# ZSCALER AND MICROSOFT SHAREPOINT ONLINE DEPLOYMENT GUIDE

FEBRUARY 2022, VERSION 1.1

BUSINESS DEVELOPMENT GUIDE

# Contents

# Terms and Acronyms

The following table defines acronyms used in this deployment guide.

| Acronym | Definition |
|---|---|
| ASIC | Application-Specific Integrated Circuit |
| CA | Central Authority (Zscaler) |
| CPU | Central Processing Unit |
| CSV | Comma-Separated Values |
| DLP | Data Loss Prevention |
| DNS | Domain Name System |
| 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 |
| POSIX | Portable Operating System Interface |
| PSK | Pre-Shared Key |
| SaaS | Software as a Service |
| SSL | Secure Socket Layer (RFC6101) |
| TLS | Transport Layer Security |
| VDI | Virtual Desktop Infrastructure |
| XFF | X-Forwarded-For (RFC7239) |
| ZCP | Zscaler Cloud Protection |
| ZDX | Zscaler Digital Experience |
| ZIA | Zscaler Internet Access (Zscaler) |
| ZEN | Zscaler Enforcement Node (Zscaler) |
| ZPA | Zscaler Private Access (Zscaler) |

# About This Document

## 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. For more information, see **Zscaler's website** or follow Zscaler on Twitter **@zscaler**.

## Microsoft Overview

Microsoft (Nasdaq: MSFT), Microsoft develops and licenses consumer and enterprise software. It is known for its Windows operating systems and Office productivity suite. The company is organized into three equally sized broad segments: productivity and business processes (legacy Microsoft Office, cloud-based Office 365, Exchange, SharePoint, Skype, LinkedIn, Dynamics), intelligence cloud (infrastructure- and platform-as-a-service offerings Azure, Windows Server OS, SQL Server), and more personal computing (Windows Client, Xbox, Bing search, display advertising, and Surface laptops, tablets, and desktops).

## Audience

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

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

## Software Versions

This document was authored using ZIA and ZPA (with Zscaler Client Connector) along with SharePoint Online Microsoft 365.

## Request for Comments

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

# Zscaler and Microsoft SharePoint Introduction

## Zscaler Overview

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

### ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet onramp—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 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, data loss prevention (DLP), SaaS Security, and browser isolation, allowing you start with the services you need now and activate others as your needs grow.

### ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user’s device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

### 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. |
| Adding SaaS Application Tenant | ZIA help article for adding SaaS application tenants. |
| SaaS Security API DLP Policy | ZIA help article for creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications. |
| SaaS Security Insights | ZIA help article for viewing and defining information that you want to view when analyzing files scanned through charts. |
| SaaS Posture Security | ZIA help article on recommended security policies to decrease security risks for your organization's SaaS applications. |
| SaaS Identity Proxy | ZIA help article for configuring Zscaler as an Identity Provider (IdP) for the following cloud apps. |
| About Data Loss Prevention | ZIA help article on different types of DLP policy rules. |
| About DLP Dictionaries | ZIA help article on creating custom dictionaries for DLP content. |
| Adding Custom DLP Engines | ZIA help article on adding a custom DLP engine. |
| Cloud Application Access Control | ZIA help article on providing granular control over popular websites and applications. |
| ZDX Predefined Applications | ZIA help article on providing quick and seamless application onboarding for admins. |
| 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. |

## SharePoint Overview

Organizations use Microsoft SharePoint to create websites. You can use it as a secure place to store, organize, share, and access information from any device. All you need is a web browser, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.

SharePoint can refer to one or more SharePoint products or technologies, including:

- **SharePoint in Microsoft 365**. A cloud-based service, hosted by Microsoft, for businesses of all sizes. Instead of installing and deploying SharePoint Server on-premises, any business can subscribe to a Microsoft 365 plan or to the standalone SharePoint Online service. Your employees can create sites to share documents and information with colleagues, partners, and customers.
- **SharePoint Server**. Organizations can deploy and manage SharePoint Server on-premises or with an Office 365 Enterprise subscription to take advantage of all the latest features. It offers additional features and capabilities, such as site pages, web parts and authoring, lists and libraries, search, integration with PowerApps, Power BI and MS Flow, and SharePoint home page.
- **SharePoint Designer 2013**. A free program last released in 2013. Use it to build powerful, workflow-enabled solutions. You can edit external content types for an external data solution based on Business Connectivity Services.
- **OneDrive sync**. A desktop program that you can use to sync documents from a team site or OneDrive for work or school to your computer for offline use.

This guide is specific to SharePoint Online for Microsoft 365.

### SharePoint Resources

The following table contains links to Microsoft SharePoint support resources.

| Name | Definition |
|---|---|
| About SharePoint | Website where you can watch a video on SharePoint uses, features, and applications. |
| SharePoint Community | A SharePoint community for news, announcements, and best practices. |
| SharePoint Support | Microsoft support portal. |

# Zscaler Data Protection and Digital Experience for SharePoint.com

Microsoft is one of the industry leaders that defined the advantages SaaS applications and the cloud can provide to an enterprise. SaaS services are popular because of the collaboration and ease of use, enabling sharing globally. However, the downside of this ease of access and sharing is risk. It is impossible to train every employee to always use best practices with SaaS applications, which can lead to costly mistakes for the organization. Risk associated with accidental data exposure, malicious intent, and compliance violations, can force companies to restrict or prevent use of these incredible business tools.

Another challenge faced by organizations migrating to cloud services in today's environment has been the ability to monitor the users' experience for the SaaS application. In today's work from anywhere corporate infrastructures, Zscaler provides a complete SharePoint solution using ZIA for security of SharePoint and Zscaler Digital Exchange (ZDX), for visibility of the users' experience.

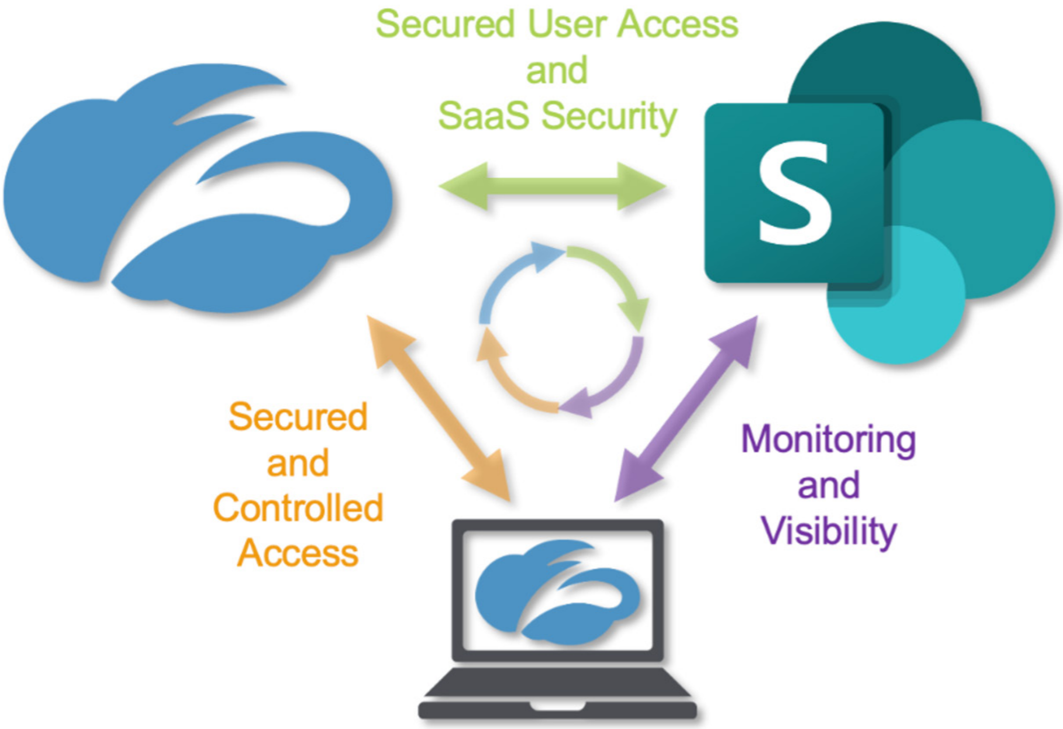


*Figure 1. Zscaler solutions for SharePoint*

## Overview

ZIA provides SharePoint security by using access control, identity control, SaaS security posture management, and the SaaS Security API to scan the SharePoint attachments for malicious content and provide DLP. ZIA also provides complete security for clients whether they are in the corporate office or their home office.

The ZDX service provides user-specific experience monitoring and visibility to the SharePoint service that helps organizations address any user experience concerns or challenges. ZDX has preconfigured monitors for SharePoint that provide performance monitoring and measurements from the users' device running the Zscaler Client Connector. These monitors provide detailed information on the user's device, the network path to SharePoint, and the SharePoint SaaS performance itself. This information is invaluable to operations when a user is experiencing issues with SharePoint and provides visibility to every corner of the internet.

Both SaaS security 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 Microsoft's SharePoint services.

This guide covers the following ZIA features for SharePoint Security, and the ZDX for SharePoint performance visibility.

- Configuring SharePoint SaaS Security
- Configuring SharePoint SaaS Data Loss Prevention
- Configuring SharePoint SaaS Malware Detection
- SaaS Security Reporting and Visibility
- Configuring SSL Inspection for SharePoint
- ZIA Cloud Application Control
- ZDX for SharePoint

### ZIA SaaS Security API Data and Malware Protection for SharePoint

The 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 with SaaS partners by preventing data exposure and ensuring compliance across the SaaS application.

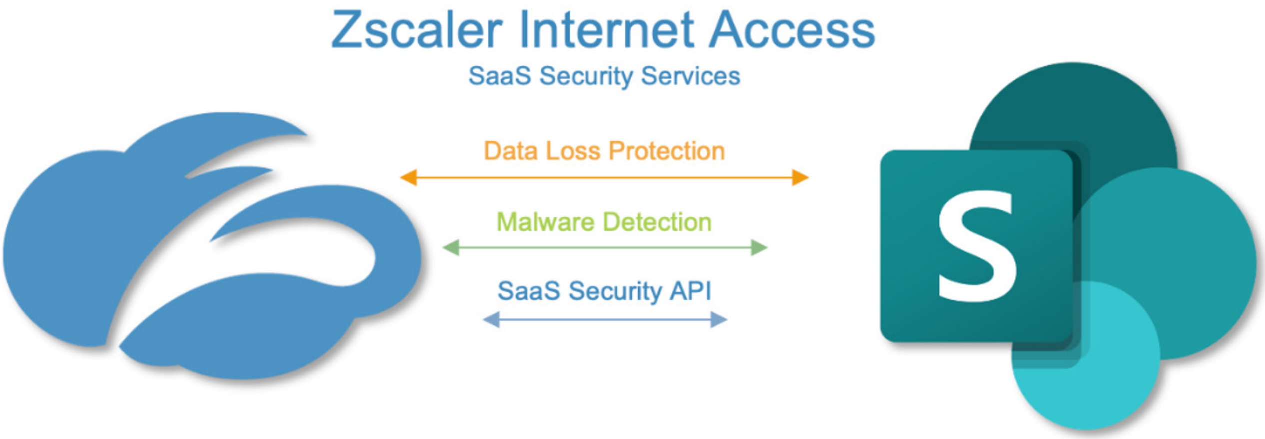


*Figure 2. Zscaler SaaS Security API in use with SharePoint*

The SaaS Security API enables organizations to securely adopt and govern the use of multiple SaaS applications. It provides real-time visibility, controlling 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 API unique?

- **Data exposure reporting and remediation**. The SaaS Security API checks SaaS applications and cloud providers' configurations and compares them to industry and organizational benchmarks to report on violations and automate remediation.
- **Threat identification and remediation**. The SaaS Security API checks SaaS applications for hidden threats being exchanged and prevents their propagation.
- **Compliance assurance**. The SaaS Security API provides compliance visibility across SaaS and cloud providers and can mitigate violations automatically.
- **Part of a larger data protection platform**. The Zscaler Zero Trust Exchange 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 ZPA for Zero Trust access to internal applications, ZDX for active monitoring of a users' experience to SaaS applications, and Zscaler Cloud Protection (ZCP) for cloud security. Zscaler provides end-to-end connectivity, security, and visibility from any location on-prem or remote.

For more information, see **Zscaler Resources**.

### ZIA SSL Inspection for SharePoint

Up to 94% of traffic traversing the internet is encrypted using SSL or TLS to protect data that is confidential and sensitive. This data is transported across the internet between browsers and cloud apps. As you connect to websites, an encrypted connection between your browser and the website (cloud application) is established.

While this encryption protects the sensitive data, it is important to mitigate risk within this traffic. Advanced threats and malware are routinely delivered within encrypted traffic. SSL decryption enables organizations to open encrypted traffic in a safe and controlled manner and inspect the data to identify threats inbound to applications, as well as outbound from users to the internet. The traffic is then re-encrypted and sent on its way. Inspecting encrypted traffic is nontrivial and it requires a proxy architecture.

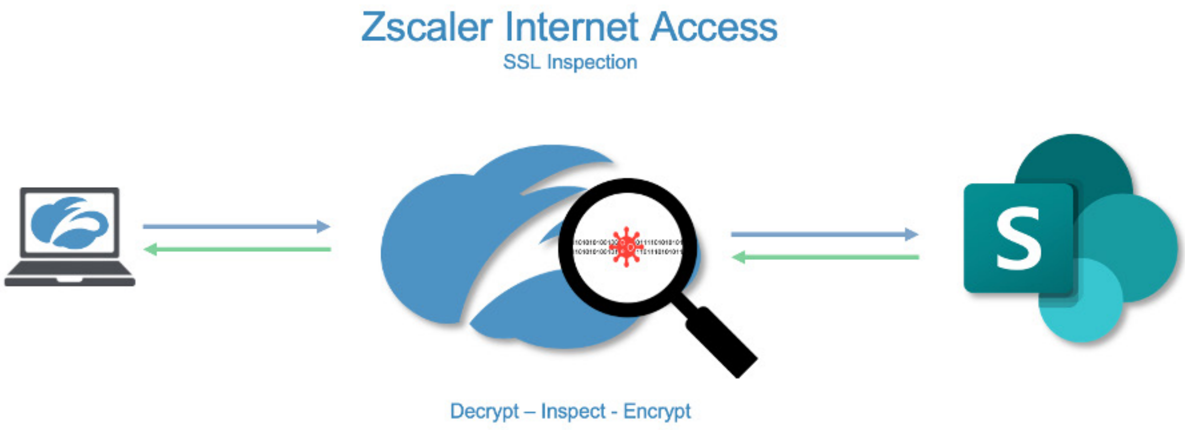


*Figure 3. SSL decryption*

Zscaler makes enabling and managing SSL inspection as manageable and operationally sound as possible. The certificates required for SSL inspection are installed during the installation of the Zscaler Client Connector, and the encryption and decryption process is performed in ASIC to nullify the latency and performance hit experienced by other security vendors. This allows organizations to enable SSL decryption for all inspectable destinations and enable security that provides cloud application control, DLP, file protection, sandbox, and malware protection.

This guide provides information about enabling SSL inspection for SharePoint, allowing you to control and secure access and the data between organizations and the SharePoint Online site.

### ZIA Cloud Application Control

The ZIA security cloud is a fully integrated cloud-based security stack that sits in-line between users and the internet, inspecting all traffic (including SSL) flowing between them. As part of the platform, Zscaler's cloud application visibility and control delivers full visibility into application usage, and granular policies that ensure the proper use of both sanctioned and unsanctioned applications.

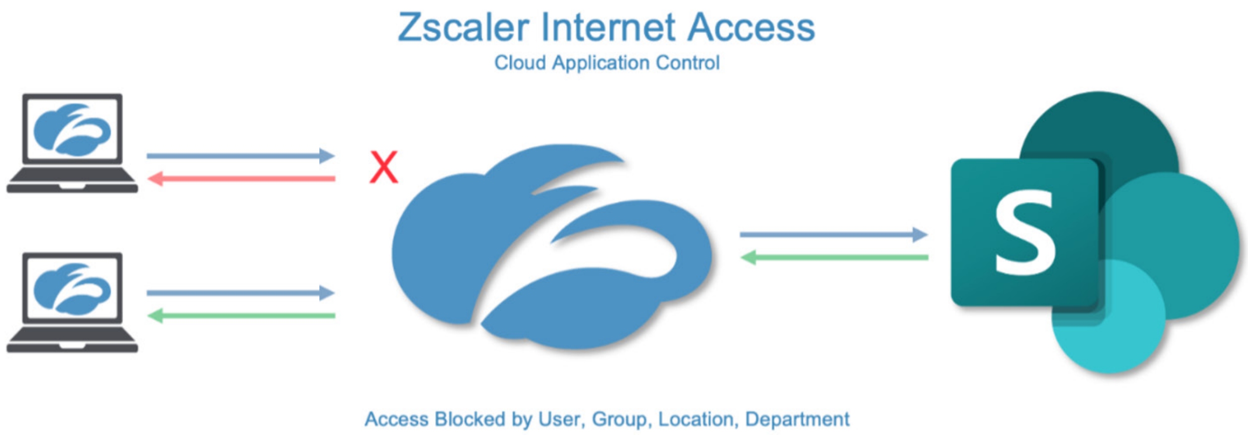

Zscaler Internet Access
Cloud Application Control
X
S
Access Blocked by User, Group, Location, Department

*Figure 4. Cloud app control*

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

### ZDX SharePoint User Experience

As applications move to the cloud, the internet becomes the new transport network. With users working from anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. SharePoint is no exception, and ZDX provides visibility into the client's experience using SharePoint. ZDX uses the Zscaler Client Connector to generate application and network probes and gather device health. ZDX is a separate service from SaaS Security API and can run with or without SaaS Security API enabled.

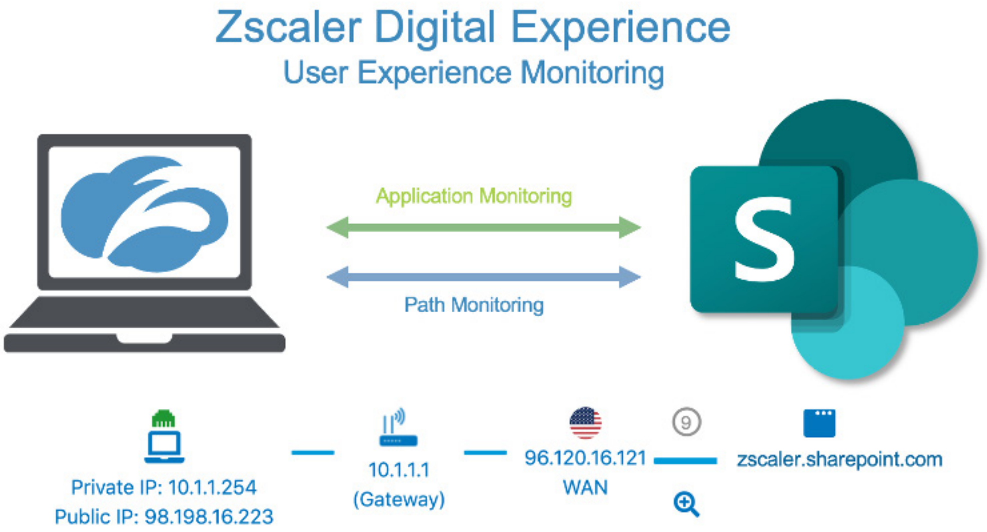


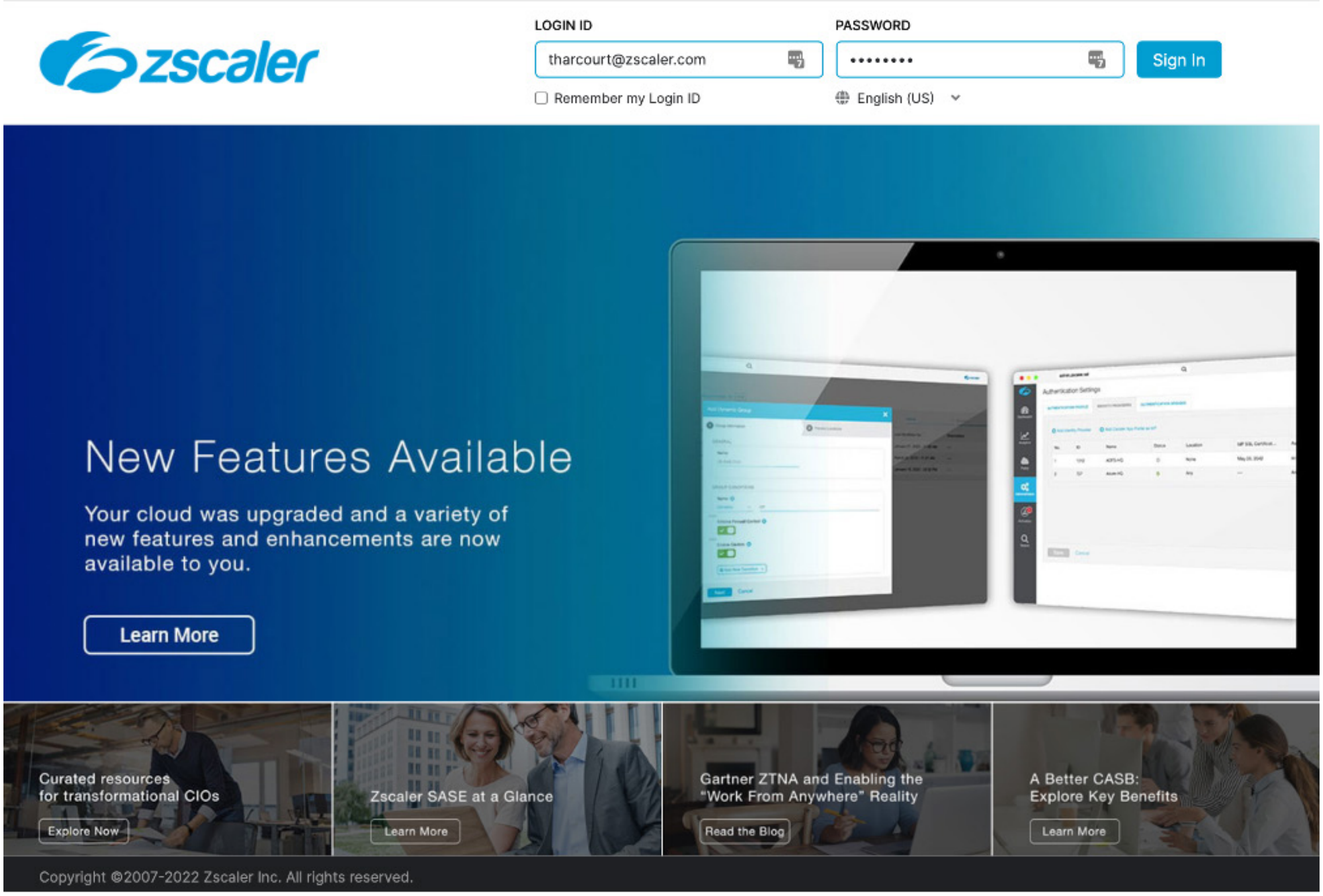
*Figure 5. ZDX for user experience monitoring for SharePoint*

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. You can 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.

ZDX continuously monitors and measures application metrics such as response time, DNS resolution, and broader availability metrics of the application. You can monitor aggregated user experience performance scores tracked over time at the user, application, location, department, and organizational level.

# Configuring SharePoint SaaS Security

Log into your tenant ZIA Admin Portal to start the installation process. Your Zscaler cloud instance may be different from the example.



LOGIN ID: tharcourt@zscaler.com

PASSWORD: ••••••••

New Features Available

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

Curated resources for transformational CIOs

Zscaler SASE at a Glance

Gartner ZTNA and Enabling the "Work From Anywhere" Reality

A Better CASB: Explore Key Benefits

Copyright ©2007-2022 Zscaler Inc. All rights reserved.

*Figure 6. ZIA Admin Portal login*

The current ZIA clouds include zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscloud.net, zscalerbeta.net, and zscalergov.net.

## Adding the SharePoint Tenant

To launch the **SaaS Application Tenants Wizard** in the ZIA Admin Portal.

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

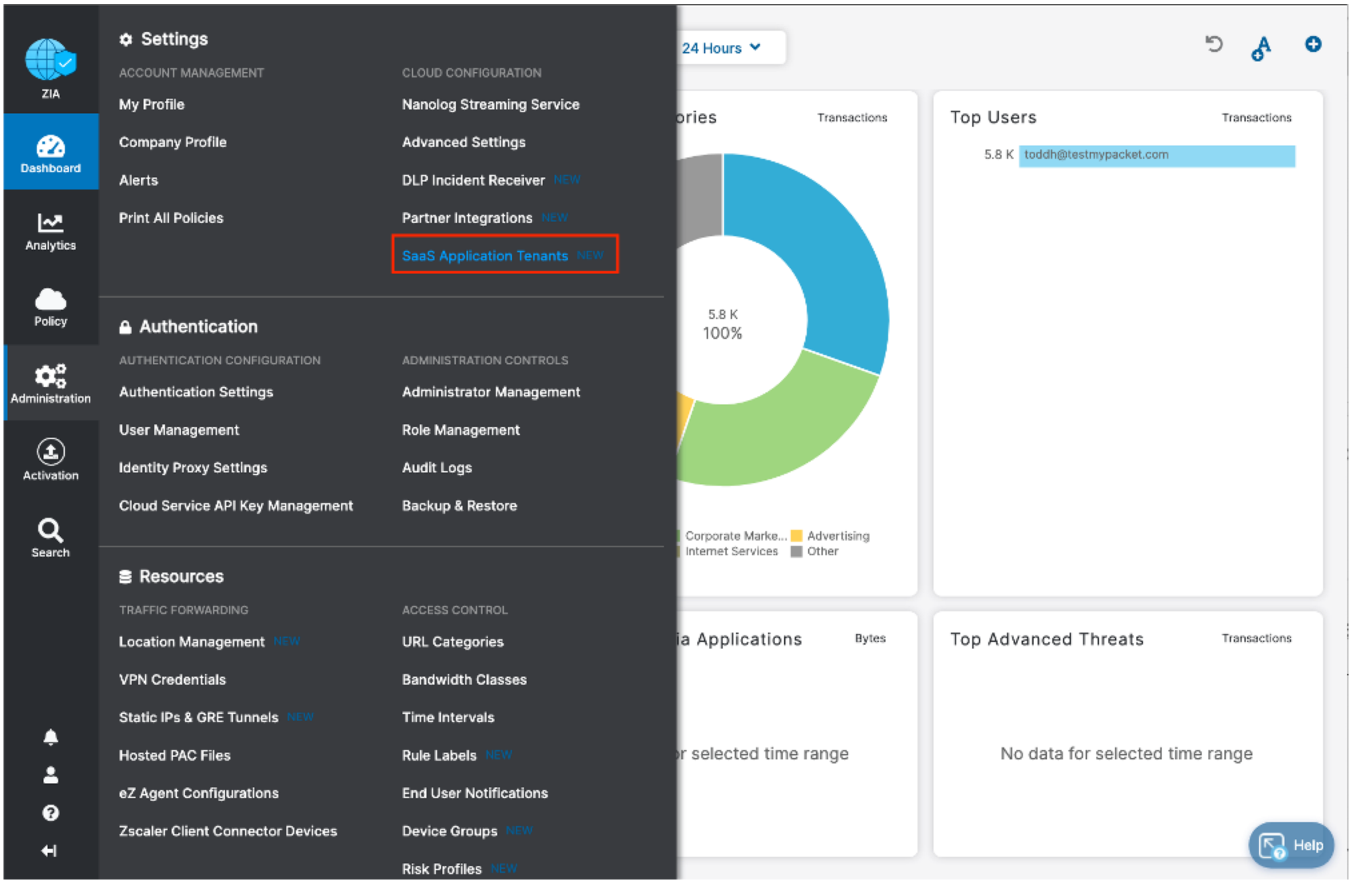


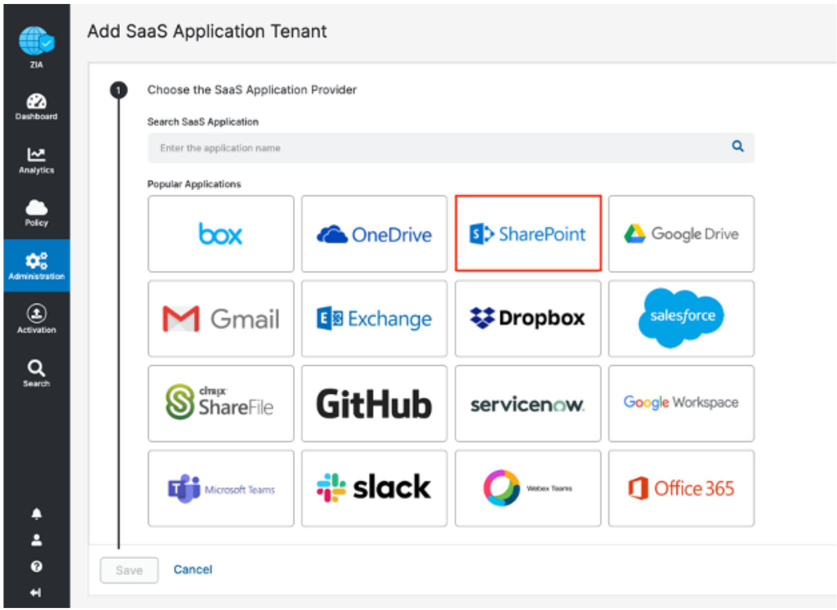
*Figure 7. SaaS Application Tenant*

3. On the SaaS Applications Tenants page, select **Add SaaS Application Tenant**.

### SaaS Tenant Configuration Wizard

After selecting Add SaaS Application Tenant, the wizard is displayed.

