# Table of Contents

## 1 Zscaler Data Protection and Digital Experience for Slack.com
   1.1 Overview .................................................................................................................. 7
   1.2 Zscaler Internet Access SaaS Identity Proxy .............................................................. 9
   1.3 Zscaler Internet Access Tenant Profiles and Tenancy Restrictions ......................... 10
   1.4 Zscaler Internet Access CASB Data and Malware Protection for Slack .................. 11
   1.5 Zscaler Digital Experience for the Slack User Experience ....................................... 13

## 2 Configure the SaaS Identity Proxy
   2.1 Configure the SaaS Identity Proxy .......................................................................... 15
   2.2 Configure the Zscaler Portal for the SaaS Identity Proxy ......................................... 16
   2.3 Configure Slack to use the Identity Proxy ............................................................... 18
   2.4 Configure Slack Single Sign-On .............................................................................. 19
   2.5 The Completed Slack Configuration ....................................................................... 21
   2.6 The Zscaler Active Identity Proxy Notification ....................................................... 23

## 3 Configuring Tenancy Restrictions for Slack
   3.1 Create a Tenant Profile ......................................................................................... 25
   3.2 Cloud Application Access Control Policy Wizard .................................................... 26

## 4 Configuring the Slack Tenant
   4.1 Adding the Slack Tenant ........................................................................................... 30
   4.2 SaaS Tenant Configuration Wizard ......................................................................... 31
   4.3 Configuring the Zscaler Tenant on Slack ................................................................. 33

## 5 Configuring Slack Policies and Scan Configuration
   5.1 Scoping the Policies and Remediation ..................................................................... 38
   5.2 Creating a DLP Policy ............................................................................................. 39
   5.3 Creating a DLP Engine ............................................................................................ 40
   5.4 Configure a SaaS DLP Policy .................................................................................. 42
   5.5 SaaS DLP Policy Details ....................................................................................... 43

## 6 Configure a SaaS Malware Policy
   6.1 SaaS Malware Policy Wizard .................................................................................. 47

## 7 Configure the Scan Schedule Configuration
   7.1 Start the Scan Schedule .......................................................................................... 50

## 8 Reporting and Visibility
   8.1 SaaS Assets and SaaS Assets Summary Report ....................................................... 52
   8.2 SaaS Security Insights ............................................................................................ 53

## 9 Zscaler Digital Exchange (ZDX) for Slack
   9.1 Configure ZDX for Slack ....................................................................................... 55
   9.2 Configure ZDX Probes for Slack ............................................................................ 58
   9.3 The ZDX Enabled Slack Application ...................................................................... 67
   9.4 Create an Alert for the Slack Service ..................................................................... 68
   9.5 The Triggered Alert for the Slack Service ............................................................... 74
   9.6 Alert Detail for the Slack Service ............................................................................ 75
   9.7 The Sent Alert Email for the Slack Service ............................................................ 76

## 10 Using ZDX – The Dashboard
........................................................................................................................................... 77
10.1 Application Overview and Performance Detail ................................................................. 78
10.2 User Overview and Detail ............................................................................................... 81

11  Appendix A: ................................................................................................................... 84
11.1 Zscaler Resources ........................................................................................................ 84
11.2 Slack.com Resources .................................................................................................... 84
# Terms and Acronyms

<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>
Zscaler / Slack Deployment Guide

About This Document

Zscaler Overview

Zscaler (Nasdaq: ZS), Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access, and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to 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, please visit www.zscaler.com or follow them on Twitter @zscaler.

Slack Overview

Slack, Inc. (NYSE: WORK), Slack, Inc. Slack is the collaboration hub that brings the right people, information, and tools together to get work done. From Fortune 100 companies to corner markets, millions of people around the world use Slack to connect their teams, unify their systems, and drive their business forward.

For more information on Slack, Inc., please visit www.Slack.com or follow them on Twitter@slackhq.
Audience

This guide is written for Zscaler Administrators, IT Administrators, and IT Analysts responsible for deploying, monitoring, and managing SaaS services in an Enterprise environment. For additional product and company resources, please refer to the Appendix section.

Document Authors

This document was authored by Solution Architects in the Zscaler Business Development / Technical Alliances team (aka “BD SA”). All solutions validated within this guide have been jointly reviewed by both vendors.

