ZSCALER AND BOX DEPLOYMENT GUIDE

JANUARY 2021, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

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

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

Trademark Notice

About This Document

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

Zscaler Overview

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

Box Overview

Box (NYSE: **BOX**) is a Leader in SaaS Cloud Content Platforms based in Redwood City, California. The company focuses on cloud content management and file sharing services for businesses. Official clients and apps are available for Windows, macOS, and several mobile platforms. Box was founded in 2005. To learn more, refer to **Box's website**.

Audience

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

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

Software Versions

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

Request for Comments

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

Zscaler and Box Introduction

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

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

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via 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, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZDX

Zscaler Digital Experience (ZDX) monitors your users' digital experiences. ZDX provides visibility across the complete user-to-cloud app experience and quickly isolates issues. By combining the Zscaler Client Connector endpoint agent with Zscaler's global cloud footprint, ZDX provides you with innovative and unprecedented end-to-end visibility, regardless of network or location.

Zscaler Resources

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

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

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

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

Box Intelligent Content Cloud Overview

Box is the Intelligent Content Cloud—the only intelligent content management platform that enables you to succeed across the full spectrum of use cases today's businesses require. Box delivers modern, easy-to-use collaboration and workflow tools, advanced data protection and compliance, and enterprise-grade AI—all built on a flexible, interoperable platform in the cloud. Box is the best place to start your intelligent content management journey.

Box Resources

The following table contains links to Box support resources.

Name	Definition
Box Support	Support services for Box products.
Box Product Guides	Online help for Box products.
Box Guidance Services	Online guidance for Box services and products.

Zscaler SaaS Security API for Box

SaaS applications that provide content management and file sharing services are popular because of the collaboration, ease of use, and sharing they enable. Box.com is one of the industry leaders. But the downside of the ease of access is risk based on the client's environment. It is impossible to train every employee to use best security practices with SaaS applications at all times, which can lead to costly mistakes for the organization. Risks associated with accidental data exposure, malicious intent, and compliance violations can force companies to restrict or prevent use of business tools.

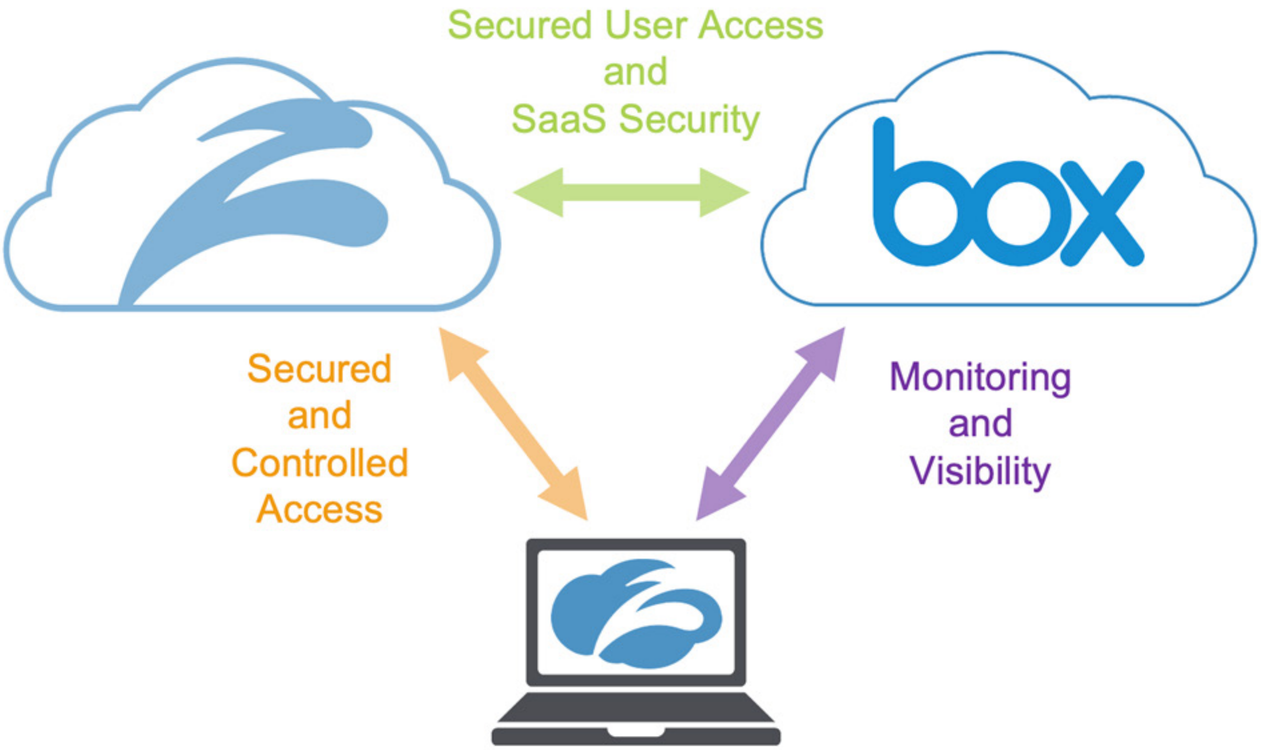


Figure 1. Zscaler Solution for Box

Another challenge organizations face when migrating to Cloud Services in today's environment is monitoring the user experience for the SaaS applications, especially in today's work from anywhere corporate infrastructures. Zscaler provides a complete Box solution using ZIA and ZDX.

ZIA provides SaaS using SaaS Security API to scan the Box data stores for malicious content and data protection. ZIA also provides complete security for clients whether they are in the corporate office or their home office.

The ZDX service provides a user-specific experience monitoring and providing visibility to the Box service to help organizations address any experience concerns or challenges. ZDX has preconfigured monitors that provide performance monitoring and measurements from the user's device running the Zscaler Client Connector. These monitors provide detailed information on the user device, the network path to Box, and the Box SaaS performance itself.

Both ZIA SaaS and ZDX SaaS monitoring operate as separate standalone 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.

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

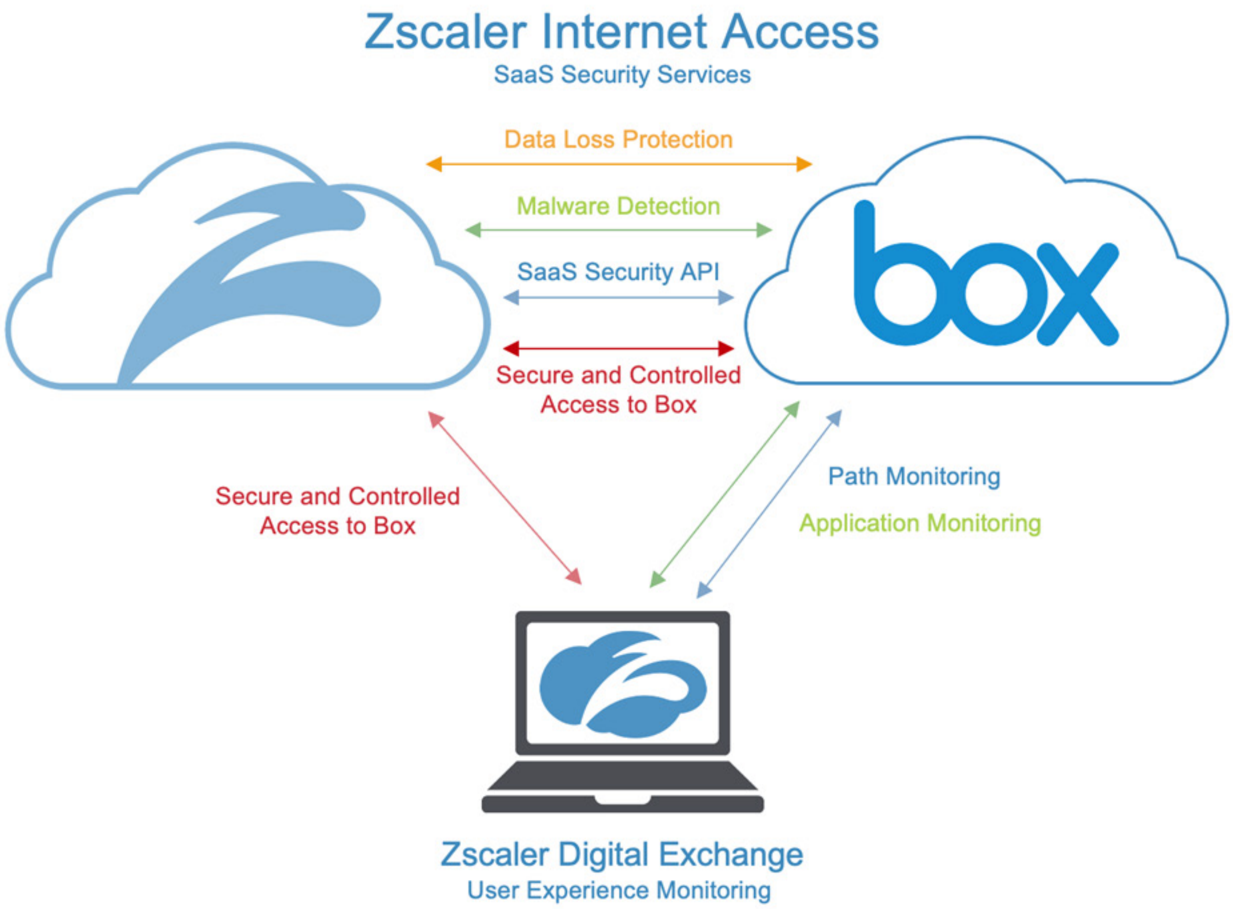


Figure 2. ZIA Cloud SaaS Security API in Use with Box

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 the 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 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 user's experience to SaaS applications, and Zscaler Cloud Protection. Zscaler provides end-to-end connectivity, security, and visibility from any location on-premises or remote.

ZDX for the Box User Experience

With 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. By combining the Zscaler Client Connector endpoint agent with Zscaler's global cloud footprint, ZDX provides you with innovative and unprecedented end-to-end visibility, regardless of network or location.

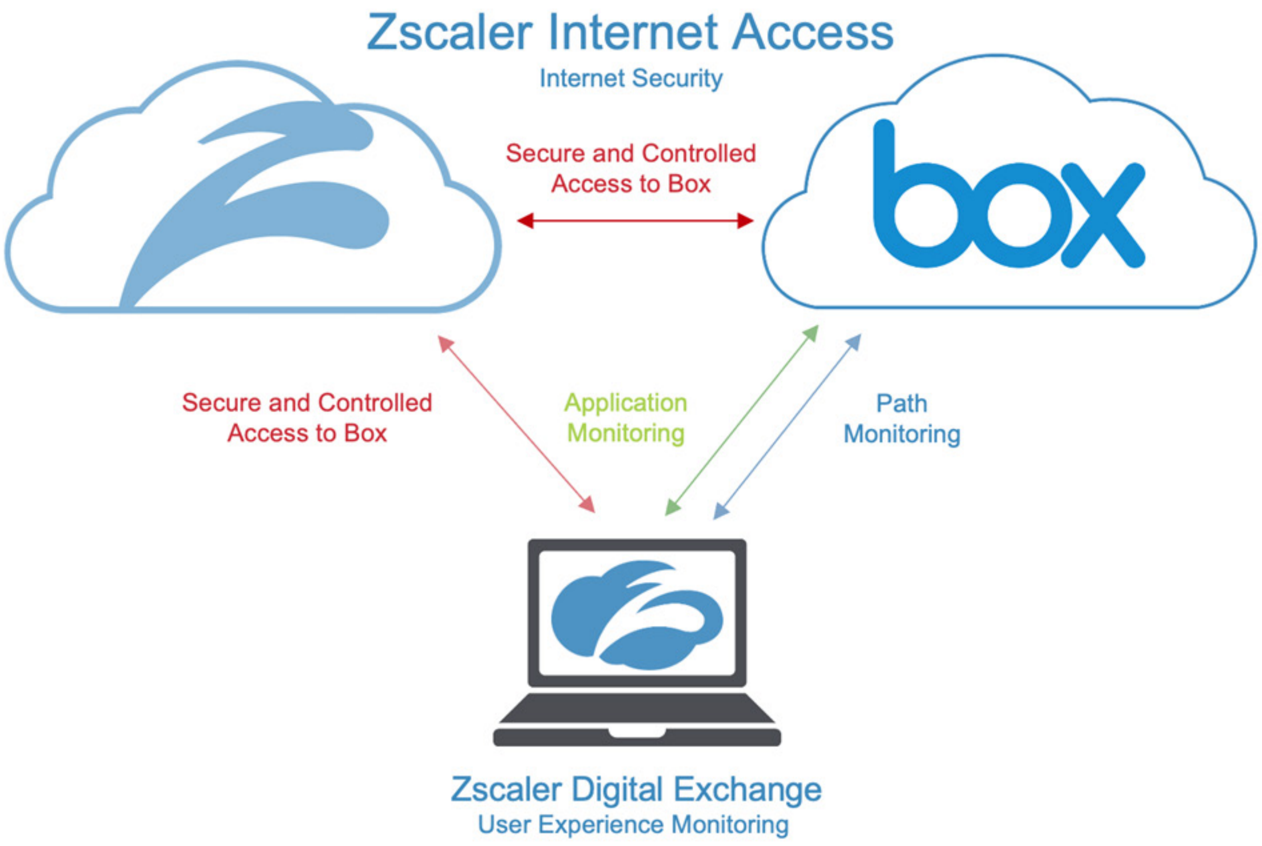


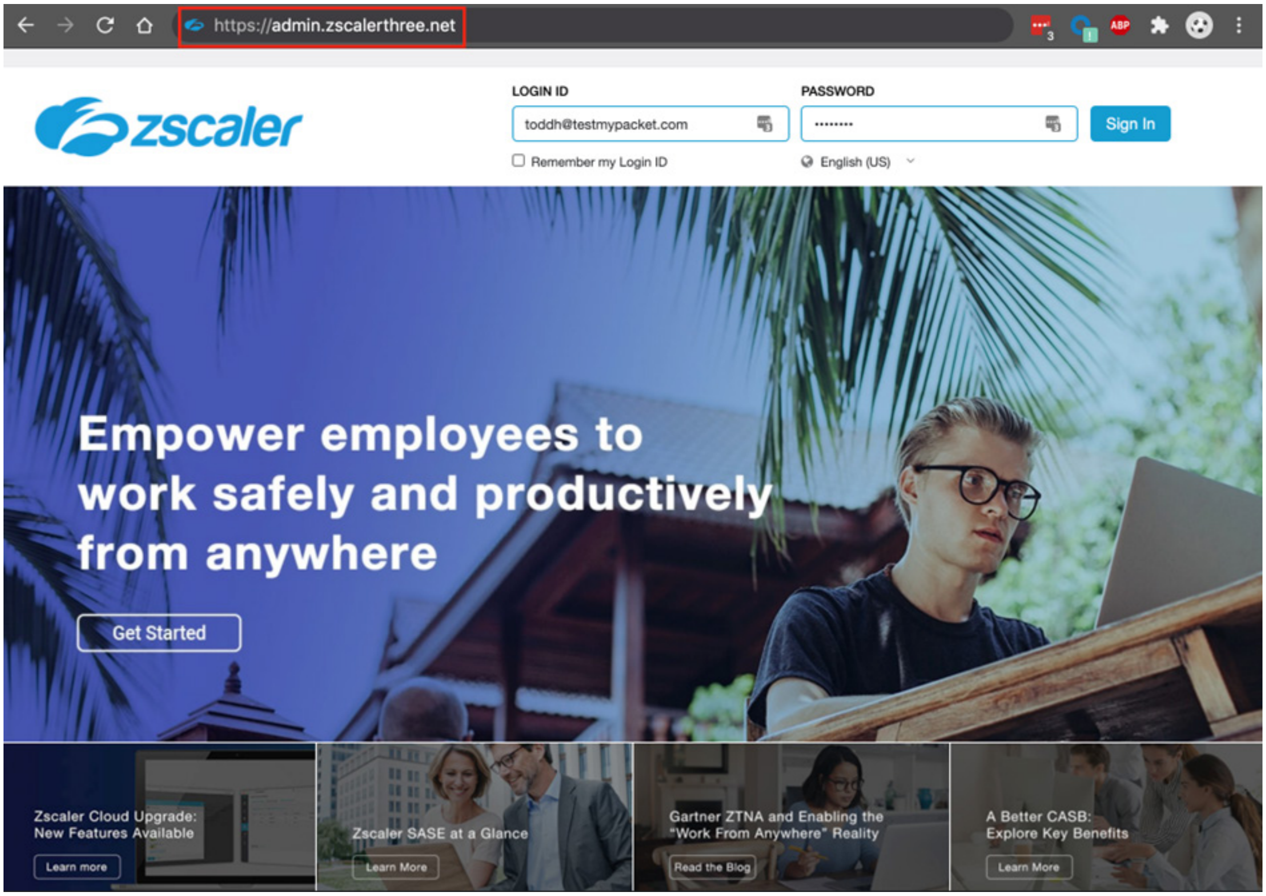
Figure 3. ZDX in Use with Box

What Makes ZDX Unique?

- End user device performance: 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.
- Cloud path performance: 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.
- 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.

Configuring Zscaler SaaS for Box

The configuration to enable the SaaS service builds on itself. Log in to the ZIA Admin Portal to start the configuration process.



https://admin.zscalerthree.net

LOGIN ID: toddh@testmypacket.com

PASSWORD: ••••••••

□ Remember my Login ID

English (US)

zscaler
Sign In
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More

Figure 4. Creating an Azure Active Directory IdP

You must complete the following steps:

- Configuring the Box Tenant on Zscaler
- Configuring the Zscaler Tenant on Box
- Configure a SaaS DLP Policy
- Configure a SaaS Malware Policy
- Configure the Scan Schedule Configuration

Configuring the Zscaler and the Box Tenant

Configure the Box SaaS Tenant under Administration in the ZIA Admin Portal.

1. Select **Administration**.
2. Select **SaaS Application Tenants**.

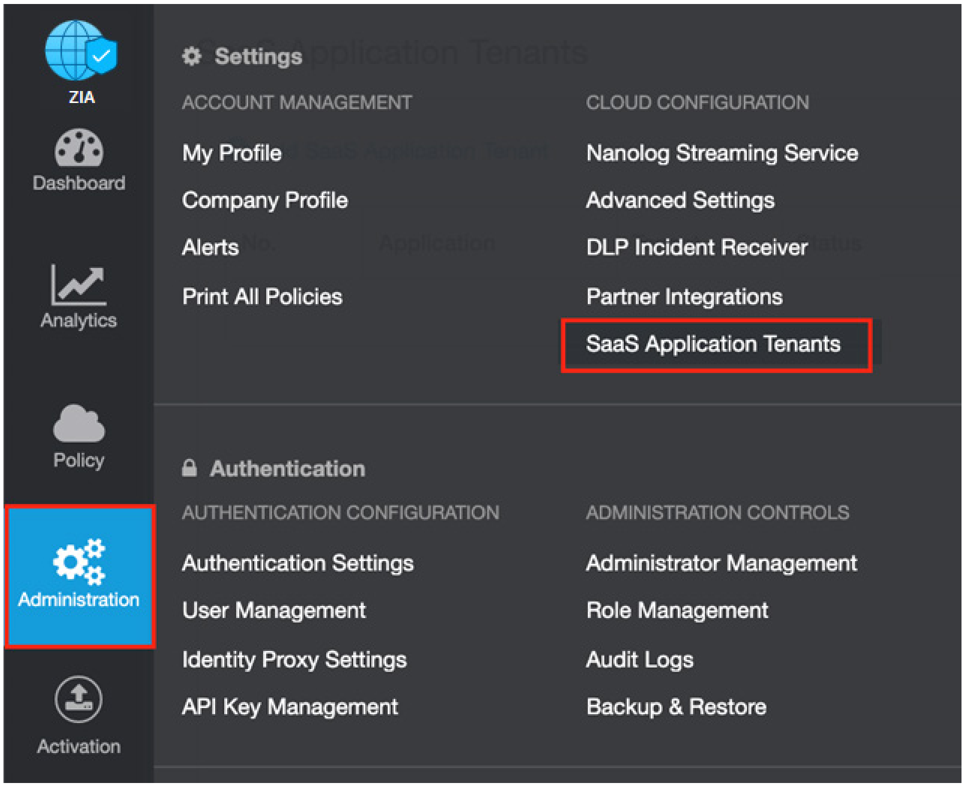
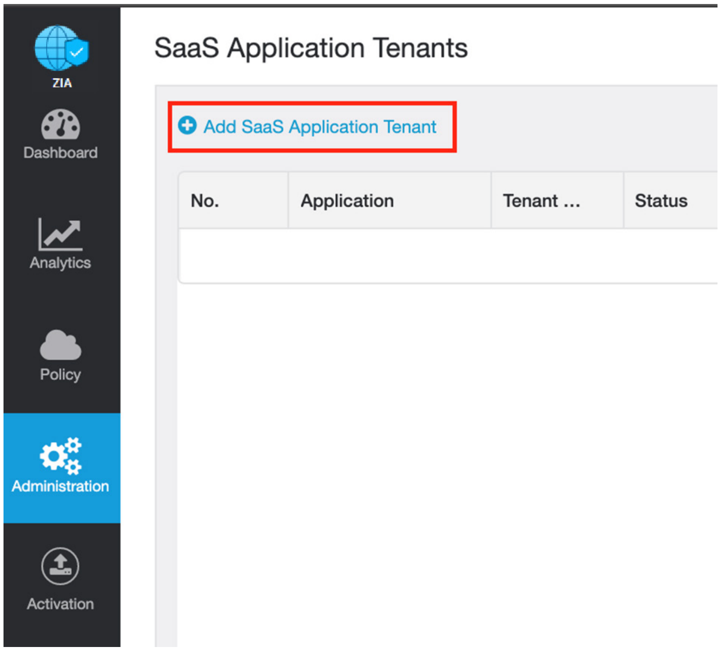


Figure 5. Adding a Box Tenant

Configuring the Box Tenant on Zscaler

Add the SaaS Application Tenant. Select **Add SaaS Application Tenant**.



SaaS Application Tenants

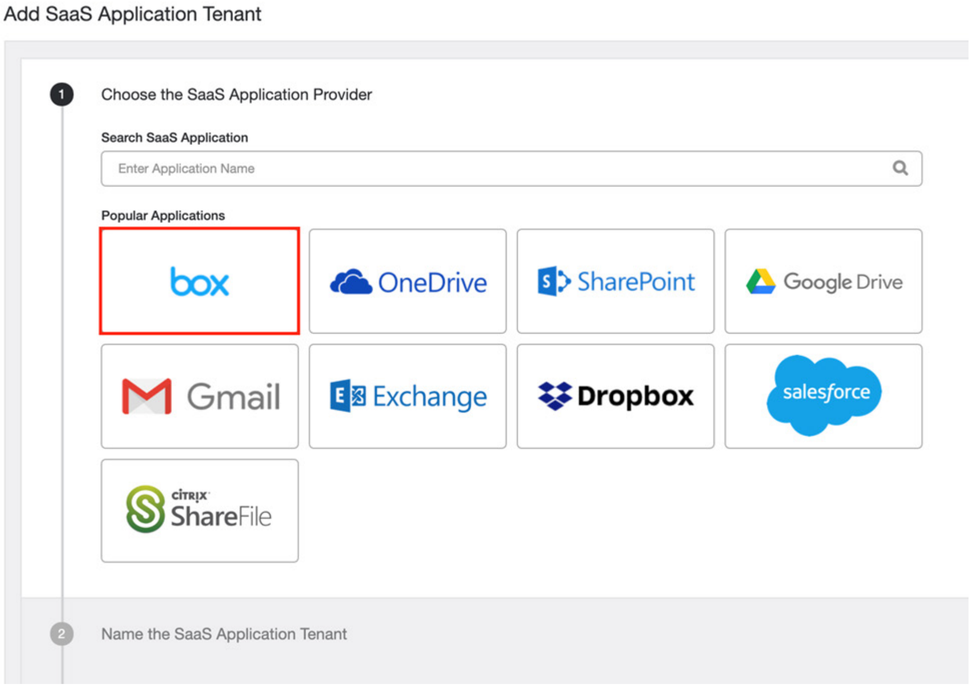
Add SaaS Application Tenant

No.	Application	Tenant ...	Status

Figure 6. Adding an Application Tenant

SaaS Tenant Configuration wizard

Select the **Box** tile under **Popular Applications** to move to the next step in the wizard.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

Search SaaS Application: Enter Application Name

Popular Applications

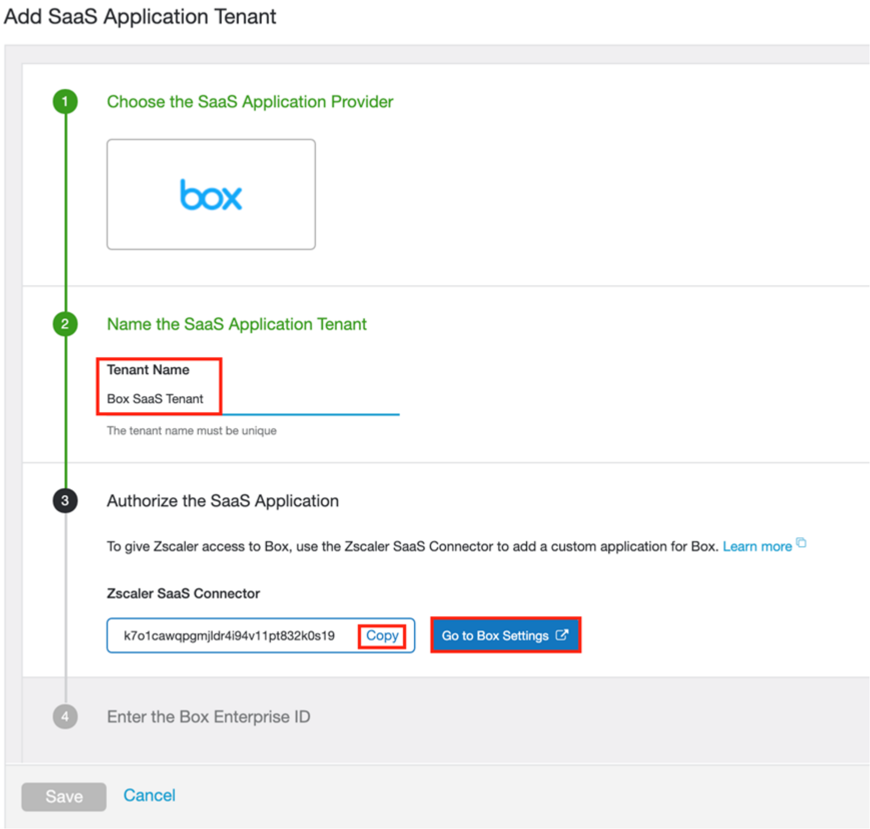
2 Name the SaaS Application Tenant

Figure 7. The SaaS Tenant configuration wizard

SaaS Tenant Configuration wizard

Give the Box tenant a name. This is the tenant's name that is selected when assigning a policy for the Zscaler security features.

