ZSCALER AND SLACK DEPLOYMENT GUIDE

AUGUST 2023, VERSION 1.2

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

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

Acronym	Definition
CA	Central Authority (Zscaler)
CI/CD	Continuous integration and continuous delivery
CRM	Customer Relationship Management
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

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

Zscaler Overview

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

Slack Overview

Slack (NYSE: WORK) transformed business communication. It's the leading channel-based messaging platform, used by millions to align their teams, unify their systems, and drive their businesses forward. Only Slack offers a secure, enterprise-grade environment that can scale with the largest companies in the world. It is a new layer of the business technology stack where people can work together more effectively, connect all their other software tools and services, and find the information they need to do their best work. Slack is where work happens. To learn more, refer to Slack'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
- Slack Resources
- Appendix A: Requesting Zscaler Support

Software Versions

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

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Slack Introduction

Overviews of the Zscaler and Slack 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, 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 ZIA as a secure internet on-ramp—just 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 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 Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZDX Overview

ZDX is a digital experience monitoring solution delivered as a service from the Zscaler cloud. ZDX provides end-to-end visibility and troubleshooting of end-user performance issues for any user or application, regardless of location. In addition, it enables continuous monitoring for network, security, desktop, and helpdesk teams with insight into the end-user device, network, and application performance issues. With ZDX, IT teams can proactively analyze and troubleshoot user experience issues, improving business productivity and IT agility.

ZPC Overview

Zscaler Posture Control (ZPC) is a multi-tenant Software as a Service (SaaS) platform that detects and responds to cloud security risks. 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 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 includes:

- 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.
ZDX Help Portal	Help Articles for ZDX.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPC Help Portal	Help articles for ZPC.
ZDX Help Portal	Help Articles for ZDX.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Slack Overview

Slack is a messaging app for business that connects people to the information they need. By bringing people together to work as one unified team, Slack transforms the way organizations communicate.

- Connected. Slack simplifies access to your colleagues—message anyone inside or outside your organization and collaborate just like you would in person. People can work in dedicated spaces called channels that bring together the right people and information.
- Flexible. Slack supports asynchronous work. When work is organized in channels, no matter your location, time zone, or function, you can access the information you need on your own time. Ask questions, get caught up, and share updates without having to coordinate schedules.
- Inclusive. In Slack, everyone in an organization has access to the same shared and searchable information. When teams work together in channels, information can be shared with everyone at once, helping keep teams stay aligned and make decisions more quickly.

Slack Resources

The following table contains links to Slack support resources.

Name	Definition
About Slack	Information about Slack Technologies.
Slack Product Documentation	Online help for Slack products.
Slack Community	Online community for Slack product help and technical questions.
Slack Resources	Browse resources tailored to your team, your needs, and all the ways you can get more out of Slack.

Zscaler Data Protection and Digital Experience for Slack.com

Slack an industry leader that helped define the advantages that the cloud and SaaS applications offer enterprises.

SaaS services facilitate collaboration, simple tool access, and enables information sharing globally. But the downside of this ease of access and sharing is security vulnerabilities based on the client's environment. It is impossible to train every employee to consistently use SaaS application best security practices, which can lead to costly mistakes for the organization. Risk associated with accidental data exposure, malicious intent, and compliance violations can force companies to restrict or prevent use of these incredible business tools.

Another challenge organizations face when migrating to today's cloud services is monitoring user experience, especially in today's work-from-anywhere corporate environments.

Zscaler provides a complete Slack solution using Zscaler Internet Services (ZIA) for security and Zscaler Digital Experience (ZDX) for user experience visibility.

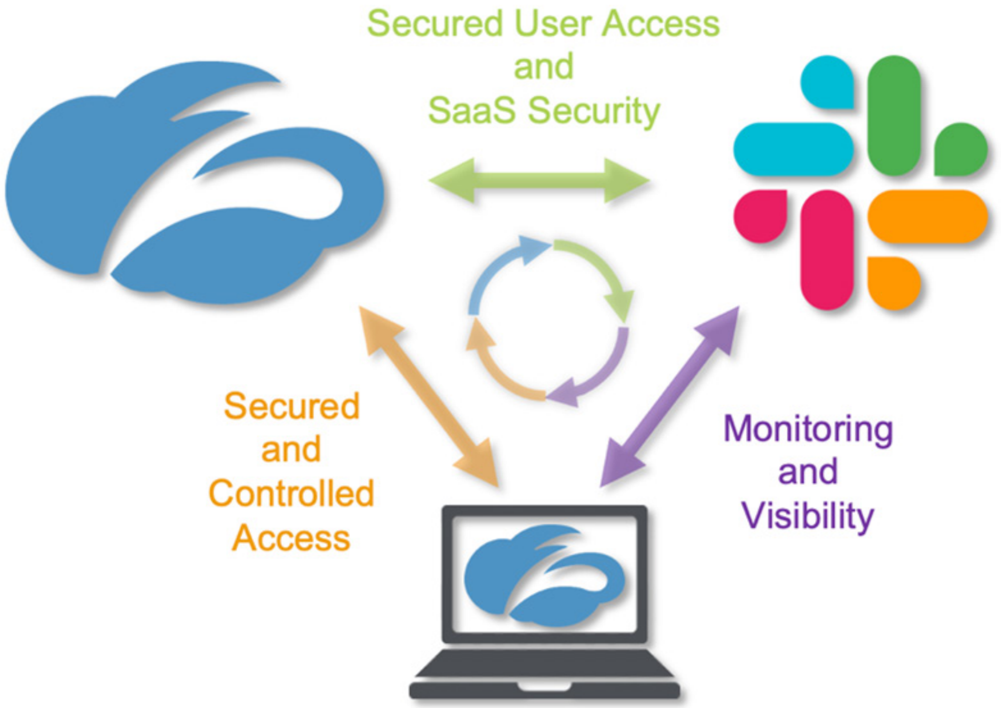


Figure 1. Zscaler solutions for Slack

ZIA provides Slack SaaS security by using access control, identity control, SaaS security, and Zscaler's SaaS Security API to scan the Slack attachments for malicious content and data loss. ZIA also provides complete security for clients, whether they are in the corporate office or their home office.

ZDX monitors the user specific experience and provides visibility to the Slack service to help organizations address any user experience concerns or challenges. ZDX provides performance monitoring and measurements from the user device running the Zscaler Client Connector. These monitors provide detailed information on user devices, the network path to Slack, and the Slack SaaS performance itself. This information is invaluable to operations when a user is experiencing Slack issues by providing visibility to every corner of the internet.

Both ZIA SaaS security and ZDX SaaS monitoring operate as separate stand-alone services and are not dependent on one or the other. However, the two services working together provide a comprehensive solution for both security and operations of the partner SaaS CRM service.

This guide covers the following ZIA security features and ZDX performance visibility features when using Slack:

- SaaS Identity Proxy
- Tenant Profiles and Tenancy Restrictions
- SaaS Security API Data and Malware Protection for Slack
- ZDX for the Slack User Experience

ZIA SaaS Identity Proxy

You can configure the Zscaler service as an identity proxy for Slack. This Zscaler feature forces users to authenticate and access Slack only through the Zscaler ZIA security cloud. This provides security, inspection of traffic, and controlled access for all users of your organization's Slack tenant.

When users try to access Slack with their corporate accounts without going through the Zscaler service, a window displays asking them to login via Zscaler. The process is controlled using SAML, the IdP that is defined on Zscaler for the ZIA service, and the Slack SSO configuration to forward auth requests to Zscaler. After the user's identity is verified, their traffic to and from Slack is secured and the user and the Slack data is inspected using ZIA.

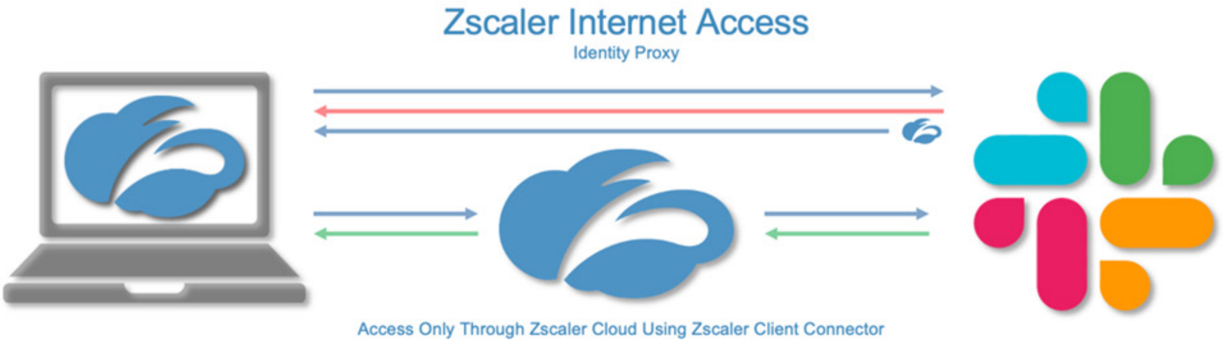

Zscaler Internet Access
Identity Proxy
Access Only Through Zscaler Cloud Using Zscaler Client Connector

Figure 2. ZIA identity proxy

ZIA sits between your users and Slack, inspecting every byte of traffic inline across multiple security techniques (even within SSL). You get full protection from web and internet threats. With a cloud platform that supports cloud firewall, cloud IPS, cloud sandbox, cloud DLP, and cloud browser isolation, you can start with the services you need today and activate others as your needs grow.

ZIA Tenant Profiles and Tenancy Restrictions

Zscaler's tenancy restrictions feature allows you to restrict access either to personal accounts, business accounts, or both for Slack. It consists of two parts: creating a tenant profile and then associating it with Cloud App Control policy rules.

By defining granular policies based on tenant profile, user group, department, or a number of other controls, you can effectively manage user access for Slack to specific tenants relative to the user's and organization's business requirements.

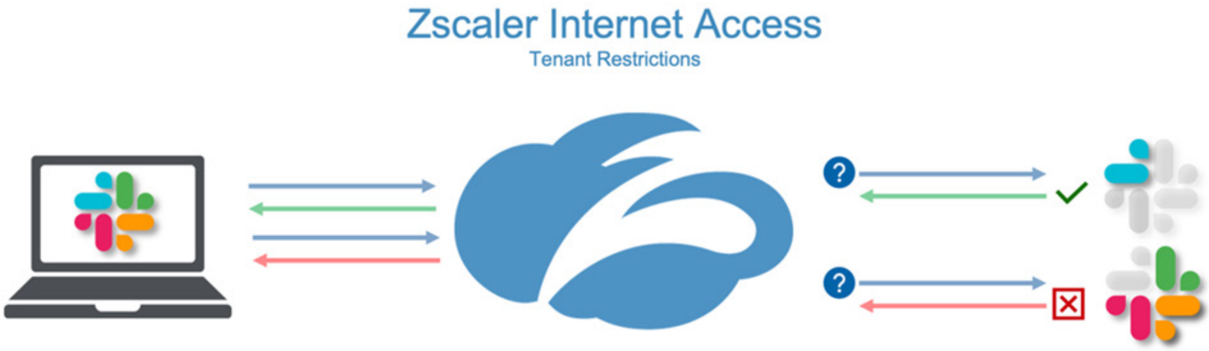


Figure 3. ZIA tenancy restrictions in use with Slack

You can combine ZIA tenant restrictions with identity proxy to provide extra security to Slack users by assuring the identity of the user. This guarantees user traffic is scanned and secured with the ZIA security features.

ZIA SaaS Security API Data and Malware Protection for Slack

The Zscaler SaaS Security API is a feature set that is part of the ZIA security cloud. It is designed specifically to help manage the risks of the collaboration SaaS partners by preventing data exposure and ensuring compliance across the SaaS application.

Zscaler SaaS Security 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.

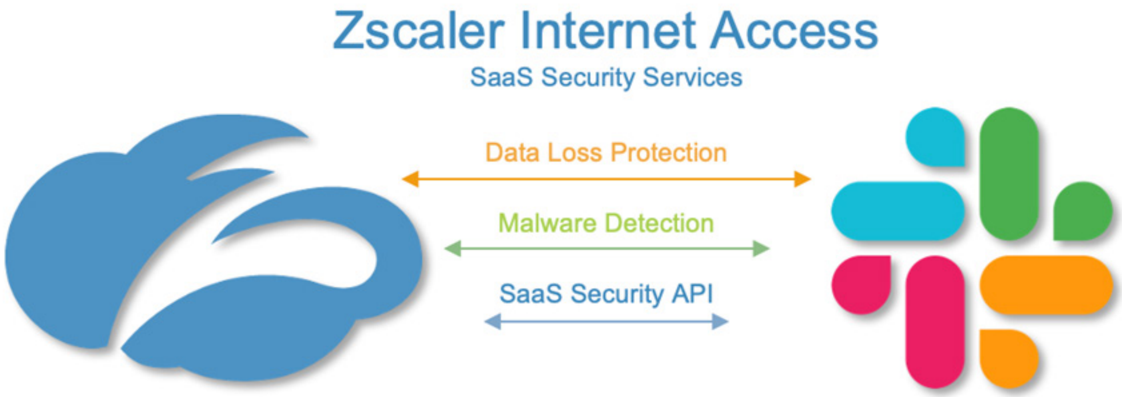


Figure 4. ZIA SaaS Security API in use with Slack

What makes Zscaler SaaS Security unique?

- Data exposure reporting and remediation. Zscaler SaaS Security checks SaaS applications and cloud provider configurations and compares them to industry and organizational benchmarks to report on violations and automate remediation.
- Threat identification and remediation. Zscaler SaaS Security checks SaaS applications for hidden threats and prevents their propagation.
- Compliance assurance. Zscaler SaaS Security 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, 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 ZPA for Zero Trust access to internal applications, ZDX for active monitoring SaaS application user experience, and Zscaler Cloud Protection (ZCP). Zscaler provides end-to-end connectivity, security, and visibility from any location on-premises or remote.

For more information, see the resources in **Zscaler Resources**.

ZDX for the Slack User Experience

With ZDX, you can easily monitor user digital experiences. ZDX provides visibility across the complete user-to-cloud app experience and quickly isolates issues. ZDX provides you with innovative and unprecedented end-to-end visibility, regardless of network or location.

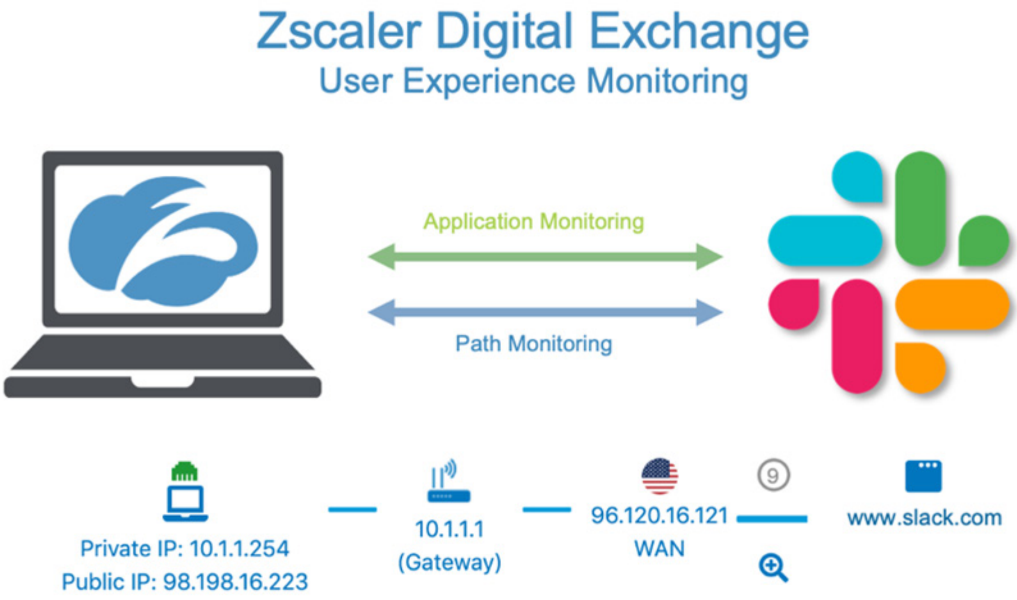


Figure 5. ZDX in use with Slack

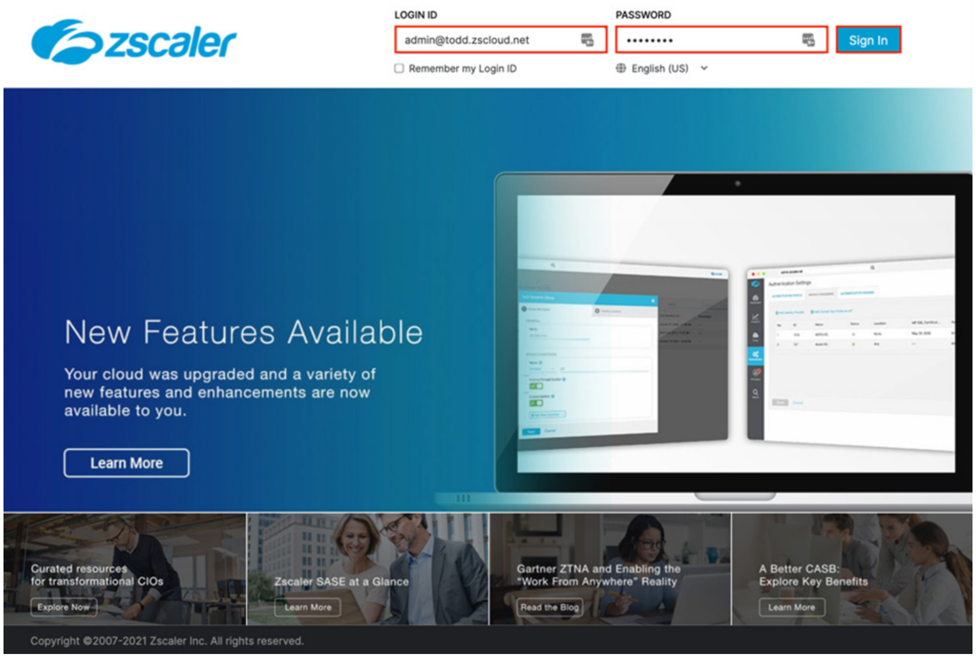
What makes ZDX unique?

- End-user device performance. Gather and analyze data on end-user device resources that impact the end-user experience.
- Cloud path performance. Measure and analyze end-to-end and hop-by-hop network path metrics from every user device to the cloud application.
- Application performance. Continuously monitor and measure application metrics, such as response time, DNS resolution, and broader availability metrics of the application.
- ZDX scoring. Monitor aggregated user experience performance scores tracked over time at the user, application, location, department, and organizational level.

For more information, see the resources in **Zscaler Resources**.

Configure the SaaS Identity Proxy

Log into the Zscaler tenant with administrator credentials.



LOGIN ID: admin@todd.zscloud.net

PASSWORD: ••••••••

Sign In

□ Remember my Login ID

English (US)

New Features Available

Your cloud was upgraded and a variety of new features and enhancements are now available to you.

Learn More

Curated resources for transformational CIOs — Explore Now

Zscaler SASE at a Glance — Learn More

Gartner ZTNA and Enabling the "Work From Anywhere" Reality — Read the Blog

A Better CASB: Explore Key Benefits — Learn More

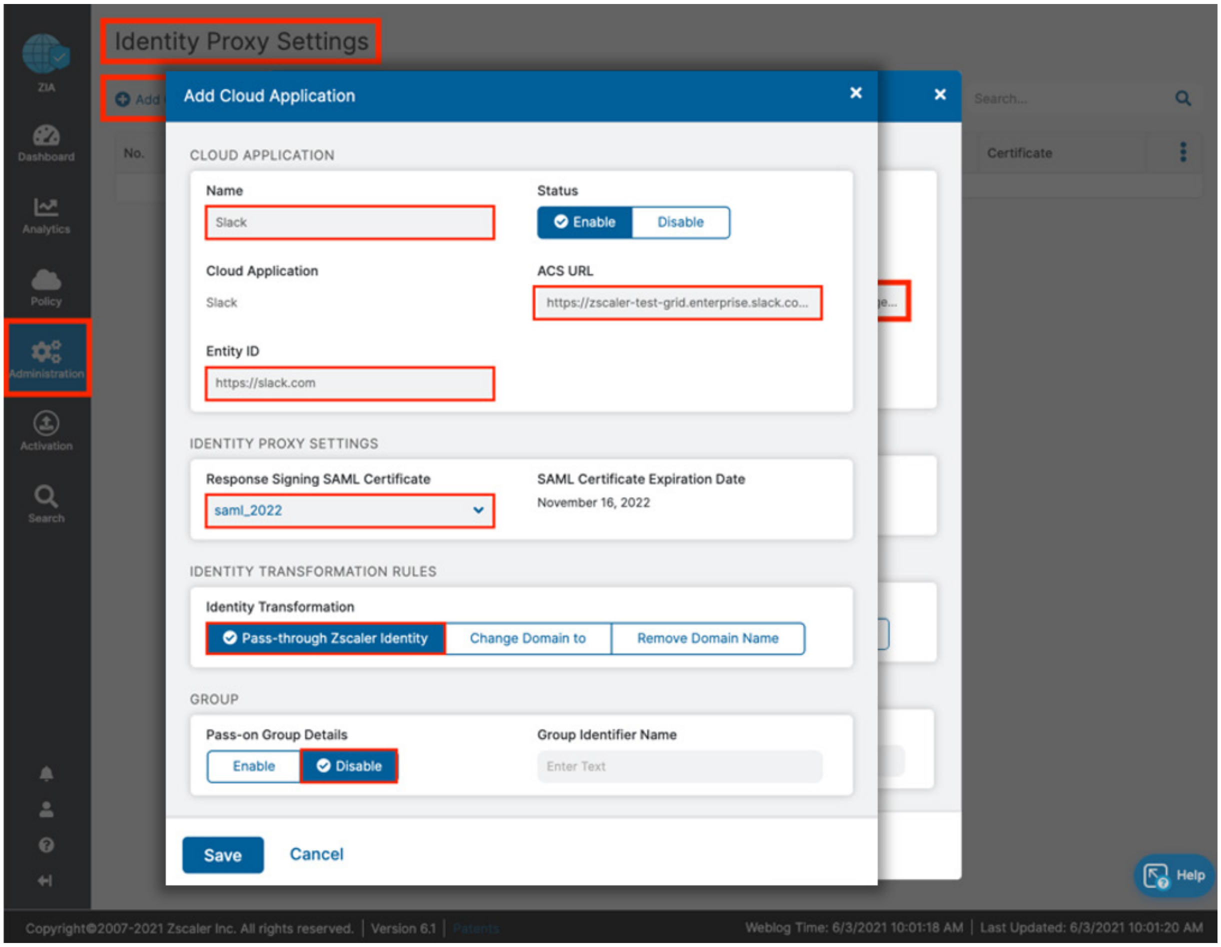
Copyright ©2007-2021 Zscaler Inc. All rights reserved.

Figure 6. ZIA Admin Portal login

Configure the ZIA Admin Portal for the SaaS Identity Proxy

To configure Zscaler for the SaaS identity proxy:

1. Go to **Administration** > **Identity Proxy Settings**.
2. Select **Add Cloud Application**. The configuration wizard is displayed.
3. Give the cloud application a **Name**.
4. Select **Enable** the **Status**.
5. Select **Slack** for **Cloud Application**.
6. Set the **ACS URL** to `https://your-slack-instance.com/sso/saml`.
7. Set the **Entity ID** to `https://slack.com`.
8. Select the **saml_2022** or later signing certificate.
9. Select **Pass-through Zscaler Identity** for **Identity Transformation**.
10. Click **Save**.



Add Cloud Application

CLOUD APPLICATION

Name: Slack

Status: ● Enable | Disable

Cloud Application: Slack

ACS URL: https://zscaler-test-grid.enterprise.slack.co...

Entity ID: https://slack.com

IDENTITY PROXY SETTINGS

Response Signing SAML Certificate: saml_2022

SAML Certificate Expiration Date: November 16, 2022

IDENTITY TRANSFORMATION RULES

Identity Transformation: ● Pass-through Zscaler Identity | Change Domain to | Remove Domain Name

GROUP

Pass-on Group Details: Enable | ● Disable

Group Identifier Name: Enter Text

Save Cancel

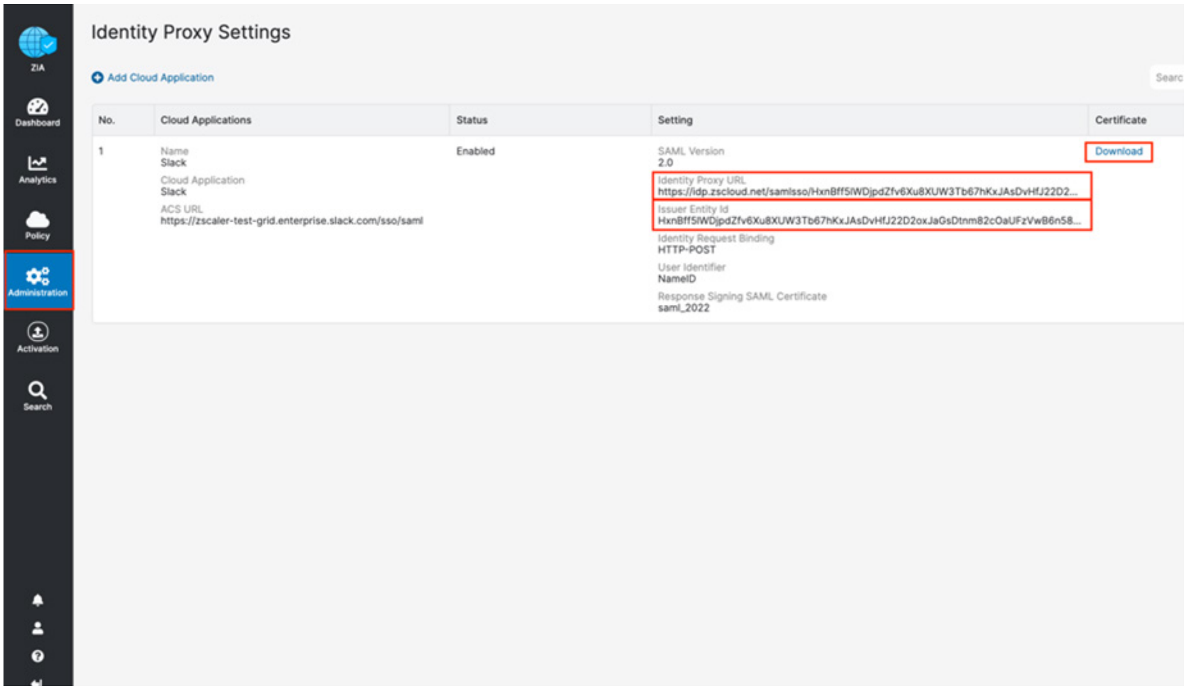
Copyright©2007-2021 Zscaler Inc. All rights reserved. | Version 6.1 | Patents   Weblog Time: 6/3/2021 10:01:18 AM | Last Updated: 6/3/2021 10:01:20 AM

Figure 7. Configure the SaaS identity proxy settings

Configure the SaaS Identity Proxy

This is the completed identity proxy configuration on the ZIA Admin Portal.

1. Copy and save the **Identity Proxy URL**.
2. Copy and save the **Issuer Entity ID**.
3. Download and save the **Signing Certificate**.



Identity Proxy Settings

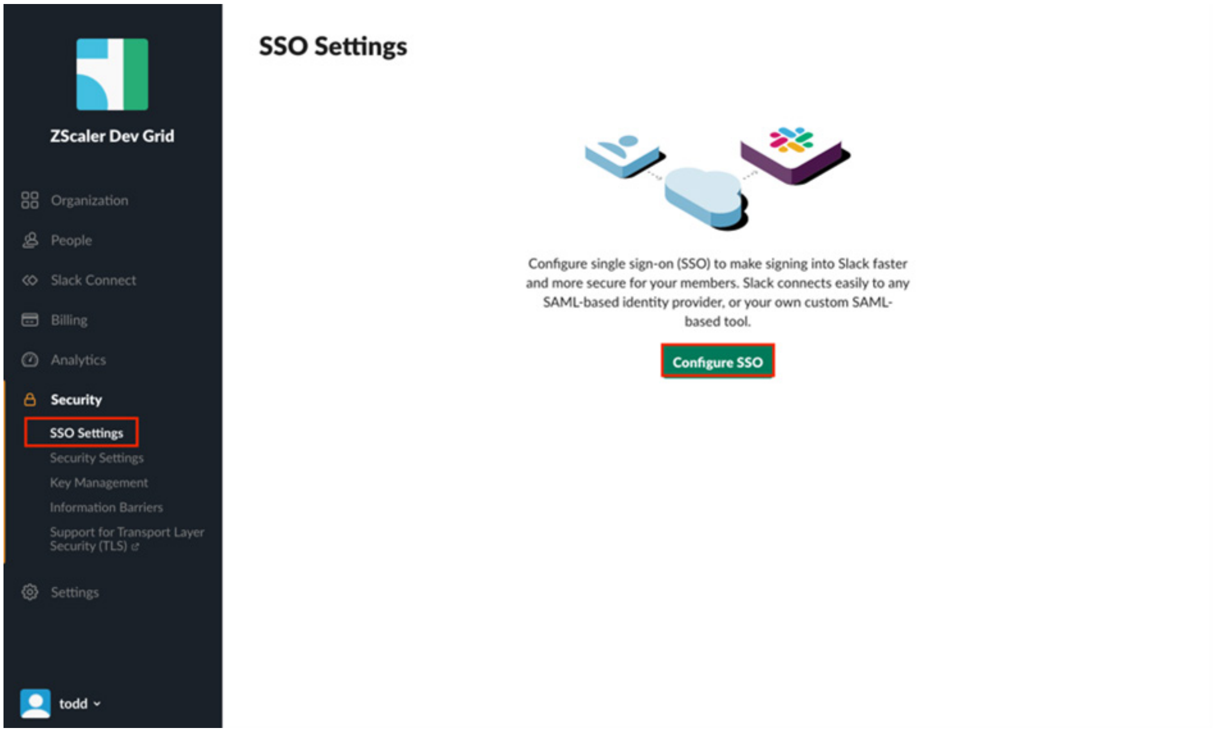
Add Cloud Application

No.	Cloud Applications	Status	Setting	Certificate
1	Name Slack Cloud Application Slack ACS URL https://zscaler-test-grid.enterprise.slack.com/sso/saml	Enabled	SAML Version 2.0 Identity Proxy URL https://idp.zscloud.net/samlsso/HxnBff5lWDjpdZfv6Xu8XUW3Tb67hKxJAsDvHfJ22D2... Issuer Entity Id HxnBff5lWDjpdZfv6Xu8XUW3Tb67hKxJAsDvHfJ22D2oxJaGsDtnm82cOaUFzVwB6n58... Identity Request Binding HTTP-POST User Identifier NameID Response Signing SAML Certificate saml_2022	Download

Figure 8. The completed identity proxy

Configure Slack to use the Identity Proxy

1. Log into the Slack tenant with administrator credentials.
2. From your **Organization Settings**, select **Security**.
3. Select **SSO Settings**.
4. Select **Configure SSO**. The **Slack SSO Configuration** wizard is displayed.



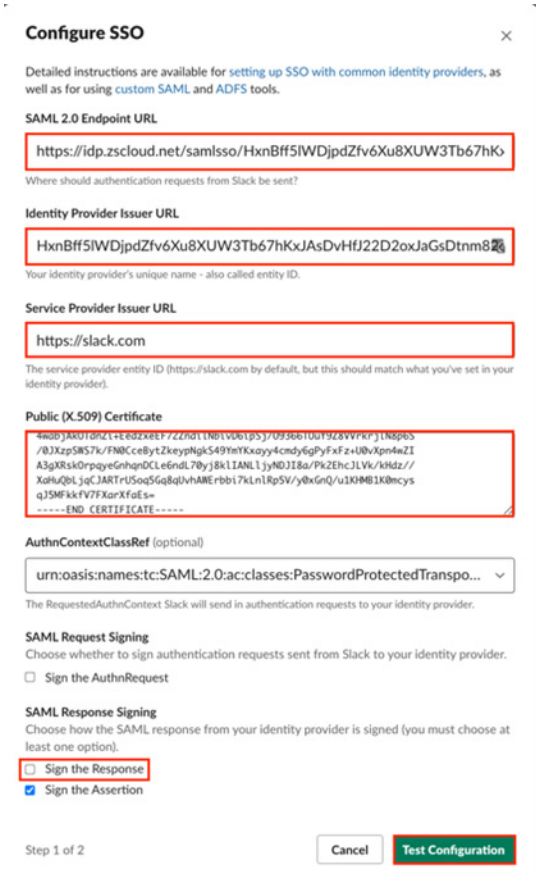
Configure single sign-on (SSO) to make signing into Slack faster and more secure for your members. Slack connects easily to any SAML-based identity provider, or your own custom SAML-based tool.

Figure 9. Configure Slack for the identity proxy

Configure Slack Single Sign-On

In the Configure SSO wizard:

1. Paste the **Zscaler Identity Proxy URL** into the **SAML 2.0 Endpoint URL** field.
2. Paste the **Zscaler Issuer Entity ID** into the **Identity Provider Issuer URL** field.
3. Set the **Service Provider Issuer URL** to `https://slack.com`.
4. Open the zscaler_certificate.cer file with a text editor, and copy and paste the entire contents into the **Public (X.509) Certificate** field.
5. Deselect the **Sign the Response** checkbox.
6. Click **Test Configuration**.



Configure SSO

Detailed instructions are available for setting up SSO with common identity providers, as well as for using custom SAML and ADFS tools.

SAML 2.0 Endpoint URL

https://idp.zscloud.net/samlsso/HxnBff5lWDjpdZfv6Xu8XUW3Tb67hK›

Where should authentication requests from Slack be sent?

Identity Provider Issuer URL

HxnBff5lWDjpdZfv6Xu8XUW3Tb67hKxJAsDvHfJ22D2oxJaGsDtnm82

Your identity provider's unique name - also called entity ID.

Service Provider Issuer URL

https://slack.com

The service provider entity ID (https://slack.com by default, but this should match what you've set in your identity provider).

Public (X.509) Certificate

```
4wdbjAkUTdnZl+EedzxeEF/ZZndlINBlvD6lpSj/U93b6TDuY9Z8VVrKrjIN8p6S
/0JXzpSWS7k/FN0CceBytZkeypNgkS49YmYKxayy4cmdy6gPyFxFz+U0vXpn4wZI
A3gXRskOrpqyeGnhqnDCLe6ndL70yj8klIANLljyNDJI8a/Pk2EhcJLVk/kHdz//
XaHuQbLjqCJARTrUSoq5Gq8qUvhAWErbbi7kLnlRpSV/y0xGnQ/u1KHMB1K0mcys
qJ5MFkkfV7FXarXfaEs=
-----END CERTIFICATE-----
```

AuthnContextClassRef (optional)

urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo...

The RequestedAuthnContext Slack will send in authentication requests to your identity provider.

SAML Request Signing

Choose whether to sign authentication requests sent from Slack to your identity provider.

☐ Sign the AuthnRequest

SAML Response Signing

Choose how the SAML response from your identity provider is signed (you must choose at least one option).

☐ Sign the Response

☑ Sign the Assertion

Step 1 of 2

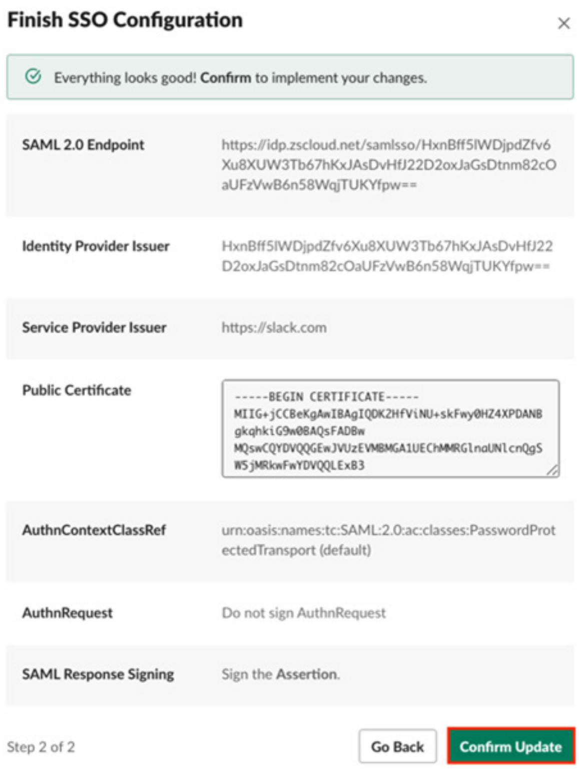
Figure 10. Slack SSO wizard confirmation

The certificate must be one continuous string with no line feeds or carriage returns.

Configure Slack Single Sign-On

If the configuration tests correctly, a confirmation is displayed (Everything looks good!). If there is a problem with the configuration, a Glitch Reported or a failure response is displayed. You must repeat the process from the beginning.

Click Confirm Update to activate the configuration.



Finish SSO Configuration

Everything looks good! **Confirm** to implement your changes.

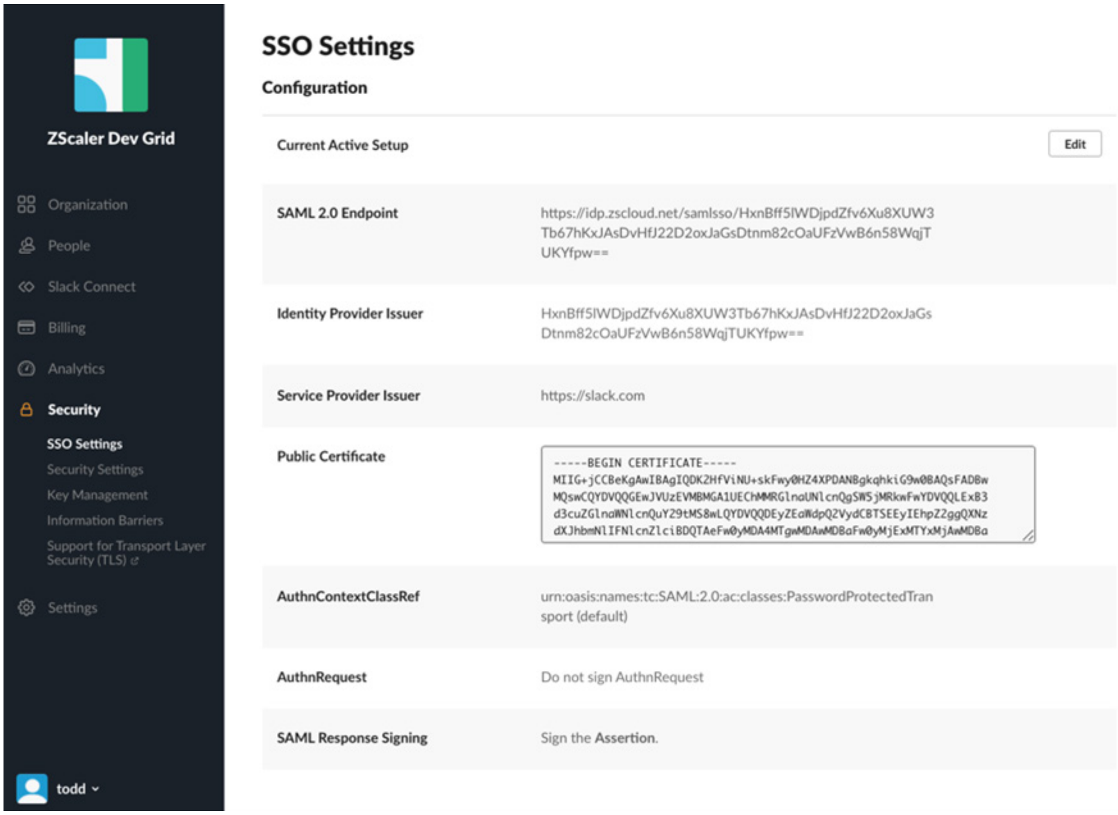
SAML 2.0 Endpoint	https://idp.zscloud.net/samlsso/HxnBff5lWDjpdZfv6Xu8XUW3Tb67hKxJAsDvHfJ22D2oxJaGsDtnm82cOaUFzVwB6n58WqjTUKYfpw==
Identity Provider Issuer	HxnBff5lWDjpdZfv6Xu8XUW3Tb67hKxJAsDvHfJ22D2oxJaGsDtnm82cOaUFzVwB6n58WqjTUKYfpw==
Service Provider Issuer	https://slack.com
Public Certificate	-----BEGIN CERTIFICATE----- MIIG+jCCBeKgAwIBAgIQDK2HfViNU+skFwy0HZ4XPDANB gkqhkiG9w0BAQsFADBw MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgS W5jMRkwFwYDVQQLExB3
AuthnContextClassRef	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport (default)
AuthnRequest	Do not sign AuthnRequest
SAML Response Signing	Sign the Assertion.

Step 2 of 2

Figure 11. Slack SSO wizard confirmation

The Completed Slack Configuration

The completed SSO configuration looks similar to the following image.



