# Table of Contents

## Terms and Acronyms

### About This Document

Zscaler Overview

Slack Overview

Audience

Software Versions

Request for Comments

### Zscaler and Slack Introduction

ZIA Overview

ZDX Overview

Zscaler Resources

Slack Overview

Slack Resources

### Zscaler Data Protection and Digital Experience for Slack.com

ZIA SaaS Identity Proxy

ZIA Tenant Profiles and Tenancy Restrictions

ZIA CASB Data and Malware Protection for Slack

ZDX for the Slack User Experience

### Configure the SaaS Identity Proxy

Configure the SaaS Identity Proxy

Configure the Zscaler Portal for the SaaS Identity Proxy

Configure Slack to use the Identity Proxy

Configure Slack Single Sign-On

The Completed Slack Configuration

User Informational Email

The Zscaler Active Identity Proxy Notification

### Configuring Tenancy Restrictions for Slack

Create a Tenant Profile
Zscaler and Slack Deployment Guide

Cloud Application Access Control Policy Wizard ................................................................. 25
Completed Tenant Restrictions ............................................................................................ 26
Tenant Restriction Alerts .................................................................................................... 27

Configuring the Slack Tenant ............................................................................................. 28
Adding the Slack Tenant ...................................................................................................... 29
SaaS Tenant Configuration Wizard ....................................................................................... 30
SaaS Tenant Configuration Wizard ....................................................................................... 31
Configuring the Zscaler Tenant on Slack .......................................................................... 32
Configuring the Zscaler Tenant on Slack .......................................................................... 33
The Active Slack Tenant ...................................................................................................... 35

Configuring Slack Policies and Scan Configuration ........................................................... 36
Scoping the Policies and Remediation .................................................................................. 37
Creating a DLP Policy .......................................................................................................... 38
Creating a DLP Engine ........................................................................................................ 39
Creating a DLP Engine ........................................................................................................ 40
Configure a SaaS DLP Policy .............................................................................................. 41
SaaS DLP Policy Details ....................................................................................................... 42
Configure a SaaS DLP Policy .............................................................................................. 43

Configure a SaaS Malware Policy ....................................................................................... 45
SaaS Malware Policy Wizard ............................................................................................... 46
SaaS Malware Policy ............................................................................................................ 47

Configure the Scan Schedule Configuration ....................................................................... 48
Start the Scan Schedule ...................................................................................................... 49

Reporting and Visibility .................................................................................................... 50
SaaS Assets and SaaS Assets Summary Report ................................................................. 51
SaaS Security Insights ......................................................................................................... 52

Zscaler Digital Exchange (ZDX) for Slack ........................................................................ 53
Log in to ZDX ....................................................................................................................... 54
Configure ZDX for Slack .................................................................................................... 55
Configure ZDX Probes for Slack ......................................................................................... 57
Configure Probes for Slack Monitoring ............................................................................. 62
Configure ZDX Probes for Slack ......................................................................................... 64
Zscaler and Slack Deployment Guide

The ZDX Enabled Slack Application ........................................................................... 66
Create an Alert for the Slack Service ........................................................................ 67
  Create an Alert for the Slack Service ..................................................................... 68
The Triggered Alert for the Slack Service .................................................................. 73
Alert Detail for the Slack Service ................................................................................ 74
The Sent Alert Email for the Slack Service ............................................................... 75

Using ZDX: The Dashboard ....................................................................................... 76
  Application Overview and Performance Detail ....................................................... 77
    Slack Application Performance Detail ................................................................ 78
  User Overview and Performance Detail .................................................................. 80
    Slack User Performance Detail .......................................................................... 81
    User Performance Detail ..................................................................................... 82

Appendix A: Requesting Zscaler Support ................................................................. 83
  Gather Support Information .................................................................................. 83
    Save Company ID ............................................................................................... 84
    Enter Support Section ....................................................................................... 85
Terms and Acronyms

The following terms and acronyms are used in this deployment guide.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
</tr>
<tr>
<td>SaaS Security API</td>
<td>Zscaler CASB Service called SaaS Security API</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
<tr>
<td>ZDX</td>
<td>Zscaler Digital Exchange (Zscaler)</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
</tbody>
</table>
About This Document

This section contains information about what this deployment guide covers.