1. Enter a name for the **Tenant Name**.
2. Copy the **Zscaler SaaS Connector** for next steps.
3. Select **Go to Box Settings** to open your Box portal.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

2 Name the SaaS Application Tenant

Tenant Name: Box SaaS Tenant

The tenant name must be unique

3 Authorize the SaaS Application

To give Zscaler access to Box, use the Zscaler SaaS Connector to add a custom application for Box. Learn more

Zscaler SaaS Connector: k7o1cawqpgmjldr4i94v11pt832k0s19

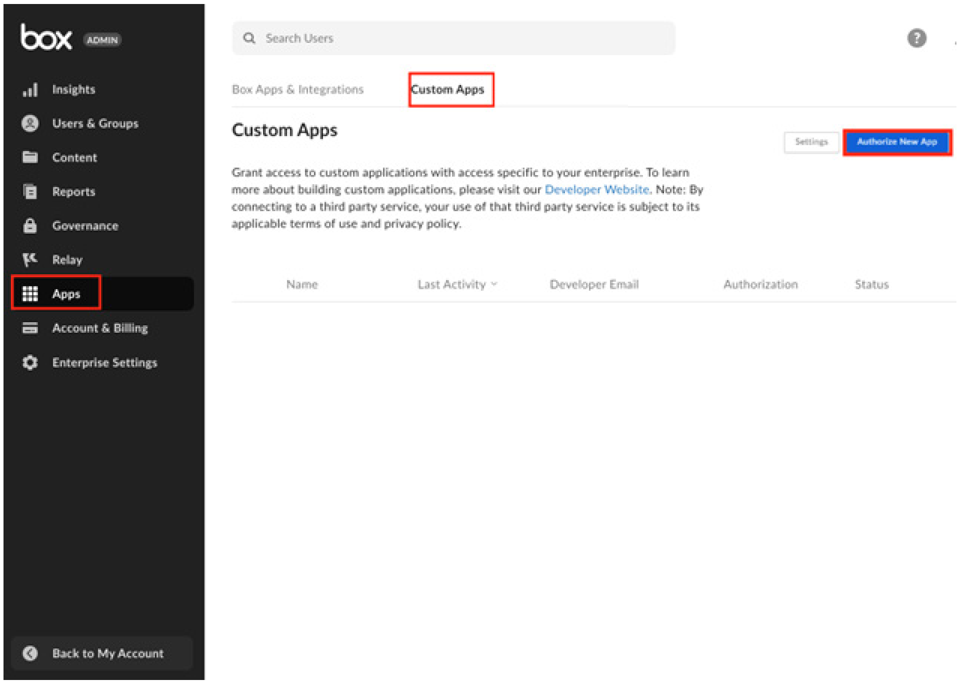
4 Enter the Box Enterprise ID

Figure 8. Open the Box Tenant

Configuring the Zscaler Tenant on Box

To configure the Zscaler Tenant from your Box Admin account:

1. Select **Apps**.
2. Select **Custom Apps**.
3. Select **Authorize New App**.



Custom Apps

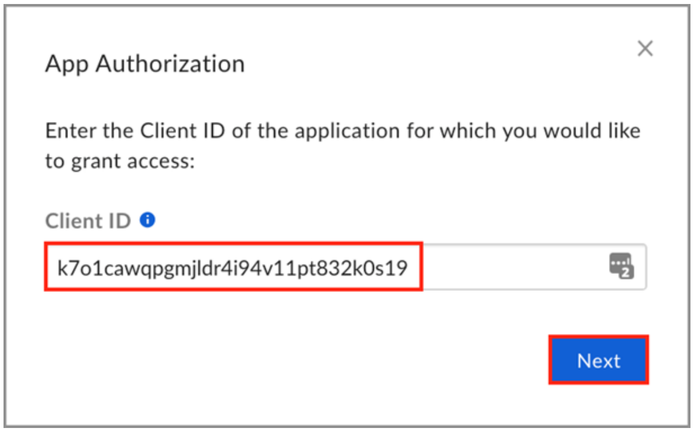
Grant access to custom applications with access specific to your enterprise. To learn more about building custom applications, please visit our Developer Website. Note: By connecting to a third party service, your use of that third party service is subject to its applicable terms of use and privacy policy.

Figure 9. Create a Custom App on the Box Tenant

Authorize the Zscaler Tenant on Box

To authorize the Custom App that is the Zscaler Tenant.

1. Paste the **Zscaler SaaS Connector** that was copied from the Zscaler wizard.
2. Click **Next**.



App Authorization

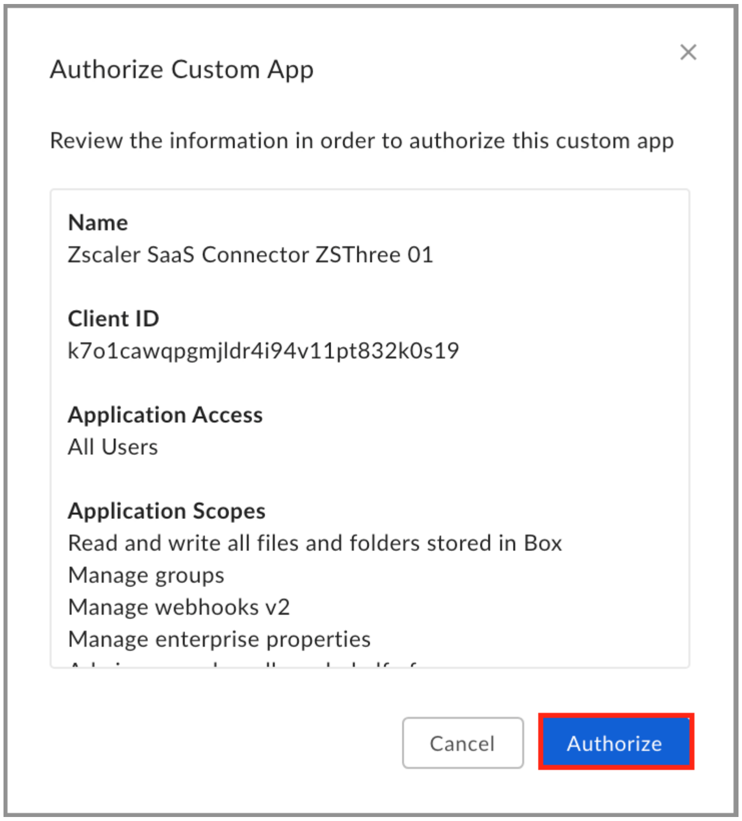
Enter the Client ID of the application for which you would like to grant access:

Client ID

k7o1cawqpgmjldr4i94v11pt832k0s19

Figure 10. Authorize the Zscaler App on the Box Tenant

3. Click **Authorize**. After the new Zscaler tenant is created, you must complete the Zscaler configuration by selecting the Enterprise ID. The Enterprise ID is pasted into the Zscaler configuration wizard later.



Authorize Custom App

Review the information in order to authorize this custom app

Name
Zscaler SaaS Connector ZSThree 01

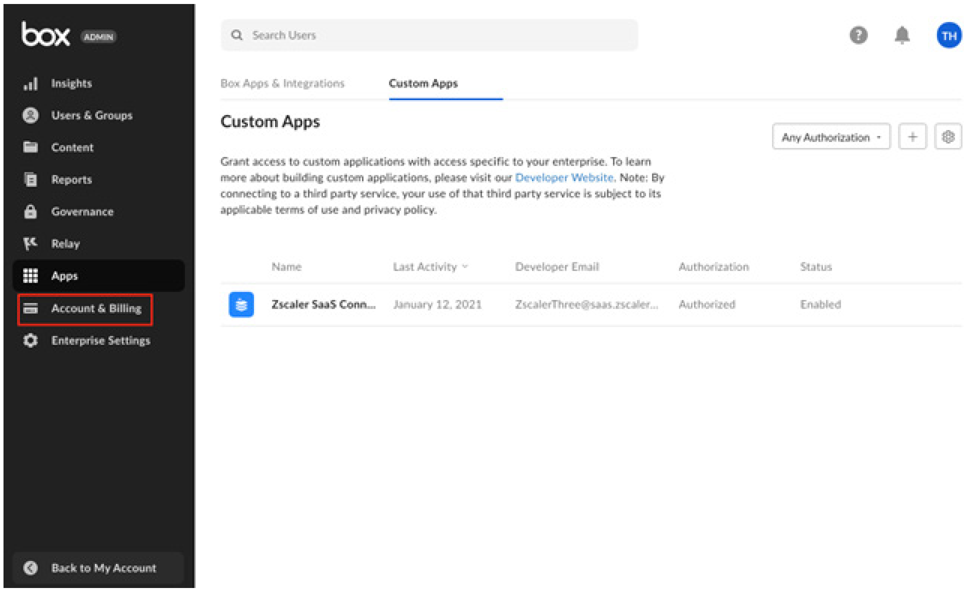
Client ID
k7o1cawqpgmjldr4i94v11pt832k0s19

Application Access
All Users

Application Scopes
Read and write all files and folders stored in Box
Manage groups
Manage webhooks v2
Manage enterprise properties

Figure 11. Authorize the Zscaler App on the Box Tenant

4. Select **Account & Billing**.



Custom Apps

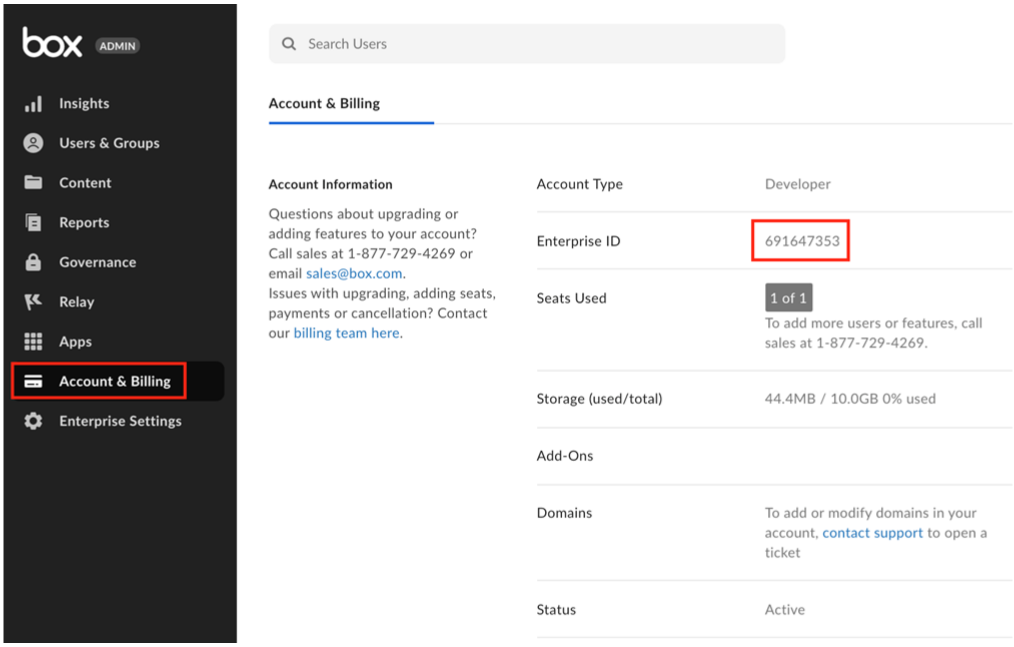
Grant access to custom applications with access specific to your enterprise. To learn more about building custom applications, please visit our Developer Website. Note: By connecting to a third party service, your use of that third party service is subject to its applicable terms of use and privacy policy.

Name	Last Activity	Developer Email	Authorization	Status
Zscaler SaaS Conn...	January 12, 2021	ZscalerThree@saas.zscaler...	Authorized	Enabled

Figure 12. The created Zscaler Tenant

Under **Account & Billing** of the Box Admin account, select and save the **Enterprise ID**. This ID is pasted into the Zscaler configuration wizard identifying the Box SaaS ID and allows the Zscaler SaaS Security API to provide security services to this Box tenant.

5. Copy and save the **Enterprise ID**.
6. Return to the Zscaler configuration wizard.



Account Information

Questions about upgrading or adding features to your account? Call sales at 1-877-729-4269 or email sales@box.com.
Issues with upgrading, adding seats, payments or cancellation? Contact our billing team here.

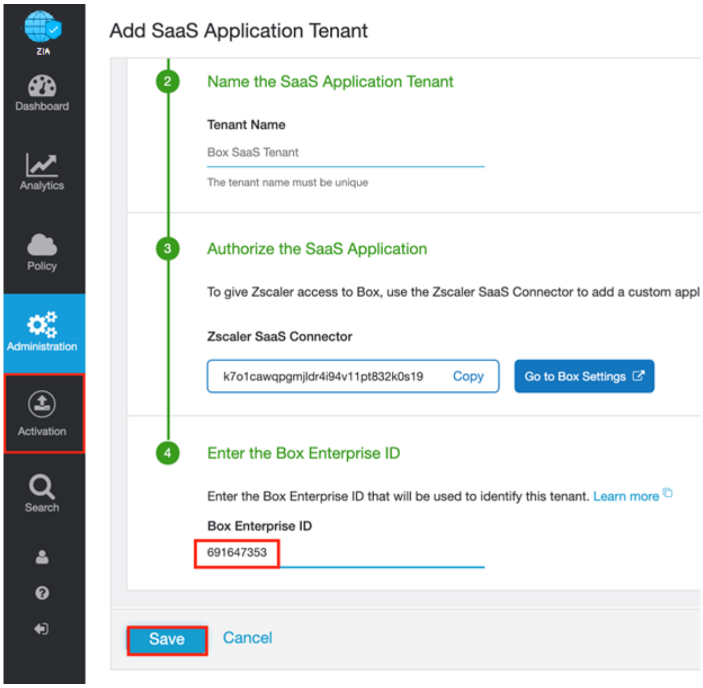
Account Type	Developer
Enterprise ID	691647353
Seats Used	1 of 1 To add more users or features, call sales at 1-877-729-4269.
Storage (used/total)	44.4MB / 10.0GB 0% used
Add-Ons	
Domains	To add or modify domains in your account, contact support to open a ticket
Status	Active

Figure 13. The Enterprise ID

Finishing the Zscaler Configuration

To finish:

1. Paste the **Box Enterprise ID** copied previously.
2. Save the **Zscaler / Box configuration**.
3. Activate your changes.



Add SaaS Application Tenant

2 Name the SaaS Application Tenant

Tenant Name: Box SaaS Tenant

The tenant name must be unique

3 Authorize the SaaS Application

To give Zscaler access to Box, use the Zscaler SaaS Connector to add a custom appl

Zscaler SaaS Connector: k7o1cawqpgmjldr4i94v11pt832k0s19 Copy

4 Enter the Box Enterprise ID

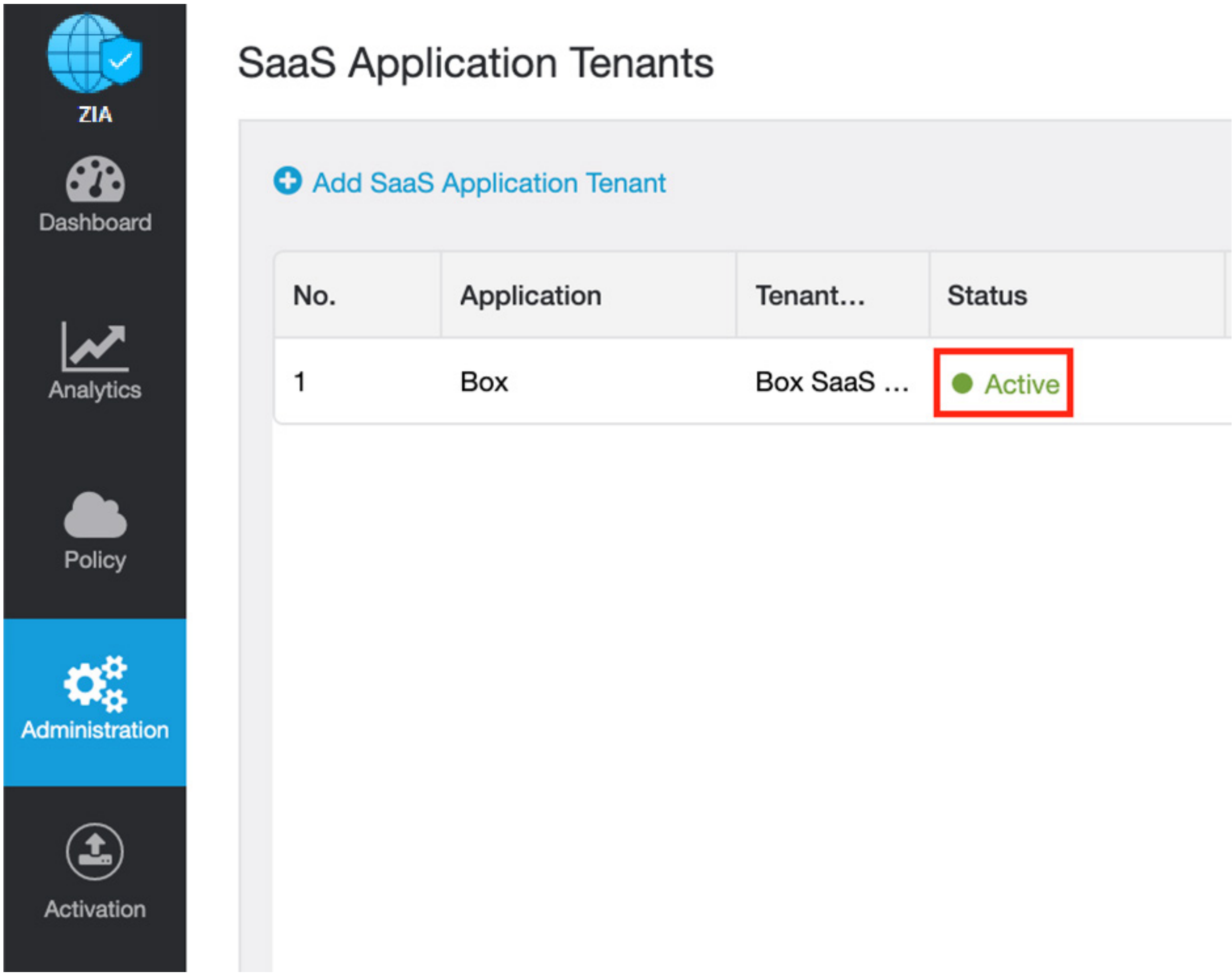
Enter the Box Enterprise ID that will be used to identify this tenant. Learn more

Box Enterprise ID: 691647353

Figure 14. Zscaler configuration wizard

The Active SaaS Security Tenant

The API credentials and connectivity are now validated. Refresh your browser to verify the Box tenant is Active.



SaaS Application Tenants

No.	Application	Tenant...	Status
1	Box	Box SaaS ...	● Active

Figure 15. Zscaler configuration wizard

You are now ready to set up the Scan Schedule, DLP policies, and Malware polices.

Configuring Box Policies and Scan Configuration

After adding the tenants, you can configure the SaaS Security API DLP policy, malware detection policy, and scan configuration. You can also view reports and data for the tenants in the SaaS report, insights, and logs.

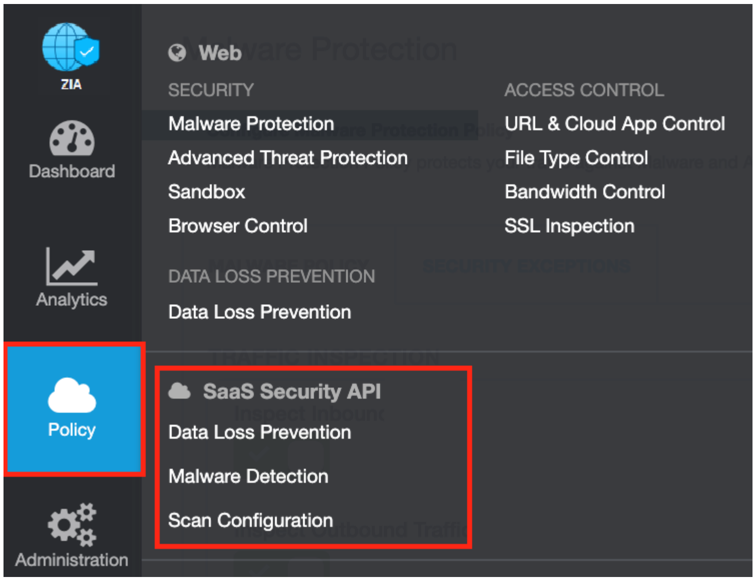


Figure 16. Zscaler SaaS Security API

Scoping the Policies and Remediation

For this deployment guide, you configure a basic DLP policy and a malware policy to scan the Box account files for matching content of the DLP policy, and scan the files for known malware for the malware policy.