1. Select the **SharePoint** tile on the wizard.



Add SaaS Application Tenant

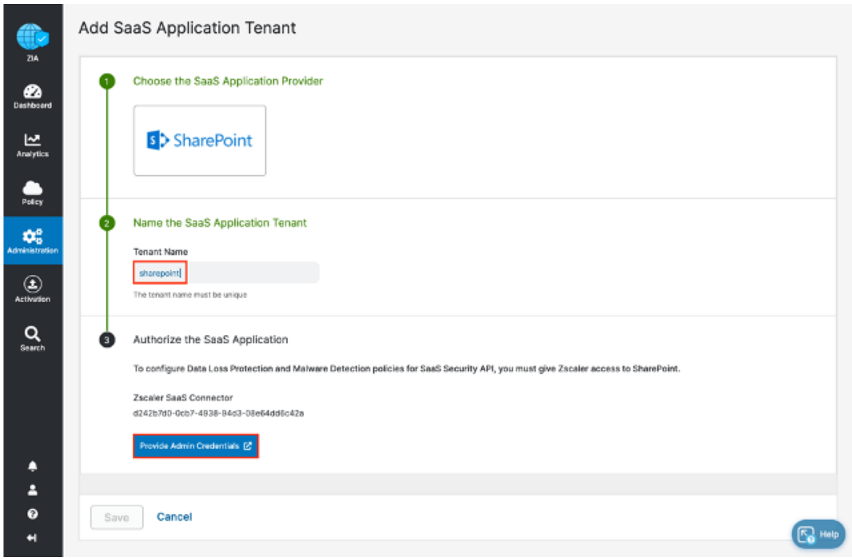
1 Choose the SaaS Application Provider

Search SaaS Application: Enter the application name

Popular Applications

*Figure 8. The SaaS tenant configuration wizard*

2. Name the SaaS Application Tenant. This is the name that is selected when assigning a policy for the Zscaler security features.
3. Click **Provide Admin Credentials**.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider: SharePoint

2 Name the SaaS Application Tenant

Tenant Name: sharepoint

The tenant name must be unique

3 Authorize the SaaS Application

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

Zscaler SaaS Connector
d242b7d0-0cb7-4938-94d3-08e64dd8c42a

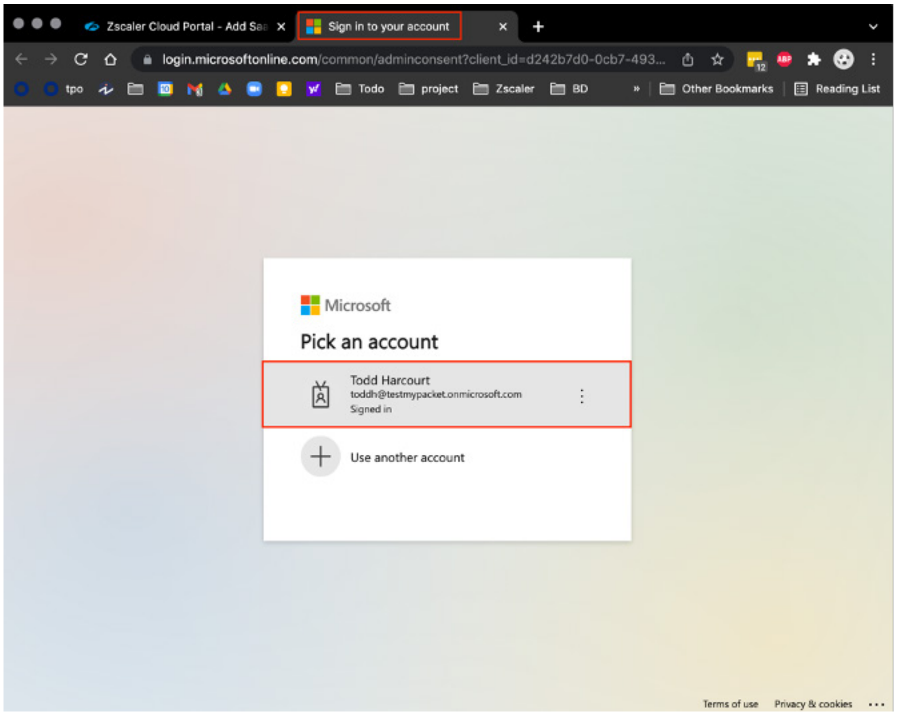
*Figure 9. Open the SharePoint tenant*

This opens a new tab in your browser where you select an account.

### Configuring the Zscaler Tenant on SharePoint

The following steps are based on procedures documented on the Microsoft website. To configure the Zscaler tenant from your SharePoint Admin account:

1. Log in to SharePoint with administrator credentials.


Zscaler Cloud Portal - Add Saa
Sign in to your account
login.microsoftonline.com/common/adminconsent?client_id=d242b7d0-0cb7-493...
tpo
Todo
project
Zscaler
BD
Other Bookmarks
Reading List
Terms of use
Privacy & cookies

Microsoft

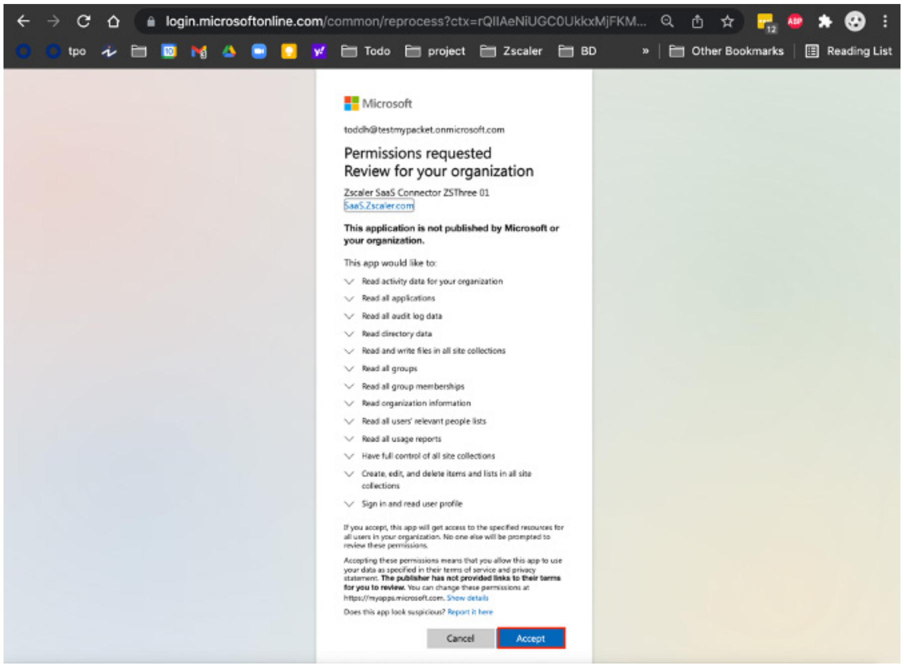
Pick an account

Todd Harcourt
toddh@testmypacket.onmicrosoft.com
Signed in

Use another account

*Figure 10. Log in to the SharePoint tenant*

2. Verify and accept the requested permissions.
3. Click **Accept**.


login.microsoftonline.com/common/reprocess?ctx=rQIIAeNiUGC0UkkxMjFKM...
tpo
Todo
project
Zscaler
BD
Other Bookmarks
Reading List

Microsoft

toddh@testmypacket.onmicrosoft.com

Permissions requested
Review for your organization

Zscaler SaaS Connector ZSThree 01
SaaS.Zscaler.com

**This application is not published by Microsoft or your organization.**

This app would like to:

- Read activity data for your organization
- Read all applications
- Read all audit log data
- Read directory data
- Read and write files in all site collections
- Read all groups
- Read all group memberships
- Read organization information
- Read all users' relevant people lists
- Read all usage reports
- Have full control of all site collections
- Create, edit, and delete items and lists in all site collections
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

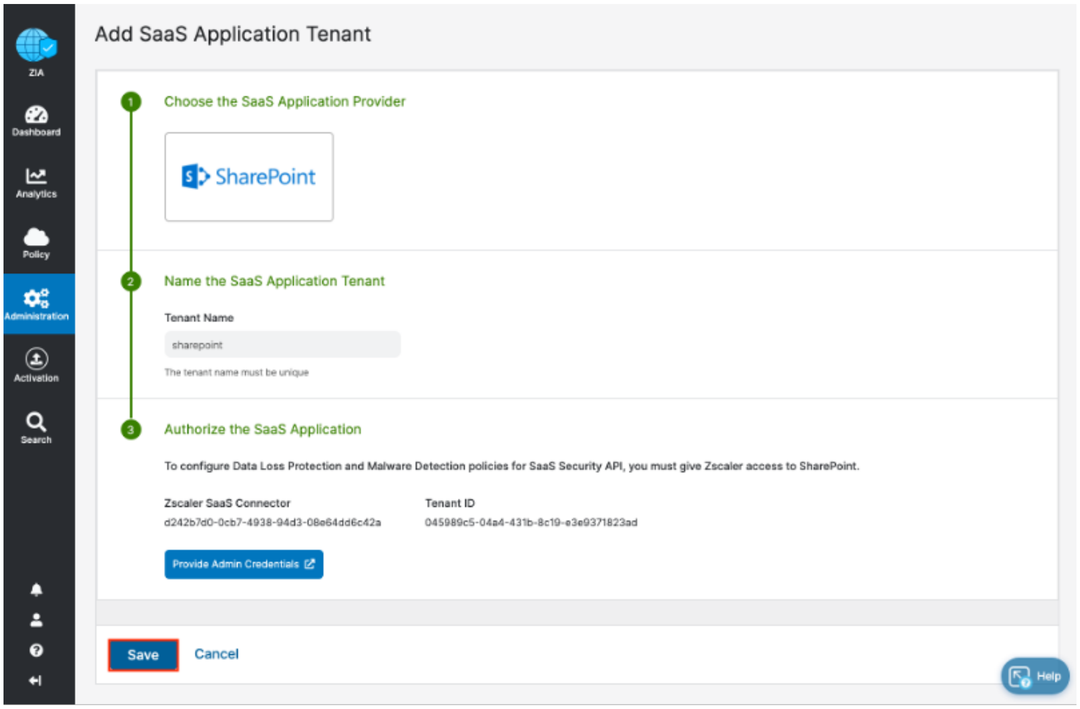
Cancel Accept

*Figure 11. Accept SharePoint permissions*

### Finishing the Zscaler Tenant on Zscaler

Save and activate the configuration changes from the ZIA Admin Portal:

1. Click **Save**.
2. **Activate** the configuration changes.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

2 Name the SaaS Application Tenant

Tenant Name: sharepoint

The tenant name must be unique

3 Authorize the SaaS Application

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

Zscaler SaaS Connector: d242b7d0-0cb7-4938-94d3-08e64dd6c42a

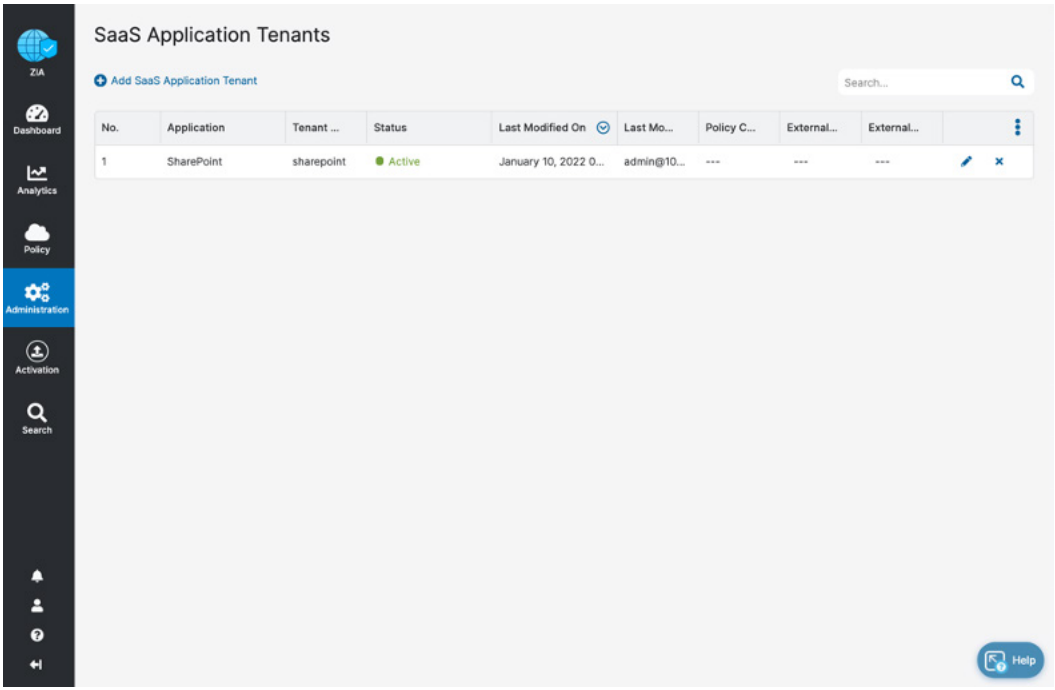
Tenant ID: 045989c5-04a4-431b-8c19-e3e9371823ad

Provide Admin Credentials

Save Cancel

*Figure 12. Finish the Zscaler tenant*

3. Return to the SaaS Application Tenants windows, then verify the SharePoint tenant is **Active**.



SaaS Application Tenants

Add SaaS Application Tenant

| No. | Application | Tenant ... | Status | Last Modified On | Last Mo... | Policy C... | External... | External... |
|---|---|---|---|---|---|---|---|---|
| 1 | SharePoint | sharepoint | ● Active | January 10, 2022 0... | admin@10... | --- | --- | --- |

*Figure 13. The completed and active SharePoint tenant*

### The Completed and Active SharePoint API Connector

After adding and configuring the SharePoint tenant, there are other actions you can take (detailed later in this guide):

- Configuring SharePoint SaaS Data Loss Prevention
- Configuring SharePoint SaaS Malware Detection
- SaaS Security Reporting and Visibility
- Configuring SSL Inspection for SharePoint

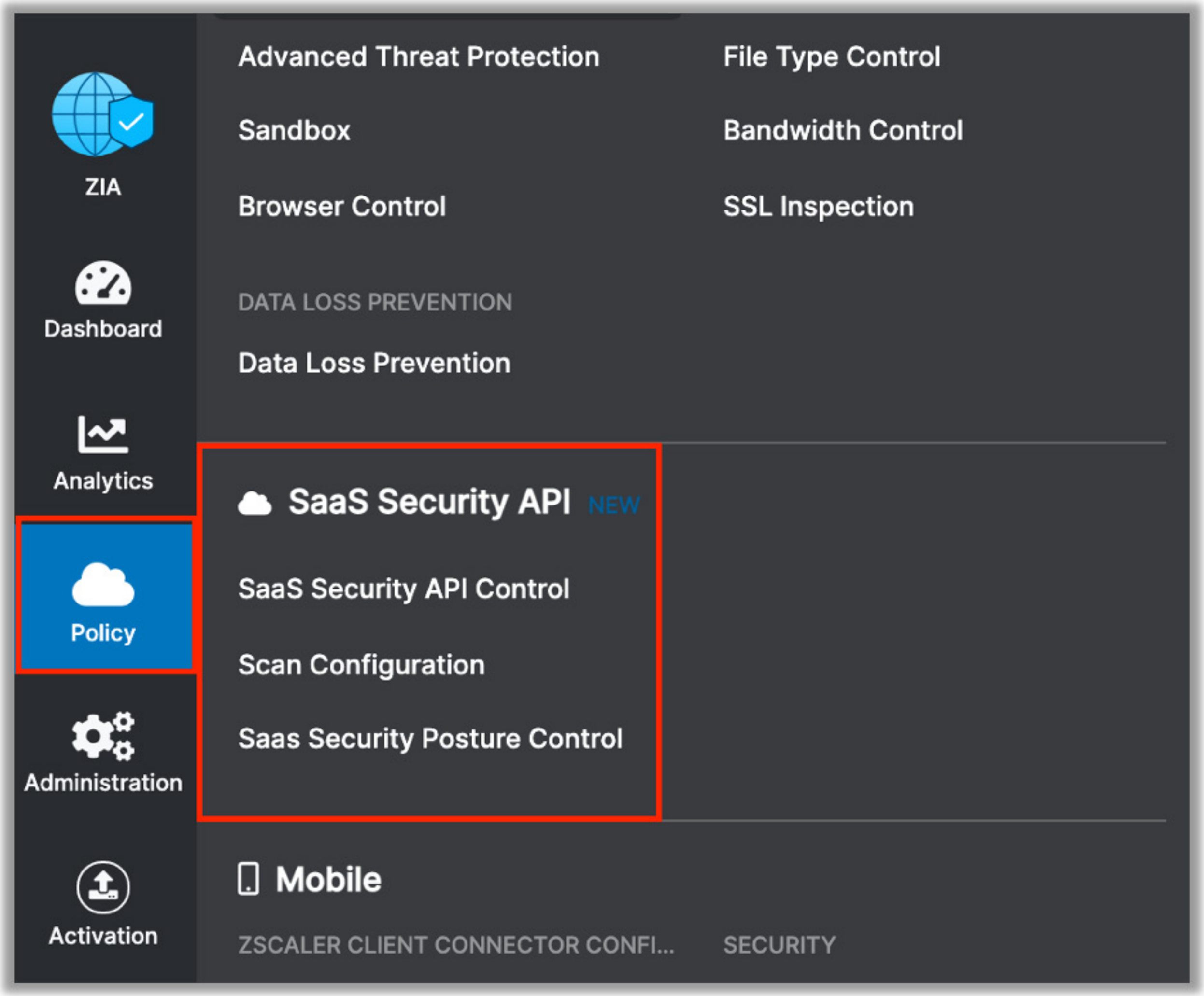


*Figure 14. Zscaler policy configuration*

# Configuring SharePoint SaaS Data Loss Prevention

The procedures for creating a DLP policy are straightforward. Create a custom dictionary (or use the available dictionaries) to identify the data for which the scan looks. This guide uses a POSIX pattern to show the power of creating a library to match any data, or you can use one of the predefined libraries as well.

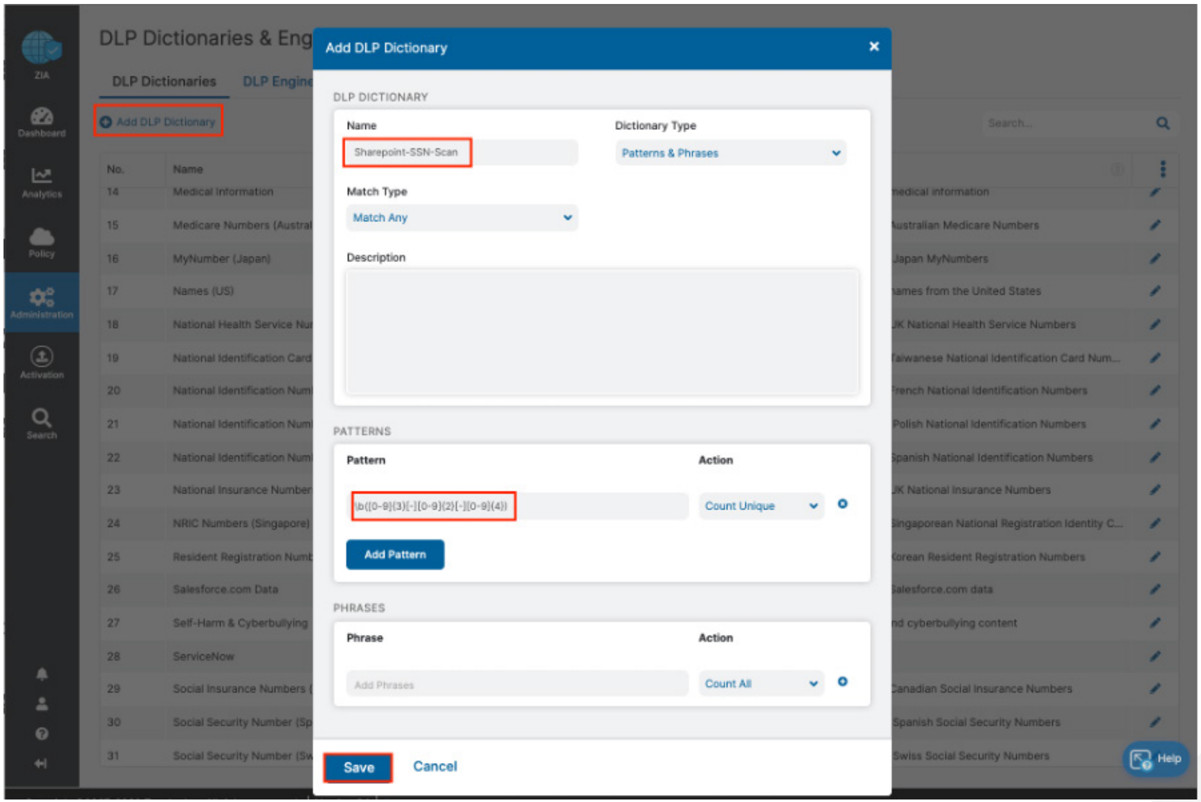
An engine is created that is the logical template for adding expressions and additional data. You then specify the SharePoint-SSN-Scan dictionary and any other criteria for the policy. The engine adds or removes data that matches violations and eliminates false positives.

## Creating a DLP Policy

Create a SaaS Security DLP policy that specifies the detail about where, when, the action taken, and whom to inform about violations. Then, apply the DLP policy to your SharePoint tenant.

In the ZIA Admin Portal:

1. Select **Administration**.
2. Select **DLP Dictionaries and Engines**.
3. Select **Add DLP Dictionary** (this opens the configuration wizard).
4. **Name** the Dictionary (in this case, `SharePoint-SSN-Scan`).
5. Specify the pattern to match the basic SSN format `[ \b([0-9]{3}[-][0-9]{2}[-][0-9]{4}) ]`.
6. Click **Save** to save the dictionary.



Add DLP Dictionary

DLP DICTIONARY

Name: Sharepoint-SSN-Scan

Dictionary Type: Patterns & Phrases

Match Type: Match Any

Description:

PATTERNS

Pattern: \b([0-9]{3}[-][0-9]{2}[-][0-9]{4})

Action: Count Unique

PHRASES

Phrase: Add Phrases

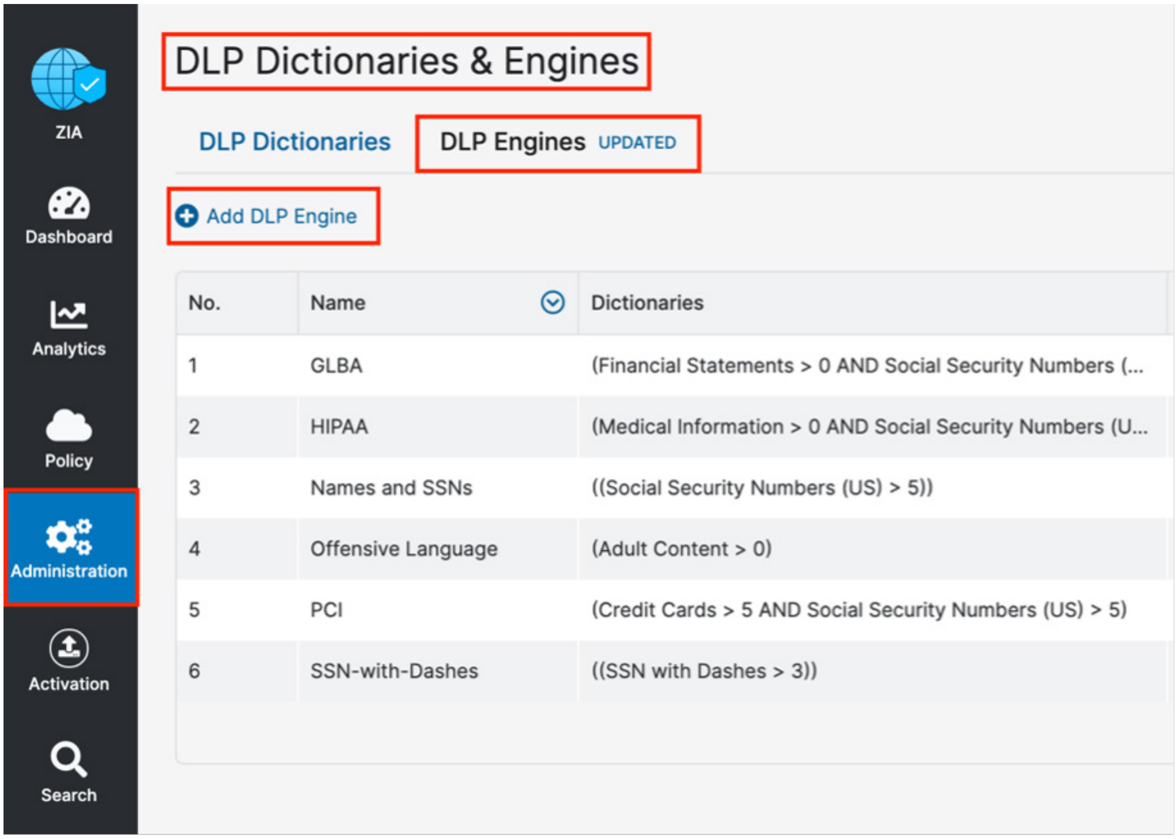
Action: Count All

*Figure 15. Creating a DLP dictionary*

## Creating a DLP Engine

Create a DLP engine that provides the logic for the DLP library. This template allows you to build Boolean expressions and hit counts to fine tune the violation criteria that prevent false positives. To create the DLP engine to use the DLP Dictionary:

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

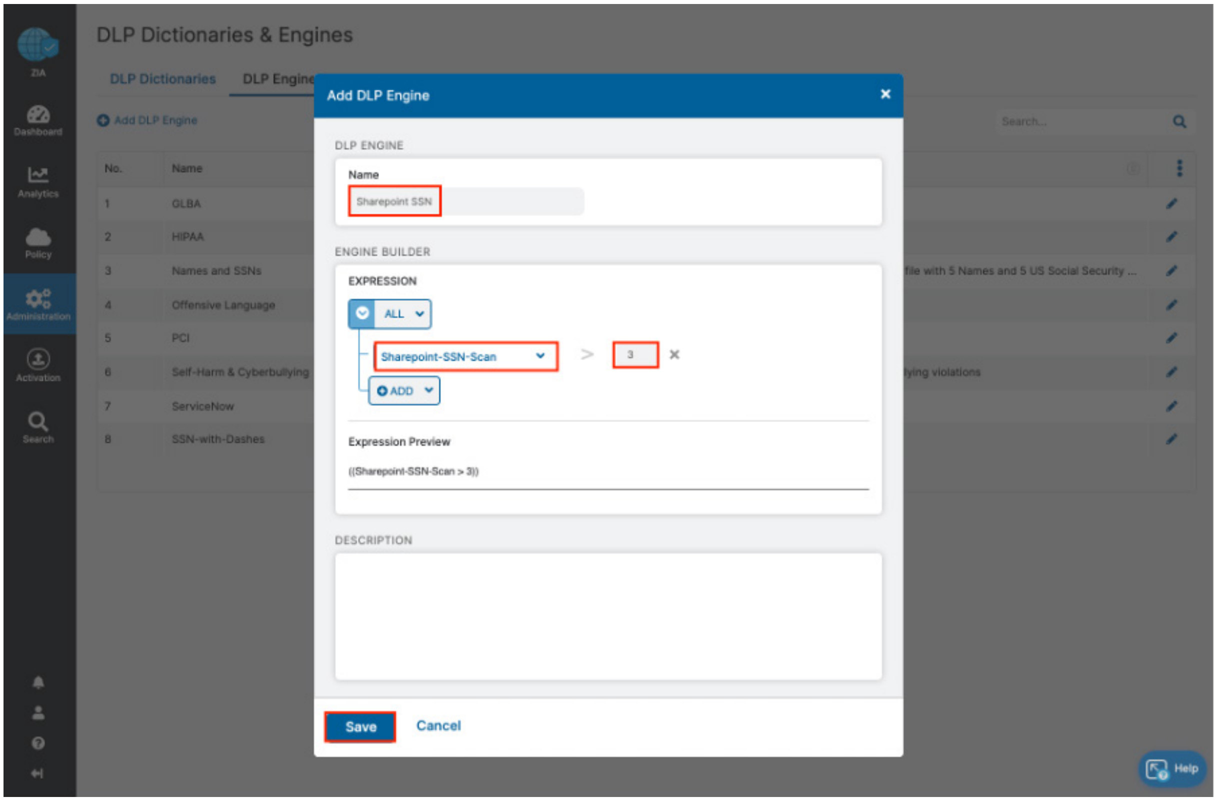


DLP Dictionaries & Engines

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

*Figure 16. Creating a DLP engine*

3. Give the DLP Engine a **Name**.
4. In the **Engine Builder** under **Expression** select your newly created dictionary.
5. Specify the **Match Count**, which is the minimum number of instances the data must occur in the file.
6. Select **ADD** to add another dictionary if desired and repeat the process.
7. Click **Save** to save the configuration.
8. **Activate** the configuration.



| No. | Name |
|---|---|
| 1 | GLBA |
| 2 | HIPAA |
| 3 | Names and SSNs |
| 4 | Offensive Language |
| 5 | PCI |
| 6 | Self-Harm & Cyberbullying |
| 7 | ServiceNow |
| 8 | SSN-with-Dashes |

file with 5 Names and 5 US Social Security ...

lying violations

Add DLP Engine

DLP ENGINE

Name: Sharepoint SSN

ENGINE BUILDER

EXPRESSION

ALL

Sharepoint-SSN-Scan > 3

ADD

Expression Preview

((Sharepoint-SSN-Scan > 3))

DESCRIPTION

Save Cancel

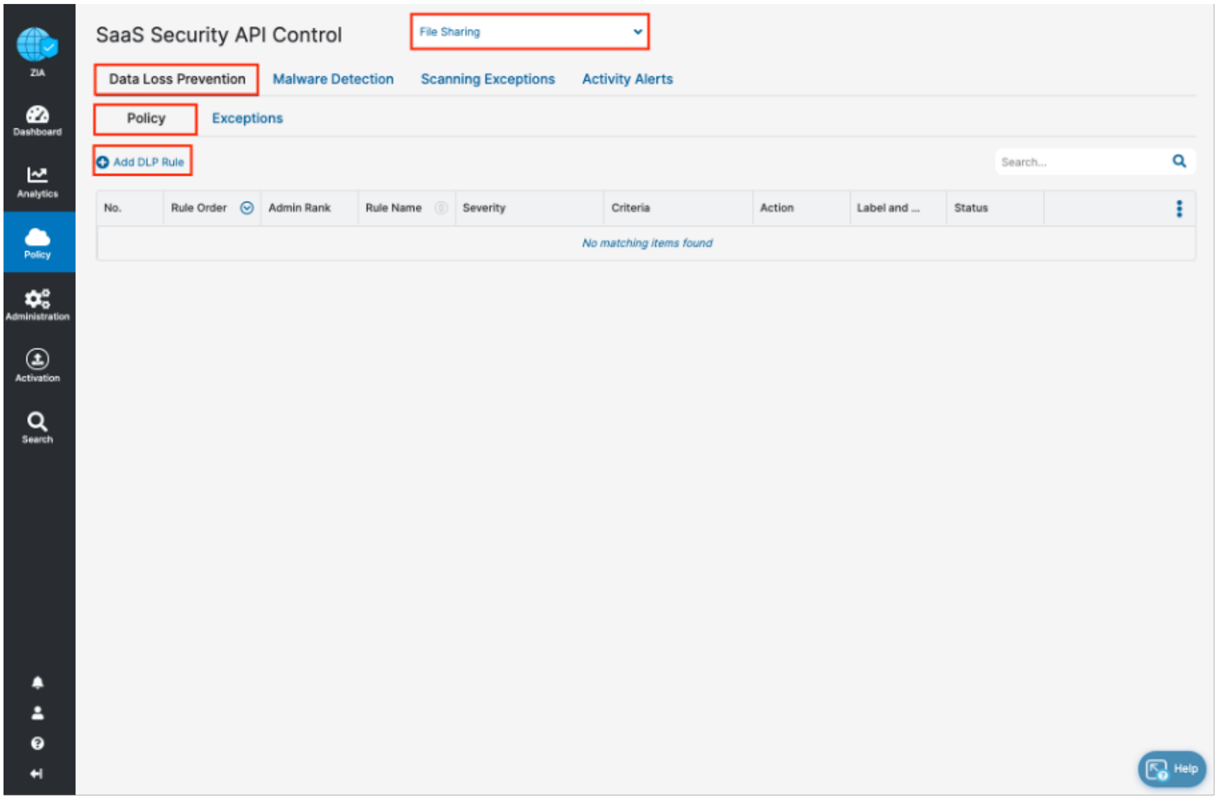
*Figure 17. The DLP engine wizard*

This policy triggers when you see the third Social Security number. This is an example only (where the criteria is too general to be a production DLP rule).