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 Digital Experience (ZDX) measures and improves user digital experiences in cloud and hybrid environments through a unified view of application performance. 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. For more information on Zscaler, go to the Zscaler website or follow Zscaler on Twitter @zscaler.

Slack Overview

Slack 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.

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, refer to:

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

Software Versions

This document was authored using ZIA v6.1 and Slack Production Release dated Jun 25, 2021. A Slack developer account was used to created and verify the features enabled and used as examples.

Request for Comments

- **For Prospects and Customers:** We value reader opinions and experiences. Contact us at 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

This section contains overviews of the Zscaler and Slack applications described in this deployment guide.

ZIA Overview

ZIA is a secure Internet and web gateway delivered as a service from the cloud. Think of it as a secure Internet onramp—all you do is make Zscaler your next hop to the Internet via one of the following methods:

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

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

You get full protection from web and Internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, CASB, and Browser 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.

Zscaler Resources

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

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>Adding SaaS Application Tenant</td>
<td>Help articles for Zscaler SaaS security APIs that provide visibility and</td>
</tr>
<tr>
<td></td>
<td>security for sanctioned SaaS applications used in your organization.</td>
</tr>
<tr>
<td>About SaaS Application Tenant</td>
<td>Help article explaining SaaS application tenants.</td>
</tr>
<tr>
<td>SaaS Security API DLP Policy</td>
<td>Help articles for the SaaS Security API Data Loss Prevention (DLP) policies</td>
</tr>
<tr>
<td></td>
<td>that create rules to discover and protect sensitive data at rest in sanctioned</td>
</tr>
<tr>
<td></td>
<td>SaaS applications.</td>
</tr>
<tr>
<td>About Data Loss Prevention</td>
<td>Help articles on how Zscaler can forward information about transactions</td>
</tr>
<tr>
<td></td>
<td>that trigger DLP policies to your third party solution.</td>
</tr>
<tr>
<td>About DLP Dictionaries</td>
<td>Help articles on how a DLP dictionary contains a set of patented algorithms</td>
</tr>
<tr>
<td></td>
<td>that are designed to detect specific kinds of information in your users’</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td>About DLP Engines</td>
<td>Help article on adding a custom DLP engine for configuring DLP policy rules.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Slack</td>
<td>Information about Slack Technologies.</td>
</tr>
<tr>
<td>Slack Product Documentation</td>
<td>Online help for Slack products.</td>
</tr>
<tr>
<td>Slack Community</td>
<td>Online community for Slack product help and technical questions.</td>
</tr>
<tr>
<td>Slack Resources</td>
<td>Browse resources tailored to your team, your needs and all the ways you can get more out of Slack.</td>
</tr>
</tbody>
</table>
Zscaler Data Protection and Digital Experience for Slack.com

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

SaaS services facilitate collaboration, simply tool access, and enable 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 Access Exchange Service (ZDX) for user experience visibility.

![Diagram of Z-Access and Z-Identity](image)

**Figure 1. Zscaler solutions for Slack**

ZIA provides Slack SaaS security by using access control, identity control, SaaS security, and Zscaler’s SaaS 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.

The ZDX service 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 our partner SaaS CRM service.

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

- SaaS Identity Proxy
- Tenant Restrictions
- SaaS Security Data Loss Protection (CASB)
- SaaS Security Malware Detection (CASB)
- Cloud Application Access Control
- ZDX for Slack

**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 pop-up screen 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. Once 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.

![Zcaler Internet Access](image)

**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, CASB 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 users and organizations 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 CASB Data and Malware Protection for Slack

The Zscaler CASB (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 our 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 CASB SaaS security in use with Slack

What makes our 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-prem or remote.

For more information, see the resources in **Appendix A: 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 *Appendix A: Zscaler Resources*. 
Configure the 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, traffic inspection, 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 pop-up 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. Once 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.