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

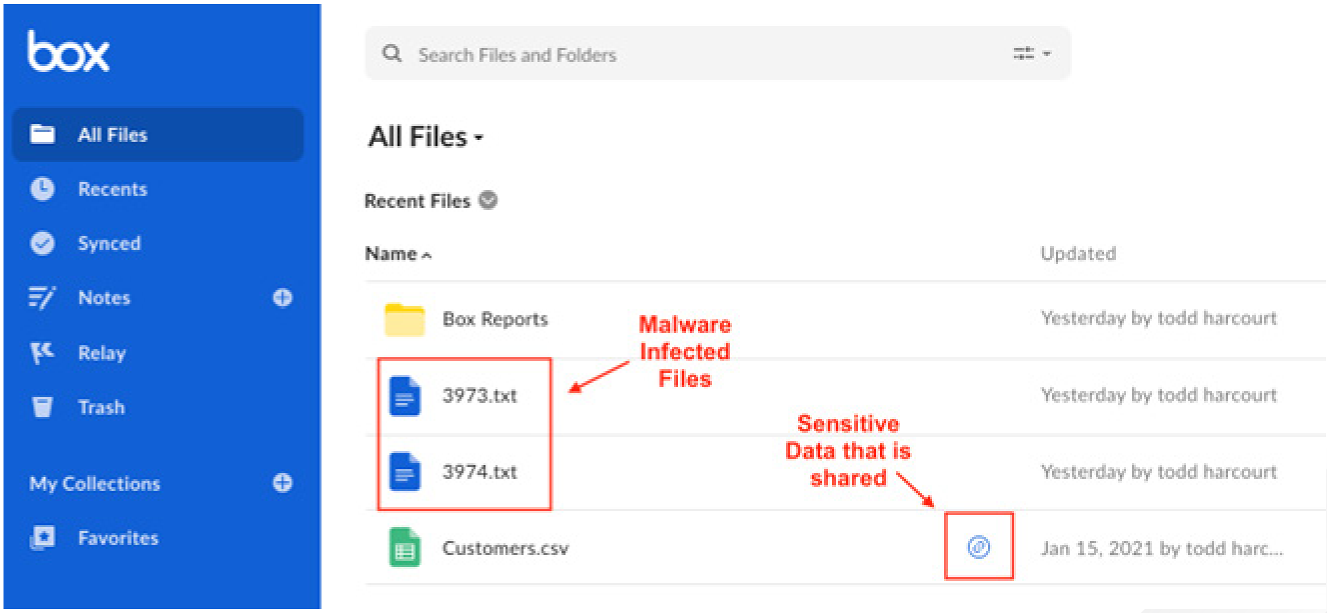


Figure 17. Box user account

For the DLP policy, create a very broad DLP policy to identify a spreadsheet with a list of US Social Security Numbers and remove the shared link to prevent further sharing of the file. DLP is a subject of its own, and this policy is used only for demonstration purposes. A true DLP policy review must be conducted to minimize false positives and false negatives.

Also note that the SaaS DLP protection is only part of the Zscaler DLP solution and is used to scan data-at-rest like the Box files. This deployment does not cover inline data protection or exact data match, although they are integral pieces of a data protection solution.

To test the DLP SaaS functionality, create a basic policy and apply it to the Box tenant.

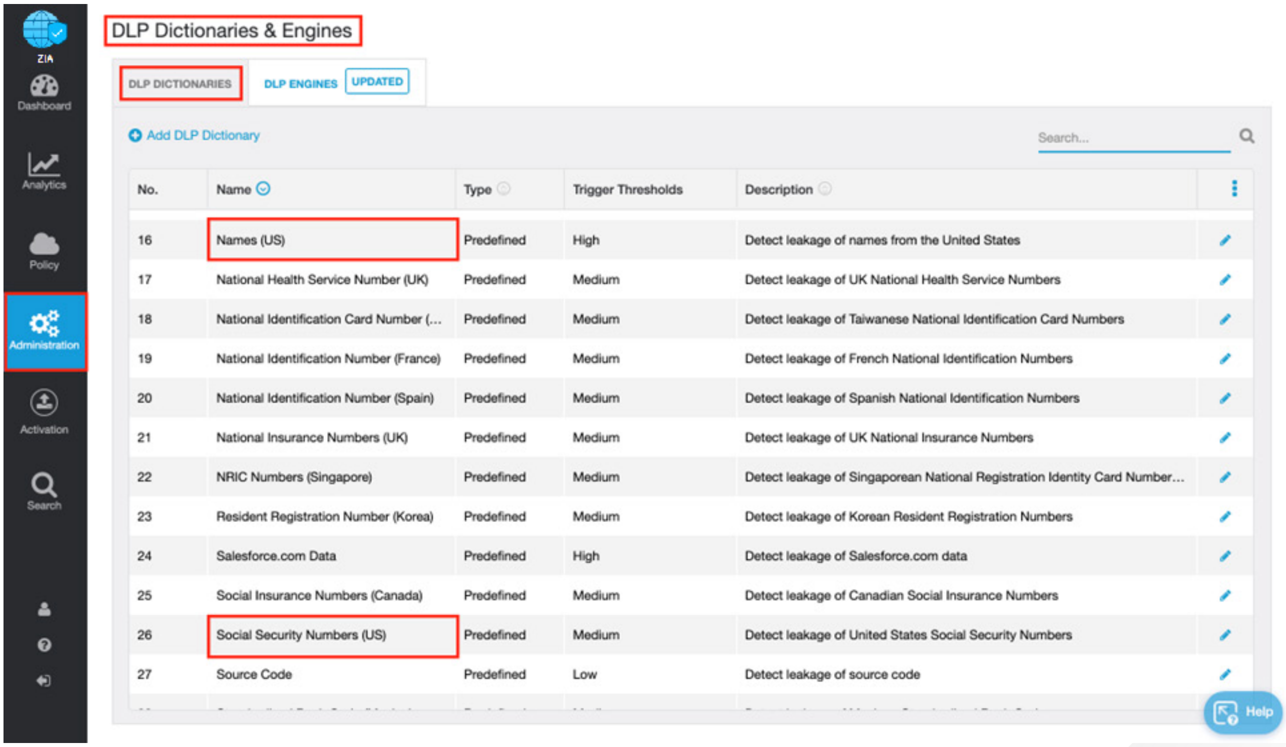
Creating a DLP Policy

The procedures for creating a DLP policy are pretty 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 US Social Security Numbers and US Names. The engine provides the means to precisely add or remove data to match violations and eliminate false positives.

A SaaS DLP policy is then created, which allows you to specify the detail about where, when, the action taken, and whom to inform about violations. Finally, the DLP policy is then applied to the Box tenant. Now verify the DLP dictionary as next steps. In the ZIA Admin Portal:

1. Select **Administration**.
2. Select **DLP Dictionaries & Engines**.
3. Select **DLP Dictionaries**.
4. Identify the dictionaries to be used. In this case, **Names (US)** and **Social Security Numbers (US)**.



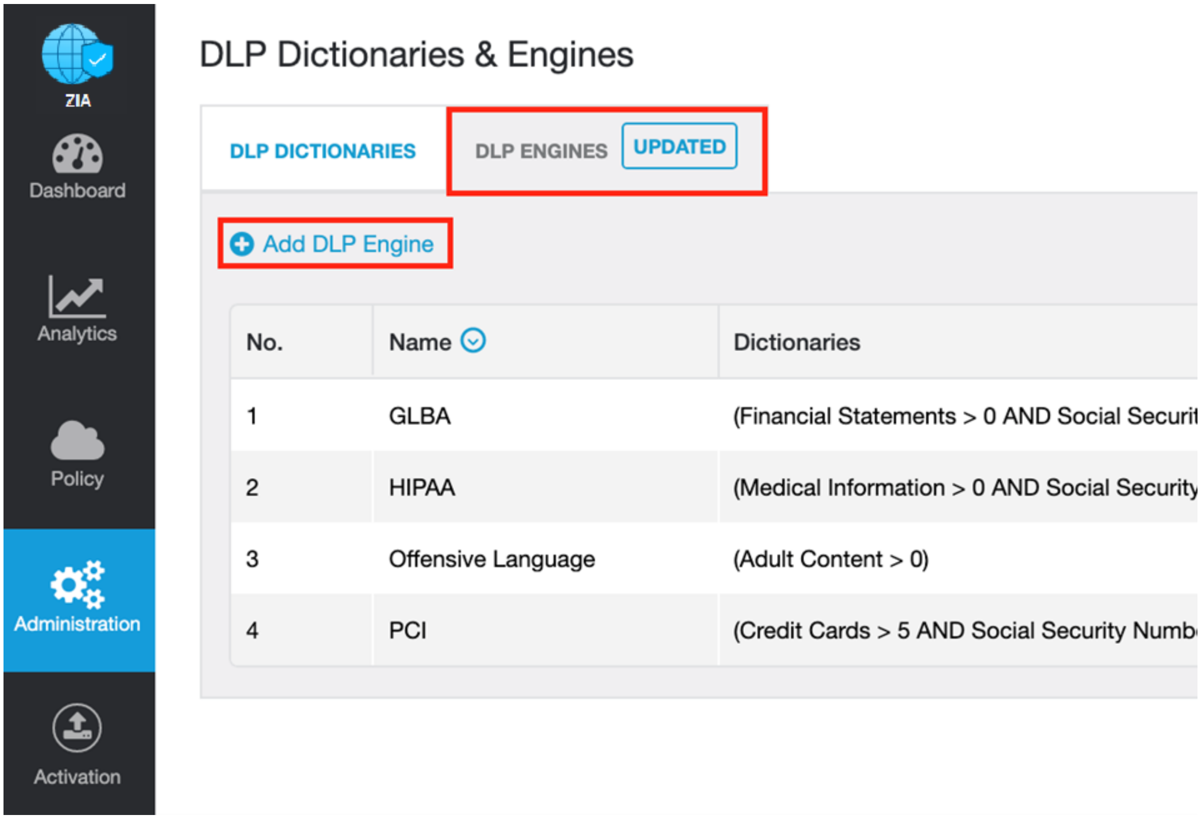
No.	Name	Type	Trigger Thresholds	Description
16	Names (US)	Predefined	High	Detect leakage of names from the United States
17	National Health Service Number (UK)	Predefined	Medium	Detect leakage of UK National Health Service Numbers
18	National Identification Card Number (...	Predefined	Medium	Detect leakage of Taiwanese National Identification Card Numbers
19	National Identification Number (France)	Predefined	Medium	Detect leakage of French National Identification Numbers
20	National Identification Number (Spain)	Predefined	Medium	Detect leakage of Spanish National Identification Numbers
21	National Insurance Numbers (UK)	Predefined	Medium	Detect leakage of UK National Insurance Numbers
22	NRIC Numbers (Singapore)	Predefined	Medium	Detect leakage of Singaporean National Registration Identity Card Number...
23	Resident Registration Number (Korea)	Predefined	Medium	Detect leakage of Korean Resident Registration Numbers
24	Salesforce.com Data	Predefined	High	Detect leakage of Salesforce.com data
25	Social Insurance Numbers (Canada)	Predefined	Medium	Detect leakage of Canadian Social Insurance Numbers
26	Social Security Numbers (US)	Predefined	Medium	Detect leakage of United States Social Security Numbers
27	Source Code	Predefined	Low	Detect leakage of source code

Figure 18. Creating a DLP Dictionary

Creating a DLP Engine

To create the DLP engine.

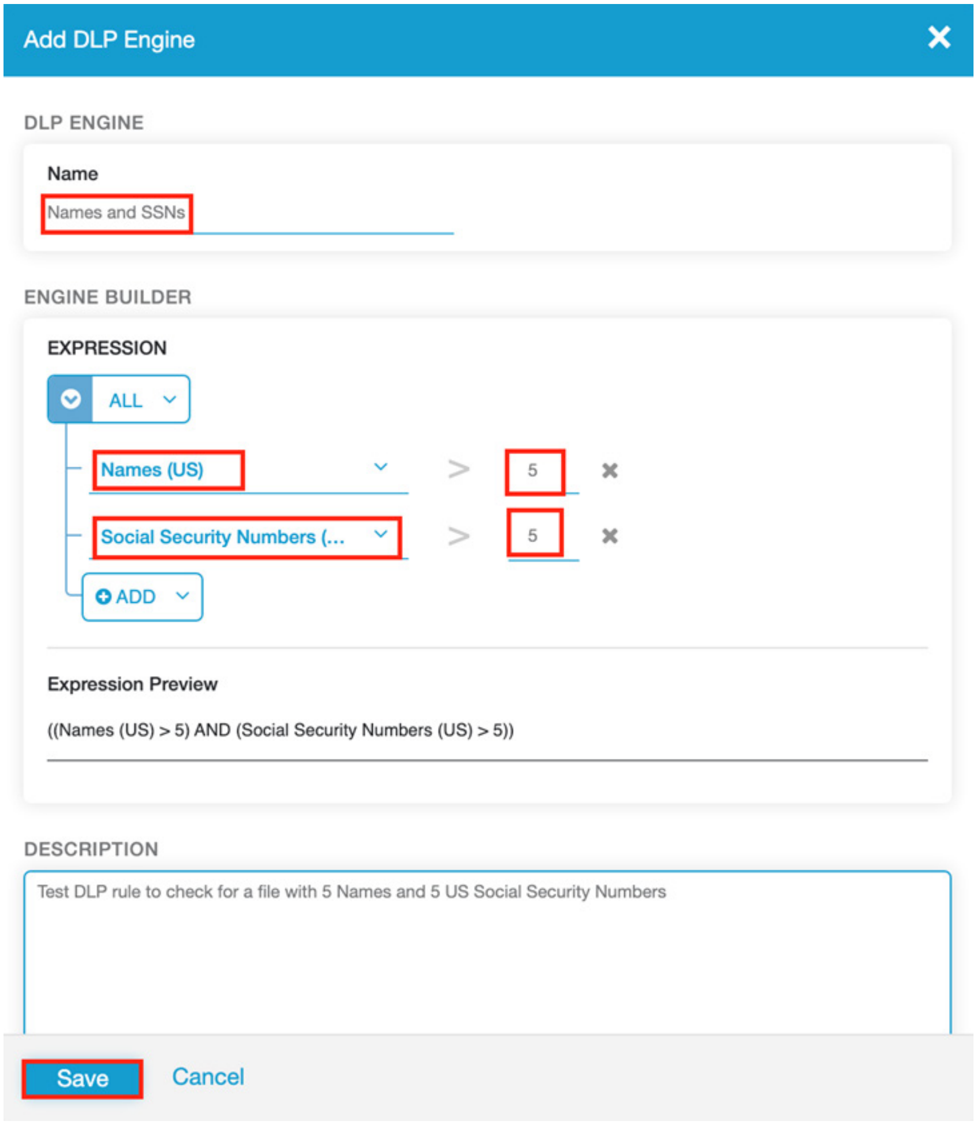
1. Select the **DLP Engines** tab.
2. Select **Add DLP Engine**.



No.	Name	Dictionaries
1	GLBA	(Financial Statements > 0 AND Social Securit
2	HIPAA	(Medical Information > 0 AND Social Security
3	Offensive Language	(Adult Content > 0)
4	PCI	(Credit Cards > 5 AND Social Security Numb

Figure 19. Creating a DLP Engine

3. Enter a **Name** for the DLP Engine.
4. In the **Engine Builder** under **Expression**, select the first dictionary.
5. Specify the **Match Count**, which is the minimum number of instances the data must occur in the file.
6. Click **Add** to add your dictionary and repeat the process.
7. Click **Save** to save the configuration.
8. Activate the configuration.



Add DLP Engine

DLP ENGINE

Name: Names and SSNs

ENGINE BUILDER

EXPRESSION

ALL

Names (US) > 5

Social Security Numbers (... > 5

Expression Preview

((Names (US) > 5) AND (Social Security Numbers (US) > 5))

DESCRIPTION

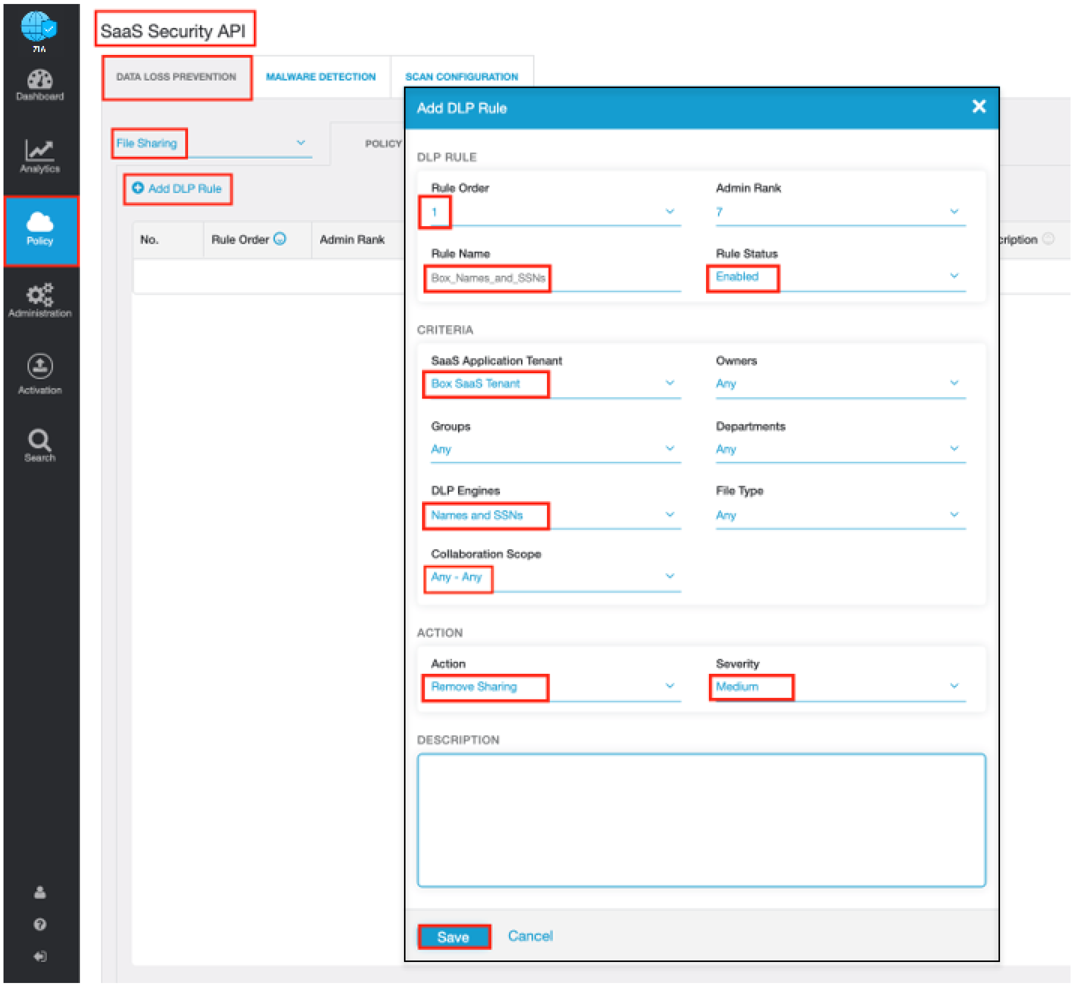
Test DLP rule to check for a file with 5 Names and 5 US Social Security Numbers

Figure 20. The DLP Engine

Configure a SaaS DLP Policy

To launch the DLP Rule wizard.

1. Go to **Policy** > **SaaS Security API** > **Data Loss Prevention**.
2. Select **File Sharing**.
3. Select **Add DLP Rule**.



Add DLP Rule

DLP RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Box_Names_and_SSNs

Rule Status: Enabled

CRITERIA

SaaS Application Tenant: Box SaaS Tenant

Owners: Any

Groups: Any

Departments: Any

DLP Engines: Names and SSNs

File Type: Any

Collaboration Scope: Any - Any

ACTION

Action: Remove Sharing

Severity: Medium

Figure 21. The SaaS DLP Policy configuration wizard

SaaS DLP Policy Details

The SaaS DLP Policy specifies the details to whom and what device 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. You specify the DLP Engine you have defined, any particular file Owners, Groups, or Departments, and the file types to inspect. The collaboration scope and the action are unique to the SaaS DLP and are explained in the following section for clarification. For this policy, select Any Collaboration, and an Action of Remove Sharing.

Collaboration Scope

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

- External Collaborators: Files that are shared with specific collaborators outside your organization.
- External Link: Files with shareable links that allow anyone outside your organization to find the files and have access.
- Internal Collaborators: Files that are shared with specific collaborators or are discoverable within your organization.
- Internal Link: Files with shareable links that allow anyone within your organization to find the files and have access.
- Private: Files that are only accessible to the owner.

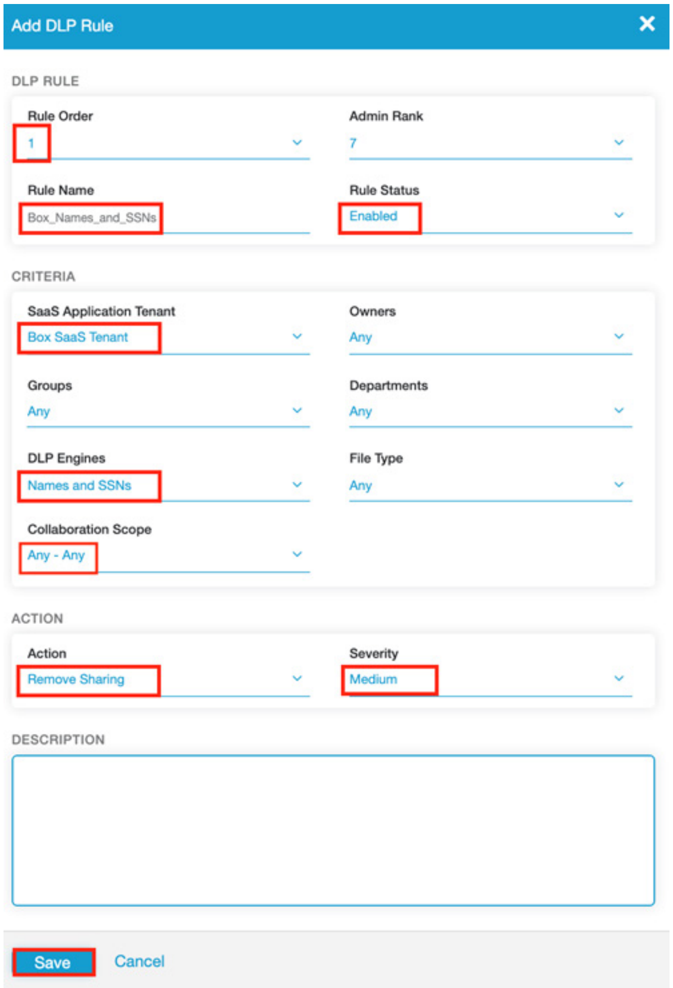
Action

- Choose the Action the rule takes upon detecting content that matches the criteria. The number of actions available depends on the selected SaaS Application Tenant.
- Change to Read Only for All Collaborators: The rule reports the incident and changes the file's collaboration scope for all collaborators to read only.
- Change to Read Only for External Collaborators: The rule reports the incident and changes the file's collaboration scope for external collaborators to read only.
- Change to Read Only for Internal Collaborators: The rule reports the incident and changes the file's collaboration scope for internal collaborators to read only.
- Remove All Collaborators: The rule reports the incident and removes all of the file's external and internal collaborators.
- Remove External Collaborators and Shareable Links: The rule reports the incident and removes all of the file's external collaborators and any shareable links.
- Remove Internal Collaborators and Shareable Links: The rule reports the incident and removes all internal collaborators and any shareable links.
- Remove Internal Shareable Link: The rule reports the incident and removes the file's internal shareable link. Existing collaborators are unaffected.
- Remove Public Shareable Link: The rule reports the incident and removes the file's public shareable link. Existing collaborators are unaffected.
- Remove Sharing: The rule reports the incident and removes all of the file's collaborators and any shareable links.
- Report Incident Only: The rule reports the incident only and makes no changes to the file's collaboration scope.
- Update to Not Discoverable Externally: The rule reports the incident and changes the file's collaboration scope to prevent it from being discoverable through public search engines.
- Update to Not Discoverable for All: The rule reports the incident and changes the file's collaboration scope to prevent it from being discoverable through public search engines or within your organization.
- Update to Not Discoverable Internally: The rule reports the incident and changes the file's collaboration scope to prevent it from being discoverable within your organization.

Configure a SaaS DLP Policy

To finish the DLP policy:

1. Specify the **Rule order** for **Processing**.
2. **Name** the rule.
3. **Enable** the rule.
4. Select the **Box SaaS Tenant**.
5. Select the **DLP Engine** created previously.
6. Select **Any-Any** for the **Collaboration Scope**.
7. Select **Remove Sharing** as the **Action**.
8. Select **Medium** as a **Severity** to allow for identification for searches and tracking.
9. **Save** and Activate your configuration.