## Configure a SaaS DLP Policy

Now apply the engine to a DLP policy that is used for the SharePoint instance. Launch the DLP Rule Wizard to start the process.

1. Select **Policy**.
2. Select **Data Loss Prevention**.
3. Select **File Sharing**.
4. Select **Policy**.
5. Select **Add DLP Rule**.


SaaS Security API Control

File Sharing

Data Loss Prevention | Malware Detection | Scanning Exceptions | Activity Alerts

Policy | Exceptions

Add DLP Rule

| No. | Rule Order | Admin Rank | Rule Name | Severity | Criteria | Action | Label and ... | Status |
|---|---|---|---|---|---|---|---|---|
| No matching items found | | | | | | | | |

*Figure 18. Launch the SaaS DLP policy configuration wizard*

This launches the **DLP Policy Wizard**.

**SaaS DLP Policy Details**

The SaaS DLP policy is like all Zscaler polices in that you specify the detail on whom and what data to which this policy applies. You also specify the rule order if you have multiple DLP policies that are processed in a specific order.

The first rule that matches is the applied rule. Specify the defined DLP engine, any file owners, groups, departments, and the file types to inspect. Select Any Collaboration, and an Action of Remove Sharing.

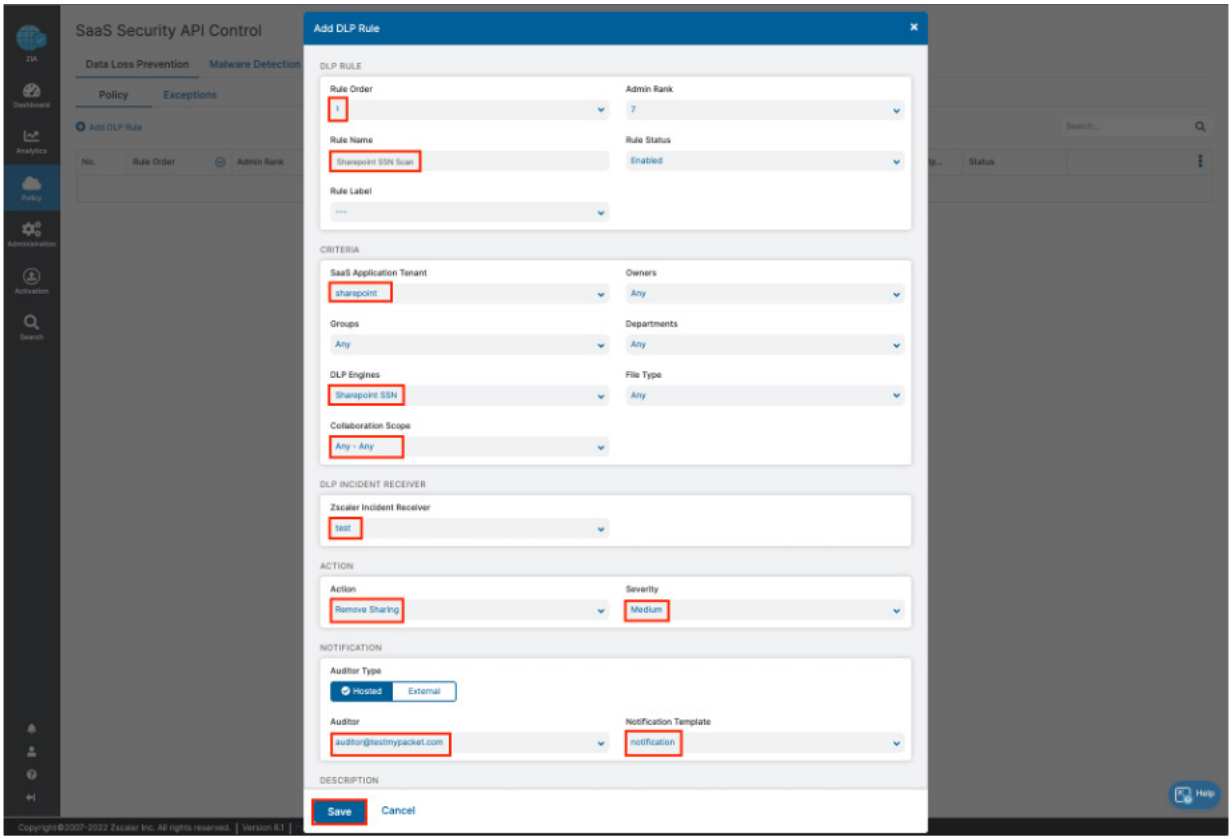
The Collaboration Scope and the Action are unique to the SaaS DLP, and are explained below for clarification:

- 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 of your organization.
  - External Link. Files with shareable links that allow anyone outside your organization to find the files and have access.
  - Internal Collaborators. Files that are shared with specific collaborators or are discoverable within your organization.
  - Internal Link. Files with shareable links that allow anyone within your organization to find the files and have access.
  - Private. Files that are only accessible to the owner.
- Action. The rule detects content that matches the criteria. The number of actions available depends on the selected SaaS application tenant. For SharePoint, the actions can remove Internal or External Collaborators and the Shareable Link, All Sharing, or Report Only.
  - Remove External Collaborators and Shareable Link. The rule reports the incident and removes all the file’s external collaborators and any shareable links.
  - Remove Internal Collaborators and Shareable Link. The rule reports the incident and removes all internal collaborators and any shareable links.
  - Remove Sharing. The rule reports the incident and removes all 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.

### SaaS DLP Policy Wizard

Configure the DLP policy. DLP Policies are evaluated in order in a top-down approach. The first policy matched is taken into effect. To configure the policy:

1. Select the **Rule Order** for evaluation.
2. Provide a **Rule Name** for the rule.
3. Select the evaluation **Criteria**:
   a. Select the SharePoint SaaS Application Tenant.
   b. Select the desired DLP Engine (SharePoint SSN from previous steps).
   c. Select the desired Collaboration Scope.
4. If configured and installed, select the **Zscaler Incident Receiver** to receive violation content.
5. Select the desired **Action**.
6. Select the **Severity** to assign the violation.
7. Select the **Auditor Type** to receive a notification email of a violation.
8. Select the **Notification Template**.
9. Click **Save**.
10. Click **Activate**.



Add DLP Rule

DLP RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Sharepoint SSN Scan

Rule Status: Enabled

Rule Label: ---

CRITERIA

SaaS Application Tenant: sharepoint

Owners: Any

Groups: Any

Departments: Any

DLP Engines: Sharepoint SSN

File Type: Any

Collaboration Scope: Any - Any

DLP INCIDENT RECEIVER

Zscaler Incident Receiver: test

ACTION

Action: Remove Sharing

Severity: Medium

NOTIFICATION

Auditor Type: ● Hosted ○ External

Auditor: auditor@testmypacket.com

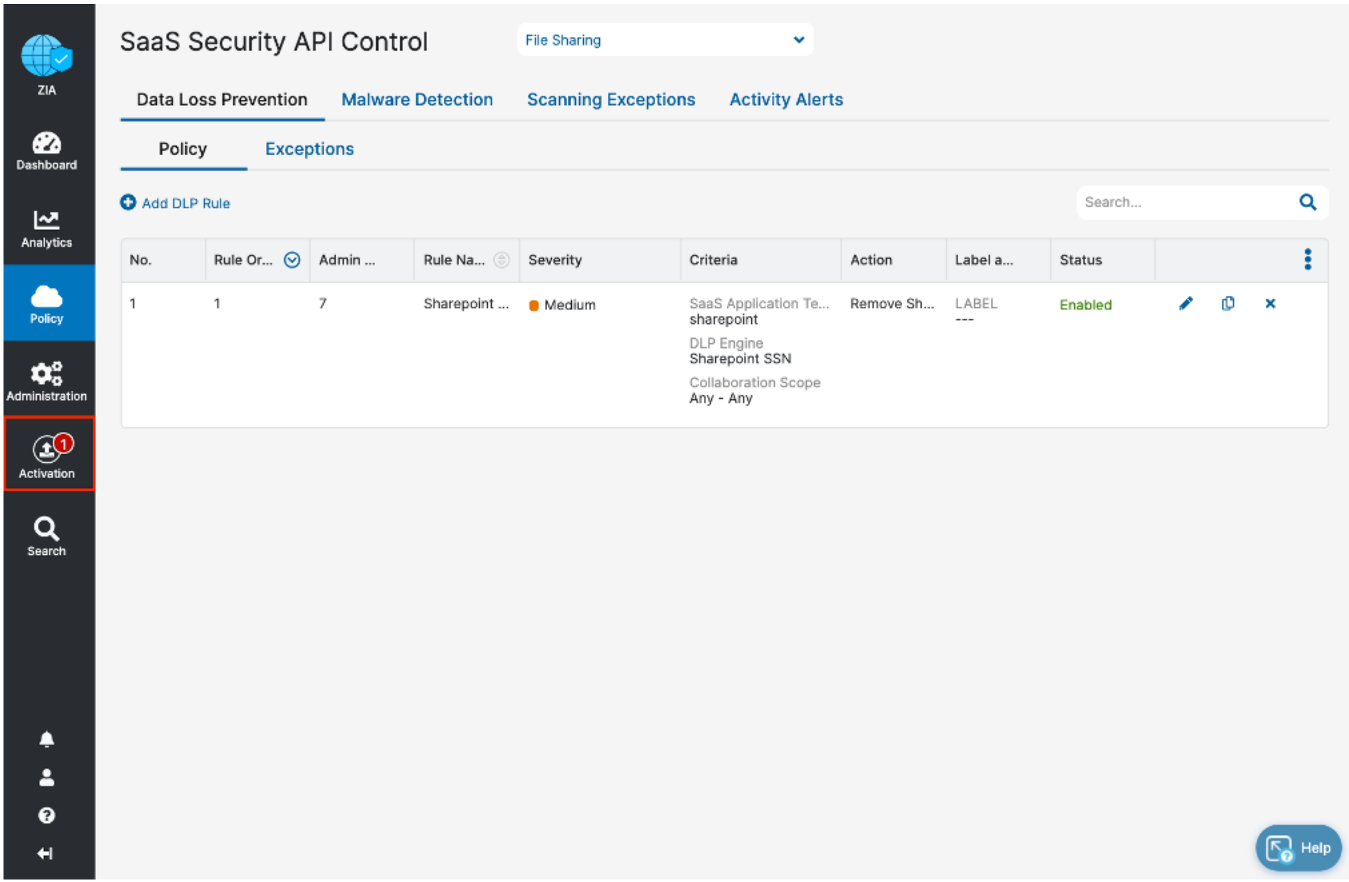
Notification Template: notification

DESCRIPTION

Save Cancel

*Figure 19. Completing the SaaS DLP policy configuration wizard*

The following image displays the completed, activated, and enabled DLP policy.



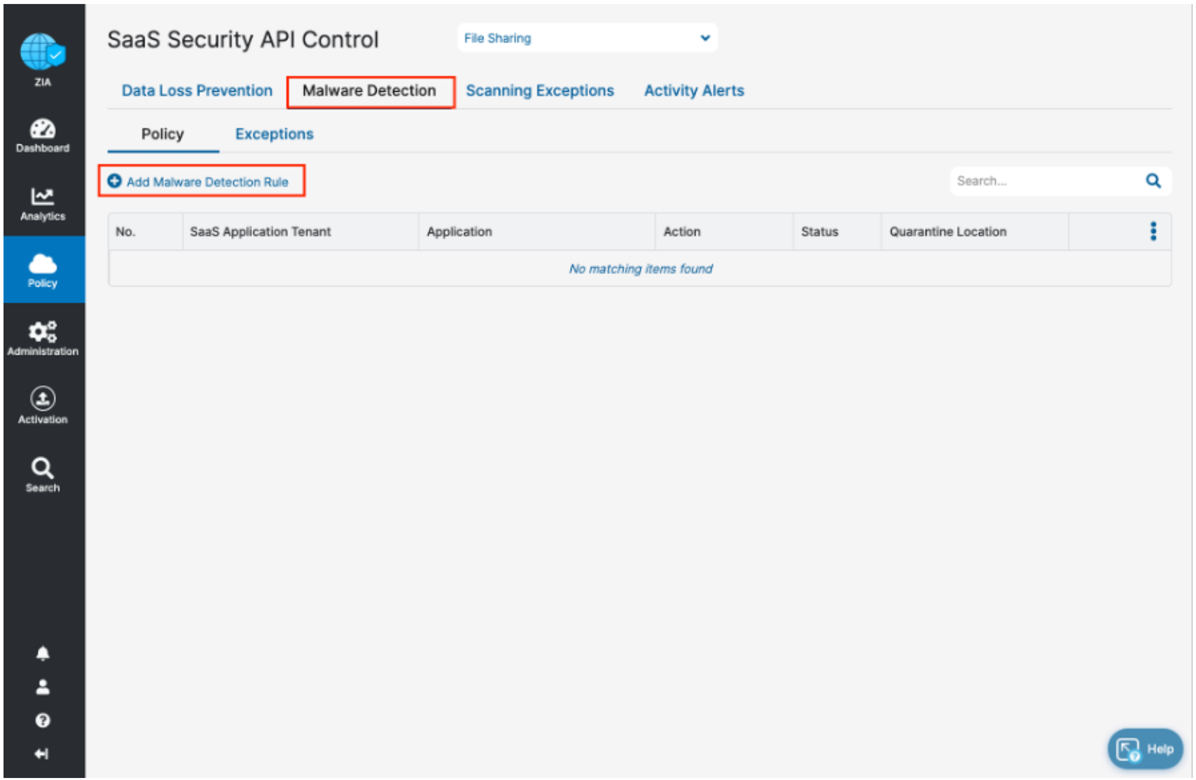
| No. | Rule Or... | Admin ... | Rule Na... | Severity | Criteria | Action | Label a... | Status |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 7 | Sharepoint ... | Medium | SaaS Application Te...<br>sharepoint<br>DLP Engine<br>Sharepoint SSN<br>Collaboration Scope<br>Any - Any | Remove Sh... | LABEL<br>--- | Enabled |

*Figure 20. The completed SaaS DLP policy*

# Configuring SharePoint SaaS Malware Detection

To create a SharePoint malware detection rule, launch the malware detection rule wizard:

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



| No. | SaaS Application Tenant | Application | Action | Status | Quarantine Location |
|---|---|---|---|---|---|
| | | *No matching items found* | | | |

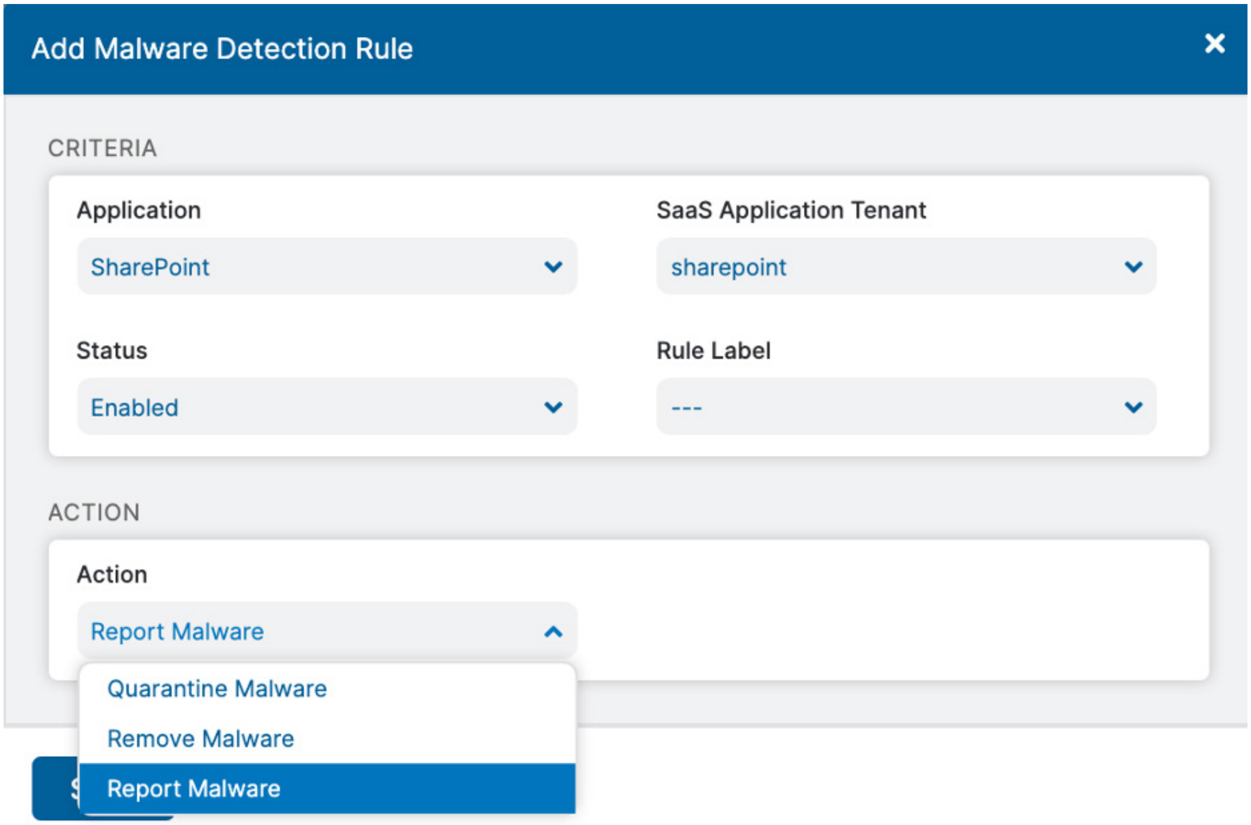
*Figure 21. Adding a SaaS malware detection policy*

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

The mitigation actions for SharePoint allow to quarantine, remove, and report malware.

After the malware detection rule wizard is displayed:

1. Select **SharePoint** as the **Application**.
2. Select the **SharePoint SaaS Application Tenant**.
3. Select **Enabled** for **Status**.
4. Select the desired **Action**. **Report Malware** shows any violations without making changes to the tenant, is the least impactful, and a good starting point to test the feature.
5. Click **Save**, then **Activate** the policy.



Add Malware Detection Rule

CRITERIA

Application: SharePoint

SaaS Application Tenant: sharepoint

Status: Enabled

Rule Label: ---

ACTION

Action: Report Malware

*Figure 22. Add malware detection rule*

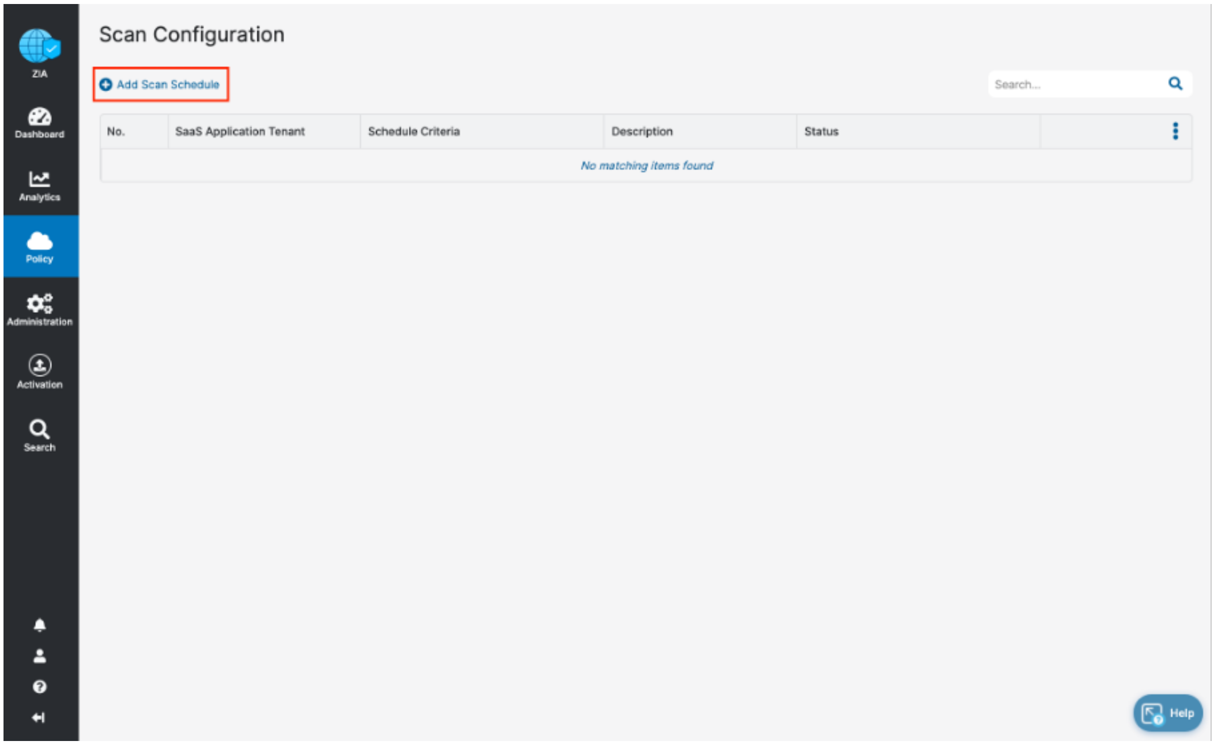
## Configuring SharePoint Security Scan for DLP and Malware

The final configuration step for SaaS data scanning is to create the scan configuration. Specify the tenant to which the scan configuration applies, any policies that are included in the scan, and what data to scan relative to a date.

## The Scan Schedule Configuration

The options for data to scan are All Data, Date Created or Modified After, or New Data Only. For this deployment guide, All Data is selected. However, if this is a proof-of-concept or a trial, the only option available is New Data Only.

To add a scan schedule, select **Policy** > **Scan Configuration** > **Add Scan Schedule**.

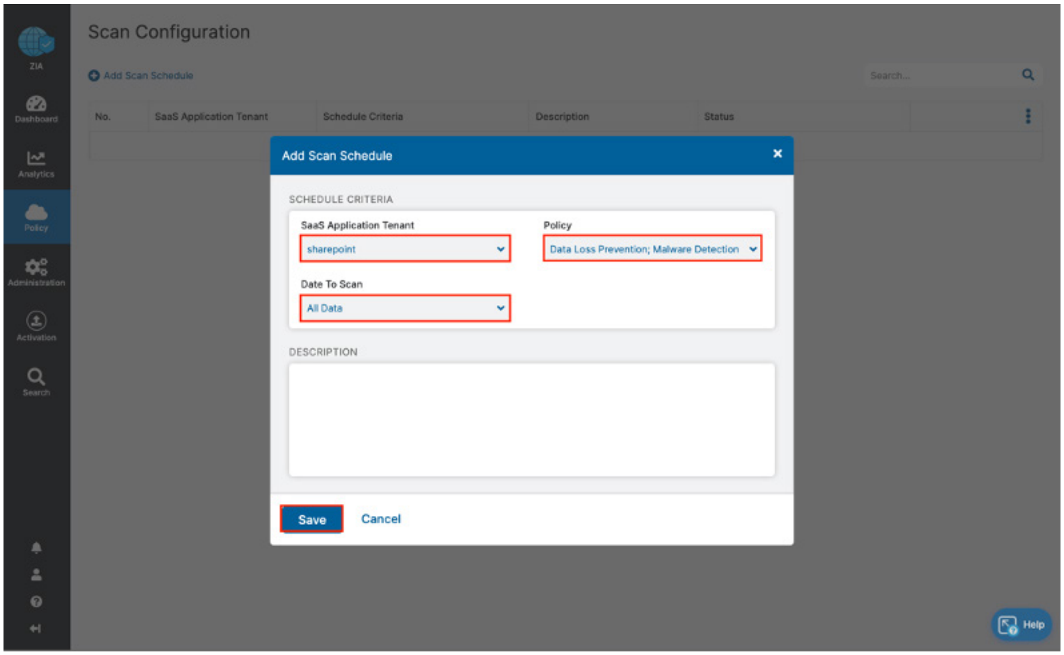


| No. | SaaS Application Tenant | Schedule Criteria | Description | Status |
|---|---|---|---|---|
| | | *No matching items found* | | |

*Figure 23. Configure the scan*

In the wizard:

1. Select **SharePoint** as the **SaaS Application Tenant**.
2. Select the **Data Loss Prevention** and **Malware Detection** policies created in prior steps.
3. Select **All Data** or **New Data Only** if this is a proof-of-concept or trial.
4. Click **Save**.



Scan Configuration

Add Scan Schedule

| No. | SaaS Application Tenant | Schedule Criteria | Description | Status |
|---|---|---|---|---|

Add Scan Schedule

SCHEDULE CRITERIA

SaaS Application Tenant: sharepoint

Policy: Data Loss Prevention; Malware Detection

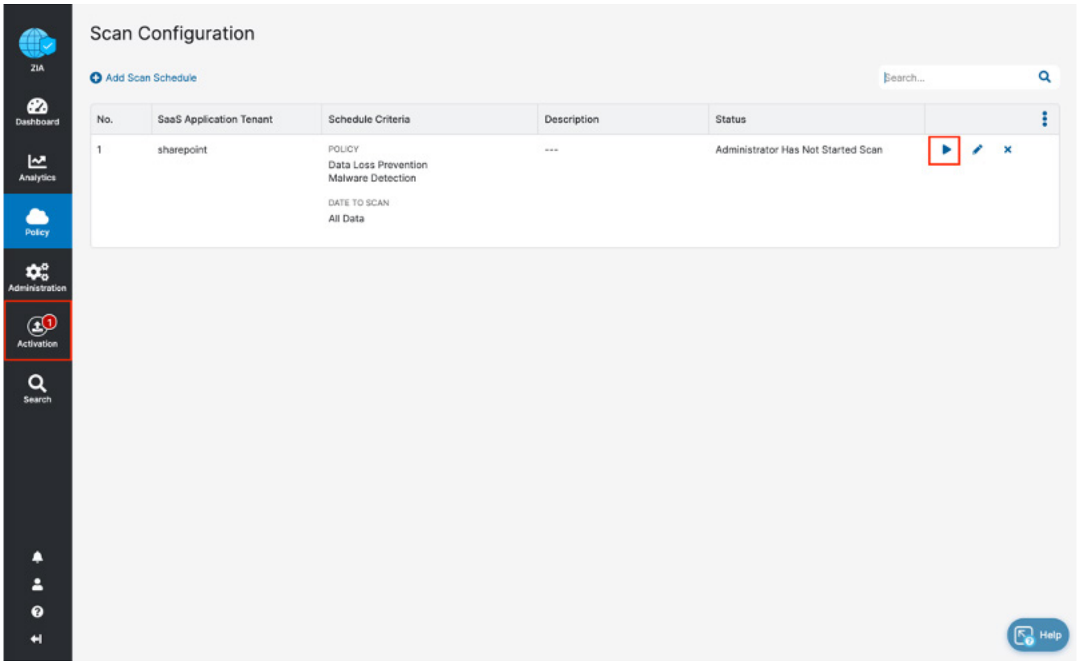
Date To Scan: All Data

DESCRIPTION

Save Cancel

*Figure 24. Scan configuration details*

5. **Activate** the configuration.
6. Start the scan by selecting the **Start** icon.