Software Revisions

This document was authored using Zscaler Internet Access 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 / Customers:** We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at:
  - partner-doc-support@zscaler.com

- **For Zscaler Employees:** If you are trying to reach the team that validated and authored the integrations contained within this document, please contact us at:
  - z-bd-sa@zscaler.com
1 Zscaler Data Protection and Digital Experience for Slack.com

Figure 1: Zscaler Solutions for Slack

1.1 Overview

Slack is one of the industry leaders that defined the utility of the Cloud, the advantages a SaaS application and the Cloud itself can provide to an Enterprise. SaaS services are popular because of the collaboration, ease of use and ease of sharing they enable globally, and our partner Slack.com helped define the cloud and is one of the industry collaboration leaders. But the downside of this ease of access and sharing is that they can present risk based on the client’s environment. It is impossible to train every employee to always use safety best practices with SaaS applications, and that 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 faced by organizations migrating to Cloud Services in today’s environment has been the ability to monitor the Users’ experience for the SaaS application. Especially in
today’s “Work from Anywhere” corporate infrastructures. Zscaler provides a complete Slack solution using our Zscaler Internet Services (ZIA) for Security of Slack and our Zscaler Digital Access Exchange Service (ZDX), for visibility of the Users’ experience.

ZIA provides Slack SaaS Security by using Access Control, Identity Control, SaaS Security, and our SaaS API to scan the Slack attachments for Malicious Content, and Data Loss Protection. 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 users’ device running the Zscaler Client Connector. These monitors provide detailed information on the Users Device, The Network Path to Slack, and the Slack SaaS performance itself. This information is invaluable to Operations when a user is experiencing issues with Slack and provides 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 Partners SaaS CRM service.

This guide will cover the following Zscaler Internet Access features for Slack Security, and the Zscaler Digital Experience for Slack performance visibility.

- SaaS Identity Proxy
- Tenant Restrictions
- SaaS Security Data Loss Protection (CASB)
- SaaS Security Malware Detection (CASB)
- Cloud Application Access Control
- Zscaler Digital Experience for Slack
1.2  Zscaler Internet Access 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 of all users of your organization Slack tenant.

When users try to access Slack with their corporate accounts without going through the Zscaler service, they will receive a Pop-up screen 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 has been verified, their traffic to and from Slack is secured and the user and the Slack data is inspected using Zscaler Internet Access.

Zscaler Internet Access 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. And 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.
1.3 Zscaler Internet Access 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 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.

ZIA Tenant Restrictions can be combined with Identity Proxy to provide extra security to Slack users by assuring the identity of the user, guaranteeing the users traffic is scanned and secured with the ZIA security features.
1.4 Zscaler Internet Access CASB Data and Malware Protection for Slack

The Zscaler CASB (SaaS Security API) is a feature set that is part of the Zscaler Internet Access security cloud and is designed specifically to help manage the risks of our Collaboration SaaS Partners, preventing data exposure and ensure compliance across the SaaS application.

The 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.

What makes our SaaS Security unique?

Data exposure reporting and remediation - Zscaler SaaS Security checks SaaS applications and cloud providers’ configurations and compares them to industry and organizational benchmarks to report on violations and automate remediation.

Threat identification and remediation - Zscaler SaaS Security checks SaaS applications for hidden threats being exchanged 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, and Malware Scanning capabilities for internet, data center, and SaaS applications, and ensures that public cloud applications are configured to prevent data exposure and maintain compliance. Zscaler also offers Zscaler Private Access for Zero-Trust access to internal applications, Zscaler Digital Experience for active monitoring of a Users’ experience to SaaS applications, and Zscaler Cloud Protection. Zscaler provides end to end connectivity, security, and visibility from any location on-prem or remote.

For more information, please see the resources in Appendix A: Zscaler Resources.
1.5 Zscaler Digital Experience for the Slack User Experience

![Zscaler Digital Exchange](image)

**Figure 5: Zscaler Internet Access Cloud SaaS Security API in Use with Slack**

With Zscaler Digital Experience (ZDX), you can now easily monitor your users' 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.

**What makes the Zscaler Digital Experience 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, please see the resources in *Appendix A: Zscaler Resources.*
2 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, inspection of traffic, and controlled access of all users of your organization Slack tenant.

When users try to access Slack with their corporate accounts without going through the Zscaler service, they will receive a Pop-up screen 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 has been verified their traffic to and from Slack is secured and the user and the Slack data is inspected using Zscaler Internet Access.