Figure 6. 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. Using a cloud platform that supports cloud firewall, cloud IPS, cloud sandbox, cloud DLP, CASB and cloud browser isolation, you can start with the services you need today and activate others as your needs grow.
Configure the SaaS Identity Proxy
Log into the Zscaler tenant with administrator credentials.

Figure 7. Configure SaaS identity proxy
Configure the Zscaler Portal for the SaaS Identity Proxy

To configure Zscaler for the SaaS identity proxy:

1. Select Administration > Identity Proxy settings.
2. Select Add Cloud Application (the configuration wizard displays).
3. Give the cloud application a Name.
4. Select Enable.
5. Select Slack for Cloud Application.
8. Select the SAML_2022 or Later Signing Certificate.
10. Click Save.

Figure 8. Configure the SaaS identity proxy settings
Configure the SaaS Identity Proxy

This is the completed identity proxy configuration on the Zscaler tenant.

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](image)

*Figure 9. 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. This brings up the Slack SSO Configuration wizard.

Figure 10. 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. Uncheck **Sign the Response**.
6. Click **Test Configuration**.

![Figure 11. Slack SSO wizard confirmation](image)

**NOTE**

The certificate must be one continuous string with no linefeeds or carriage returns.
Configure Slack Single Sign-On

If the configuration tests correctly a confirmation that **Everything looks good!** displays. If there is a problem with the configuration, a **Glitch Reported** or a failure response displays. You need to repeat the process from the beginning.

Click **Confirm Update** to activate the configuration.

**Figure 12. Slack SSO wizard confirmation**
The Completed Slack Configuration

The completed SSO configuration.

Figure 13. The completed identity provider configuration
User Informational Email

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

![Single sign-on enabled](image)

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/zsso-2207485401043-2256570469712-92c368b416fa36685c47d7030f51e14cc3903d43562713ffaf12d4cab0dd272a](https://slack.com/zsso-2207485401043-2256570469712-92c368b416fa36685c47d7030f51e14cc3903d43562713ffaf12d4cab0dd272a)

Thanks,
The team at Slack

**Figure 14. 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 is going through Zscaler they can access Slack as usual.

Figure 15. 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 CASB for data-at-rest, Zscaler Cloud Application security is inline CASB.

Cloud App Control provides SaaS application intelligence to consolidate all associated URL’s 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.

![Zscaler Internet Access](image)

**Figure 16. 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.

Let’s define a tenant profile and a Cloud Application Control policy to allow all Slack users in a Slack organization to a specific Slack tenant.
Create a Tenant Profile

To create our tenant profile to allow our specific users:

1. Sign into your organization’s ZIA Admin Portal with admin credentials.
2. Select Administration > Tenant Profile.
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 org ID or workspace ID for the Workspace ID.
7. Add the Allowed Tenants by org ID or workspace ID.
8. Save the configuration.

*Figure 17. Add tenant profile*
Cloud Application Access Control Policy Wizard

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

1. Select **Policy > URL & App Control > Cloud App Control Policy**.
2. Select **Add** and from the pull down 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 Access**.
6. Select the **Slack Tenant Profile** we just created.
7. Click **Save**.

![Figure 18. Create a Cloud App Control Allow policy](image)

**NOTE**

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

Our completed access policies. **Activate** the policy additions.

*Figure 19. Completed Cloud Application 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.

*Figure 20. Alerts when accessing blocked Slack tenants*
Configuring the Slack Tenant

The Slack tenant must be configured 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 CASB services, DLP, and malware protection.

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

![ZIA Admin Portal](image)

*Figure 21. ZIA Admin Portal*
Adding the Slack Tenant

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

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

![ZIA SaaS Application Tenant](image)

*Figure 22. 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.

![Add SaaS Application Tenant](image)

*Figure 23. 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 a **Name** for the **Tenant Name**.
2. Enter an **Email ID** for 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.

*Figure 24. 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.
3. We must approve the Zscaler application on Slack.

*Figure 25. 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 you need to go back to the Zscaler Admin Portal and execute the next step of the installation.