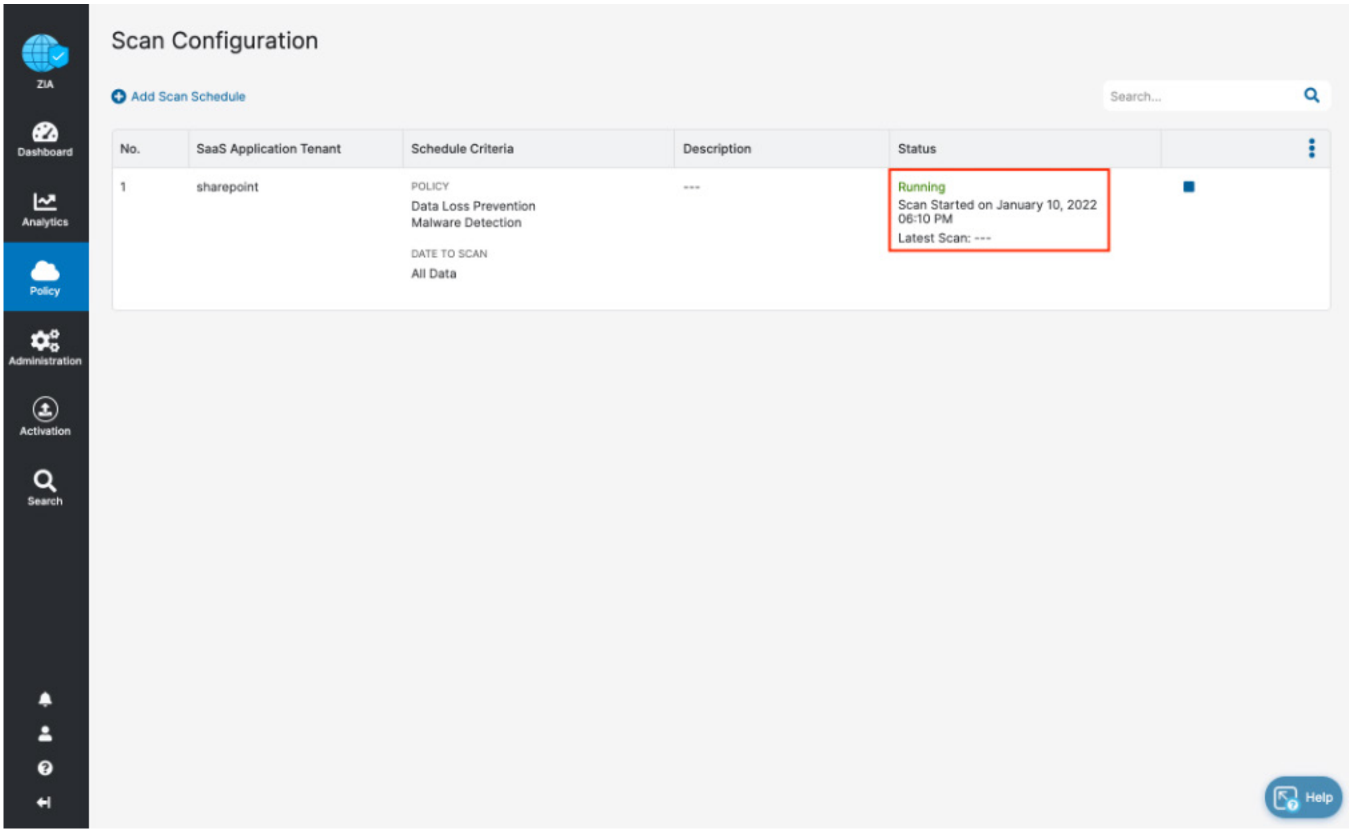
Scan Configuration

Add Scan Schedule

| No. | SaaS Application Tenant | Schedule Criteria | Description | Status |
|---|---|---|---|---|
| 1 | sharepoint | POLICY<br>Data Loss Prevention<br>Malware Detection<br>DATE TO SCAN<br>All Data | --- | Administrator Has Not Started Scan |

*Figure 25. Start the scan*

The DLP and malware policies are now active, and the files are scanned for content violation and malware.



Scan Configuration

| No. | SaaS Application Tenant | Schedule Criteria | Description | Status |
|---|---|---|---|---|
| 1 | sharepoint | POLICY<br>Data Loss Prevention<br>Malware Detection<br>DATE TO SCAN<br>All Data | --- | Running<br>Scan Started on January 10, 2022 06:10 PM<br>Latest Scan: --- |

*Figure 26. The active and running scan*

# SaaS Security Reporting and Visibility

Zscaler analytics provide detailed reporting of all user activity, down to each session created by the user when visiting a destination. Zscaler extends that visibility to include reporting of activity, malware incidents, and DLP violations of data at rest associated with the user. For 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.

The tools are discussed briefly. For more information of the SaaS security analytics tools, see **Zscaler help portal on analytics**.

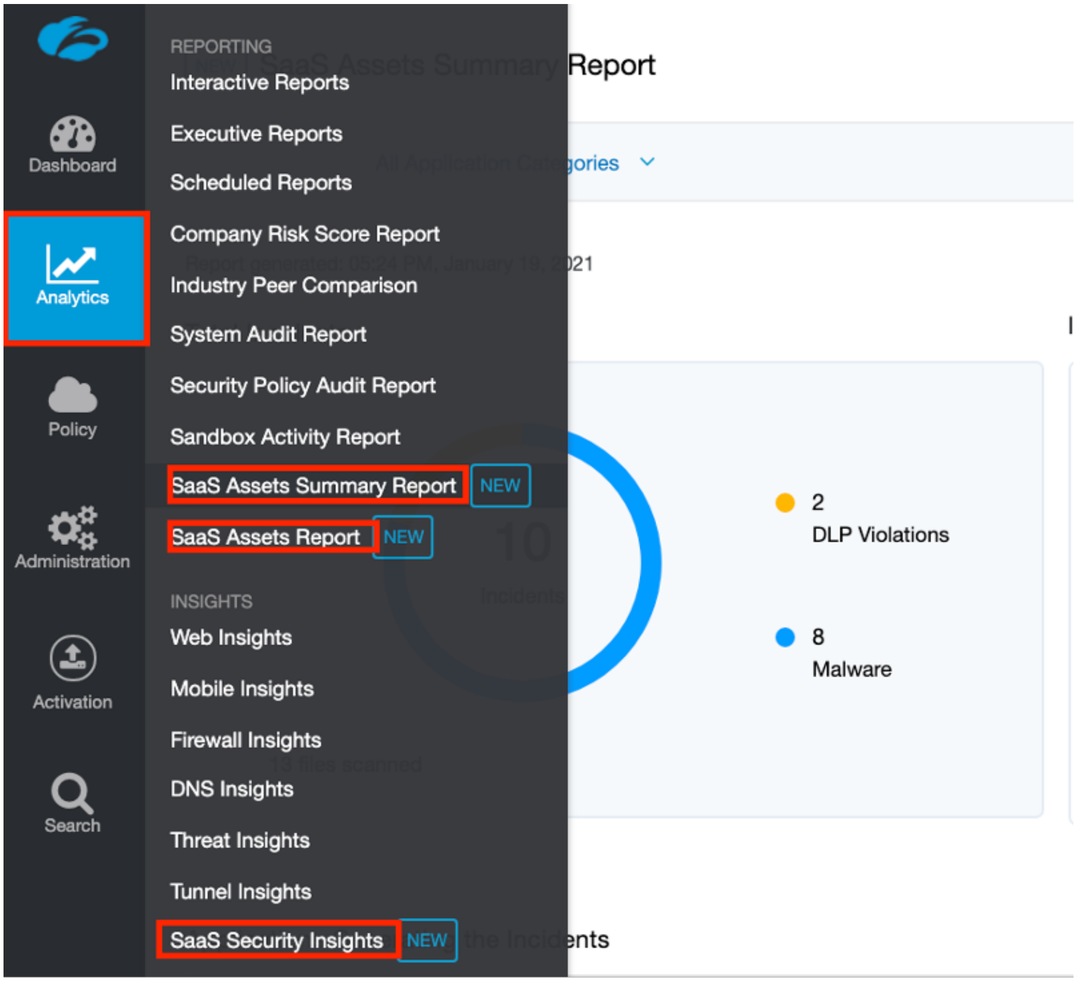
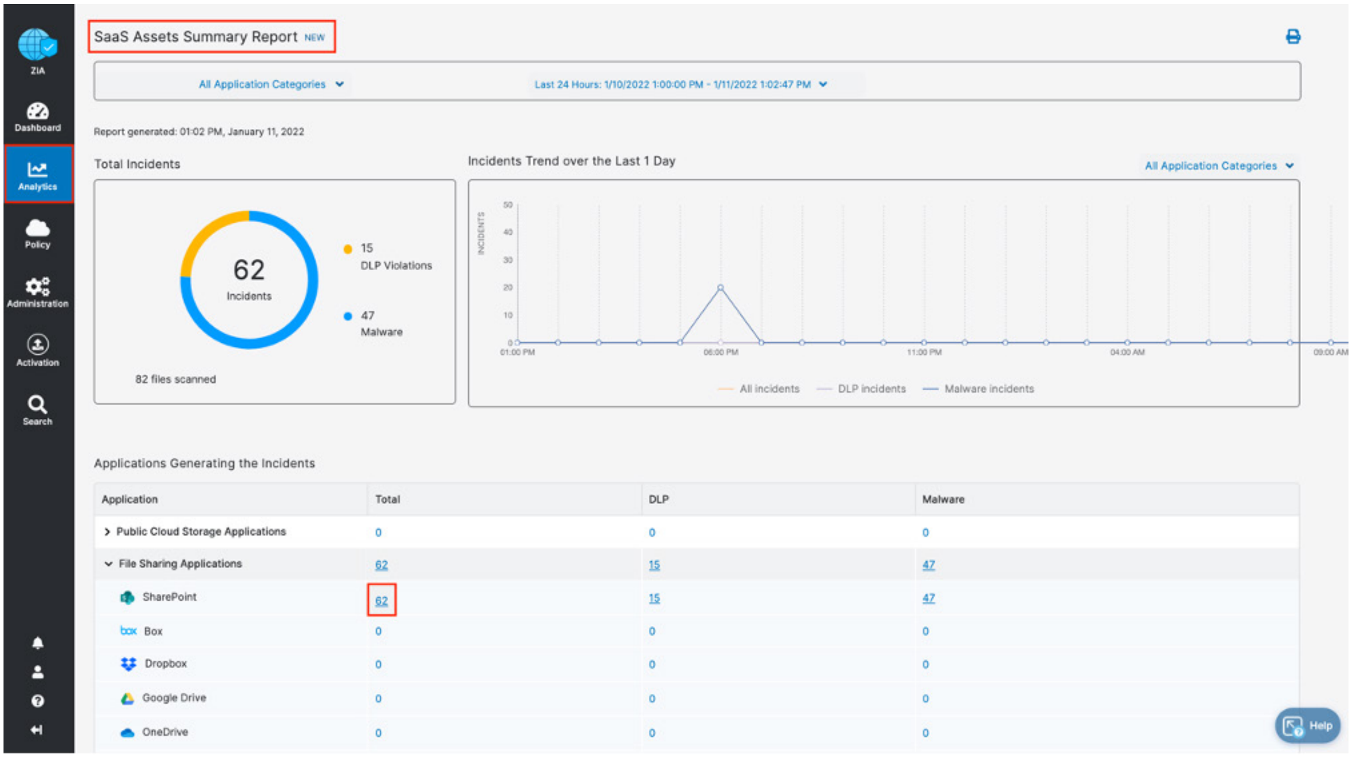


*Figure 27. SaaS security visibility*

## SaaS Assets and SaaS Assets Summary Report

The SaaS Asset Reports provide a summary or customizable reporting to have a quick view of your content violations and discovered malware. The SaaS Assets Summary Report provides all activity and violations in a quick glance. The report identifies all SaaS tenant information from a single screen. The data is hyperlinked, and you can easily pivot from a summary to individual logs and activities provided by SaaS Security Insights.

Select the **Total Incidents** number (62) next to SharePoint to pivot to SaaS Security Insights.



SaaS Assets Summary Report NEW

All Application Categories

Last 24 Hours: 1/10/2022 1:00:00 PM - 1/11/2022 1:02:47 PM

Report generated: 01:02 PM, January 11, 2022

Total Incidents

62 Incidents

15 DLP Violations

47 Malware

82 files scanned

Incidents Trend over the Last 1 Day

All Application Categories

Applications Generating the Incidents

| Application | Total | DLP | Malware |
|---|---|---|---|
| Public Cloud Storage Applications | 0 | 0 | 0 |
| File Sharing Applications | 62 | 15 | 47 |
| SharePoint | 62 | 15 | 47 |
| Box | 0 | 0 | 0 |
| Dropbox | 0 | 0 | 0 |
| Google Drive | 0 | 0 | 0 |
| OneDrive | 0 | 0 | 0 |

*Figure 28. Summary reports*

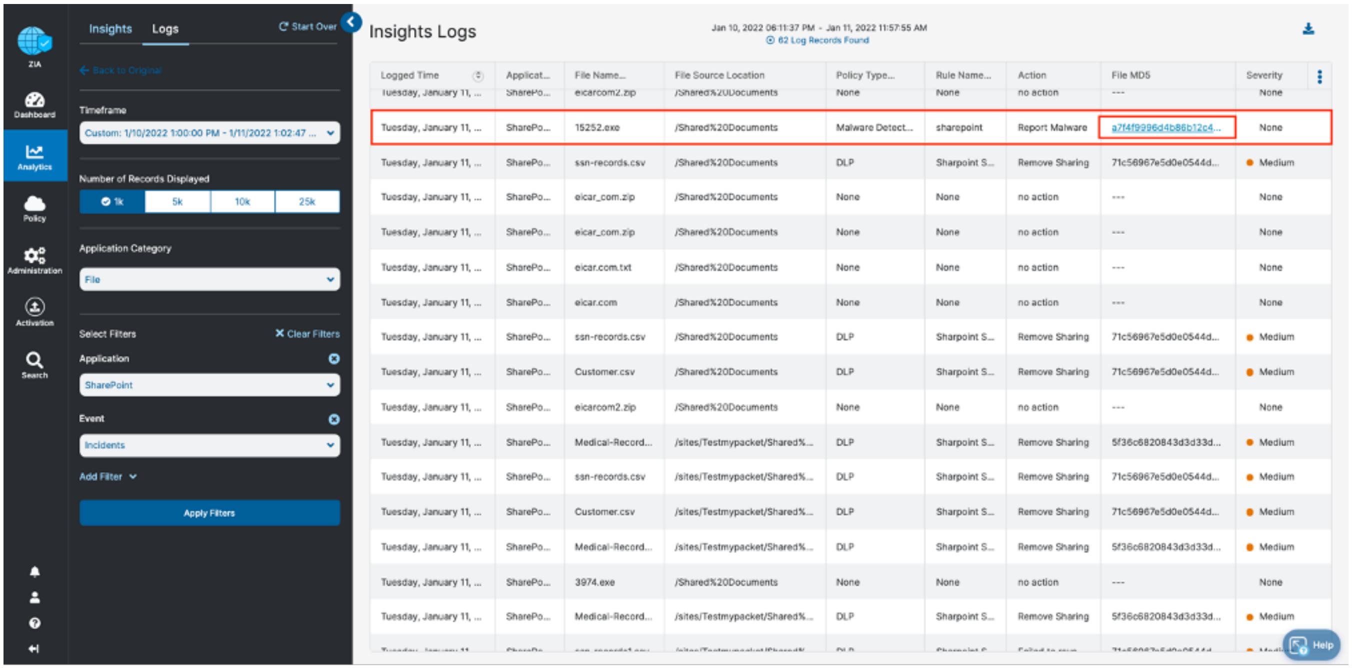
This opens SaaS Security Insights and the log data for each violation containing over 30 metadata points of information.

## SaaS Security Insights

The SaaS Security Insights page lets you view and select information fields for 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



Timeframe: Custom: 1/10/2022 1:00:00 PM - 1/11/2022 1:02:47 ...

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

Application Category: File

Select Filters — ✕ Clear Filters

Application: SharePoint

Event: Incidents

Add Filter

Apply Filters

Insights Logs

Jan 10, 2022 06:11:37 PM - Jan 11, 2022 11:57:55 AM
62 Log Records Found

| Logged Time | Applicat... | File Name... | File Source Location | Policy Type... | Rule Name... | Action | File MD5 | Severity |
|---|---|---|---|---|---|---|---|---|
| Tuesday, January 11, ... | SharePo... | eicarcom2.zip | /Shared%20Documents | None | None | no action | --- | None |
| Tuesday, January 11, ... | SharePo... | 15252.exe | /Shared%20Documents | Malware Detect... | sharepoint | Report Malware | a7f4f9996d4b86b12c4... | None |
| Tuesday, January 11, ... | SharePo... | ssn-records.csv | /Shared%20Documents | DLP | Sharpoint S... | Remove Sharing | 71c56967e5d0e0544d... | ● Medium |
| Tuesday, January 11, ... | SharePo... | eicar_com.zip | /Shared%20Documents | None | None | no action | --- | None |
| Tuesday, January 11, ... | SharePo... | eicar_com.zip | /Shared%20Documents | None | None | no action | --- | None |
| Tuesday, January 11, ... | SharePo... | eicar.com.txt | /Shared%20Documents | None | None | no action | --- | None |
| Tuesday, January 11, ... | SharePo... | eicar.com | /Shared%20Documents | None | None | no action | --- | None |
| Tuesday, January 11, ... | SharePo... | ssn-records.csv | /Shared%20Documents | DLP | Sharpoint S... | Remove Sharing | 71c56967e5d0e0544d... | ● Medium |
| Tuesday, January 11, ... | SharePo... | Customer.csv | /Shared%20Documents | DLP | Sharpoint S... | Remove Sharing | 71c56967e5d0e0544d... | ● Medium |
| Tuesday, January 11, ... | SharePo... | eicarcom2.zip | /Shared%20Documents | None | None | no action | --- | None |
| Tuesday, January 11, ... | SharePo... | Medical-Record... | /sites/Testmypacket/Shared%... | DLP | Sharpoint S... | Remove Sharing | 5f36c6820843d3d33d... | ● Medium |
| Tuesday, January 11, ... | SharePo... | ssn-records.csv | /sites/Testmypacket/Shared%... | DLP | Sharpoint S... | Remove Sharing | 71c56967e5d0e0544d... | ● Medium |
| Tuesday, January 11, ... | SharePo... | Customer.csv | /sites/Testmypacket/Shared%... | DLP | Sharpoint S... | Remove Sharing | 71c56967e5d0e0544d... | ● Medium |
| Tuesday, January 11, ... | SharePo... | Medical-Record... | /sites/Testmypacket/Shared%... | DLP | Sharpoint S... | Remove Sharing | 5f36c6820843d3d33d... | ● Medium |
| Tuesday, January 11, ... | SharePo... | 3974.exe | /Shared%20Documents | None | None | no action | --- | None |
| Tuesday, January 11, ... | SharePo... | Medical-Record... | /sites/Testmypacket/Shared%... | DLP | Sharpoint S... | Remove Sharing | 5f36c6820843d3d33d... | ● Medium |

*Figure 29. SaaS security insights*

# Configuring SSL Inspection for SharePoint

Up to 94% of traffic traversing the internet is encrypted using SSL or TLS to protect confidential and sensitive data. This data is transported across the internet between browsers, cloud apps, and websites through an encrypted connection between your browser and the website (cloud application).

While this encryption protects the sensitive data, it is important to mitigate risk within this traffic. Advanced threats and malware are routinely delivered within encrypted traffic. SSL decryption enables organizations to open encrypted traffic in a safe and controlled manner and inspect the data to identify threats inbound to applications, as well as outbound from users to the internet. The traffic is then re-encrypted and sent on its way. Inspecting encrypted traffic is nontrivial and it requires a proxy architecture.

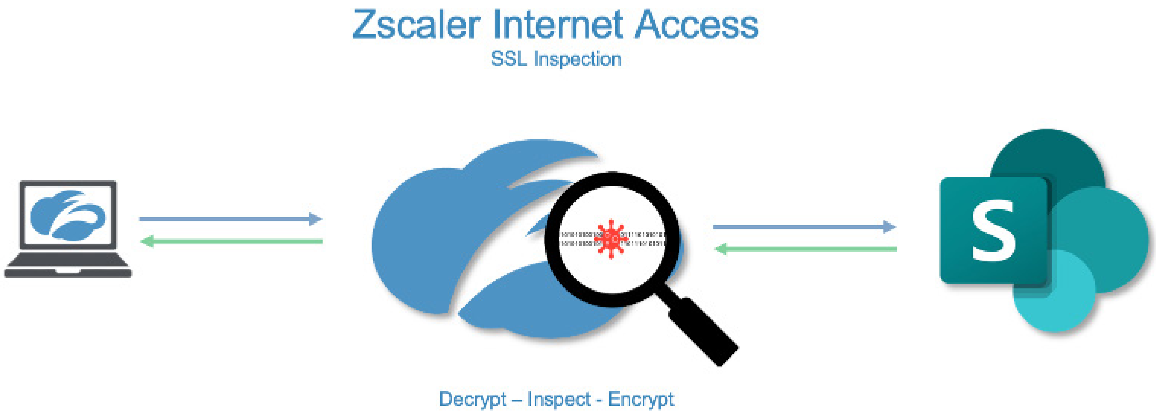


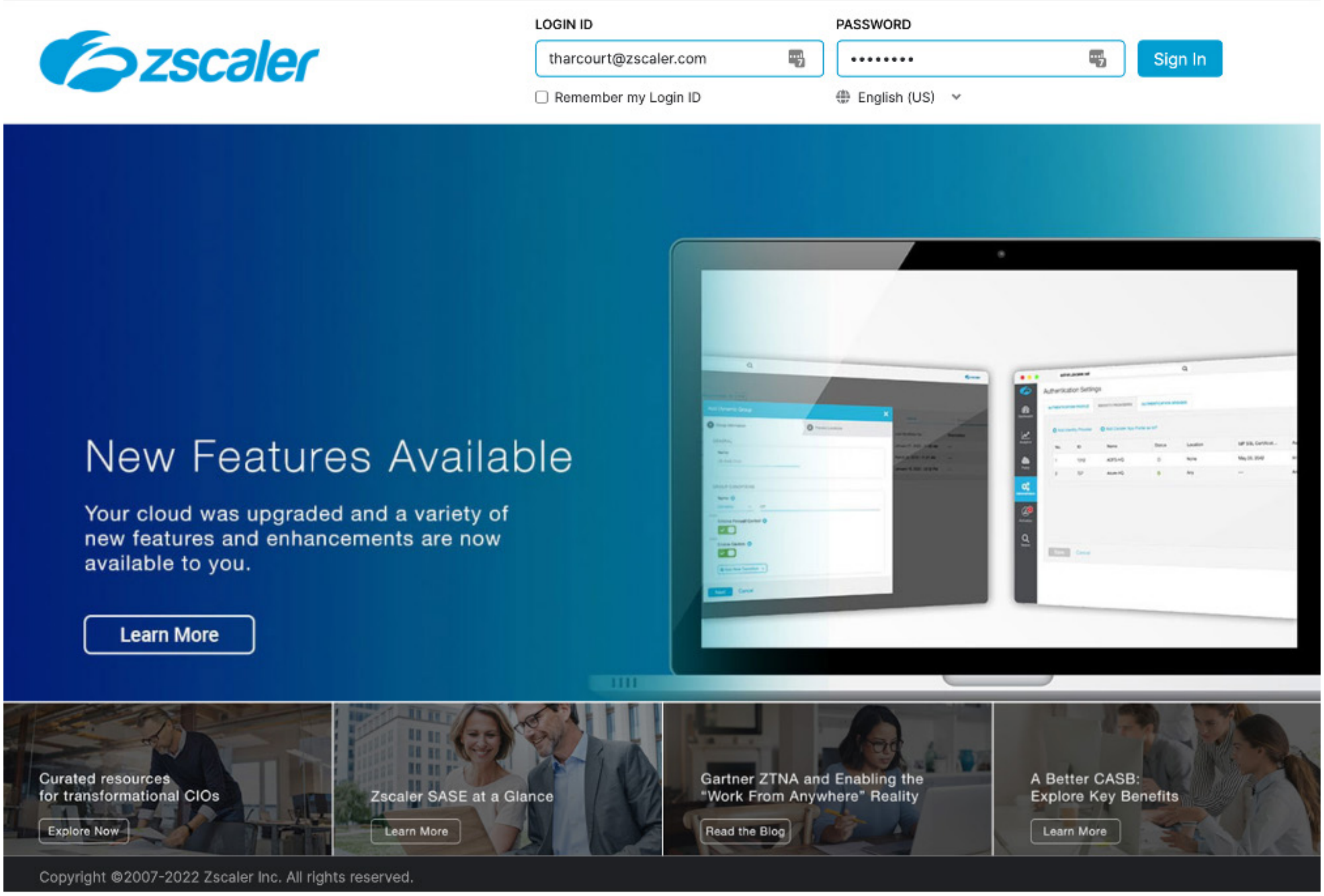
*Figure 30. SSL decryption*

Zscaler has made enabling and managing SSL Inspection as manageable and operationally sound as possible. The certificates required for SSL Inspection are installed during the installation of the Zscaler Client Connector, and the encryption and decryption process is performed in ASIC to nullify the latency and performance hit experienced by other security vendors. This allows organizations to enable SSL visibility for all inspectable destinations. It enables security and provides cloud application control, DLP, file protection, sandbox, and malware protection where it did not exist previously.

This guide provides the process of enabling SSL inspection for SharePoint, allowing you to control access and secure the data between your organizations and the SharePoint Online site.

## Configuring SSL Inspection for SharePoint

Log into your ZIA tenant with Admin credentials to start the installation process. Your Zscaler cloud instance may be different from the example.


LOGIN ID

tharcourt@zscaler.com

PASSWORD

••••••••

zscaler
Sign In
□ Remember my Login ID
English (US)
New Features Available
Your cloud was upgraded and a variety of new features and enhancements are now available to you.
Learn More
Curated resources for transformational CIOs
Explore Now
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2022 Zscaler Inc. All rights reserved.

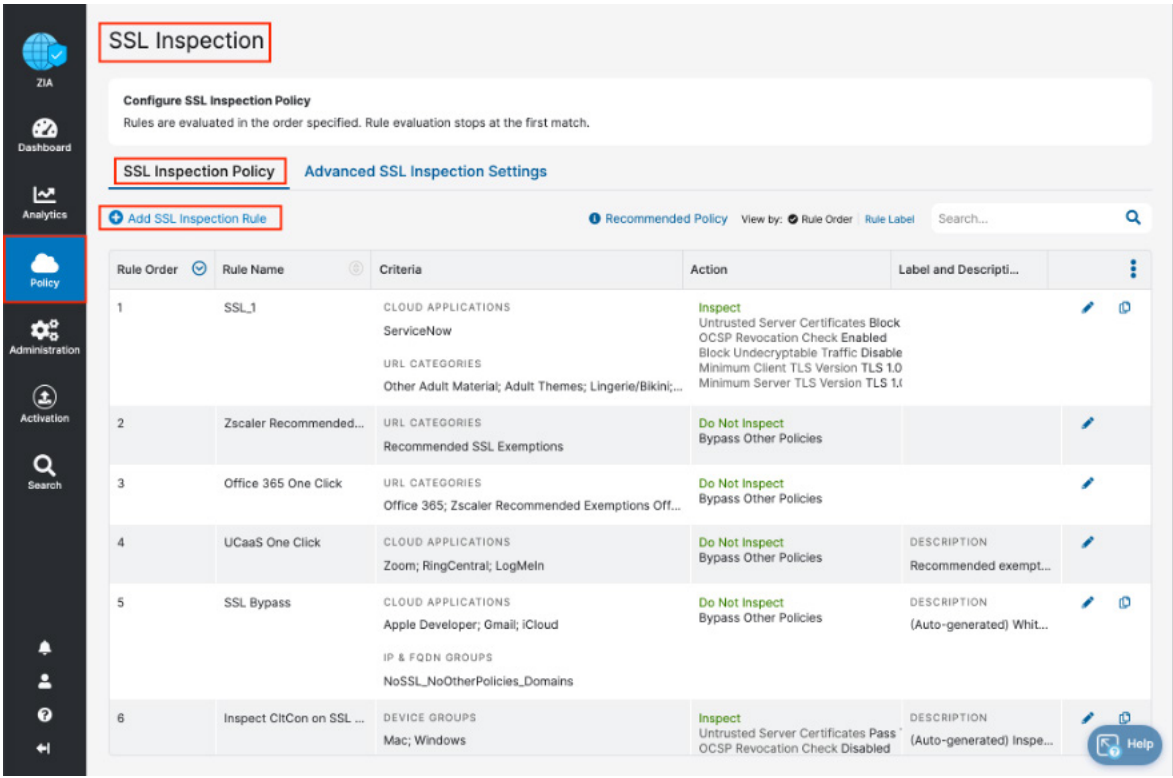
*Figure 31. ZIA tenant*

The current ZIA clouds include zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscloud.net, zscalerbeta.net, and zscalergov.net.