Zscaler Internet Access 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. And 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.
2.1 Configure the SaaS Identity Proxy

Figure 7: Configure The SaaS Identity Proxy

- Log into the Zscaler Tenant with Administrator Credentials
2.2 Configure the Zscaler Portal for the SaaS Identity Proxy

To configure Zscaler for the SaaS Identity Proxy.

- Select **Administration / Identity Proxy Settings**
- Then Select **Add Cloud Application** (This will open the configuration Wizard)
- Give the Cloud Application a **Name**
- Select **Enable**
- For Cloud Application Select **Slack**
- Set the ACS URL to **https://your-slack-instance.com/sso/saml**
- Set the Entity ID to **https://slack.com**
- Select the **SAML_2022** or Later Signing Certificate
- Select **Pass-through Zscaler Identity** for the Identity Transformation
- Select **Save**

![Figure 8: Configure the SaaS Identity Proxy Settings](image)
2.2.1 Configure the SaaS Identity Proxy

This is the completed Identity Proxy configuration on the Zscaler Tenant. We need to copy and save the Identity Proxy URL and the Issuer Entity ID for later in the Slack configuration. We also need to download and save the Signing Certificate.

- Copy and Save the **Identity Proxy URL**
- Copy and Save the Issuer **Entity ID**
- Download and Save the **Signing Certificate**
2.3 Configure Slack to use the Identity Proxy

Figure 10: Configure Slack for the Identity Proxy

- Log into the Slack Tenant with Administrator Credentials
- From your Organization Settings – Select Security
- Then Select SSO Settings
- Select Configure SSO

This will bring up the Slack SSO Configuration Wizard.
2.4 Configure Slack Single Sign-On

In the Configure SSO Wizard:

- Paste the Zscaler Identity Proxy URL into the SAML 2.0 Endpoint URL Field
- Paste the Zscaler Issuer Entity ID into the Identity Provider Issuer URL Field
- Set the Service Provider Issuer URL to “https://slack.com”
- Open the zscaler_certificate.cer file with a text editor, Copy and Paste the entire contents into the Public (X.509) Certificate Field
- Uncheck Sign the Response
- Select Test Configuration

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

![Figure 12: Slack SSO Wizard Confirmation](image)

If the configuration tests correctly you will get confirmation that “Everything looks good!” If there is a problem with the configuration you will either get a “Glitch Reported” or a failure and will have to start over from the beginning.

- Select **Confirm Update** to activate the configuration
2.5 The Completed Slack Configuration

Figure 13: The Completed Identity Provider Configuration

The completed SSO configuration.
2.5.1 User Informational Email

![Email Informing Users](image)

**Figure 14: Email Informing Users**

Users will receive an email stating they will now need to use their Single Sign-On credentials.
2.6 The Zscaler Active Identity Proxy Notification

![Image of the Active Authentication Proxy notification]

**Figure 15: The Active Authentication Proxy**

This is the Notification a Slack user will receive if they are trying to log into Slack without going through Zscaler. When your user traffic is going through Zscaler they will be able to access Slack as usual.
3 Configuring Tenancy Restrictions for Slack

The Zscaler Internet Access security cloud is a fully integrated cloud-based security stack that sits in line between users and the internet, inspecting all traffic, including SSL, flowing between them. 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 referred to as out-of-band CASB for data-at-rest, Zscaler Cloud Application security is referred to as 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’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.
3.1 Create a Tenant Profile

To create our tenant profile to allow our specific users please follow the below steps.

- Sign into your organizations ZIA UI with Administrator Credentials
- Select Administration
- Select Tenant Profile
- Select Add Tenant Profile

This will launch the Add Tenant Profile Wizard to create the profile.

- Select Slack as the Cloud Application
- Provide a Name for the Tenant Profile
- Provide Org ID or Workspace ID for the Workspace ID
- Add the Allowed Tenants by Org ID or Workspace ID
- Save the configuration
### 3.2 Cloud Application Access Control Policy Wizard

To create our Cloud Application policy to allow users to our specific Tenant please follow the below steps.