SSO Settings

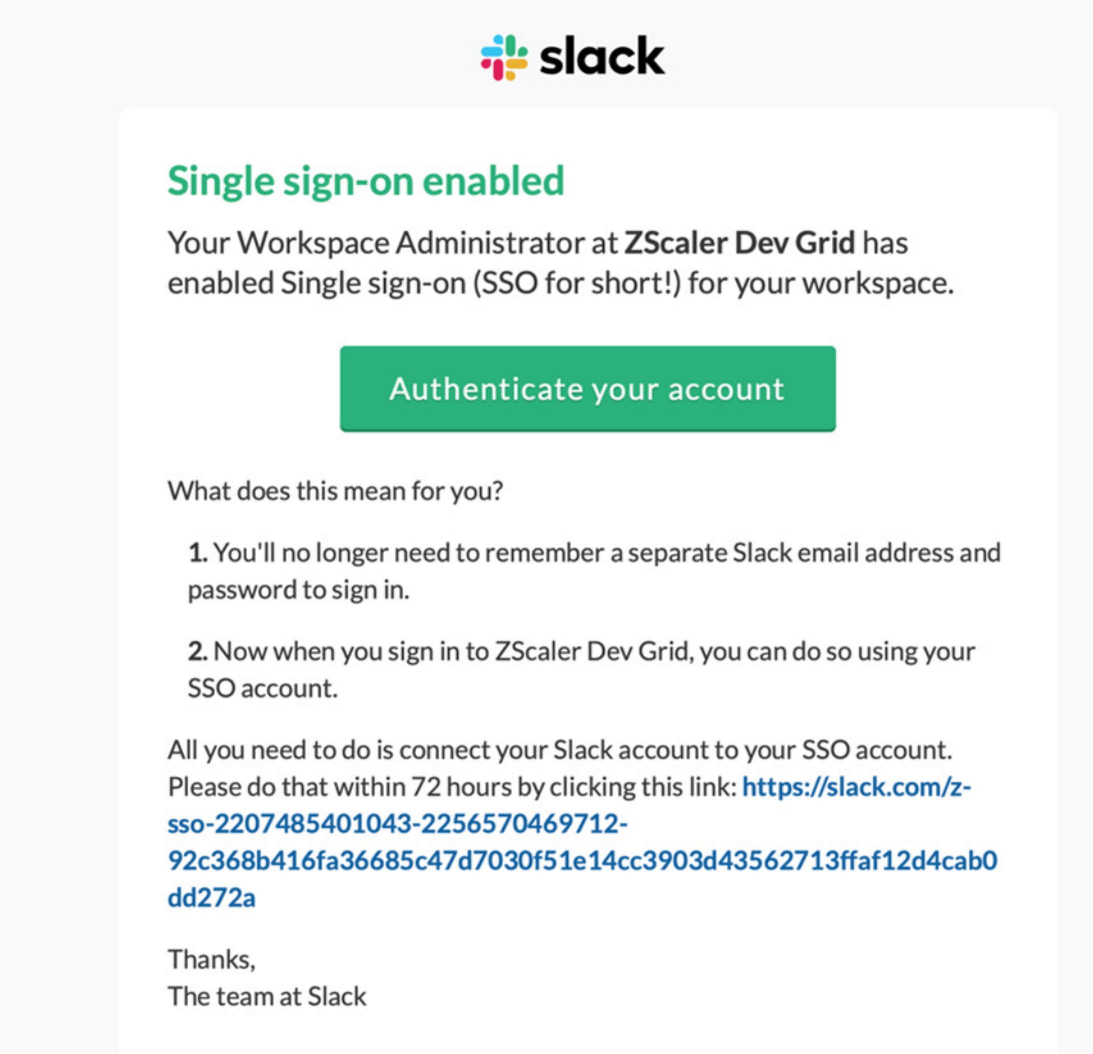
Configuration

Current Active Setup	
SAML 2.0 Endpoint	https://idp.zscloud.net/samlsso/HxnBff5lWDjpdZfv6Xu8XUW3Tb67hKxJAsDvHfJ22D2oxJaGsDtnm82cOaUFzVwB6n58WqjTUKYfpw==
Identity Provider Issuer	HxnBff5lWDjpdZfv6Xu8XUW3Tb67hKxJAsDvHfJ22D2oxJaGsDtnm82cOaUFzVwB6n58WqjTUKYfpw==
Service Provider Issuer	https://slack.com
Public Certificate	-----BEGIN CERTIFICATE----- MIIG+jCCBeKgAwIBAgIQDK2HfViNU+skFwy0HZ4XPDANBgkqhkiG9w0BAQsFADBw MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3 d3cuZGlnaWNlcnQuY29tMS8wLQYDVQQDEyZEaWdpQ2VydCBTSEEyIEhpZ2ggQXNz dXJhbmNlIFNlcnZlciBDQTAeFw0yMDA4MTgwMDAwMDBaFw0yMjExMTYxMjAwMDBa
AuthnContextClassRef	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport (default)
AuthnRequest	Do not sign AuthnRequest
SAML Response Signing	Sign the Assertion.

Figure 12. The completed identity provider configuration

User Informational Email

Users receive an email stating they need to use their Single Sign-On credentials.



slack

Single sign-on enabled

Your Workspace Administrator at **ZScaler Dev Grid** has enabled Single sign-on (SSO for short!) for your workspace.

What does this mean for you?

1. You'll no longer need to remember a separate Slack email address and password to sign in.

2. Now when you sign in to ZScaler Dev Grid, you can do so using your SSO account.

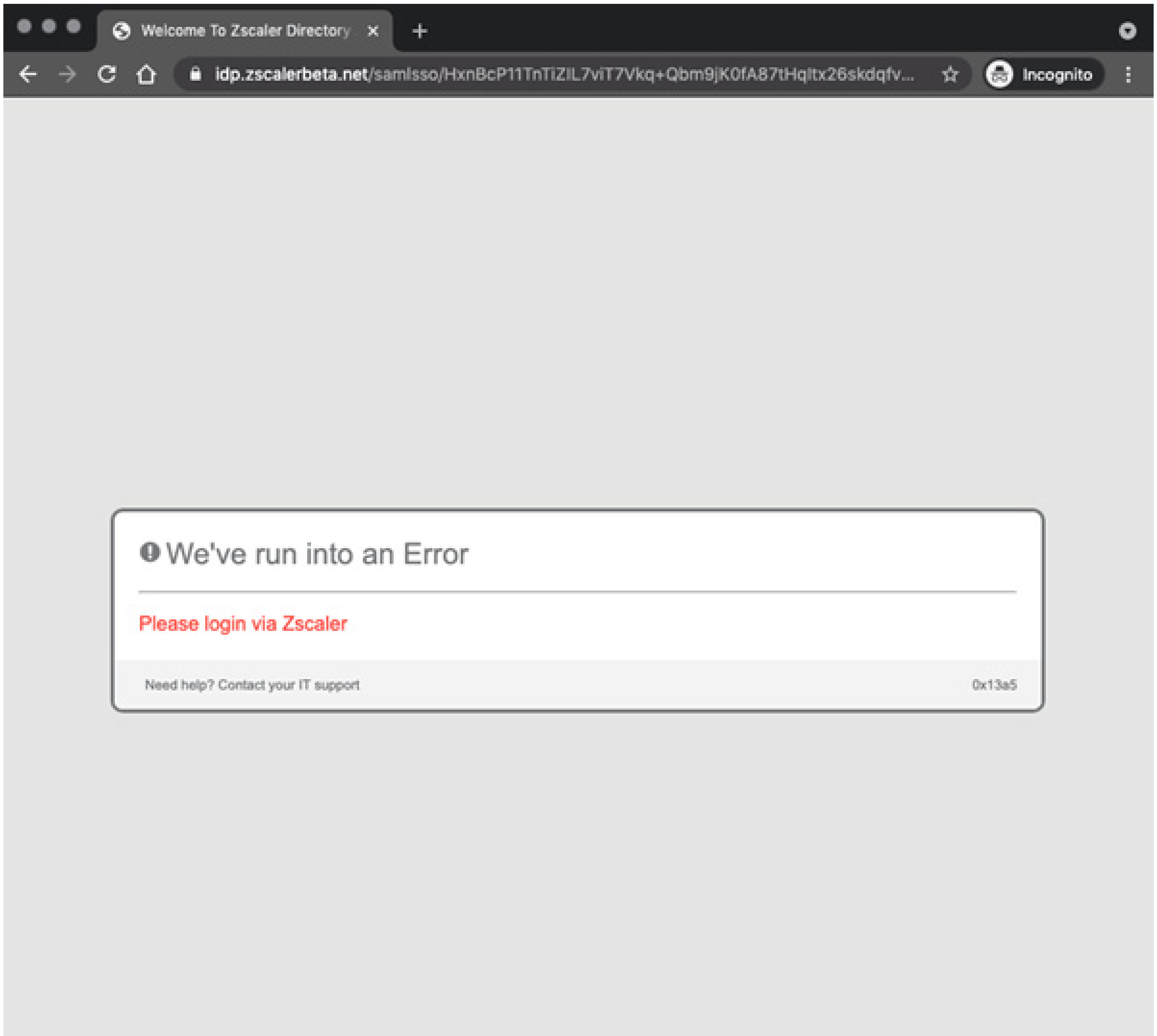
All you need to do is connect your Slack account to your SSO account. Please do that within 72 hours by clicking this link: **https://slack.com/z-sso-2207485401043-2256570469712-92c368b416fa36685c47d7030f51e14cc3903d43562713ffaf12d4cab0dd272a**

Thanks,
The team at Slack

Figure 13. Email informing users

The Zscaler Active Identity Proxy Notification

This is the notification a Slack user receives if they are trying to log into Slack without going through Zscaler. When your user traffic goes through Zscaler, they can access Slack as usual.


Welcome To Zscaler Directory
idp.zscalerbeta.net/samlsso/HxnBcP11TnTiZIL7viT7Vkq+Qbm9jK0fA87tHqltx26skdqfv...
Incognito

We've run into an Error

Please login via Zscaler

Need help? Contact your IT support

0x13a5

Figure 14. The active authentication proxy

Configuring Tenancy Restrictions for Slack

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) flows between them. As part of the platform, Zscaler Cloud Application Visibility & Control delivers full visibility into application usage, and granular policies ensure the proper use of both sanctioned and unsanctioned applications. While SaaS Tenant Security is out-of-band for data-at-rest, Zscaler Cloud Application security is inline.

Cloud App Control provides SaaS application intelligence to consolidate all associated URLs and functions of the application in a single security setting. This allows you to control specific access, tenant, user, groups, locations, or departments, and only allow the required users to the application and the correct tenant within Slack.

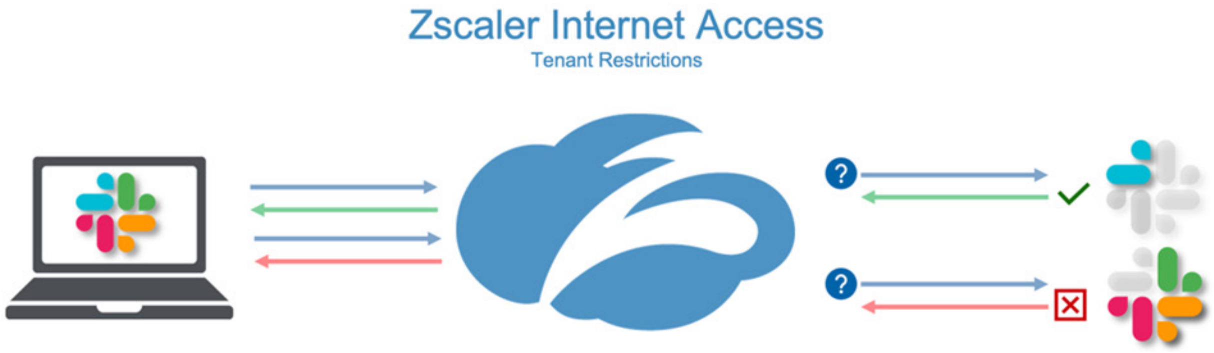


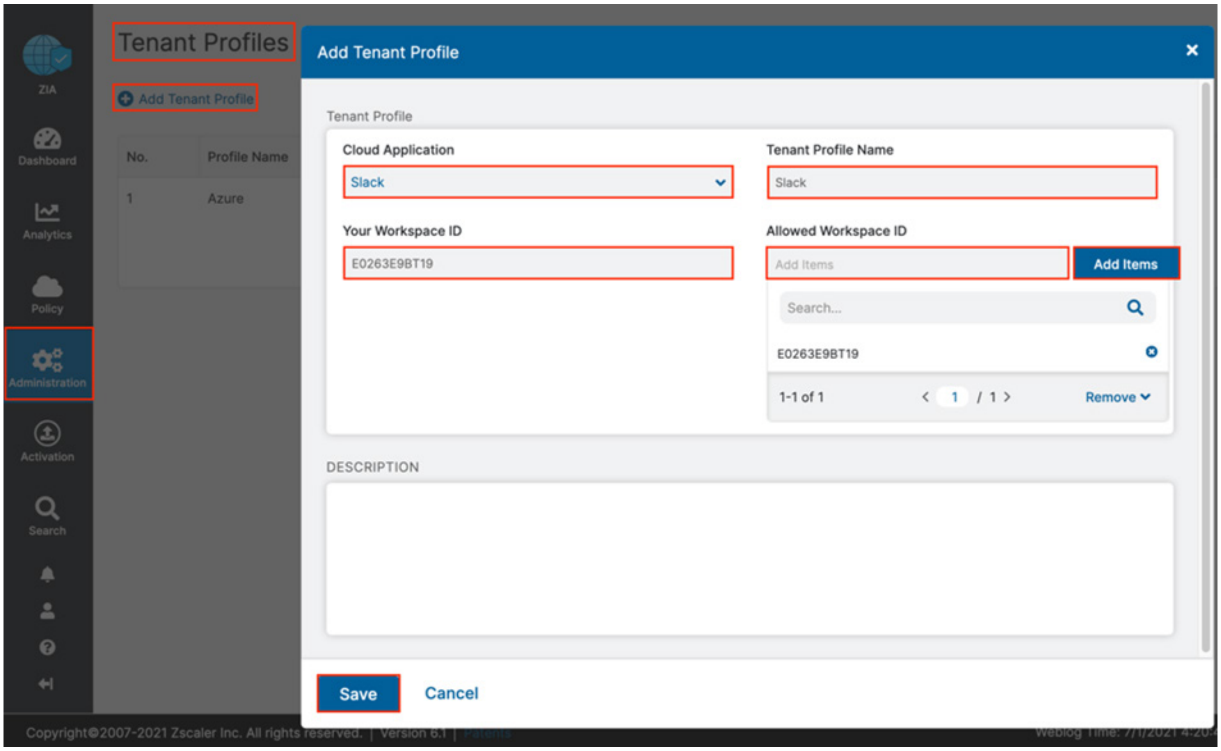
Figure 15. ZIA tenancy restrictions in use with Slack

Zscaler's tenancy restrictions feature allows you to restrict access either to personal accounts, business accounts, or both for Slack. It consists of two parts: creating a tenant profile and associating it with Cloud App Control policy rules.

Create a Tenant Profile

To create the tenant profile to allow specific users:

1. Sign into your organization's ZIA Admin Portal with admin credentials.
2. Go to **Administration** > **Tenant Profiles**.
3. Select **Add Tenant Profile**. This launches the **Add Tenant Profile** wizard to create the profile.
4. Select **Slack** as the **Cloud Application**.
5. Provide a **Name** for the **Tenant Profile**.
6. Provide an org ID or workspace ID for the **Workspace ID**.
7. Add the **Allowed Tenants** by org ID or workspace ID.
8. Click **Save**.



Add Tenant Profile

Tenant Profile

Cloud Application: Slack

Tenant Profile Name: Slack

Your Workspace ID: E0263E9BT19

Allowed Workspace ID: E0263E9BT19

1-1 of 1

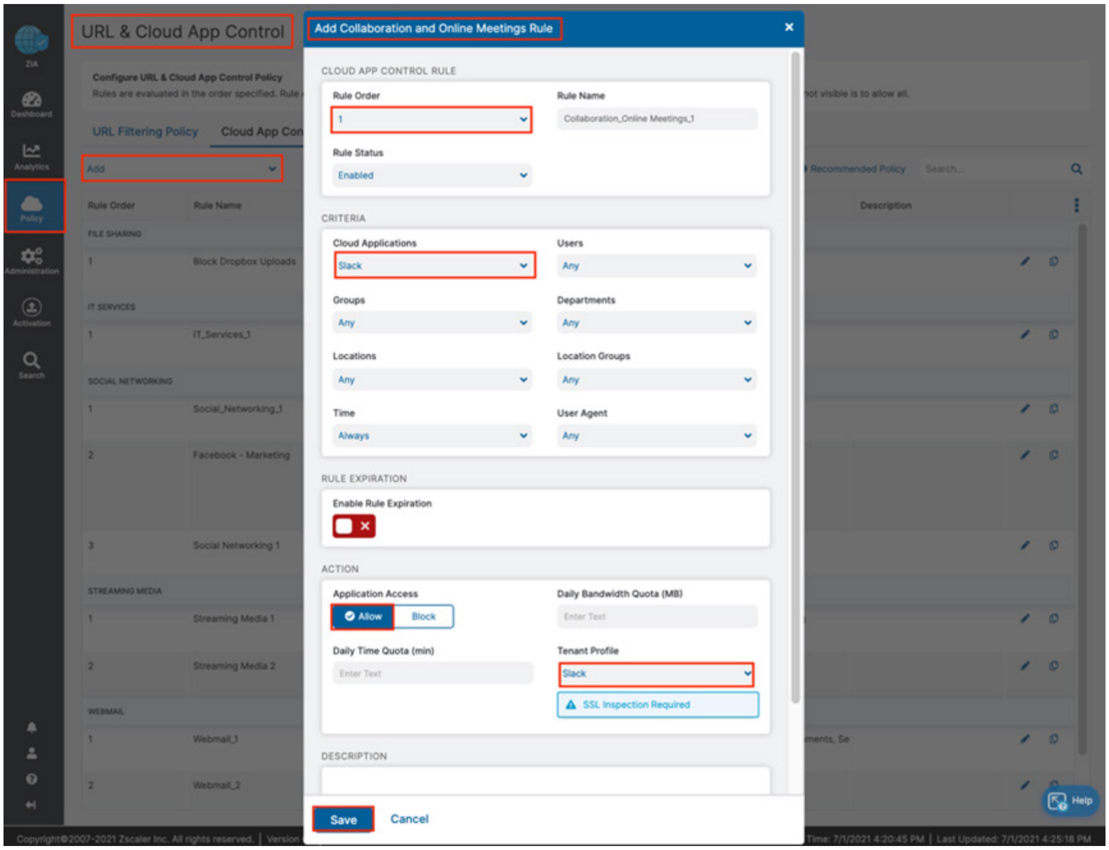
DESCRIPTION

Figure 16. Add tenant profile

Cloud Application Control Policy Wizard

Follow these steps to create a Cloud Application Control policy that allows users to the specific tenant:

1. Go to **Policy** > **URL & Cloud App Control** > **Cloud App Control Policy**.
2. Select **Add** and from the drop-down menu, select **Collaboration & Online Meetings**.
3. Set the **Rule Order** to ensure execution of the policy.
4. Select **Slack** for the **Cloud Application**.
5. Select **Allow** for **Application Access**.
6. Select **Slack** as the **Tenant Profile** you just created.
7. Click **Save**.



Add Collaboration and Online Meetings Rule

CLOUD APP CONTROL RULE

Rule Order: 1

Rule Name: Collaboration_Online Meetings_1

Rule Status: Enabled

CRITERIA

Cloud Applications: Slack

Users: Any

Groups: Any

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

User Agent: Any

RULE EXPIRATION

Enable Rule Expiration: ☒

ACTION

Application Access: [✓ Allow] Block

Daily Bandwidth Quota (MB): Enter Text

Daily Time Quota (min): Enter Text

Tenant Profile: Slack

SSL Inspection Required

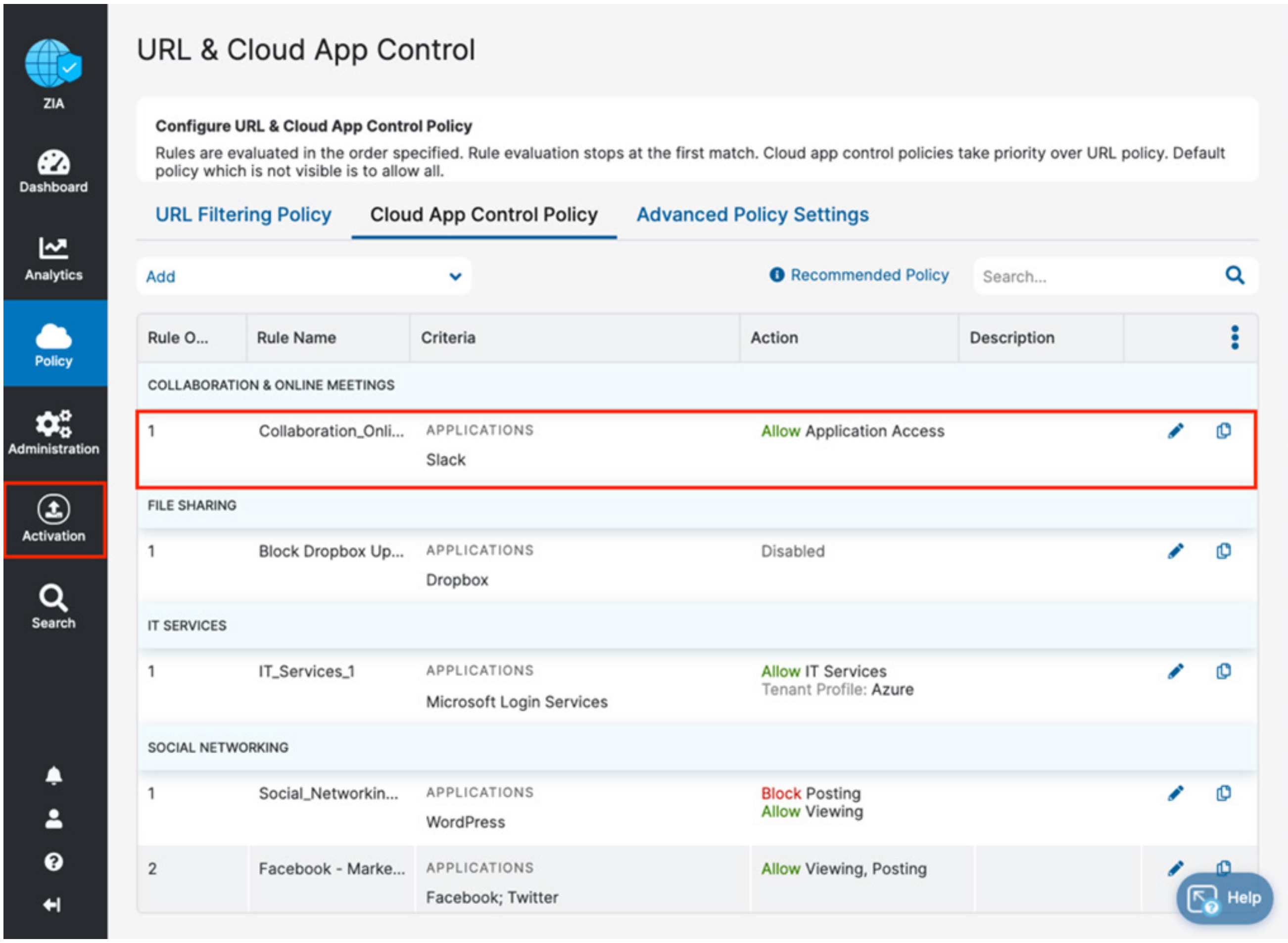
DESCRIPTION

Figure 17. Create a Cloud App Control allow policy

SSL Inspection is required for the feature to work. Make sure Slack traffic is getting inspected.

Completed Tenant Restrictions

You can see the completed access policies. Activate the policy additions.



URL & Cloud App Control

Configure URL & Cloud App Control Policy

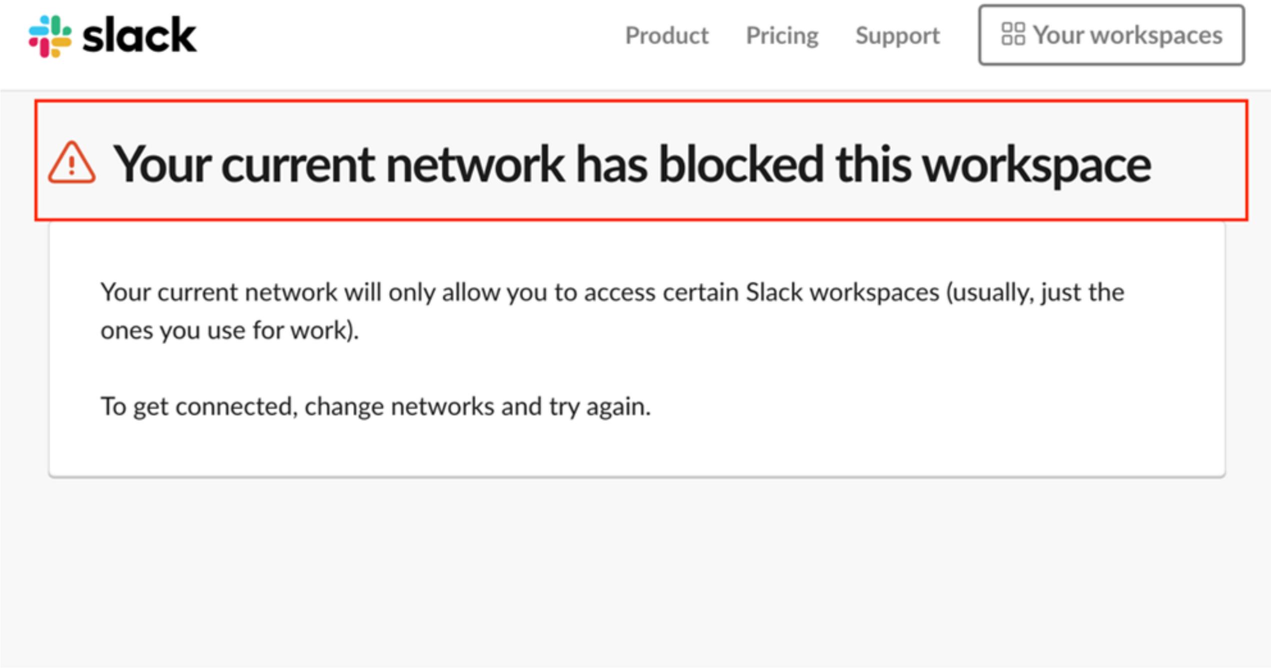
Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is to allow all.

Rule O...	Rule Name	Criteria	Action	Description
COLLABORATION & ONLINE MEETINGS				
1	Collaboration_Onli...	APPLICATIONS Slack	Allow Application Access	
FILE SHARING				
1	Block Dropbox Up...	APPLICATIONS Dropbox	Disabled	
IT SERVICES				
1	IT_Services_1	APPLICATIONS Microsoft Login Services	Allow IT Services Tenant Profile: Azure	
SOCIAL NETWORKING				
1	Social_Networkin...	APPLICATIONS WordPress	Block Posting Allow Viewing	
2	Facebook - Marke...	APPLICATIONS Facebook; Twitter	Allow Viewing, Posting	

Figure 18. Completed Cloud Application Control Policy with the tenant profile

Tenant Restriction Alerts

Users who try to access the Slack application through either a browser or the application who do not have permission receive an alert and the event is logged.



⚠ Your current network has blocked this workspace

Your current network will only allow you to access certain Slack workspaces (usually, just the ones you use for work).

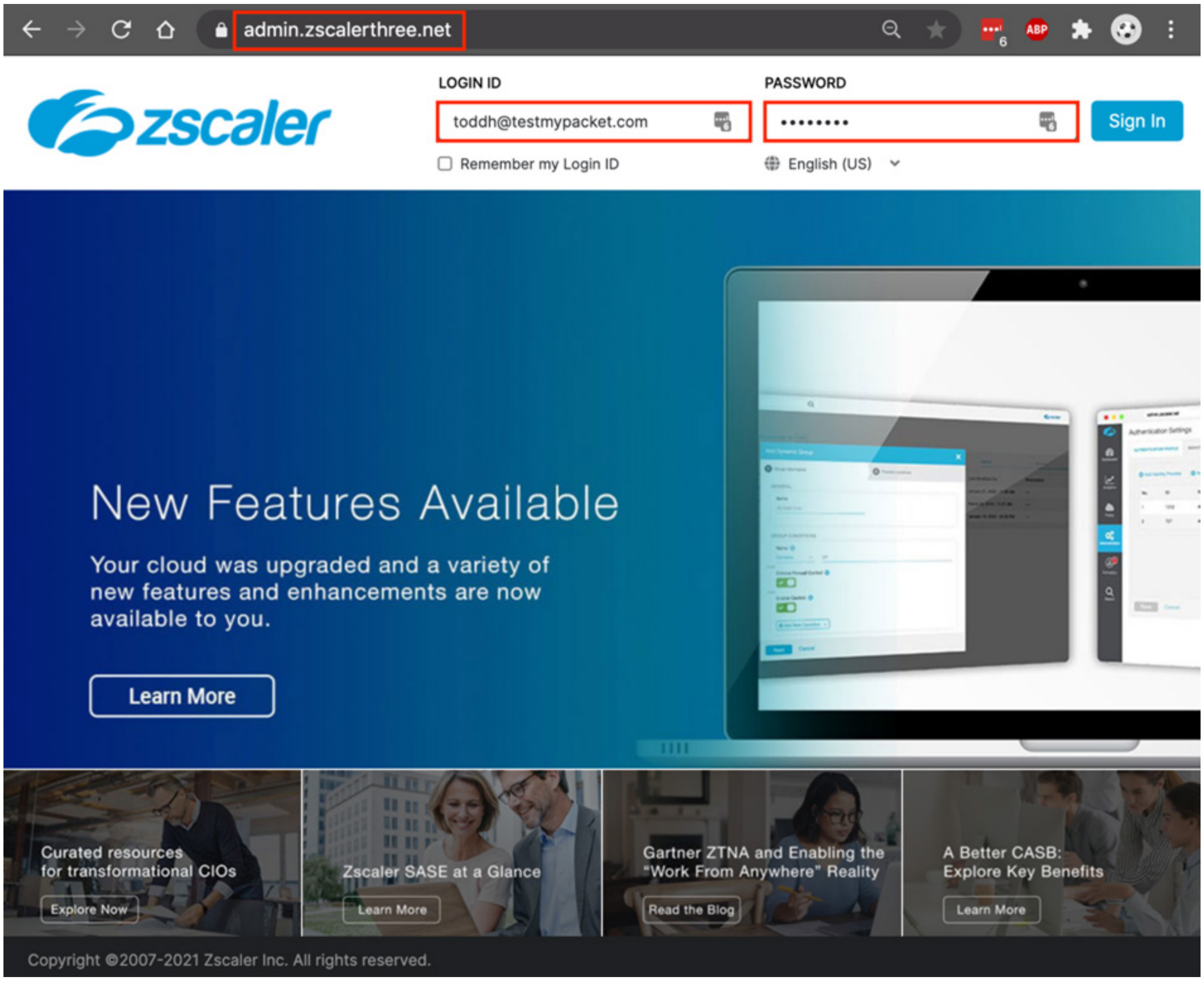
To get connected, change networks and try again.

Figure 19. Alerts when accessing blocked Slack tenants

Configuring the Slack Tenant

You must configure the Slack tenant to allow authenticated API calls to be made between the Zscaler and Slack cloud platforms. Adding the tenant is a requirement to enable the Zscaler SaaS Security API services, DLP, and malware protection.

To start the configuration process, log into your ZIA Admin Portal with admin credentials. Your Zscaler cloud instance might be different from the example. The current ZIA clouds include: zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscloud.net, zscalerbeta.net, and zscalergov.net.



admin.zscalerthree.net

LOGIN ID: toddh@testmypacket.com

PASSWORD: ••••••••

□ Remember my Login ID

English (US)

New Features Available

Your cloud was upgraded and a variety of new features and enhancements are now available to you.

Curated resources for transformational CIOs

Zscaler SASE at a Glance

Gartner ZTNA and Enabling the "Work From Anywhere" Reality

A Better CASB: Explore Key Benefits

Copyright ©2007-2021 Zscaler Inc. All rights reserved.

Figure 20. ZIA Admin Portal

Adding the Slack Tenant

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

1. Go to **Administration** > **SaaS Application Tenants**.
2. On the **SaaS Applications Tenants** page, select **Add SaaS Application Tenant**.

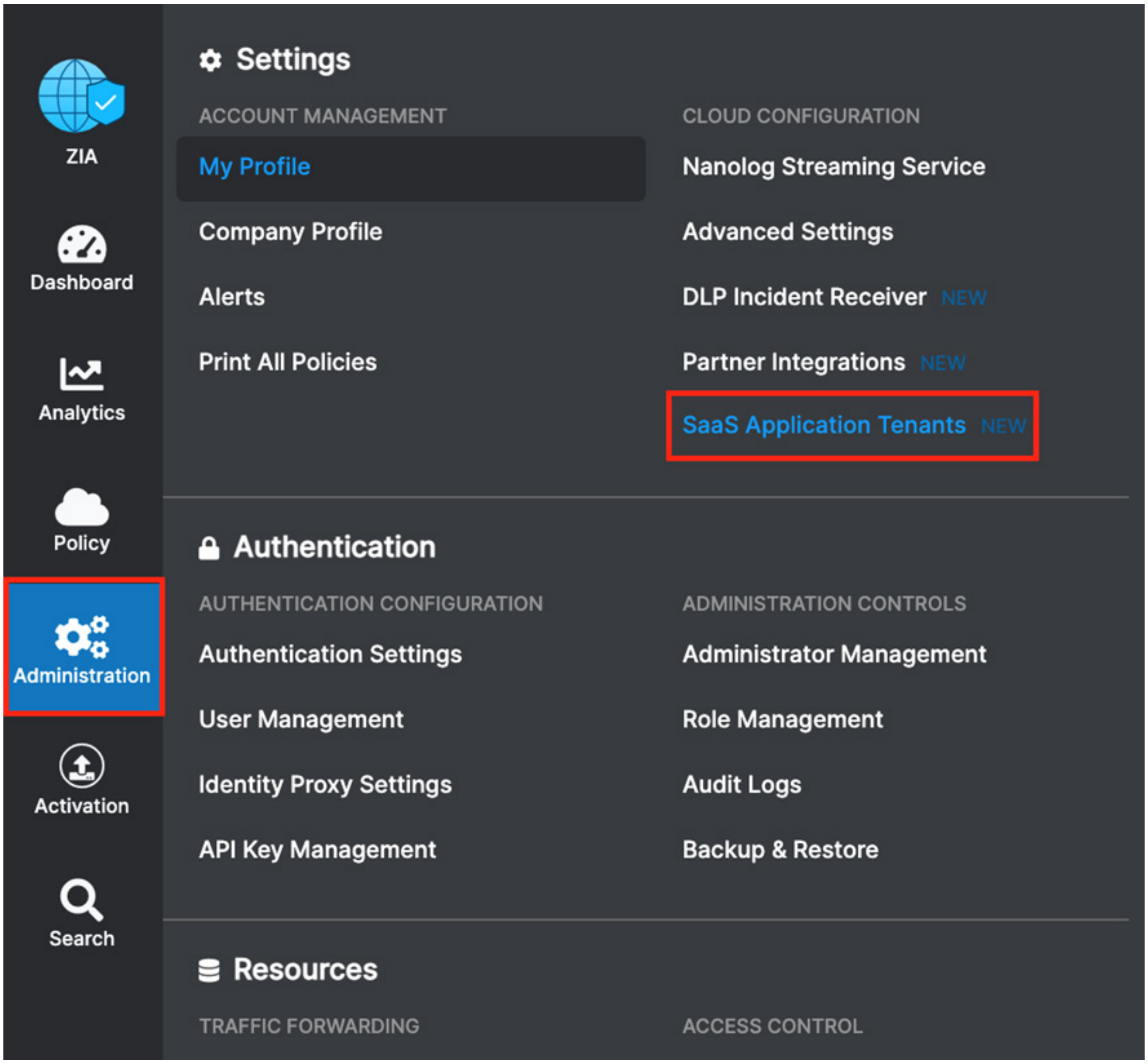


Figure 21. ZIA SaaS Application Tenant

SaaS Tenant Configuration Wizard

To start the wizard:

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

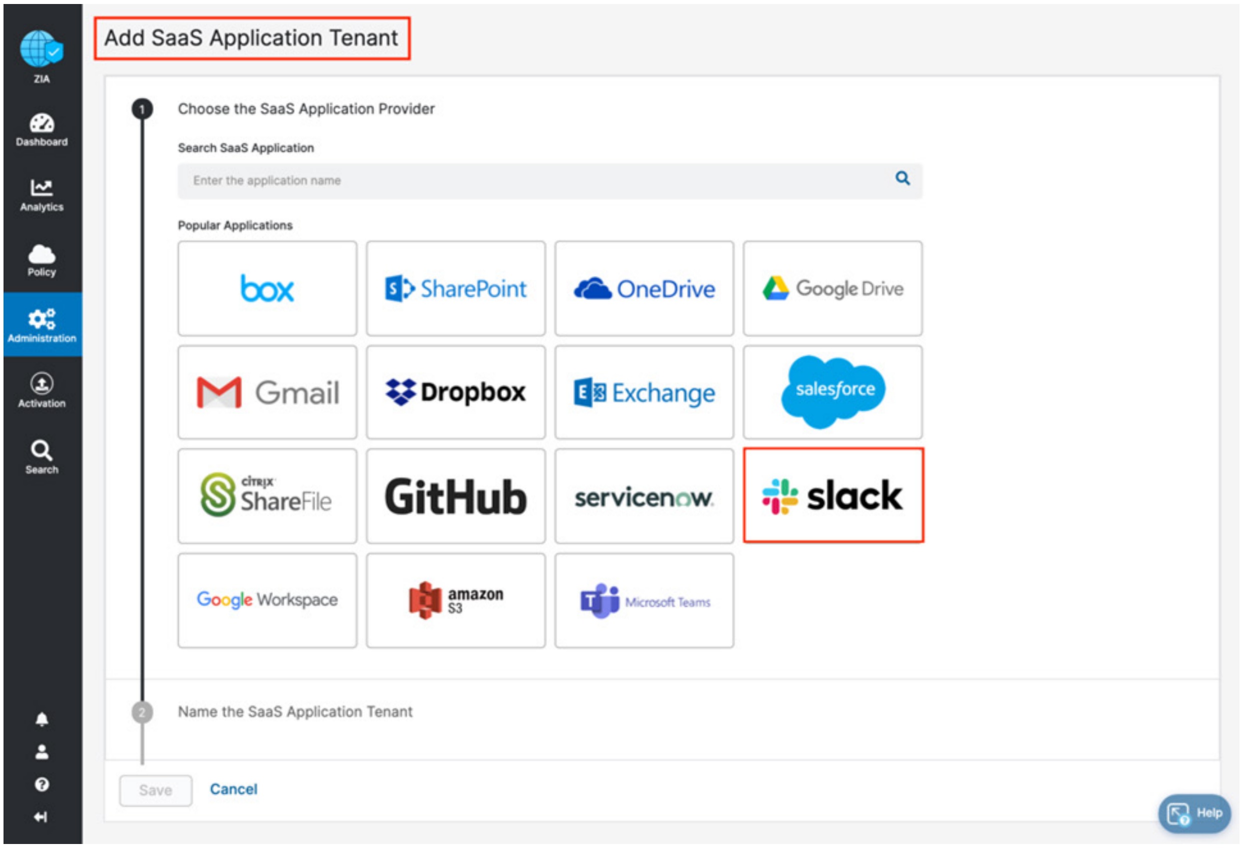
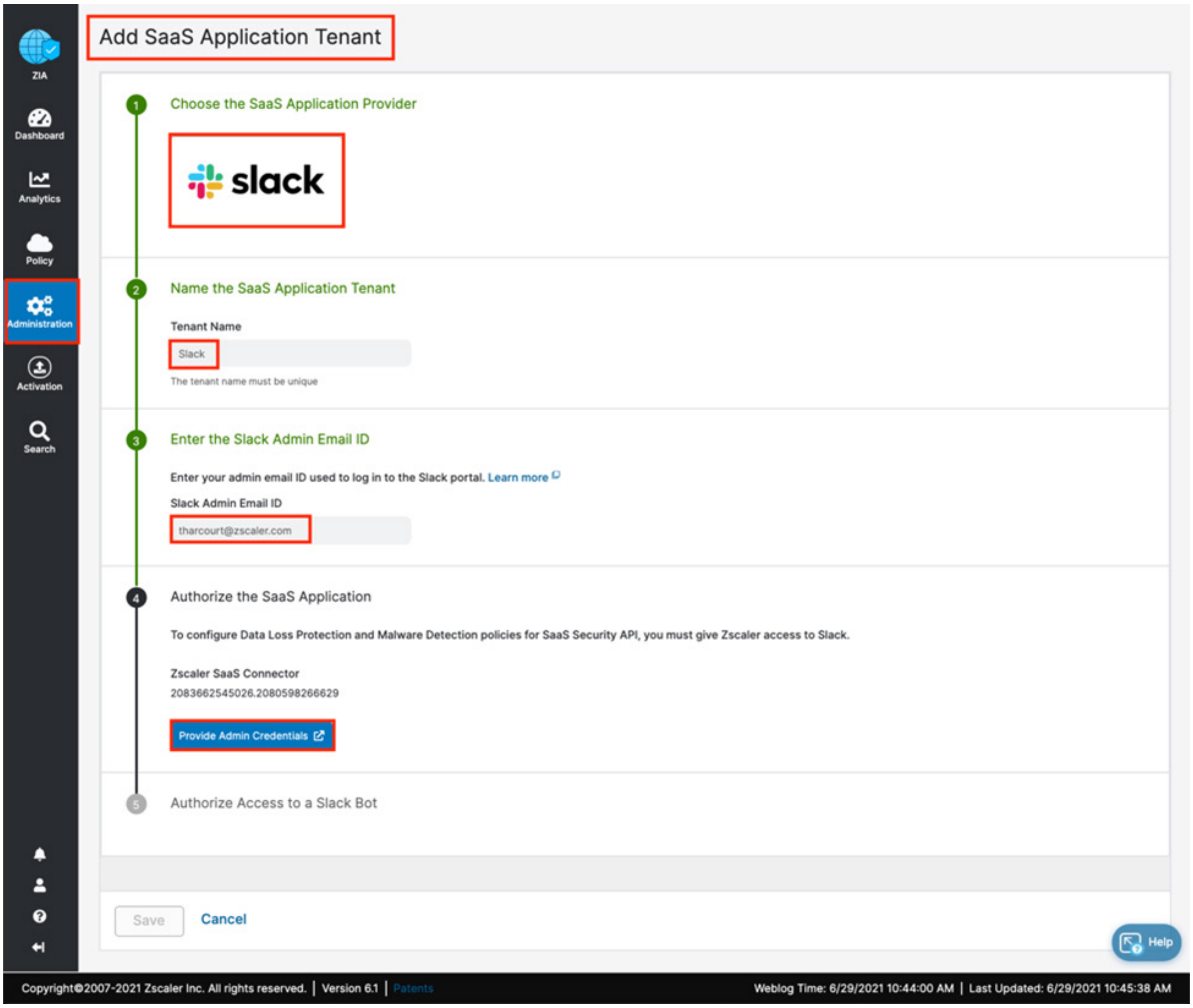


Figure 22. The SaaS Tenant Configuration wizard

SaaS Tenant Configuration Wizard

Give the Slack tenant a name. This is the name used when assigning a policy for the Zscaler security features:

1. Enter the **Tenant Name**.
2. Enter the **Slack Admin Email ID**.
3. Right-click the **Provide Admin Credentials** link, and open the link in a new tab.
4. Open a new browser tab and login to your Slack tenant with admin role credentials.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

2 Name the SaaS Application Tenant

Tenant Name

Slack

The tenant name must be unique

3 Enter the Slack Admin Email ID

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

Slack Admin Email ID

tharcourt@zscaler.com

4 Authorize the SaaS Application

To configure Data Loss Protection and Malware Detection policies for SaaS Security API, you must give Zscaler access to Slack.

