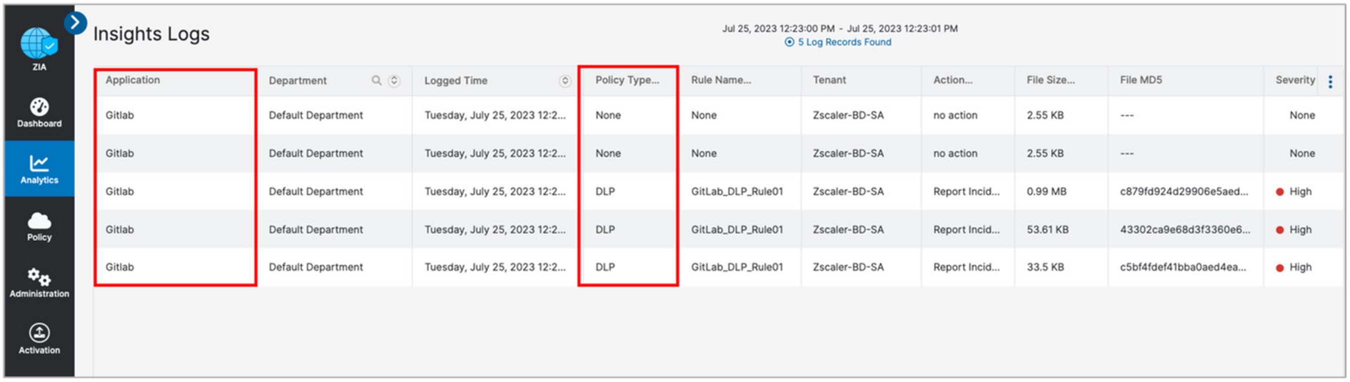
Figure 55. GitLab SaaS Assets Summary reports

SaaS Security Insights

The SaaS Security Insights Log 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 data 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



Insights Logs

Jul 25, 2023 12:23:00 PM - Jul 25, 2023 12:23:01 PM
5 Log Records Found

Application	Department	Logged Time	Policy Type...	Rule Name...	Tenant	Action...	File Size...	File MD5	Severity
Gitlab	Default Department	Tuesday, July 25, 2023 12:2...	None	None	Zscaler-BD-SA	no action	2.55 KB	---	None
Gitlab	Default Department	Tuesday, July 25, 2023 12:2...	None	None	Zscaler-BD-SA	no action	2.55 KB	---	None
Gitlab	Default Department	Tuesday, July 25, 2023 12:2...	DLP	GitLab_DLP_Rule01	Zscaler-BD-SA	Report Incid...	0.99 MB	c879fd924d29906e5aed...	● High
Gitlab	Default Department	Tuesday, July 25, 2023 12:2...	DLP	GitLab_DLP_Rule01	Zscaler-BD-SA	Report Incid...	53.61 KB	43302ca9e68d3f3360e6...	● High
Gitlab	Default Department	Tuesday, July 25, 2023 12:2...	DLP	GitLab_DLP_Rule01	Zscaler-BD-SA	Report Incid...	33.5 KB	c5bf4fdef41bba0aed4ea...	● High