Figure 26. Approve the Zscaler application
In the Zscaler Tenant setup select the **Provide Admin Credentials** link on Step 5. After you have provided the admin credentials, the tenant configuration is complete.

1. Right click the **Provide Admin Credentials** link on Step 5, and open the link in a new tab.
2. **Save and Activate** the configuration.
3. This completes the creation of the Slack tenant. We can now apply CASB controls on our Slack instance using Zscaler data and malware protect.

![Add SaaS Application Tenant](image)

*Figure 27. Authorize access to the Slack bot*
The Active Slack Tenant

Check that the Status of Slack tenant is Active. Select Administration > SaaS Application Tenants.

![SaaS Application Tenants](image)

**Figure 28. 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 29. Zcaler 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 our 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.

Figure 30. Slack incident with malicious attachments

The DLP policy creates a very broad guidelines to identify 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 fingerprinting), although they are integral pieces of a complete data protection solution.

For next steps to test the DLP SaaS functionality we will create a basic policy and apply it to our 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 our violation and eliminate false positives.

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

Let’s verify our DLP dictionary as next steps in the ZIA Admin Portal:

1. Select Administration > DLP Dictionaries and Engines.
2. Select DLP Dictionaries.
3. Identify and Select the Dictionary to be used (in this case SSN with dashes), then verify the data to search for.

![DLP Dictionaries & Engines]

**Figure 31. Creating a DLP Dictionary**
Creating a DLP Engine

To create the DLP engine using the verified DLP dictionary:

1. Select Administration > DLP Dictionaries and Engines.
2. Select the DLP Engines tab.
3. Select Add DLP Engine.

![DLP Dictionaries & Engines]

*Figure 32. 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# triggers a match.
4. Select ADD to add our next dictionary and repeat the process if desired.
5. Click Save.
6. Activate the configuration.

![Add DLP Engine](image)

Figure 33. The DLP engine wizard

NOTE
This policy triggers when we see the 4th 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

Let’s apply the engine to a DLP policy that is used for our Slack instance. Launch the DLP Rule Wizard to start the process.

2. Select Collaboration.
3. Select Add DLP Rule. This launches the Add DLP Rule wizard for detailed configuration.

![Image of Add DLP Rule wizard]

**Figure 34. Launch the SaaS DLP Policy Configuration wizard**
SaaS DLP Policy Details

The SaaS DLP policy is like all Zscaler policies in that you specify the detail on whom this policy, and to 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. We specify the DLP engine we have 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 below 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 **Message** or **Channel** types:

- 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 (at this time).

- **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 our 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 the last step.
6. Select Any for the Content Location.
7. Select High as a Severity to allow for identification for searches and tracking.
8. Save and Activate your configuration.

Figure 35. The SaaS DLP Policy Configuration wizard
The completed DLP rule ready to be applied with a scanning schedule.

![Policy Table]

**Figure 36.** The configured DLP policy
Configure a SaaS Malware Policy

To Launch the Malware Rule wizard:

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 by selecting the Exemption tab under Malware Detection. To add a malware policy, we specify the application, the SaaS tenant, and the status.

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

![Figure 37. Launch the Malware Policy Configuration wizard](image)
**SaaS Malware Policy Wizard**

Configure the **Malware Rule** wizard:

1. Select **Policy > SaaS Security API > 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.
7. Select **Action Report Malware**.
8. Click **Save**.

*Figure 38. The Malware Policy Configuration wizard*
**SaaS Malware Policy**

The completed SaaS Security malware policy for the Slack SaaS tenant is ready to be applied to our Slack instance with a scanning schedule.

**Activate** your configuration.

*Figure 39. The Completed Malware Policy Configuration wizard*
Configure the Scan Schedule Configuration

The final configuration step is to create a scan configuration. We specify the tenant the scan configuration applies to, any policies that are to be included in the scan, and what data to scan relative to a date. The options for Data to Scan are All Data, Date Created or Modified After, or New Data Only. For this deployment guide we select 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. Select Policy > SaaS Security API > 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.