- Select **Policy / URL & App Control / The Cloud App Control Policy Tab**
- Select **Add** and from the pull down select **Collaboration & Online Meetings**
- Set the **Rule Order** to ensure execution of the policy
- Select **Slack** for the Cloud Application
- Select **Allow Access**
- Select the **Slack Tenant Profile** we just created
- Select **Save** to save our changes

**NOTE:** SSL Inspection is required for the feature to work. Please make sure Slack traffic is being inspected.
3.2.1 Completed Tenant Restrictions

Figure 19: Completed Cloud Application Policy with the Tenant Profile

Our completed Access Policies.

- Activate the Policy additions
### 3.2.2 Tenant Restriction Alerts

![Alerts when accessing blocked Slack tenants](image)

**Figure 20: Alerts when accessing blocked Slack tenants**

Users who now try to access the Slack application through either a browser or the Application who do not have permission will receive an alert and the event will be logged.
4 Configuring the Slack Tenant

Figure 21: Zscaler Internet Access Admin Console

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 tenant with Admin credentials. Your Zscaler Cloud Instance may be different from the example. The current Zscaler Internet Access clouds include zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscloud.net, zscalerbeta.net, and zscalergov.net.
4.1 Adding the Slack Tenant

To launch the SaaS Application Tenants Wizard for the ZIA Admin Interface.

- Select **Administration**
- Select **SaaS Application Tenants**
- On the SaaS Applications Tenants page Select “**Add SaaS Application Tenant**”
4.2 SaaS Tenant Configuration Wizard

Figure 23: The SaaS Tenant Configuration Wizard

To start the Wizard select Add SaaS Application Tenant. The above Wizard will then appear. Select the Slack Tile under popular applications to move to the next step in the Wizard.

- Select **Add SaaS Application Tenant** on the Tenant page
- Select the **Slack tile** on the Wizard
4.2.1 SaaS Tenant Configuration Wizard

Figure 24: Open the Slack Tenant

Give the Slack tenant a name. This will be the name that will be selected when assigning a policy for the Zscaler security features.

- Enter a **Name** for the Tenant Name
- Enter an **Email ID** for the Slack Admin
- Right Click the “Provide Admin Credentials” link, and open the link in a new Tab.
- Open a new browser tab and login to your Slack Tenant with Admin role credentials
4.3 Configuring the Zscaler Tenant on Slack

Figure 25: Allow Zscaler Access to the Slack Tenant

To configure the Zscaler Tenant from your Slack Admin account.

- **Log in to Slack** with Administrator Credentials
- **Select Allow** to enable communication between the cloud platforms

We must now approve the Zscaler application on Slack.
4.3.1 Configuring the Zscaler Tenant on Slack

![Figure 26: Approve the Zscaler Application](image)

We need to approve the Zscaler application to allow API calls to be made from Zscaler to Slack.

- As an Administrator Select **Manage Organization**
- Under Organization Select **Apps**
- Select **Approve** for the Zscaler Application

Once the Zscaler Application is approved as seen above, you will need to go back to the Zscaler UI and execute the next step of the installation.
4.3.2 Configuring the Zscaler Tenant on Slack

Figure 27: Authorize Access to the Slack Bot

In the Zscaler Tenant setup select the Provide Admin Credentials link on Step 5. After you have provided the Admin credentials the Tenant configuration will be completed.

- Right Click the **Provide Admin Credentials** link on Step 5, and open the link in a new Tab.
- **Save and Activate** the Configuration

This completes the creation of the Slack Tenant. We will now be able to apply CASB controls on our Slack instance using Zscaler Data and Malware protect.
4.3.3 The Active Slack Tenant

Check that the Status of Slack Tenant is Active.

- Select **Administration**
- Select **SaaS Application Tenants**
5 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.
5.1 Scoping the Policies and Remediation

Zscaler SaaS Security scans Slack file attachments. For this Deployment Guide, we will configure 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 has been 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.

For our DLP policy we are going to create a very broad DLP policy to identify a spreadsheet with a list of US Social Security Numbers. Data Loss Protection 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, 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 will not 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 we will create a basic policy and apply it to our Slack tenant. If you already have DLP policies created skip ahead to Section 4.
5.2 Creating a DLP Policy

![Figure 31: Creating a DLP Dictionary](image)

The procedures for creating a DLP policy are straightforward. Create a custom dictionary, or use the available dictionaries, to identify the data the scan is going to look for. Then an engine is created which 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.

A SaaS Security DLP policy is then created which allows us to specify the detail about where, when, the action taken, and whom to inform about Violations. Finally, the DLP policy is then applied to our Slack tenant. Let’s verify our DLP dictionary as next steps in the ZIA UI.