## Configuring an SSL Inspection Rule

To enable SSL inspection, first create an inspection rule to identify the SaaS application or destination to inspect.

1. Select **Policy**.
2. Select **SSL Inspection**.
3. Select **SSL Inspection Policy**.
4. Click **Add SSL Inspection Rule**.



SSL Inspection

**Configure SSL Inspection Policy**

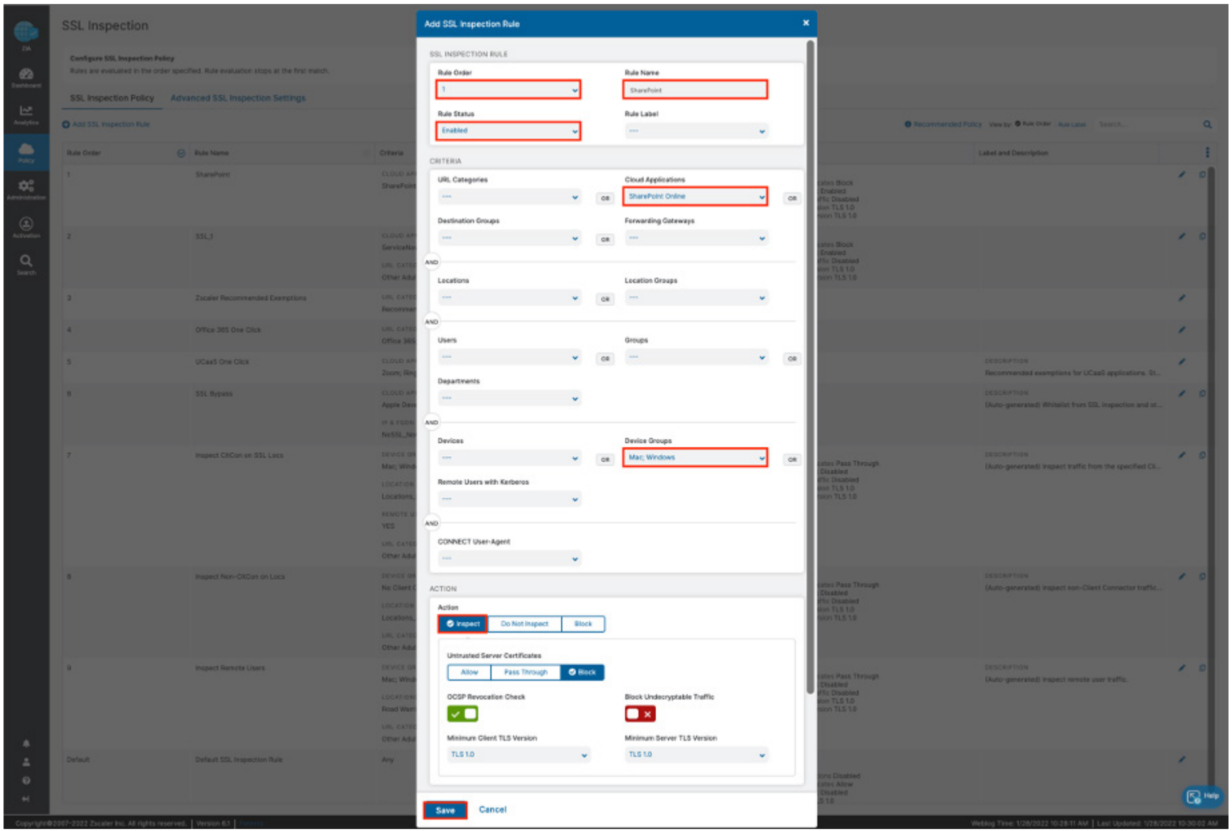
Rules are evaluated in the order specified. Rule evaluation stops at the first match.

| Rule Order | Rule Name | Criteria | Action | Label and Descripti... |
|---|---|---|---|---|
| 1 | SSL_1 | CLOUD APPLICATIONS<br>ServiceNow<br>URL CATEGORIES<br>Other Adult Material; Adult Themes; Lingerie/Bikini;... | Inspect<br>Untrusted Server Certificates Block<br>OCSP Revocation Check Enabled<br>Block Undecryptable Traffic Disable<br>Minimum Client TLS Version TLS 1.0<br>Minimum Server TLS Version TLS 1.( | |
| 2 | Zscaler Recommended... | URL CATEGORIES<br>Recommended SSL Exemptions | Do Not Inspect<br>Bypass Other Policies | |
| 3 | Office 365 One Click | URL CATEGORIES<br>Office 365; Zscaler Recommended Exemptions Off... | Do Not Inspect<br>Bypass Other Policies | |
| 4 | UCaaS One Click | CLOUD APPLICATIONS<br>Zoom; RingCentral; LogMeIn | Do Not Inspect<br>Bypass Other Policies | DESCRIPTION<br>Recommended exempt... |
| 5 | SSL Bypass | CLOUD APPLICATIONS<br>Apple Developer; Gmail; iCloud<br>IP & FQDN GROUPS<br>NoSSL_NoOtherPolicies_Domains | Do Not Inspect<br>Bypass Other Policies | DESCRIPTION<br>(Auto-generated) Whit... |
| 6 | Inspect CltCon on SSL ... | DEVICE GROUPS<br>Mac; Windows | Inspect<br>Untrusted Server Certificates Pass<br>OCSP Revocation Check Disabled | DESCRIPTION<br>(Auto-generated) Inspe... |

*Figure 32. SSL inspection rules*

Complete the necessary fields to create the SharePoint SSL inspection rule. Rule order is important as the rules are evaluated top down, and the first rule matched is the processed rule. Make sure the inspection rule for SharePoint is in the correct order and is evaluated before the default MS365 bypass rule, or any other bypass rule.

5. Specify **Rule Order**.
6. Provide an intuitive **Rule Name**.
7. Make sure the **Rule Status** is **Enabled**.
8. In **Cloud Application**, search and select the **SharePoint Online** cloud application.
9. Select the **Windows** and **Mac Device Groups** (**Mobile** is discussed in a separate guide).
10. Select **Inspect** for the **Action**.
11. Click **Save**, then **Activate** the configuration changes.



Add SSL Inspection Rule

SSL INSPECTION RULE

Rule Order: 1
Rule Name: SharePoint
Rule Status: Enabled
Rule Label: ---

CRITERIA

URL Categories: --- OR Cloud Applications: SharePoint Online OR
Destination Groups: --- OR Forwarding Gateways: ---
AND
Locations: --- OR Location Groups: ---
AND
Users: --- OR Groups: --- OR
Departments: ---
AND
Devices: --- OR Device Groups: Mac; Windows OR
Remote Users with Kerberos: ---
AND
CONNECT User-Agent: ---

ACTION

Action: [✓ Inspect] Do Not Inspect Block

Untrusted Server Certificates: Allow Pass Through [✓ Block]
OCSP Revocation Check: ✓
Block Undecryptable Traffic: ✕
Minimum Client TLS Version: TLS 1.0
Minimum Server TLS Version: TLS 1.0

*Figure 33. SSL inspection rule wizard*

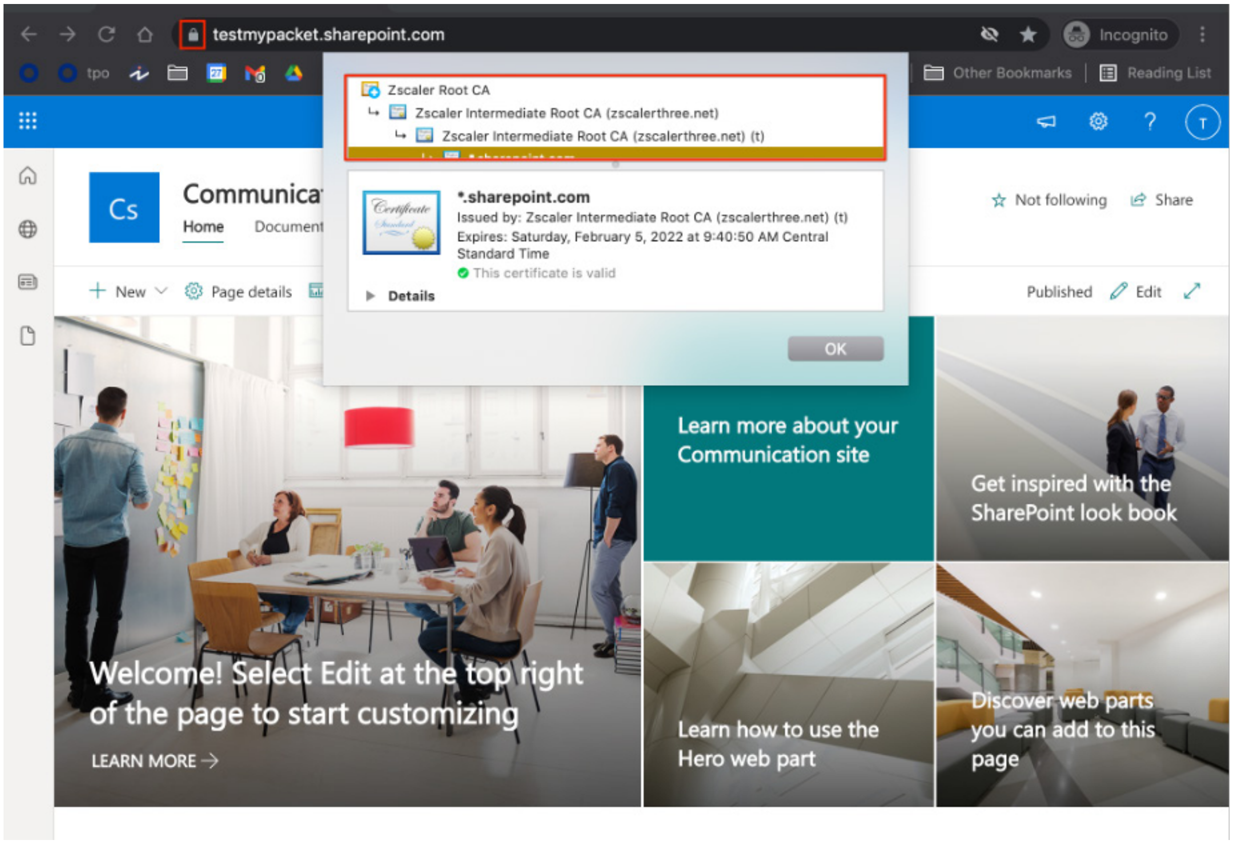
## Verify SSL Inspection

To verify SSL inspection is now active for the SharePoint site, look at the certificate that is used between the browser and Zscaler. This process is different for each browser. Although the procedures below are for Chrome, you can view the certificate in any browser.

> After enabling SSL inspection, use an incognito window to verify there are no caching issues to invalidate your testing.

1. Click the lock next to the SharePoint URL.
2. Select **Connection is secure**.
3. Select **Certificate is Valid**.

Validate that you're using the Zscaler Intermediate Root CA certificate instead of the SharePoint site certificate. You could use a custom certificate for your installation if it was set up. For more information, see [SSL Inspection Using a Custom Intermediate Root Certificate]().



Zscaler Root CA
↳ Zscaler Intermediate Root CA (zscalerthree.net)
↳ Zscaler Intermediate Root CA (zscalerthree.net) (t)

*.sharepoint.com
Issued by: Zscaler Intermediate Root CA (zscalerthree.net) (t)
Expires: Saturday, February 5, 2022 at 9:40:50 AM Central Standard Time
This certificate is valid

testmypacket.sharepoint.com
Incognito
tpo
Other Bookmarks
Reading List
Cs
Communica
Home
Document
Not following
Share
New
Page details
Published
Edit
Details
OK
Learn more about your Communication site
Get inspired with the SharePoint look book
Welcome! Select Edit at the top right of the page to start customizing
LEARN MORE →
Learn how to use the Hero web part
Discover web parts you can add to this page

*Figure 34. Verifying SSL inspection for SharePoint*

You can configure and enable the feature that requires deep packet inspection.

## ZIA Cloud Application Control

The ZIA security cloud is a fully integrated cloud-based security stack that sits in-line between users and the internet, inspecting all traffic (including SSL) flowing between them. As part of the platform, Zscaler cloud application control delivers full visibility into application usage, and granular policies ensure the proper use of both sanctioned and unsanctioned applications.

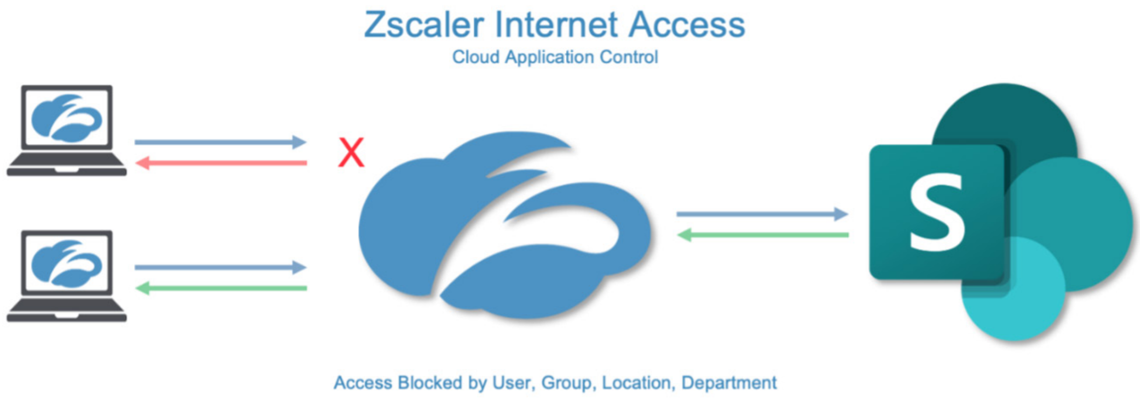

Zscaler Internet Access
Cloud Application Control
X
Access Blocked by User, Group, Location, Department

*Figure 35. Cloud app control*

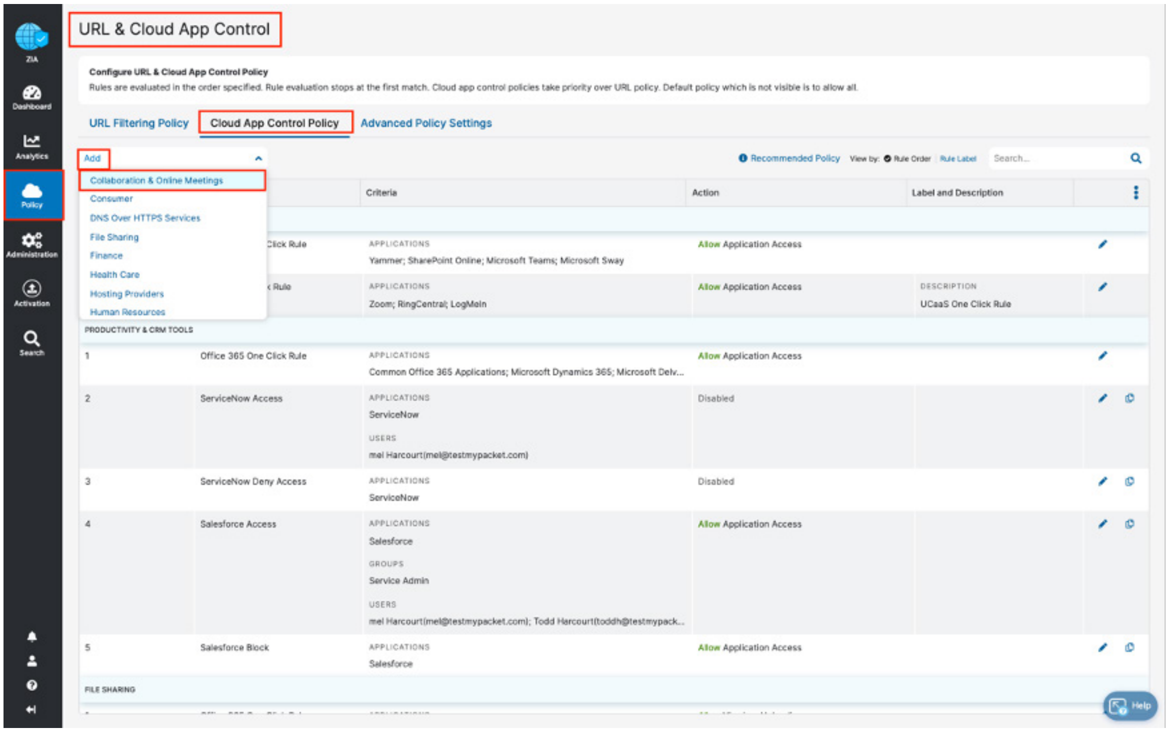
Cloud app control provides SaaS application intelligence to consolidate all associated URLs and functions of the application in a single security setting. This allows you to control specific user, groups, locations, or departments, and only allow application access to the correct users.

For most Microsoft 365 installations, the Zscaler one-click configuration is enabled by default. The one-click configuration bypasses inspection capabilities of most Zscaler features (including SSL inspection), which is required for deep packet inspection of data. To perform in-line inspection of data destined to SharePoint, re-enable SSL inspection, then enable cloud application policies controlling access and cloud app control for SharePoint.

## ZIA Cloud Application Control Policy

To configure Zscaler Cloud Application access policies, create a rule to allow traffic to SharePoint for users in a specific security group, and a rule to block all other traffic destined to SharePoint (otherwise known as a Block Any Any rule). The block rule is the last rule in the series and you must configure any user that needs to access SharePoint higher in the rule order.

1. Click **Policy**.
2. Select the **Cloud App Control Policy** tab.
3. Select **Add**.
4. Select **Collaboration & Online Meetings**.



URL & Cloud App Control

**Configure URL & Cloud App Control Policy**

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

| | | Criteria | Action | Label and Description |
|---|---|---|---|---|
| | Click Rule | APPLICATIONS<br>Yammer; SharePoint Online; Microsoft Teams; Microsoft Sway | Allow Application Access | |
| | k Rule | APPLICATIONS<br>Zoom; RingCentral; LogMeIn | Allow Application Access | DESCRIPTION<br>UCaaS One Click Rule |
| PRODUCTIVITY & CRM TOOLS | | | | |
| 1 | Office 365 One Click Rule | APPLICATIONS<br>Common Office 365 Applications; Microsoft Dynamics 365; Microsoft Delv... | Allow Application Access | |
| 2 | ServiceNow Access | APPLICATIONS<br>ServiceNow<br>USERS<br>mel Harcourt(mel@testmypacket.com) | Disabled | |
| 3 | ServiceNow Deny Access | APPLICATIONS<br>ServiceNow | Disabled | |
| 4 | Salesforce Access | APPLICATIONS<br>Salesforce<br>GROUPS<br>Service Admin<br>USERS<br>mel Harcourt(mel@testmypacket.com); Todd Harcourt(toddh@testmypack... | Allow Application Access | |
| 5 | Salesforce Block | APPLICATIONS<br>Salesforce | Allow Application Access | |
| FILE SHARING | | | | |

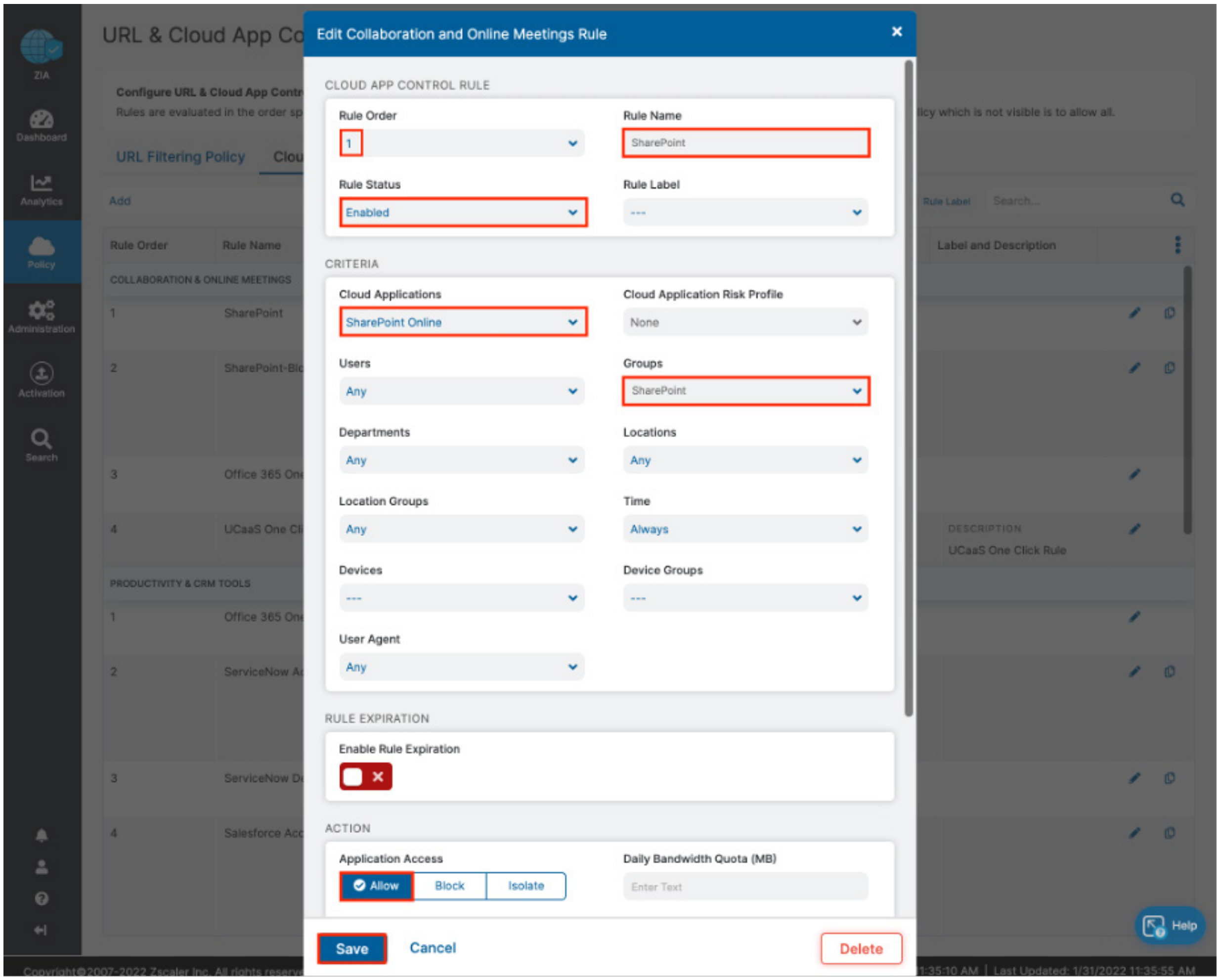
*Figure 36. Cloud app control*

This starts the rule wizard.

### ZIA Cloud Application Control

To create the SharePoint allow policy:

1. Select **1** for the **Rule Order**.
2. Give the rule an intuitive name.
3. Select **Enabled** for **Rule Status**.
4. Select **SharePoint Online** for the **Cloud Application**.
5. Select the **SharePoint** security group and other matching criteria.
6. Select **Allow** for **Application Access**.
7. Click **Save**, then **Activate** the configuration changes.



Edit Collaboration and Online Meetings Rule

CLOUD APP CONTROL RULE

Rule Order: 1

Rule Name: SharePoint

Rule Status: Enabled

Rule Label: ---

CRITERIA

Cloud Applications: SharePoint Online

Cloud Application Risk Profile: None

Users: Any

Groups: SharePoint

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

Devices: ---

Device Groups: ---

User Agent: Any

RULE EXPIRATION

Enable Rule Expiration

ACTION

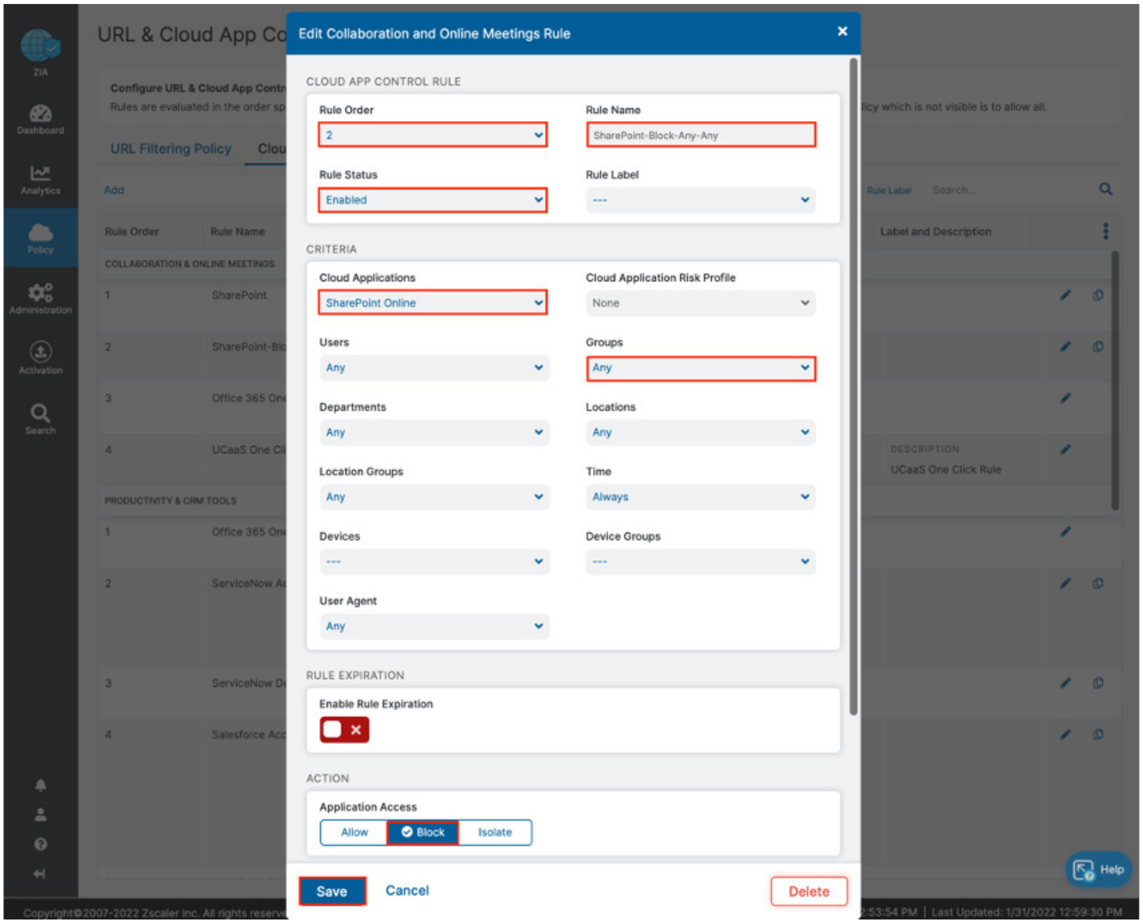
Application Access: ● Allow | Block | Isolate

Daily Bandwidth Quota (MB): Enter Text

*Figure 37. Cloud app control rule 1*

To create the SharePoint Block Any Any policy:

1. Select **2** for the **Rule Order**.
2. Give the rule an intuitive name.
3. Select **Enabled** for **Rule Status**.
4. Select **SharePoint Online** for the **Cloud Application**.
5. Select **Any Users** and **Any Groups**.
6. Select **Block** for **Application Access**.
7. Click **Save**, then **Activate** the configuration changes.