**Figure 40. Create and enable a scan for the SaaS tenant**

**NOTE**
For a POV select New Data Only.
Start the Scan Schedule

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

Select the **Blue Arrow** on the Scan configuration to start SaaS API security on the Slack tenant.

The Status should say **Running** with a **Start Date** and a **Latest Scan Date**.

*Figure 41. 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 our SaaS partners. This gives visibility from a high-level and lets you manage individual logs and violations.

We will take a brief look at the tools, but for detailed information of the SaaS Security Analytics tools go to the Zscaler online documentation.

![SaaS Security Visibility](image)

*Figure 42. SaaS security visibility*
SaaS Assets and SaaS Assets Summary Report

The SaaS asset reports provide a summary or customizable reporting to have 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.

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

Select the three (3) **Total Incidents**. This opens **SaaS Security Insights** and the log data for each violation containing over 30 meta-data points of information.

![Summary reports](image)

*Figure 43. 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 datapoints 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

![SaaS Security Insights](image)

*Figure 44. SaaS security insight*
Zscaler Digital Exchange (ZDX) for Slack

ZDX is the missing link needed for our 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. Zscaler 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 45. 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.

![ZDX Admin Portal Login](image)

Figure 46. ZDX for user experience monitoring for Slack
Configure ZDX for Slack

Slack is not a predefined application in ZDX, but the configuration is very simple. 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. This brings up the New App wizard to enter a name and to enable the Slack application.

![Figure 47. Onboard the Slack app](image)

Copyright 2022, Zscaler, Inc.
To configure the Slack application for monitoring:

1. Add a **Name** for the Slack application.
2. Select **Enable** for **Status**.
3. Click **Save**.

![Add New Custom Application](image)

**Figure 48. Onboard the Slack app**

This defines the application. We need to create the web probe and the network probe for monitoring the application.
Configure ZDX Probes for Slack

Slack is defined as an application in ZDX. We must configure the probes. Select **Add New Probe** under the Slack Application we just created.

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

![ZDX Dashboard with applications list]

**Figure 49. 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. Select **5 minutes** as the **Run Frequency**.
6. Click **Next**.

*Figure 50. Configure the Slack probes*
1. Enter the **Slack Instance URL** for the **Destination URL**.
2. Click **Next**.

*Figure 51. Configuring the web probe*
Verify the web probe configuration and make any changes necessary and then submit the probe configuration. Click **Submit**.

*Figure 52. Configuring the web probe*
We see our completed web probe. Click Add New Probe. This again brings up the Probe Configuration wizard to create the cloud path probe to monitor the network.

---

**Figure 53. The completed web probe**
Configure Probes for Slack Monitoring

To enable monitoring for the new probe:

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

Figure 54. Create the cloud path probe
To enable Slack monitoring for the probe:

1. Select **ICMP** as the **Protocol**.
2. Enter the **Slack Instance URL** for your **Organization**.
3. Click **Next** to review the probe configuration.

Figure 55. Create the cloud path probe
Configure ZDX Probes for Slack

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

![Add New Probe](image)

**Figure 56. The completed cloud path probe**
Our completed Slack probes. **Activate** the changes to enable the probes.

*Figure 57. ZDX probes monitoring for Slack*
The ZDX Enabled Slack Application

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

Figure 58. Active Slack monitoring
Create an Alert for the Slack Service

As a final configuration step let’s create an alert to email us when there is service degradation of the Slack application. An alert can be configured for network, application, or device thresholds. An alert rule can be created 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, WIFI Signal Strength, Memory, Sent and Received Mbps

To create our alert on page fetch times:

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

*Figure 59. 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 a **Type** of application.
5. Click **Next**.