Figure 56. GitLab SaaS security insight

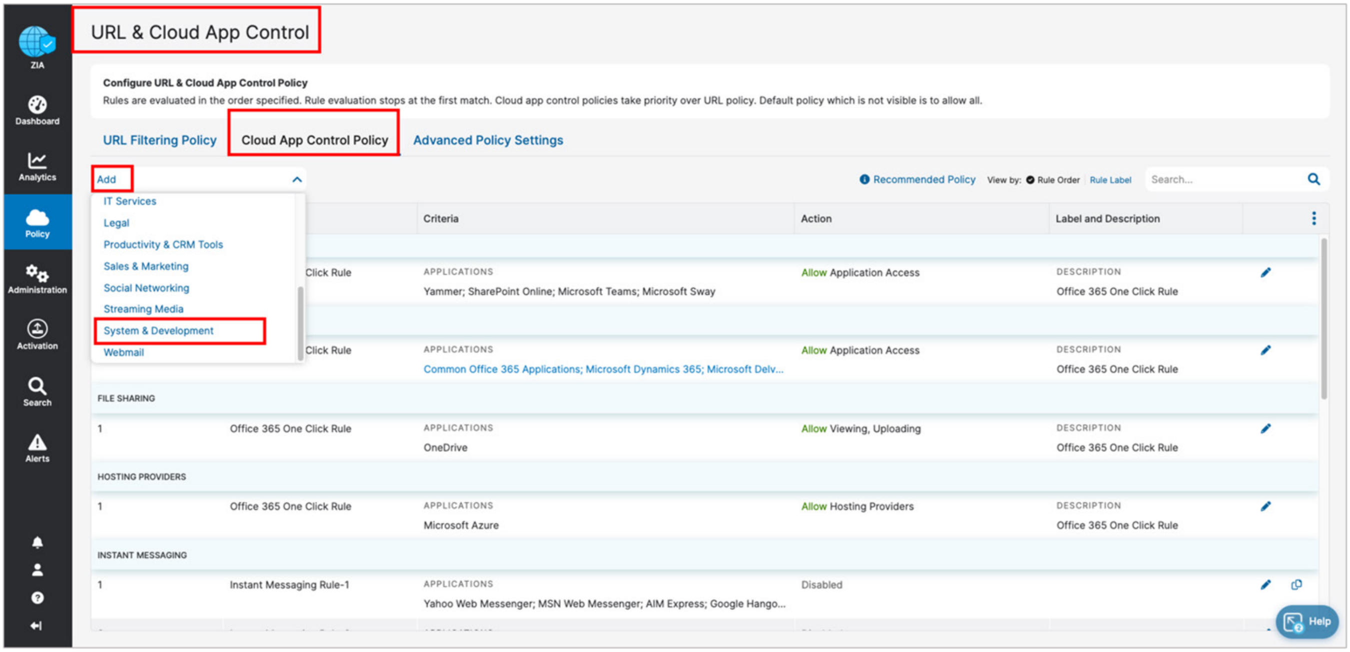
Cloud App Control

The following sections describe how to configure Cloud App Control for use with ServiceNow.

Cloud App Control Policy

Create the policy to allow specific users in a security group to access GitLab:

1. Sign into your organization's ZIA Admin Portal with administrator credentials.
2. Select **Policy**.
3. Select **URL & Cloud App Control**.
4. Select the **Cloud App Control Policy** tab.
5. Select **Add**.
6. Select **System & Development**.



Configure URL & Cloud App Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is to allow all.

		Criteria	Action	Label and Description
	Click Rule	APPLICATIONS Yammer; SharePoint Online; Microsoft Teams; Microsoft Sway	Allow Application Access	DESCRIPTION Office 365 One Click Rule
	Click Rule	APPLICATIONS Common Office 365 Applications; Microsoft Dynamics 365; Microsoft Delv...	Allow Application Access	DESCRIPTION Office 365 One Click Rule
FILE SHARING				
1	Office 365 One Click Rule	APPLICATIONS OneDrive	Allow Viewing, Uploading	DESCRIPTION Office 365 One Click Rule
HOSTING PROVIDERS				
1	Office 365 One Click Rule	APPLICATIONS Microsoft Azure	Allow Hosting Providers	DESCRIPTION Office 365 One Click Rule
INSTANT MESSAGING				
1	Instant Messaging Rule-1	APPLICATIONS Yahoo Web Messenger; MSN Web Messenger; AIM Express; Google Hango...	Disabled	