Zscaler SaaS Connector

2083662545026.2080598266629

Provide Admin Credentials

5 Authorize Access to a Slack Bot

Save Cancel

Copyright©2007-2021 Zscaler Inc. All rights reserved. | Version 6.1 | Patents

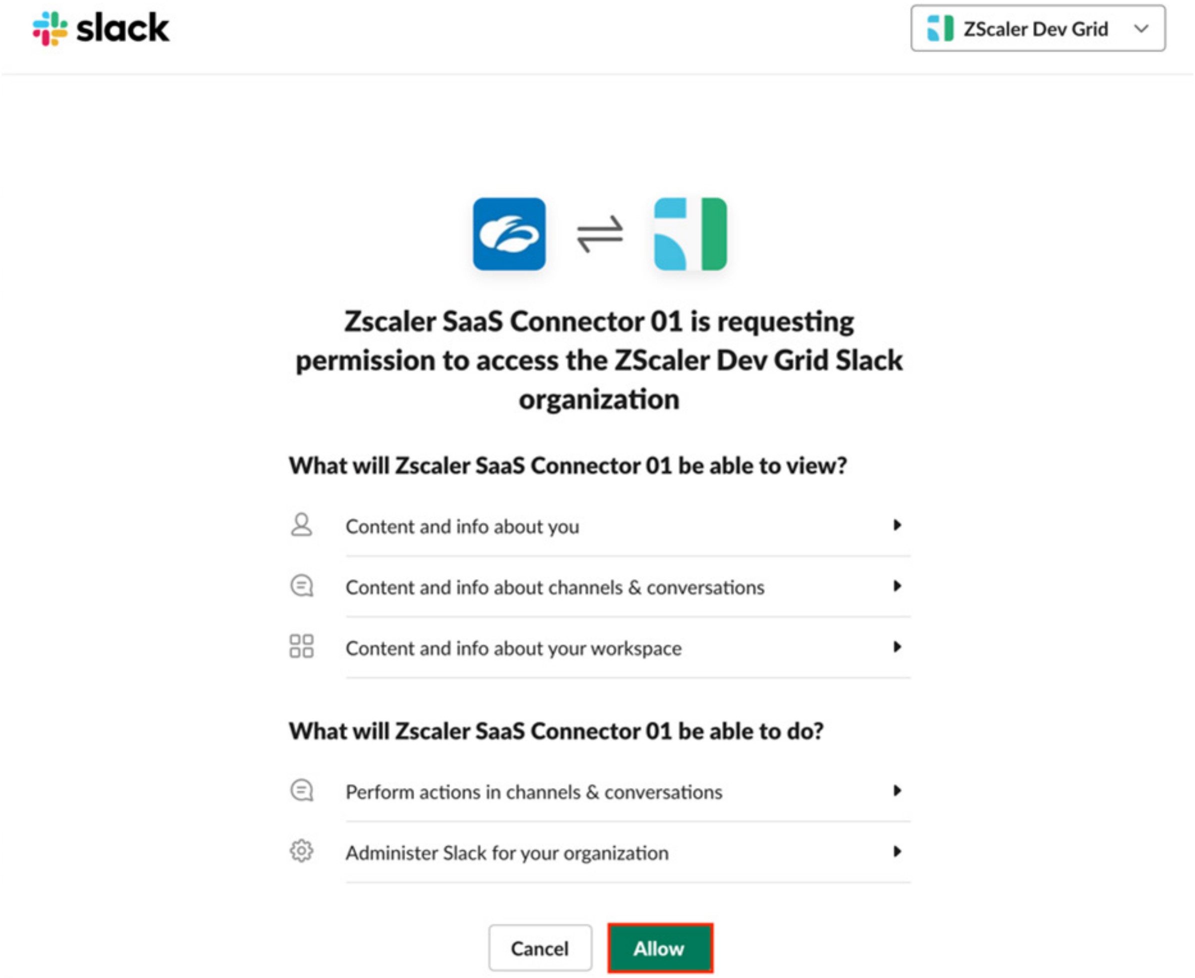
Weblog Time: 6/29/2021 10:44:00 AM | Last Updated: 6/29/2021 10:45:38 AM

Figure 23. Open the Slack tenant

Configuring the Zscaler Tenant on Slack

To configure the Zscaler tenant from your Slack admin account:

1. Log in to Slack with admin credentials.
2. Click **Allow** to enable communication between the cloud platforms. You must approve the Zscaler application on Slack.



Zscaler SaaS Connector 01 is requesting permission to access the ZScaler Dev Grid Slack organization

What will Zscaler SaaS Connector 01 be able to view?

- Content and info about you
- Content and info about channels & conversations
- Content and info about your workspace

What will Zscaler SaaS Connector 01 be able to do?

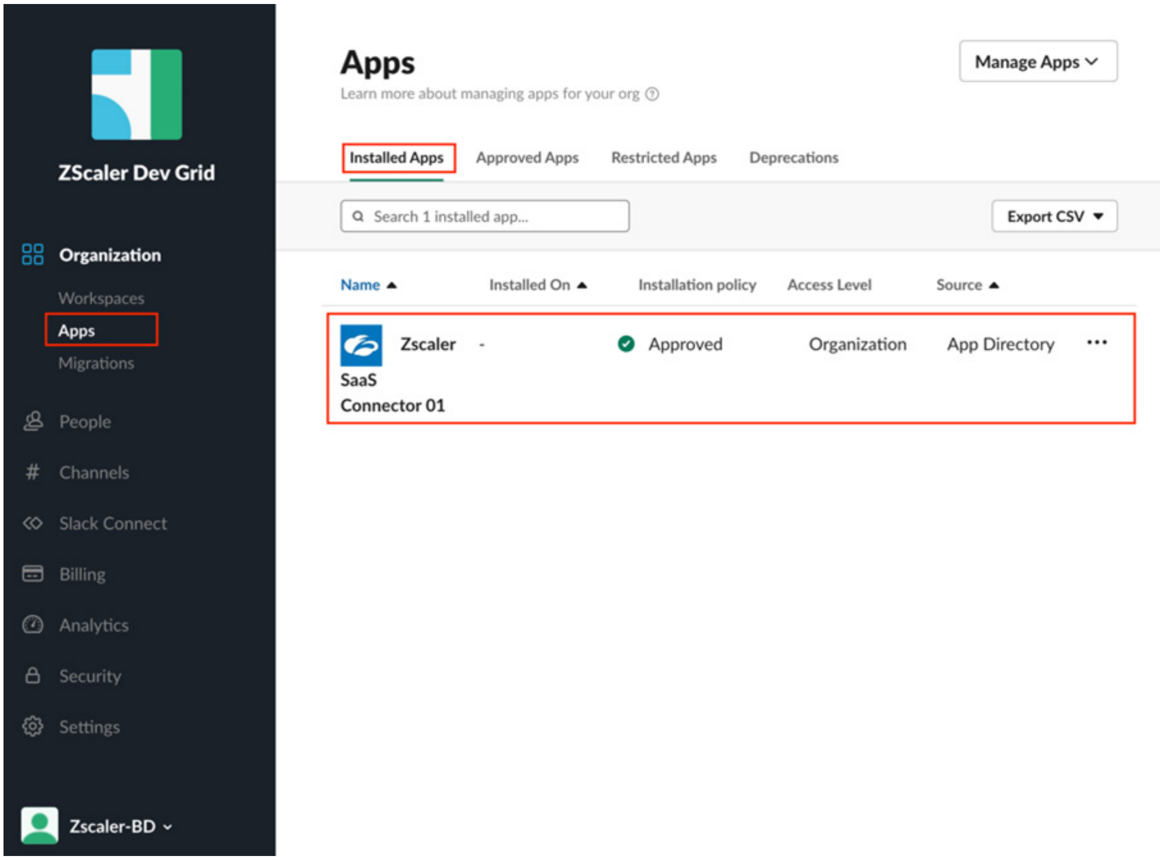
- Perform actions in channels & conversations
- Administer Slack for your organization

Figure 24. Allow Zscaler access to the Slack tenant

Configuring the Zscaler Tenant on Slack

To approve the Zscaler application to allow API calls to be made from Zscaler to Slack:

1. As an admin, select **Manage Organization**.
2. Under **Organization**, select **Apps**.
3. Select **Approve** for the Zscaler Application.
4. After the Zscaler application is approved, return to the ZIA Admin Portal and execute the next step of the installation.

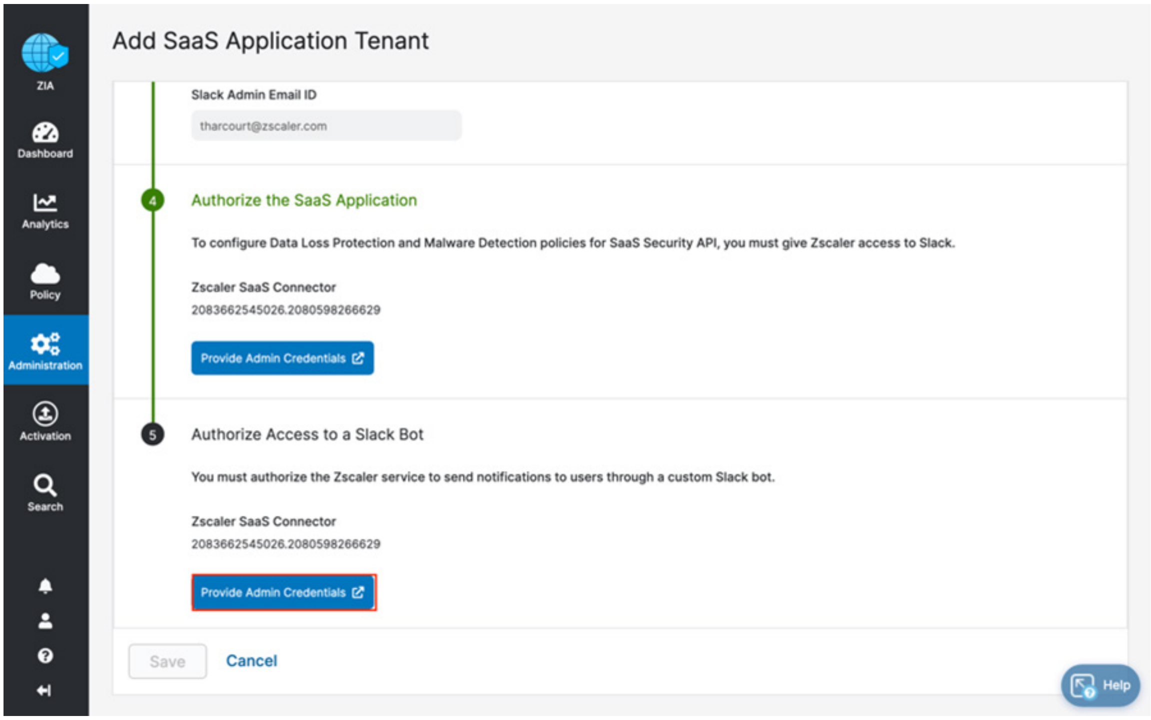


Name	Installed On	Installation policy	Access Level	Source
Zscaler SaaS Connector 01	-	Approved	Organization	App Directory

Figure 25. Approve the Zscaler application

In the **Zscaler Tenant** setup, select the **Provide Admin Credentials** link on Step 5, next. After you have provided the admin credentials, the tenant configuration is complete.

5. Right-click the **Provide Admin Credentials** link and open the link in a new tab.
6. **Save** and **Activate** the configuration. This completes the creation of the Slack tenant. You can now apply Zscaler SaaS Security API controls on the Slack instance using Zscaler data and malware protection.



Add SaaS Application Tenant

Slack Admin Email ID

tharcourt@zscaler.com

4 Authorize the SaaS Application

To configure Data Loss Protection and Malware Detection policies for SaaS Security API, you must give Zscaler access to Slack.

Zscaler SaaS Connector

2083662545026.2080598266629

5 Authorize Access to a Slack Bot

You must authorize the Zscaler service to send notifications to users through a custom Slack bot.

Zscaler SaaS Connector

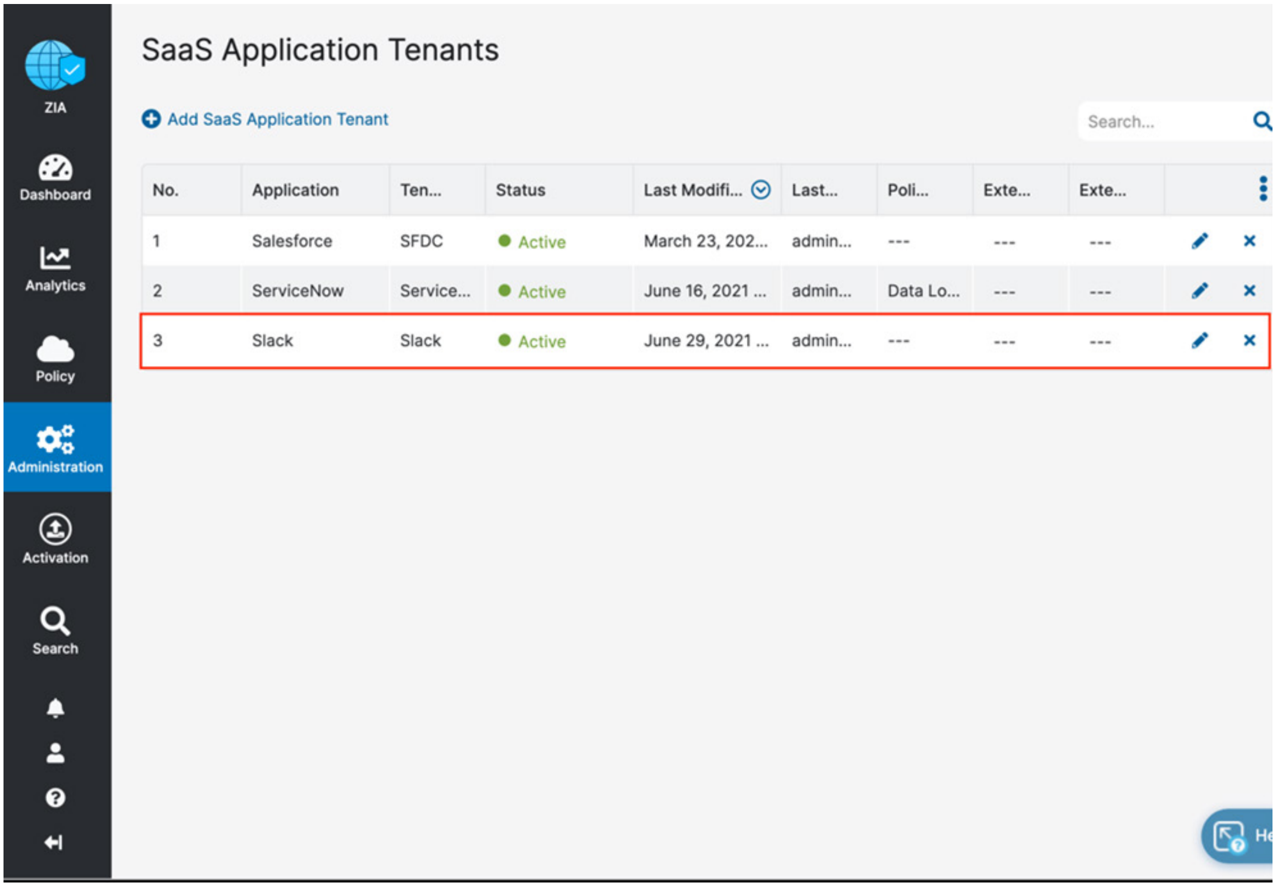
2083662545026.2080598266629

Figure 26. Authorize access to the Slack bot

The Active Slack Tenant

Check that the Status of Slack tenant is Active.

Go to **Administration** > **SaaS Application Tenants**.



No.	Application	Ten...	Status	Last Modifi...	Last...	Poli...	Exte...	Exte...
1	Salesforce	SFDC	● Active	March 23, 202...	admin...	---	---	---
2	ServiceNow	Service...	● Active	June 16, 2021 ...	admin...	Data Lo...	---	---
3	Slack	Slack	● Active	June 29, 2021 ...	admin...	---	---	---

Figure 27. Tenant status

Configuring Slack Policies and Scan Configuration

After adding and configuring the Slack tenant, you can configure the SaaS Security API Control, DLP,and malware policies, and the Scan Configuration for the policies. You can also view reports and data for Slack in Analytics, SaaS Security Insights, and Logs.

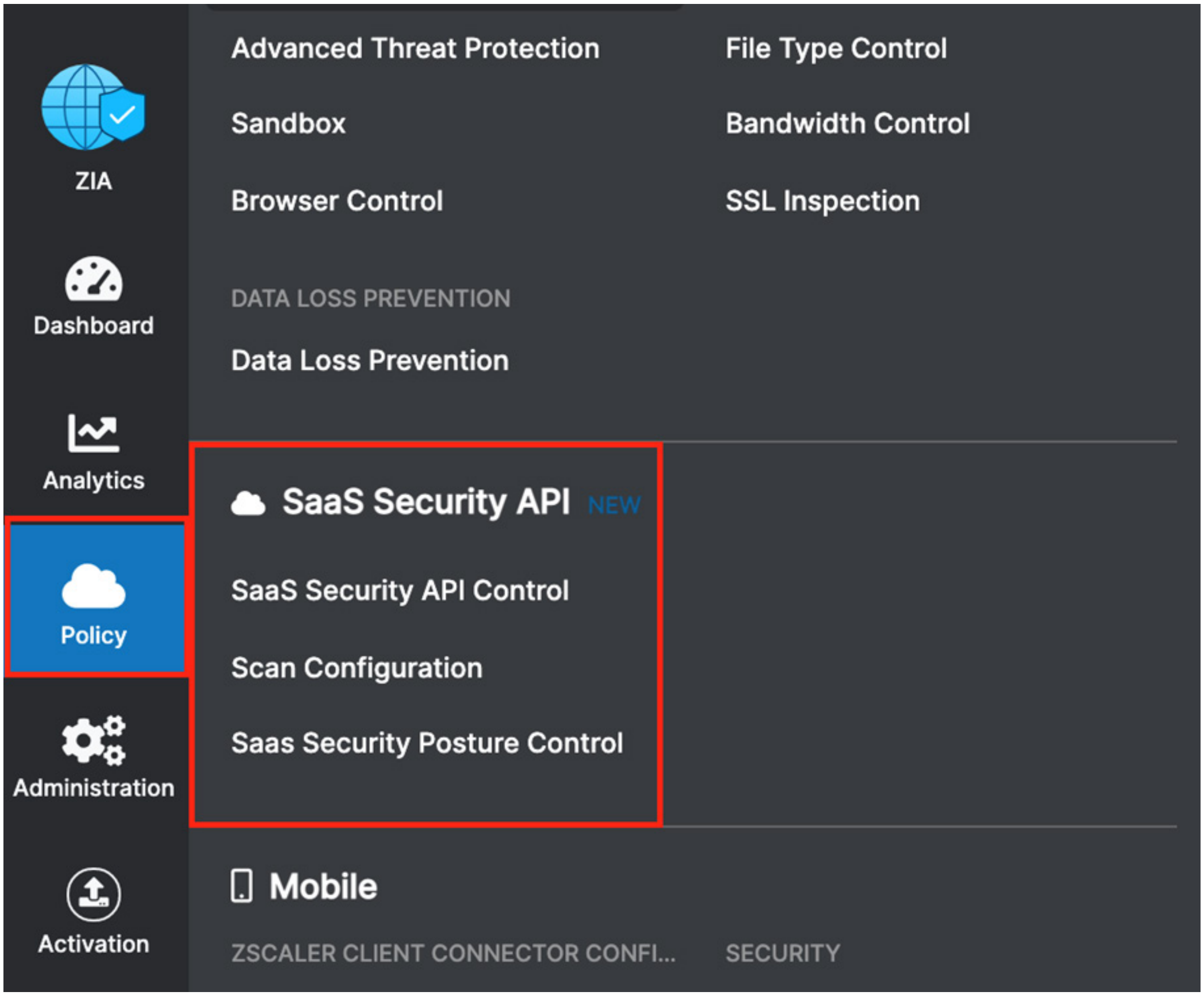
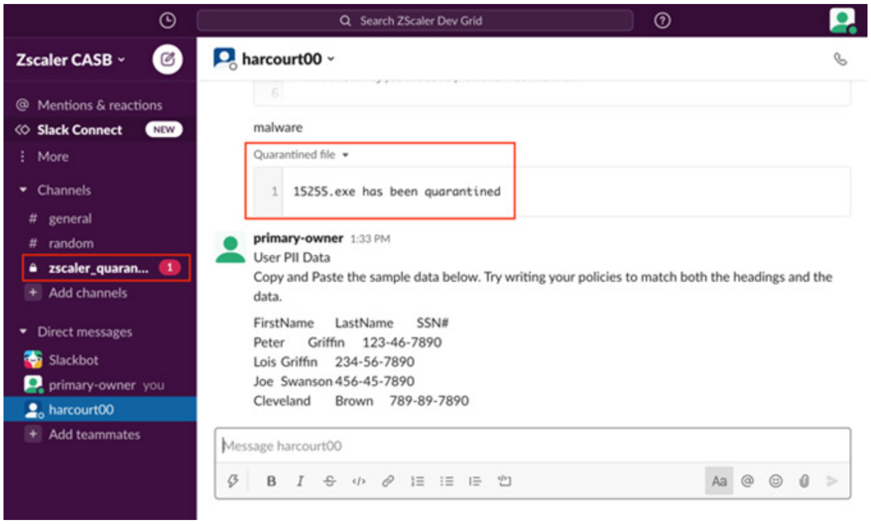


Figure 28. Zscaler policy configuration

Scoping the Policies and Remediation

Zscaler SaaS security scans Slack file attachments. This deployment guide configures a basic DLP policy and a malware policy to scan the Slack account attachment files for matching content of the DLP policy, and to scan the files for known malware using the malware policy. A Slack incident 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, intentional data exposure, and compliance violations that would otherwise go unnoticed.



malware

Quarantined file

```
15255.exe has been quarantined
```

primary-owner 1:33 PM

User PII Data

Copy and Paste the sample data below. Try writing your policies to match both the headings and the data.

FirstName LastName SSN#
Peter Griffin 123-46-7890
Lois Griffin 234-56-7890
Joe Swanson 456-45-7890
Cleveland Brown 789-89-7890

Figure 29. Slack incident with malicious attachments

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 only 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 the SaaS DLP protection is only part of the Zscaler DLP solution, and is used to scan data at rest like the Slack files. This deployment doesn't cover inline data protection, exact data match, or indexed document matching (document template finger printing), although they are integral pieces of a complete data protection solution.

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

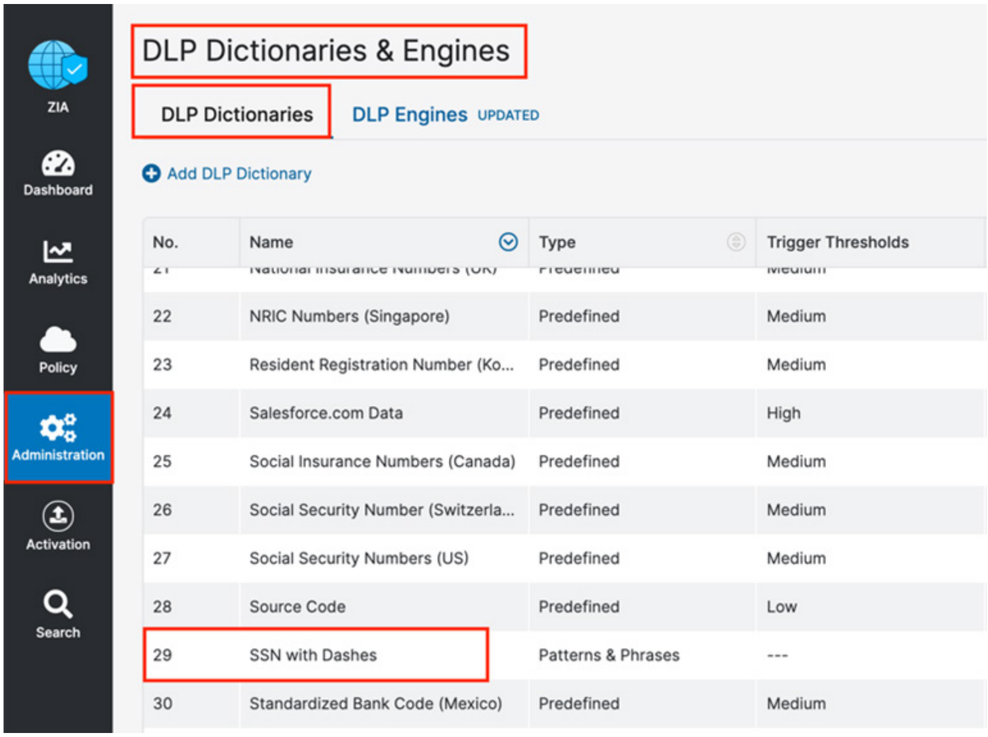
Creating a DLP Policy

The procedures for creating a DLP policy are straightforward. Create a custom dictionary, or use the available dictionaries, to identify the data for which the scan looks. 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 the violation and eliminate false positives.

Next, create a SaaS security DLP policy that allows you to specify the detail about where, when, what action to take, and whom to inform about violations. Finally, the DLP policy is applied to the Slack tenant.

Verify the DLP dictionary as next steps in the ZIA Admin Portal:

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. Select **DLP Dictionaries**.
3. Identify and select the dictionary to be used (in this case, **SSN with Dashes**), then verify the data search parameters.



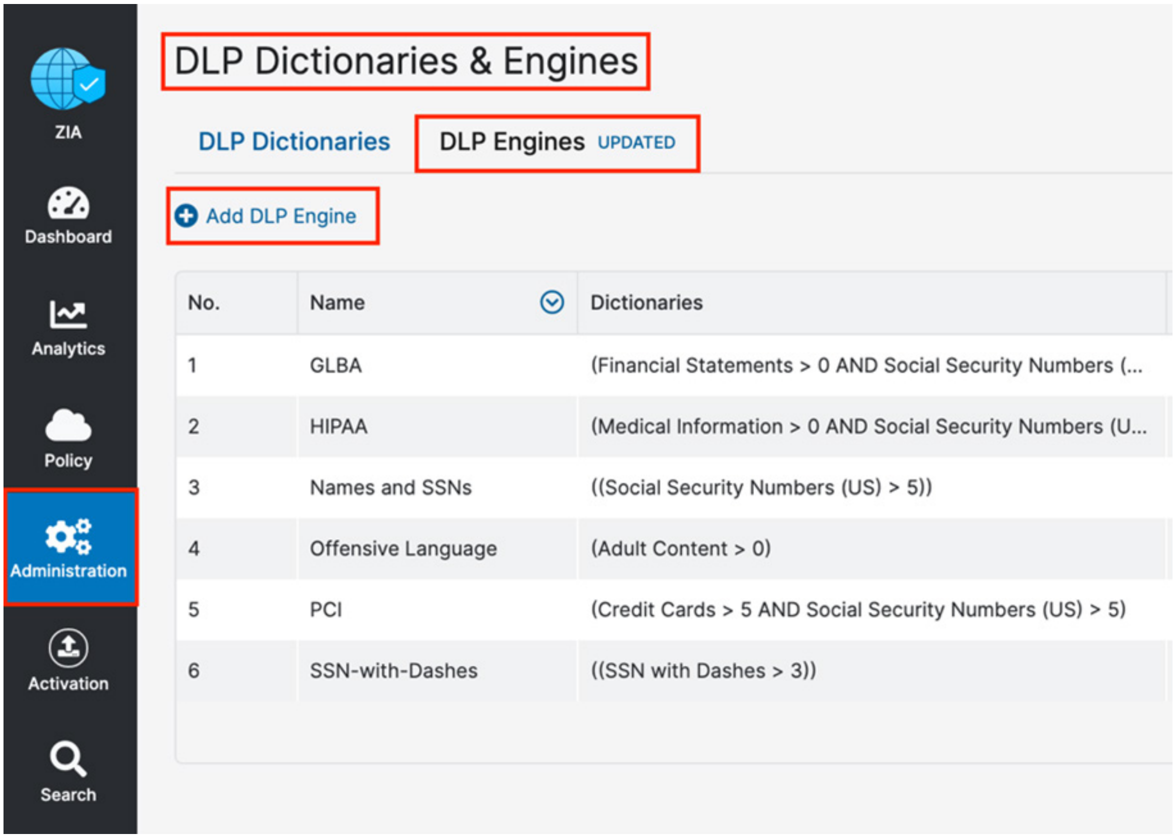
No.	Name	Type	Trigger Thresholds
21	National Insurance Numbers (UK)	Predefined	Medium
22	NRIC Numbers (Singapore)	Predefined	Medium
23	Resident Registration Number (Ko...	Predefined	Medium
24	Salesforce.com Data	Predefined	High
25	Social Insurance Numbers (Canada)	Predefined	Medium
26	Social Security Number (Switzerla...	Predefined	Medium
27	Social Security Numbers (US)	Predefined	Medium
28	Source Code	Predefined	Low
29	SSN with Dashes	Patterns & Phrases	---
30	Standardized Bank Code (Mexico)	Predefined	Medium

Figure 30. Creating a DLP dictionary

Creating a DLP Engine

To create the DLP engine using the verified DLP dictionary:

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. Select the **DLP Engines** tab.
3. Select **Add DLP Engine**.

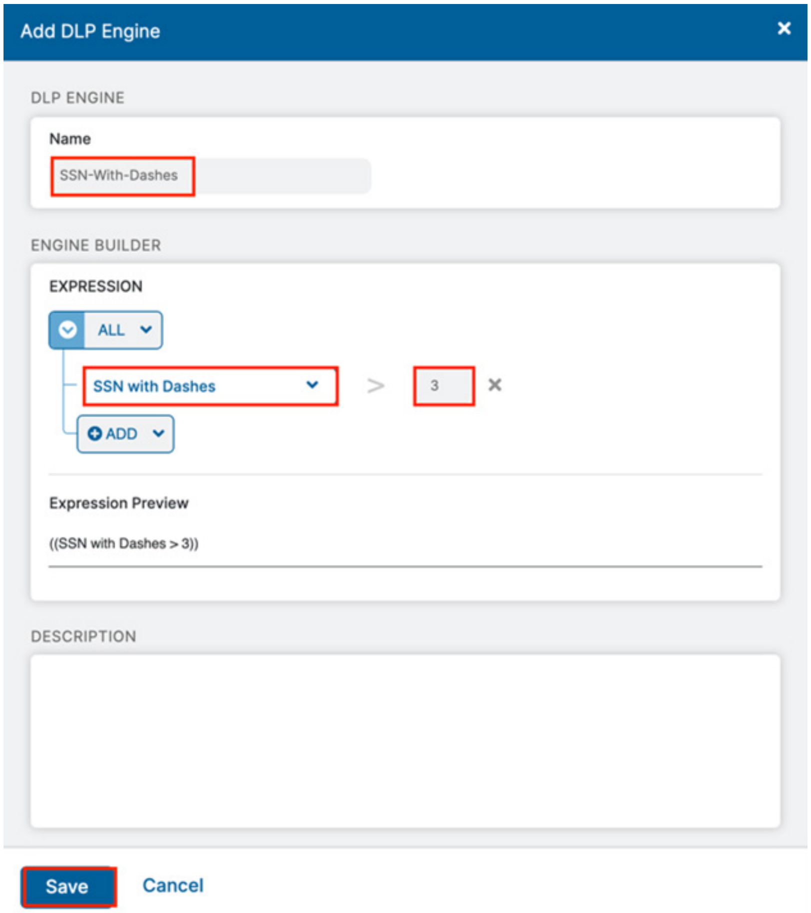


No.	Name	Dictionaries
1	GLBA	(Financial Statements > 0 AND Social Security Numbers (...
2	HIPAA	(Medical Information > 0 AND Social Security Numbers (U...
3	Names and SSNs	((Social Security Numbers (US) > 5))
4	Offensive Language	(Adult Content > 0)
5	PCI	(Credit Cards > 5 AND Social Security Numbers (US) > 5)
6	SSN-with-Dashes	((SSN with Dashes > 3))

Figure 31. Creating a DLP engine

Creating a DLP Engine

1. Give the DLP engine a **Name**.
2. Select the verified dictionary in the **Expression** section under **Engine Builder**.
3. Specify the **Match Count**, which is the minimum number of instances the data can occur in the file before a match is made. In this case, the fourth unique SSN number triggers a match.
4. (Optional) Select **Add** to add the next dictionary and repeat the process if desired.
5. Click **Save**.
6. Activate the configuration.



Add DLP Engine

DLP ENGINE

Name: SSN-With-Dashes

ENGINE BUILDER

EXPRESSION

ALL

SSN with Dashes > 3

Expression Preview

((SSN with Dashes > 3))

DESCRIPTION

Figure 32. The DLP engine wizard

This policy triggers when you see the fourth 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

Apply the engine to a DLP policy that is used for the Slack instance. Launch the DLP Rule Wizard to start the process.

1. Go to **Policy** > **SaaS Security API Control** > **Data Loss Prevention**.
2. Select **Collaboration**.
3. Select **Add DLP Rule**. This launches the **Add DLP Rule** wizard for detailed configuration.

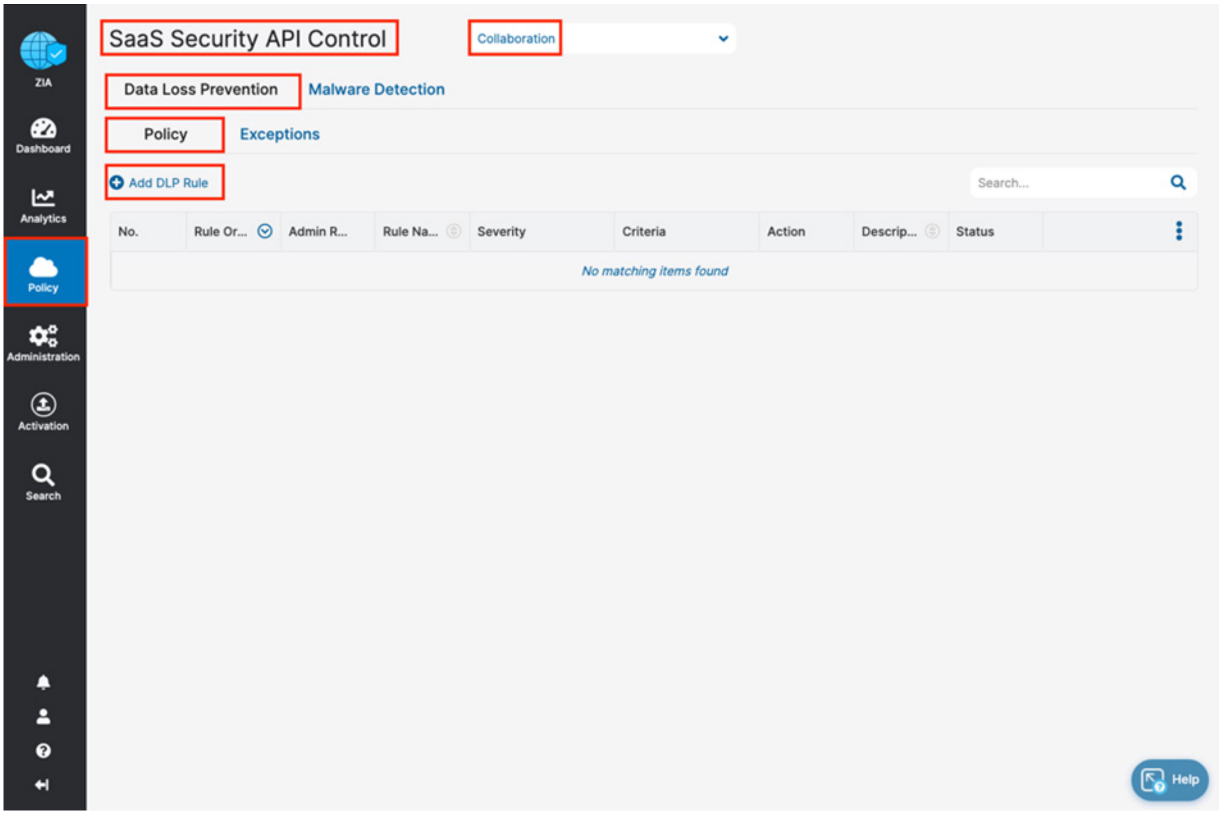


Figure 33. Launch the SaaS DLP Policy Configuration wizard

SaaS DLP Policy Details

The SaaS DLP specifies the details on whom and what data this policy applies. You specify the rule order if you have multiple DLP policies that 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 Content Location and the Action are unique to the SaaS DLP and are explained next for clarification.

Content Location is the location type for the content in Slack that the Zscaler service inspects for sensitive data. Choose Any to inspect all content locations or choose one of the Messages or Channels:

- Direct Messages
- Group Direct Messages
- Private Channels
- Public Channels
- Shared Channels

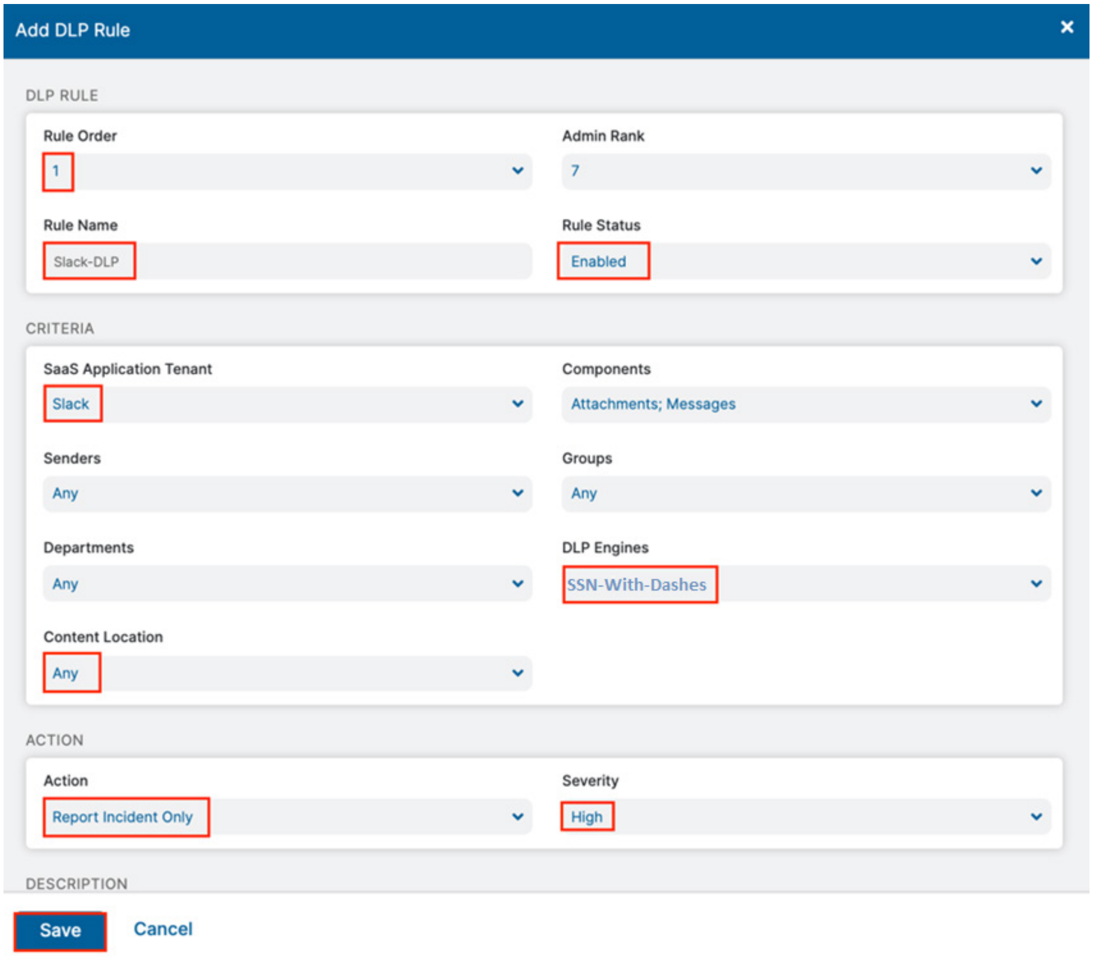
The Action the rule takes upon detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application tenant. For Slack, the action is Report Only. This means that any violations are reported in the Zscaler SaaS Analytics and Alerts.

Report Incident Only: The rule reports the incident only and makes no changes to the file's collaboration scope..

Configure a SaaS DLP Policy

To finish the DLP policy:

1. Specify the **Rule Order** for processing (the first rule matched is executed).
2. **Name** the rule.
3. **Enable** the **Rule Status**.
4. Select **Slack** as the **SaaS Application Tenant**.
5. Select the **DLP Engine** created in Creating a DLP Policy.
6. Select **Any** for the **Content Location**.
7. Select **Report Incident Only** as the **Action**.
8. Select **High** as a **Severity** to allow for identification for searches and tracking.
9. Click **Save** and **Activate** your configuration.