- Select **Administration**
- Select **DLP Dictionaries and Engines**
- Select **DLP Dictionaries**
- Identify and **Select the Dictionary to be used** (In this case SSN with Dashes), then verify the Data to Search for.
5.3 Creating a DLP Engine

To create the DLP engine using the verified DLP dictionary:

- Select **Administration**
- Select **DLP Dictionaries and Engines**
- Select the **DLP Engines TAB**
- Select **Add DLP Engine**

**Figure 32: Creating a DLP Engine**
5.3.1 Creating a DLP Engine

- Give the DLP Engine a **Name**
- In the Engine Builder under Expression select the verified **Dictionary**
- 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 forth unique SSN# will trigger a match.
- Select **ADD** to add our next dictionary and repeat the process if desired.
- Select **Save** to save the configuration
- **Activate** the Configuration

**Figure 33: The DLP Engine Wizard**

Note: This policy will trigger when we see the 4th Social Security Number. Again, this in a demonstration and the criteria is too general to be a production DLP rule.
5.4 Configure a SaaS DLP Policy

Figure 34: Launch the SaaS DLP Policy Configuration Wizard

Now let’s apply the engine to a DLP policy that will be used for our Slack instance. Launch the DLP Rule Wizard to start the process.

- Select **Policy / SaaS Security API / Data Loss Prevention**
- Select **Collaboration**
- Select **Add DLP Rule**

This will launch the Add DLP Rule Wizard for detailed configuration. See the detail of the DLP policy on the following pages.
5.5 SaaS DLP Policy Details

The SaaS DLP Policy is like all Zscaler Policies where you will specify the detail on whom this policy, and to what data this policy will apply to. You will specify the rule order if you have multiple DLP policies which are processed in an ascending manner. The first rule that matches will be the applied rule. We will 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 below Message or Channel type.

- 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 will be reported in the Zscaler SaaS Analytics and Alerts only at this time.

- **Report Incident Only**: The rule reports the incident only and makes no changes to the file’s collaboration scope.
5.5.1 Configure a SaaS DLP Policy

Figure 35: The SaaS DLP Policy Configuration Wizard

To Finish our DLP Policy

- Specify the **Rule order** for Processing (The first rule matched will be executed)
- **Name** the Rule
- **Enable** the Rule Status
- Select the **Slack Application Tenant**
- Select the **DLP Engine** created in the last step
- Select **Any** for the Content Location
- Select **High** as a Severity to allow for identification for searches and tracking
- **Save and Activate** your configuration
5.5.2 Configure a SaaS DLP Policy

Figure 36: The Configure DLP Policy

The completed DLP rule ready to be applied with a scanning schedule.
6 Configure a SaaS Malware Policy

To Launch the Malware Rule Wizard.

- Select Policy / SaaS Security API / Malware Detection
- Select Collaboration
- Select Add Malware Detection Rule

The SaaS Malware Detection Policy is an all-encompassing policy and all files in the Tenant will be scanned unless removed from the scope by specifying any exemptions by selecting the Exemption Tab under Malware Detection. To add a malware policy, we will specify the Application, the SaaS Tenant, and the Status.

The Action for Slack is limited to Report Malware only.
6.1 SaaS Malware Policy Wizard

Configure the Malware Rule Wizard.

- Select Policy / SaaS Security API / Malware Detection
- Select Collaboration
- Select Add Malware Detection Rule
- Under Criteria Select Slack as the Application
- Select the Slack Application Tenant to apply the policy
- Select Enabled for Status
- Select Action Report Malware
- Select Save
6.1.1 SaaS Malware Policy

The completed SaaS Security Malware policy for the Slack SaaS Tenant ready to be applied to our Slack instance with a Scanning Schedule.