Figure 57. URL & Cloud App Control

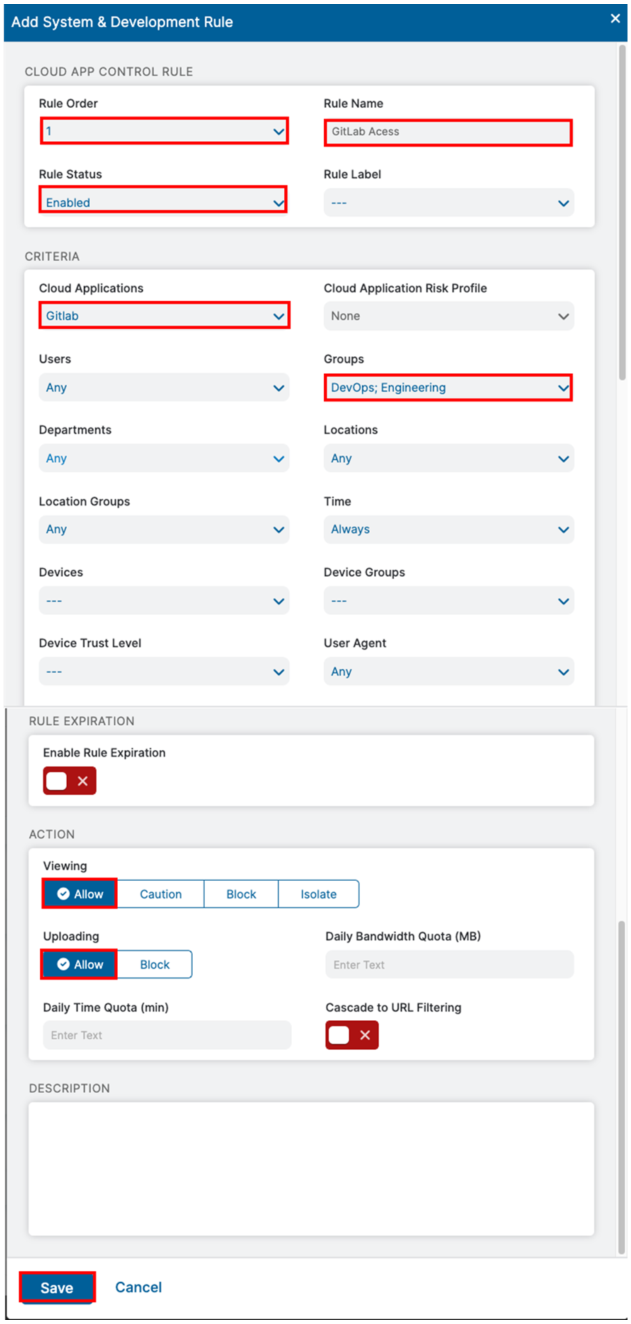
Cloud App Control Policy Wizard

To create an Cloud App Control policy:

1. Set the Rule Order to **1**.
2. Enter an intuitive **Rule Name**.
3. Select **GitLab** for the **Cloud Application**.
4. Select the security **Group** that contains the GitLab users.

5. In **Action**, choose between the viewing and uploading actions.
   a. **Viewing**:
      - **Allow**. Allows users to view the content on the GitLab cloud applications.
      - **Caution**. Warn users with a notification before they can proceed.
      - **Block**. Block users.
      - **Isolate**. Allow users to view the content of a GitLab repository remote browser Isolation.

   b. **Uploading**. Allow or block users from uploading content to a GitLab repository.
6. Click **Save** and then **Activate** changes.