Add DLP Rule

DLP RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Slack-DLP

Rule Status: Enabled

CRITERIA

SaaS Application Tenant: Slack

Components: Attachments; Messages

Senders: Any

Groups: Any

Departments: Any

DLP Engines: SSN-With-Dashes

Content Location: Any

ACTION

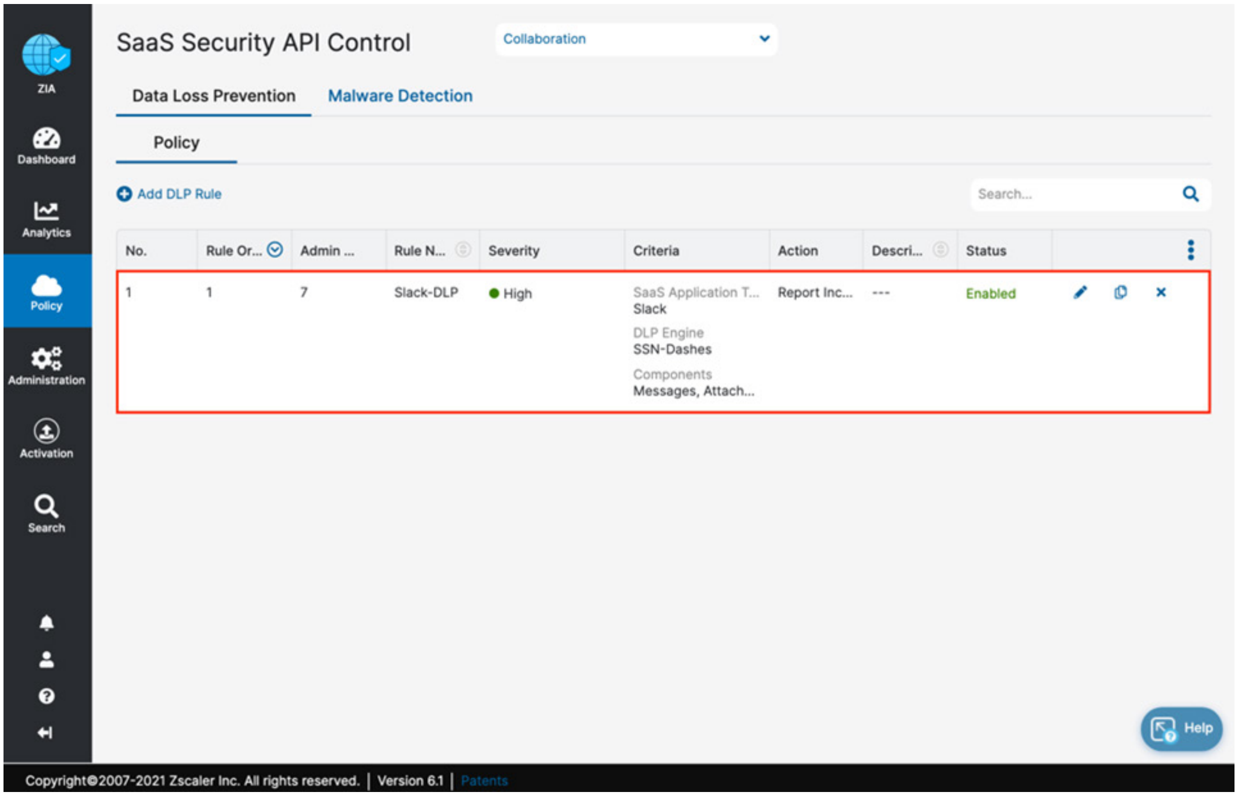
Action: Report Incident Only

Severity: High

DESCRIPTION

Figure 34. The SaaS DLP Policy configuration wizard

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



SaaS Security API Control

Collaboration

Data Loss Prevention | Malware Detection

Policy

Add DLP Rule

Search...

No.	Rule Or...	Admin ...	Rule N...	Severity	Criteria	Action	Descri...	Status
1	1	7	Slack-DLP	● High	SaaS Application T... Slack DLP Engine SSN-Dashes Components Messages, Attach...	Report Inc...	---	Enabled

Copyright©2007-2021 Zscaler Inc. All rights reserved. | Version 6.1 | Patents

Figure 35. The configured DLP policy

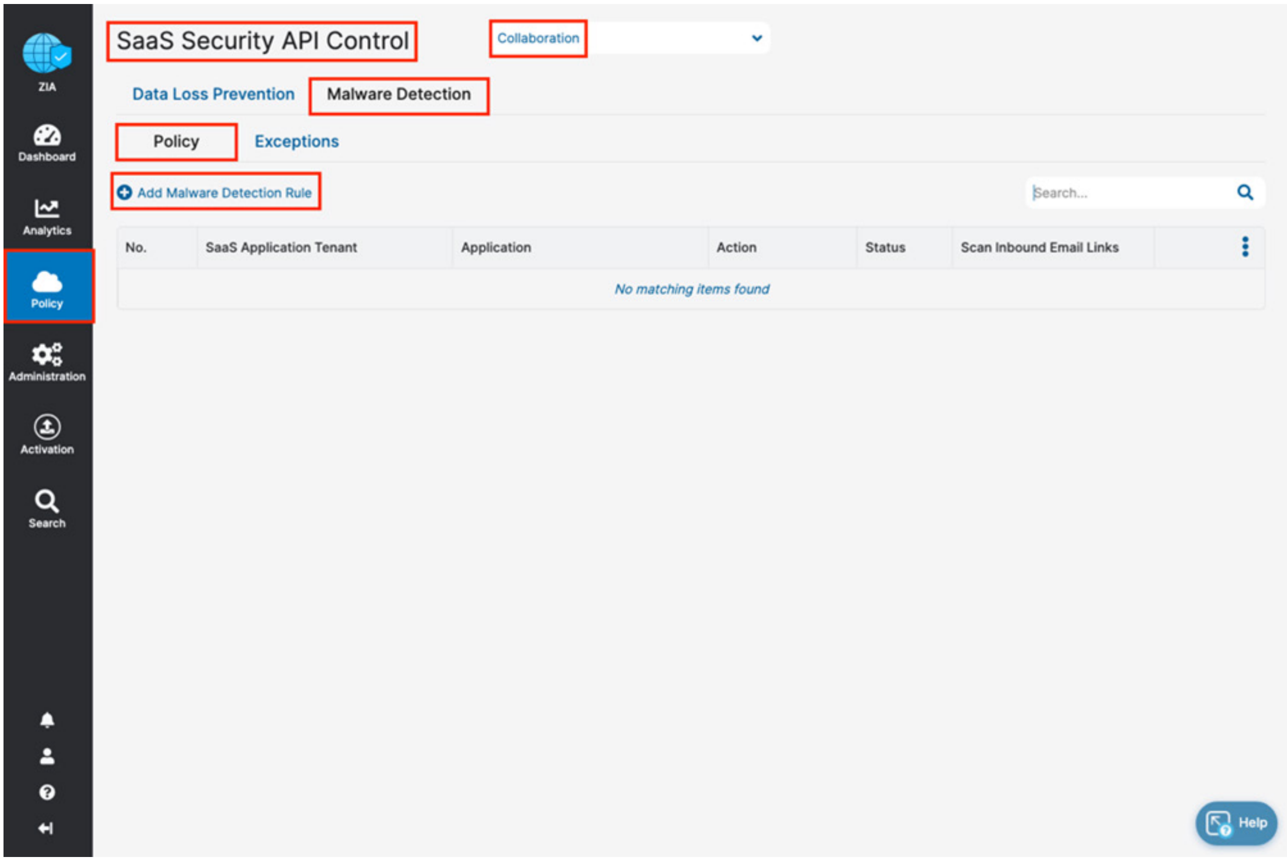
Configure a SaaS Malware Policy

To launch the Malware Rule wizard:

1. Go to **Policy** > **SaaS Security API Control** > **Malware Detection**.
2. Select **Collaboration**.
3. Select **Add Malware Detection Rule**.

   The SaaS Malware Detection policy is an all-encompassing policy. All files in the tenant are scanned unless removed from the scope by specifying any exemptions using the **Exemption** tab under Malware Detection. To add a malware policy, specify the application, the SaaS tenant, and the status.

4. The **Action** for Slack is limited to **Report Malware only**.



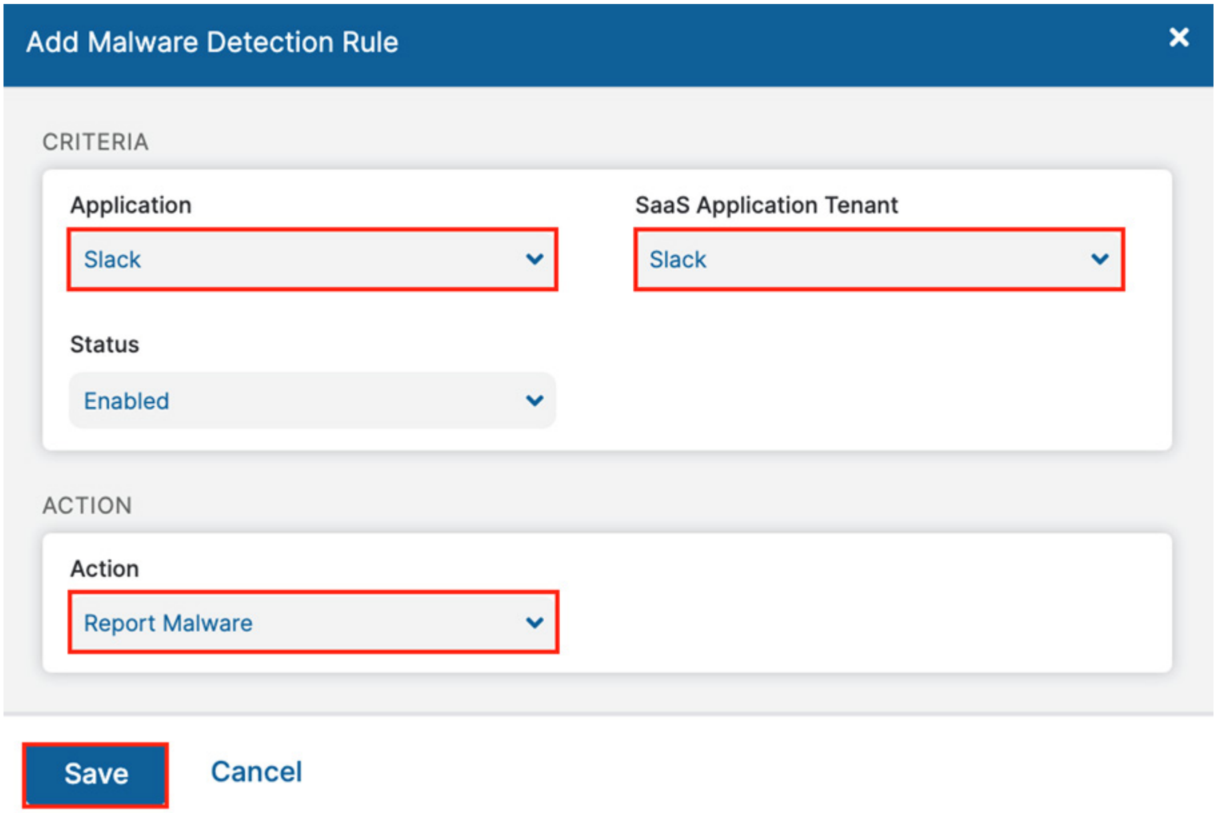
No.	SaaS Application Tenant	Application	Action	Status	Scan Inbound Email Links
No matching items found					

Figure 36. Launch the Malware Policy configuration wizard

SaaS Malware Detection Policy Wizard

Configure the Malware Rule wizard:

1. Go to **Policy** > **SaaS Security API Control** > **Malware Detection**.
2. Select **Collaboration**.
3. Select **Add Malware Detection Rule**.
4. Under **Criteria**, select **Slack** as the **Application**.
5. Select the **Slack Application Tenant** to apply the policy.
6. Select **Enabled** for **Status**.
7. Select **Report Malware** as the **Action**.
8. Click **Save**.



Add Malware Detection Rule

CRITERIA

Application: Slack

SaaS Application Tenant: Slack

Status: Enabled

ACTION

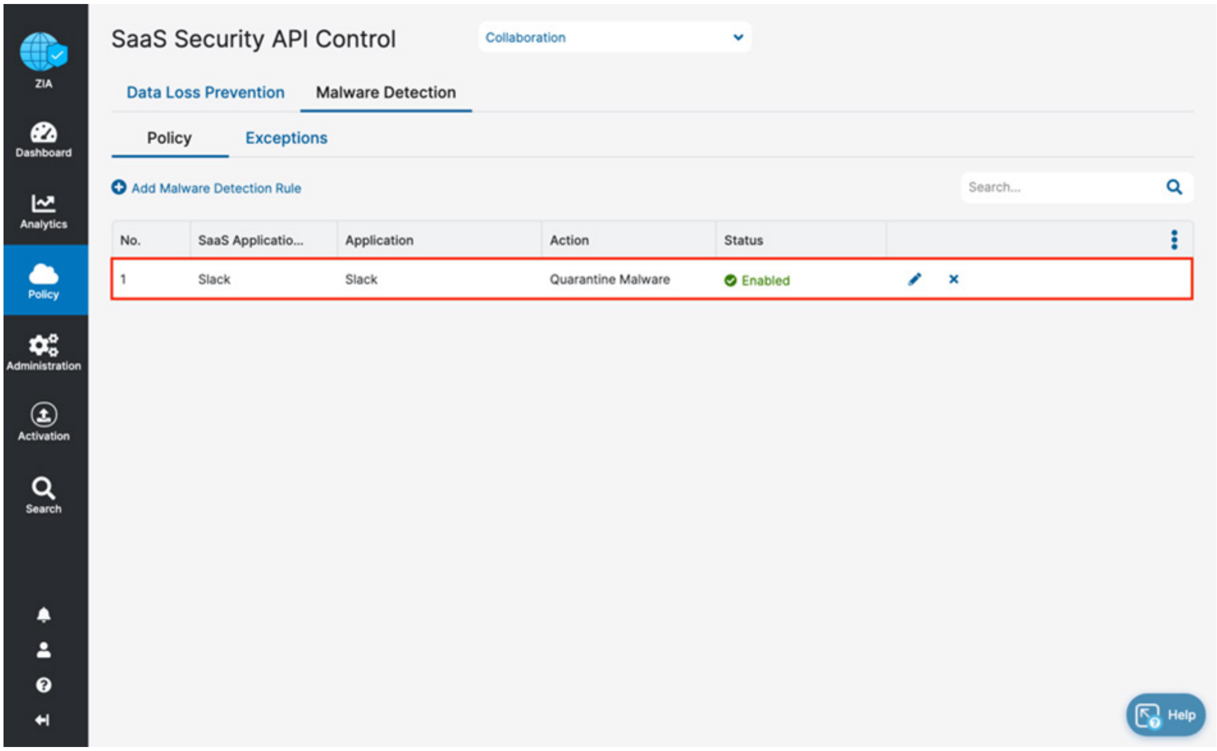
Action: Report Malware

Figure 37. The Malware Detection Policy configuration wizard

SaaS Malware Detection Policy

Apply the completed SaaS Security Malware Detection policy for the Slack SaaS tenant to the Slack instance with a scanning schedule.

Activate your configuration.



No.	SaaS Applicatio...	Application	Action	Status
1	Slack	Slack	Quarantine Malware	Enabled

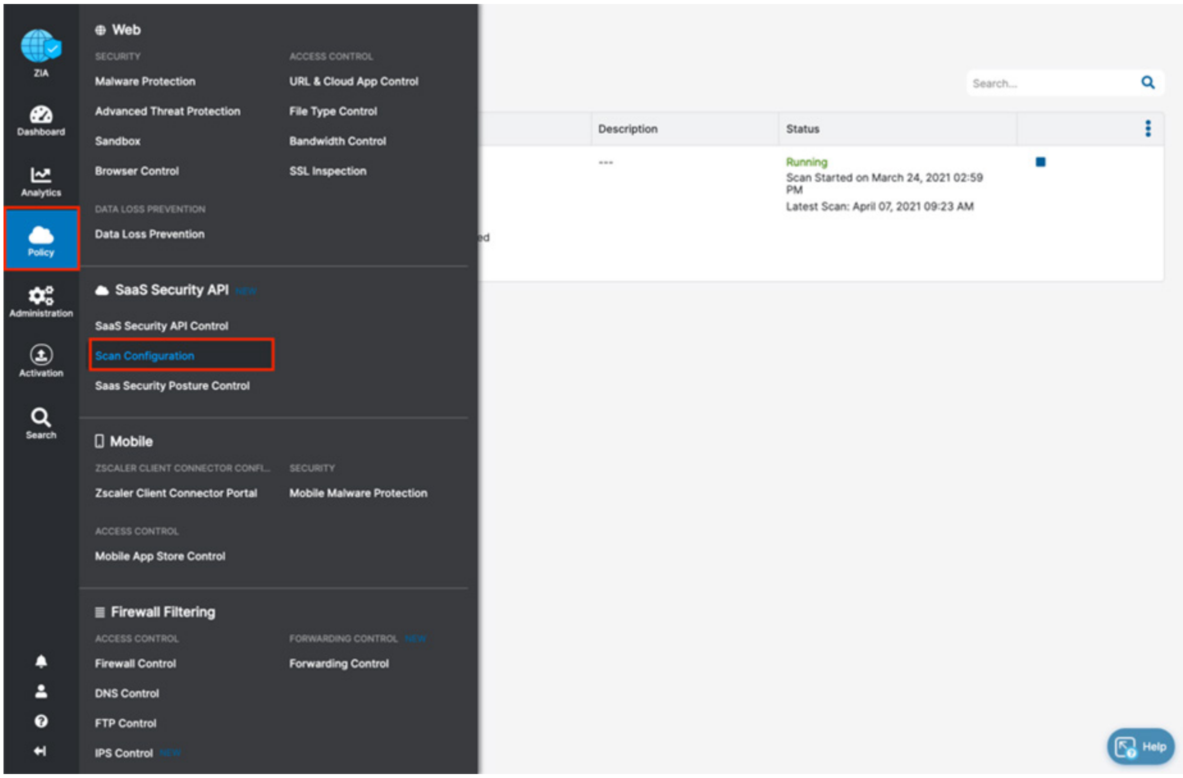
Figure 38. The completed Malware Detection policy configuration wizard

Configure the Scan Schedule Configuration

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. This deployment guide selects All Data. However, if this is a 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 **Slack SaaS Tenant** for the **SaaS Application Tenant**.
3. Select the data loss policy and the malware policy created in prior steps.
4. Select **All Data**.
5. Click **Save** to save the scan schedule and activate the configuration.



Description	Status
---	Running Scan Started on March 24, 2021 02:59 PM Latest Scan: April 07, 2021 09:23 AM

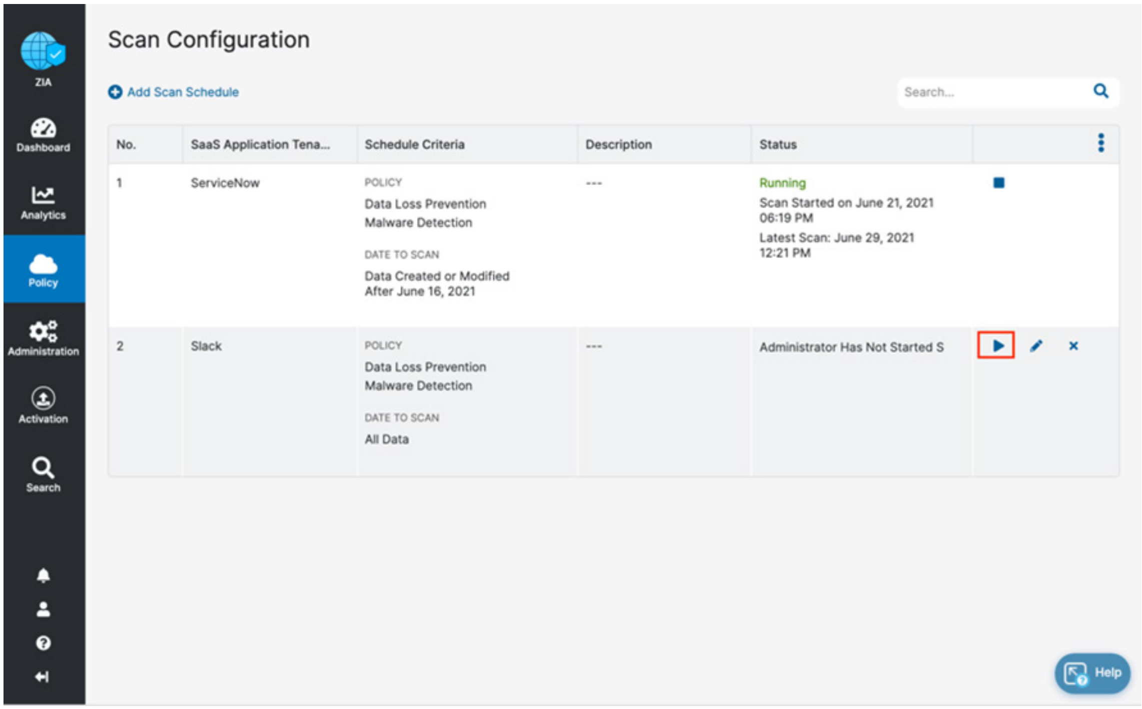
Figure 39. Create and enable a scan for the SaaS tenant

For a POV or Trial, select New Data Only.

Start the Scan Schedule

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

1. Click the **Start** icon.
2. Review the **Status** column and ensure it is **Running** with a start date and a latest scan date.



Scan Configuration

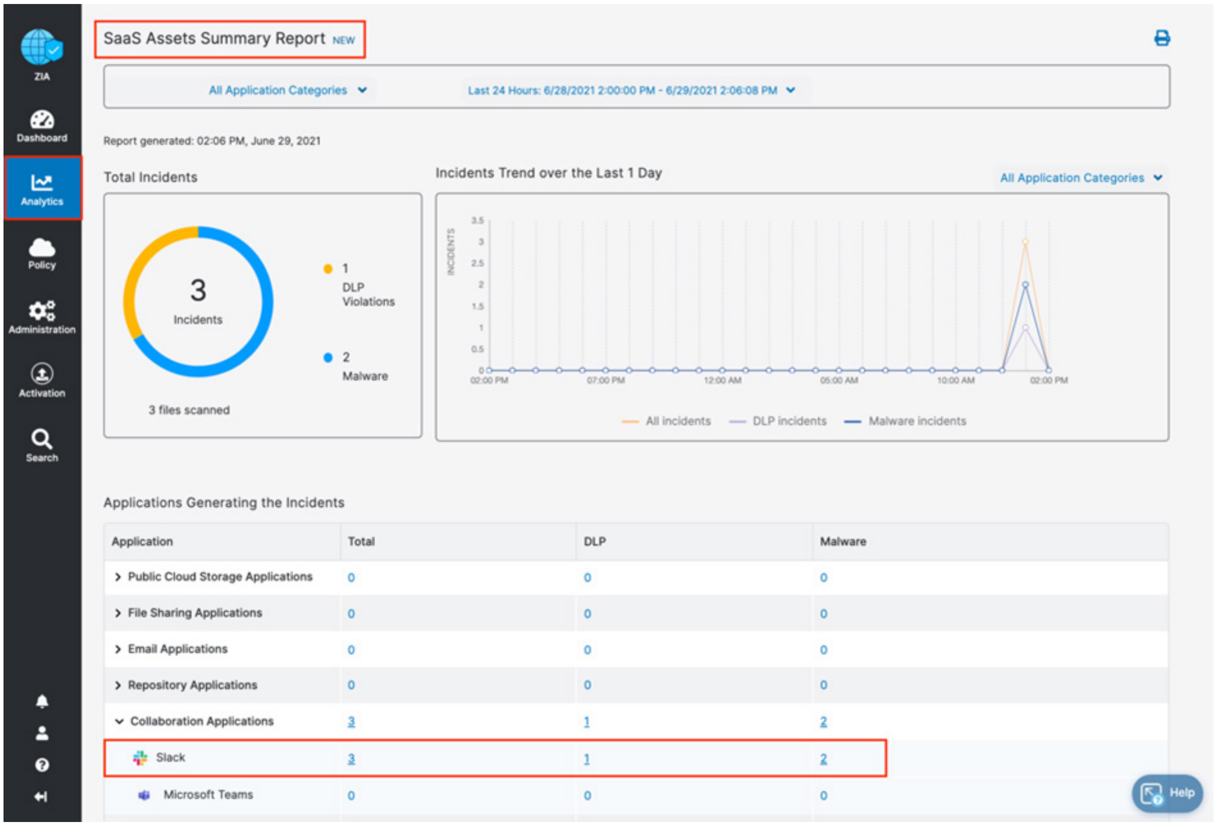
No.	SaaS Application Tena...	Schedule Criteria	Description	Status
1	ServiceNow	POLICY Data Loss Prevention Malware Detection DATE TO SCAN Data Created or Modified After June 16, 2021	---	Running Scan Started on June 21, 2021 06:19 PM Latest Scan: June 29, 2021 12:21 PM
2	Slack	POLICY Data Loss Prevention Malware Detection DATE TO SCAN All Data	---	Administrator Has Not Started S

Figure 40. Starting the scan

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 for data-at-rest associated with the user. Zscaler provides reports and SaaS security insights for the SaaS partners. This gives visibility from a high-level and lets you manage individual logs and violations.

Take a brief look at the tools, but for detailed information of the SaaS Security Analytics tools, see **SaaS Security Alerts & Activities Report** (government agencies, see **SaaS Security Alerts & Activities Report**).



SaaS Assets Summary Report NEW

All Application Categories

Last 24 Hours: 6/28/2021 2:00:00 PM - 6/29/2021 2:06:08 PM

Report generated: 02:06 PM, June 29, 2021

Total Incidents

3 files scanned

Incidents Trend over the Last 1 Day

All Application Categories

Applications Generating the Incidents

Application	Total	DLP	Malware
› Public Cloud Storage Applications	0	0	0
› File Sharing Applications	0	0	0
› Email Applications	0	0	0
› Repository Applications	0	0	0
⌄ Collaboration Applications	3	1	2
Slack	3	1	2
Microsoft Teams	0	0	0

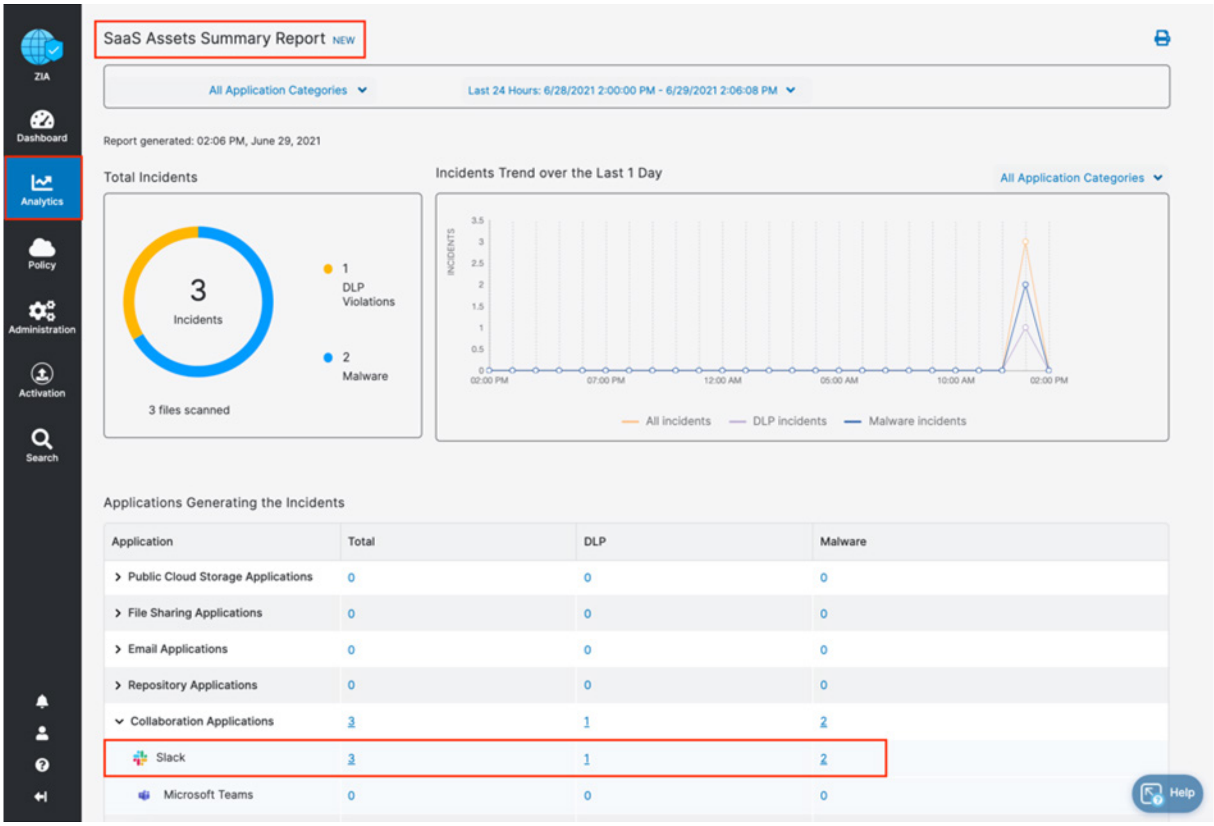
Figure 41. SaaS security visibility

SaaS Assets and SaaS Assets Summary Report

The SaaS asset reports provide a summary or customizable reporting to provide a quick view of your files and emails. The SaaS Assets Summary Report provides all activity and violations in a quick glance. The report identifies all SaaS tenant information from a single screen.

The Slack activity over the creation of this deployment guide is shown, but any tenant configured is also displayed on this summary screen. The data is hyperlinked, and you can pivot from a summary to individual logs and activities provided by SaaS security insights.

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



SaaS Assets Summary Report NEW

All Application Categories | Last 24 Hours: 6/28/2021 2:00:00 PM - 6/29/2021 2:06:08 PM

Report generated: 02:06 PM, June 29, 2021

Total Incidents

3 Incidents

● 1 DLP Violations

● 2 Malware

3 files scanned

Incidents Trend over the Last 1 Day | All Application Categories

Applications Generating the Incidents

Application	Total	DLP	Malware
› Public Cloud Storage Applications	0	0	0
› File Sharing Applications	0	0	0
› Email Applications	0	0	0
› Repository Applications	0	0	0
⌄ Collaboration Applications	3	1	2
Slack	3	1	2
Microsoft Teams	0	0	0

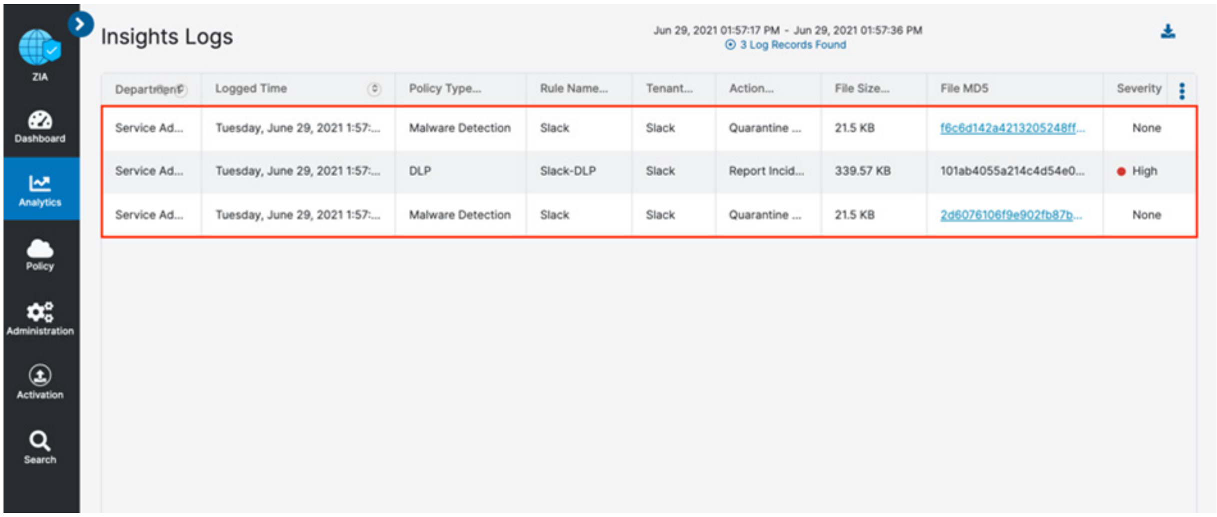
Figure 42. Summary reports

SaaS Security Insights

The SaaS Security Insights page is where you can view and select information fields that you want to view 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 and their associated filters:

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



Insights Logs

Jun 29, 2021 01:57:17 PM - Jun 29, 2021 01:57:36 PM
3 Log Records Found

Department	Logged Time	Policy Type...	Rule Name...	Tenant...	Action...	File Size...	File MD5	Severity
Service Ad...	Tuesday, June 29, 2021 1:57:...	Malware Detection	Slack	Slack	Quarantine ...	21.5 KB	f6c6d142a4213205248ff...	None
Service Ad...	Tuesday, June 29, 2021 1:57:...	DLP	Slack-DLP	Slack	Report Incid...	339.57 KB	101ab4055a214c4d54e0...	● High
Service Ad...	Tuesday, June 29, 2021 1:57:...	Malware Detection	Slack	Slack	Quarantine ...	21.5 KB	2d6076106f9e902fb87b...	None

Figure 43. SaaS security insight

Zscaler Digital Exchange (ZDX) for Slack

ZDX is the missing link needed for customers and their SaaS applications. As applications move to the cloud, the internet is your new transport network. With users working from anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. ZDX provides visibility into the client's experience using Slack. ZDX uses the Zscaler Client Connector to generate application and network probes and gather device health. ZDX is a separate service from ZIA SaaS Security and can run with or without SaaS Security enabled.

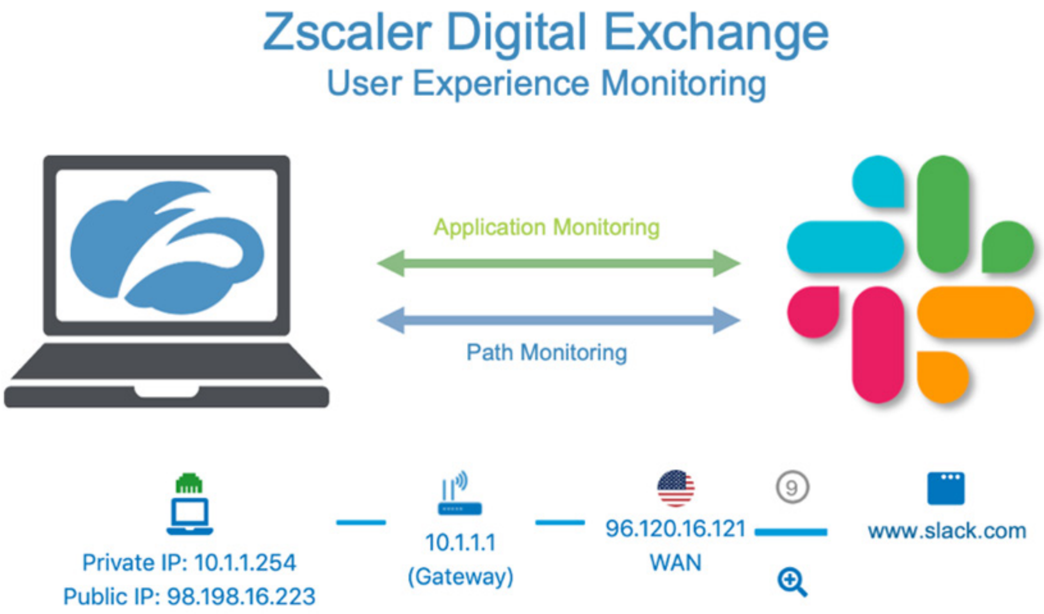


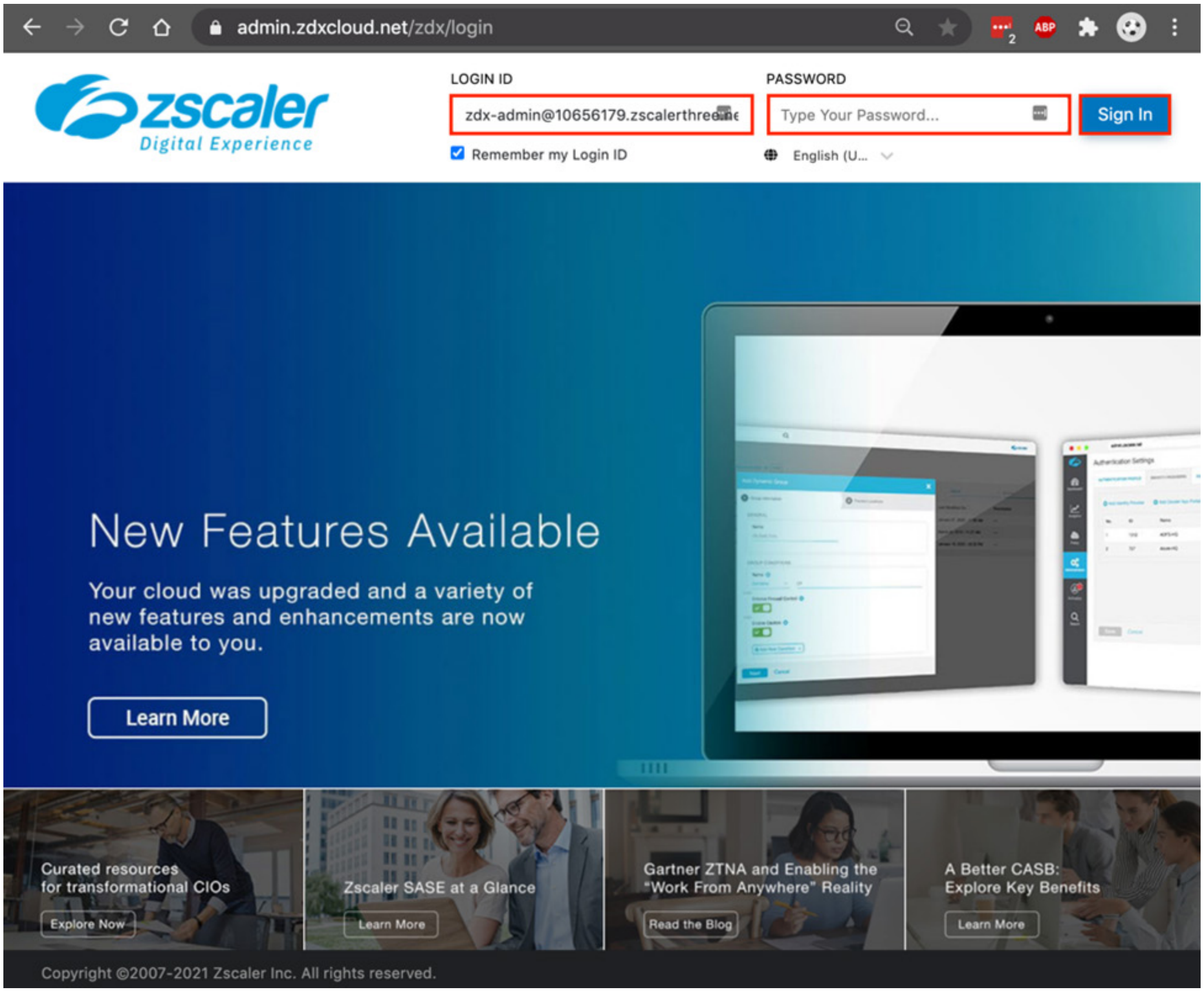
Figure 44. ZDX for user experience monitoring for Slack

ZDX allows organizations to continuously gather and analyze data on end-user device resources and events, such as CPU, memory usage, and Wi-Fi connectivity issues that impact end-user experiences. Measure and analyze end-to-end and hop-by-hop network path metrics from every user device to the cloud application. With cloud path visibility, you can proactively detect and resolve end-user connectivity issues to cloud applications.

Continuously monitor and measure application metrics, such as response time, DNS resolution, and broader availability metrics of the application. Monitor aggregated user experience performance scores tracked over time at the user, application, location, department, and organizational level.

Log in to ZDX

Log into the ZDX Admin Portal with admin credentials to begin the configuration process.



admin.zdxcloud.net/zdx/login

LOGIN ID: zdx-admin@10656179.zscalerthree.ne

PASSWORD: Type Your Password...

☑ Remember my Login ID

English (U...

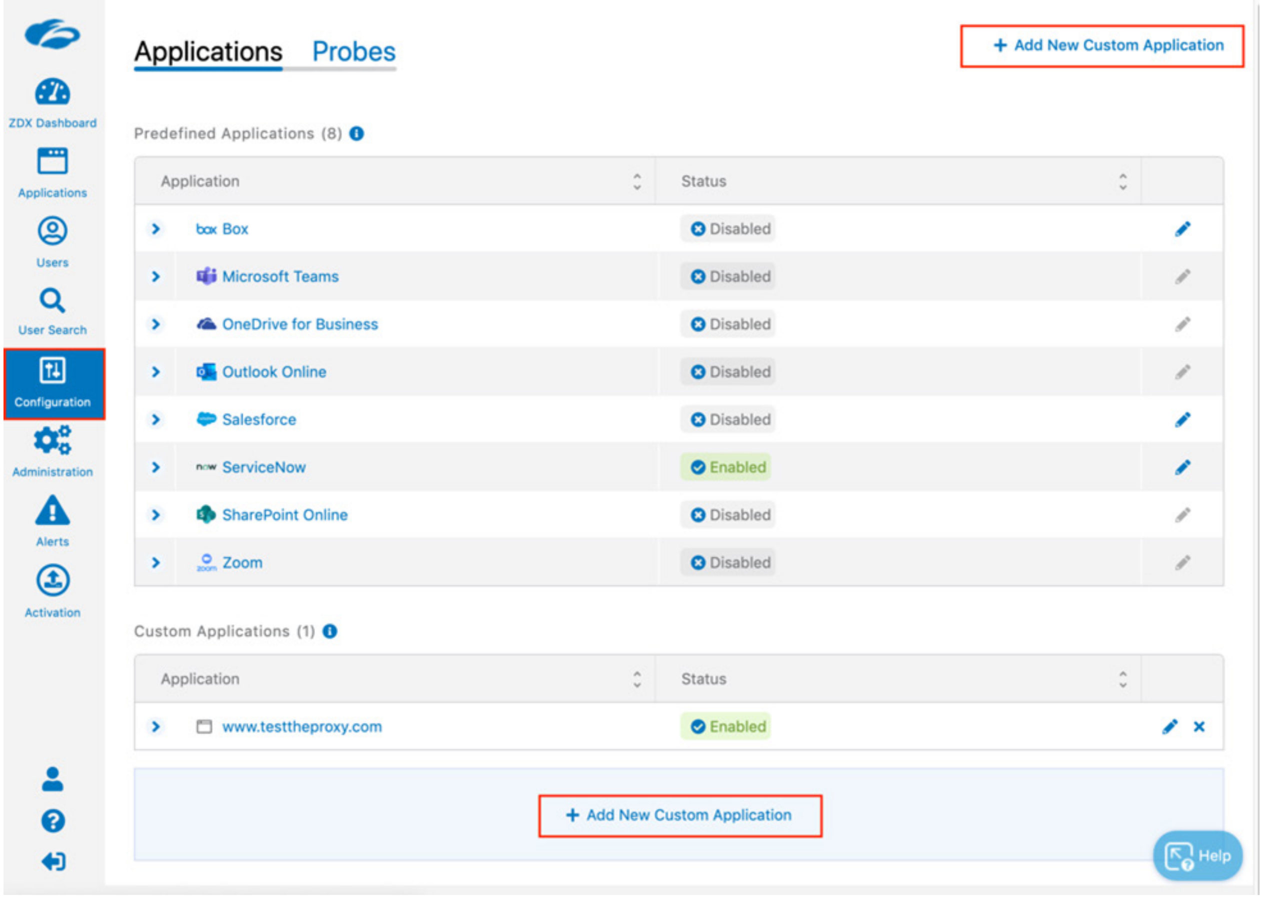
zscaler
Digital Experience
Sign In
New Features Available
Your cloud was upgraded and a variety of new features and enhancements are now available to you.
Learn More
Curated resources for transformational CIOs
Explore Now
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2021 Zscaler Inc. All rights reserved.