Add DLP Rule

DLP RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Box_Names_and_SSNs

Rule Status: Enabled

CRITERIA

SaaS Application Tenant: Box SaaS Tenant

Owners: Any

Groups: Any

Departments: Any

DLP Engines: Names and SSNs

File Type: Any

Collaboration Scope: Any - Any

ACTION

Action: Remove Sharing

Severity: Medium

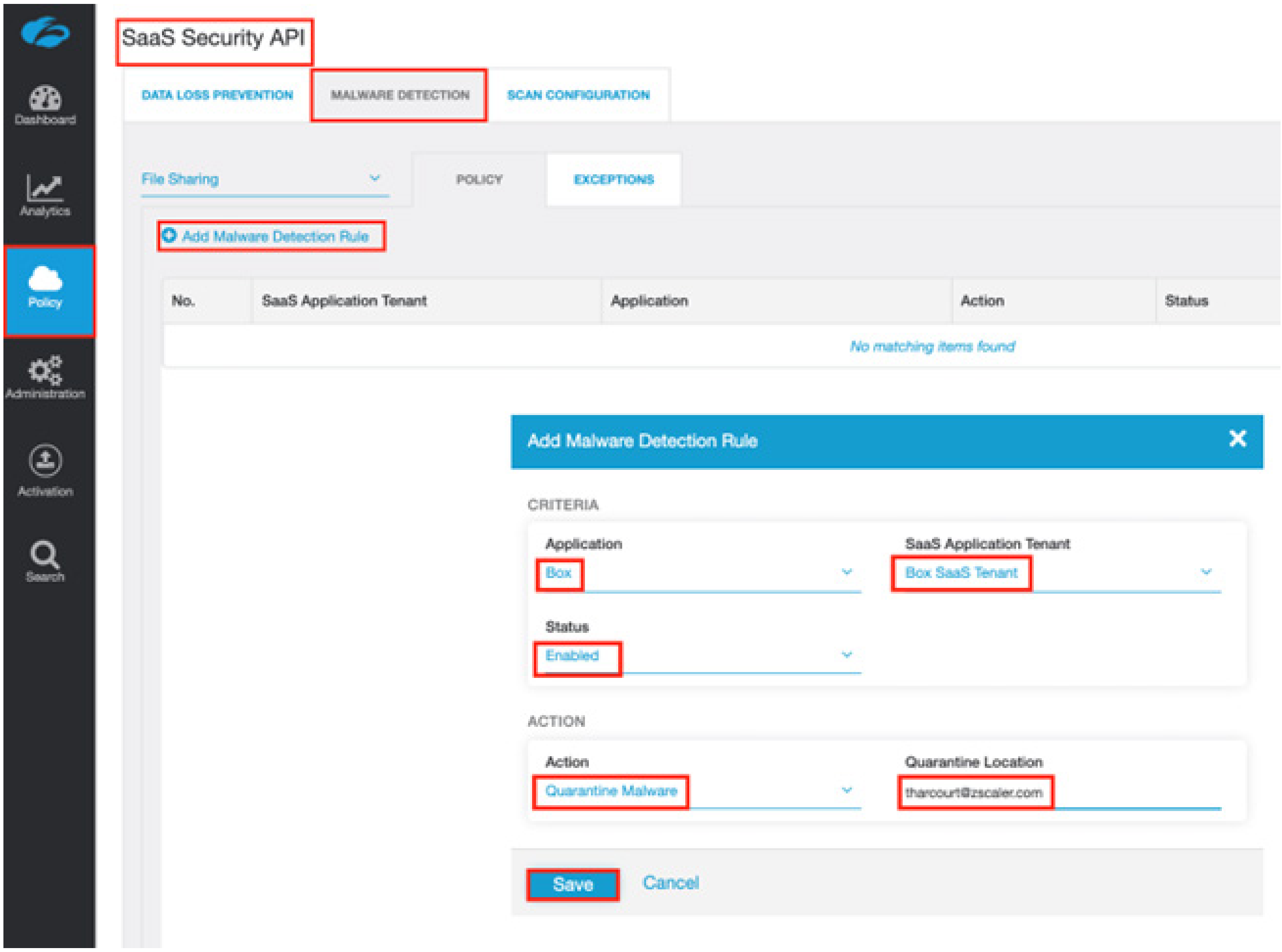
DESCRIPTION

Figure 22. The SaaS DLP Policy configuration wizard

Configure a SaaS Malware Policy

To launch the DLP Rule wizard:

1. Select **Policy** > **SaaS Security API** > **Malware Detection**.
2. Select **File Sharing**.
3. Select **Add Malware Detection Rule**.



SaaS Security API

File Sharing

No.	SaaS Application Tenant	Application	Action	Status
No matching items found				

Add Malware Detection Rule

CRITERIA

Application: Box

SaaS Application Tenant: Box SaaS Tenant

Status: Enabled

ACTION

Action: Quarantine Malware

Quarantine Location: tharcourt@zscaler.com

Figure 23. The Malware Policy configuration wizard

The SaaS Malware Detection Policy is an all-encompassing policy and 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, specify the Application, the SaaS Tenant, the Status, the Action, and the Quarantine Location.

The Action and the Quarantine Location are unique to the SaaS Tenants. For the Action, you can select Quarantine, Remove, or report a violation. If you select Quarantine, you must specify the Box ID for the user where the files are quarantined. This would typically be the Security Operations Group.

Action

Select the action for the rule to take when it detects malware.

- Quarantine Malware: The Zscaler service quarantines the suspicious file.
- Remove Malware: The service deletes the suspicious file.
- Report Malware: The Zscaler service reports the incident but doesn't quarantine or remove the malware.

Quarantine Location

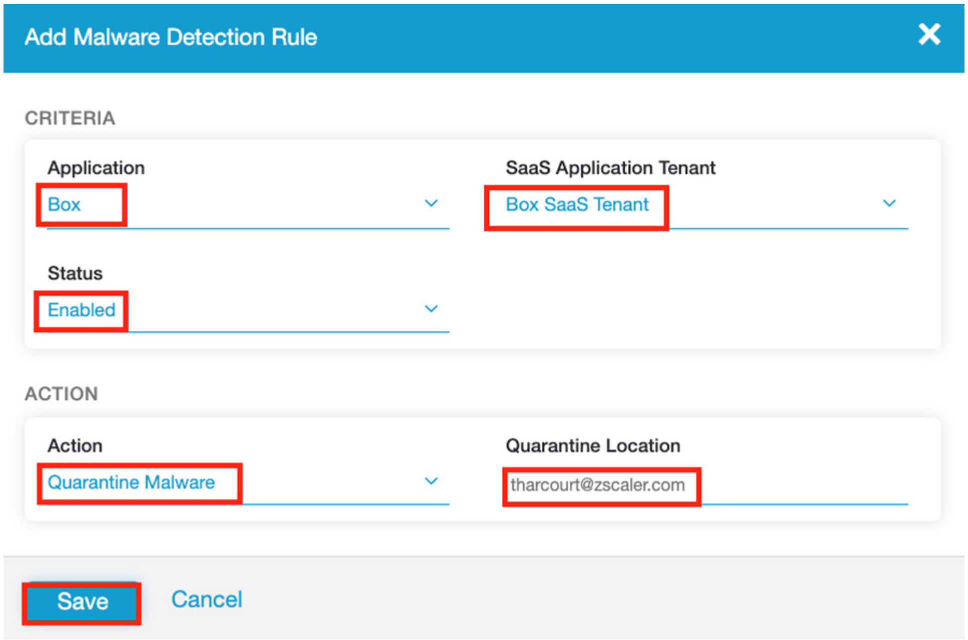
This field appears only if you select the Quarantine Malware action.

- This is the location where malicious files are moved for quarantine. The Zscaler service creates a folder or library called Zscaler_Quarantine for the location.
- To specify the quarantine location, enter the Box ID for the user who owns the folder. The service creates the folder on the user's account.

Configure a SaaS Malware Policy

To configure the Malware Rule wizard:

1. Select **Policy** > **SaaS Security API** > **Malware Detection**.
2. Select **File Sharing**.
3. Select **Add Malware Detection Rule**.
4. Under **Criteria**, select **Box** as the **Application**.
5. Select the **Box SaaS Tenant** to apply the policy.
6. Select **Enabled** for **Status**.
7. Select **Quarantine Malware** as the **Action**.
8. Select the **User ID** where the **Quarantine** folder is created, and the infected files are stored.
9. Select **Save**.



Add Malware Detection Rule

CRITERIA

Application: Box

SaaS Application Tenant: Box SaaS Tenant

Status: Enabled

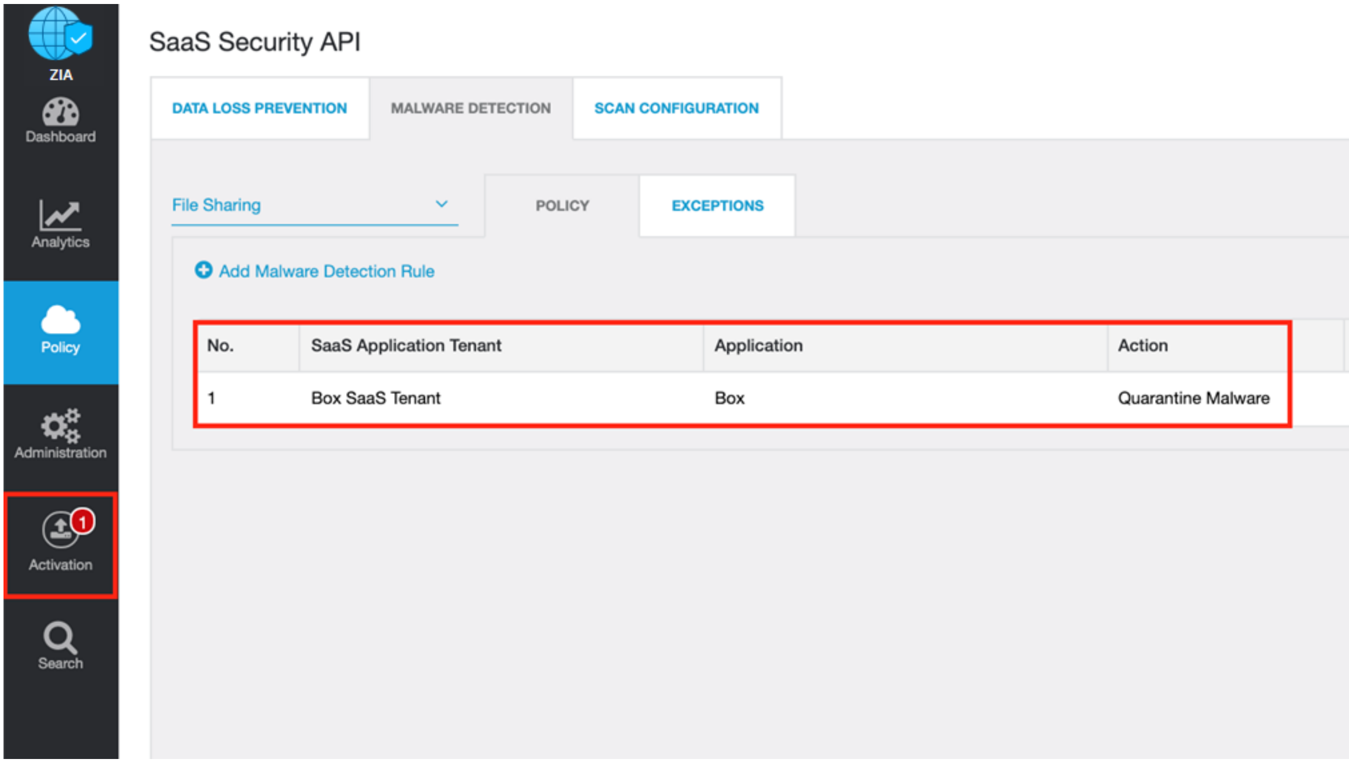
ACTION

Action: Quarantine Malware

Quarantine Location: tharcourt@zscaler.com

Figure 24. The Malware Policy configuration wizard

The following is the completed SaaS Malware policy for the Box SaaS Tenant. Activate your configuration.



No.	SaaS Application Tenant	Application	Action
1	Box SaaS Tenant	Box	Quarantine Malware

Figure 25. The Completed Malware Policy configuration wizard

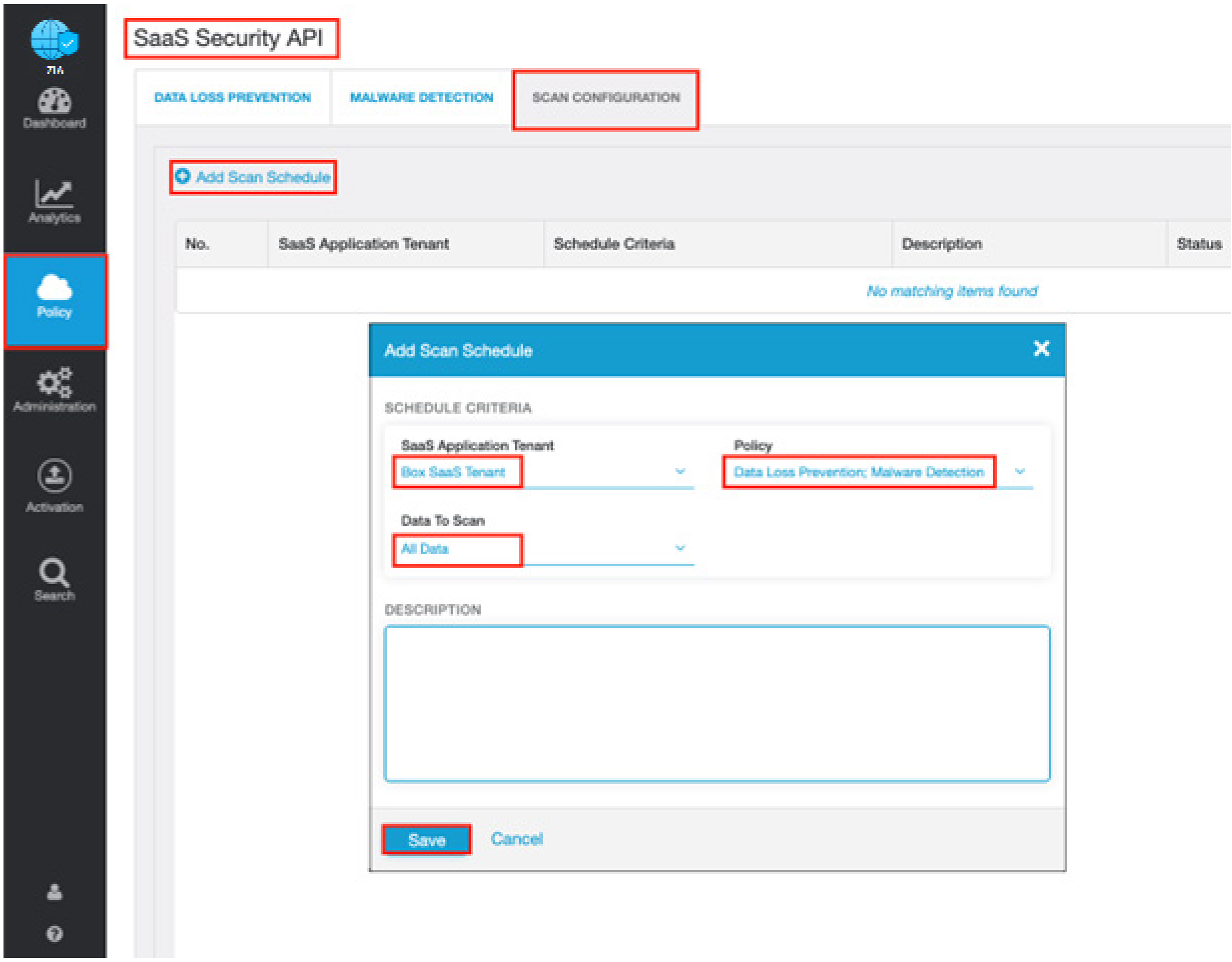
Configure the Scan Schedule Configuration

The final configuration step is to create a Scan Configuration. Specify that the Tenant to which the Scan Configuration applies are any policies that are to be included in the scan, and any data to scan relative to a date.

The options for Data to Scan are All Data, Date Created or Modified After, or New Data Only. For this deployment guide, select All Data. However, if this is a 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 **Box SaaS Tenant** for the **SaaS Application Tenant**.
3. Select the **Data Loss Prevention** policy and the **Malware Detection** policy created previously.
4. Select **All Data** or **New Data Only** if this is a POV.
5. Select **Save** to save the Scan Schedule.



No.	SaaS Application Tenant	Schedule Criteria	Description	Status
			No matching items found	

Add Scan Schedule

SCHEDULE CRITERIA

SaaS Application Tenant: Box SaaS Tenant

Policy: Data Loss Prevention; Malware Detection

Data To Scan: All Data

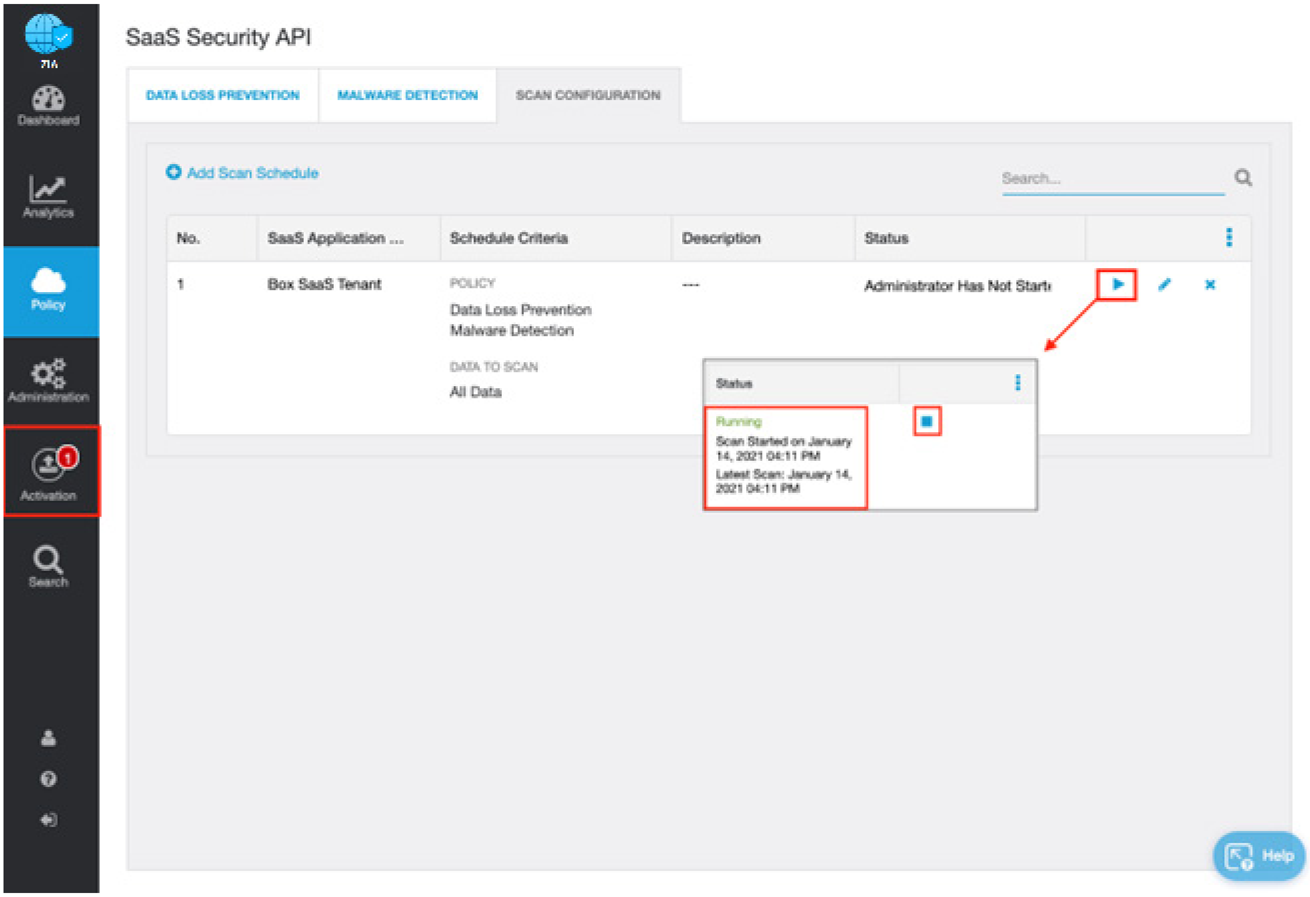
DESCRIPTION

Figure 26. Create and enable a scan for the SaaS Tenant

Start the Scan Schedule Configuration

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

1. Activate the configuration changes.
2. Select the **Blue Arrow** on the **Scan configuration** to start SaaS Security API on the Box Tenant. The Status displays `Active` with a **Start Date** and a **Latest Scan Date**.



SaaS Security API

No.	SaaS Application ...	Schedule Criteria	Description	Status
1	Box SaaS Tenant	POLICY Data Loss Prevention Malware Detection DATA TO SCAN All Data	---	Administrator Has Not Start

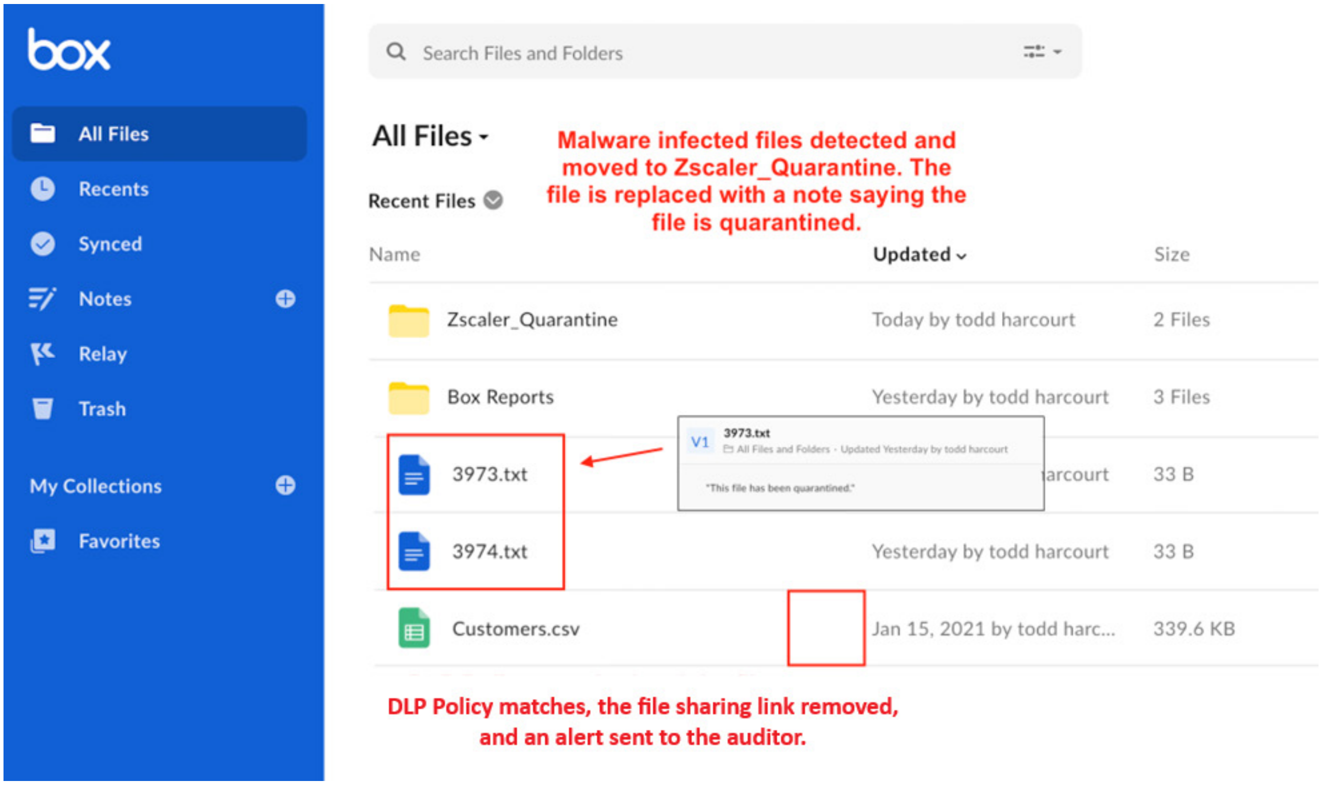
Status
Running Scan Started on January 14, 2021 04:11 PM Latest Scan: January 14, 2021 04:11 PM

Figure 27. Starting the scan

The Box Tenant Post Scan

The following figure shows the Box Tenant after completing the Scan Schedule. The Malware Policy detected Malware in the two infected files, the SaaS Security API created the Quarantine folder and moved the files into the folder. A file with the same name was created to replace the infected file with a note letting the user know that the file was quarantined.

The DLP Policy also found the configured violation and, after the file containing the sensitive data was identified and the shared link was removed, prevented the file from being distributed.



Malware infected files detected and moved to Zscaler_Quarantine. The file is replaced with a note saying the file is quarantined.

Name	Updated	Size
Zscaler_Quarantine	Today by todd harcourt	2 Files
Box Reports	Yesterday by todd harcourt	3 Files
3973.txt	arcourt	33 B
3974.txt	Yesterday by todd harcourt	33 B
Customers.csv	Jan 15, 2021 by todd harc...	339.6 KB

V1 3973.txt
All Files and Folders · Updated Yesterday by todd harcourt
"This file has been quarantined."

DLP Policy matches, the file sharing link removed, and an alert sent to the auditor.