- Activate your configuration
7 Configure the Scan Schedule Configuration

![Diagram of Zscaler dashboard with options to configure scan schedules and policies]

**Figure 40: Create and Enable a Scan for the SaaS Tenant**

The final configuration step is to create a Scan Configuration. We will 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 will select All Data. **However, if this is a POV or a Trial, the only option available will be New Data Only.** To add a Scan Schedule:

- Select **Policy / SaaS Security API / Scan Configuration / Add Scan Schedule**
- Select the **Slack** SaaS Tenant for the SaaS Application Tenant
- Select the **Data Loss Policy and the Malware Policy Created** in Prior Steps
- Select **All Data**
- Select **Save** to save the Scan Schedule and Activate the configuration

**NOTE:** For a POV Select New Data Only
7.1 Start the Scan Schedule

Once the Schedule has been 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 now say “Running” with a Start Date and a Latest Scan Date.
8 Reporting and Visibility

Figure 42: SaaS Security 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. For our SaaS partners Zscaler provides Reports and SaaS Security Insights. This provides visibility from a high-level overview to management of the individual logs and violations.

We will take a brief look at the tools, but for detailed information of the SaaS Security Analytics tools visit the Zscaler online documentation.
8.1 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 above is the SaaS Assets Summary Report, which 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 above, 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 3 Total Violations next to Slack to pivot to SaaS Security Insights

This will open SaaS Security Insights and the log data for each violation containing over 30 meta-data points of information.
8.2 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
9  Zscaler Digital Exchange (ZDX) for Slack

![ZDX Diagram]

Figure 45: ZDX for User Experience Monitoring for Slack

ZDX has become the missing link needed for our customers and their SaaS applications. As applications move to the cloud, the Internet becomes your new transport network. With users working from anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. Slack is no exception to this and Zscaler ZDX provides visibility into the client’s experience using Slack. ZDX utilizes the Zscaler Endpoint 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 being enabled.

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.
9.1 Configure ZDX for Slack

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

- Log Into your organizations ZDX portal
9.1.1 Configure ZDX for Slack

Figure 47: Onboard the Slack App

Slack is not a predefined application in ZDX, however the configuration is very simple. To configure the Slack application for monitoring. We configure Slack as an application and add a Web Probe and a Network Probe.

- Select Configuration
- Select Applications
- Select Add New Custom Application

This will bring up the New App Wizard to enter a name and to enable the Slack Application.
9.1.2 Configure ZDX for Slack

Figure 48: Onboard the Slack App

To configure the Slack application for monitoring.

- Add a **Name** for the Slack Application.
- Select **Enable** for Status
- Select **Save**

This will define the Application. We now need to create the Web Probe and the Network Probe for monitoring the application.
9.2 Configure ZDX Probes for Slack

Slack is now defined as an application in ZDX. We must now configure the probes.

- Select Add New Probe under the Slack Application we just created

This will launch the Probe Wizard to create our probes for monitoring the Slack application.
9.2.1 Configure ZDX Probes for Slack

For the Web Probe.

- Give the Web Probe a logical **Name**
- Select **Enable** for Status
- Select **Slack** as the Application
- Select **Web** as a Probe type
- Select **5 minutes** as the Run Frequency
- Select **Next**
9.2.2 Configure ZDX Probes for Slack

Figure 51: Configuring the Web Probe

- Enter the Slack Instance URL for the Destination URL
- Select Next
9.2.3 Configure ZDX Probes for Slack

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

- Select Submit
9.2.4 Configure ZDX Probes for Slack

We now see our completed Web Probe. Select Add New Probe to configure our Network Probe.

- Select **Add New Probe**

This will again bring up the Probe Configuration Wizard to create the Cloud Path Probe to monitor the Network.
9.2.5 Configure Probes for Slack Monitoring

Figure 54: Create the Cloud Path Probe

- Give the probe an intuitive **Name**
- Verify the probe is **Enabled**
- Select **Cloud Path** as a Probe Type
- For Follow Web Probe Select **Slack**
- Select **Next** to move to the Probe detail
9.2.6 Configure Probes for Slack Monitoring

Figure 55: Create the Cloud Path Probe

- Select ICMP as the Protocol
- Enter the Slack Instance URL for your Organization
- Select Next to review the probe configuration
9.2.7 Configure ZDX Probes for Slack

**Figure 56: The Completed Cloud Path Probe**

Review the probe configuration and then Submit and Activate your configuration.

- Select **Submit**
9.2.8 Configure ZDX Probes for Slack

Our completed Slack probes.

- **Activate** the Changes to enable the probes
9.3 The ZDX Enabled Slack Application

The Slack application monitoring has now been activated and our Probes will begin from all our users that are using the Zscaler Client Connector (ZCC). The above figure shows ZCC running the Digital Experience and the Cloud Service is Enabled and Active.
9.4 Create an Alert for the Slack Service

![Alerts Rules](image)

Figure 59: Creating an Alert

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 below 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.