Add System & Development Rule ×

CLOUD APP CONTROL RULE

Rule Order: 1

Rule Name: GitLab Acess

Rule Status: Enabled

Rule Label: ---

CRITERIA

Cloud Applications: Gitlab

Cloud Application Risk Profile: None

Users: Any

Groups: DevOps; Engineering

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

Devices: ---

Device Groups: ---

Device Trust Level: ---

User Agent: Any

RULE EXPIRATION

Enable Rule Expiration: ☒

ACTION

Viewing: [✓ Allow] Caution Block Isolate

Uploading: [✓ Allow] Block

Daily Bandwidth Quota (MB): Enter Text

Daily Time Quota (min): Enter Text

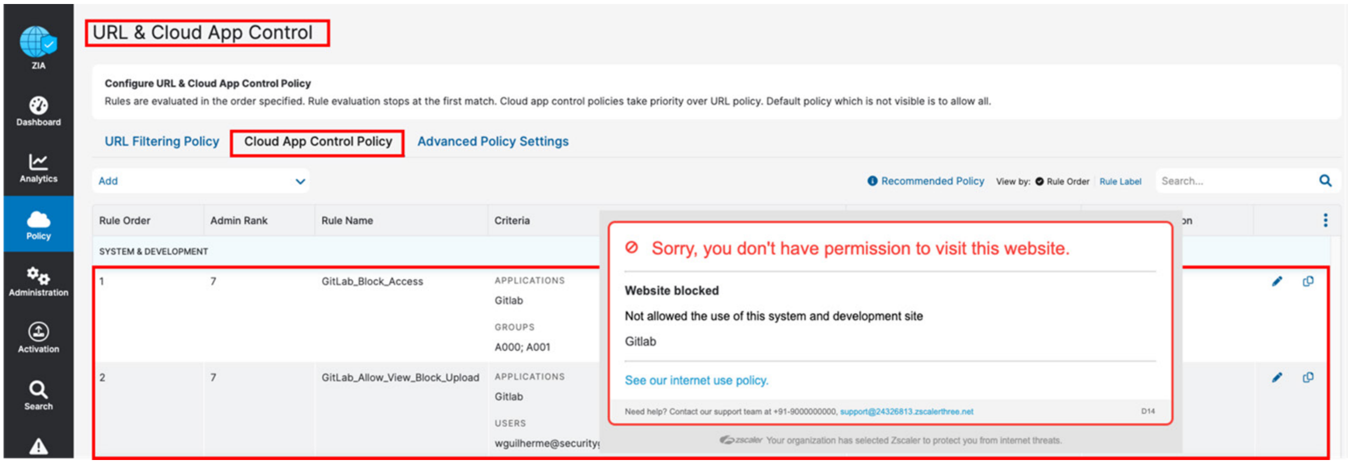
Cascade to URL Filtering: ☒

DESCRIPTION

Save Cancel

Figure 58. Create a Cloud App Control allow policy

Users who try to access the GitLab application through Zscaler and do not have permission get the following Website blocked window. Zscaler administrators receive alerts and logs about the event.



URL & Cloud App Control

Configure URL & Cloud App Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is to allow all.

Rule Order	Admin Rank	Rule Name	Criteria
SYSTEM & DEVELOPMENT			
1	7	GitLab_Block_Access	APPLICATIONS Gitlab GROUPS A000; A001
2	7	GitLab_Allow_View_Block_Upload	APPLICATIONS Gitlab USERS wguilherme@security

Sorry, you don't have permission to visit this website.

Website blocked

Not allowed the use of this system and development site

Gitlab

See our internet use policy.

Need help? Contact our support team at +91-9000000000, support@24326813.zscalerthree.net D14

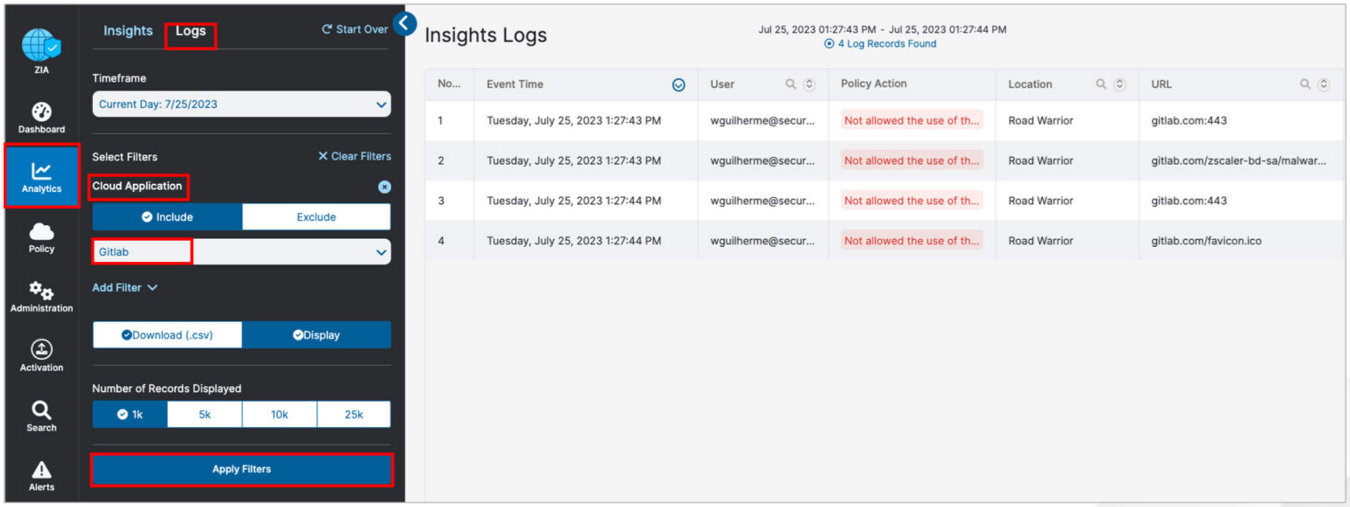
zscaler Your organization has selected Zscaler to protect you from internet threats.