Figure 28. The SaaS results

Reporting and Visibility

Zscaler Analytics provide detailed reporting of all user activity down to each session created by the user when attaching to destination. Zscaler extends that visibility to include reporting of activity, malware incidents, and DLP violations of data at rest associated with the user. For SaaS partners, Zscaler provides Reports and SaaS Insights. This provides visibility from a high-level overview to management of the individual logs and violations.

The following sections review the tools, but for detailed information of the SaaS Analytics tools, visit the **Zscaler Help Portal** (government agencies, see **Zscaler Help Portal**).

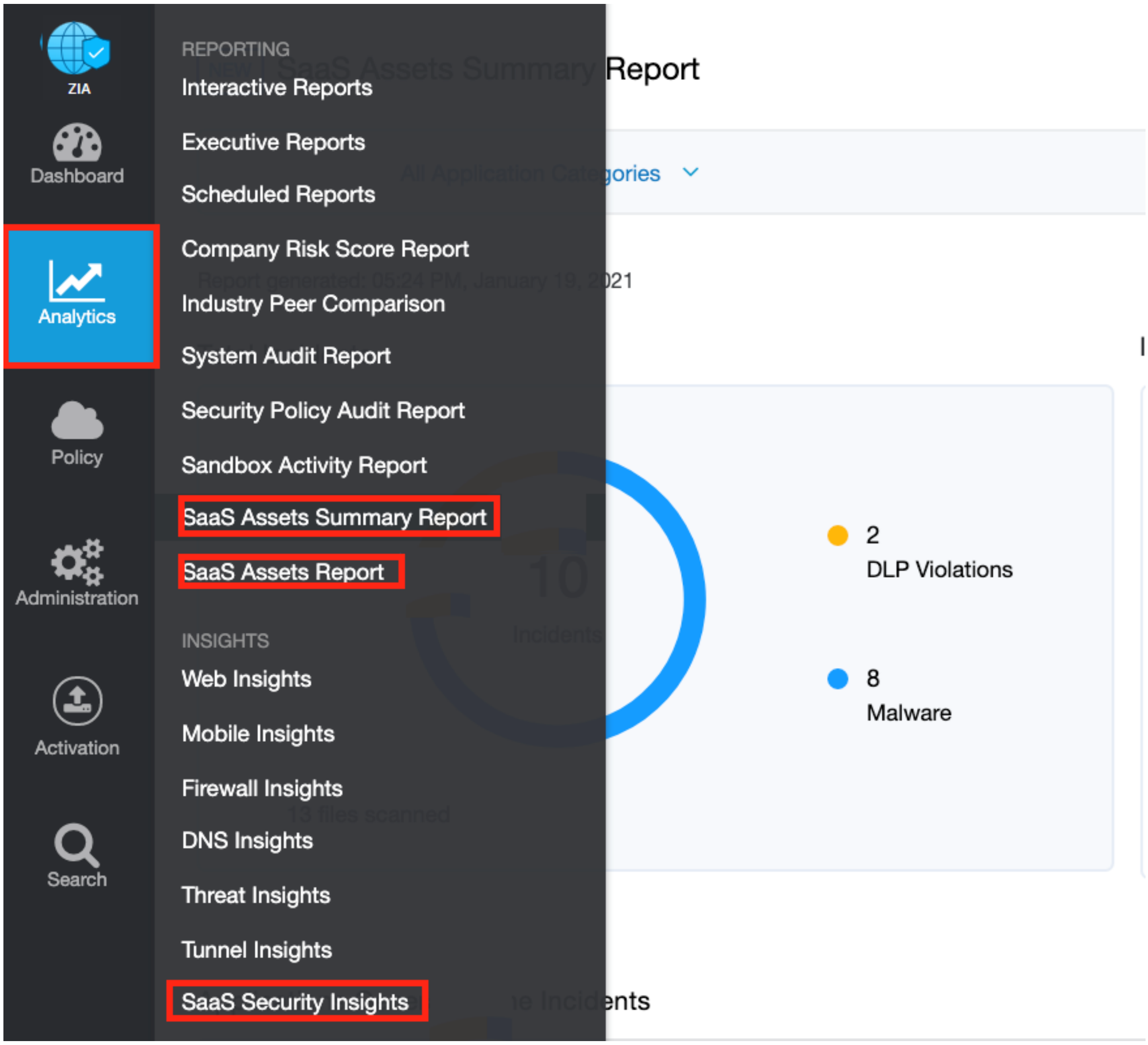
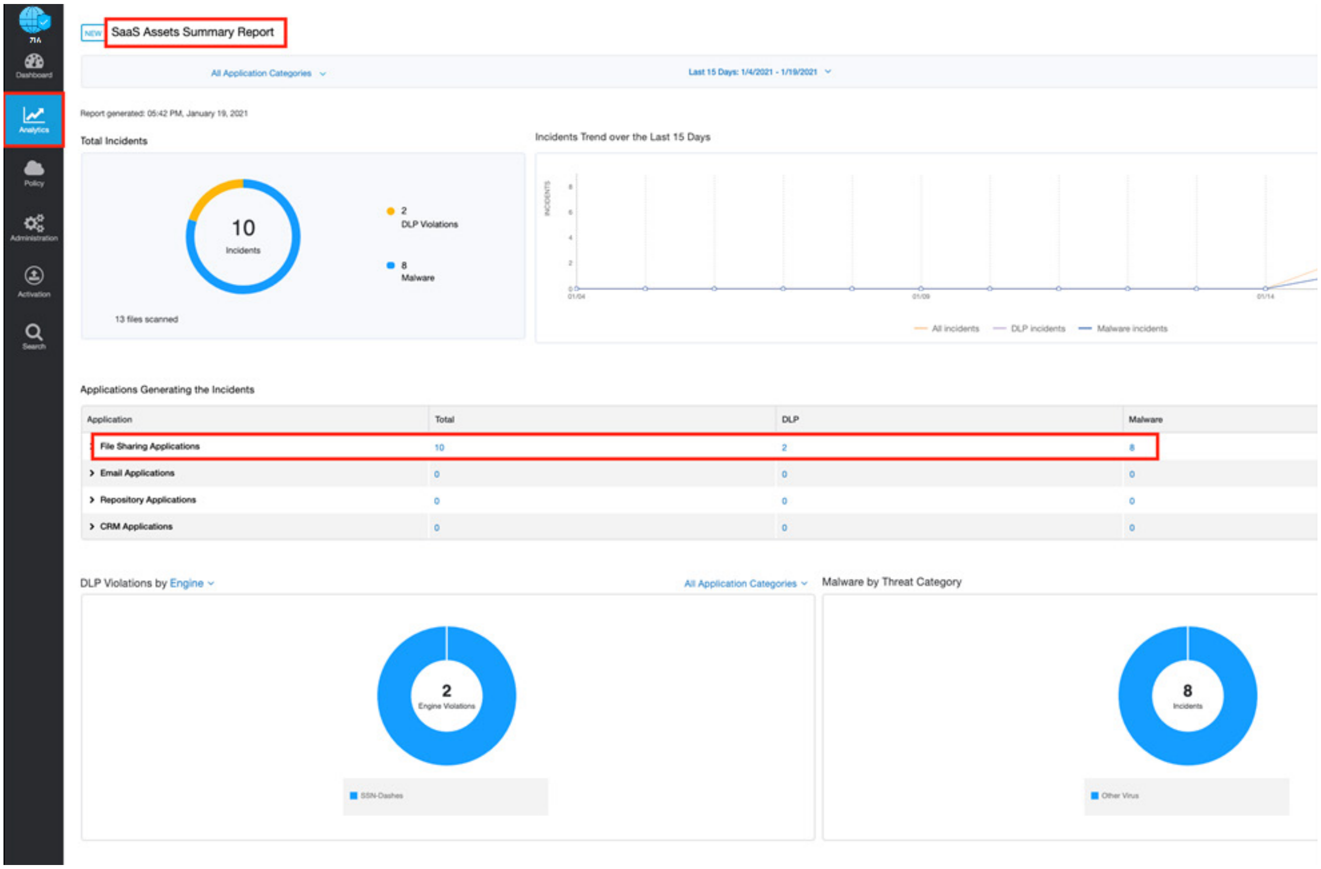


Figure 29. SaaS Visibility

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 following figure is the SaaS Assets Summary Report, which provides all activity and violations at a quick glance. The report identifies all SaaS Tenant information from a single screen. The Box activity over the creation of this deployment guide is shown, but any Tenant configured is also displayed on this summary screen. The data is hyperlinked, and you can pivot from a Summary to individual logs and activities provided by SaaS Insights.

Select the 10 Total Violations to pivot to SaaS Insights.



Applications Generating the Incidents

Application	Total	DLP	Malware
File Sharing Applications	10	2	8
› Email Applications	0	0	0
› Repository Applications	0	0	0
› CRM Applications	0	0	0

Figure 30. Summary reports

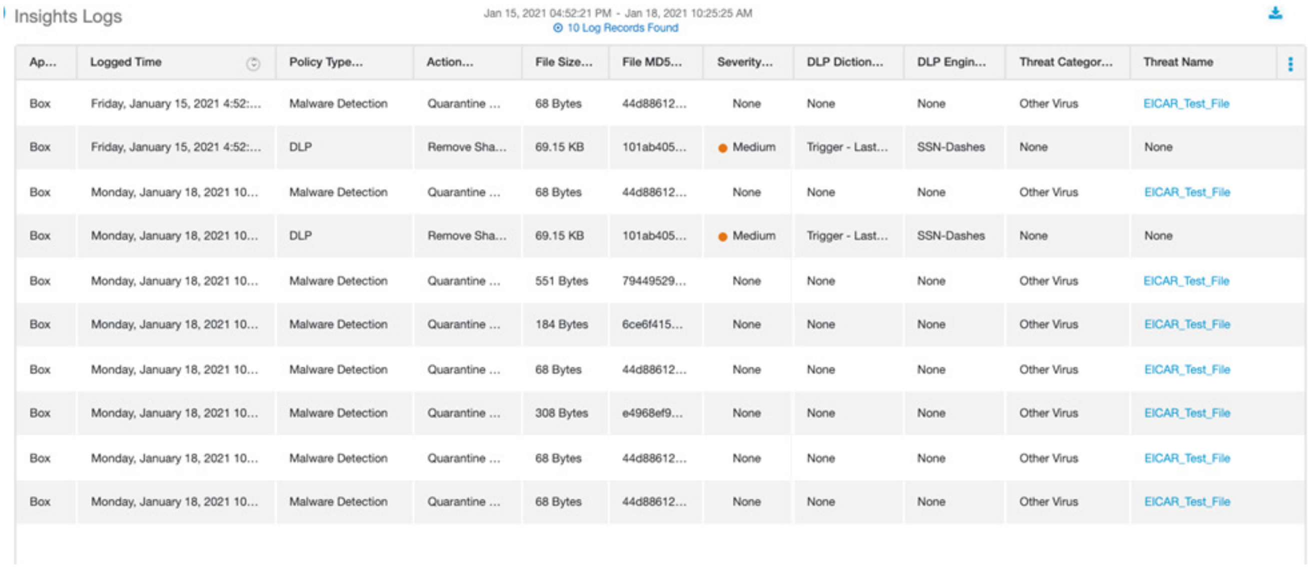
This opens SaaS Insights and the log data for each violation containing over 30 metadata points of information.

SaaS Insights

The SaaS Insights page is where you can view and define information that you want to view when analyzing files scanned through charts. These logs provide the details 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 data types and their associated filters:

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



Insights Logs

Jan 15, 2021 04:52:21 PM - Jan 18, 2021 10:25:25 AM
10 Log Records Found

Ap...	Logged Time	Policy Type...	Action...	File Size...	File MD5...	Severity...	DLP Diction...	DLP Engin...	Threat Categor...	Threat Name
Box	Friday, January 15, 2021 4:52:...	Malware Detection	Quarantine ...	68 Bytes	44d88612...	None	None	None	Other Virus	EICAR_Test_File
Box	Friday, January 15, 2021 4:52:...	DLP	Remove Sha...	69.15 KB	101ab405...	● Medium	Trigger - Last...	SSN-Dashes	None	None
Box	Monday, January 18, 2021 10...	Malware Detection	Quarantine ...	68 Bytes	44d88612...	None	None	None	Other Virus	EICAR_Test_File
Box	Monday, January 18, 2021 10...	DLP	Remove Sha...	69.15 KB	101ab405...	● Medium	Trigger - Last...	SSN-Dashes	None	None
Box	Monday, January 18, 2021 10...	Malware Detection	Quarantine ...	551 Bytes	79449529...	None	None	None	Other Virus	EICAR_Test_File
Box	Monday, January 18, 2021 10...	Malware Detection	Quarantine ...	184 Bytes	6ce6f415...	None	None	None	Other Virus	EICAR_Test_File
Box	Monday, January 18, 2021 10...	Malware Detection	Quarantine ...	68 Bytes	44d88612...	None	None	None	Other Virus	EICAR_Test_File
Box	Monday, January 18, 2021 10...	Malware Detection	Quarantine ...	308 Bytes	e4968ef9...	None	None	None	Other Virus	EICAR_Test_File
Box	Monday, January 18, 2021 10...	Malware Detection	Quarantine ...	68 Bytes	44d88612...	None	None	None	Other Virus	EICAR_Test_File
Box	Monday, January 18, 2021 10...	Malware Detection	Quarantine ...	68 Bytes	44d88612...	None	None	None	Other Virus	EICAR_Test_File

Figure 31. SaaS Insights

ZDX for Box

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. And with users working from home and anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. Box is no exception to this and Zscaler ZDX provides visibility into the client's experience using Box. ZDX utilizes the Zscaler Client Connector to generate application and network probes, and to gather device health. ZDX is a separate service from ZIA SaaS and can run with or without SaaS 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. ZDX measures and analyzes 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.

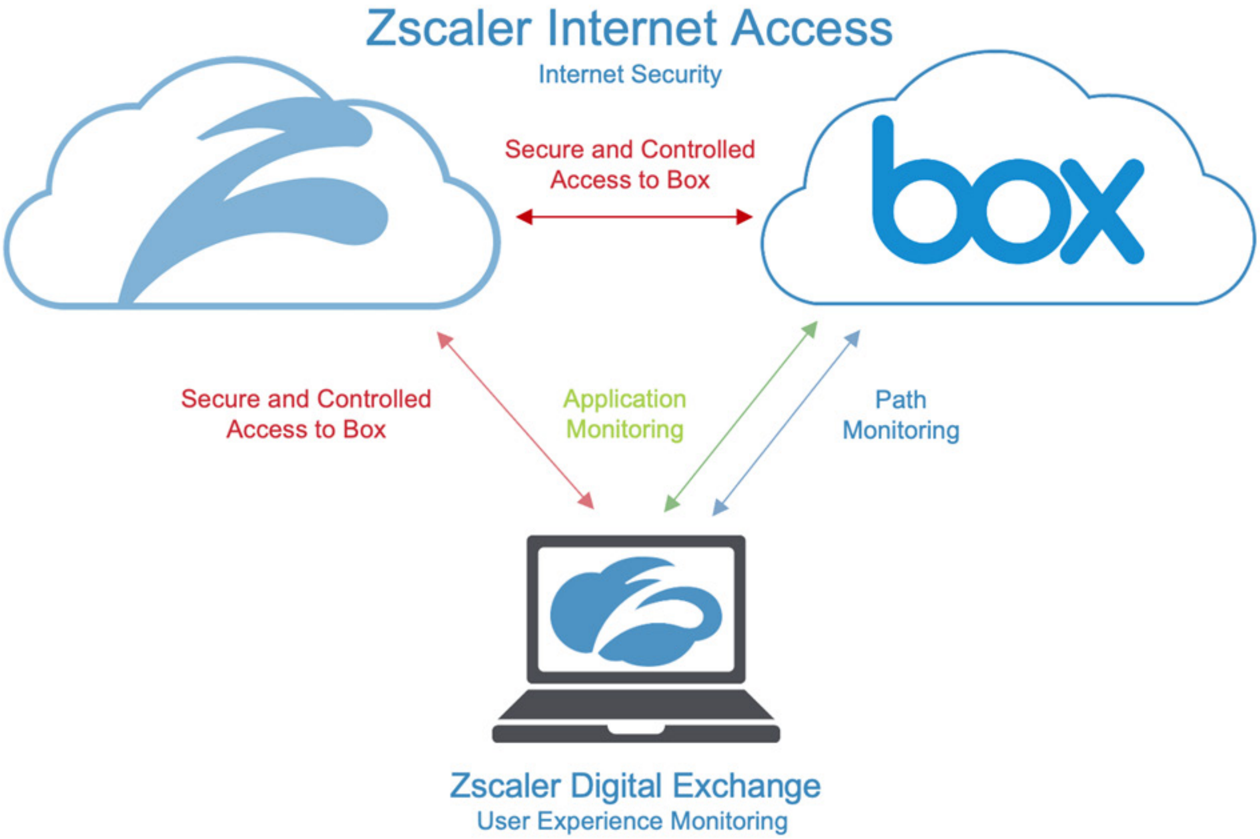
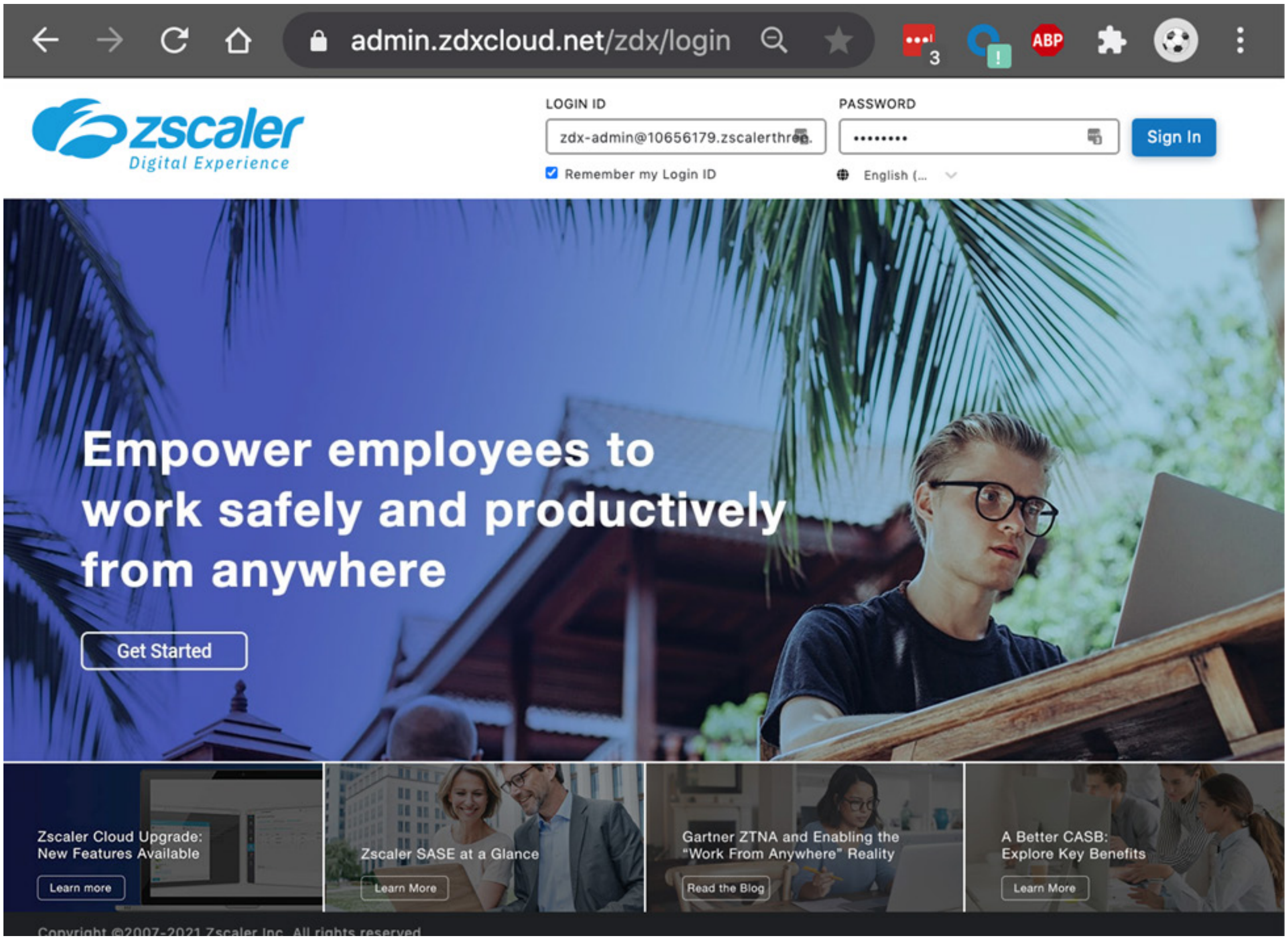


Figure 32. ZDX for User Experience Monitoring for Box

Configure ZDX for Box

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



admin.zdxcloud.net/zdx/login

LOGIN ID: zdx-admin@10656179.zscalerthree.

PASSWORD: ••••••••

☑ Remember my Login ID

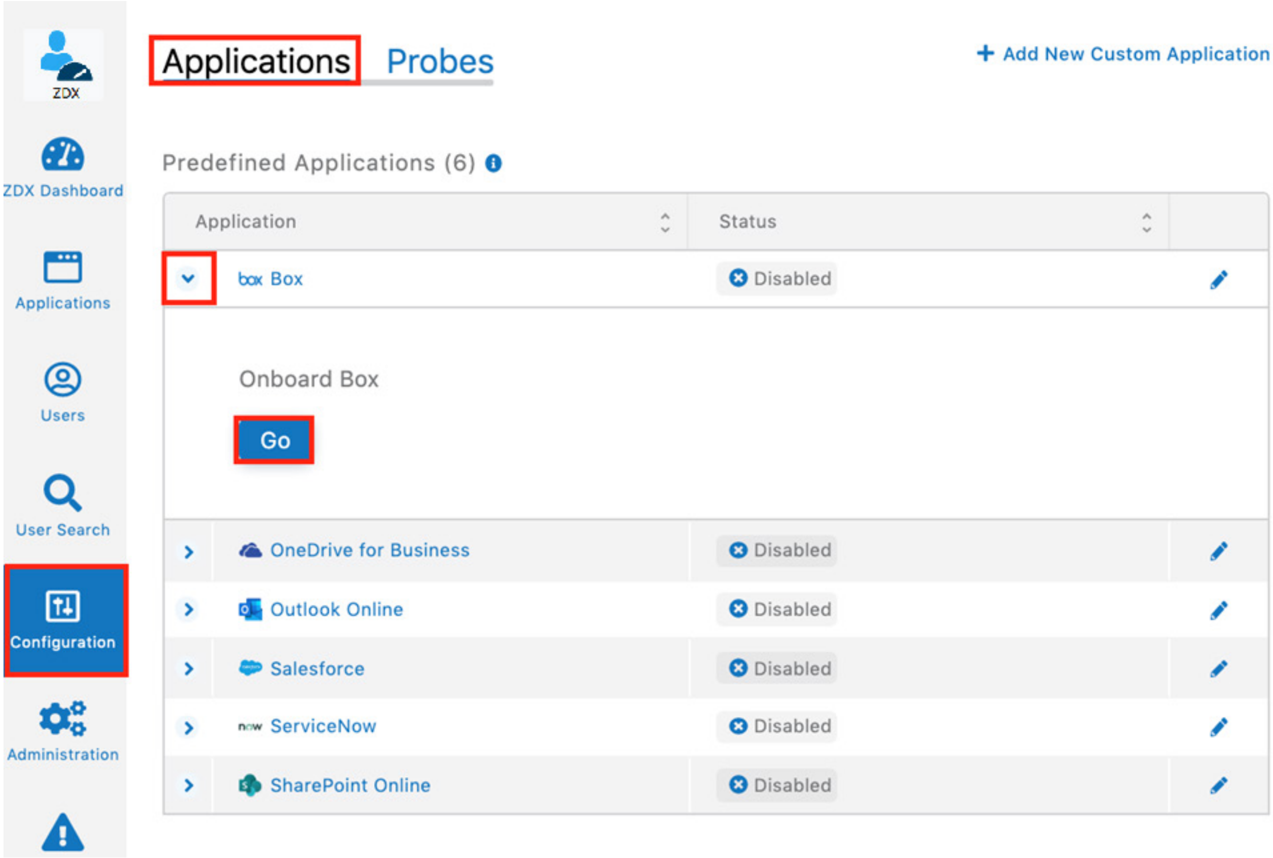
zscaler
Digital Experience
Sign In
English (...
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2021 Zscaler Inc. All rights reserved.