Figure 45. ZDX for user experience monitoring for Slack

Configure ZDX for Slack

Although Slack is not a predefined application in ZDX, you can configure it. To configure the Slack application for monitoring, configure Slack as an application and add a Web probe and a network probe:

1. Select **Configuration**.
2. Select **Applications**.
3. Select **Add New Custom Application**. The **New App** wizard is displayed for you to enter a name and to enable the Slack application.



Predefined Applications (8)

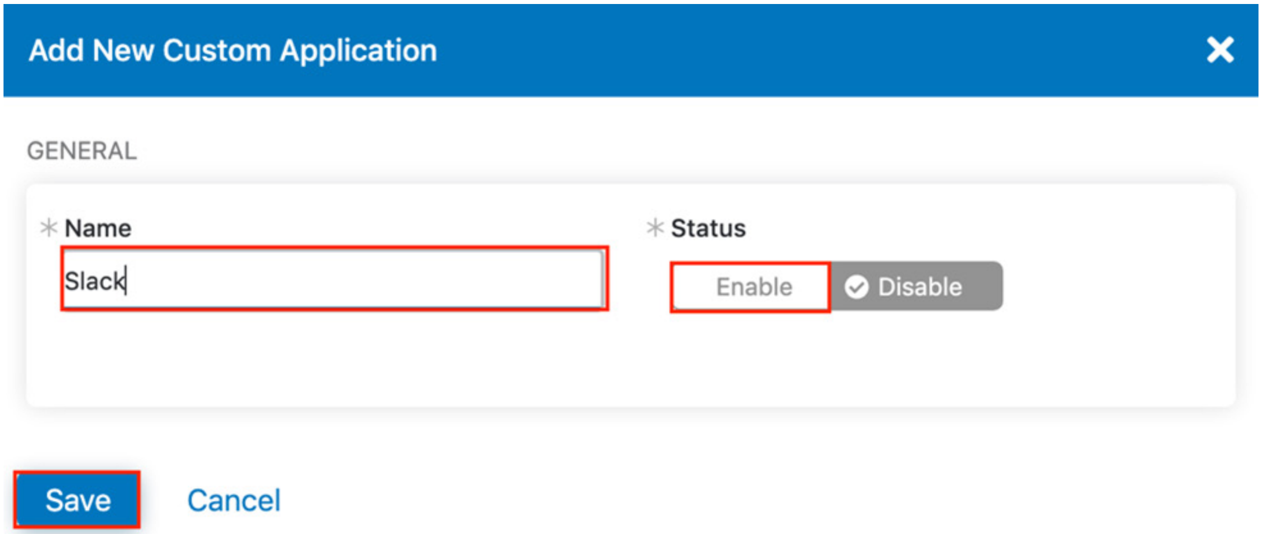
Application	Status
Box	Disabled
Microsoft Teams	Disabled
OneDrive for Business	Disabled
Outlook Online	Disabled
Salesforce	Disabled
ServiceNow	Enabled
SharePoint Online	Disabled
Zoom	Disabled

Custom Applications (1)

Application	Status
www.testtheproxy.com	Enabled

Figure 46. Onboard the Slack app

4. To configure the Slack application for monitoring, add a **Name** for the Slack application.
5. Select **Enable** for **Status**.
6. Click **Save**.



Add New Custom Application

GENERAL

* Name: Slack

* Status: Enable | Disable

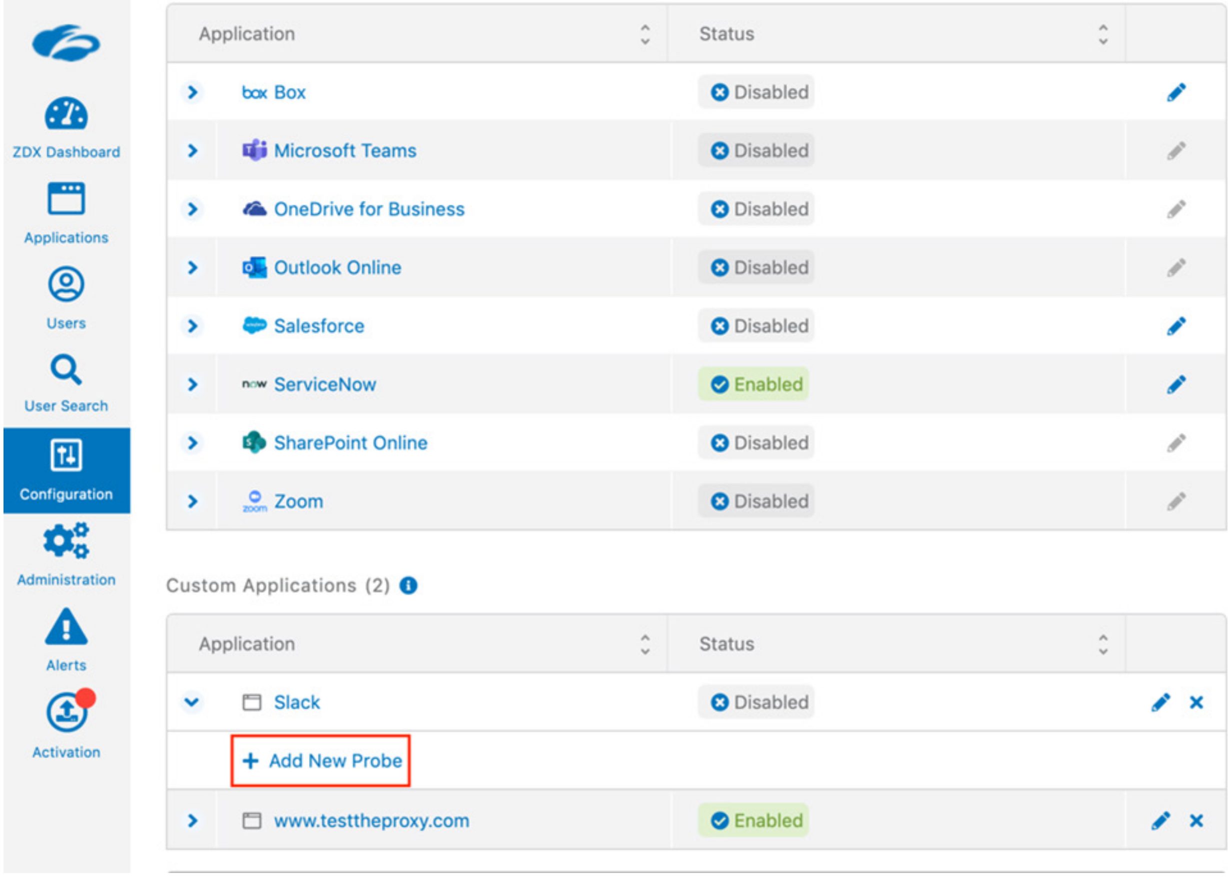
Figure 47. Onboard the Slack app

This defines the application. Create the Web probe and the Cloud Path probe for monitoring the application.

Configure ZDX Probes for Slack

Slack is defined as an application in ZDX. You must configure the probes. Select Add New Probe under the Slack application you just created.

This launches the Probe wizard to create the probes for monitoring the Slack application.



Application	Status
Box	Disabled
Microsoft Teams	Disabled
OneDrive for Business	Disabled
Outlook Online	Disabled
Salesforce	Disabled
ServiceNow	Enabled
SharePoint Online	Disabled
Zoom	Disabled

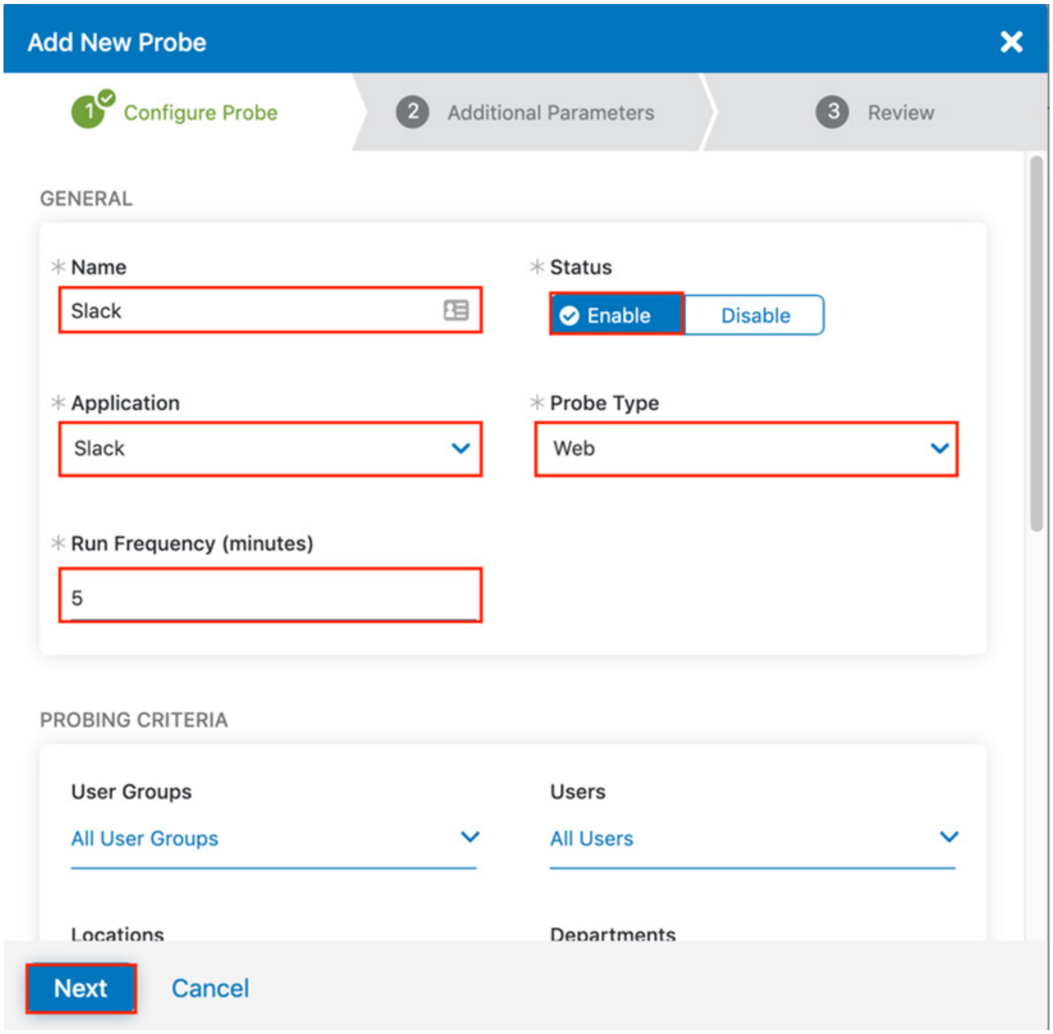
Custom Applications (2)

Application	Status
Slack	Disabled
+ Add New Probe	
www.testtheproxy.com	Enabled

Figure 48. Onboard the Slack app

For the Web probe:

1. Give the Web probe a logical **Name**.
2. Select **Enable** for **Status**.
3. Select **Slack** as the **Application**.
4. Select **Web** as a **Probe Type**.
5. Enter **5** minutes as the **Run Frequency**.
6. Click **Next**.



Add New Probe

1 Configure Probe — 2 Additional Parameters — 3 Review

GENERAL

* Name: Slack

* Status: Enable | Disable

* Application: Slack

* Probe Type: Web

* Run Frequency (minutes): 5

PROBING CRITERIA

User Groups: All User Groups

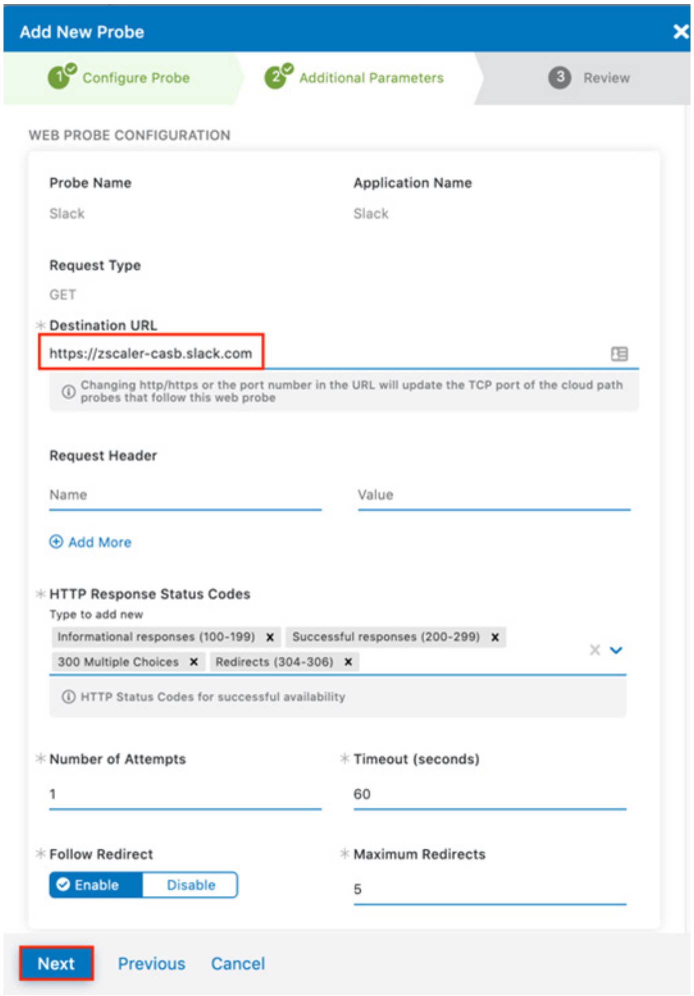
Users: All Users

Locations

Departments

Figure 49. Configure the Slack probes

7. Enter the Slack Instance URL for the **Destination URL**.
8. Click **Next**.



Add New Probe

1 Configure Probe · 2 Additional Parameters · 3 Review

WEB PROBE CONFIGURATION

Probe Name: Slack

Application Name: Slack

Request Type: GET

* Destination URL: https://zscaler-casb.slack.com

Changing http/https or the port number in the URL will update the TCP port of the cloud path probes that follow this web probe

Request Header

Name | Value

Add More

* HTTP Response Status Codes

Type to add new

Informational responses (100-199) ✕ Successful responses (200-299) ✕ 300 Multiple Choices ✕ Redirects (304-306) ✕

HTTP Status Codes for successful availability

* Number of Attempts: 1

* Timeout (seconds): 60

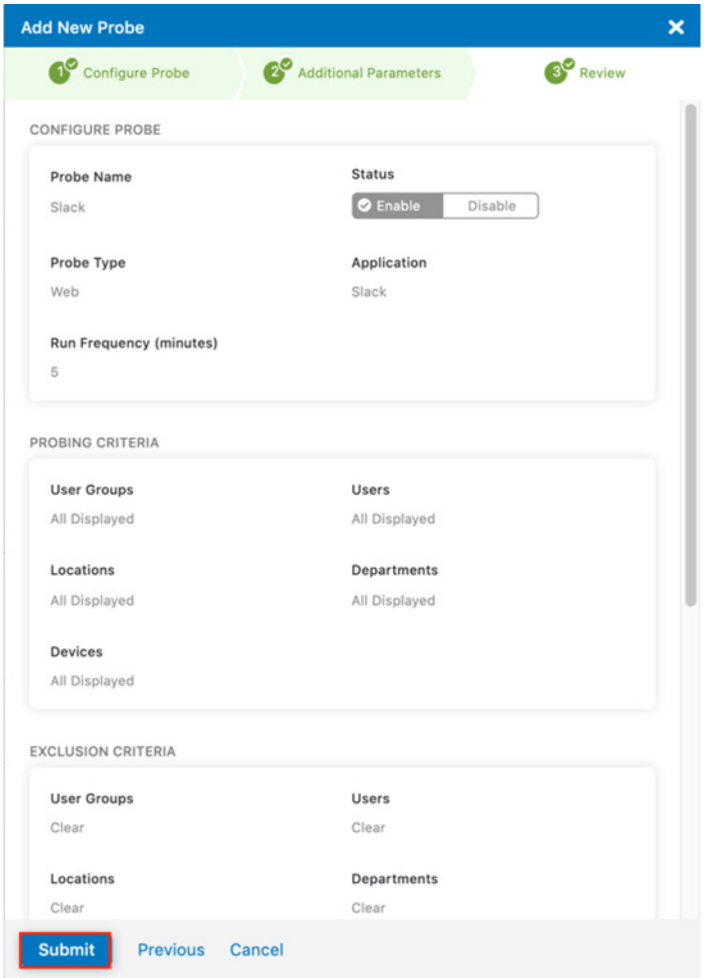
* Follow Redirect: Enable | Disable

* Maximum Redirects: 5

Next · Previous · Cancel

Figure 50. Configuring the Web probe

Verify the Web probe configuration and make any changes necessary and then submit the probe configuration. Click Submit.



Add New Probe

CONFIGURE PROBE

Probe Name: Slack

Status: Enable | Disable

Probe Type: Web

Application: Slack

Run Frequency (minutes): 5

PROBING CRITERIA

User Groups: All Displayed

Users: All Displayed

Locations: All Displayed

Departments: All Displayed

Devices: All Displayed

EXCLUSION CRITERIA

User Groups: Clear

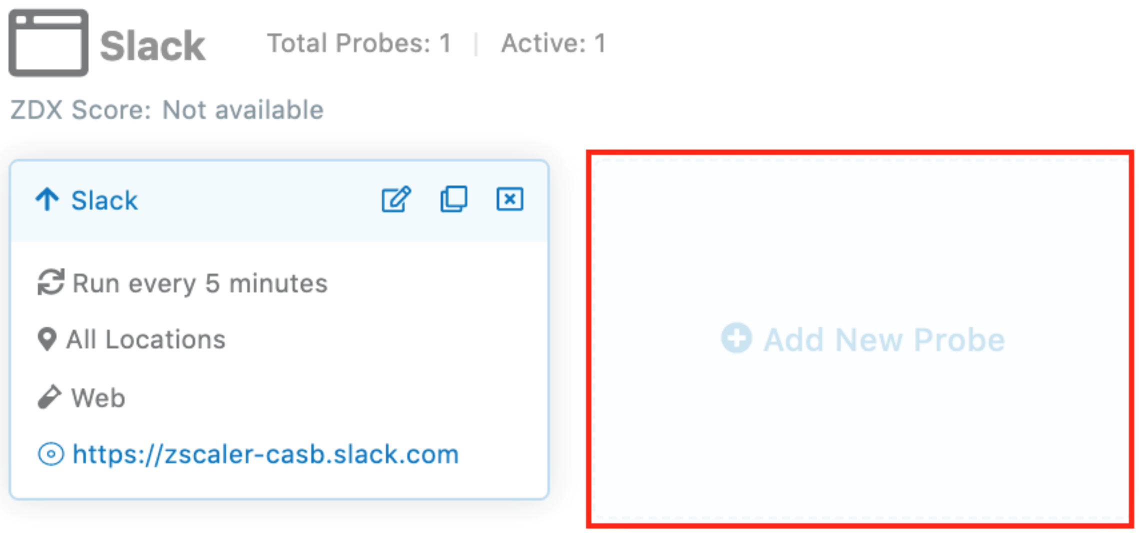
Users: Clear

Locations: Clear

Departments: Clear

Figure 51. Configuring the Web probe

The completed Web probe is displayed. Click Add New Probe. This displays the Probe Configuration wizard to create the Cloud Path probe to monitor the network.



Slack Total Probes: 1 | Active: 1

ZDX Score: Not available

Slack

Run every 5 minutes

All Locations

Web

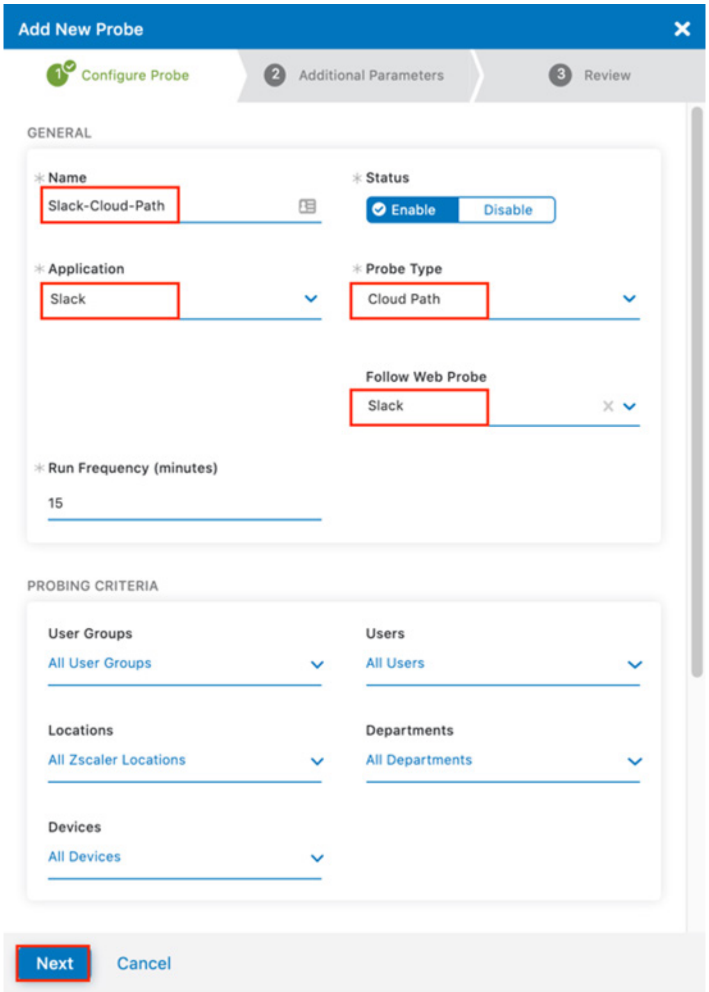
https://zscaler-casb.slack.com

Figure 52. The completed Web probe

Configure Probes for Slack Monitoring

To enable monitoring for the new probe:

1. Enter a **Name** for the probe.
2. Verify the probe is **Enabled**.
3. Select **Cloud Path** as the **Probe Type**.
4. For **Follow Web Probe**, select **Slack**.
5. Click **Next** to move to the probe detail.



Add New Probe

1 Configure Probe | 2 Additional Parameters | 3 Review

GENERAL

* Name: Slack-Cloud-Path

* Status: Enable | Disable

* Application: Slack

* Probe Type: Cloud Path

Follow Web Probe: Slack

* Run Frequency (minutes): 15

PROBING CRITERIA

User Groups: All User Groups

Users: All Users

Locations: All Zscaler Locations

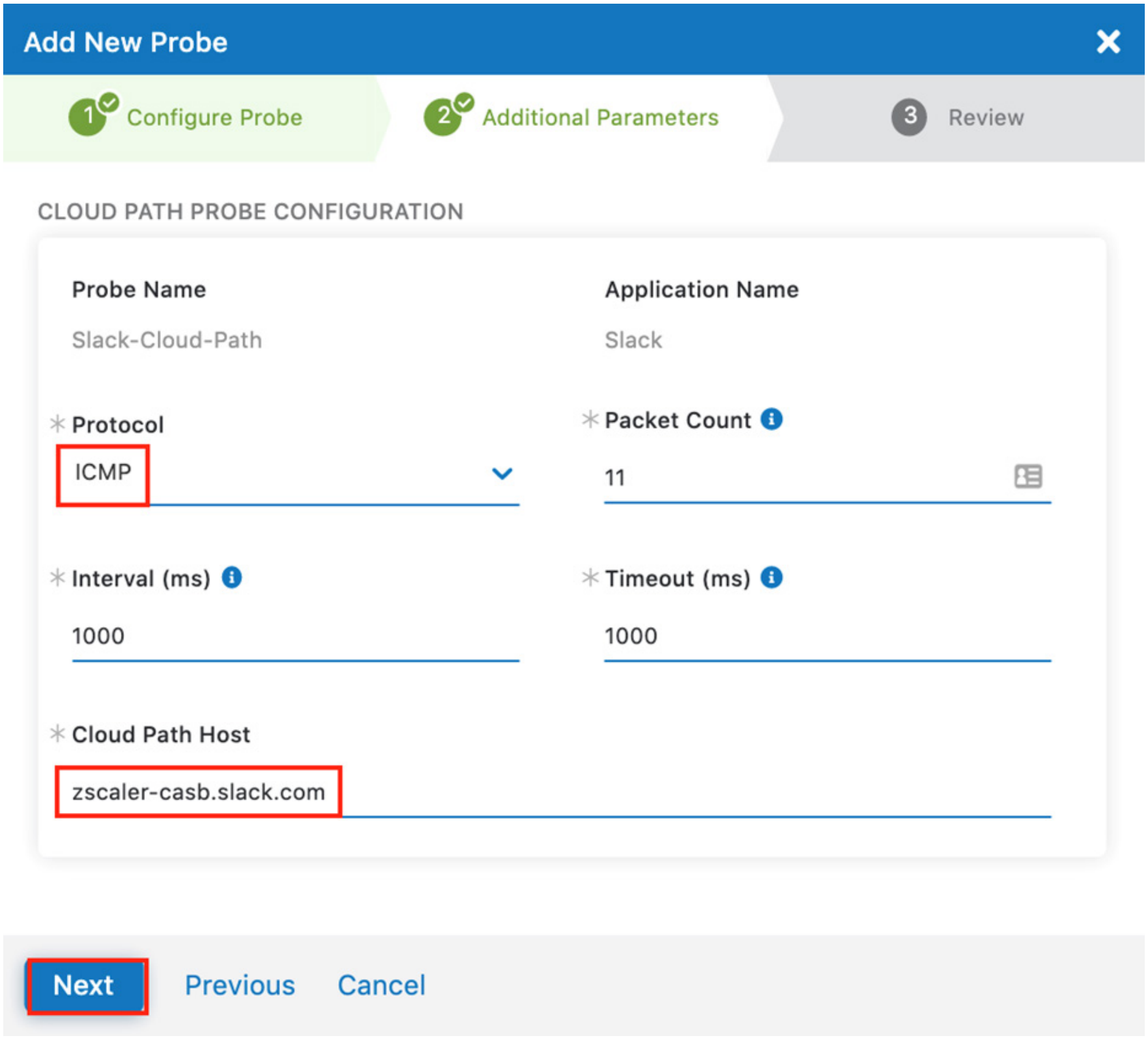
Departments: All Departments

Devices: All Devices

Next | Cancel

Figure 53. Create the Cloud Path probe

6. To enable Slack monitoring for the probe, select **ICMP** as the **Protocol**.
7. Enter the **Slack Instance URL** for your organization in the **Cloud Path Host** field.
8. Click **Next** to review the probe configuration.



CLOUD PATH PROBE CONFIGURATION

Probe Name: Slack-Cloud-Path

Application Name: Slack

* Protocol: ICMP

* Packet Count: 11

* Interval (ms): 1000

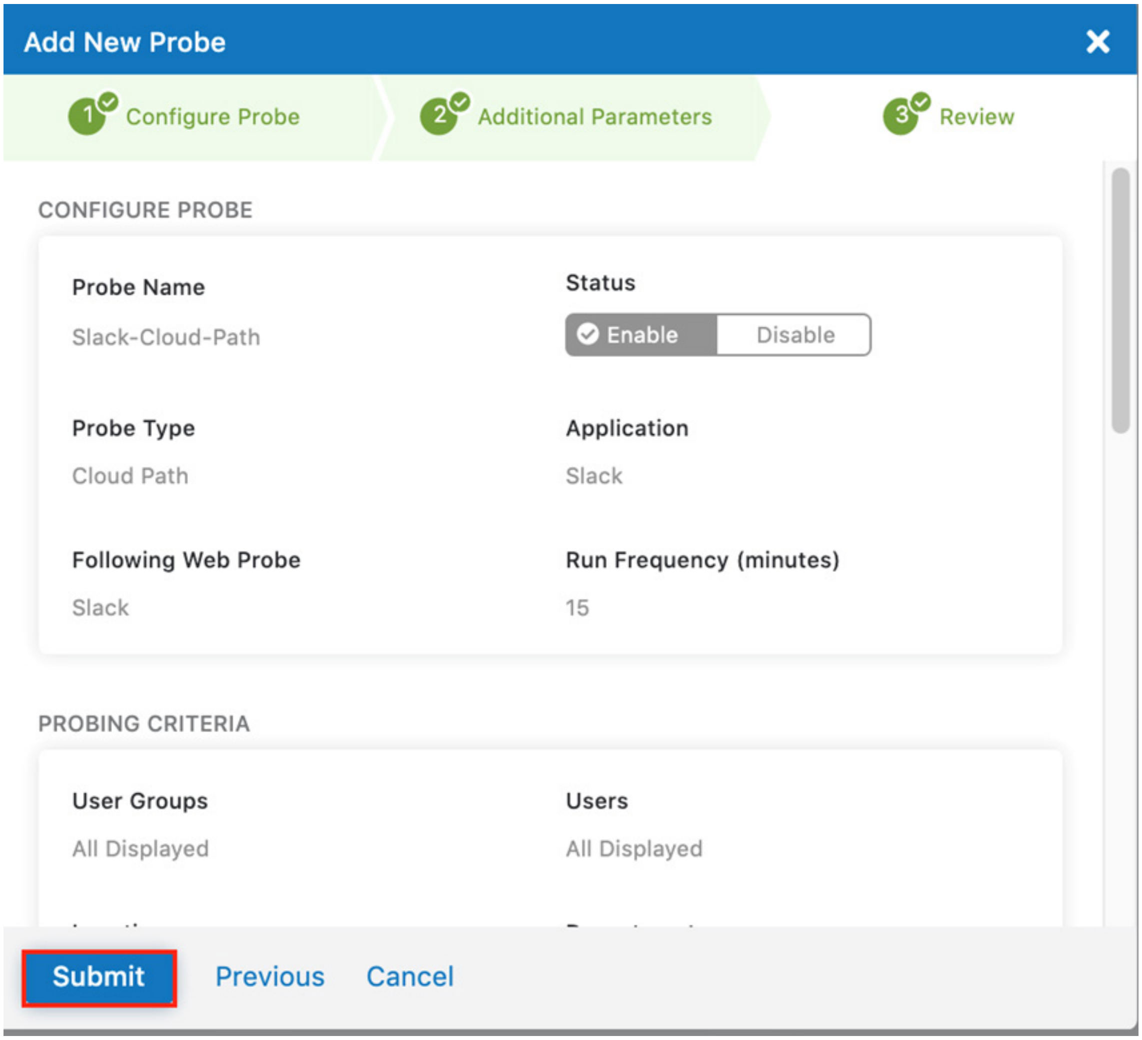
* Timeout (ms): 1000

* Cloud Path Host: zscaler-casb.slack.com

Figure 54. Create the Cloud Path probe

Configure ZDX Probes for Slack

Review the probe configuration and then click Submit to activate your probe.



CONFIGURE PROBE

Probe Name: Slack-Cloud-Path

Status: Enable | Disable

Probe Type: Cloud Path

Application: Slack

Following Web Probe: Slack

Run Frequency (minutes): 15

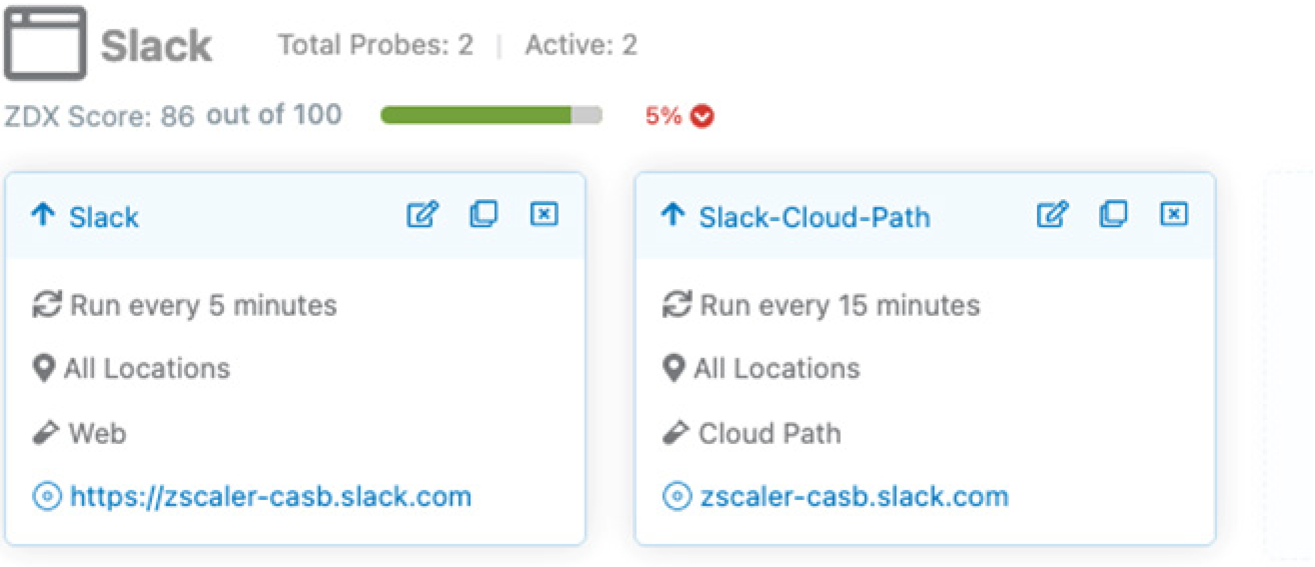
PROBING CRITERIA

User Groups: All Displayed

Users: All Displayed

Figure 55. The completed Cloud Path probe

The completed Slack probes are displayed. Activate the changes to enable the probes.



Slack Total Probes: 2 | Active: 2

ZDX Score: 86 out of 100 5%

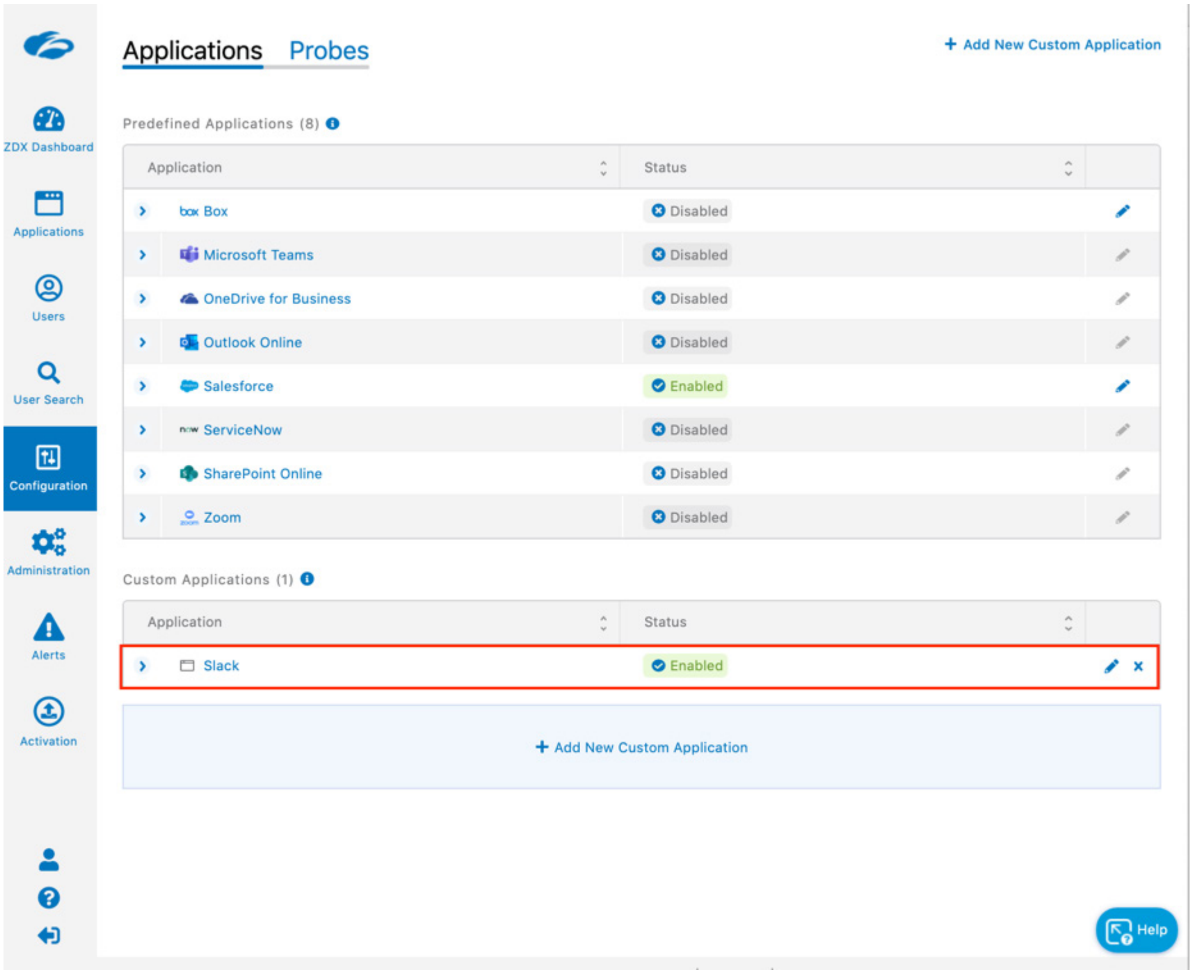
Slack
Run every 5 minutes
All Locations
Web
https://zscaler-casb.slack.com

Slack-Cloud-Path
Run every 15 minutes
All Locations
Cloud Path
zscaler-casb.slack.com

Figure 56. ZDX probes monitoring for Slack

The ZDX-Enabled Slack Application

The Slack application monitoring is activated and the probes begin monitoring users using the Zscaler Client Connector. The figure shows the Zscaler Client Connector running the ZDX and the cloud service is enabled and active.



Predefined Applications (8)

Application	Status
Box	Disabled
Microsoft Teams	Disabled
OneDrive for Business	Disabled
Outlook Online	Disabled
Salesforce	Enabled
ServiceNow	Disabled
SharePoint Online	Disabled
Zoom	Disabled

Custom Applications (1)

Application	Status
Slack	Enabled

+ Add New Custom Application

Figure 57. Active Slack monitoring

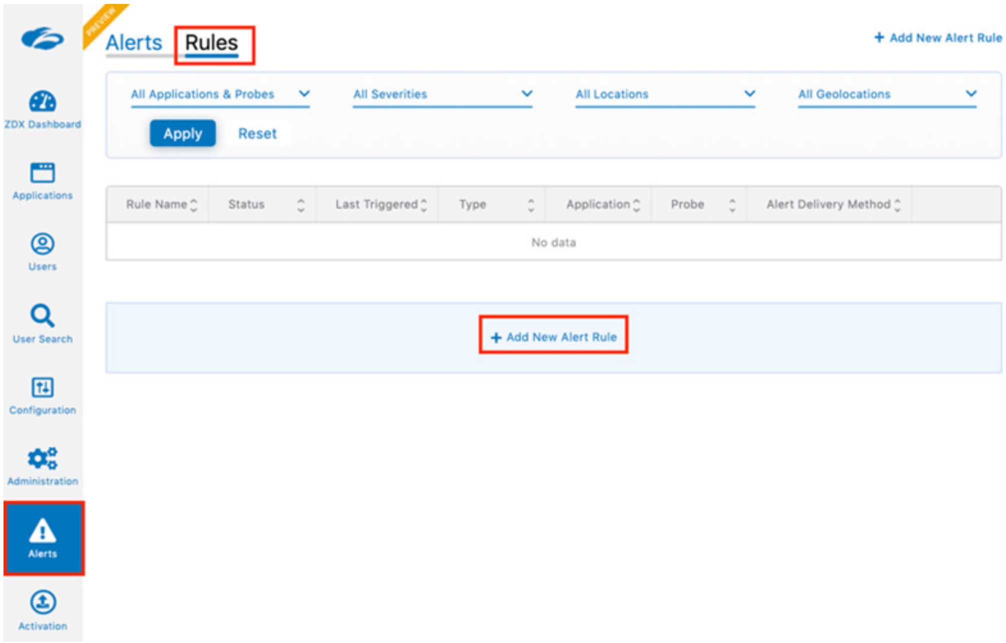
Create an Alert for the Slack Service

As a final configuration step, create an alert to email when there is service degradation of the Slack application. You can create an alert for network, application, or device thresholds. Create an alert rule with any of the following information:

- Network Probe. Latency, MTR, Packet Loss, Number of Hops
- Application Probe. DNS Response Time, Page Fetch Time, Server Response Time, Web Request Availability
- Device Monitor. CPU Usage, Bandwidth, Battery, CPU, Disk, Wi-Fi Signal Strength, Memory, Sent and Received Mbps

To create the alert on page fetch times:

1. Select **Alerts**.
2. Select **Rules**.
3. Select **Add New Alert Rule**.



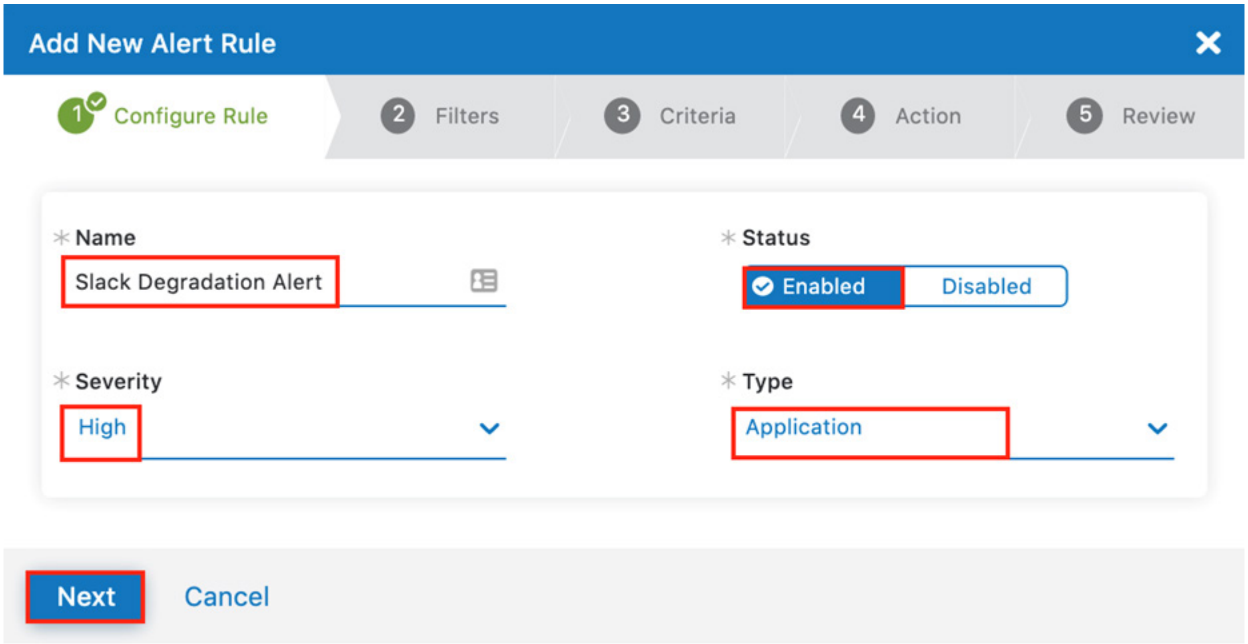
Rule Name	Status	Last Triggered	Type	Application	Probe	Alert Delivery Method
No data						

Figure 58. Creating an alert

Create an Alert for the Slack Service

Step one of the Add New Alert Rule wizard:

1. **Name** the Rule.
2. Select **Enable** under **Status**.
3. Give the alert an appropriate **Severity**.
4. Select **Application** under **Type**.
5. Click **Next**.