Figure 59. Create a Cloud App Control deny policy

Cloud App Control Logs

Zscaler analytics provide visibility to see any activity for GitLab access, or to get usage reports. To view the GitLab logs for a certain time frame:

1. Sign into your organization's ZIA Admin Portal with administrator credentials.
2. Select **Analytics**.
3. Select **Web Insights**.
4. Select the **Logs** tab.
5. Select the desired time frame, or custom time frame.
6. Select **Add Filter**.
7. Select **Cloud Application**.
8. Select **GitLab**.
9. Click **Apply Filters**.



Timeframe: Current Day: 7/25/2023

Cloud Application: Include: Gitlab

Number of Records Displayed: 1k 5k 10k 25k

Insights Logs

Jul 25, 2023 01:27:43 PM - Jul 25, 2023 01:27:44 PM

4 Log Records Found

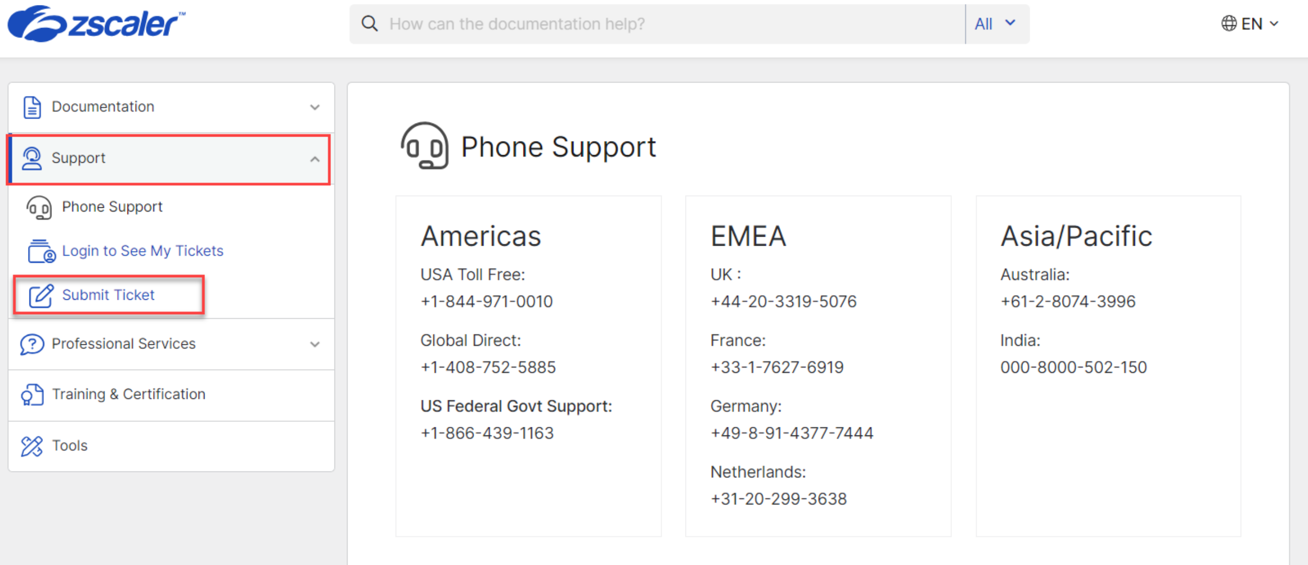
No...	Event Time	User	Policy Action	Location	URL
1	Tuesday, July 25, 2023 1:27:43 PM	wguilherme@secur...	Not allowed the use of th...	Road Warrior	gitlab.com:443
2	Tuesday, July 25, 2023 1:27:43 PM	wguilherme@secur...	Not allowed the use of th...	Road Warrior	gitlab.com/zscaler-bd-sa/malwar...
3	Tuesday, July 25, 2023 1:27:44 PM	wguilherme@secur...	Not allowed the use of th...	Road Warrior	gitlab.com:443
4	Tuesday, July 25, 2023 1:27:44 PM	wguilherme@secur...	Not allowed the use of th...	Road Warrior	gitlab.com/favicon.ico

Figure 60. Create a Cloud App Control log

Appendix A: Requesting Zscaler Support

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**.