Edit Collaboration and Online Meetings Rule

CLOUD APP CONTROL RULE

Rule Order: 2

Rule Name: SharePoint-Block-Any-Any

Rule Status: Enabled

Rule Label: ---

CRITERIA

Cloud Applications: SharePoint Online

Cloud Application Risk Profile: None

Users: Any

Groups: Any

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

Devices: ---

Device Groups: ---

User Agent: Any

RULE EXPIRATION

Enable Rule Expiration: ✕

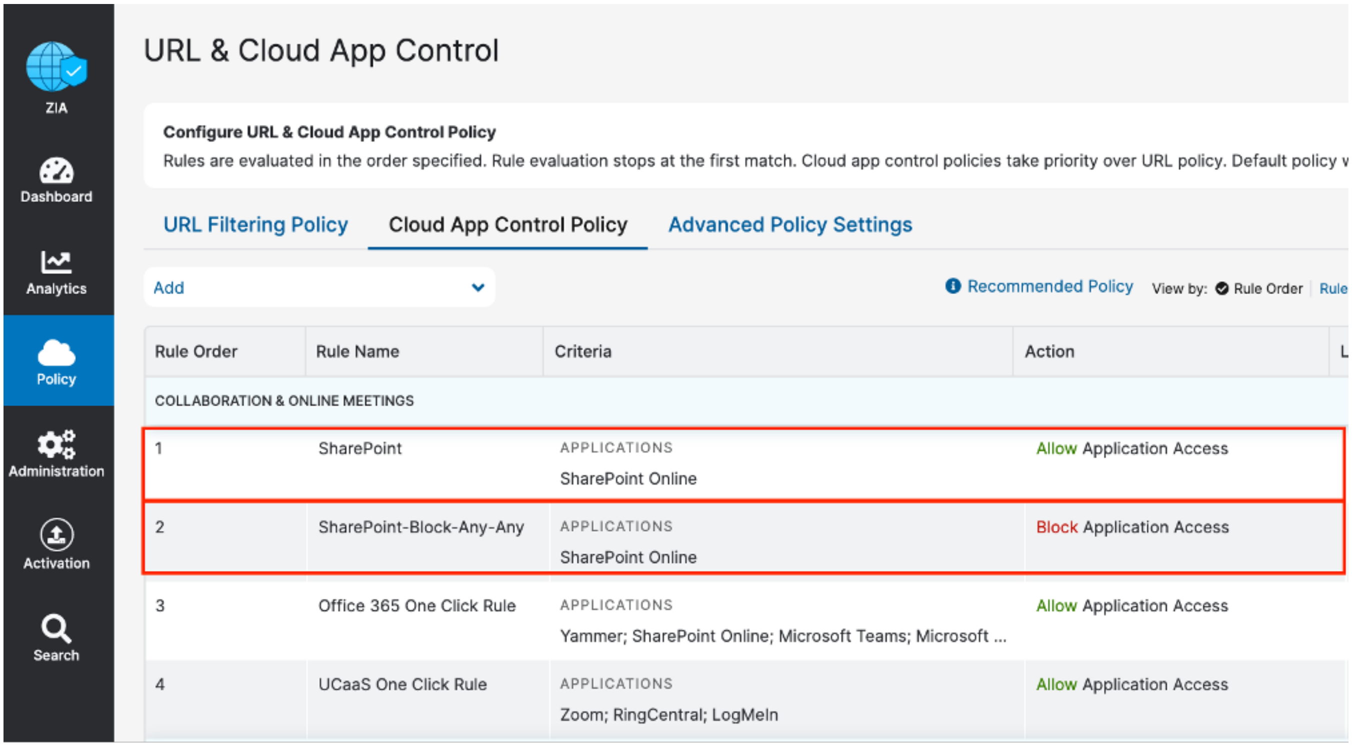
ACTION

Application Access: Allow [✓ Block] Isolate

Save Cancel Delete

*Figure 38. Cloud app control rule 2*

The completed policies are displayed.



URL & Cloud App Control

**Configure URL & Cloud App Control Policy**

Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy v

| Rule Order | Rule Name | Criteria | Action | L |
|---|---|---|---|---|
| COLLABORATION & ONLINE MEETINGS | | | | |
| 1 | SharePoint | APPLICATIONS<br>SharePoint Online | Allow Application Access | |
| 2 | SharePoint-Block-Any-Any | APPLICATIONS<br>SharePoint Online | Block Application Access | |
| 3 | Office 365 One Click Rule | APPLICATIONS<br>Yammer; SharePoint Online; Microsoft Teams; Microsoft ... | Allow Application Access | |
| 4 | UCaaS One Click Rule | APPLICATIONS<br>Zoom; RingCentral; LogMeIn | Allow Application Access | |

*Figure 39. Cloud app control completed policies*

## ZDX for SharePoint

As applications move to the cloud, the internet becomes a new transport network. With users working from anywhere, IT teams struggle to monitor and isolate issues affecting the user-to-cloud app experience. SharePoint is no exception, and ZDX provides visibility into the client's experience using SharePoint. ZDX uses the Zscaler Client Connector to generate application and network probes and gather device health. ZDX is a separate service from the Zscaler SaaS Security API and can run with or without SaaS security enabled.

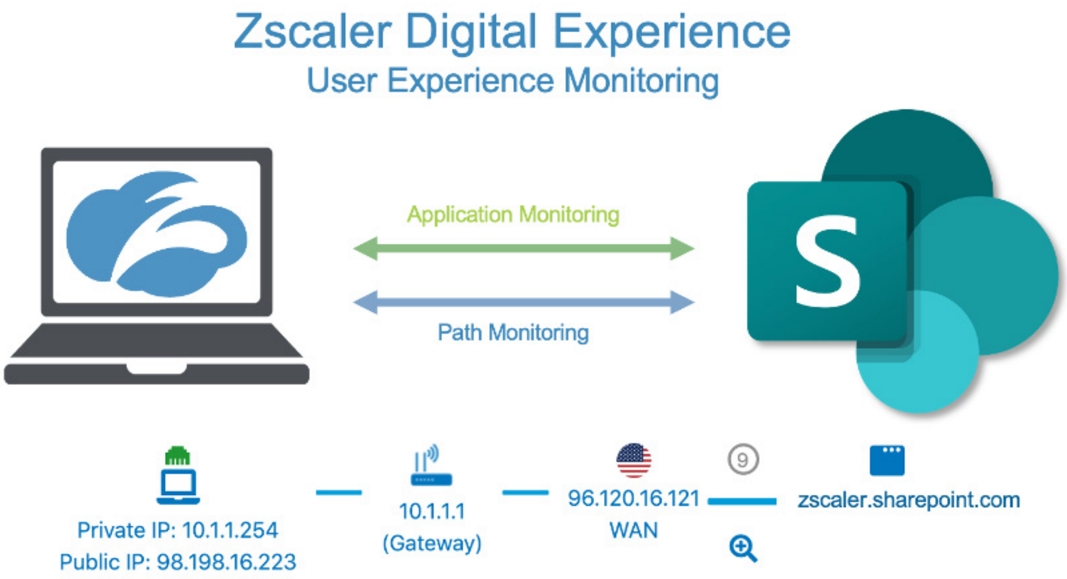


*Figure 40. ZDX for user experience monitoring for SharePoint*

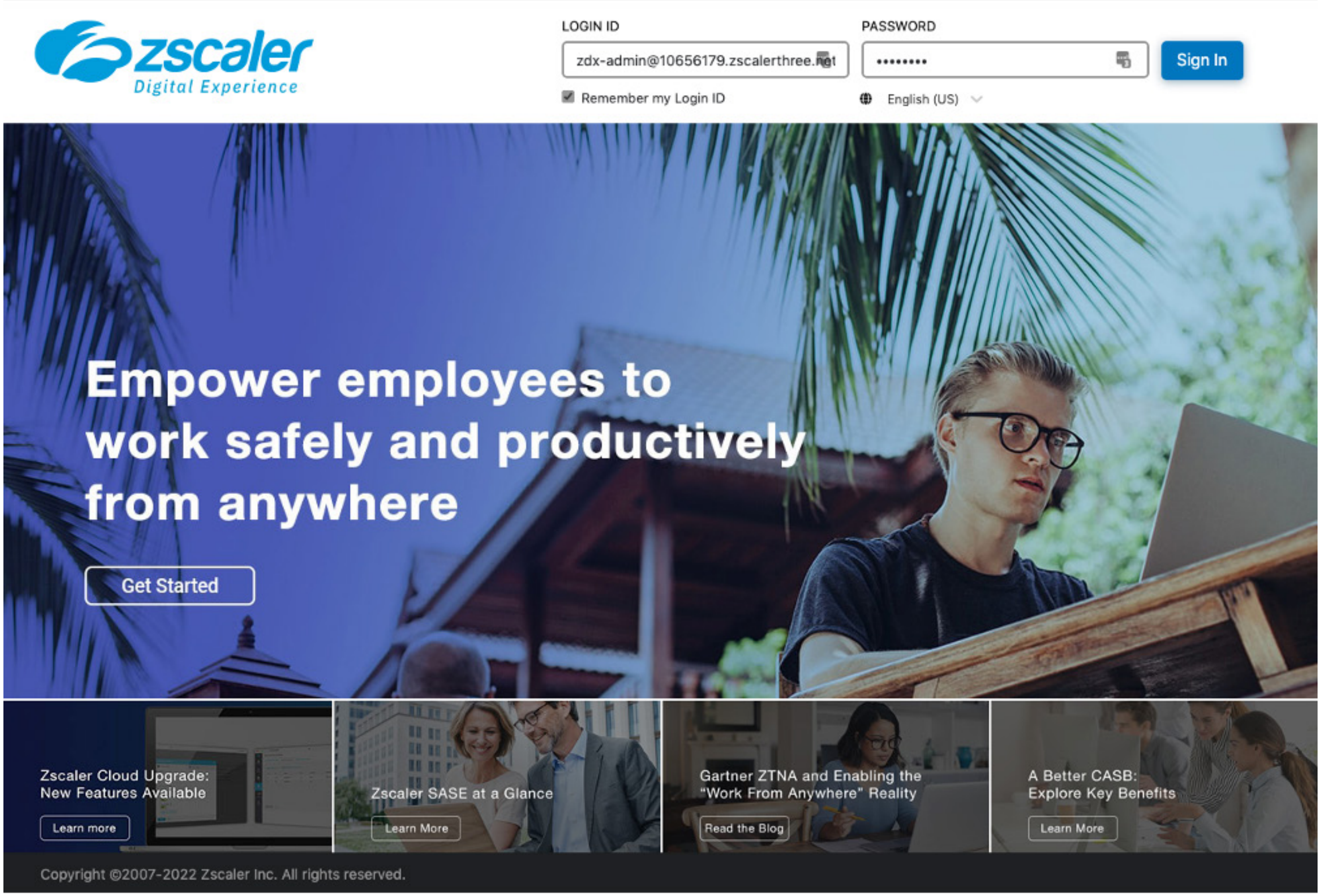
ZDX allows organizations to continuously gather and analyze data on end-user device resources and events such as CPU, memory usage, and Wi-Fi connectivity issues that impact end-user experiences. You can measure and analyze end-to-end and hop-by-hop network path metrics from every user device to the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

ZDX continuously monitors and measures application metrics such as response time, DNS resolution, and broader availability metrics of the application. You can monitor aggregated user experience performance scores tracked over time at the user, application, location, department, and organizational level.

## Configure ZDX for SharePoint

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

Log in to your organization's ZDX Admin Portal.



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

PASSWORD: ••••••••

☑ Remember my Login ID

English (US)

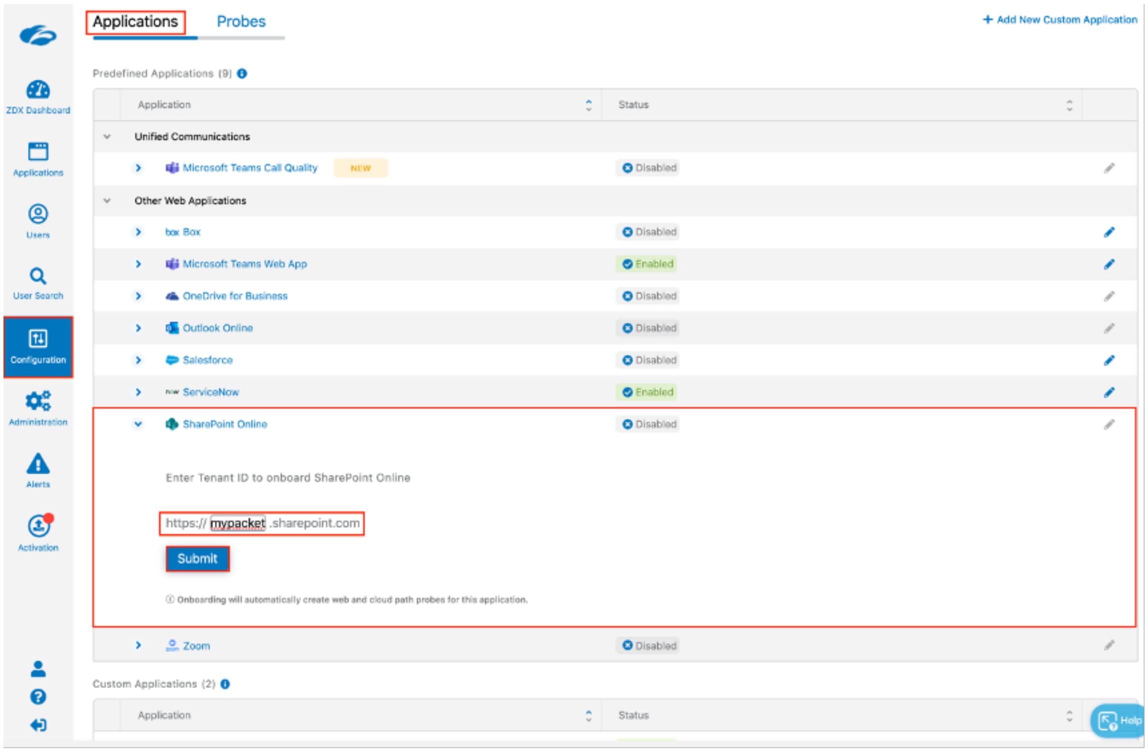
zscaler
Digital Experience
Sign In
Empower employees to work safely and productively from anywhere
Get Started
Zscaler Cloud Upgrade: New Features Available
Learn more
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2022 Zscaler Inc. All rights reserved.

*Figure 41. ZDX for user experience monitoring for SharePoint*

### Configure ZDX for SharePoint

SharePoint is a predefined application in ZDX. To configure the SharePoint application for monitoring:

1. Select **Configuration**.
2. Select **Applications**.
3. Select the Expand icon to the left of the SharePoint Online app.
4. Enter the URL for your **SharePoint Tenant ID**.
5. Click **Submit** to Onboard SharePoint.



Predefined Applications (9)

| Application | Status |
|---|---|
| Unified Communications | |
| Microsoft Teams Call Quality NEW | Disabled |
| Other Web Applications | |
| Box | Disabled |
| Microsoft Teams Web App | Enabled |
| OneDrive for Business | Disabled |
| Outlook Online | Disabled |
| Salesforce | Disabled |
| ServiceNow | Enabled |
| SharePoint Online | Disabled |
| Zoom | Disabled |

Enter Tenant ID to onboard SharePoint Online

https:// mypacket .sharepoint.com

Submit

ⓘ Onboarding will automatically create web and cloud path probes for this application.

Custom Applications (2)

| Application | Status |
|---|---|

*Figure 42. Onboard the SharePoint Online app*

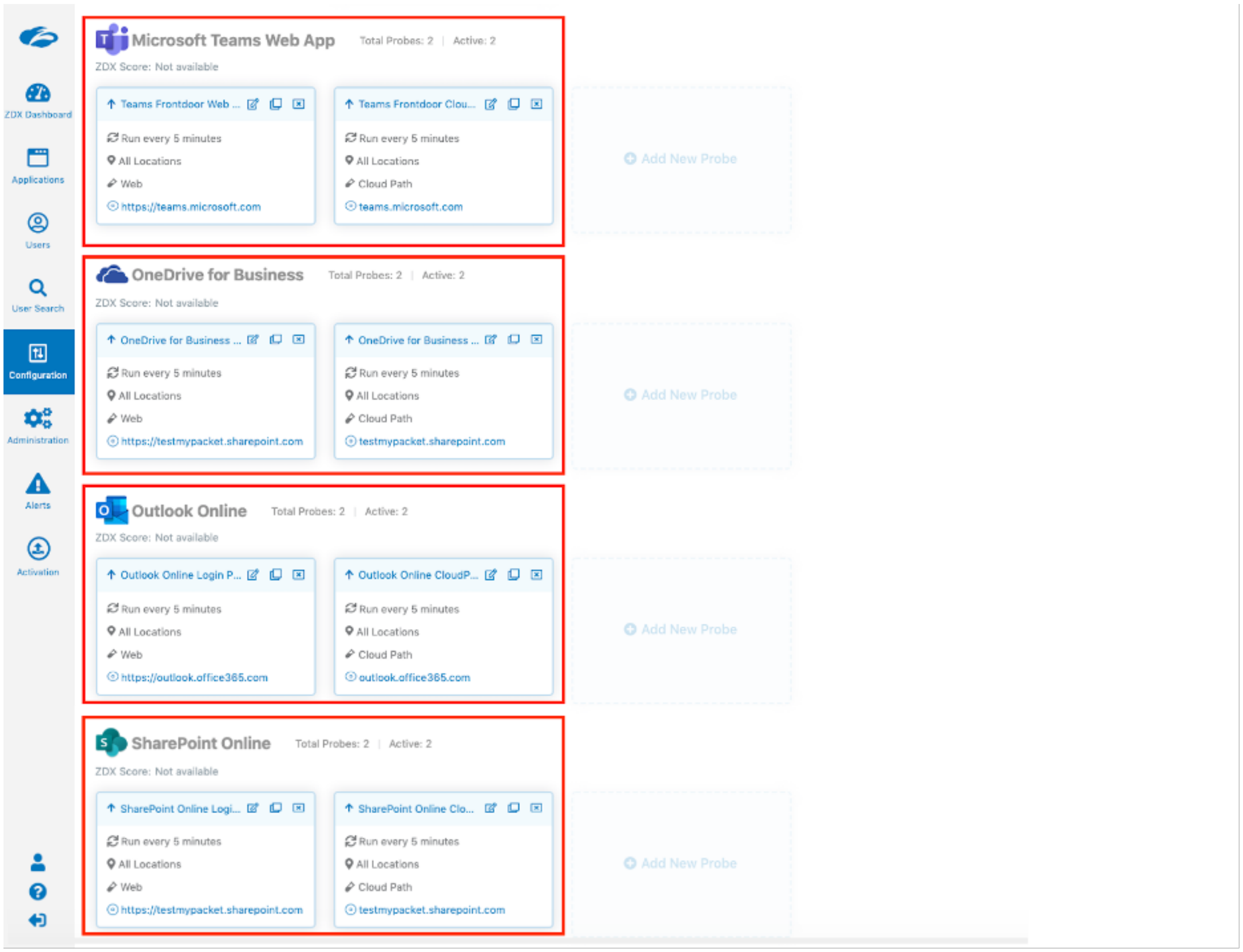
### Configure Probes for SharePoint Monitoring

Clicking Submit enables the SharePoint app for monitoring, and the pre-configured probes are displayed. The probes consist of a Cloud Path probe which uses ICMP Trace Route, and a landing page probe to the `testmypacket.sharepoint.com` location to monitor page load times.

You must make one change to the Cloud Path probe to have it follow the path of the landing page probe so there is no confusion of the results since this is entirely for SharePoint monitoring.

To edit the rule:

1. **Activate** the changes.
2. In the **SharePoint Online Cloud** pane, select the Edit icon to edit the probe.



Microsoft Teams Web App Total Probes: 2 | Active: 2
ZDX Score: Not available

Teams Frontdoor Web ...
Run every 5 minutes
All Locations
Web
https://teams.microsoft.com

Teams Frontdoor Clou...
Run every 5 minutes
All Locations
Cloud Path
teams.microsoft.com

OneDrive for Business Total Probes: 2 | Active: 2
ZDX Score: Not available

OneDrive for Business ...
Run every 5 minutes
All Locations
Web
https://testmypacket.sharepoint.com

OneDrive for Business ...
Run every 5 minutes
All Locations
Cloud Path
testmypacket.sharepoint.com

Outlook Online Total Probes: 2 | Active: 2
ZDX Score: Not available

Outlook Online Login P...
Run every 5 minutes
All Locations
Web
https://outlook.office365.com

Outlook Online CloudP...
Run every 5 minutes
All Locations
Cloud Path
outlook.office365.com

SharePoint Online Total Probes: 2 | Active: 2
ZDX Score: Not available

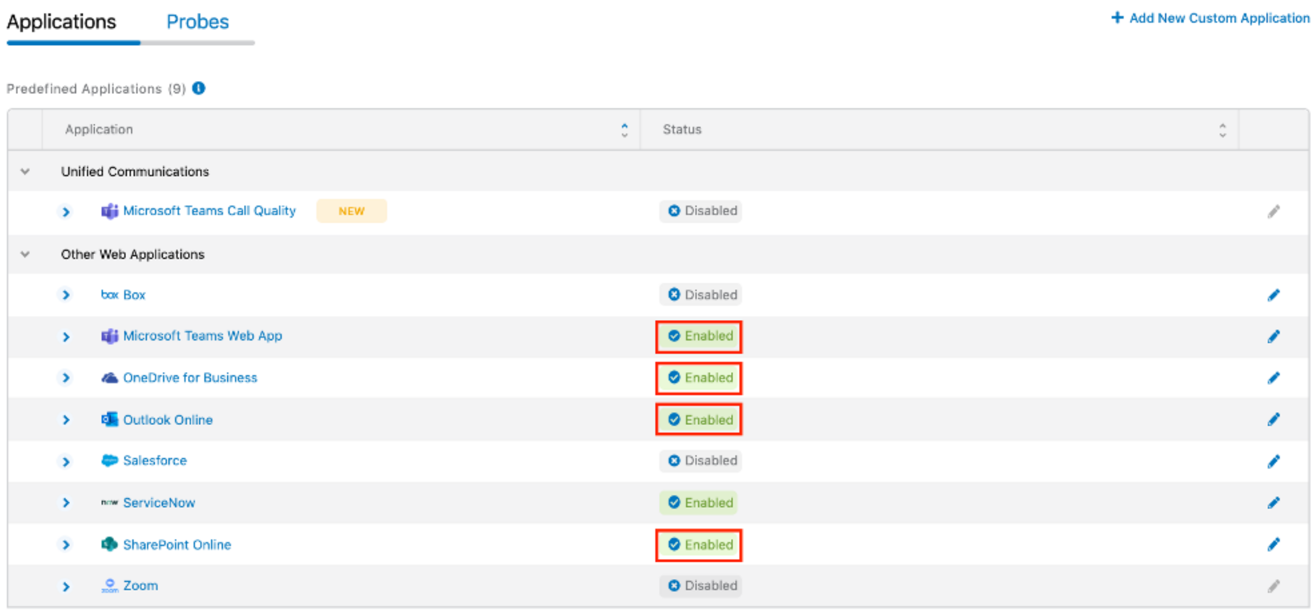
SharePoint Online Logi...
Run every 5 minutes
All Locations
Web
https://testmypacket.sharepoint.com

SharePoint Online Clo...
Run every 5 minutes
All Locations
Cloud Path
testmypacket.sharepoint.com

*Figure 43. ZDX for user experience monitoring for SharePoint*

## The ZDX-Enabled SharePoint Application

The SharePoint application monitoring is activated, and the probes begin to monitor all users that are using the Zscaler Client Connector.



Predefined Applications (9)

| Application | Status |
|---|---|
| Unified Communications | |
| Microsoft Teams Call Quality NEW | Disabled |
| Other Web Applications | |
| Box | Disabled |
| Microsoft Teams Web App | Enabled |
| OneDrive for Business | Enabled |
| Outlook Online | Enabled |
| Salesforce | Disabled |
| ServiceNow | Enabled |
| SharePoint Online | Enabled |
| Zoom | Disabled |

*Figure 44. Active SharePoint monitoring*

## Create an Alert for the SharePoint Service

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

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

To create your alert on page fetch times, select **Alerts** > **Rules** > **Add New Alert Rule**.

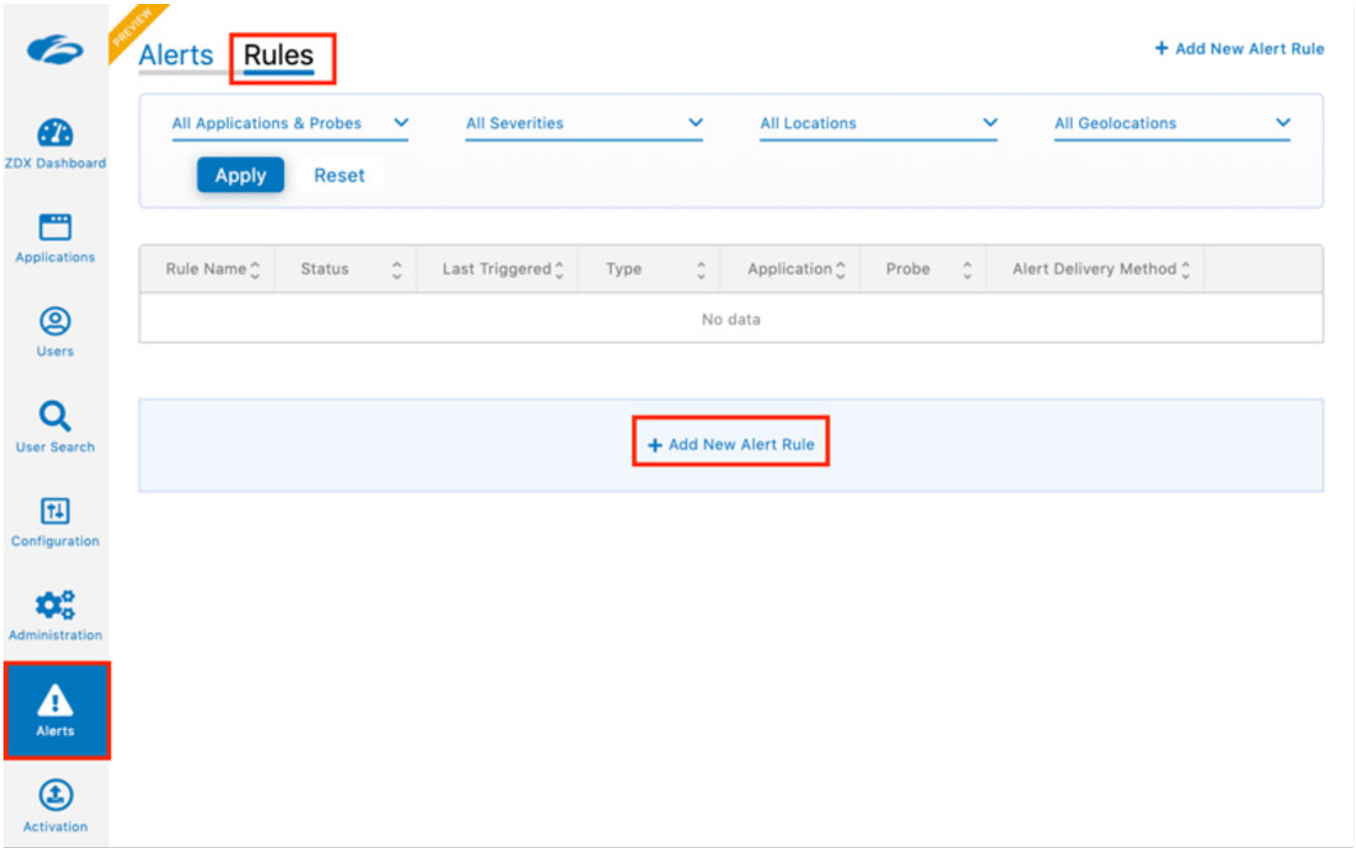
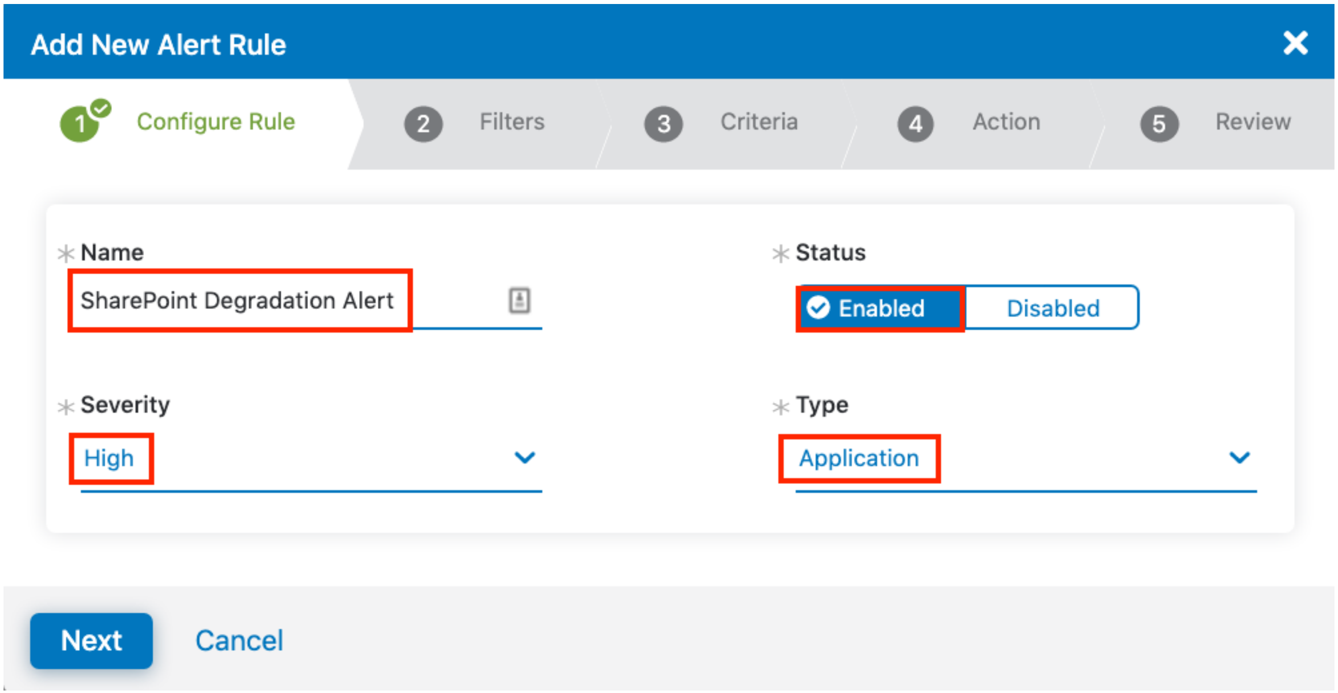


*Figure 45. Creating an alert*

This starts the Add New Rule Alert wizard.

To configure the Add New Rule Alert:

1. Name the **Rule**.
2. Select **Enabled** under **Status**.
3. Give the **Alert** an appropriate **Severity**.
4. Select a **Type** of **Application**.
5. Click **Next**.