Name: Slack Degradation Alert

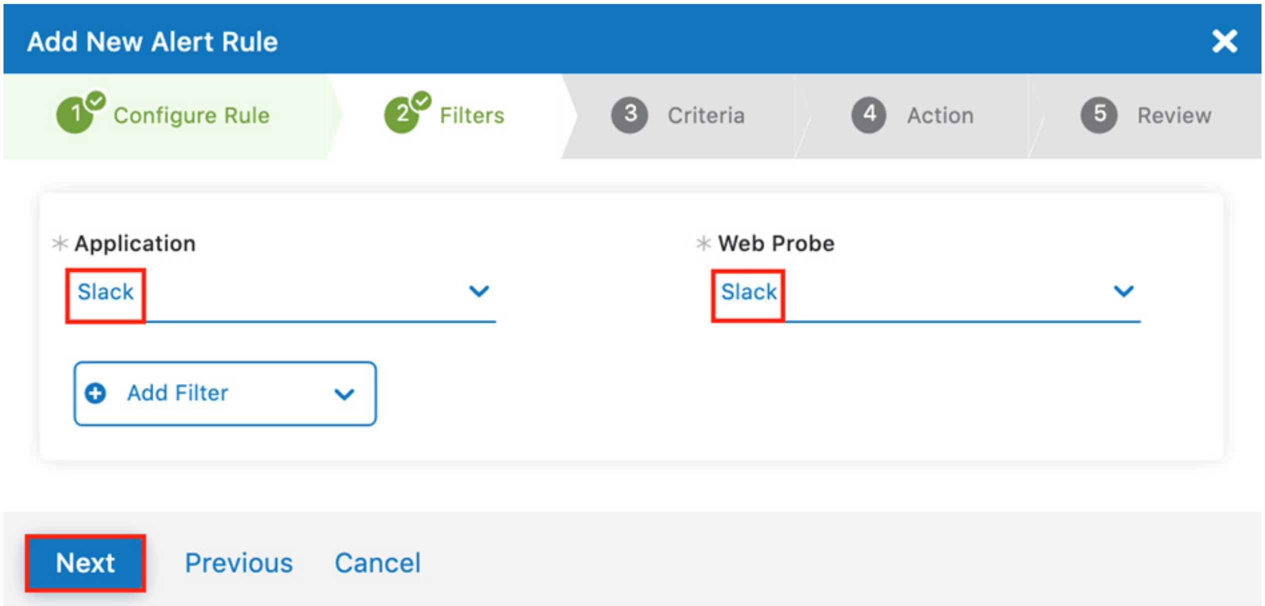
Status: Enabled | Disabled

Severity: High

Type: Application

Figure 59. The alert creation wizard, step one

6. Select **Slack** as the **Application**.
7. Select **Slack** as the **Web Probe**.
8. Click **Next**.

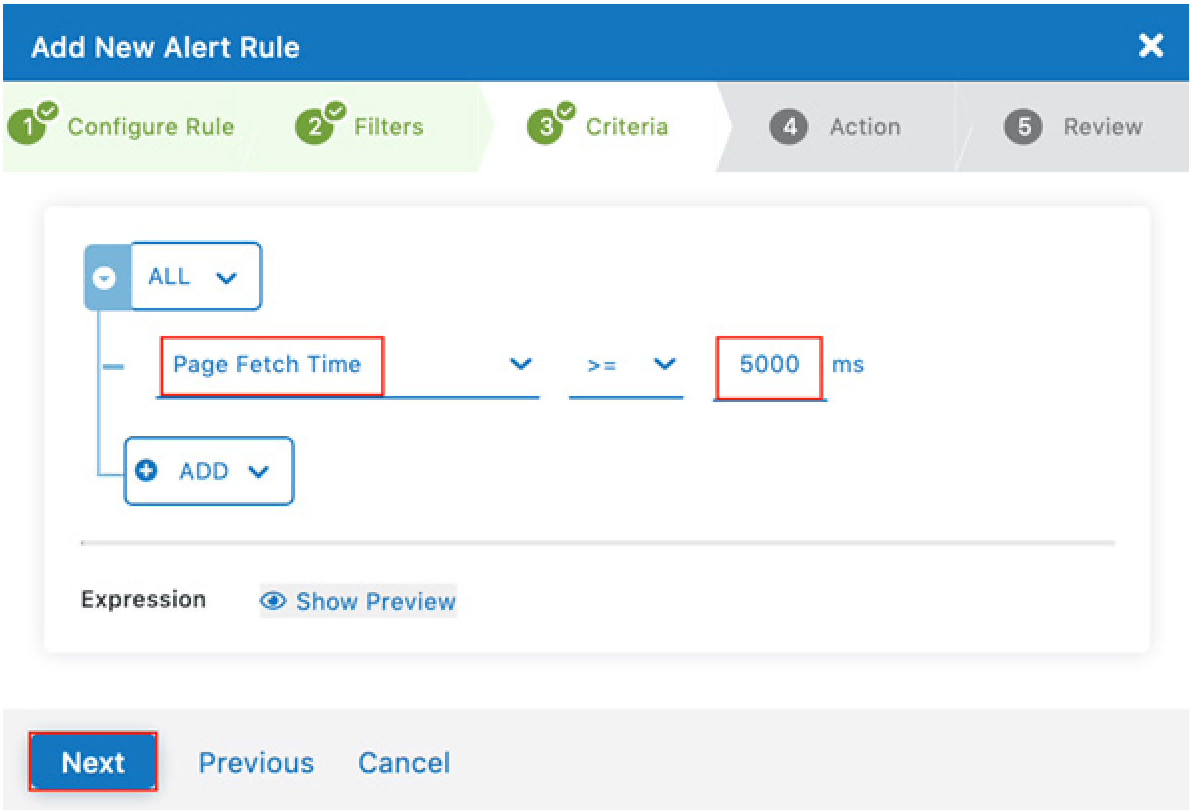


* Application: Slack

* Web Probe: Slack

Figure 60. The alert creation wizard, step two

9. Step three of the **Add New Alert Rule** wizard creates the threshold that is triggered the if exceeded. Use multiple variables to eliminate a false positive:
   a. Select **Page Fetch Time**.
   b. Select the time to exceed 5000ms (5 seconds).
   c. Click **Next**.



Add New Alert Rule

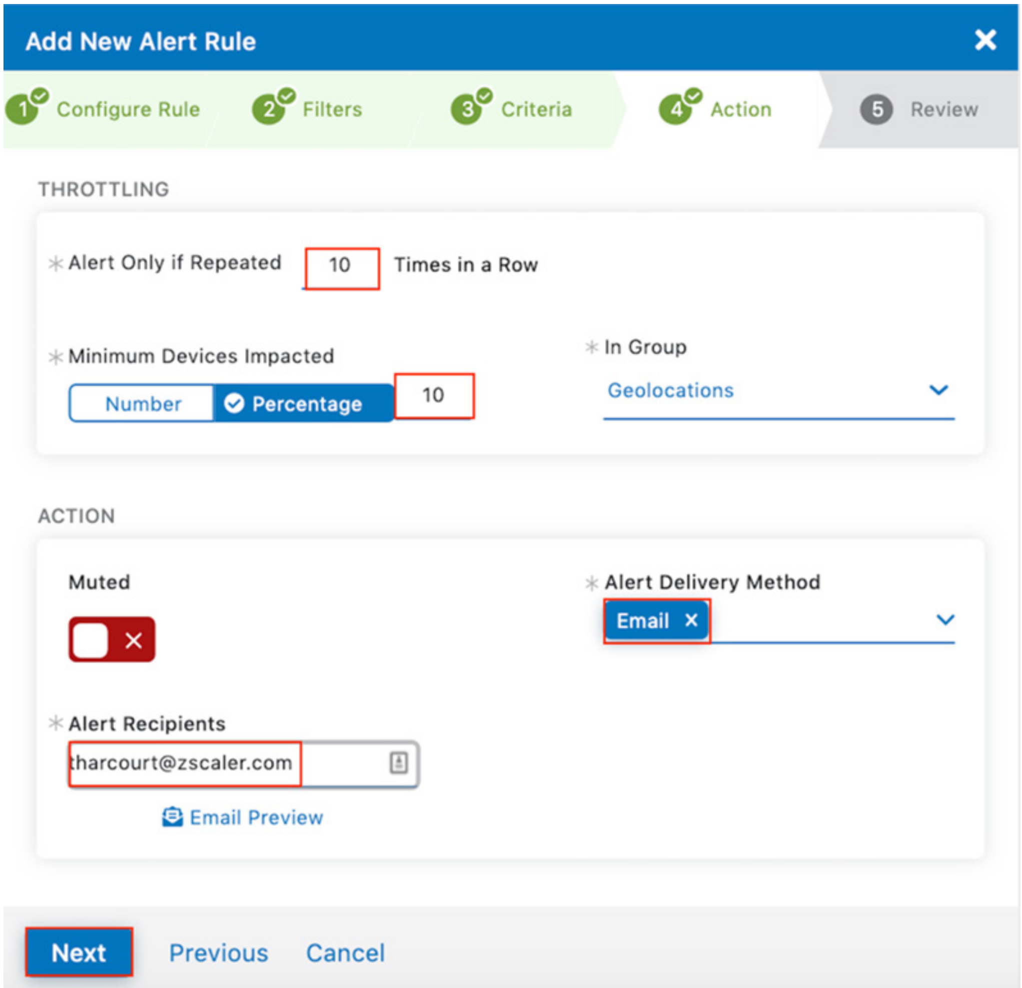
1 Configure Rule · 2 Filters · 3 Criteria · 4 Action · 5 Review

ALL

Page Fetch Time >= 5000 ms

Figure 61. The alert creation wizard, step three

10. Step four of the Add New Alert Rule wizard adds throttling to control the scope of the alert, and defines the action. You can define the action as an authenticated webhook to send the alert to a Slack channel:
    a. Enter `10` for the number of times the probe time must exceed the threshold.
    b. Enter `10` and select **Percentage** for the **Minimum Devices Impacted**.
    c. Select **Email** as the **Delivery Method**.
    d. Enter the **Alert Recipients** email address (or multiple addresses separated by commas).



THROTTLING

* Alert Only if Repeated 10 Times in a Row

* Minimum Devices Impacted: Number / ● Percentage 10

* In Group: Geolocations

ACTION

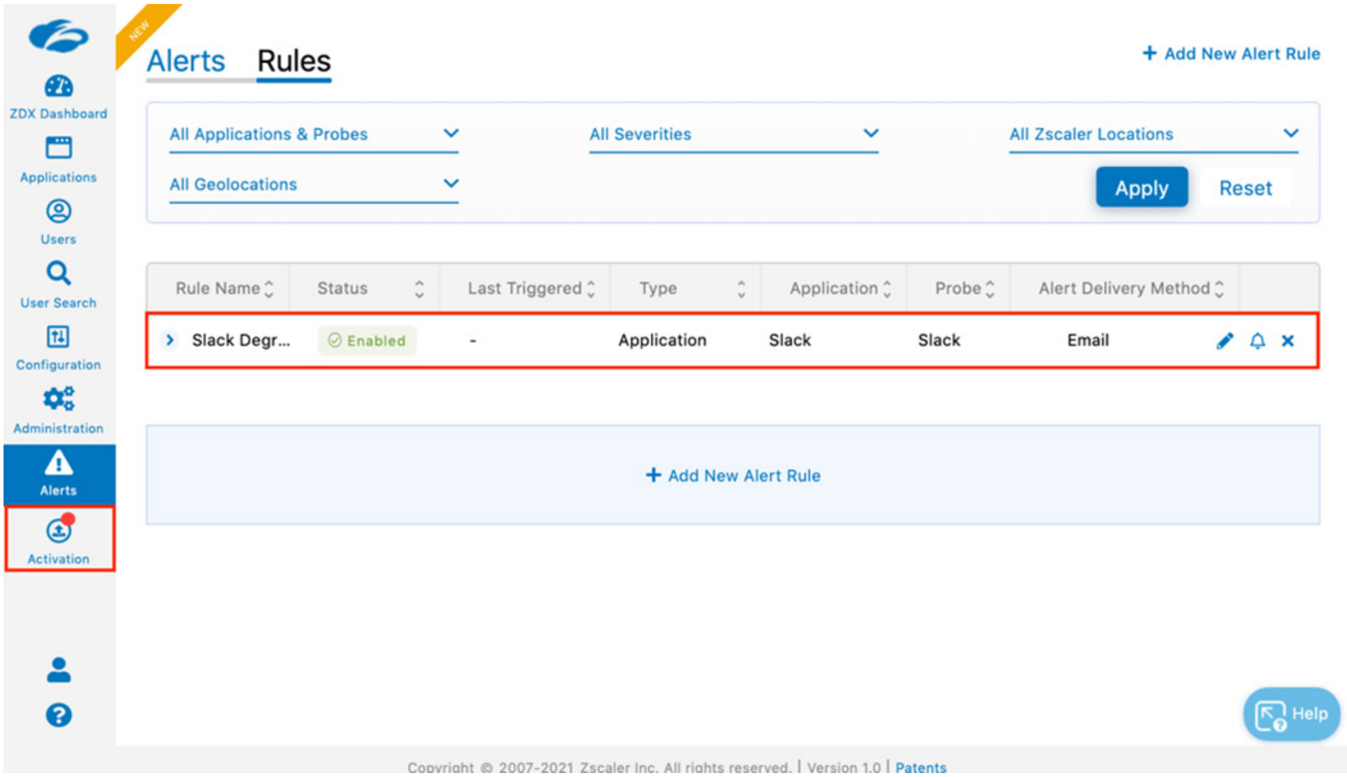
Muted: ✕

* Alert Delivery Method: Email ✕

* Alert Recipients: tharcourt@zscaler.com

Figure 62. The alert creation wizard, step four

The completed rule set for the alert is displayed. Activate the configuration.



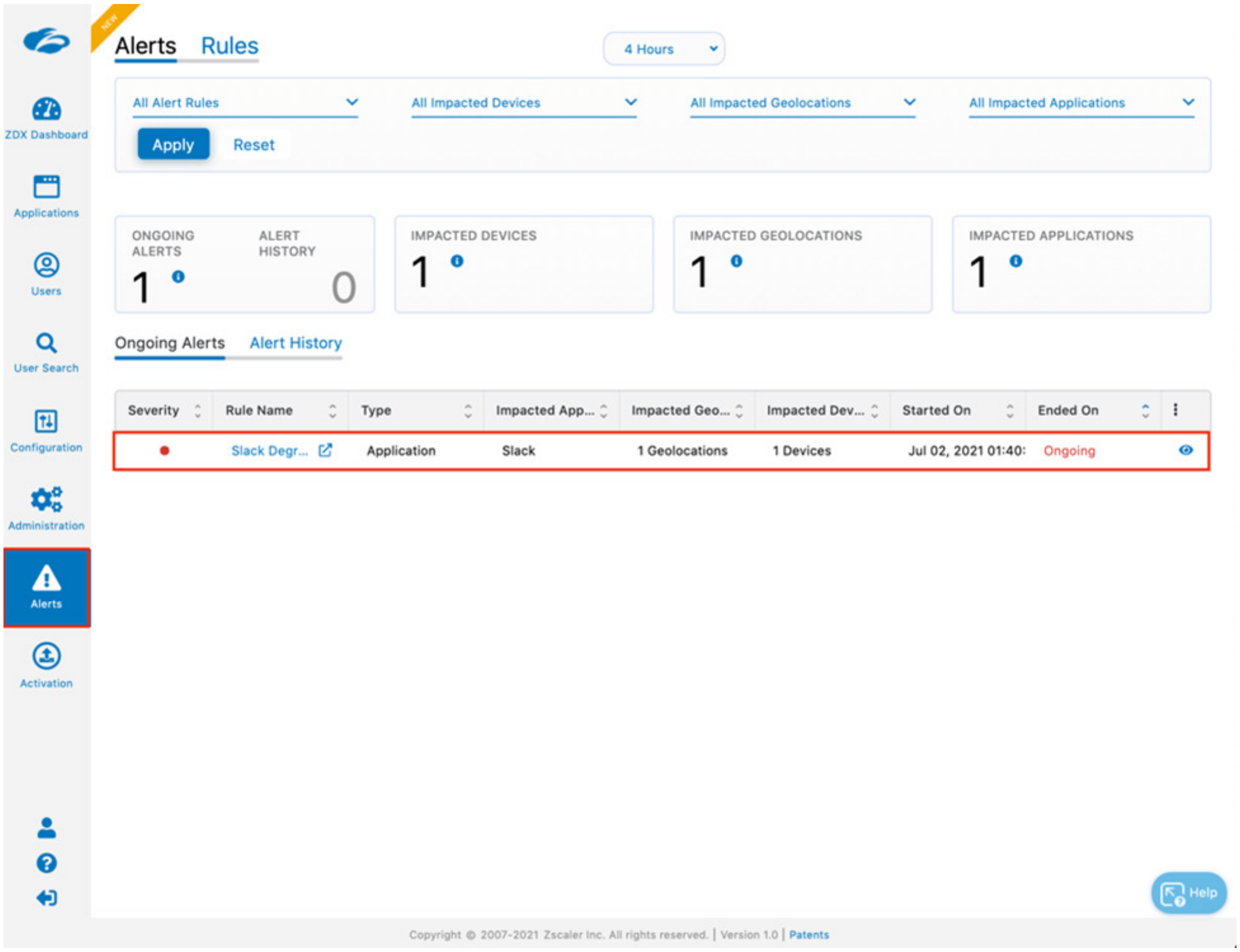
Rule Name	Status	Last Triggered	Type	Application	Probe	Alert Delivery Method
Slack Degr...	Enabled	-	Application	Slack	Slack	Email

Figure 63. *The completed alert rule set*

The Triggered Alert for the Slack Service

The Alerts tab shows the triggered alert generated by the exceeded threshold settings in the rule set. You can click the Rule Name or click the View icon to see more detail about the alert.

1. Select **Alerts**.
2. Select the **Rule Name**.



ONGOING ALERTS 1 | ALERT HISTORY 0 | IMPACTED DEVICES 1 | IMPACTED GEOLOCATIONS 1 | IMPACTED APPLICATIONS 1

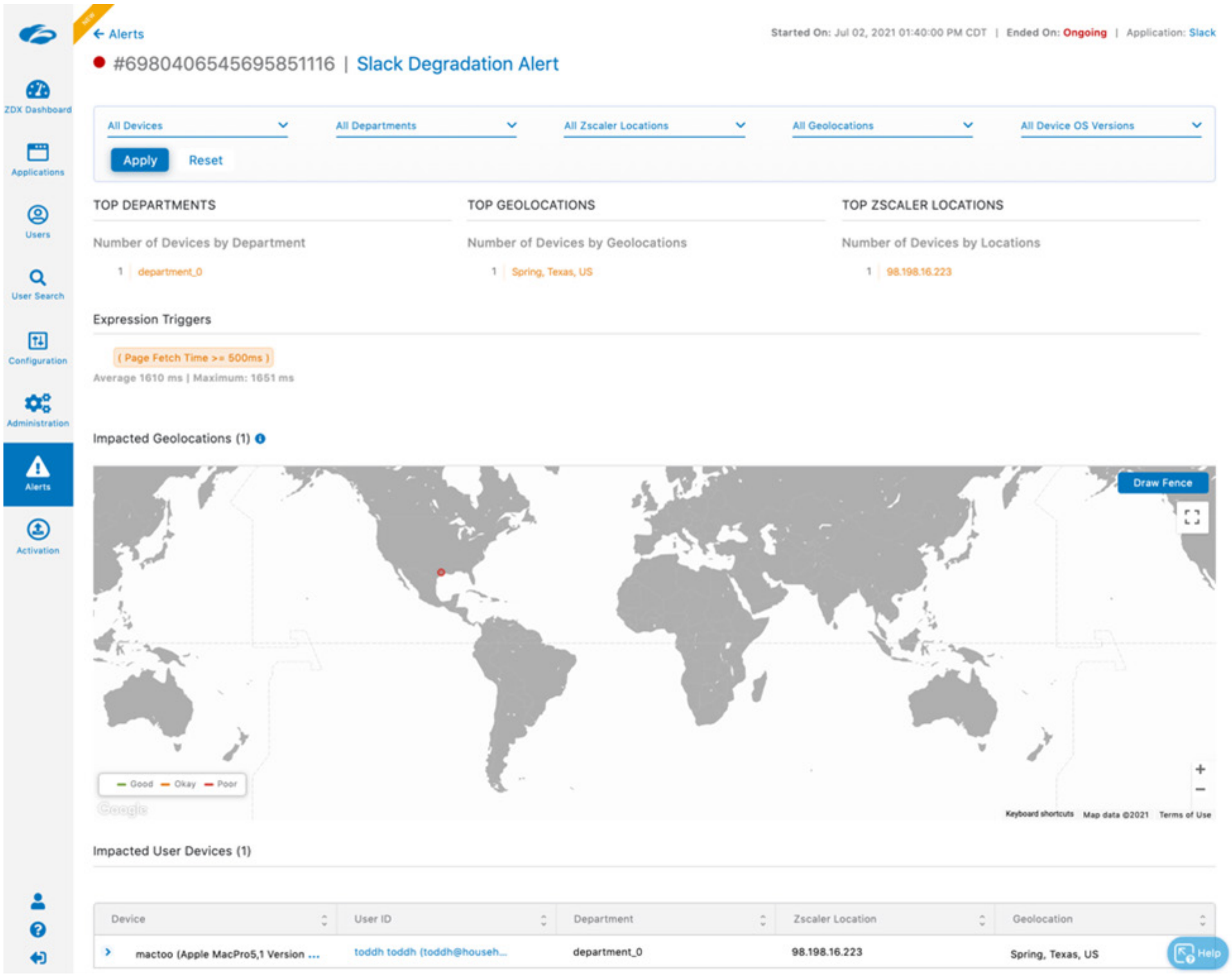
Severity	Rule Name	Type	Impacted App...	Impacted Geo...	Impacted Dev...	Started On	Ended On
●	Slack Degr...	Application	Slack	1 Geolocations	1 Devices	Jul 02, 2021 01:40:	Ongoing

Copyright © 2007-2021 Zscaler Inc. All rights reserved. | Version 1.0 | Patents

Figure 64. The alert

Alert Detail for the Slack Service

The Alerts window displays the alert detail for the triggered Slack alert showing impacted user and devices, impact location, and threshold details.



← Alerts

Started On: Jul 02, 2021 01:40:00 PM CDT | Ended On: Ongoing | Application: Slack

● #698040654569585116 | Slack Degradation Alert

TOP DEPARTMENTS

Number of Devices by Department

1 | department_0

TOP GEOLOCATIONS

Number of Devices by Geolocations

1 | Spring, Texas, US

TOP ZSCALER LOCATIONS

Number of Devices by Locations

1 | 98.198.16.223

Expression Triggers

(Page Fetch Time >= 500ms)

Average 1610 ms | Maximum: 1651 ms

Impacted Geolocations (1)

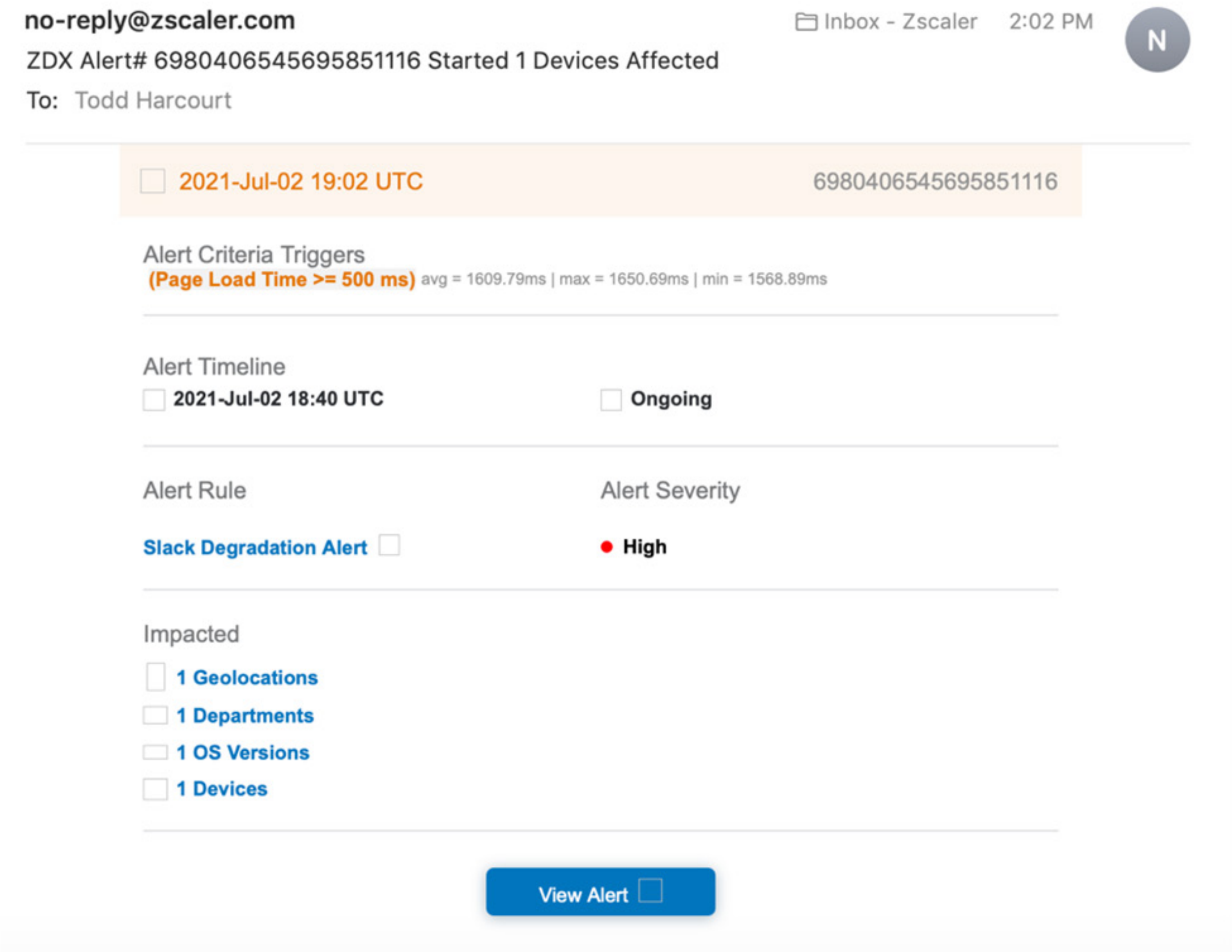
Impacted User Devices (1)

Device	User ID	Department	Zscaler Location	Geolocation
› mactoo (Apple MacPro5,1 Version ...	toddh toddh (toddh@househ...	department_0	98.198.16.223	Spring, Texas, US

Figure 65. Alert details

The Sent Alert Email for the Slack Service

The following is an example of the email alert that was sent to the recipients after the threshold was exceeded. Another email is sent when the threshold returns to normal values if the alert was an ongoing or continuous alert.



no-reply@zscaler.com

Inbox - Zscaler 2:02 PM

ZDX Alert# 6980406545695851116 Started 1 Devices Affected

To: Todd Harcourt

□ 2021-Jul-02 19:02 UTC 6980406545695851116

Alert Criteria Triggers

(Page Load Time >= 500 ms) avg = 1609.79ms | max = 1650.69ms | min = 1568.89ms

Alert Timeline

□ **2021-Jul-02 18:40 UTC** □ **Ongoing**

Alert Rule: **Slack Degradation Alert** □

Alert Severity: ● **High**

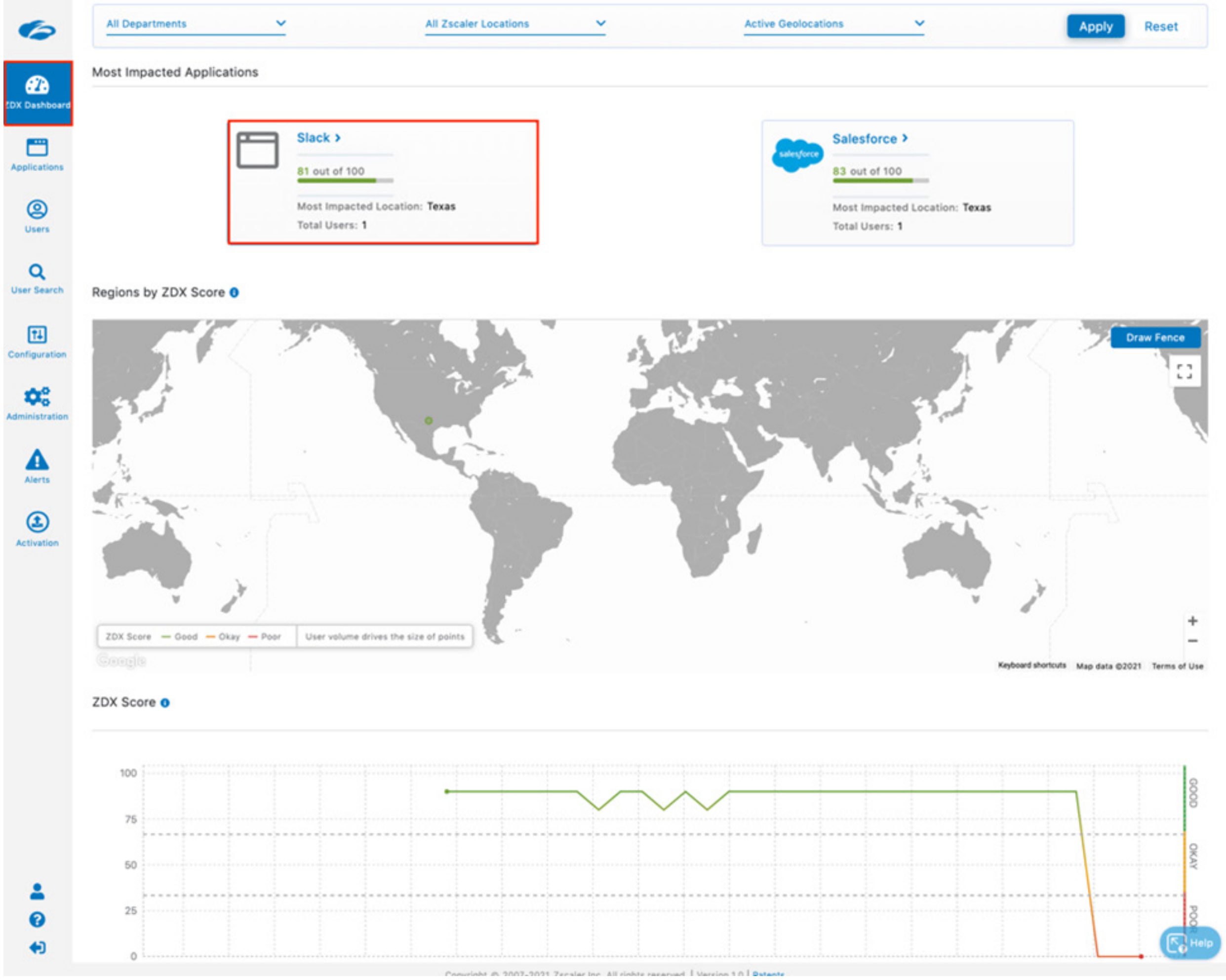
Impacted

- □ **1 Geolocations**
- □ **1 Departments**
- □ **1 OS Versions**
- □ **1 Devices**

Figure 66. The alert email

Using the ZDX Dashboard

The ZDX dashboard provides a single page to monitor the user experience (ZDX Score) of all users and all applications. An active heat map also shows you any locations globally that might have issues.



Slack >
81 out of 100
Most Impacted Location: Texas
Total Users: 1

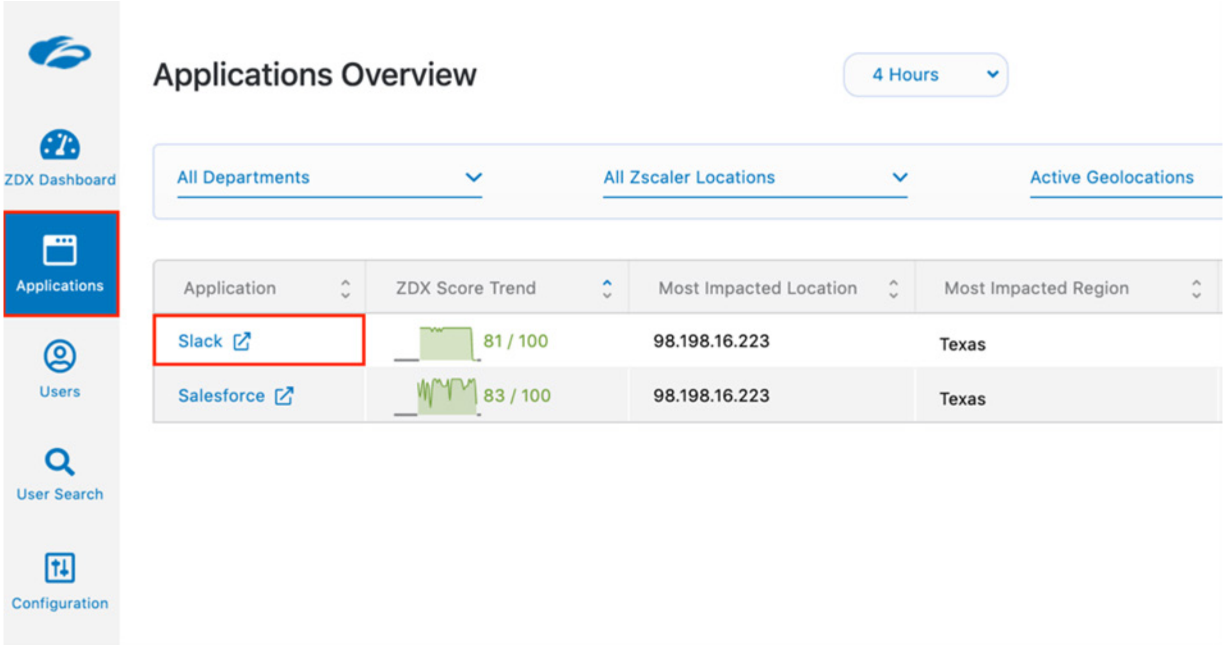
Salesforce >
83 out of 100
Most Impacted Location: Texas
Total Users: 1

Figure 67. The ZDX Dashboard

Application Overview and Performance Detail

Selecting Application on the left-side navigation of the ZDX Admin Portal displays the Applications Overview, which shows all the configured applications and the individual ZDX Score.

1. Select **Applications**.
2. Select the **Slack** application.



Application	ZDX Score Trend	Most Impacted Location	Most Impacted Region
Slack	81 / 100	98.198.16.223	Texas
Salesforce	83 / 100	98.198.16.223	Texas

Figure 68. Application overview

Slack Application Performance Detail

The top portion of the application detail shows a historical view of the ZDX Score Over Time and the Page Fetch Time. The failure of the page fetch time indicates a service loss of the Slack service itself.

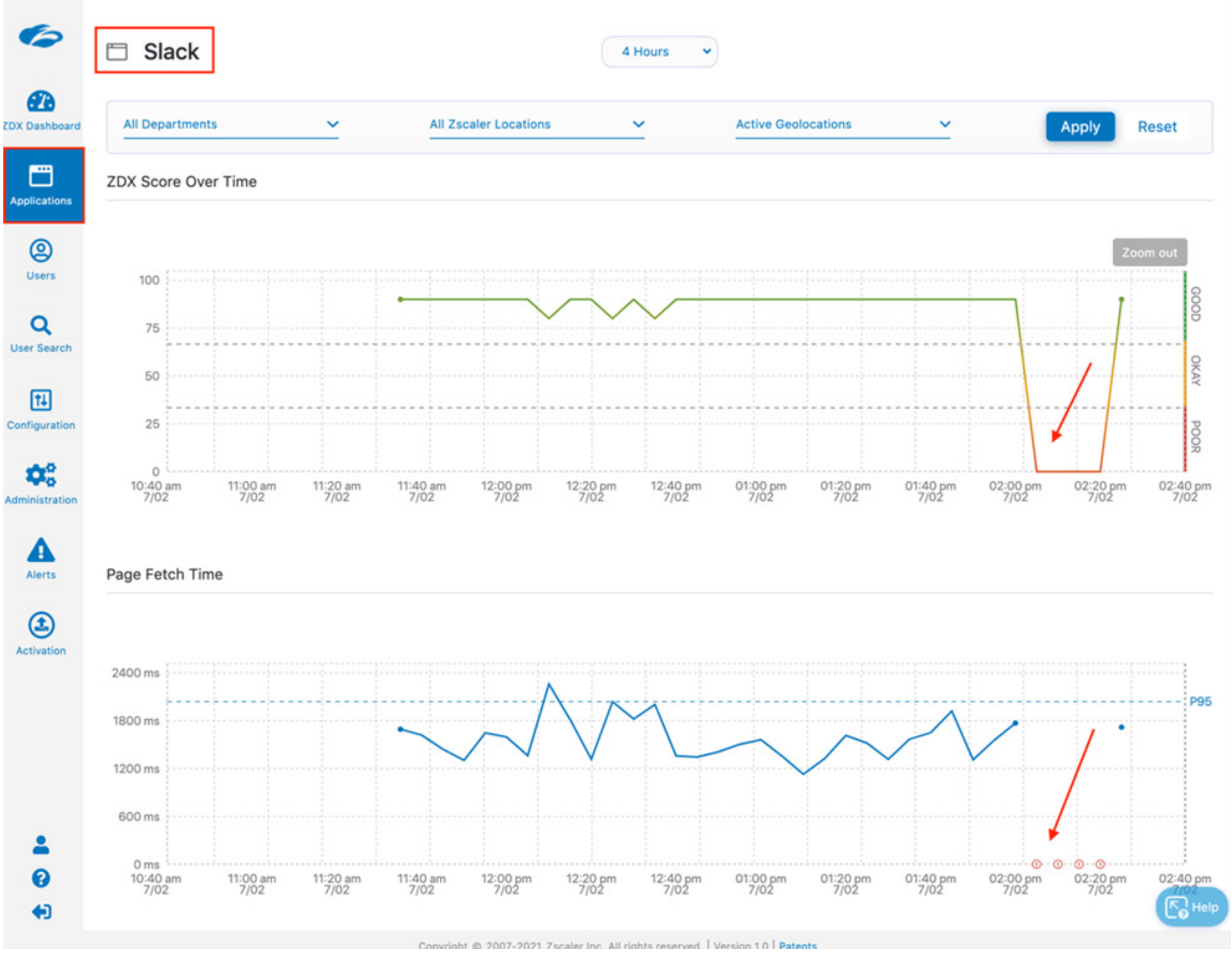
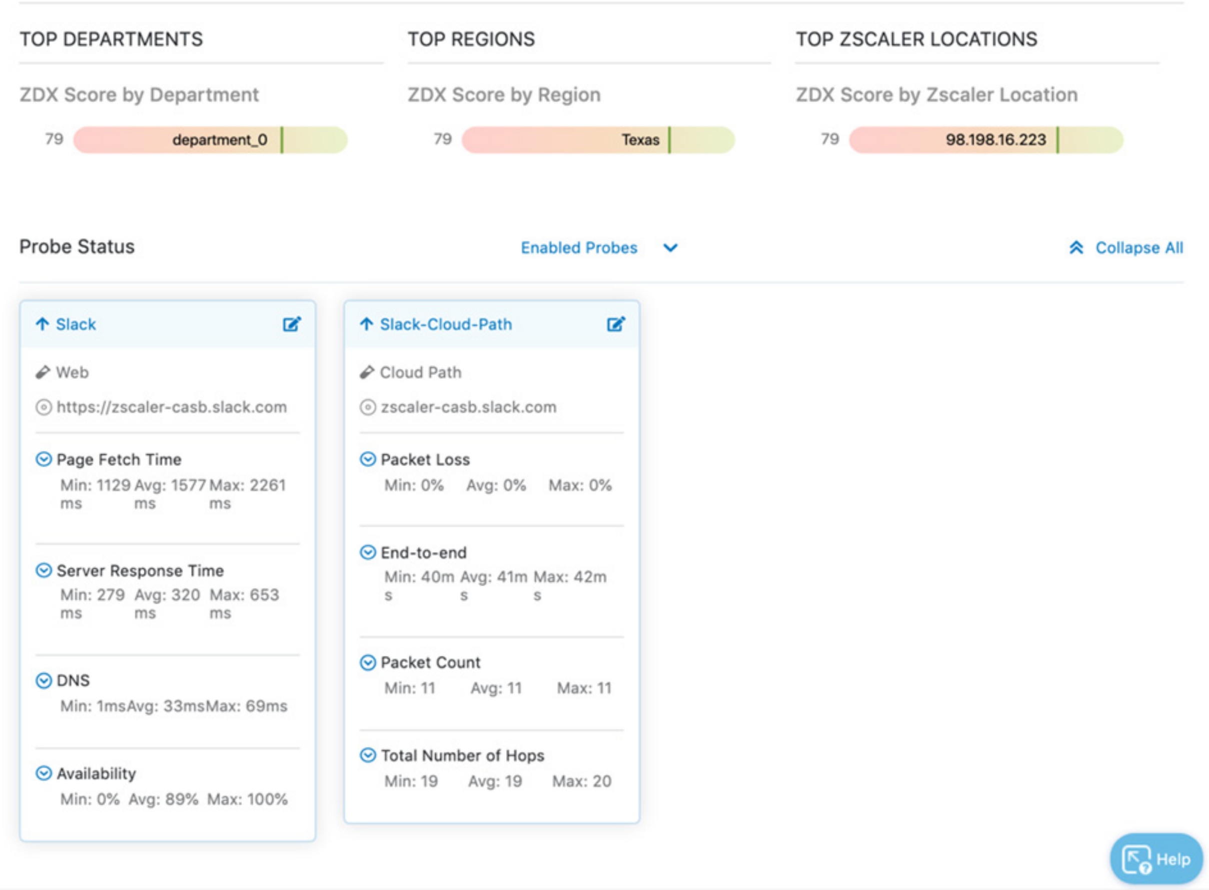


Figure 69. Application performance detail

The bottom portion of the application detail shows the Top Departments, Top Regions, and Top Zscaler Locations using the application and the ZDX scores at a glance. You also see probe data, with minimum, average, and maximum response times.