Figure 33. ZDX for User Experience Monitoring for Box

Onboard the Box App

Box is a predefined application in ZDX, and configuration is very simple. To configure the Box application for monitoring:

1. Select **Configuration**.
2. Select **Applications**.
3. Select the blue arrow next to the Box application.
4. Select **Go** under **Onboard Box**.



Predefined Applications (6)

Application	Status
Box	Disabled
OneDrive for Business	Disabled
Outlook Online	Disabled
Salesforce	Disabled
ServiceNow	Disabled
SharePoint Online	Disabled

Figure 34. Onboard the Box application

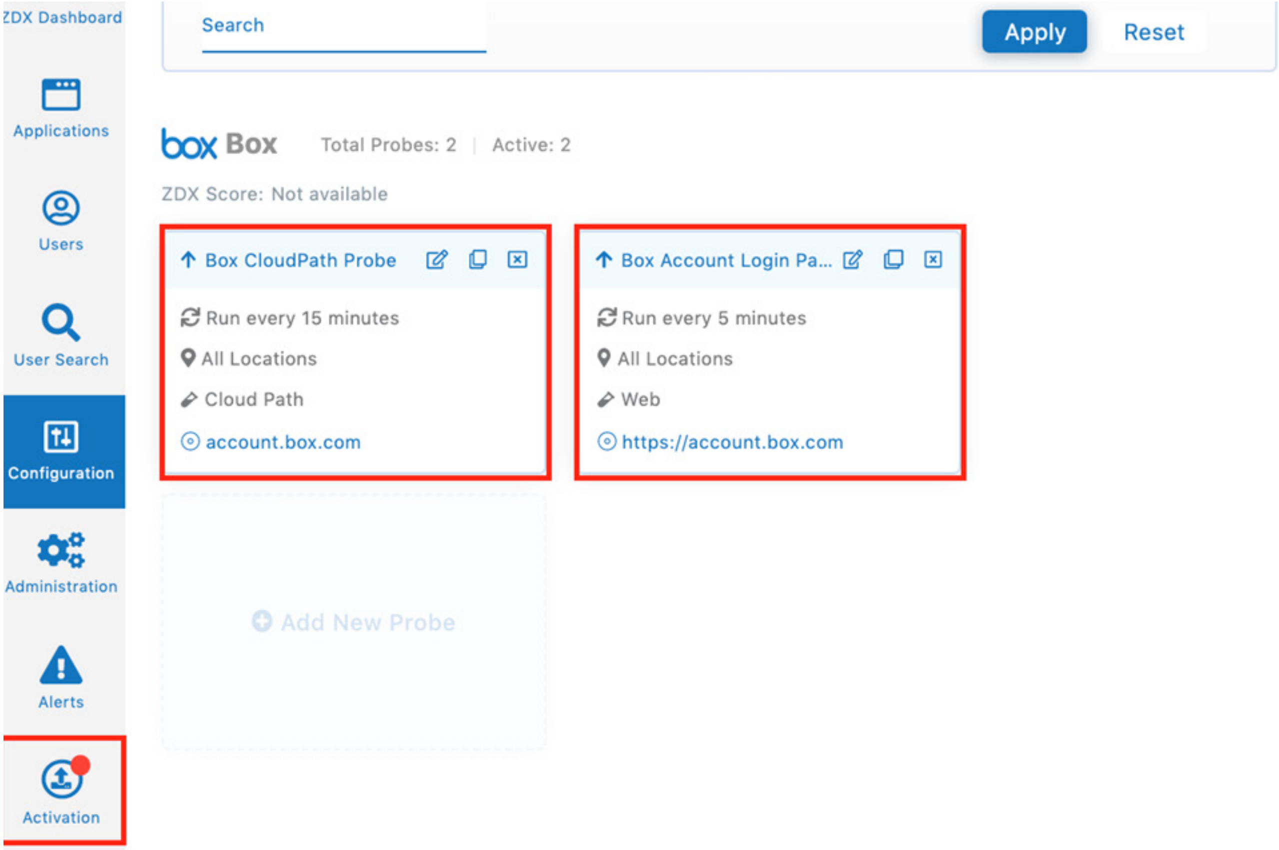
Configure Probes for Box Monitoring

After you click Go, the Box app monitoring and the preconfigured probes are displayed. The probes consist of a Network Probe, which uses an ICMP Trace Route and a Web Page Probe to the account.box.com location to monitor page load times.

Make a change to the Network Probe to have it follow the path of the Webpage Probe so there is no confusion with the results since this is entirely for Box monitoring.

To edit the rule:

1. Activate the changes.
2. Select the blue pencil to edit the probe.



Total Probes: 2 | Active: 2

ZDX Score: Not available

Box CloudPath Probe
- Run every 15 minutes
- All Locations
- Cloud Path
- account.box.com

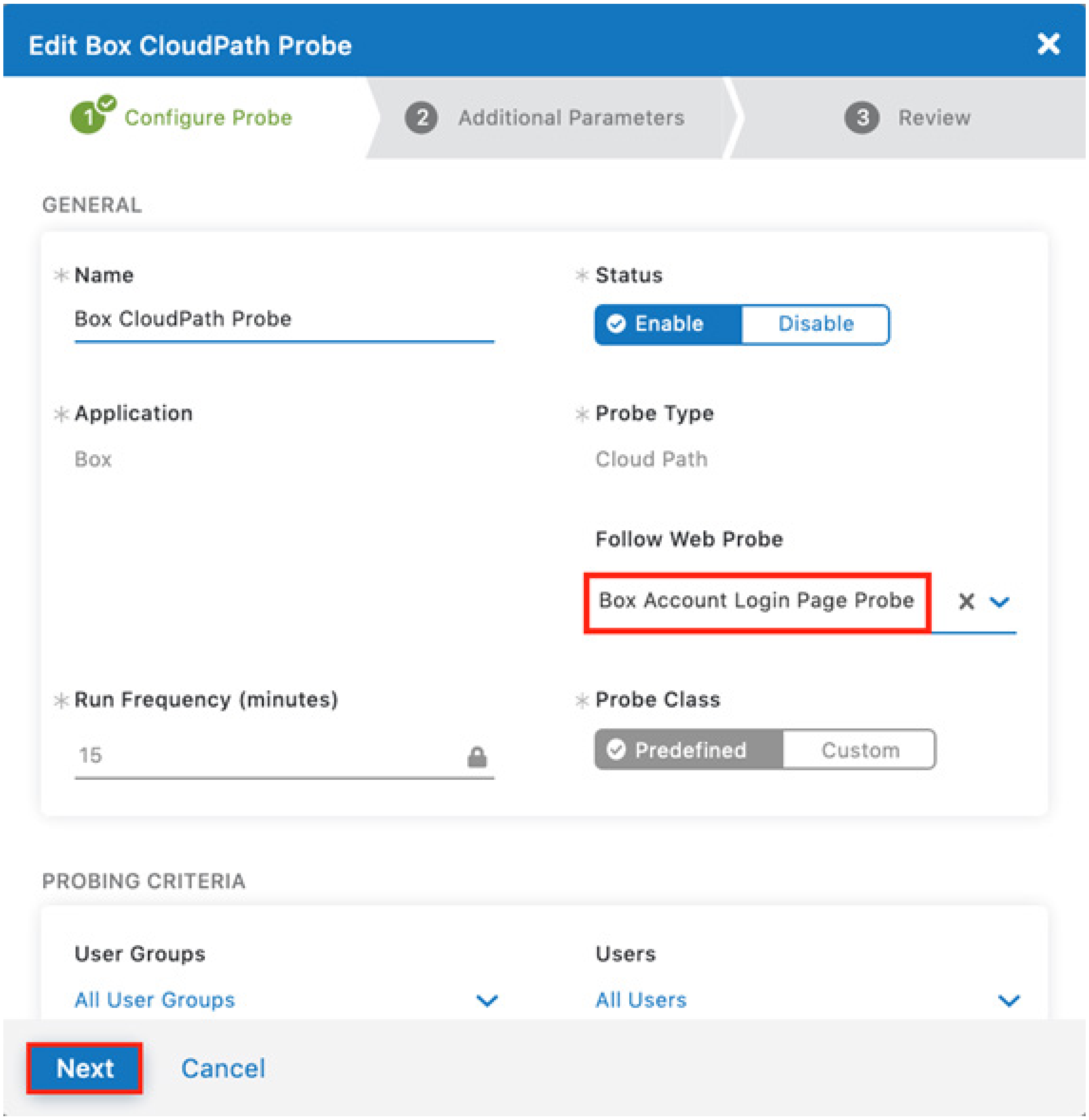
Box Account Login Pa...
- Run every 5 minutes
- All Locations
- Web
- https://account.box.com

Figure 35. ZDX for User Experience Monitoring for Box

Edit the Network Probe

To edit the network probe:

1. Select **Box Account Login Page Probe** under **Follow Web Probe**.
2. Select **Next**.



Edit Box CloudPath Probe

1 Configure Probe | 2 Additional Parameters | 3 Review

GENERAL

* Name: Box CloudPath Probe
* Status: ● Enable ○ Disable
* Application: Box
* Probe Type: Cloud Path

Follow Web Probe: Box Account Login Page Probe

* Run Frequency (minutes): 15
* Probe Class: ● Predefined ○ Custom

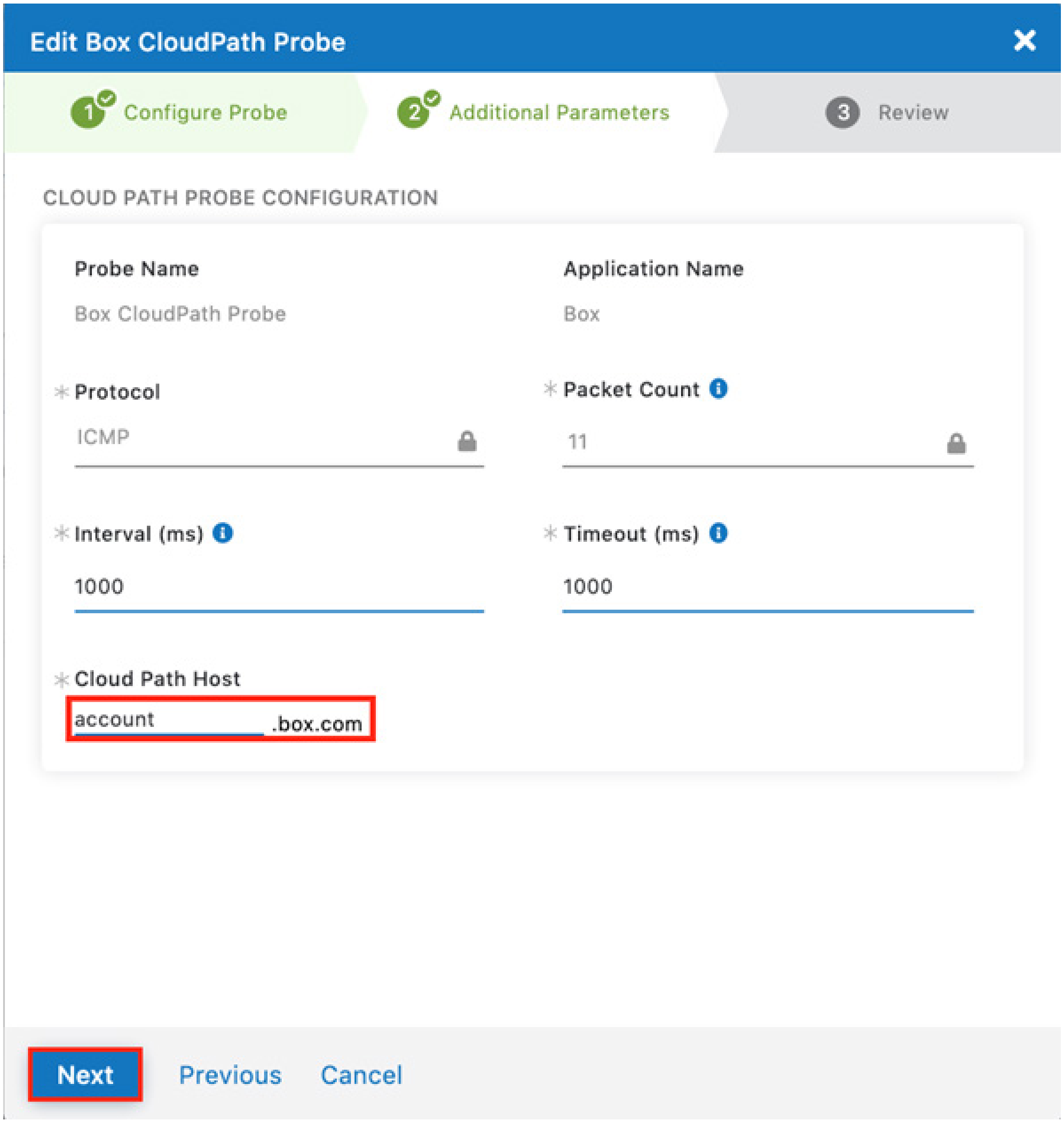
PROBING CRITERIA

User Groups: All User Groups

Users: All Users

Figure 36. Edit the network probe

3. Validate the destination host to monitor (e.g., account.box.com).
4. Select **Next**.
5. Review and activate the changes to the probe.



Edit Box CloudPath Probe

CLOUD PATH PROBE CONFIGURATION

Probe Name: Box CloudPath Probe

Application Name: Box

* Protocol: ICMP

* Packet Count: 11

* Interval (ms): 1000

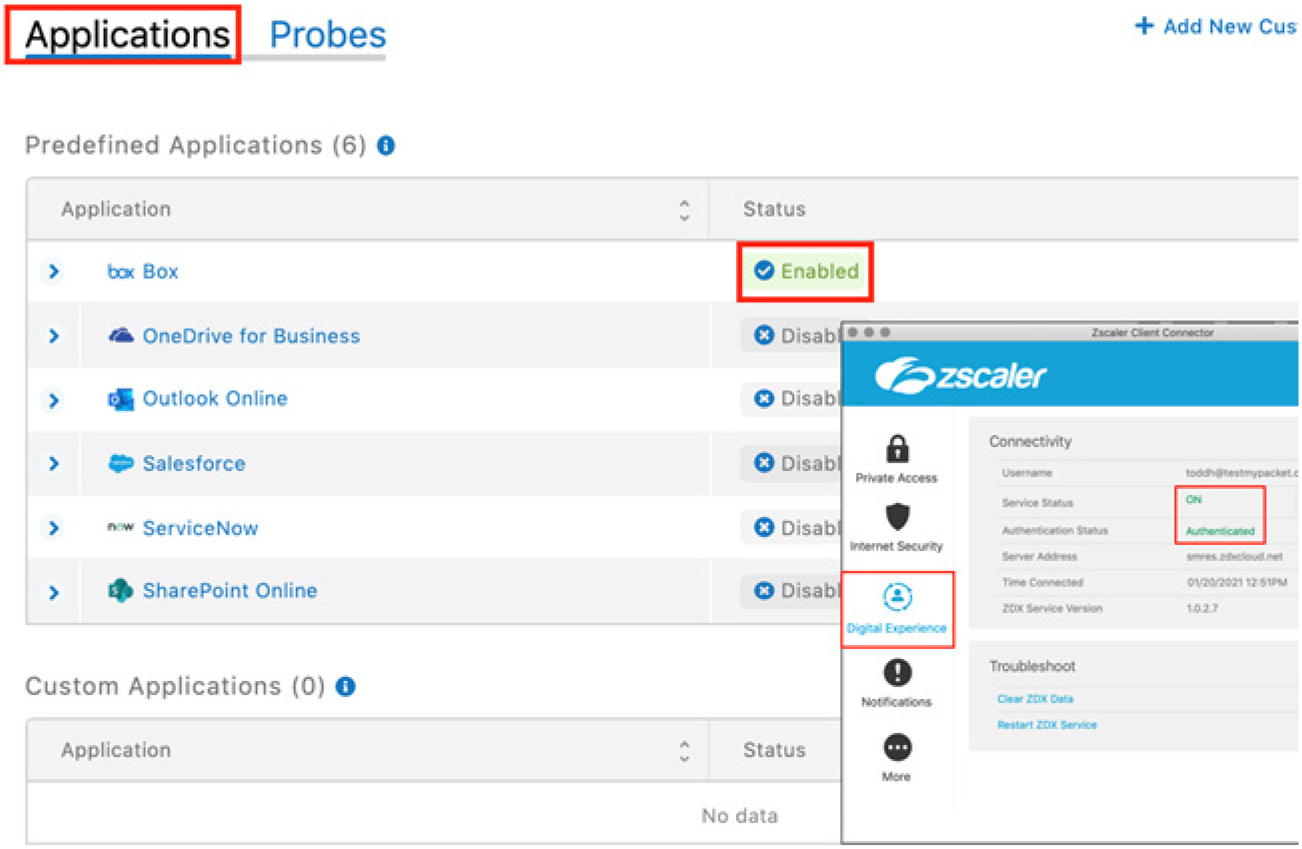
* Timeout (ms): 1000

* Cloud Path Host: account .box.com

Figure 37. Edit the network probe

The Enabled Box Application

The Box application monitoring is now activated and probes begin from all of your users that are using the Zscaler Client Connector. The following figure shows Zscaler Client Connector running Digital Experience and the Service Status is On.



Predefined Applications (6)

Application	Status
Box	Enabled
OneDrive for Business	Disabl
Outlook Online	Disabl
Salesforce	Disabl
ServiceNow	Disabl
SharePoint Online	Disabl

Custom Applications (0)

Application	Status
No data	

Connectivity

Username	toddh@testmypacket.c
Service Status	ON
Authentication Status	Authenticated
Server Address	smres.zdxcloud.net
Time Connected	01/20/2021 12:51PM
ZDX Service Version	1.0.2.7

Troubleshoot

Clear ZDX Data

Restart ZDX Service

Figure 38. Active Box monitoring

Create an Alert for the Box Service

As a final configuration step, create an alert to email Zscaler when there is service degradation of the Box application. You can configure an alert for Network, Application, or Device thresholds. You can create an alert with any of the following information.

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

To create an alert on Page Fetch Times.

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

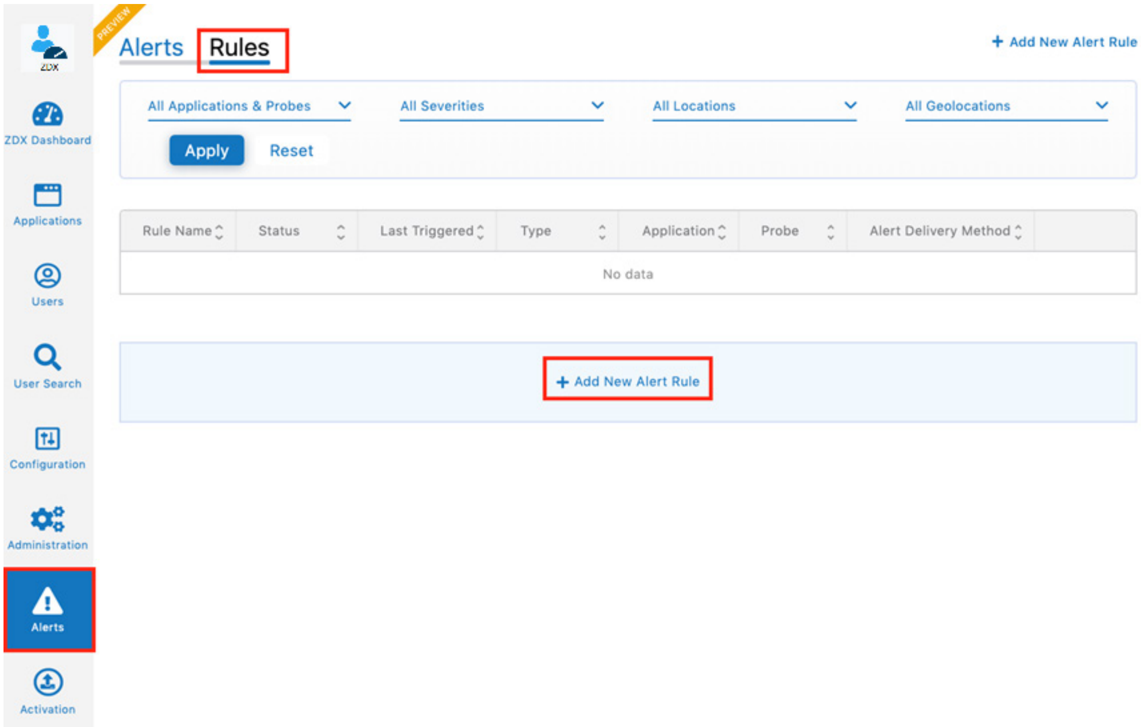
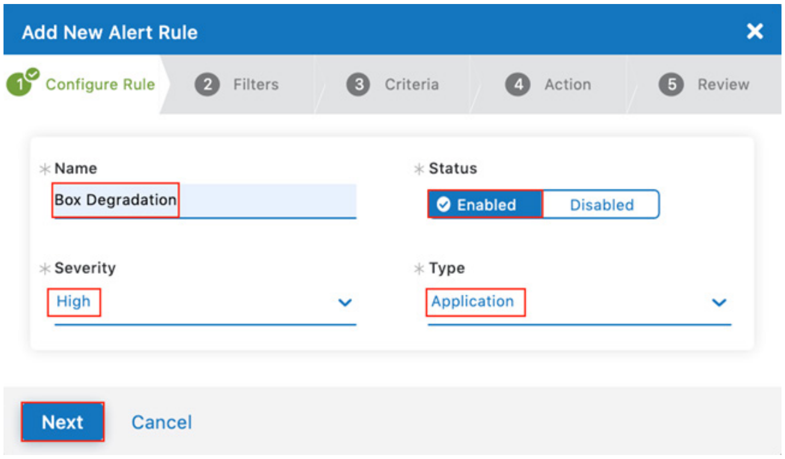


Figure 39. Creating an Alert

Run the Alert Creation wizard

Step One of the rule wizard:

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



Add New Alert Rule

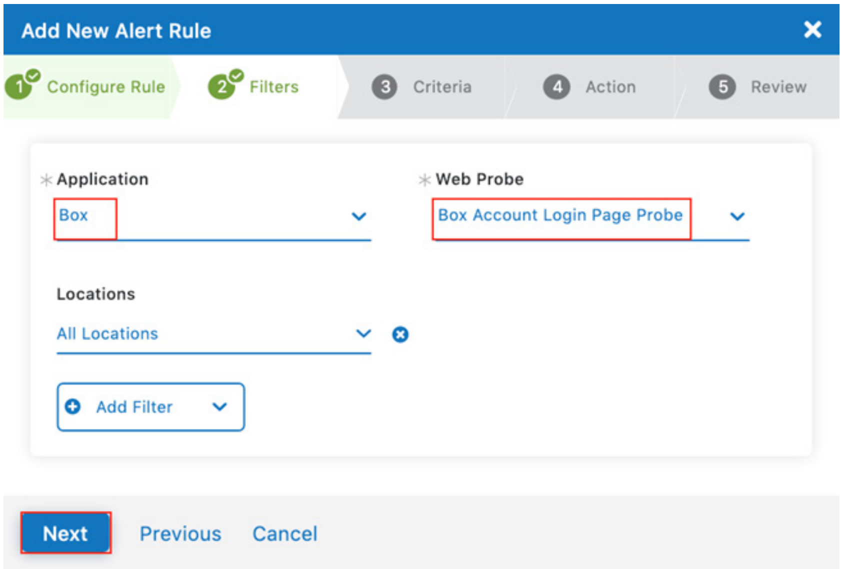
1 Configure Rule · 2 Filters · 3 Criteria · 4 Action · 5 Review

* Name: Box Degradation
* Status: Enabled | Disabled
* Severity: High
* Type: Application

Figure 40. The Alert Creation wizard

Step Two of the rule wizard.

1. Select **Box** as the application.
2. Select **Box Account Login Page Probe** for the **Web Probe**.
3. Select **Next**.



Add New Alert Rule

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

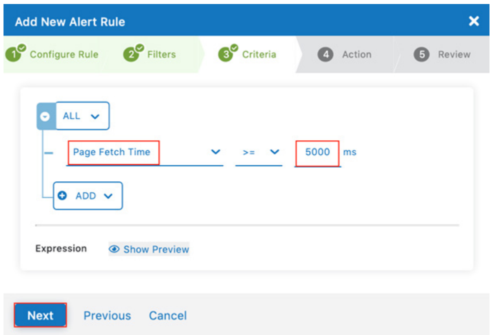
* Application: Box
* Web Probe: Box Account Login Page Probe

Locations: All Locations

Figure 41. The Alert Creation wizard (Filters)

Step Three creates the criteria, a threshold, for which the Alert is triggered if exceeded. You can use multiple variables to eliminate false positives.