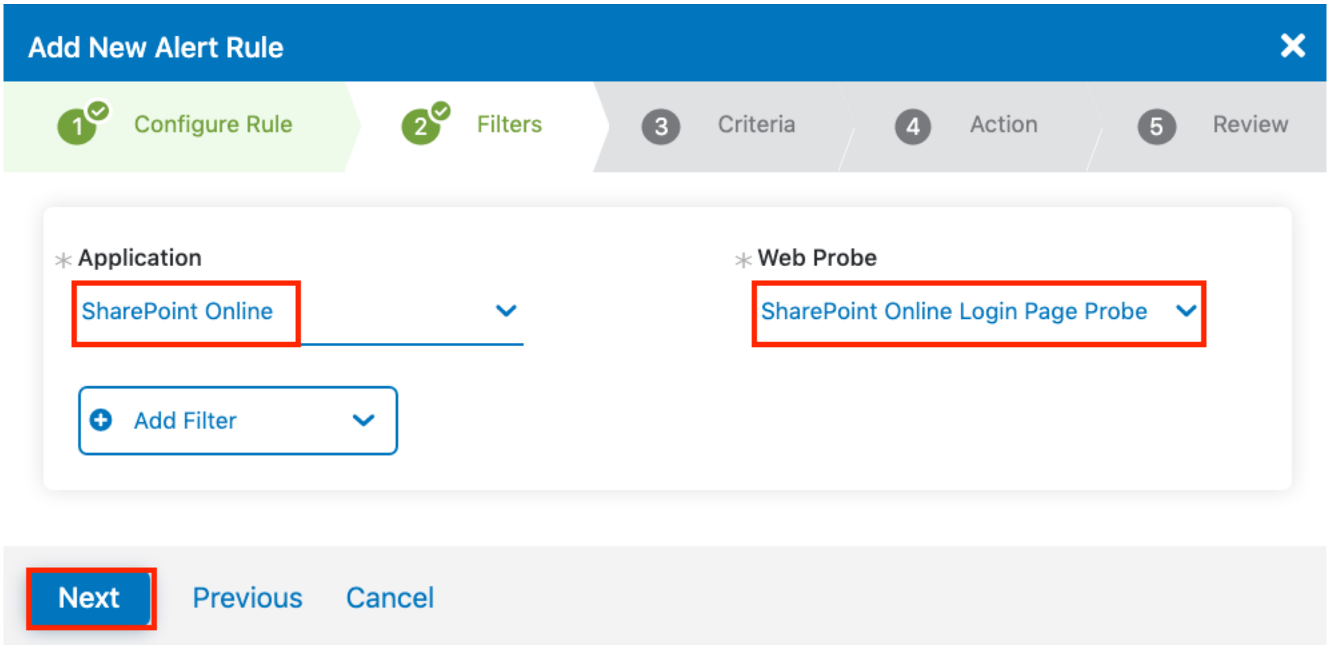
Add New Alert Rule

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

*Figure 46. Configure the new alert rule*

To add filters to the new rule alert:

1. Select **SharePoint Online** as the application.
2. Select **SharePoint Online Landing Page Probe** as the **Web Probe**.
3. Click **Next**.



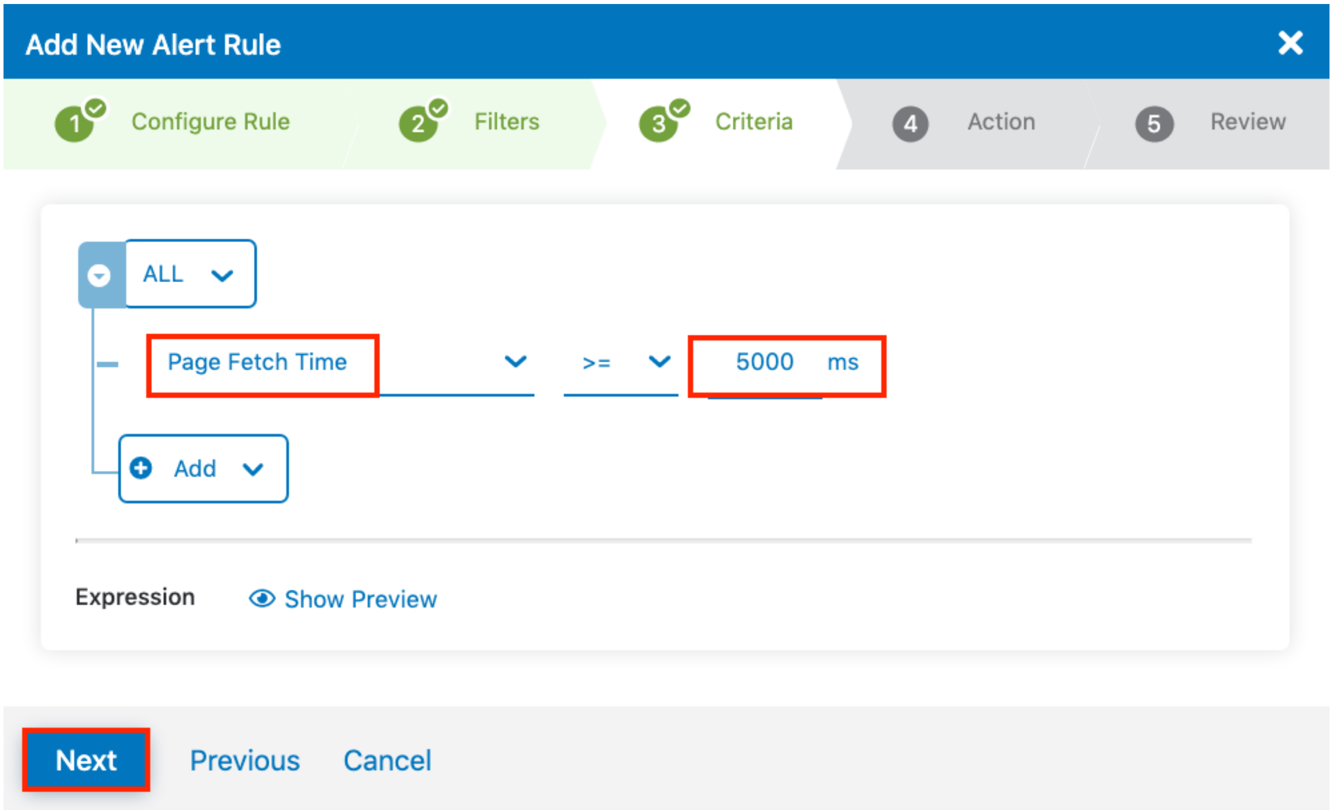
* Application: SharePoint Online

* Web Probe: SharePoint Online Login Page Probe

*Figure 47. Add filters to the alert*

When you create the criteria that triggers the alert when the threshold is exceeded, you can use multiple variables to eliminate false positives:

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



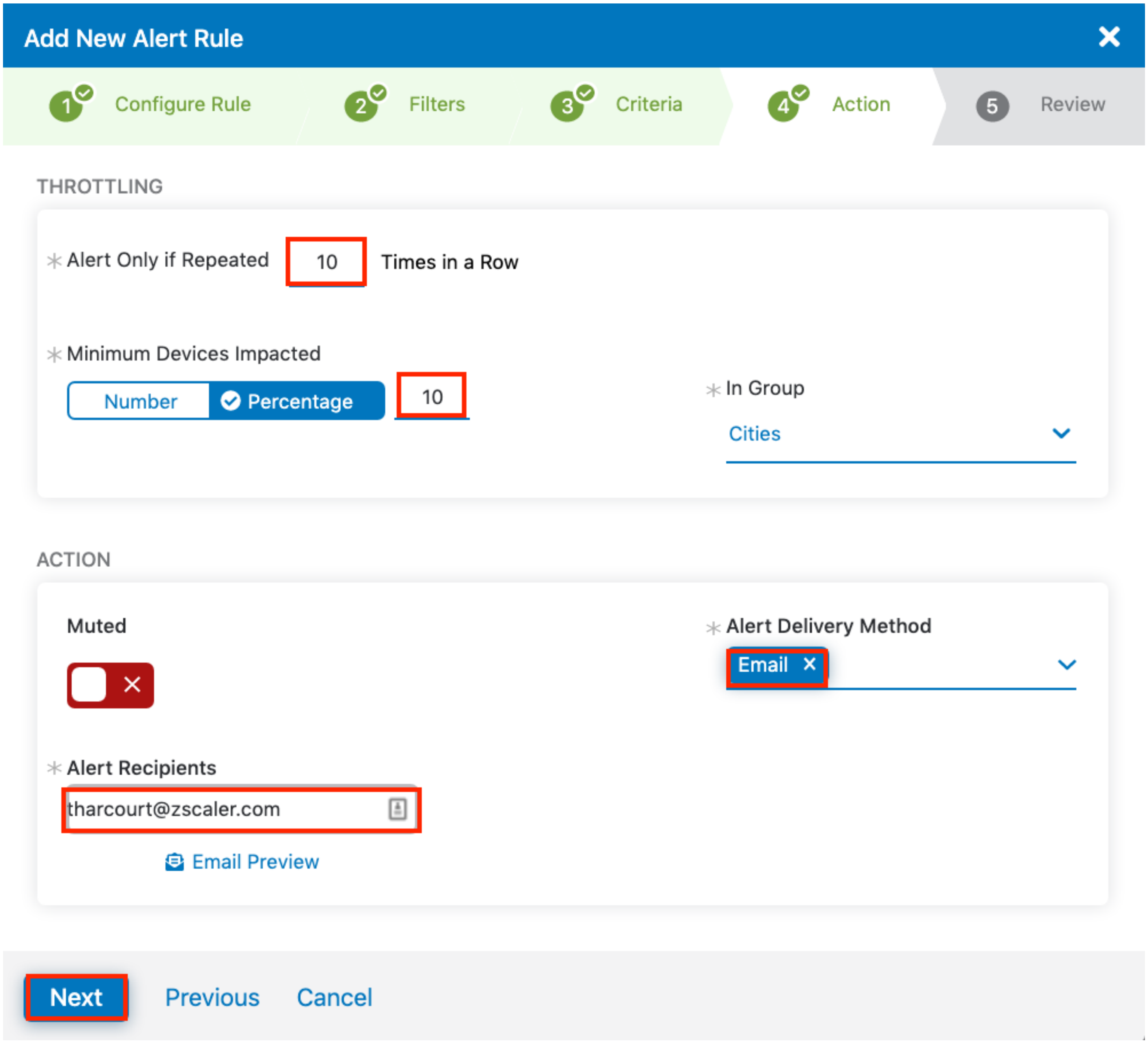
Add New Alert Rule

Page Fetch Time >= 5000 ms

*Figure 48. Create the criteria for the alert*

Add throttling to control the scope of the alert, then define the Action as Email. You can also define the action as an authenticated Webhook, which is used to send the alert to a Slack channel:

1. Enter `10` for the number of times the probe time must exceed the threshold.
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.
5. Click **Next**.


Add New Alert Rule

THROTTLING

* Alert Only if Repeated: 10 Times in a Row

* Minimum Devices Impacted: Percentage 10

* In Group: Cities

ACTION

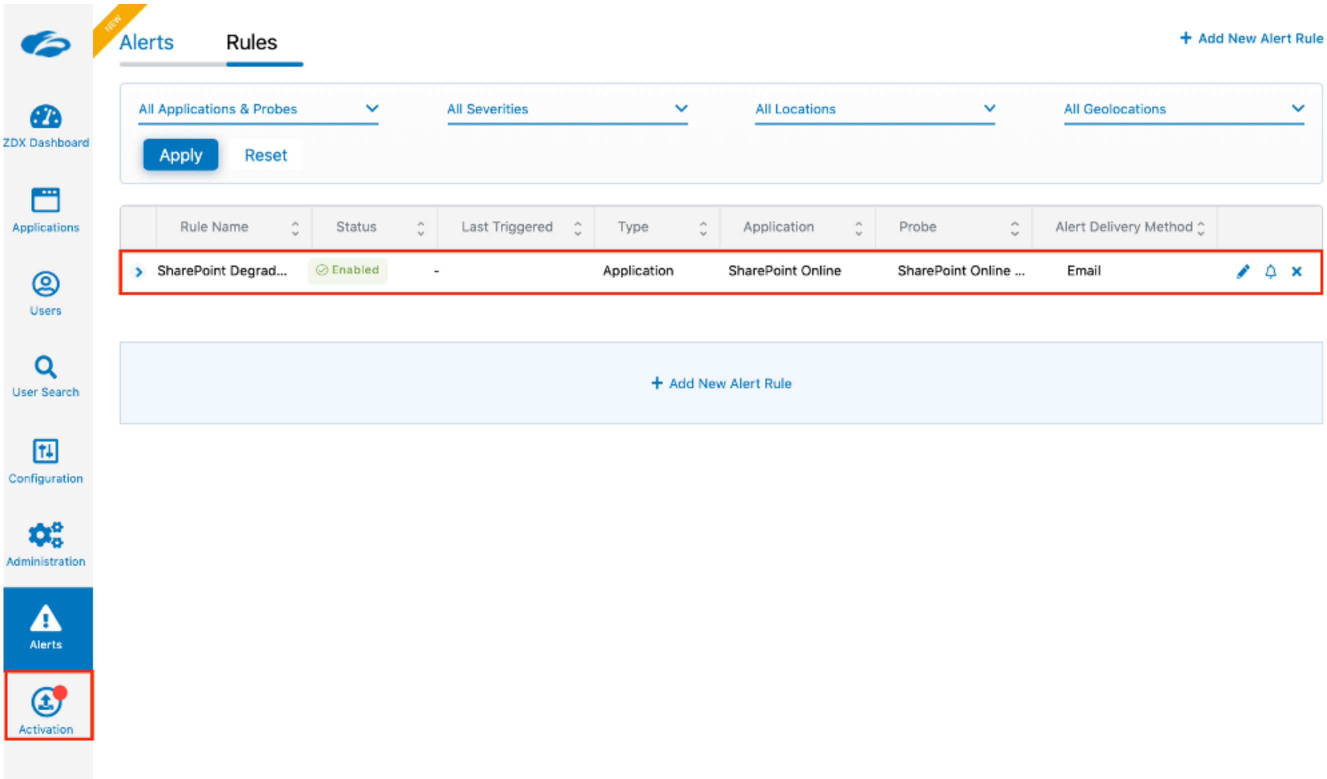
Muted: ☒

* Alert Delivery Method: Email

* Alert Recipients: tharcourt@zscaler.com

*Figure 49. Add throttling and define the action for the alert*

The following is the completed rule set for the alert.



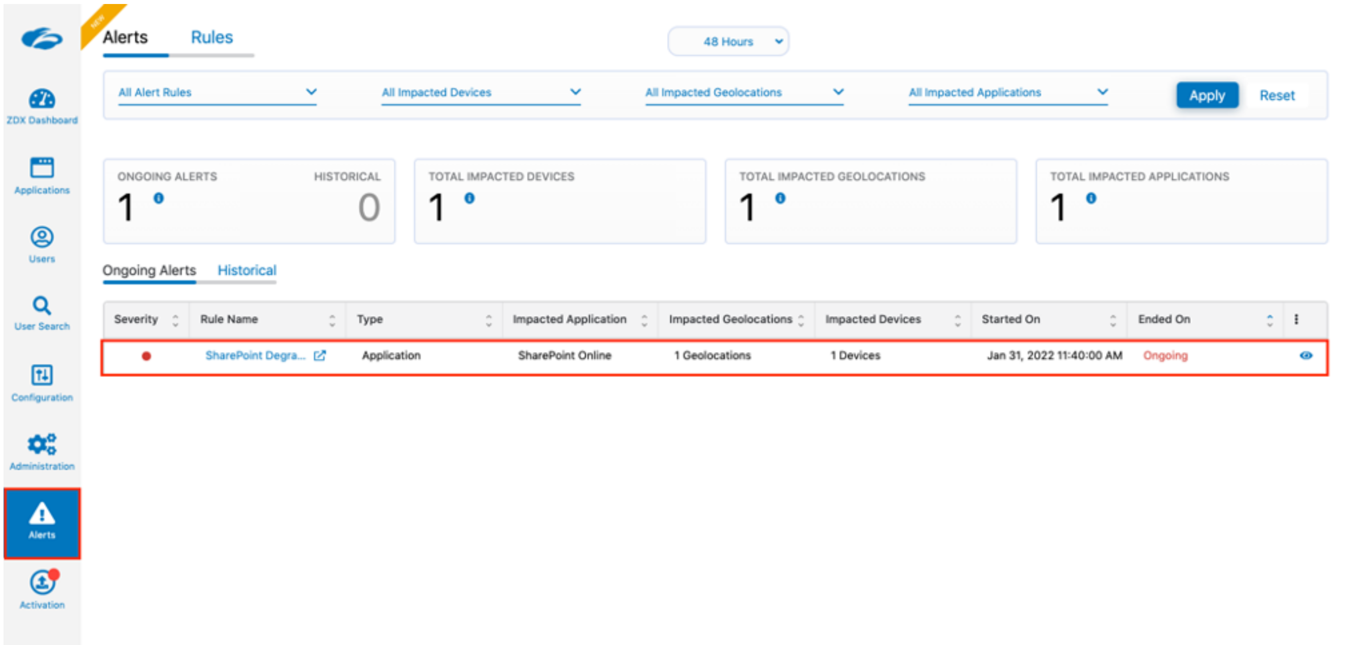
All Applications & Probes | All Severities | All Locations | All Geolocations

| | Rule Name | Status | Last Triggered | Type | Application | Probe | Alert Delivery Method | |
|---|---|---|---|---|---|---|---|---|
| › | SharePoint Degrad... | Enabled | - | Application | SharePoint Online | SharePoint Online ... | Email | |

*Figure 50. The completed rule set*

## The Triggered Alert for the SharePoint Service

You can see the triggered alert generated because the threshold settings are exceeded. You can click Rule Name or click the View icon to see more detail about the alert.



ONGOING ALERTS 1 HISTORICAL 0

TOTAL IMPACTED DEVICES 1

TOTAL IMPACTED GEOLOCATIONS 1

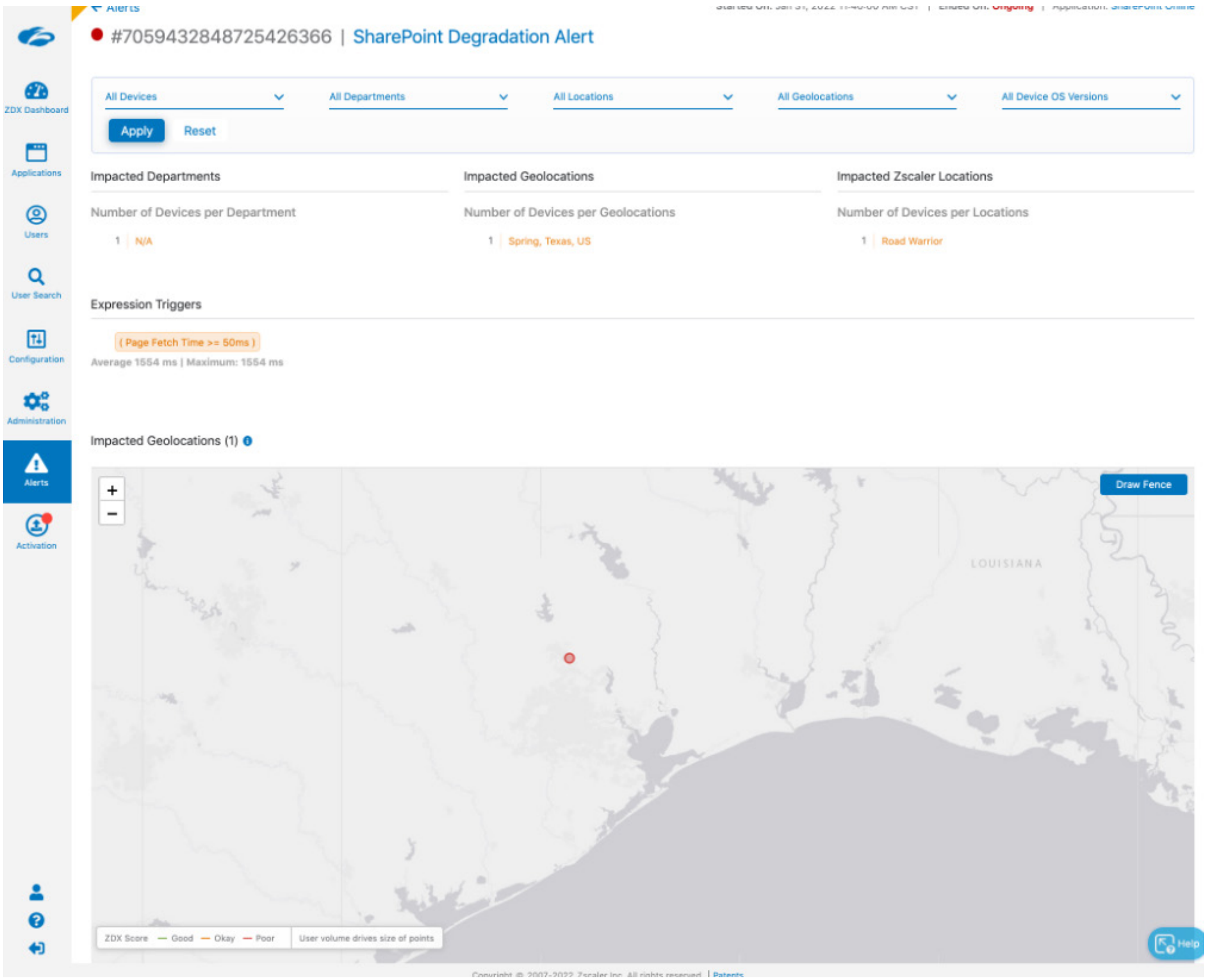
TOTAL IMPACTED APPLICATIONS 1

| Severity | Rule Name | Type | Impacted Application | Impacted Geolocations | Impacted Devices | Started On | Ended On |
|---|---|---|---|---|---|---|---|
| ● | SharePoint Degra... | Application | SharePoint Online | 1 Geolocations | 1 Devices | Jan 31, 2022 11:40:00 AM | Ongoing |

*Figure 51. The triggered alert*

### Alert Detail for the SharePoint Service

You can see the triggered alert details showing impacted user and devices, impact location, and threshold details.



Started On: Jan 31, 2022 11:40:00 AM CST | Ended On: Ongoing | Application: SharePoint Online

● #7059432848725426366 | SharePoint Degradation Alert

Impacted Departments

Number of Devices per Department

1 | N/A

Impacted Geolocations

Number of Devices per Geolocations

1 | Spring, Texas, US

Impacted Zscaler Locations

Number of Devices per Locations

1 | Road Warrior

Expression Triggers

( Page Fetch Time >= 50ms )

Average 1554 ms | Maximum: 1554 ms

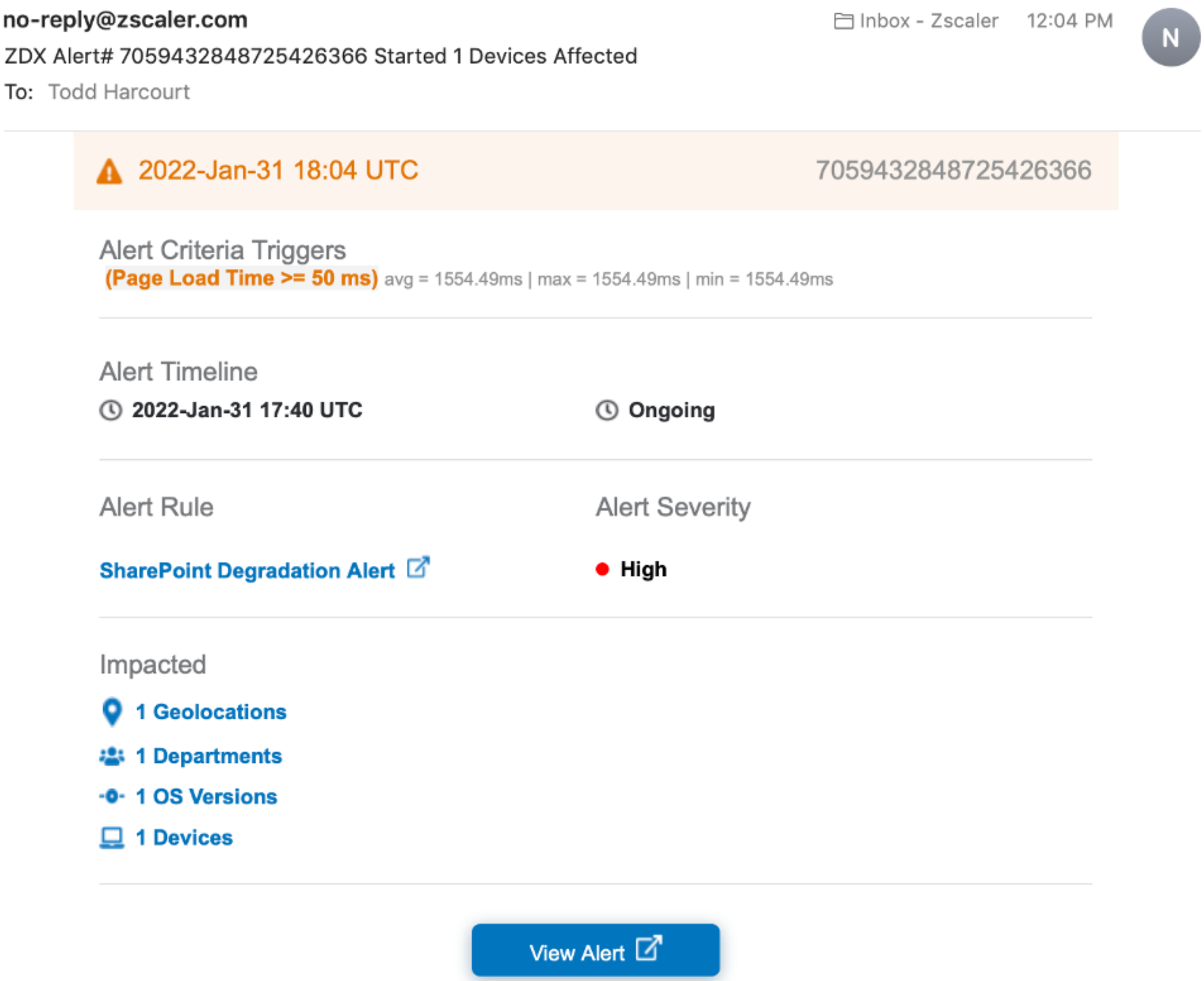
Impacted Geolocations (1)

ZDX Score — Good — Okay — Poor | User volume drives size of points

*Figure 52. Alert details*

## The Sent Alert Email for the SharePoint Service

You can see the email alert sent to the recipients after the threshold is 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# 7059432848725426366 Started 1 Devices Affected

To: Todd Harcourt

Inbox - Zscaler 12:04 PM

2022-Jan-31 18:04 UTC 7059432848725426366

Alert Criteria Triggers

**(Page Load Time >= 50 ms)** avg = 1554.49ms | max = 1554.49ms | min = 1554.49ms

Alert Timeline

**2022-Jan-31 17:40 UTC** **Ongoing**

Alert Rule: **SharePoint Degradation Alert**

Alert Severity: ● **High**

Impacted

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

*Figure 53. The alert email*

## Using ZDX: The Dashboard

The dashboard provides a single page for monitoring the user experience (ZDX Score) of all users and all applications. An active heat map shows you any locations globally that might be having issues.