Phone Support

Americas

USA Toll Free:
+1-844-971-0010

Global Direct:
+1-408-752-5885

US Federal Govt Support:
+1-866-439-1163

EMEA

UK :
+44-20-3319-5076

France:
+33-1-7627-6919

Germany:
+49-8-91-4377-7444

Netherlands:
+31-20-299-3638

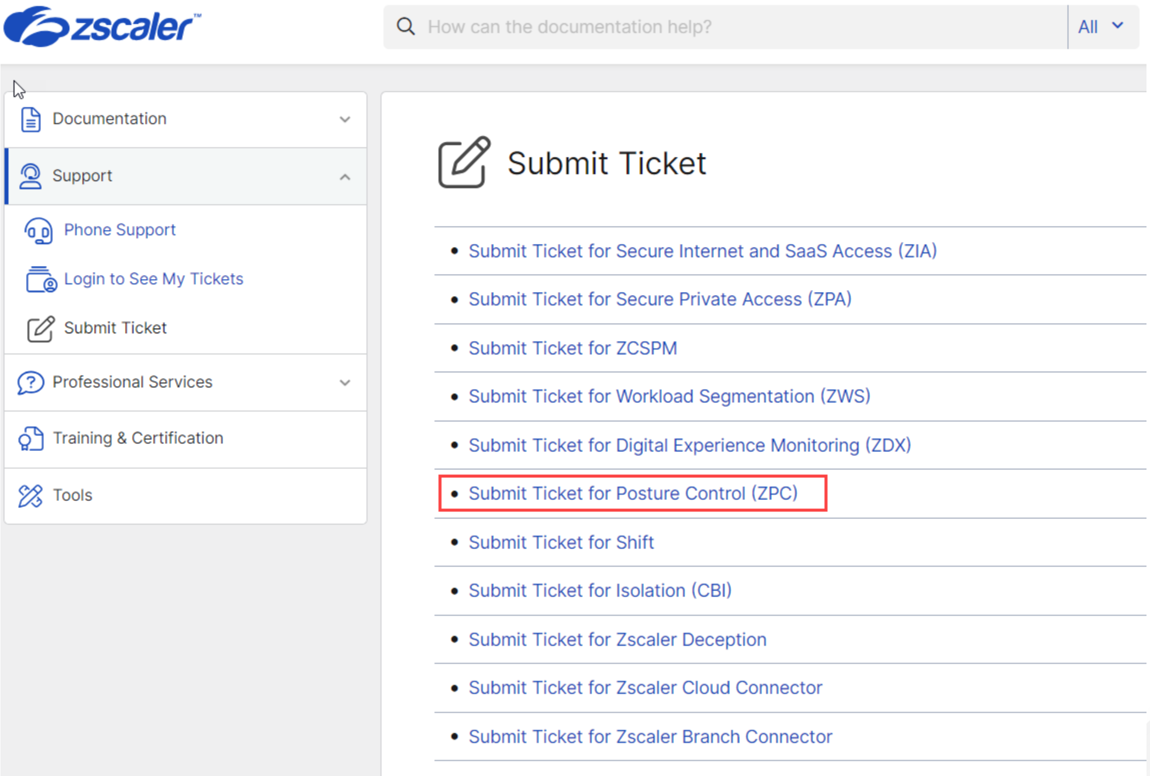
Asia/Pacific

Australia:
+61-2-8074-3996

India:
000-8000-502-150

Figure 61. ZPC Help

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



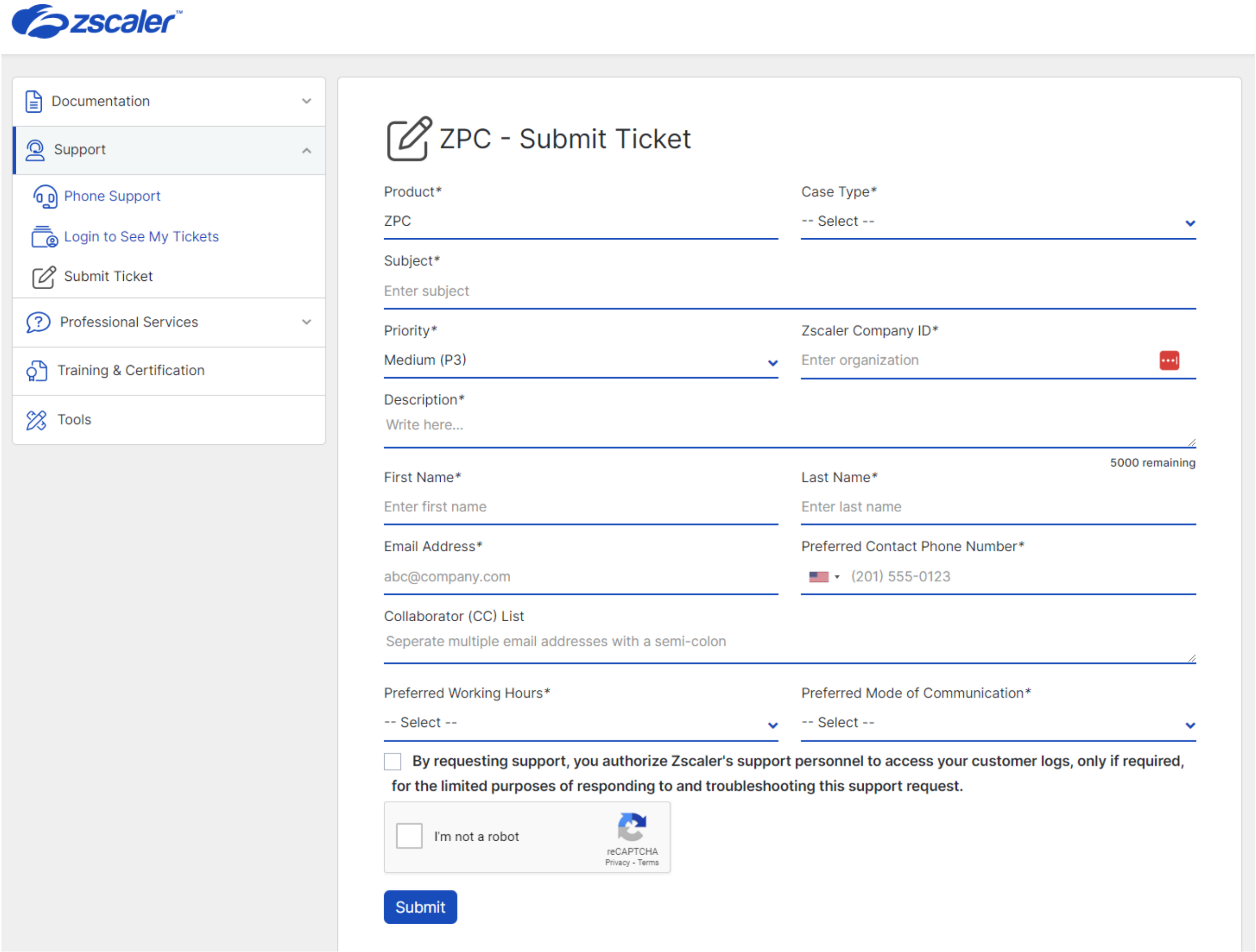
Submit Ticket

- Submit Ticket for Secure Internet and SaaS Access (ZIA)
- Submit Ticket for Secure Private Access (ZPA)
- Submit Ticket for ZCSPM
- Submit Ticket for Workload Segmentation (ZWS)
- Submit Ticket for Digital Experience Monitoring (ZDX)
- Submit Ticket for Posture Control (ZPC)
- Submit Ticket for Shift
- Submit Ticket for Isolation (CBI)
- Submit Ticket for Zscaler Deception
- Submit Ticket for Zscaler Cloud Connector
- Submit Ticket for Zscaler Branch Connector

Figure 62. ZPC Support

©2024 Zscaler, Inc. All rights reserved.

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



ZPC - Submit Ticket

Product* ZPC

Case Type* -- Select --

Subject* Enter subject

Priority* Medium (P3)

Zscaler Company ID* Enter organization

Description* Write here...

5000 remaining

First Name* Enter first name

Last Name* Enter last name

Email Address* abc@company.com

Preferred Contact Phone Number* (201) 555-0123

Collaborator (CC) List Seperate multiple email addresses with a semi-colon

Preferred Working Hours* -- Select --

Preferred Mode of Communication* -- Select --

□ **By requesting support, you authorize Zscaler's support personnel to access your customer logs, only if required, for the limited purposes of responding to and troubleshooting this support request.**

□ I'm not a robot reCAPTCHA Privacy - Terms

Figure 63. 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.