1. Select **Page Fetch Time**.
2. Select the time to exceed **5000 ms**.
3. Select **Next**.



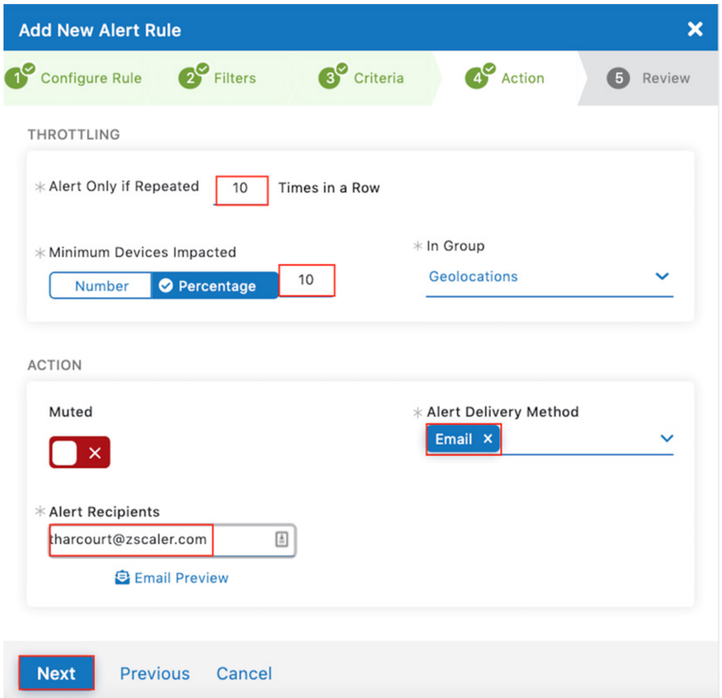
Page Fetch Time >= 5000 ms

Expression

Figure 42. The Alert Creation wizard (Criteria)

Step Four of the rule wizard adds Throttling to control the scope of the Alert. You then define the Action as Email. You can also define the action as an authenticated Webhook, which you can use to send the Alert to a Slack channel.

1. Enter `10` for the number of **Times in a Row**.
2. Enter `10` percent for the **Minimum Devices Impacted**.
3. Select **Email** as the **Alert Delivery Method**.
4. Enter the **Alert Recipients** email addresses, separated by commas.



THROTTLING

*Alert Only if Repeated 10 Times in a Row

*Minimum Devices Impacted: Number / ● Percentage 10

*In Group: Geolocations

ACTION

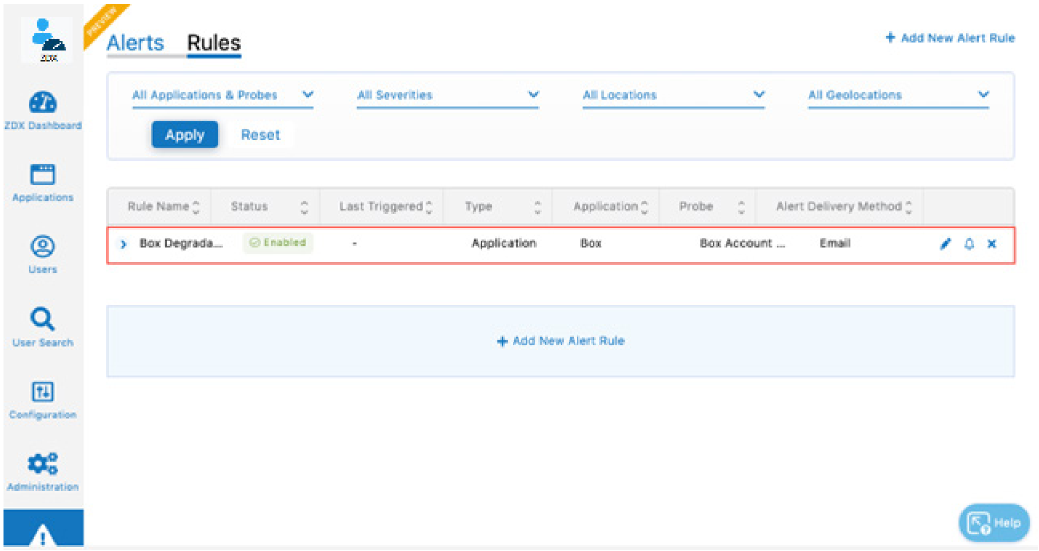
Muted: ✕

*Alert Delivery Method: Email ✕

*Alert Recipients: tharcourt@zscaler.com

Figure 43. The Alert Creation wizard (Action)

The following figure shows the completed rule set for the Alert.

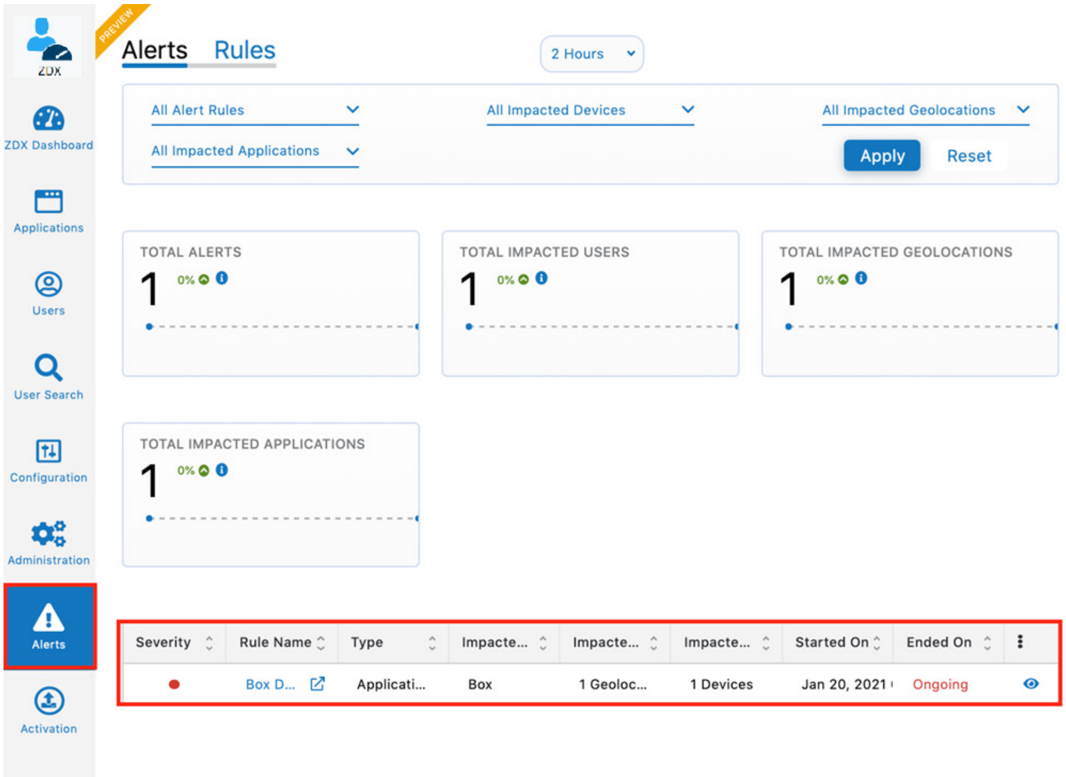


Rule Name	Status	Last Triggered	Type	Application	Probe	Alert Delivery Method
Box Degrada...	Enabled	-	Application	Box	Box Account ...	Email

Figure 44. Create an alert for the Box service (completed)

The Triggered Alert for the Box Service

The following image is the triggered alert generated by the threshold settings in the rule set that are exceeded. Click the Rule Name to review the setting or click the View icon to see more detail about the Alert.



TOTAL ALERTS 1 0%

TOTAL IMPACTED USERS 1 0%

TOTAL IMPACTED GEOLOCATIONS 1 0%

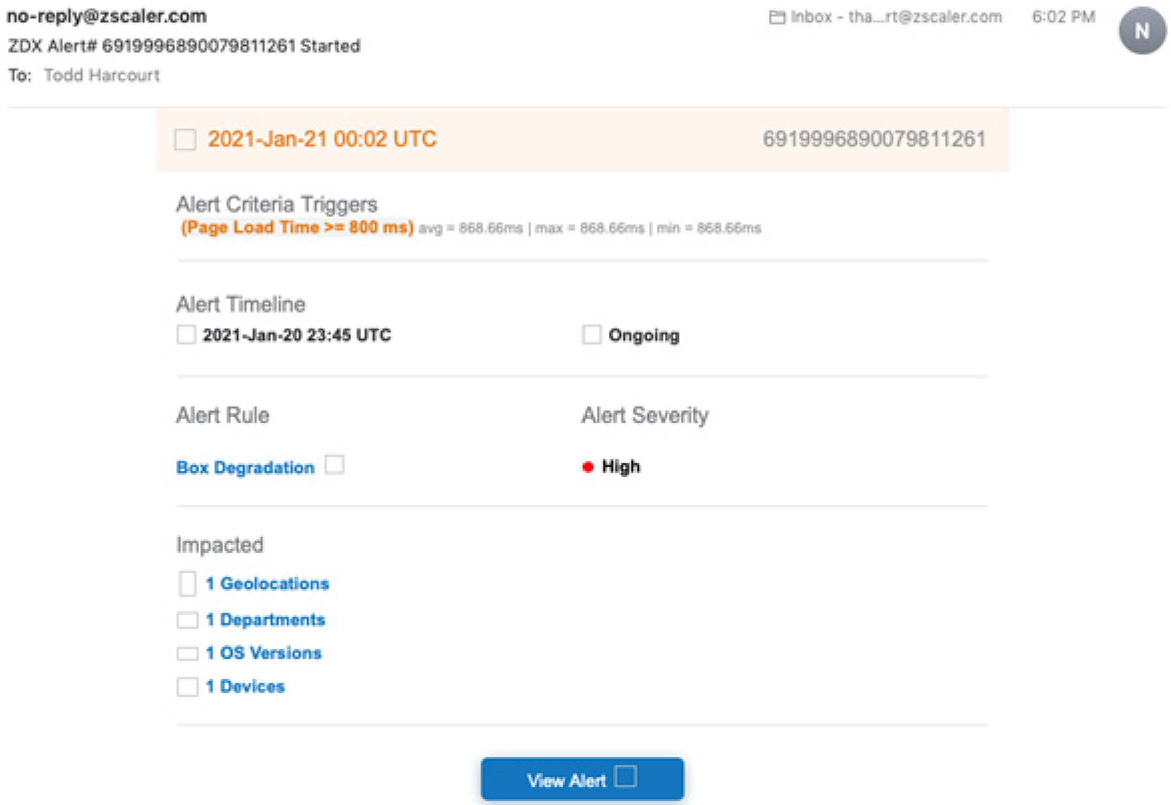
TOTAL IMPACTED APPLICATIONS 1 0%

Severity	Rule Name	Type	Impacte...	Impacte...	Impacte...	Started On	Ended On
●	Box D...	Applicati...	Box	1 Geoloc...	1 Devices	Jan 20, 2021	Ongoing

Figure 45. The Alert

The Sent Alert Email for the Box Service

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



no-reply@zscaler.com
ZDX Alert# 6919996890079811261 Started
To: Todd Harcourt

□ 2021-Jan-21 00:02 UTC 6919996890079811261

Alert Criteria Triggers
(Page Load Time >= 800 ms) avg = 868.66ms | max = 868.66ms | min = 868.66ms

Alert Timeline
□ **2021-Jan-20 23:45 UTC** □ **Ongoing**

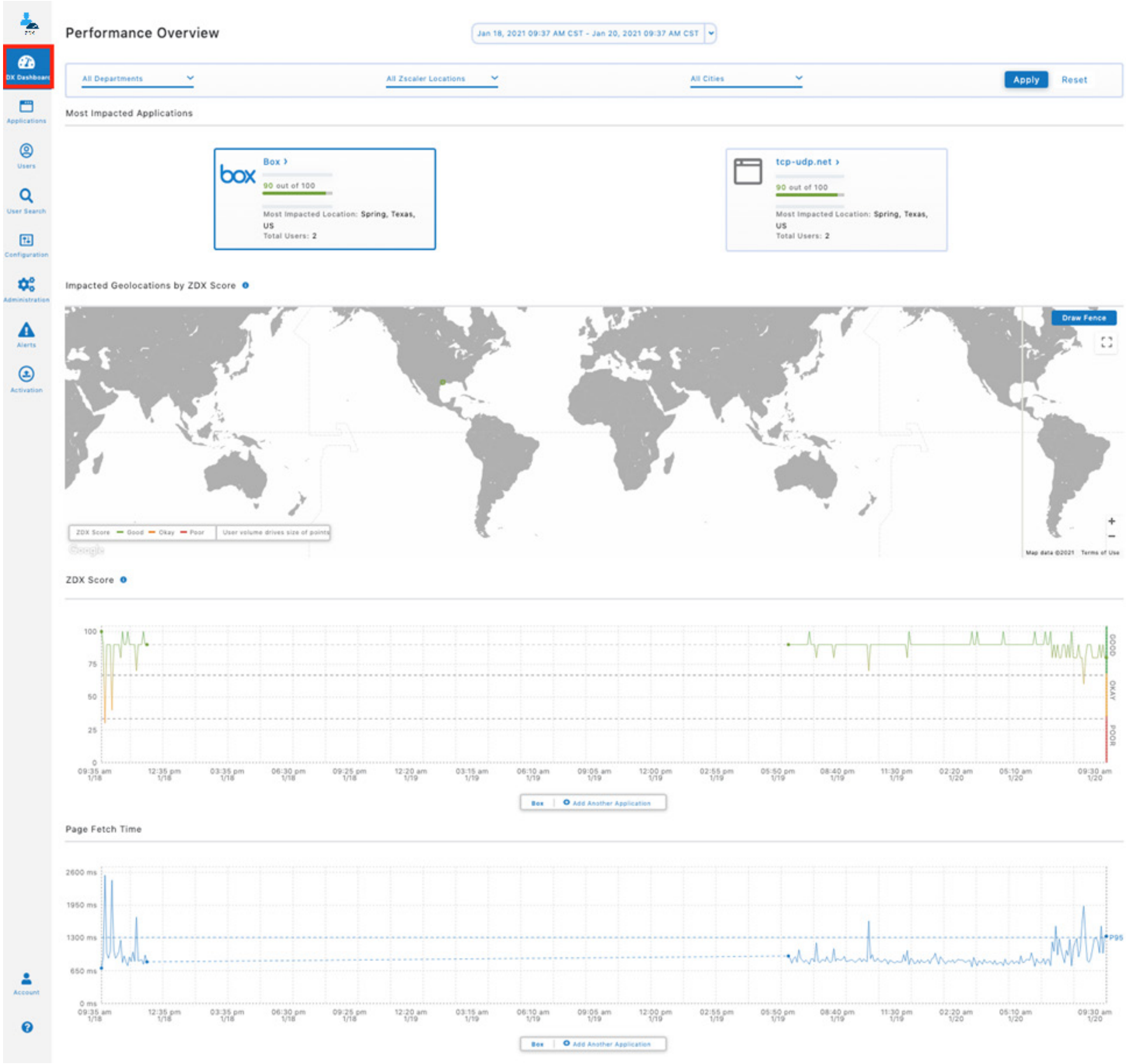
Alert Rule: **Box Degradation** □
Alert Severity: ● **High**

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

Figure 46. The Alert email

Using ZDX—The Dashboard

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



Jan 18, 2021 09:37 AM CST - Jan 20, 2021 09:37 AM CST

Box ›
90 out of 100
Most Impacted Location: Spring, Texas, US
Total Users: 2

tcp-udp.net ›
90 out of 100
Most Impacted Location: Spring, Texas, US
Total Users: 2

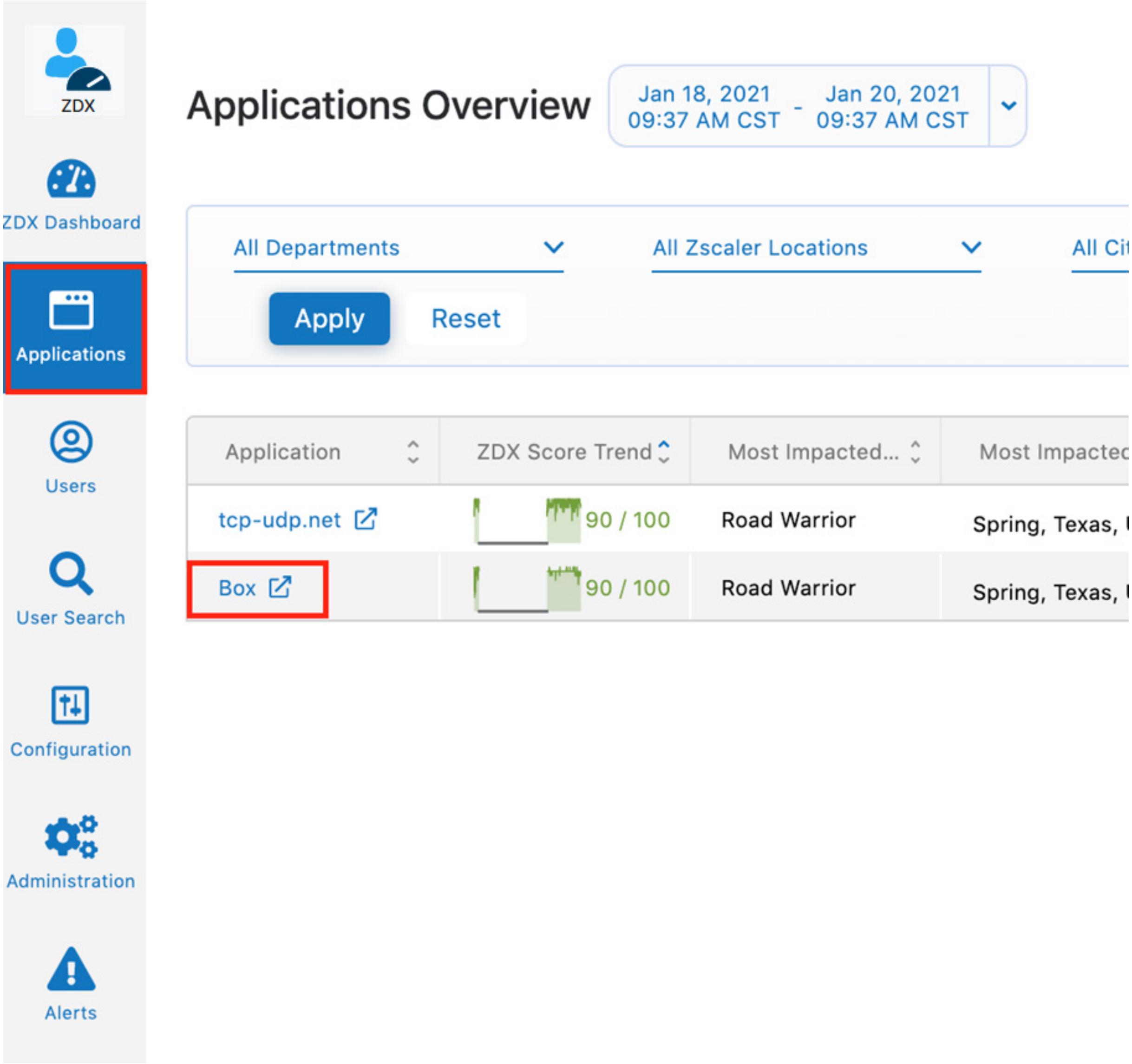
Figure 47. The ZDX Dashboard

Using ZDX—Application Overview

Selecting Applications in the left-side navigation brings up the Applications Overview and shows the configured applications and the individual ZDX score.

To open the details of the Box application:

1. Select **Applications**.
2. Select the **Box App**.



Jan 18, 2021 09:37 AM CST - Jan 20, 2021 09:37 AM CST

Application	ZDX Score Trend	Most Impacted...	Most Impacted
tcp-udp.net	90 / 100	Road Warrior	Spring, Texas,
Box	90 / 100	Road Warrior	Spring, Texas,

Figure 48. Applications Overview

Application Detail

The top portion of the application detail shows a historical view of the ZDX score and the Page Fetch Time. The spike of the page fetch time indicates a possible slowdown of the Box service.

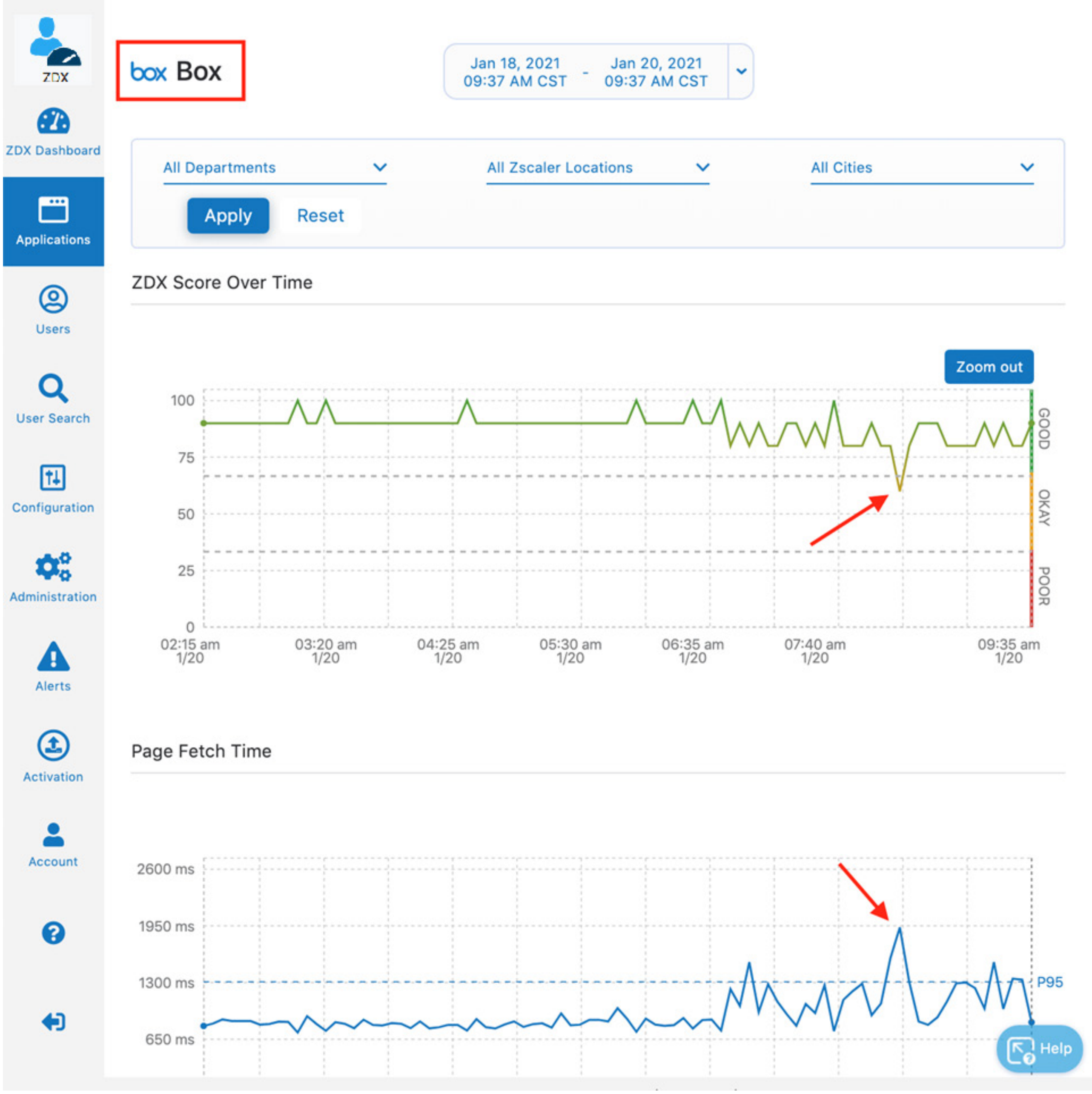
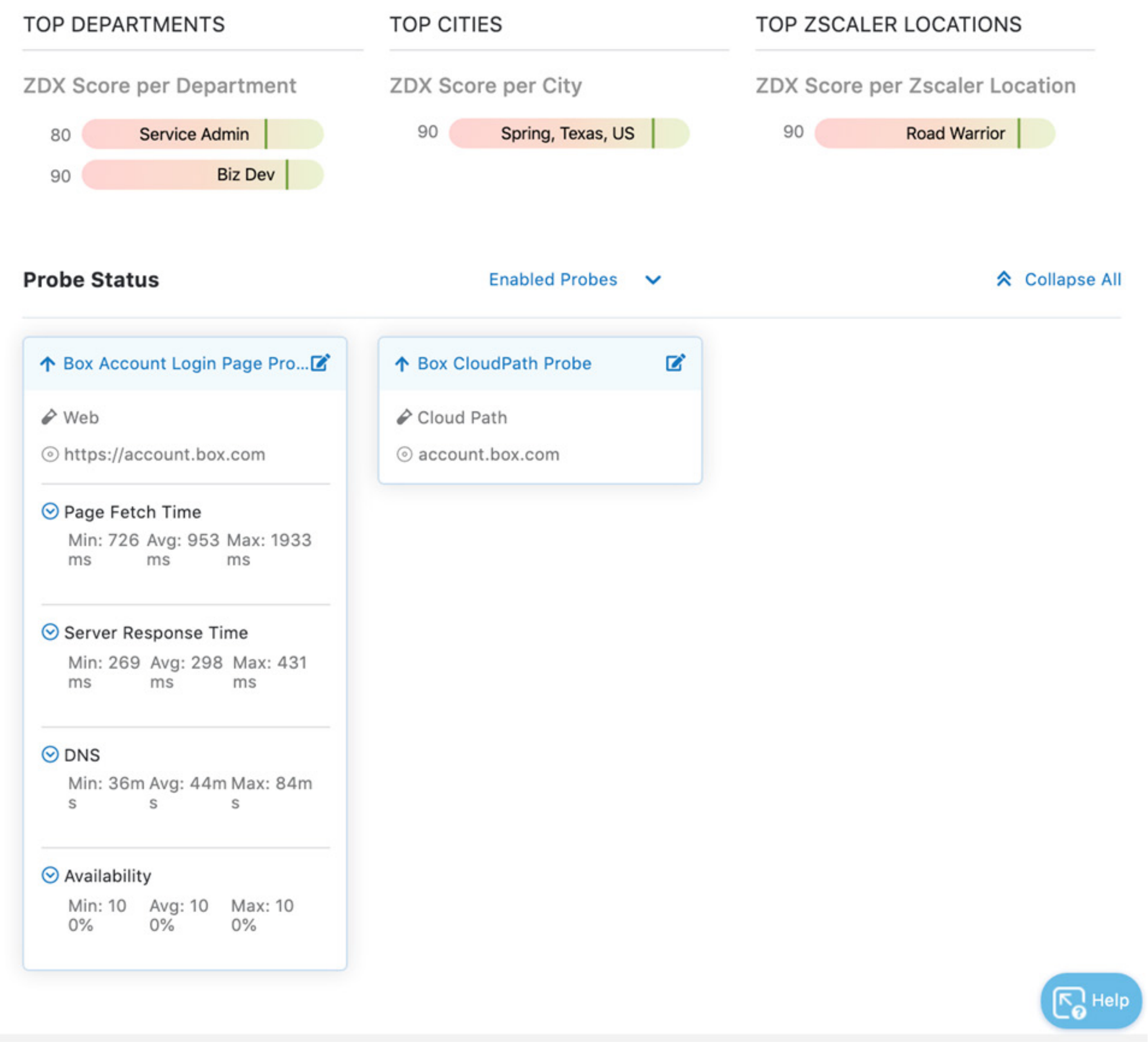


Figure 49. Application Detail

The bottom portion of the Application Detail shows the Top Departments, Top Cities, and Top Zscaler Locations using the Application, and the ZDX Scores at a glance. You can also see the probe data, with minimum, maximum, and average response times.