- Select **Alerts**
- Select **Rules**
- Select **Add New Alert Rule**
9.4.1 Create an Alert for the Slack Service

![Add New Alert Rule](image)

**Figure 60: The Alert Creation Wizard**

Step One of the rule Wizard.

- **Name** the Rule
- Select **Enable** Under Status
- Give the Alert an appropriate **Severity**
- Select a Type of **Application**
- Select **Next**
9.4.2 Create an Alert for the Slack Service

Figure 61: The Alert Creation Wizard

Step Two of the rule Wizard.

- Select Slack as the application
- Select Slack as the Web Probe
- Select Next
9.4.3  Create an Alert for the Slack Service

Step Three of the rule Wizard we will create the criteria for which the Alert will trigger if the threshold is exceeded. We can use multiple variables to eliminate false positive.

- Select Page Fetch Time
- Select the time to exceed 5000ms (5 Seconds)
- Select Next
9.4.4 Create an Alert for the Slack Service

Step Four of the rule Wizard we will add Throttling to control the scope of the Alert. We will then define the Action as Email. The action can also be defined as an authenticated Webhook, which could be used to send the Alert to a Slack Channel.

- Enter 10 for the number of times the Probe time must exceed our threshold
- Enter 10 and Select Percent for the Minimum Number of Devices that must be impacted
- Select Email as the Delivery Method
- Enter the Alert Recipients Email Address or multiple addresses separated by commas
9.4.5 Create an Alert for the Slack Service

Figure 64: The Completed Alert Rule Set

Our Completed Rule Set for the Alert.

- **Activate** the Configuration
9.5 The Triggered Alert for the Slack Service

Figure 65: The Alert

The above is the triggered alert generated by our Threshold Settings in our Rule Set being exceeded. You can click on the Rule Name or click the eye to see more detail about the Alert.

- Select Alerts
- Select the Rule Name
9.6 Alert Detail for the Slack Service

Figure 66: Alert Details

The above is the alert detail for our triggered Slack alert showing impacted user and devices, impact location, and threshold details.
9.7 The Sent Alert Email for the Slack Service

The above is the Email Alert that was sent to the recipients once our threshold was exceeded. Another email will be sent when the threshold returns to normal values if the alert was an ongoing or continuous alert.

Figure 67: The Alert Email
10 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 will also show you any locations globally that may be having issues.
10.1 Application Overview and Performance Detail

Selecting the Applications Tile on the left of the UI will bring up the Applications Overview and will show all the configured applications and the individual ZDX score. Let’s look at the detail of our Slack application.

- Select Applications
- Select the Slack App
10.1.1 Slack Application Performance Detail

The top portion of the application detail shows a historical view of the ZDX score and the Page Fetch Time. The failure of the page fetch time indicates a service loss of the Slack service itself.
10.1.2 Slack Application Performance Detail

The bottom portion of the App detail show the Top Zscaler Locations, Top Cities, and the Top Departments using the Application and the ZDX Scores at a glance. We also see our probe data, with minimum, maximum, and average response times.

Figure 71: Application Performance Detail
10.2 User Overview and Detail

The User Overview will provide 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.

- Select Users
- Select the Slack App
- Select Apply
10.2.1 Slack User Detail

The User Detail will show 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 will provide the Users Devices and will provide 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
10.2.2 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.
11 Appendix A:

11.1 Zscaler Resources

Zscaler Internet Access (ZIA)
https://www.zscaler.com/products/zscaler-internet-access

Adding SaaS Application Tenant
https://help.zscaler.com/zia/adding-saas-application-tenants

About SaaS Application Tenant
https://help.zscaler.com/zia/about-saas-application-tenants

SaaS Security API DLP Policy

About Data Loss Prevention

About DLP Dictionaries

About DLP Engines

SaaS Security Insights

SaaS Posture Security

Cloud Application Access Control
https://help.zscaler.com/zia/about-cloud-app-control

SaaS Identity Proxy

ZDX
https://help.zscaler.com/zdx

ZDX Predefined Applications
https://help.zscaler.com/zdx/predefined-applications-zdx

11.2 Slack.com Resources

About Slack
https://www.slack.com/company.html

Slack Product Documentation
https://slack.com/help

Slack Community
https://slackcommunity.com

Slack Resources
https://slack.com/resources