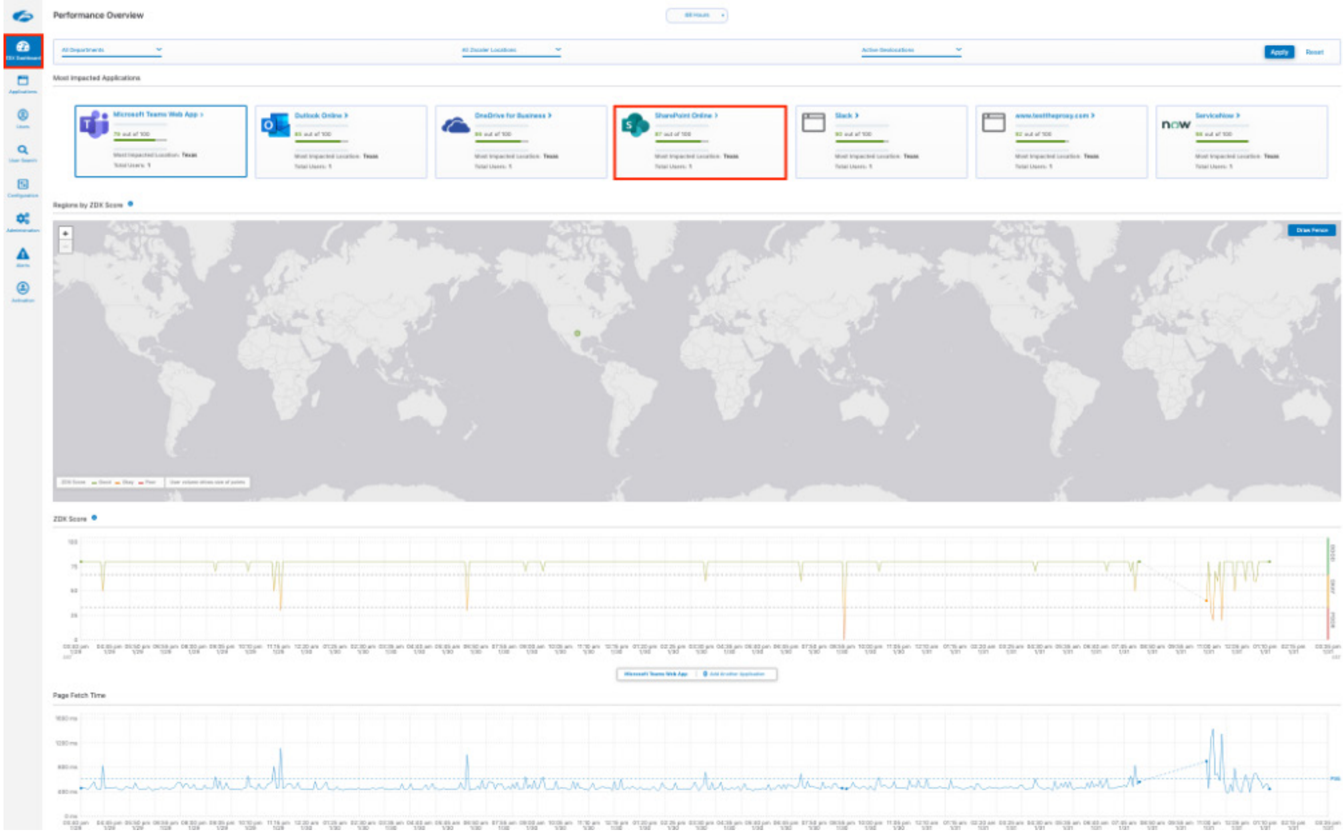


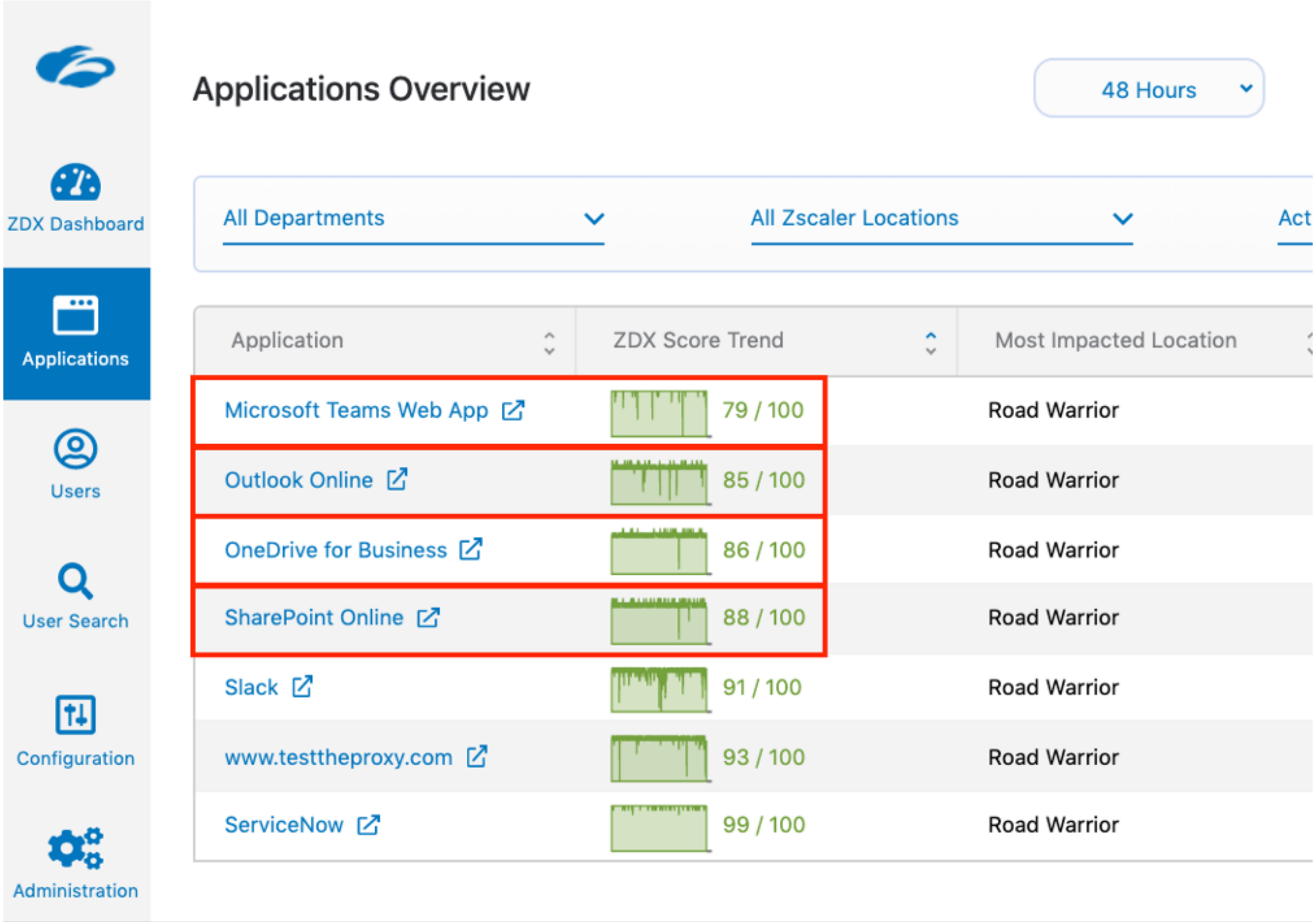
*Figure 54. The dashboard*

### Application Overview

Selecting Applications on the left-hand navigation pane of the ZDX Admin Portal displays the Applications Overview, which and shows all the configured applications and the individual ZDX score.

To see the details of the SharePoint application:

1. Select **Applications**.
2. Select **SharePoint Online**.



| Application | ZDX Score Trend | Most Impacted Location |
|---|---|---|
| Microsoft Teams Web App | 79 / 100 | Road Warrior |
| Outlook Online | 85 / 100 | Road Warrior |
| OneDrive for Business | 86 / 100 | Road Warrior |
| SharePoint Online | 88 / 100 | Road Warrior |
| Slack | 91 / 100 | Road Warrior |
| www.testtheproxy.com | 93 / 100 | Road Warrior |
| ServiceNow | 99 / 100 | Road Warrior |

*Figure 55. Application overview*

## SharePoint Application Performance 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 SharePoint service itself.

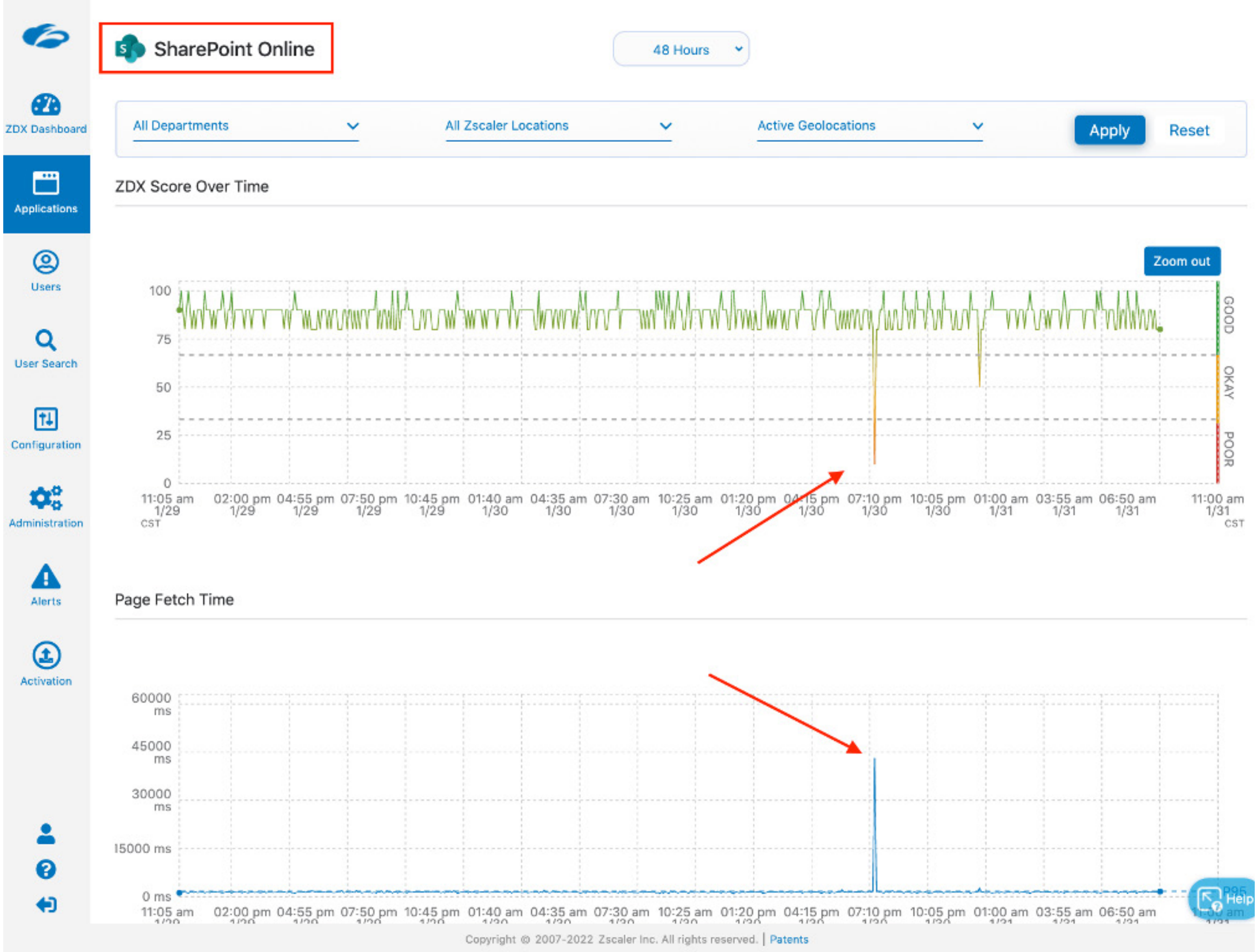
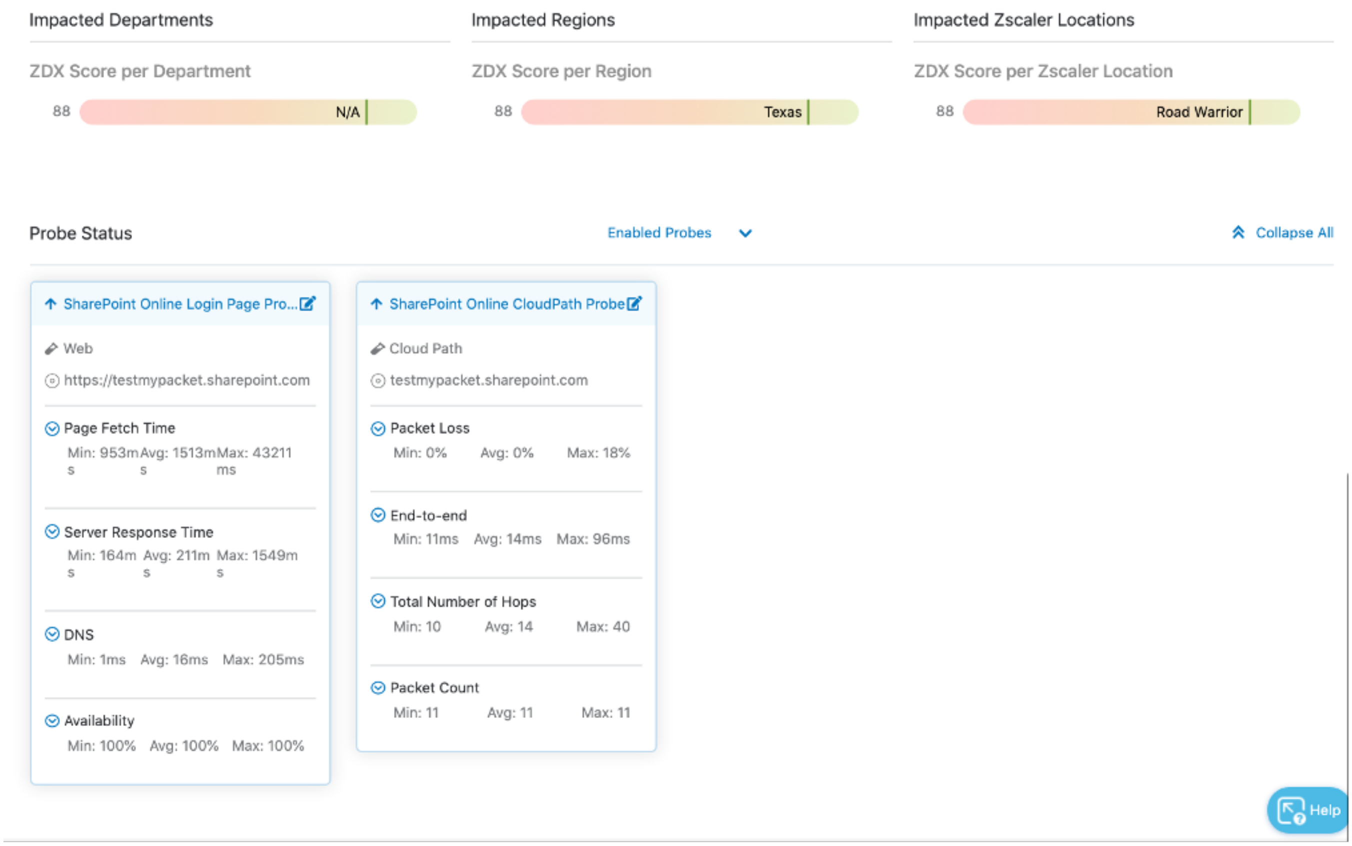


*Figure 56. Application detail*

The bottom portion of the screen shows the top Zscaler locations, top cities, and the top departments using the application and the ZDX scores. You also see the probe data, with minimum, maximum, and average response times.



Impacted Departments

ZDX Score per Department

88 N/A

Impacted Regions

ZDX Score per Region

88 Texas

Impacted Zscaler Locations

ZDX Score per Zscaler Location

88 Road Warrior

Probe Status

Enabled Probes

Collapse All

SharePoint Online Login Page Pro...

Web

https://testmypacket.sharepoint.com

Page Fetch Time

Min: 953ms Avg: 1513ms Max: 43211 ms

Server Response Time

Min: 164ms Avg: 211ms Max: 1549ms

DNS

Min: 1ms Avg: 16ms Max: 205ms

Availability

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

SharePoint Online CloudPath Probe

Cloud Path

testmypacket.sharepoint.com

Packet Loss

Min: 0% Avg: 0% Max: 18%

End-to-end

Min: 11ms Avg: 14ms Max: 96ms

Total Number of Hops

Min: 10 Avg: 14 Max: 40

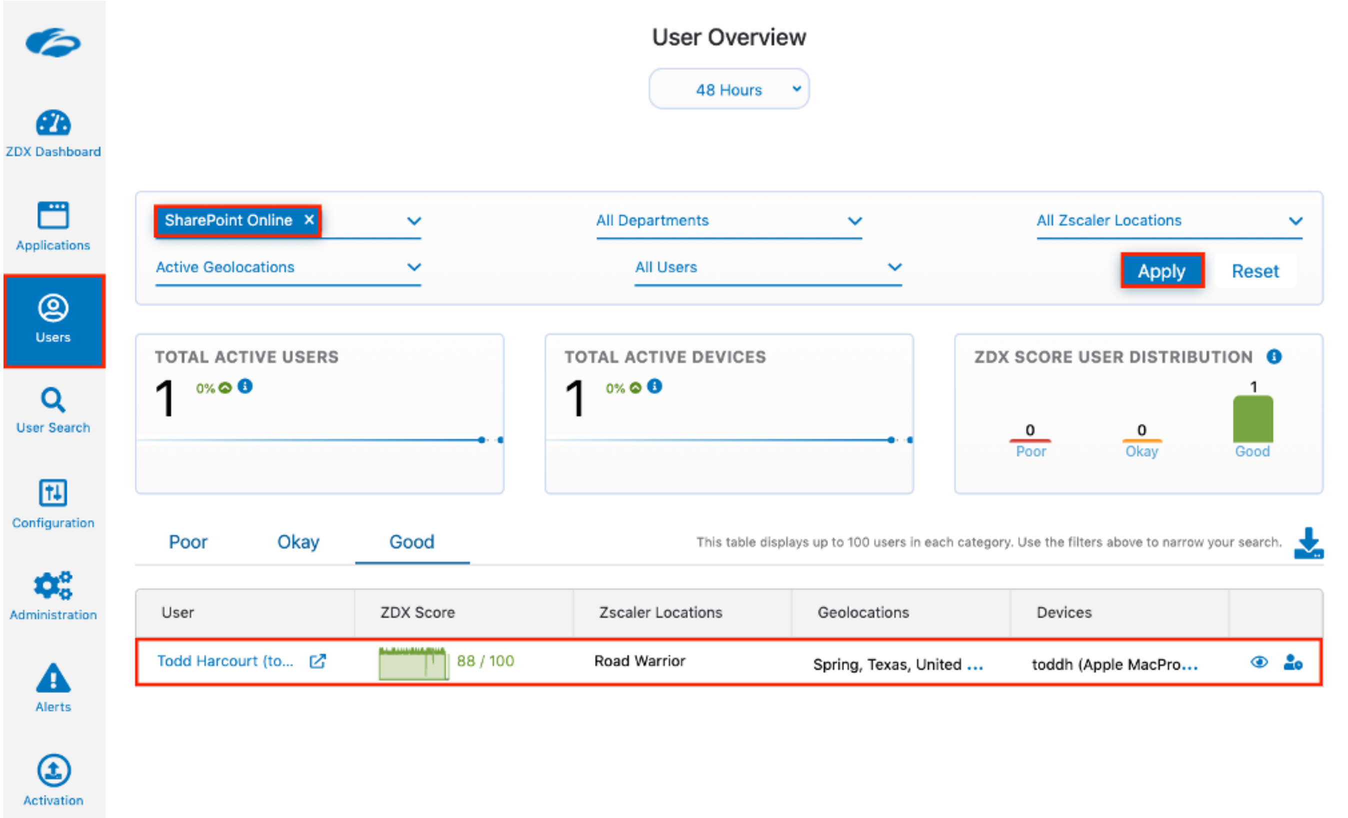
Packet Count

Min: 11 Avg: 11 Max: 11

*Figure 57. Application detail*

## User Overview

The User Overview shows all the users of an application. Select SharePoint Online and then click Apply to see all SharePoint users. The ZDX score is provided, and users are selected by a Poor, Okay, or a Good ZDX score. You can get more detail on the user by clicking the name or the View icon on the right.



User Overview

48 Hours

SharePoint Online ×

All Departments

All Zscaler Locations

Active Geolocations

All Users

TOTAL ACTIVE USERS 1 0%

TOTAL ACTIVE DEVICES 1 0%

ZDX SCORE USER DISTRIBUTION

| Poor | Okay | Good |
|---|---|---|
| 0 | 0 | 1 |

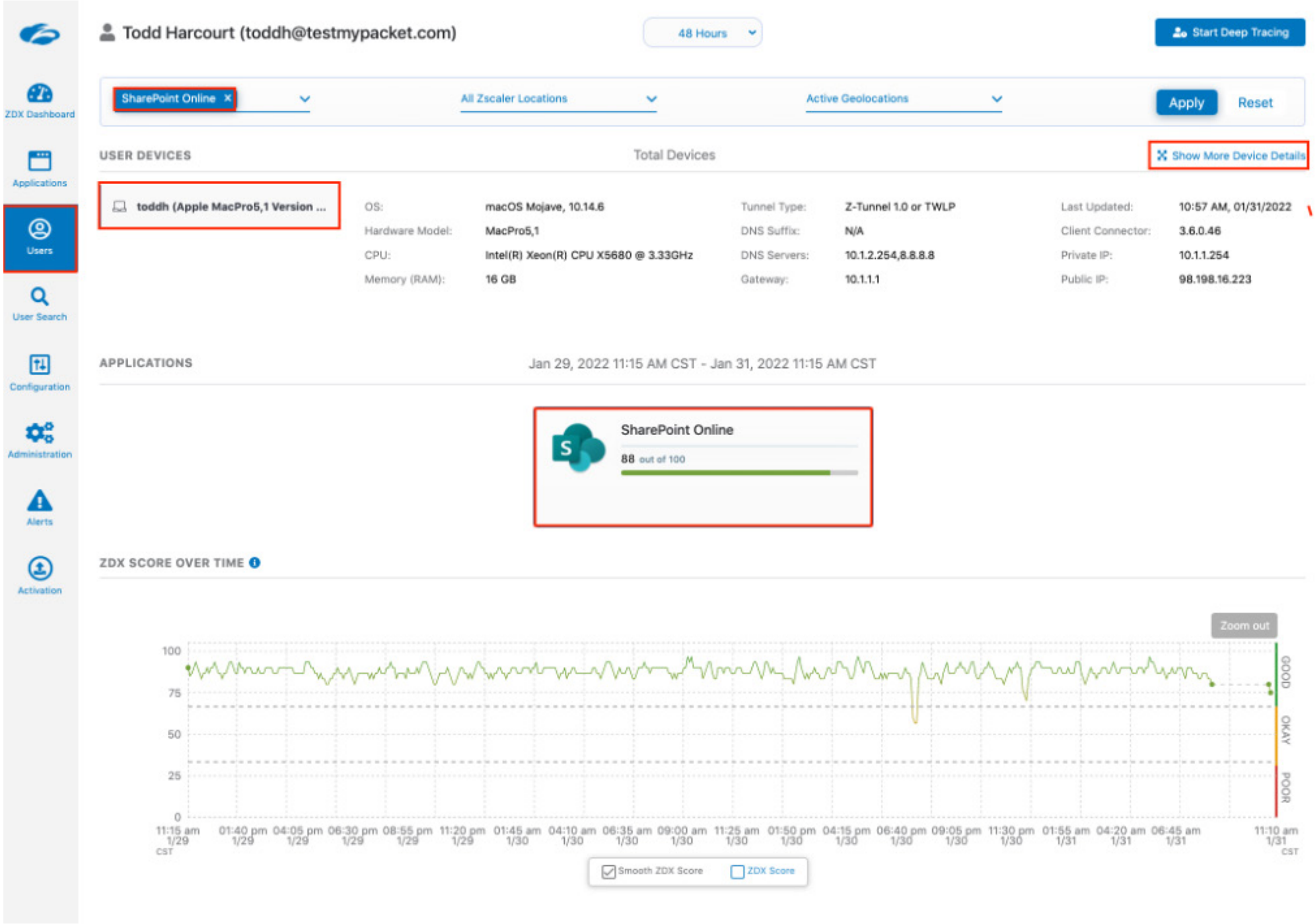
This table displays up to 100 users in each category. Use the filters above to narrow your search.

| User | ZDX Score | Zscaler Locations | Geolocations | Devices |
|---|---|---|---|---|
| Todd Harcourt (to... | 88 / 100 | Road Warrior | Spring, Texas, United ... | toddh (Apple MacPro... |

*Figure 58. User overview*

### SharePoint User Detail

The User Detail shows data to help isolate any user experience issues. Select and apply the SharePoint application to see the detail of the user experience for the SharePoint app. Clicking a device on this report provides the users devices and the device-specific detail (OS, device type, network Information, etc.). It displays the ZDX score in a timeline, and detail of page fetch times, server response, DNS response, probe detail, and device health as well.



Todd Harcourt (toddh@testmypacket.com)

USER DEVICES

toddh (Apple MacPro5,1 Version ...

| | | | | | |
|---|---|---|---|---|---|
| OS: | macOS Mojave, 10.14.6 | Tunnel Type: | Z-Tunnel 1.0 or TWLP | Last Updated: | 10:57 AM, 01/31/2022 |
| Hardware Model: | MacPro5,1 | DNS Suffix: | N/A | Client Connector: | 3.6.0.46 |
| CPU: | Intel(R) Xeon(R) CPU X5680 @ 3.33GHz | DNS Servers: | 10.1.2.254,8.8.8.8 | Private IP: | 10.1.1.254 |
| Memory (RAM): | 16 GB | Gateway: | 10.1.1.1 | Public IP: | 98.198.16.223 |

APPLICATIONS

Jan 29, 2022 11:15 AM CST - Jan 31, 2022 11:15 AM CST

SharePoint Online

88 out of 100

*Figure 59. User detail*

# Appendix A: Requesting Zscaler Support

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

## Gather Support Information

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

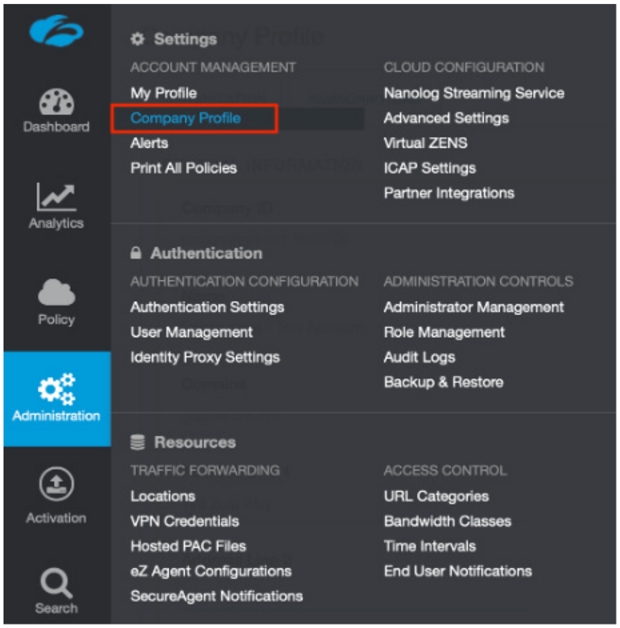
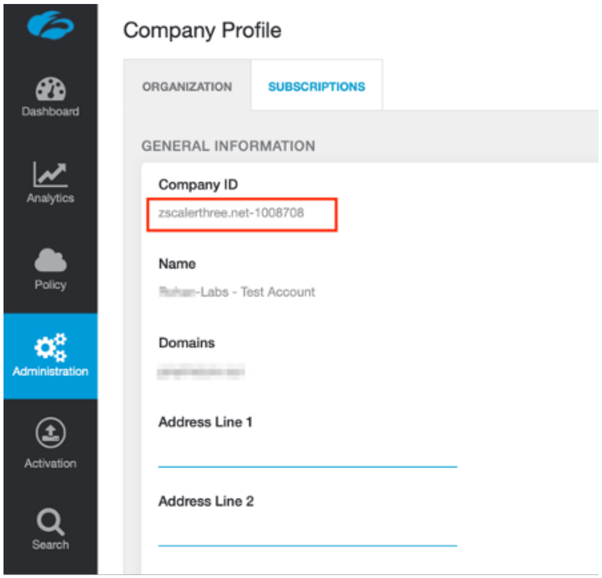


*Figure 60. Collecting details to open support case with Zscaler TAC*

### Save Company ID

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 61. Company ID*

### Enter Support Section

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

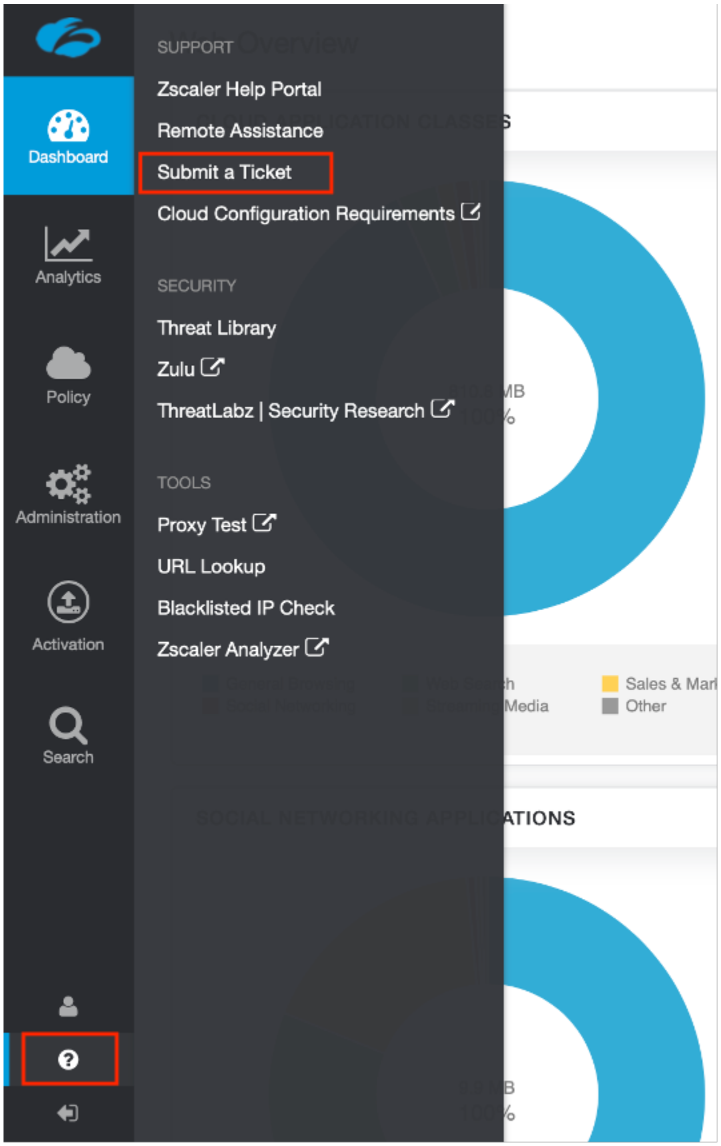


*Figure 62. Submit a Ticket*