TOP DEPARTMENTS

ZDX Score per Department

80	Service Admin
90	Biz Dev

TOP CITIES

ZDX Score per City

90	Spring, Texas, US

TOP ZSCALER LOCATIONS

ZDX Score per Zscaler Location

90	Road Warrior

Probe Status

Box Account Login Page Pro...

Web

https://account.box.com

Page Fetch Time

Min: 726 ms Avg: 953 ms Max: 1933 ms

Server Response Time

Min: 269 ms Avg: 298 ms Max: 431 ms

DNS

Min: 36ms Avg: 44ms Max: 84ms

Availability

Min: 100% Avg: 100% Max: 100%

Box CloudPath Probe

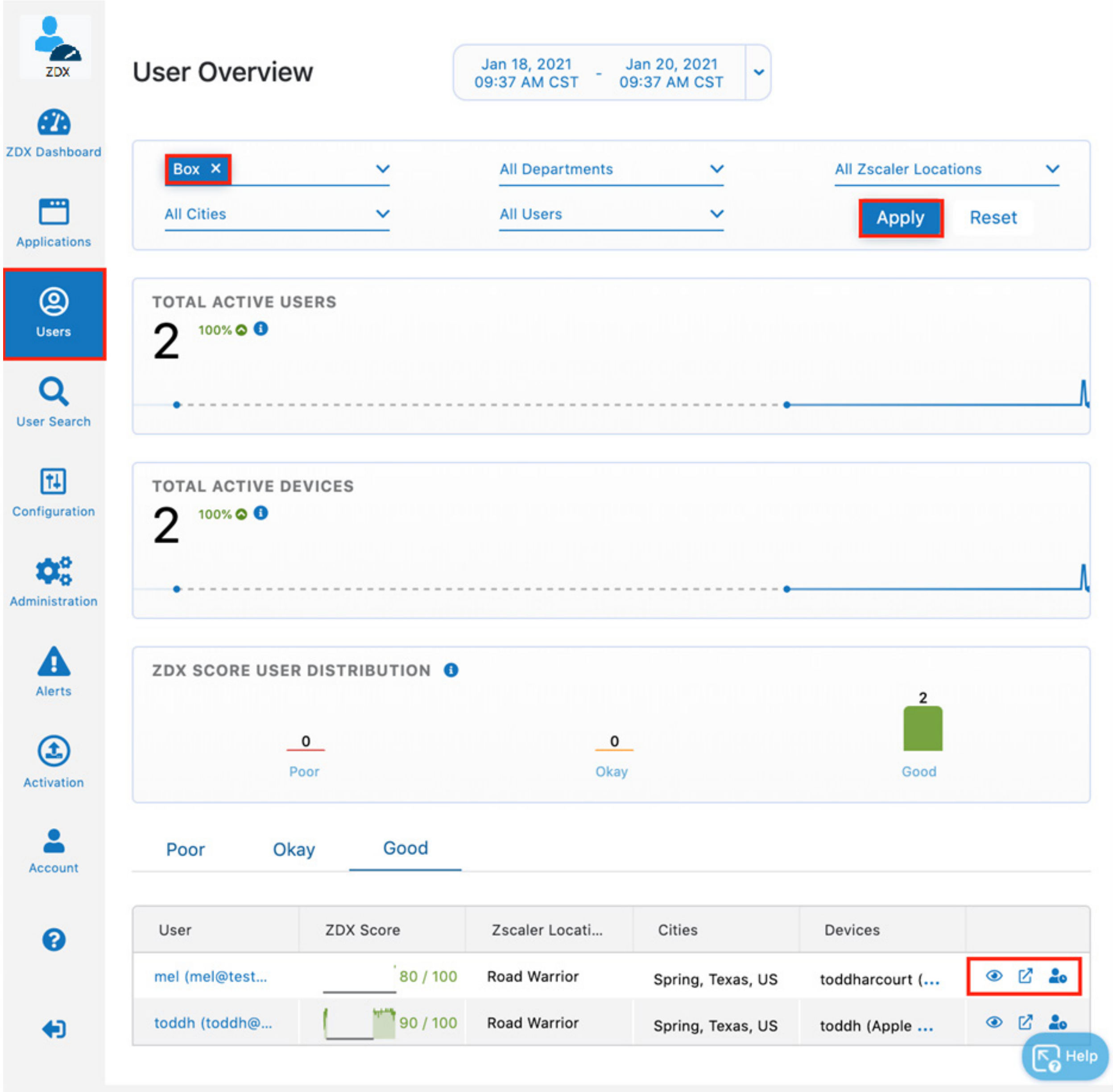
Cloud Path

account.box.com

Figure 50. Application Detail

User Overview

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



User Overview

Jan 18, 2021 09:37 AM CST - Jan 20, 2021 09:37 AM CST

Box ×

All Departments

All Zscaler Locations

All Cities

All Users

TOTAL ACTIVE USERS

2 100%

TOTAL ACTIVE DEVICES

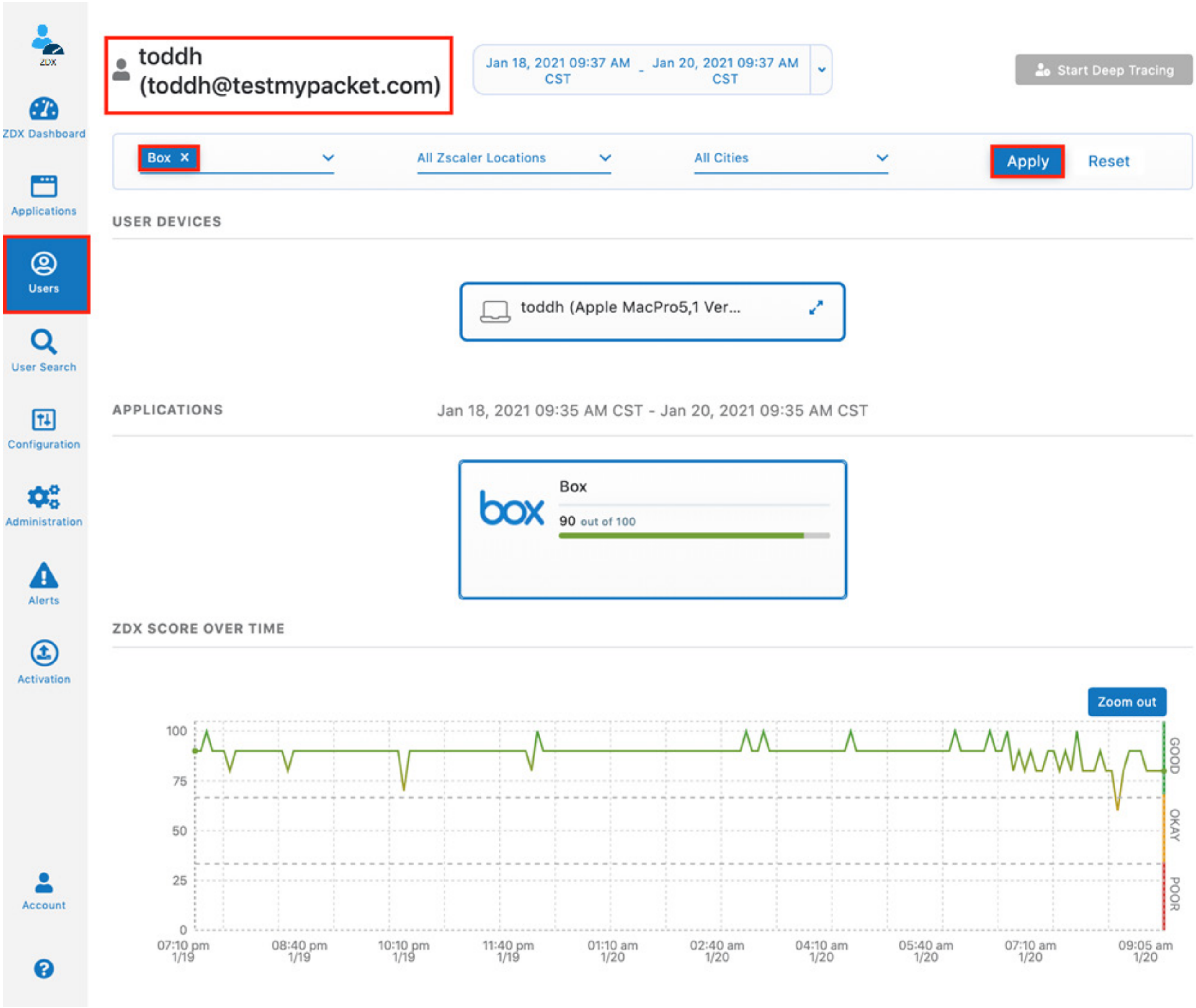
2 100%

ZDX SCORE USER DISTRIBUTION

User	ZDX Score	Zscaler Locati...	Cities	Devices
mel (mel@test...	80 / 100	Road Warrior	Spring, Texas, US	toddharcourt (...
toddh (toddh@...	90 / 100	Road Warrior	Spring, Texas, US	toddh (Apple ...

Figure 51. User Overview

The top portion of the User Detail shows very useful data to help isolate any user experience issues. Select and apply the Box application to see the details of the user experience for the Box app. This report provides the User Devices and provides the device-specific details (OS, Device type, Network Information, etc.) by clicking the device. The ZDX Score is also displayed in a timeline, and details of Page Fetch Times, Server Response, DNS Response, Probe Detail, and Device Health are all shown on this page.



toddh (toddh@testmypacket.com)

Jan 18, 2021 09:37 AM CST - Jan 20, 2021 09:37 AM CST

Box × | All Zscaler Locations | All Cities

USER DEVICES

toddh (Apple MacPro5,1 Ver...

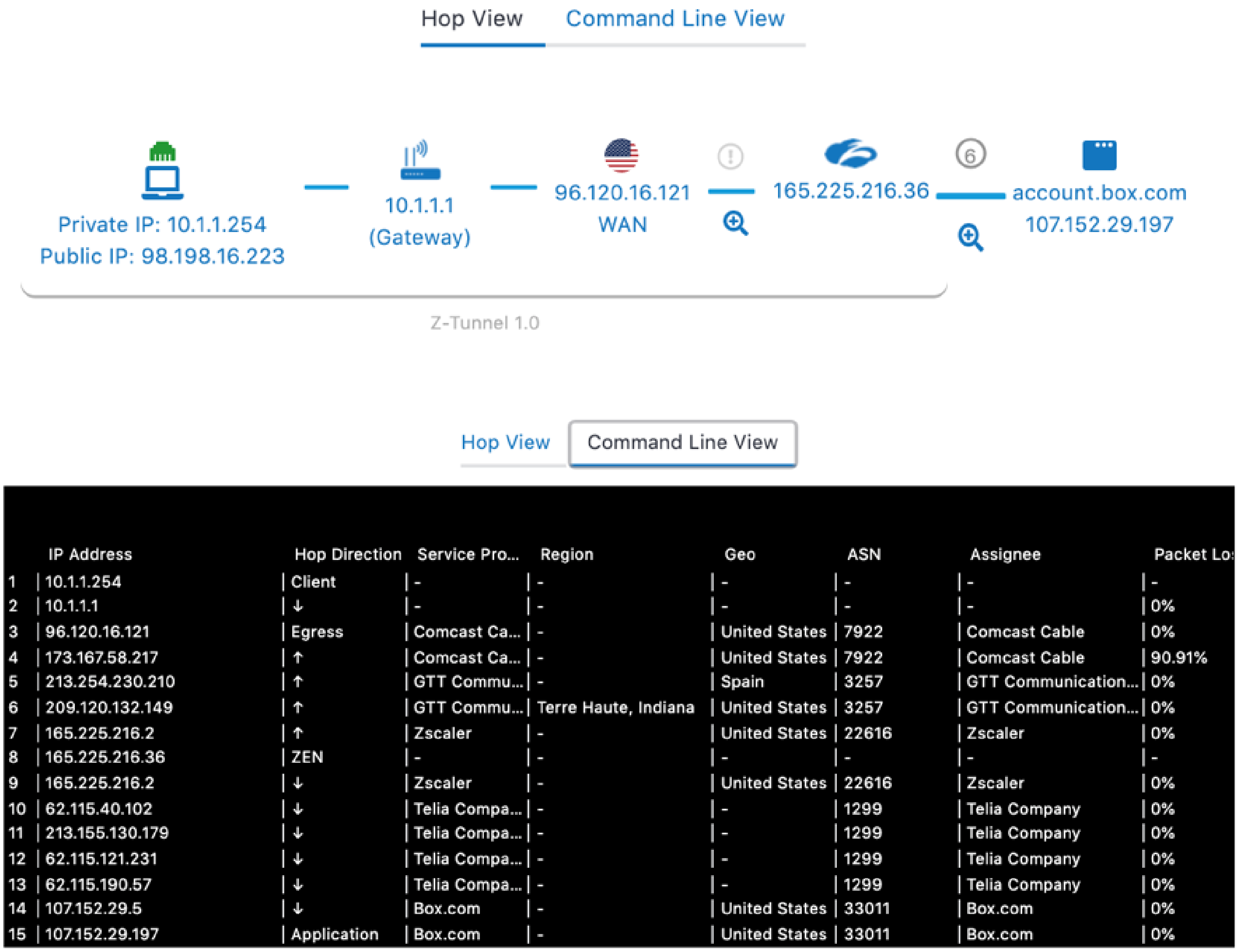
APPLICATIONS Jan 18, 2021 09:35 AM CST - Jan 20, 2021 09:35 AM CST

Box
90 out of 100

ZDX SCORE OVER TIME

Figure 52. User Detail

The following figure is the end-to-end visibility of the Data Path the user is taking to get to the Box SaaS service. If there is any issue from the user's device health, the network at the home office, any Service Provider in the path, or an issue with the Box SaaS itself, ZDX provides visibility from the cloud to the Zscaler administrators from any of their users' individual environments.



```
     IP Address        Hop Direction   Service Pro...  Region                  Geo             ASN     Assignee                Packet Lo:
1  | 10.1.1.254      | Client        | -             | -                     | -             | -     | -                     | -
2  | 10.1.1.1        | ↓             | -             | -                     | -             | -     | -                     | 0%
3  | 96.120.16.121   | Egress        | Comcast Ca... | -                     | United States | 7922  | Comcast Cable         | 0%
4  | 173.167.58.217  | ↑             | Comcast Ca... | -                     | United States | 7922  | Comcast Cable         | 90.91%
5  | 213.254.230.210 | ↑             | GTT Commu...  | -                     | Spain         | 3257  | GTT Communication...  | 0%
6  | 209.120.132.149 | ↑             | GTT Commu...  | Terre Haute, Indiana  | United States | 3257  | GTT Communication...  | 0%
7  | 165.225.216.2   | ↑             | Zscaler       | -                     | United States | 22616 | Zscaler               | 0%
8  | 165.225.216.36  | ZEN           | -             | -                     | -             | -     | -                     | -
9  | 165.225.216.2   | ↓             | Zscaler       | -                     | United States | 22616 | Zscaler               | 0%
10 | 62.115.40.102   | ↓             | Telia Compa...| -                     | -             | 1299  | Telia Company         | 0%
11 | 213.155.130.179 | ↓             | Telia Compa...| -                     | -             | 1299  | Telia Company         | 0%
12 | 62.115.121.231  | ↓             | Telia Compa...| -                     | -             | 1299  | Telia Company         | 0%
13 | 62.115.190.57   | ↓             | Telia Compa...| -                     | -             | 1299  | Telia Company         | 0%
14 | 107.152.29.5    | ↓             | Box.com       | -                     | United States | 33011 | Box.com               | 0%
15 | 107.152.29.197  | Application   | Box.com       | -                     | United States | 33011 | Box.com               | 0%
```

Figure 53. End-to-End connection detail

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support:

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

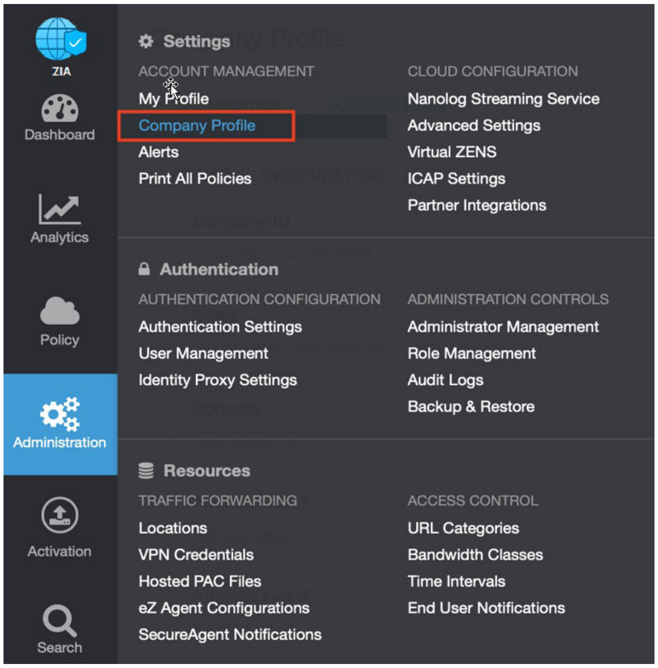
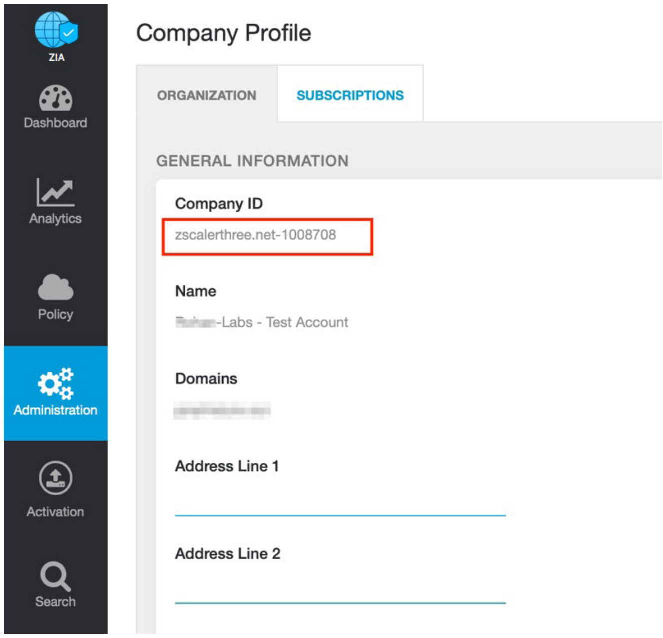


Figure 54. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 55. Company ID

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

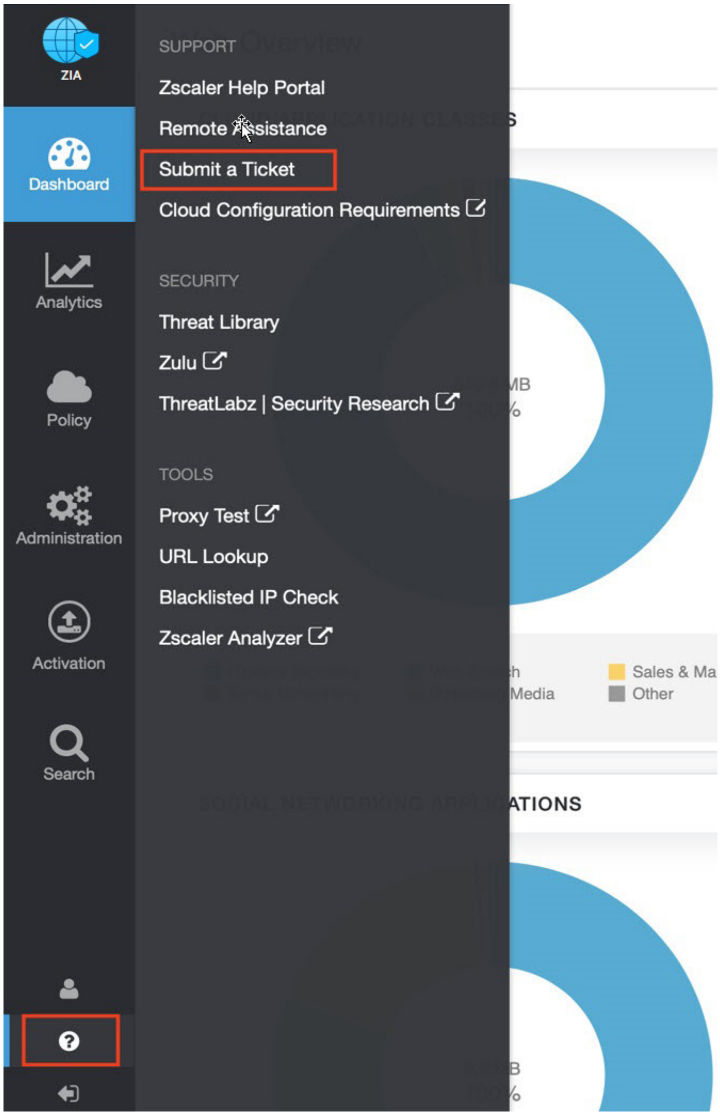


Figure 56. Submit a ticket