*Figure 60. The alert creation wizard, step one*
Step two of the Add New Alert Rule wizard:

1. Select Slack as the Application.
2. Select Slack as the Web Probe.
3. Click Next.

*Figure 61. The alert creation wizard, step two*
Step three of the Add New Alert Rule wizard creates the threshold that triggers the if exceeded. We can use multiple variables to eliminate false positive:

1. Select Page Fetch Time.
2. Select the time to exceed 5000ms (5 seconds).
3. Click Next.

![Figure 62. The alert creation wizard, step three](image-url)
Step four of the Add New Alert Rule wizard we adds throttling to control the scope of the alert, and defines the action. The action can also be defined as an authenticated webhook, which could be used to send the alert to a Slack Channel:

1. Enter 10 for the number of times the probe time must exceed our threshold.
2. Enter 10 and select Percentage for the Minimum Devices Impacted.
3. Select Email as the Delivery Method.
4. Enter the Alert Recipients email address (or multiple addresses separated by commas).

![Add New Alert Rule](image)

*Figure 63. The alert creation wizard, step four*
Our completed rule set for the alert. **Activate** the configuration.

*Figure 64. 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 our rule set. You can click on the Rule Name or click the eye to see more detail about the alert.

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

Figure 65. The alert
Alert Detail for the Slack Service

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

Figure 66. Alert details
The Sent Alert Email for the Slack Service

Below is the email alert that was sent to the recipients after our threshold was exceeded. Another email is sent when the threshold returns to normal values if the alert was an ongoing or continuous alert.

![Alert Email](image)

Figure 67. The alert email
Using ZDX: The Dashboard

The dashboard provides 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.

![Dashboard Screenshot]

*Figure 68. The dashboard*
Application Overview and Performance Detail

Selecting the Applications tile on the left of the ZDX Admin Portal brings up the Applications Overview, which shows all the configured applications and the individual ZDX score. Let’s look at the detail of our Slack application.

1. Select Applications.
2. Select the Slack App.

![Applications Overview](image)

Figure 69. 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.

![Application Performance Detail](image)

*Figure 70. Application performance detail*
The bottom portion of the app detail show the **Top Departments**, **Top Regions**, and **Top Zscaler Locations** using the application and the ZDX scores at a glance. We also see our probe data, with minimum, maximum, and average response times.

<table>
<thead>
<tr>
<th>TOP DEPARTMENTS</th>
<th>TOP REGIONS</th>
<th>TOP ZSCALER LOCATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZDX Score by Department</td>
<td>ZDX Score by Region</td>
<td>ZDX Score by Zscaler Location</td>
</tr>
<tr>
<td>70</td>
<td>70</td>
<td>70</td>
</tr>
</tbody>
</table>

![Application performance detail](image)

Figure 71. 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 our Slack users. The ZDX score is provided, and users can be selected by **Poor**, **Okay**, or a **Good** ZDX Score. You can get more detail on the user by clicking the name or the eye on the right. Select a User to bring up more detail.

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

![User Overview](image)

**Figure 72. User overview**
Slack User Detail

The User Detail shows an incredible amount of useful 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 users devices and provides the device specific detail (OS, Device Type, Network Information, etc....) by clicking on the device. The ZDX score is also displayed in a timeline, and detail of Page Fetch Times, Server Response, DNS Response, Probe Detail, and Device Health can all be seen from this page.

Select the User Device.

Figure 73. User detail
User Detail

The above is the End-to-End visibility of the Data Path the user is taking to get to the Slack SaaS service. 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.

Figure 74. User detail, end-to-end connection detail
Appendix A: Requesting Zscaler Support

Gather Support Information

You might sometimes need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

To contact Zscaler support, select Administration > Settings > and then click Company profile.

![Figure 75. Collecting details to open support case with Zscaler TAC](image-url)
**Save Company ID**

Copy the Company ID, as shown below.

**Company Profile**

![Company Profile Screenshot]

**Company ID**

zscalerthree.net-1008708

**Name**

- [Name Redacted] - Test Account

**Domains**

- [Domains Redacted]

**Address Line 1**

- [Address Line 1 Redacted]

**Address Line 2**

- [Address Line 2 Redacted]

*Figure 76. Company ID*
Enter Support Section

Now that you have our company ID, you can open a support ticket. Navigate to Dashboard > Support > Submit a Ticket.

![Submit ticket](image)

*Figure 77. Submit ticket*