TOP DEPARTMENTS

ZDX Score by Department

79 department_0

TOP REGIONS

ZDX Score by Region

79 Texas

TOP ZSCALER LOCATIONS

ZDX Score by Zscaler Location

79 98.198.16.223

Probe Status

Slack

Web

https://zscaler-casb.slack.com

Page Fetch Time
Min: 1129 ms Avg: 1577 ms Max: 2261 ms

Server Response Time
Min: 279 ms Avg: 320 ms Max: 653 ms

DNS
Min: 1ms Avg: 33ms Max: 69ms

Availability
Min: 0% Avg: 89% Max: 100%

Slack-Cloud-Path

Cloud Path

zscaler-casb.slack.com

Packet Loss
Min: 0% Avg: 0% Max: 0%

End-to-end
Min: 40ms Avg: 41ms Max: 42ms

Packet Count
Min: 11 Avg: 11 Max: 11

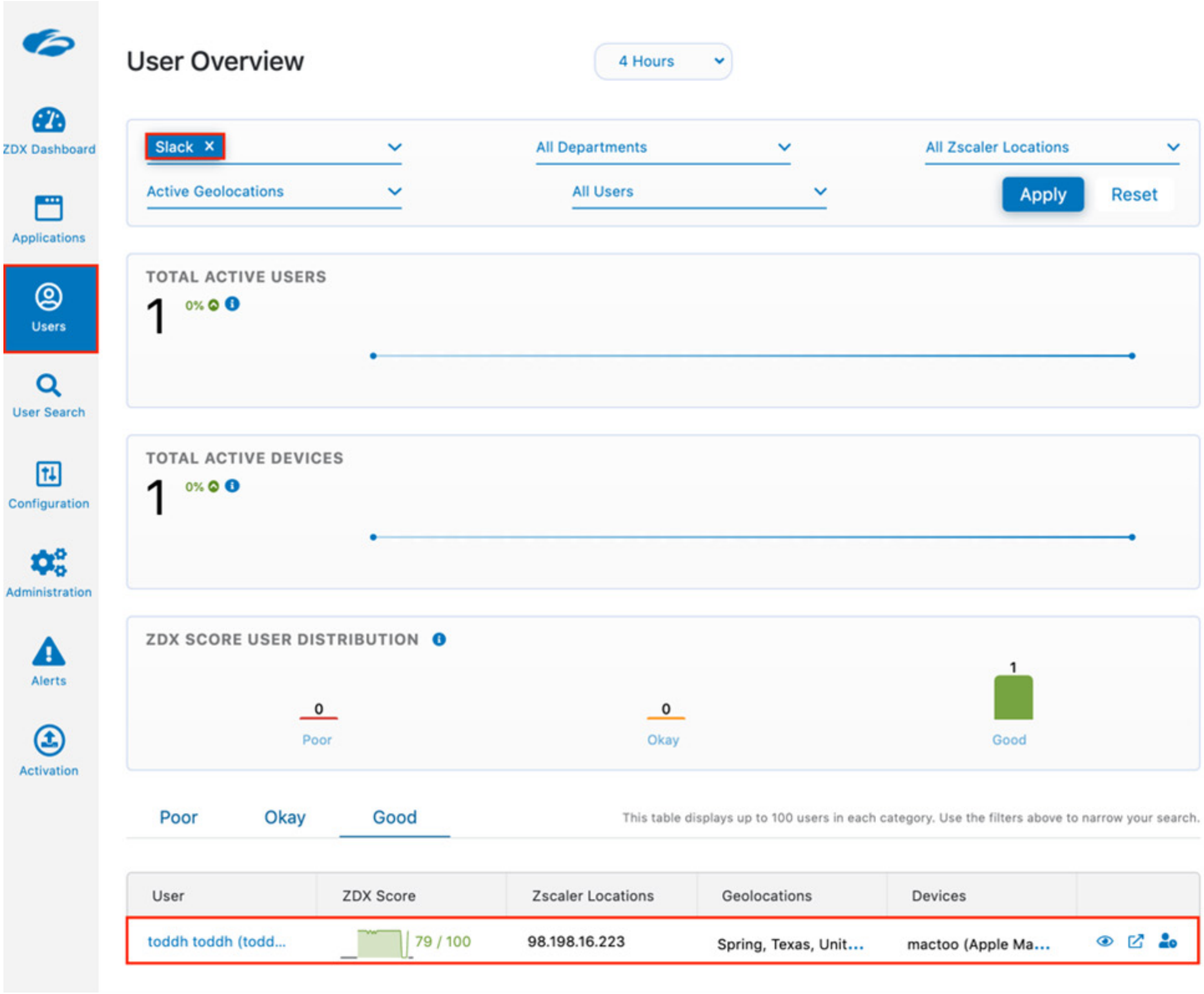
Total Number of Hops
Min: 19 Avg: 19 Max: 20

Figure 70. Application performance detail

User Overview and Detail

The User Overview provides all the users of an application. Select Slack and then Apply to see all Slack users. The ZDX score is provided, and you can select users by Poor, Okay, or a Good ZDX Score. You can get more detail on the user by clicking the name or the View icon on the right. Select a User to display more detail.

1. Select **Users**.
2. Select the **Slack** application.
3. Click **Apply**.



This table displays up to 100 users in each category. Use the filters above to narrow your search.

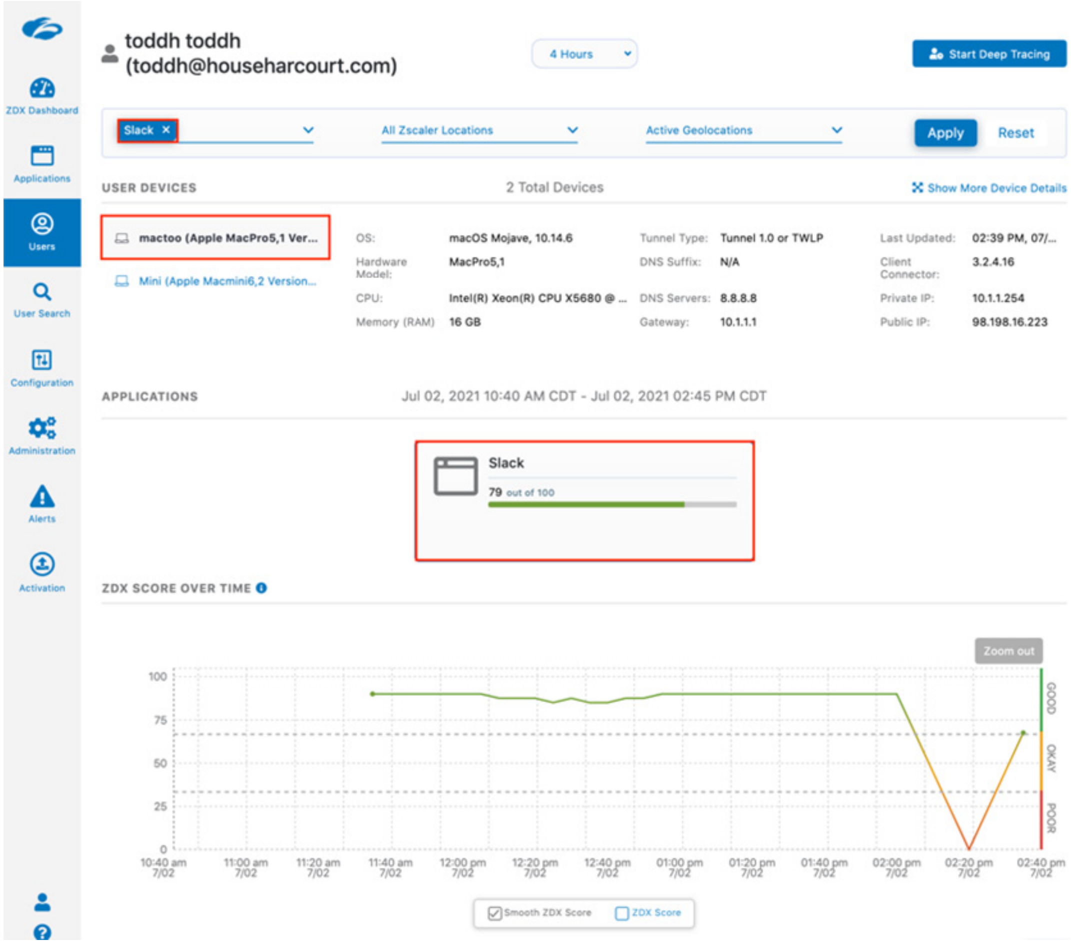
User	ZDX Score	Zscaler Locations	Geolocations	Devices
toddh toddh (todd...	79 / 100	98.198.16.223	Spring, Texas, Unit...	mactoo (Apple Ma...

Figure 71. User overview

Slack User Detail

The User Detail shows data to help isolate any user experience issues. Select and apply the Slack application to see the detail of the user experience for the Slack app. This report displays the user’s devices and provides the device-specific detail (OS, Device Type, Network Information, etc.) by clicking the device. From this page, you can see the ZDX Score in a timeline, and details of Page Fetch Times, Server Response, DNS Response, Probe Detail, and Device Health.

Select the User Device.



toddh toddh (toddh@househarcourt.com)

USER DEVICES — 2 Total Devices

- mactoo (Apple MacPro5,1 Ver...
- Mini (Apple Macmini6,2 Version...

OS:	macOS Mojave, 10.14.6	Tunnel Type:	Tunnel 1.0 or TWLP	Last Updated:	02:39 PM, 07/...
Hardware Model:	MacPro5,1	DNS Suffix:	N/A	Client Connector:	3.2.4.16
CPU:	Intel(R) Xeon(R) CPU X5680 @ ...	DNS Servers:	8.8.8.8	Private IP:	10.1.1.254
Memory (RAM)	16 GB	Gateway:	10.1.1.1	Public IP:	98.198.16.223

APPLICATIONS — Jul 02, 2021 10:40 AM CDT - Jul 02, 2021 02:45 PM CDT

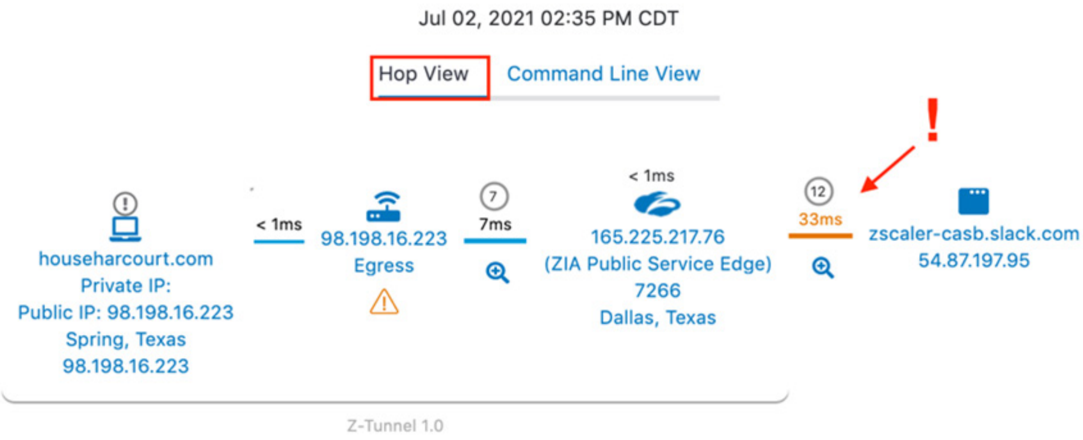
Slack — 79 out of 100

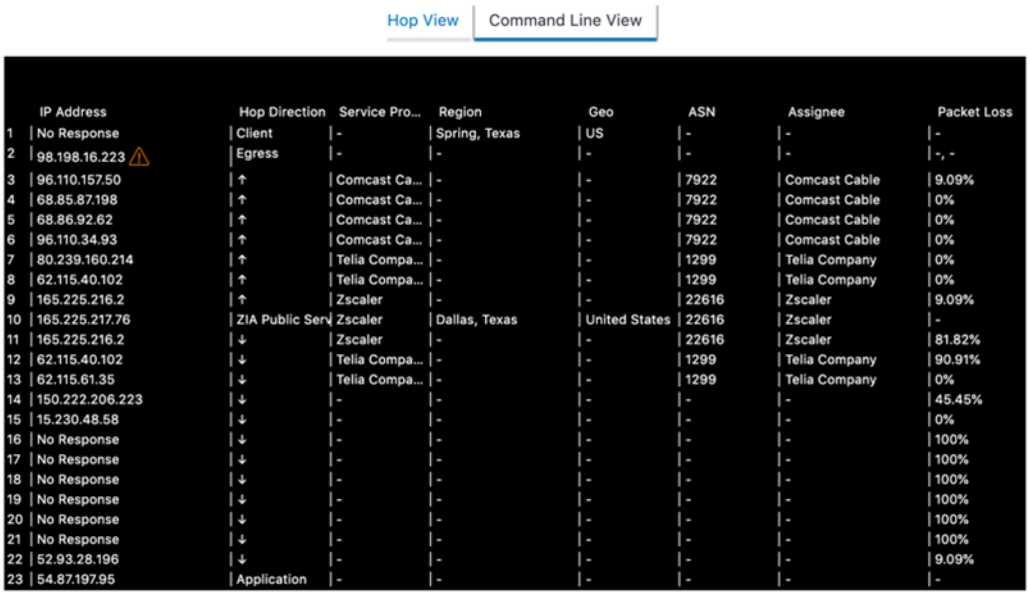
ZDX SCORE OVER TIME

Figure 72. User detail

User Detail

If there is any issue from the users' device health, the network at the home office, any Service Provider in the path, or an issue with Zscaler, or Slack itself, ZDX provides the visibility of the cloud to the Zscaler administrators from any of their users' individual environments.





	IP Address	Hop Direction	Service Pro...	Region	Geo	ASN	Assignee	Packet Loss
1	No Response	Client	-	Spring, Texas	US	-	-	-
2	98.198.16.223 ⚠	Egress	-	-	-	-	-	-, -
3	96.110.157.50	↑	Comcast Ca...	-	-	7922	Comcast Cable	9.09%
4	68.85.87.198	↑	Comcast Ca...	-	-	7922	Comcast Cable	0%
5	68.86.92.62	↑	Comcast Ca...	-	-	7922	Comcast Cable	0%
6	96.110.34.93	↑	Comcast Ca...	-	-	7922	Comcast Cable	0%
7	80.239.160.214	↑	Telia Compa...	-	-	1299	Telia Company	0%
8	62.115.40.102	↑	Telia Compa...	-	-	1299	Telia Company	0%
9	165.225.216.2	↑	Zscaler	-	-	22616	Zscaler	9.09%
10	165.225.217.76	ZIA Public Serv	Zscaler	Dallas, Texas	United States	22616	Zscaler	-
11	165.225.216.2	↓	Zscaler	-	-	22616	Zscaler	81.82%
12	62.115.40.102	↓	Telia Compa...	-	-	1299	Telia Company	90.91%
13	62.115.61.35	↓	Telia Compa...	-	-	1299	Telia Company	0%
14	150.222.206.223	↓	-	-	-	-	-	45.45%
15	15.230.48.58	↓	-	-	-	-	-	0%
16	No Response	↓	-	-	-	-	-	100%
17	No Response	↓	-	-	-	-	-	100%
18	No Response	↓	-	-	-	-	-	100%
19	No Response	↓	-	-	-	-	-	100%
20	No Response	↓	-	-	-	-	-	100%
21	No Response	↓	-	-	-	-	-	100%
22	52.93.28.196	↓	-	-	-	-	-	9.09%
23	54.87.197.95	Application	-	-	-	-	-	-

Figure 73. User detail, end-to-end connection detail

Zscaler Posture Control (ChatOps) and Slack

You can integrate Zscaler Posture Control (ZPC) with Slack, a tool for centralized communication and collaboration. ZPC detects various security issues in your public cloud infrastructure and misconfigurations in the CI/CD pipeline. These issues are sent as alert notifications on Slack so you can investigate and address the issues on a common platform and streamline the mitigation directly into your developer tool.

Prerequisites

Before integrating ZPC with Slack, you must set up a Slack webhook endpoint.

1. Login to the Slack administrator portal.
2. Select **Configure Apps**.
3. In the **Slack app directory** select **Build**.

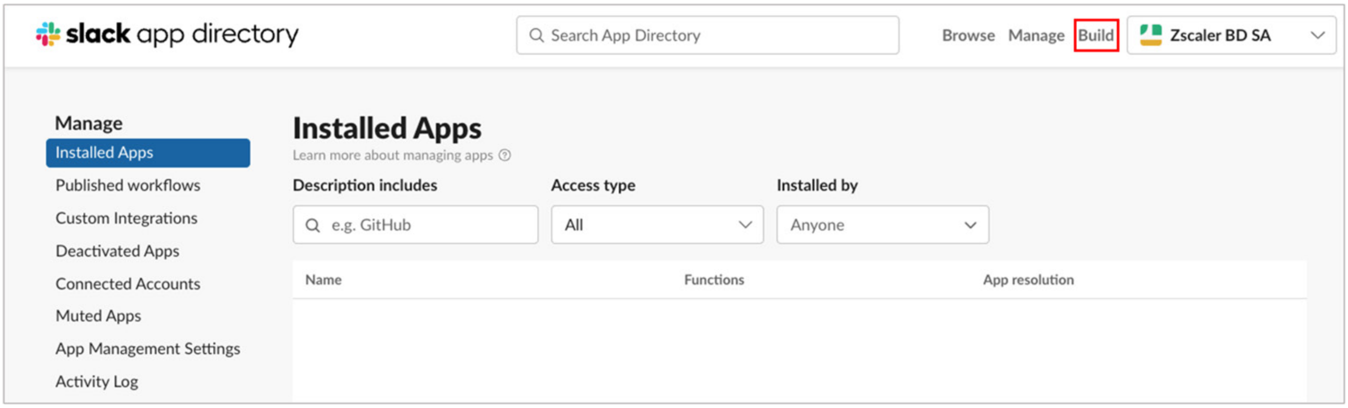
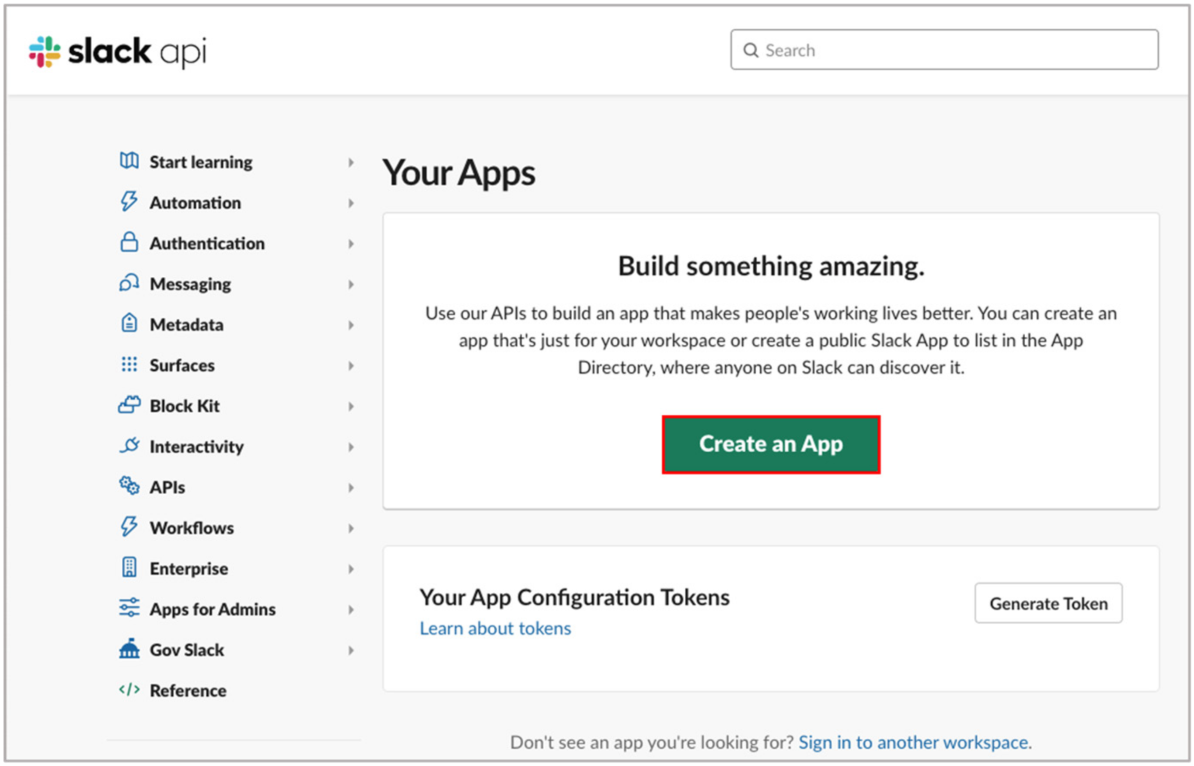


Figure 74. Slack app directory

4. Click **Create an App**.



Your Apps

Build something amazing.

Use our APIs to build an app that makes people's working lives better. You can create an app that's just for your workspace or create a public Slack App to list in the App Directory, where anyone on Slack can discover it.

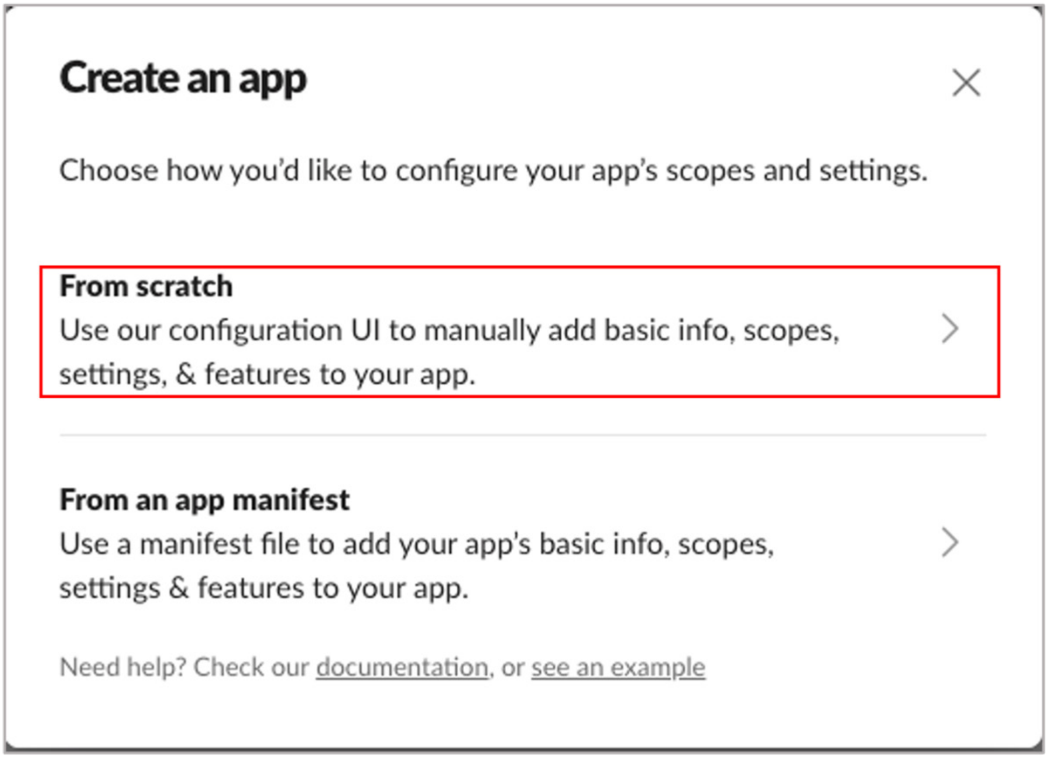
Your App Configuration Tokens

Learn about tokens

Don't see an app you're looking for? Sign in to another workspace.

Figure 75. Create custom app

5. Select **From scratch**.



Create an app

Choose how you'd like to configure your app's scopes and settings.

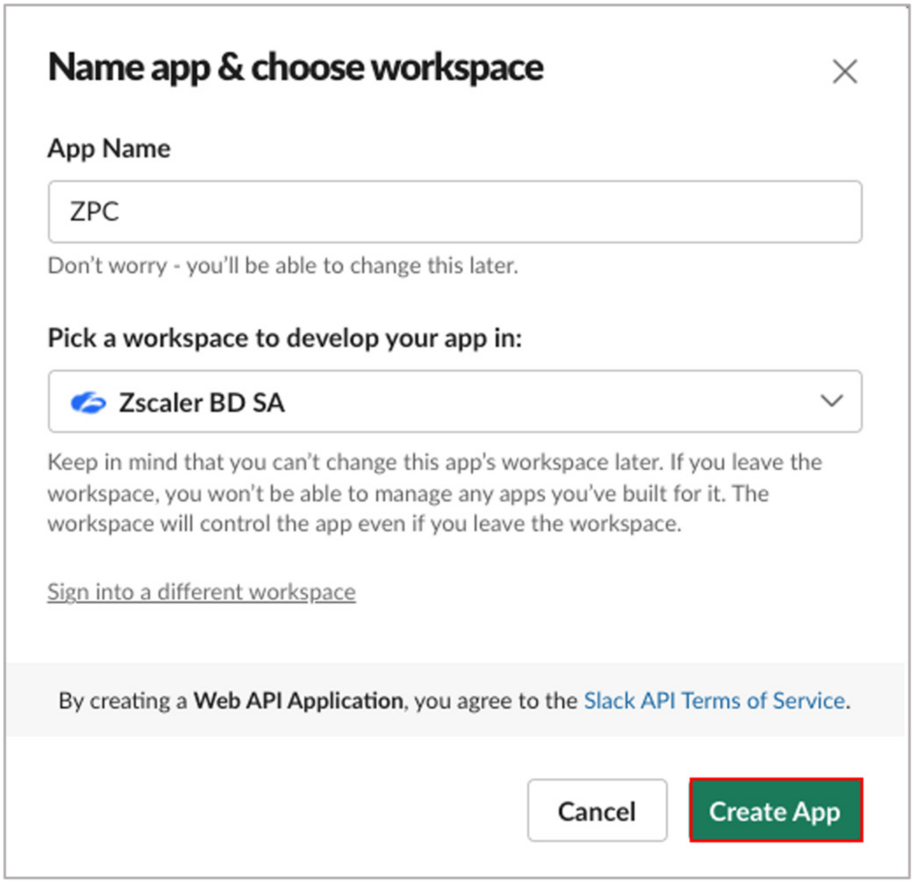
From scratch
Use our configuration UI to manually add basic info, scopes, settings, & features to your app.

From an app manifest
Use a manifest file to add your app's basic info, scopes, settings & features to your app.

Need help? Check our documentation, or see an example

Figure 76. Create an app

6. In the **Name app & choose workspace** window:
   a. **App Name**: Enter a name for the app.
   b. **Pick a workspace to develop your app in**: Select the Slack workspace from the drop-down menu.



Name app & choose workspace

App Name

ZPC

Don't worry - you'll be able to change this later.

Pick a workspace to develop your app in:

Zscaler BD SA

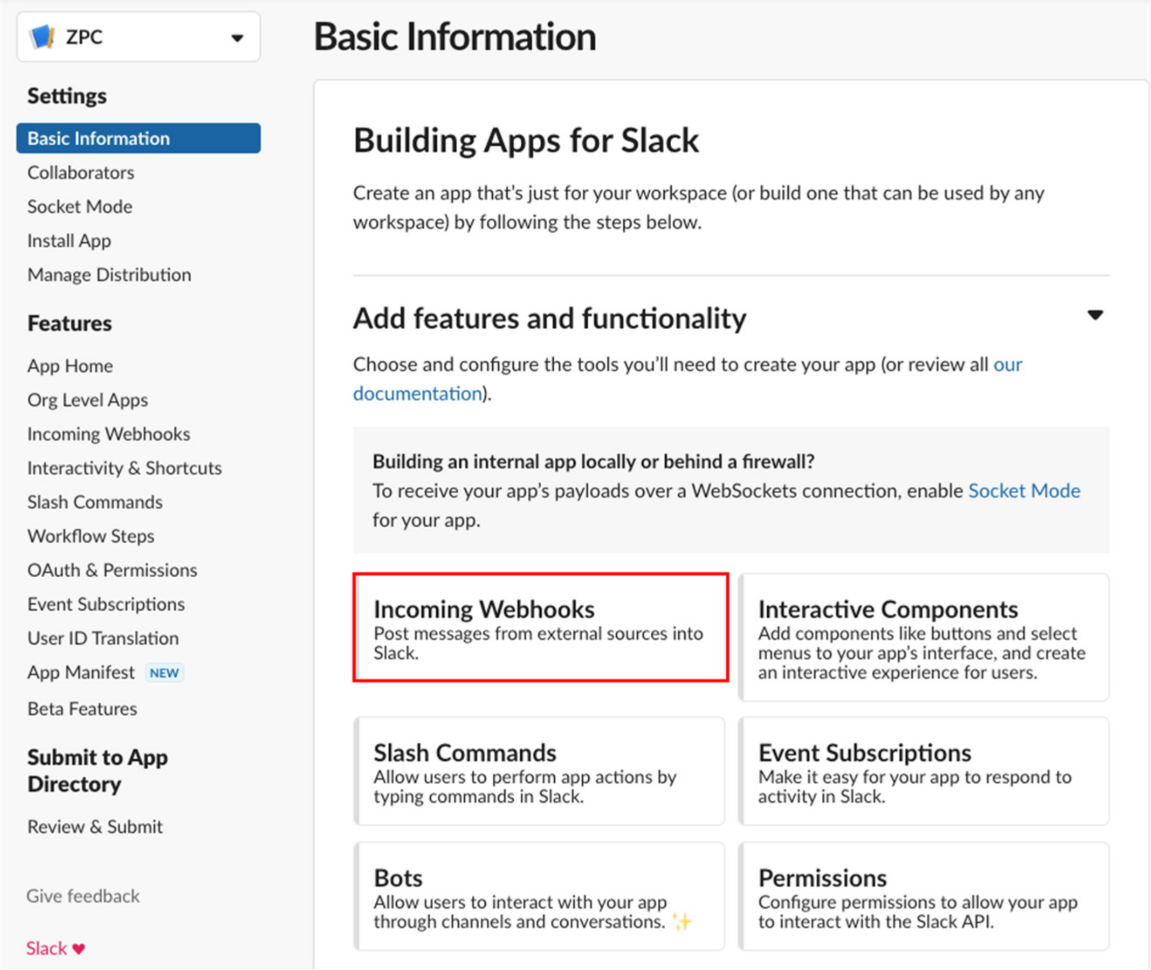
Keep in mind that you can't change this app's workspace later. If you leave the workspace, you won't be able to manage any apps you've built for it. The workspace will control the app even if you leave the workspace.

Sign into a different workspace

By creating a **Web API Application**, you agree to the Slack API Terms of Service.

Figure 77. Name app & choose workspace

7. Click **Create App**.
8. On the Basic Information page, select **Incoming Webhooks**.



Basic Information

Building Apps for Slack

Create an app that's just for your workspace (or build one that can be used by any workspace) by following the steps below.

Add features and functionality

Choose and configure the tools you'll need to create your app (or review all our documentation).

Building an internal app locally or behind a firewall?
To receive your app's payloads over a WebSockets connection, enable Socket Mode for your app.

Incoming Webhooks
Post messages from external sources into Slack.

Interactive Components
Add components like buttons and select menus to your app's interface, and create an interactive experience for users.

Slash Commands
Allow users to perform app actions by typing commands in Slack.

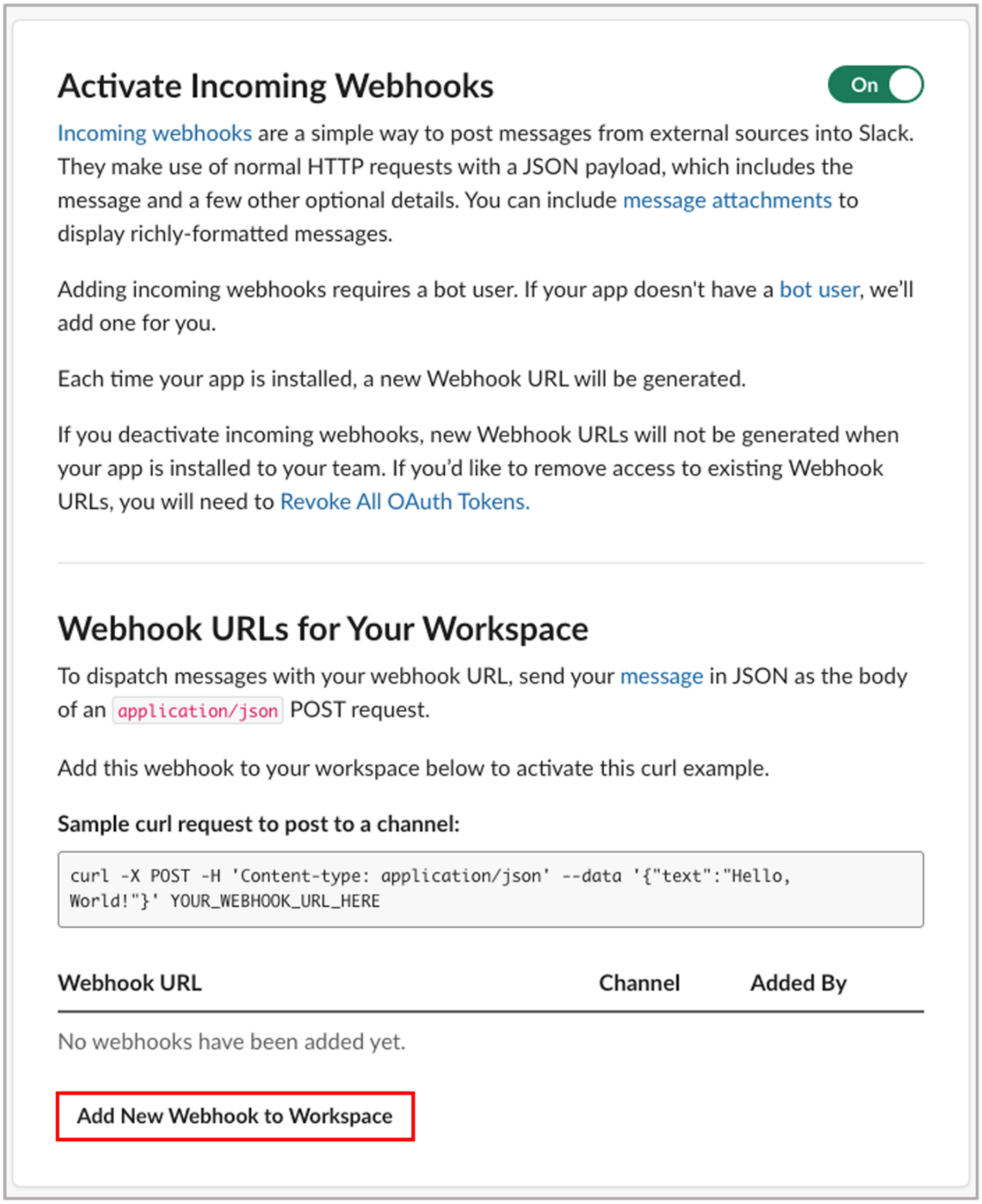
Event Subscriptions
Make it easy for your app to respond to activity in Slack.

Bots
Allow users to interact with your app through channels and conversations. ✨

Permissions
Configure permissions to allow your app to interact with the Slack API.

Figure 78. Incoming webhooks

9. On the **Incoming Webhooks** page:
    a. Enable **Activate Incoming Webhooks**.
    b. Click **Add New Webhook to Workspace**.



Activate Incoming Webhooks

Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include message attachments to display richly-formatted messages.

Adding incoming webhooks requires a bot user. If your app doesn't have a bot user, we'll add one for you.

Each time your app is installed, a new Webhook URL will be generated.

If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to Revoke All OAuth Tokens.

Webhook URLs for Your Workspace

To dispatch messages with your webhook URL, send your message in JSON as the body of an `application/json` POST request.

Add this webhook to your workspace below to activate this curl example.

Sample curl request to post to a channel:

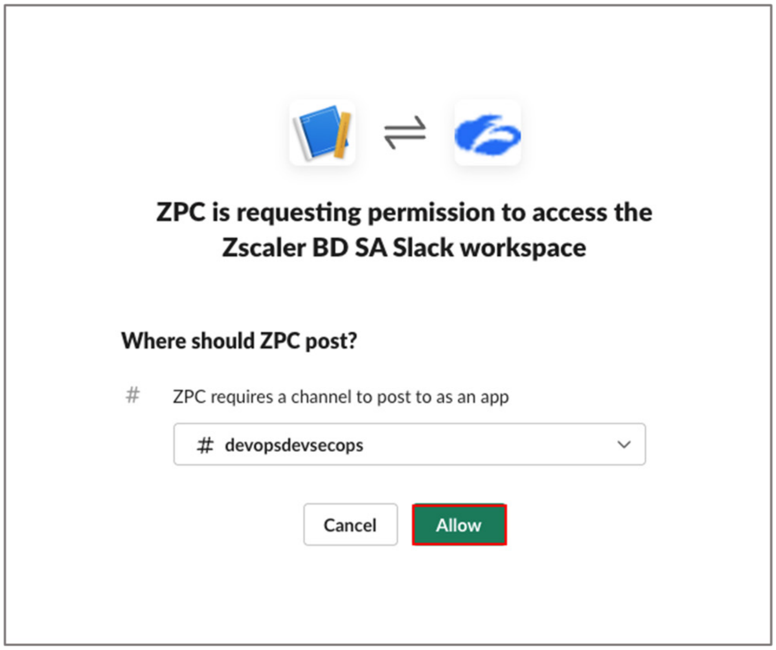
```
curl -X POST -H 'Content-type: application/json' --data '{"text":"Hello,
World!"}' YOUR_WEBHOOK_URL_HERE
```

Webhook URL	Channel	Added By

No webhooks have been added yet.

Figure 79. Activate incoming webhooks

10. Select the Slack channel to which ZPC must send notifications, then click **Allow**.



ZPC is requesting permission to access the Zscaler BD SA Slack workspace

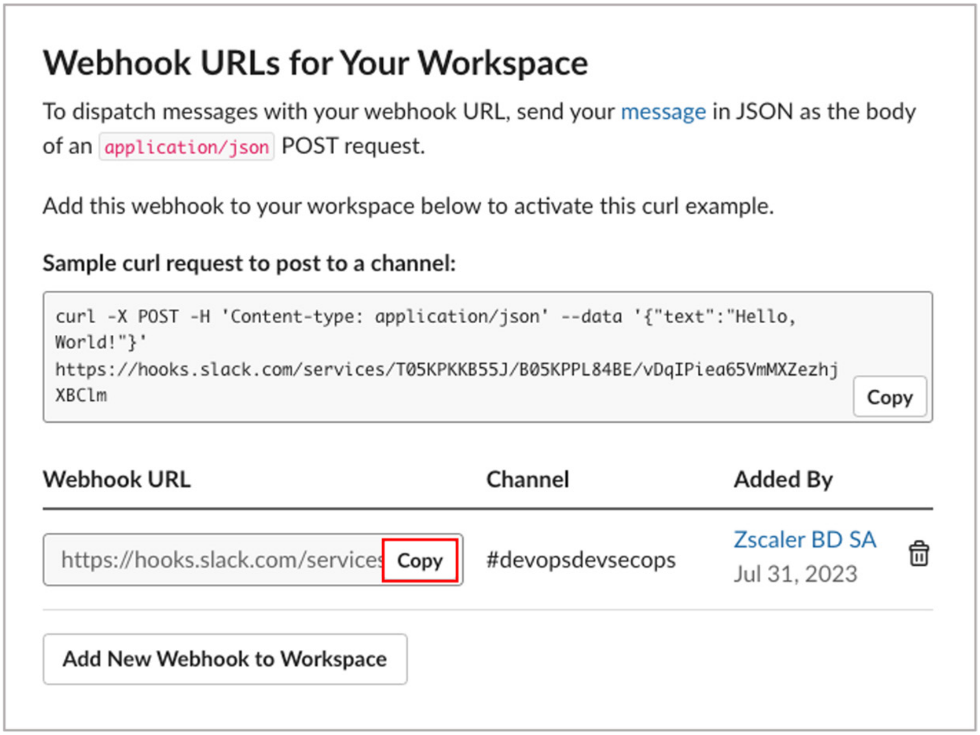
Where should ZPC post?

ZPC requires a channel to post to as an app

devopsdevsecops

Figure 80. Allow Slack channel

11. Copy the Webhook URL. You must specify this URL when integrating ZPC with Slack.



Webhook URLs for Your Workspace

To dispatch messages with your webhook URL, send your message in JSON as the body of an `application/json` POST request.

Add this webhook to your workspace below to activate this curl example.

Sample curl request to post to a channel:

```
curl -X POST -H 'Content-type: application/json' --data '{"text":"Hello,
World!"}'
https://hooks.slack.com/services/T05KPKKB55J/B05KPPL84BE/vDqIPiea65VmMXZezhj
XBClm
```

Webhook URL	Channel	Added By
https://hooks.slack.com/services Copy	#devopsdevsecops	Zscaler BD SA Jul 31, 2023

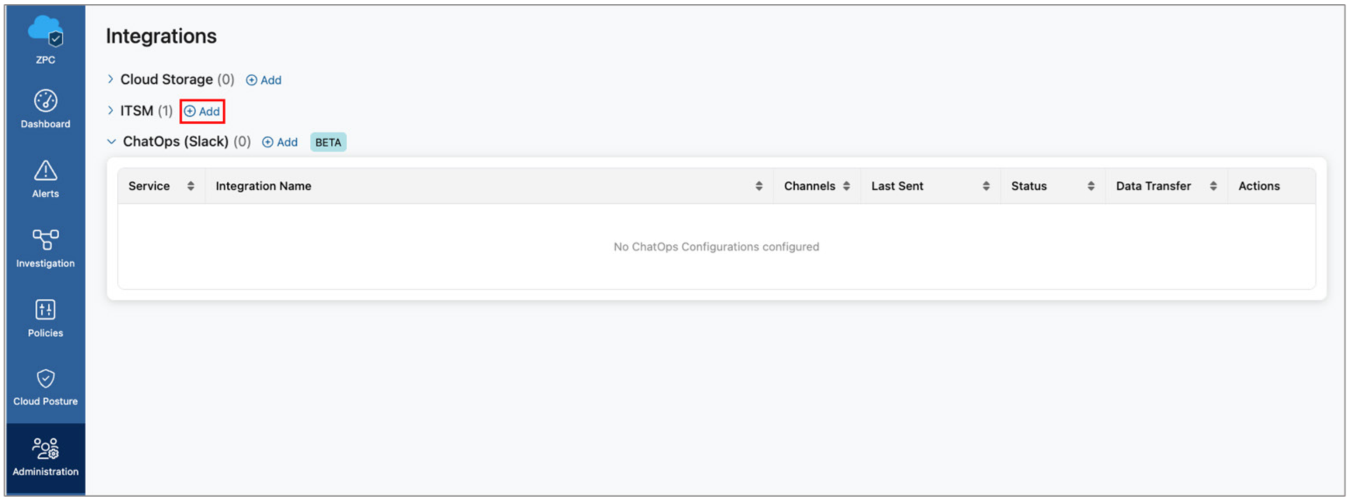
Figure 81. Copy Webhook URL

You can add only one Webhook per Slack channel.

Integrating ZPC and Slack

To integrate ZPC with Slack:

1. From the ZPC Admin Portal, go to **Administration** > **Integrations**.
2. To the right of **ChatOps (Slack)**, click **Add**.



Service	Integration Name	Channels	Last Sent	Status	Data Transfer	Actions

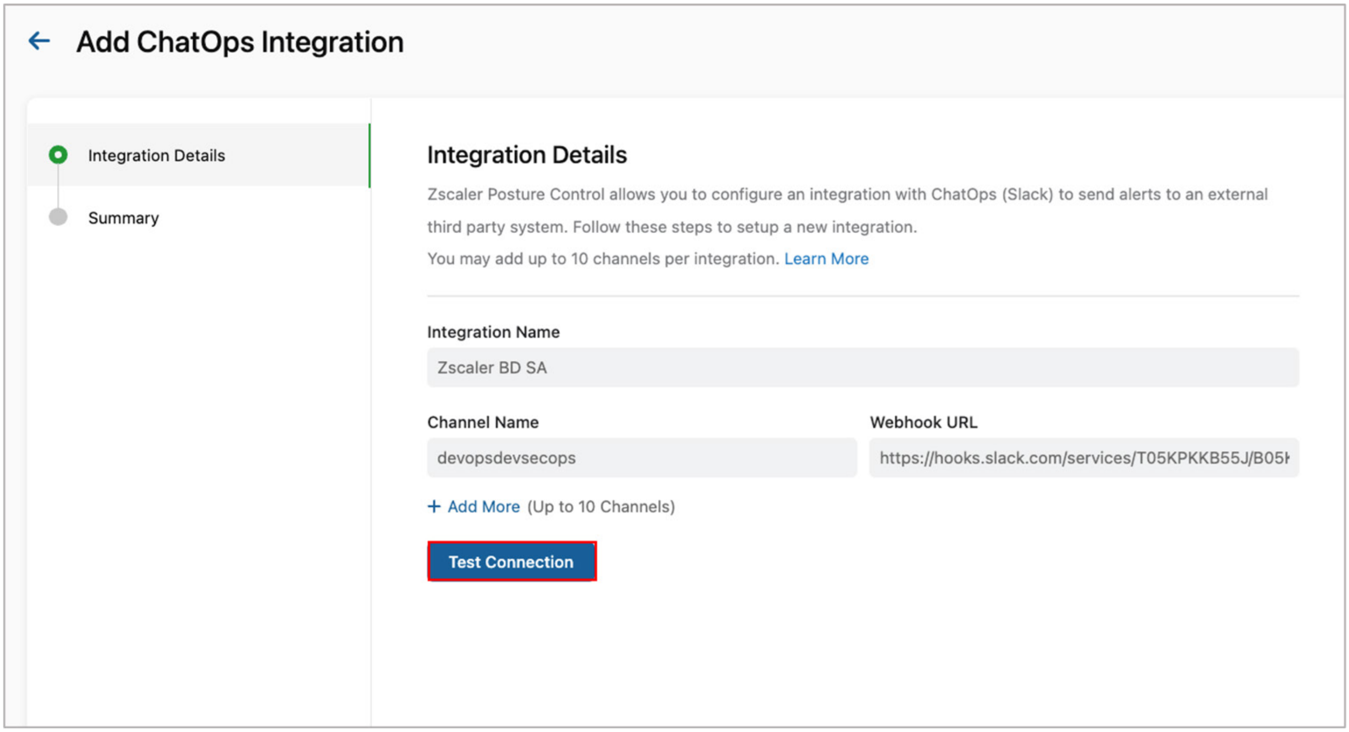
No ChatOps Configurations configured

Figure 82. Add ChatOps Slack integration

3. On the **Integration Details** page:
   a. **Integration Name**: Enter a unique name for the integration.
   b. **Channel Name**: Enter the name of the Slack channel where you want to receive alert notifications.
   c. **Webhook URL**: Enter the webhook URL that you copied from the Slack portal. The URL allows ZPC to connect and communicate with the Slack channel.
   d. **Add More**: (Optional) Click to include additional channels where you want to receive alert notifications.

ZPC allows you to add ten channels per integration. You can configure another integration to add more channels.

4. Click **Test Connection** to validate the Slack connection. A confirmation message appears that the Slack connection is verified. If not, then check the previous steps and try again.
5. Review the integration details on the **Summary** page.



Add ChatOps Integration

Integration Details

Zscaler Posture Control allows you to configure an integration with ChatOps (Slack) to send alerts to an external third party system. Follow these steps to setup a new integration.

You may add up to 10 channels per integration. Learn More

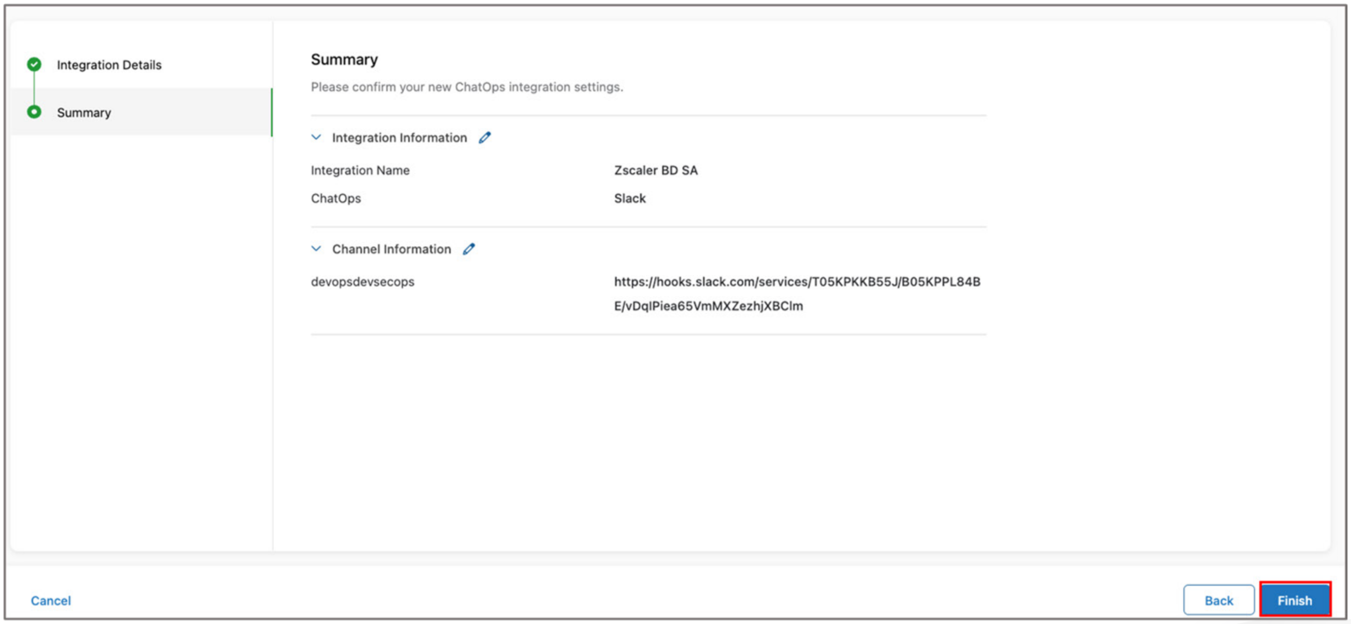
Integration Name: Zscaler BD SA

Channel Name: devopsdevsecops

Webhook URL: https://hooks.slack.com/services/T05KPKKB55J/B05I

Figure 83. Test ChatOps channel connection

6. Click **Next** and then **Finish**.



Summary

Please confirm your new ChatOps integration settings.

Integration Information

Integration Name: Zscaler BD SA

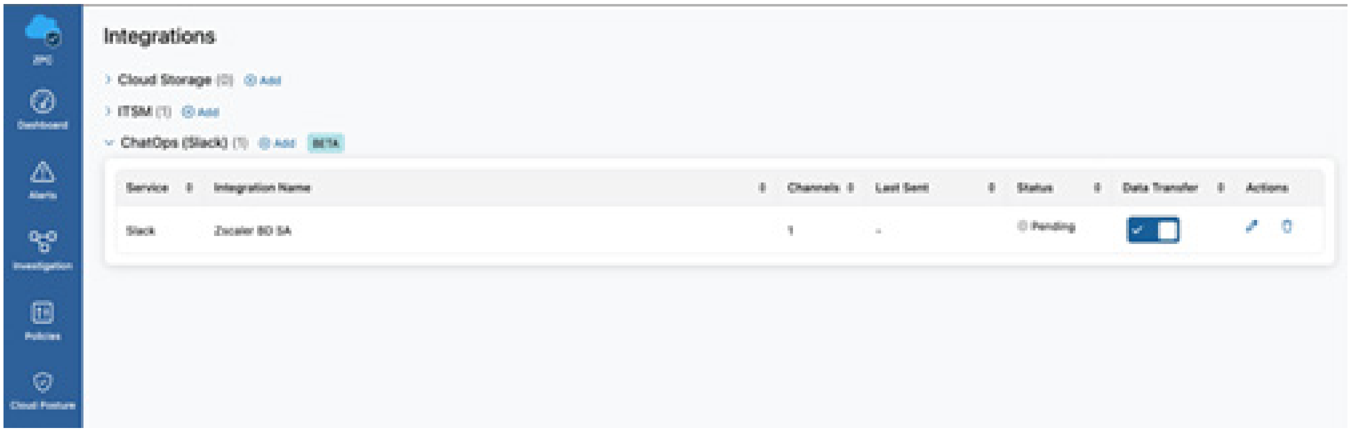
ChatOps: Slack

Channel Information

devopsdevsecops: https://hooks.slack.com/services/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

Figure 84. ChatOps configuration summary

The Slack integration is completed and the details are displayed on the **Integrations** page.



Service	Integration Name	Channels	Last Sent	Status	Data Transfer	Actions
Slack	Zscaler BD SA	1	-	Pending	✓	

Figure 85. ChatOps completed integration

Create Notification Rules

ZPC can send notifications to Slack ChatOps based on alerts generated due to security and compliance violations in cloud workloads and IaC.

On the ZPC Admin Portal page:

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

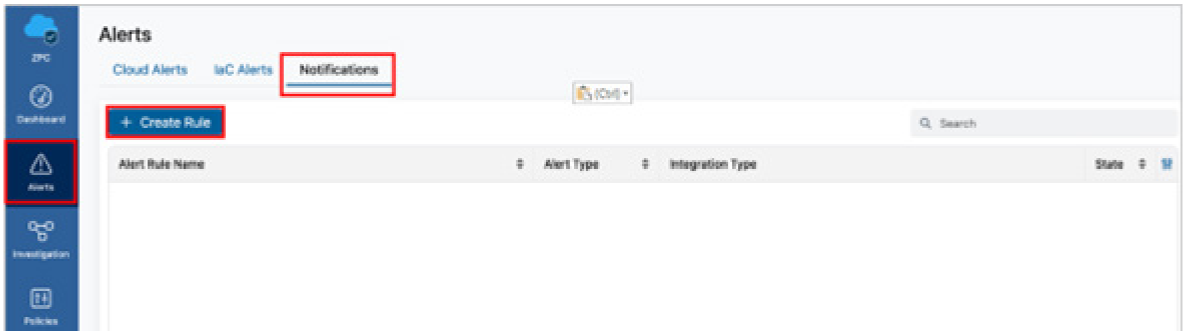
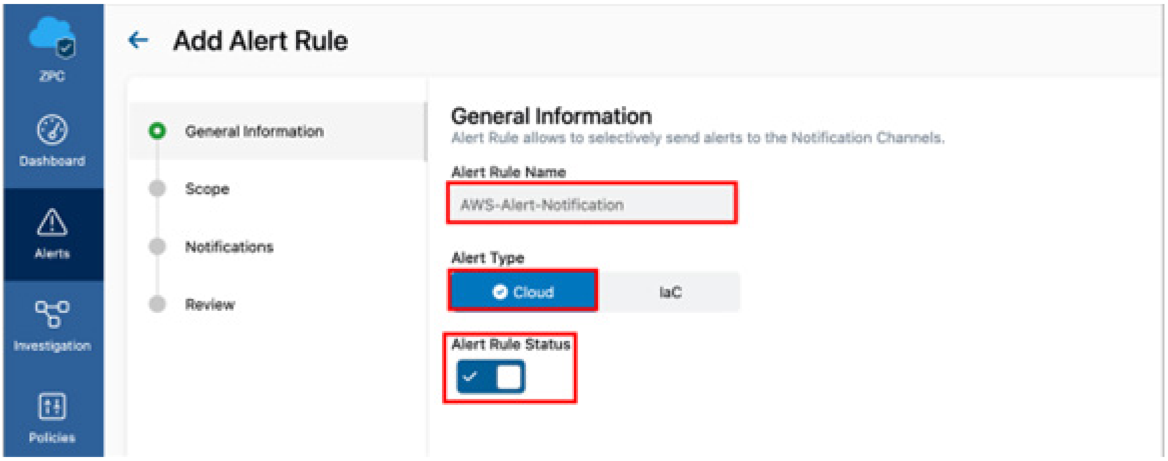


Figure 86. Notifications

Create a Cloud Notification Rule

To create a cloud notification rule:

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



Add Alert Rule

General Information

Alert Rule allows to selectively send alerts to the Notification Channels.

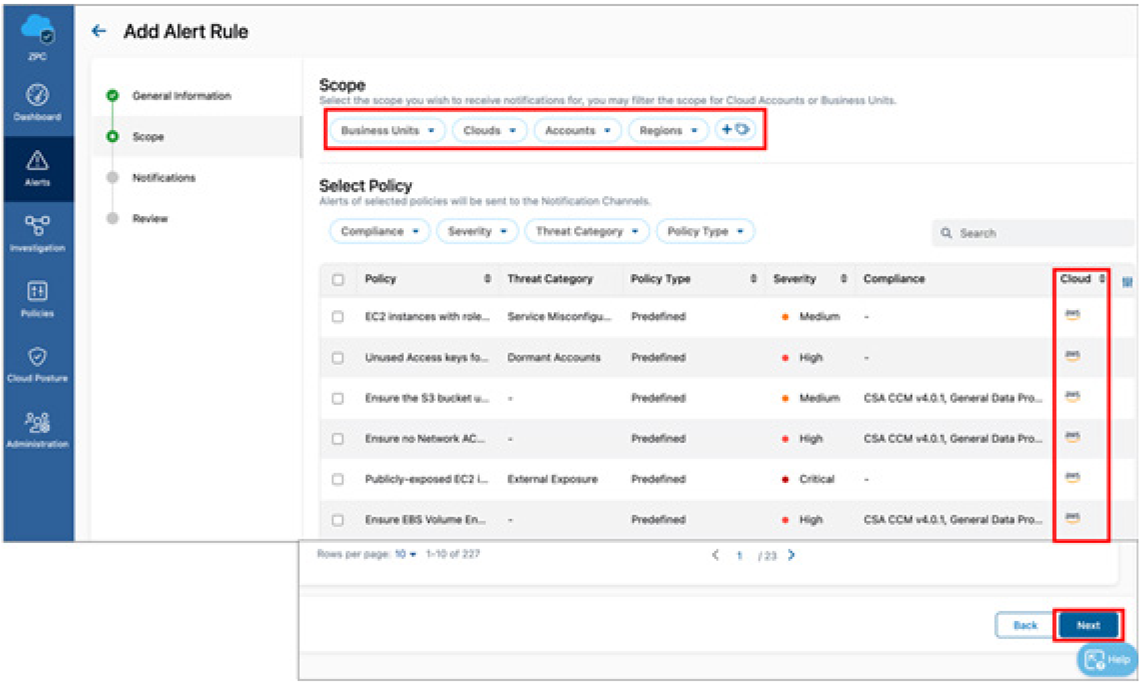
Alert Rule Name: AWS-Alert-Notification

Alert Type: ● Cloud | IaC

Alert Rule Status: ✓

Figure 87. Add Alert Rule

5. In the **Scope** page, select the scope for that you want to receive notifications.
6. In the **Select Policy** section, select the policies to which you want alerts sent to Slack.
7. Click **Next**.



Add Alert Rule

Scope

Select the scope you wish to receive notifications for, you may filter the scope for Cloud Accounts or Business Units.

Select Policy

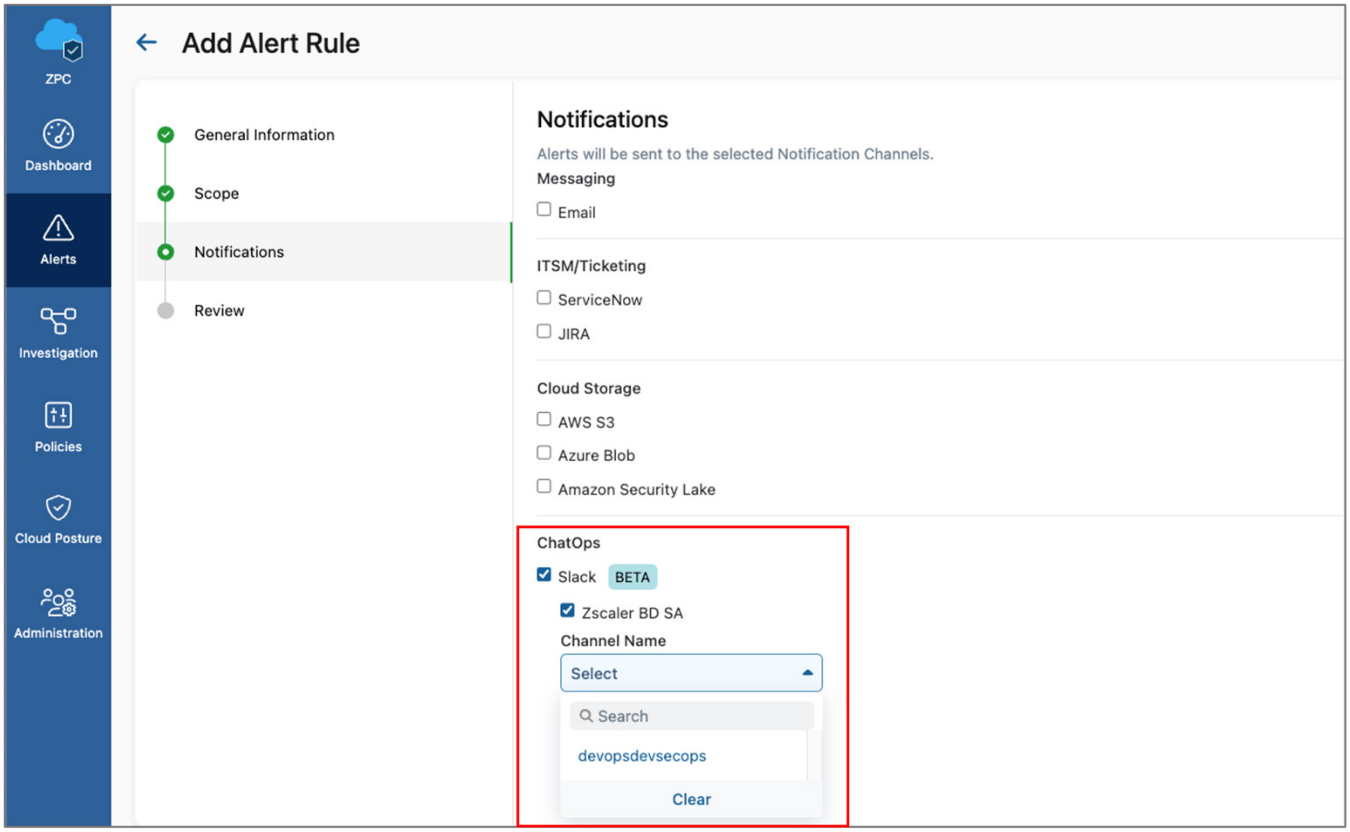
Alerts of selected policies will be sent to the Notification Channels.

□	Policy	Threat Category	Policy Type	Severity	Compliance	Cloud
□	EC2 instances with role...	Service Misconfigu...	Predefined	● Medium	-	aws
□	Unused Access keys fo...	Dormant Accounts	Predefined	● High	-	aws
□	Ensure the S3 bucket u...	-	Predefined	● Medium	CSA CCM v4.0.1, General Data Pro...	aws
□	Ensure no Network AC...	-	Predefined	● High	CSA CCM v4.0.1, General Data Pro...	aws
□	Publicly-exposed EC2 i...	External Exposure	Predefined	● Critical	-	aws
□	Ensure EBS Volume En...	-	Predefined	● High	CSA CCM v4.0.1, General Data Pro...	aws

Rows per page: 10 1-10 of 227 ‹ 1 / 23 ›

Figure 88. Add Alert Rule Scope

8. In the **Notifications** page, select **Slack** in the **ChatOps** section.
9. Select the name of the configured integration.
10. In **Channel Name**, select the channel where notifications should be posted.



Notifications

Alerts will be sent to the selected Notification Channels.

Messaging

□ Email

ITSM/Ticketing

□ ServiceNow

□ JIRA

Cloud Storage

□ AWS S3

□ Azure Blob

□ Amazon Security Lake

ChatOps

☑ Slack BETA

☑ Zscaler BD SA

Channel Name

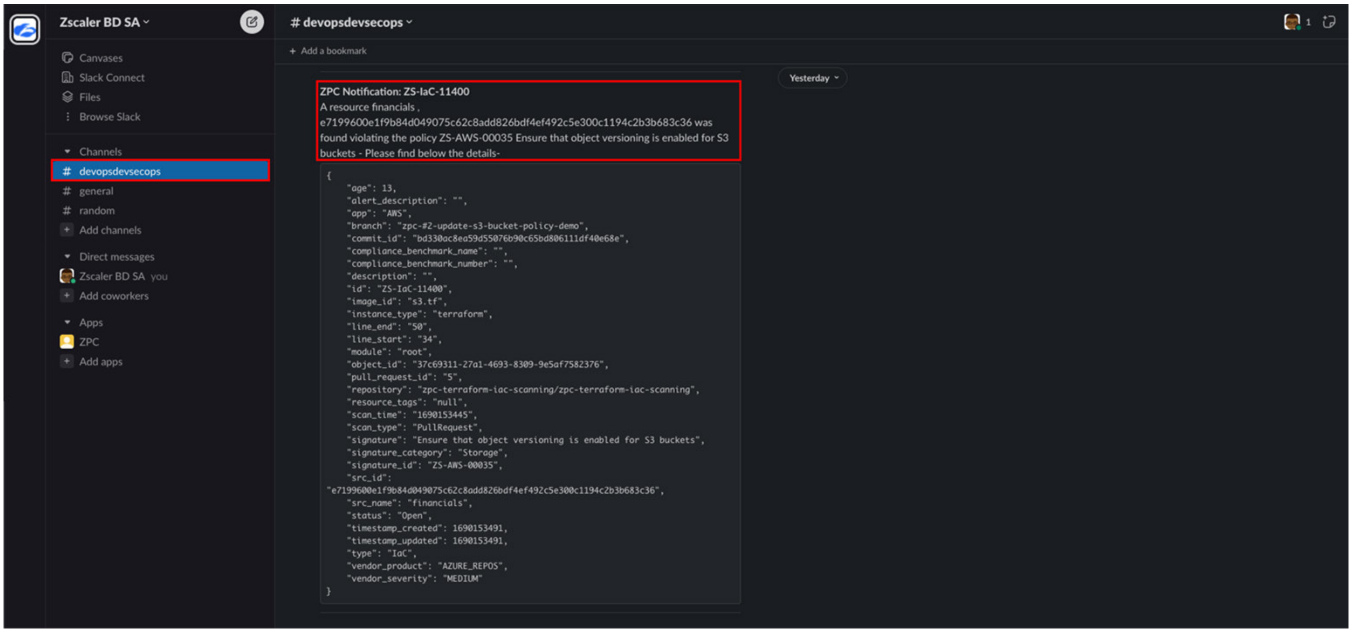
Select

Figure 89. ChatOps Notification Alert

11. Click **Next**.

Analyzing ZPC Alerts in Slack

To visualize a ZPC alert in Slack, open the Slack channel configured in the ChatOps integration.



ZPC Notification: ZS-IaC-11400
A resource financials ,
e7199600e1f9b84d049075c62c8add826bdf4ef492c5e300c1194c2b3b683c36 was found violating the policy ZS-AWS-00035 Ensure that object versioning is enabled for S3 buckets - Please find below the details-

```
{
    "age": 13,
    "alert_description": "",
    "app": "AWS",
    "branch": "zpc-#2-update-s3-bucket-policy-demo",
    "commit_id": "bd330ac8ea59d55076b90c65bd806111df40e68e",
    "compliance_benchmark_name": "",
    "compliance_benchmark_number": "",
    "description": "",
    "id": "ZS-IaC-11400",
    "image_id": "s3.tf",
    "instance_type": "terraform",
    "line_end": "50",
    "line_start": "34",
    "module": "root",
    "object_id": "37c69311-27a1-4693-8309-9e5af7582376",
    "pull_request_id": "5",
    "repository": "zpc-terraform-iac-scanning/zpc-terraform-iac-scanning",
    "resource_tags": "null",
    "scan_time": "1690153445",
    "scan_type": "PullRequest",
    "signature": "Ensure that object versioning is enabled for S3 buckets",
    "signature_category": "Storage",
    "signature_id": "ZS-AWS-00035",
    "src_id":
"e7199600e1f9b84d049075c62c8add826bdf4ef492c5e300c1194c2b3b683c36",
    "src_name": "financials",
    "status": "Open",
    "timestamp_created": 1690153491,
    "timestamp_updated": 1690153491,
    "type": "IaC",
    "vendor_product": "AZURE_REPOS",
    "vendor_severity": "MEDIUM"
}
```

Figure 90. Slack Channel ZPC Alert

Appendix A: Requesting Zscaler Support

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

Requesting Help via ZIA

To contact Zscaler Support:

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

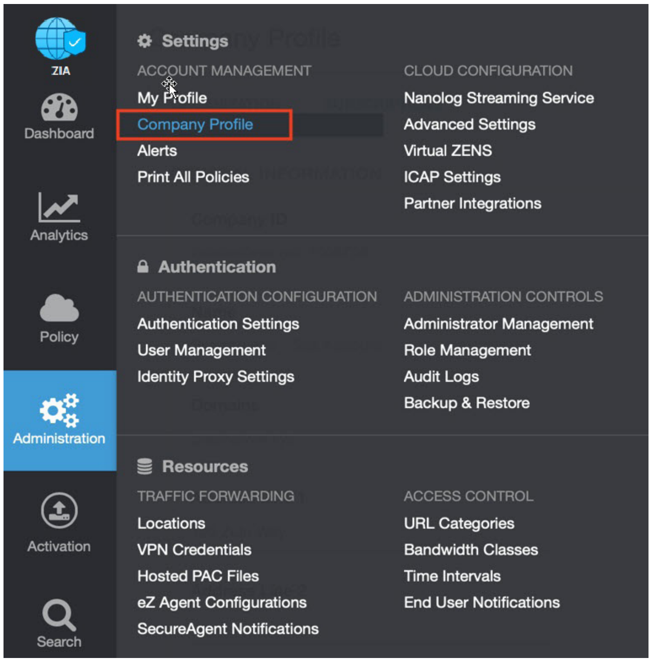
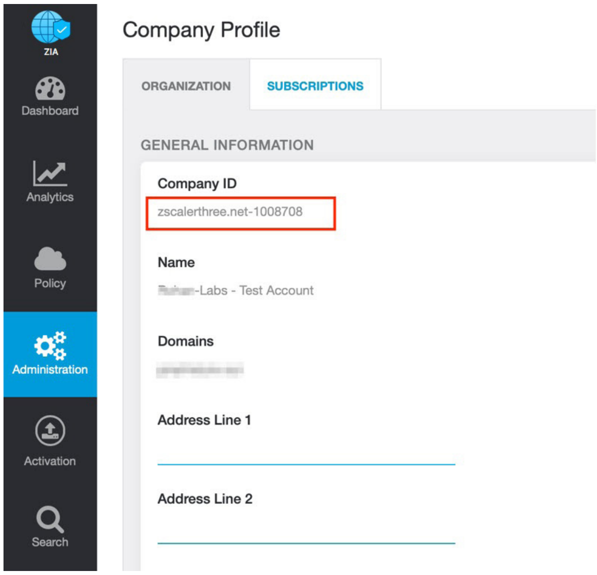


Figure 91. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 92. Company ID

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

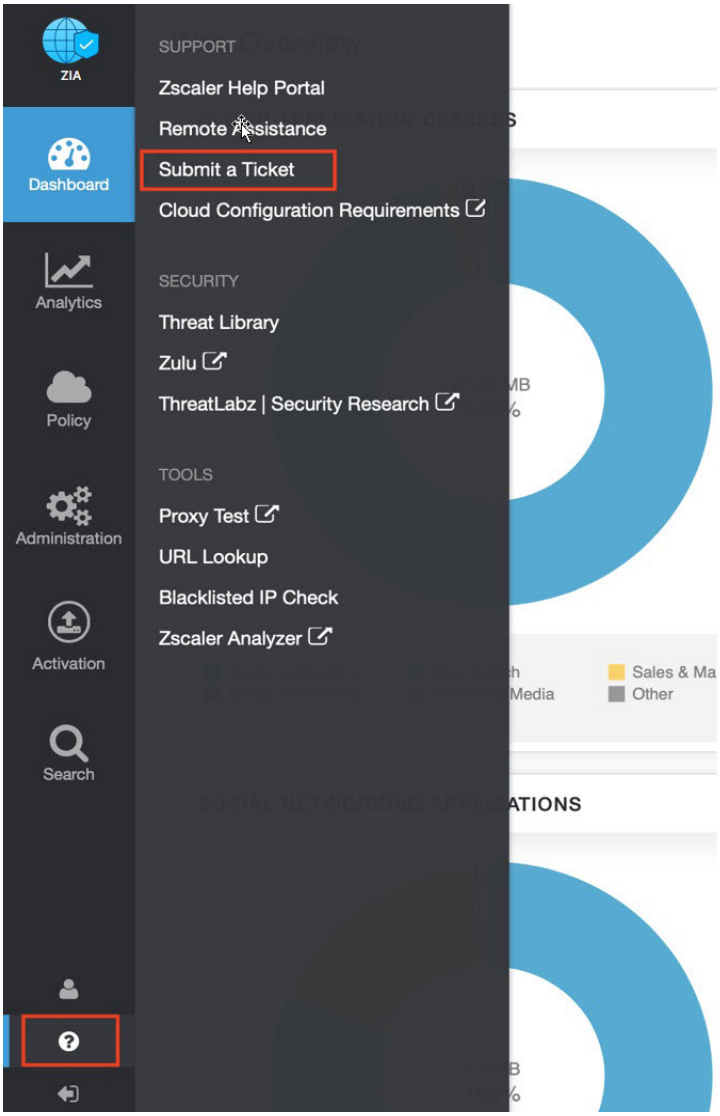
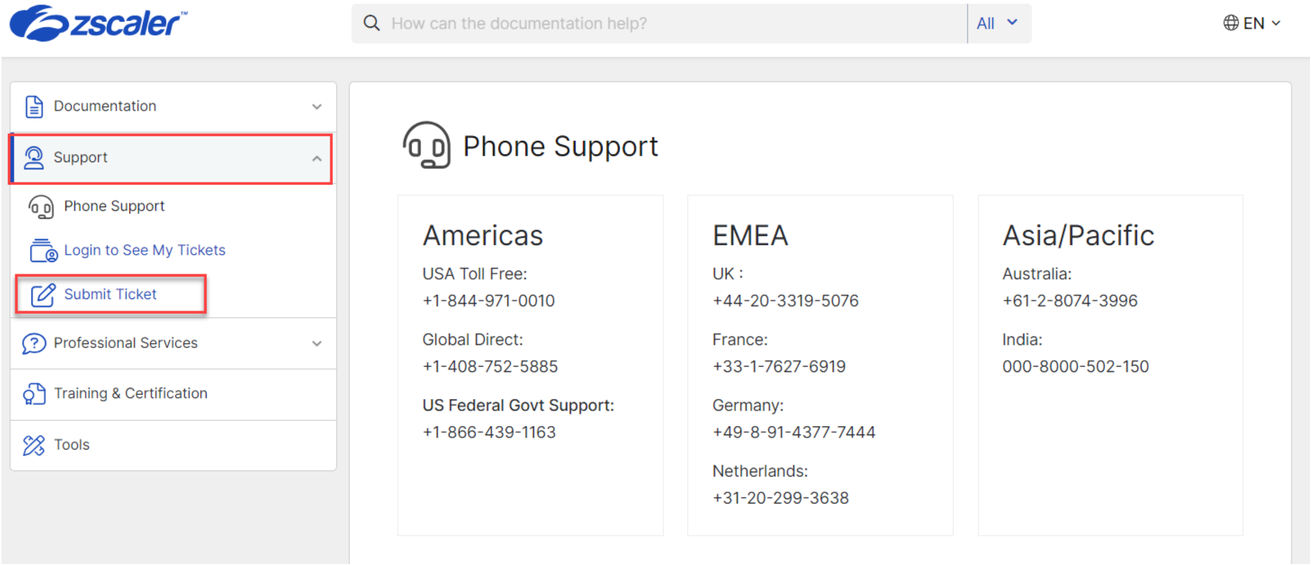


Figure 93. Submit a ticket

Requesting Zscaler Support via ZPC

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

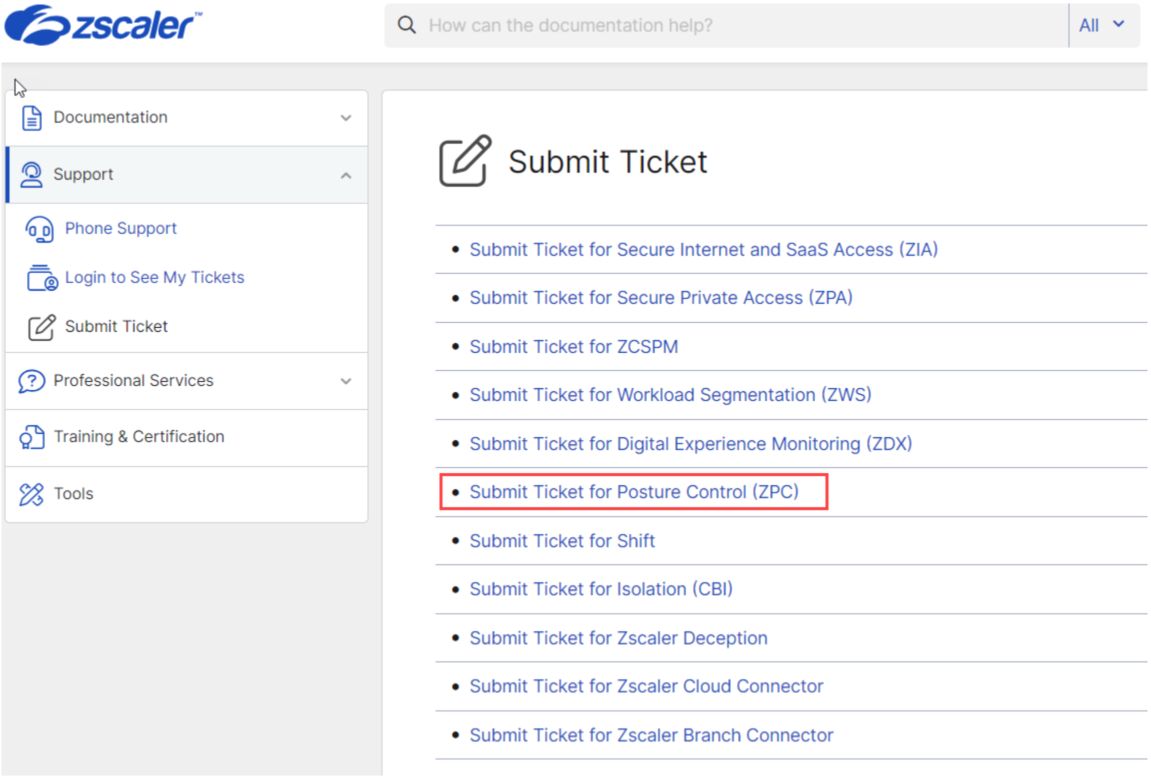
Asia/Pacific

Australia:
+61-2-8074-3996

India:
000-8000-502-150

Figure 94. ZPC Help

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

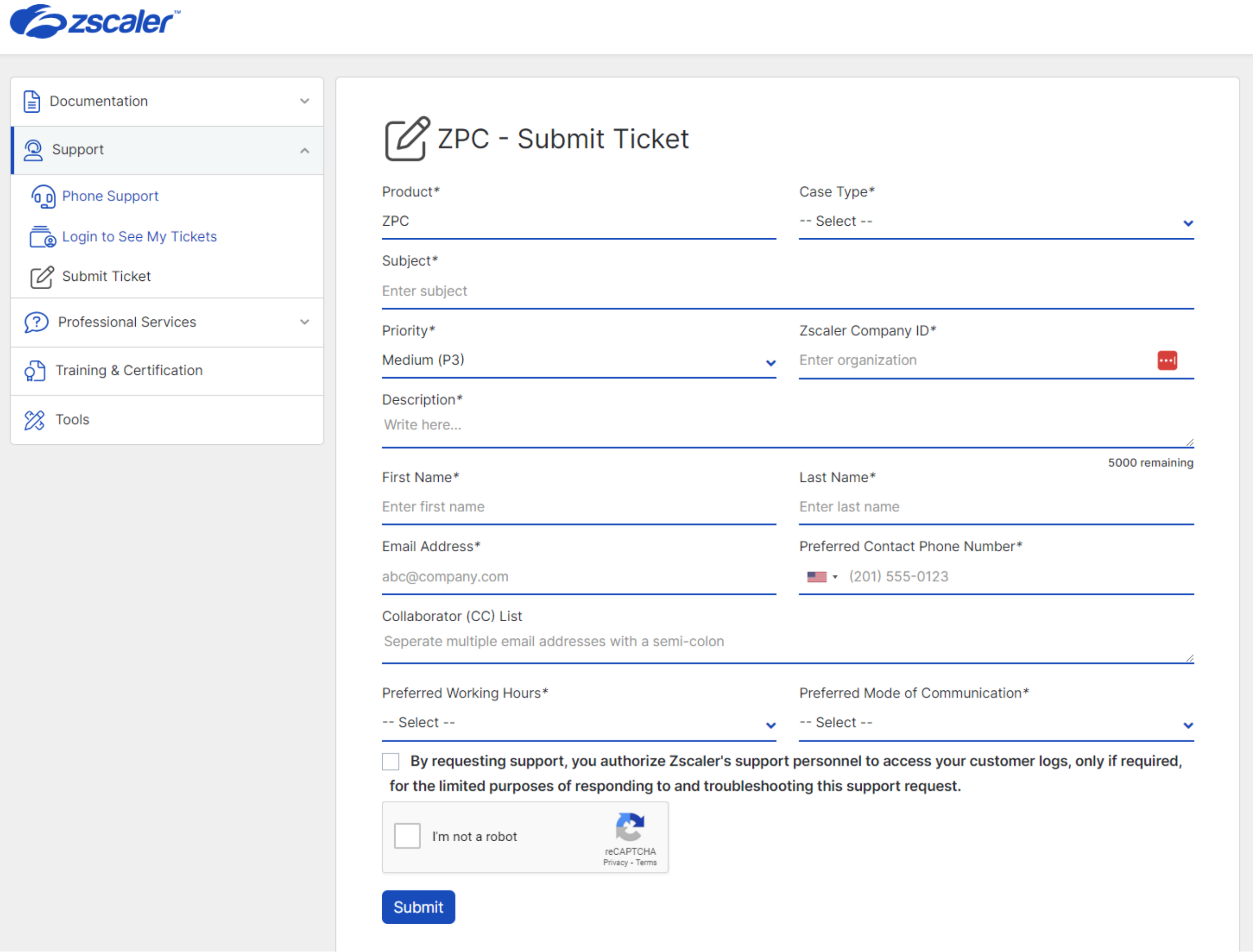


Submit Ticket

- 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 95. ZPC Support

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

Submit

Figure 96. 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.