



ZSCALER AND MICROSOFT SHAREPOINT ONLINE DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	5
Zscaler Overview	5
Microsoft Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and Microsoft SharePoint Introduction	6
ZIA Overview	6
ZPA Overview	6
Zscaler Resources	7
SharePoint Overview	8
SharePoint Resources	8
Zscaler Data Protection and Digital Experience for SharePoint.com	9
Overview	10
ZIA SaaS Security API Data and Malware Protection for SharePoint	10
ZIA Cloud Application Control	12
ZDX SharePoint User Experience	13
Configuring SharePoint SaaS Security	14
Adding the SharePoint Tenant	15
SaaS Tenant Configuration Wizard	16
Configuring the Zscaler Tenant on SharePoint	17

Finishing the Zscaler Tenant on Zscaler	18
The Completed and Active SharePoint API Connector	19
Configuring SharePoint SaaS Data Loss Prevention	20
Creating a DLP Policy	20
Creating a DLP Engine	21
Configure a SaaS DLP Policy	23
SaaS DLP Policy Details	24
SaaS DLP Policy Wizard	25
Configuring SharePoint SaaS Malware Detection	27
Configuring SharePoint Security Scan for DLP and Malware	29
The Scan Schedule Configuration	29
SaaS Security Reporting and Visibility	32
SaaS Assets and SaaS Assets Summary Report	33
SaaS Security Insights	34
Configuring SSL Inspection for SharePoint	35
Configuring SSL Inspection for SharePoint	36
Configuring an SSL Inspection Rule	37
Verify SSL Inspection	39
ZIA Cloud Application Control	40
ZIA Cloud Application Control Policy	41
ZIA Cloud Application Control	42
ZDX for SharePoint	45
Configure ZDX for SharePoint	46
Configure ZDX for SharePoint	47

Configure Probes for SharePoint Monitoring	48
The ZDX-Enabled SharePoint Application	49
Create an Alert for the SharePoint Service	50
The Triggered Alert for the SharePoint Service	56
Alert Detail for the SharePoint Service	57
The Sent Alert Email for the SharePoint Service	58
Using ZDX: The Dashboard	59
Application Overview	60
SharePoint Application Performance Detail	61
User Overview	63
SharePoint User Detail	64
Appendix A: Requesting Zscaler Support	65

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. To learn more, 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). To learn more, refer to [Microsoft'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 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:** 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 Microsoft SharePoint Introduction

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



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

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 isolation, allowing you to 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 a 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.
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.

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.

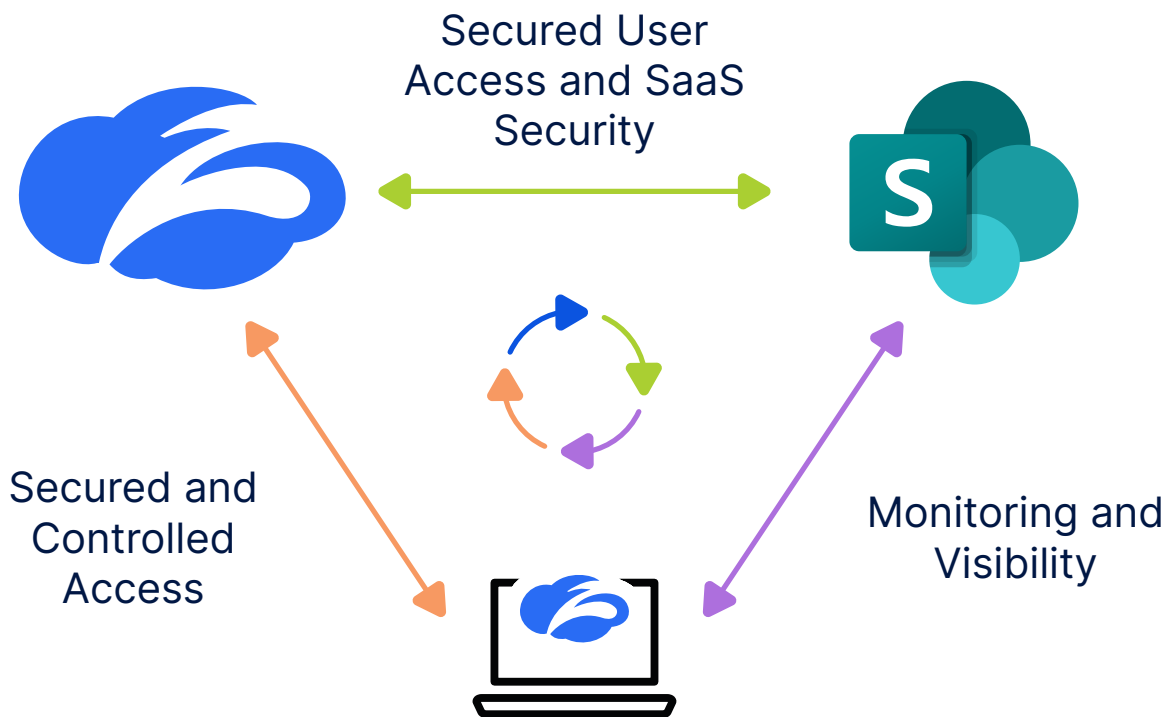


Figure 1. Zscaler solutions for SharePoint

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.

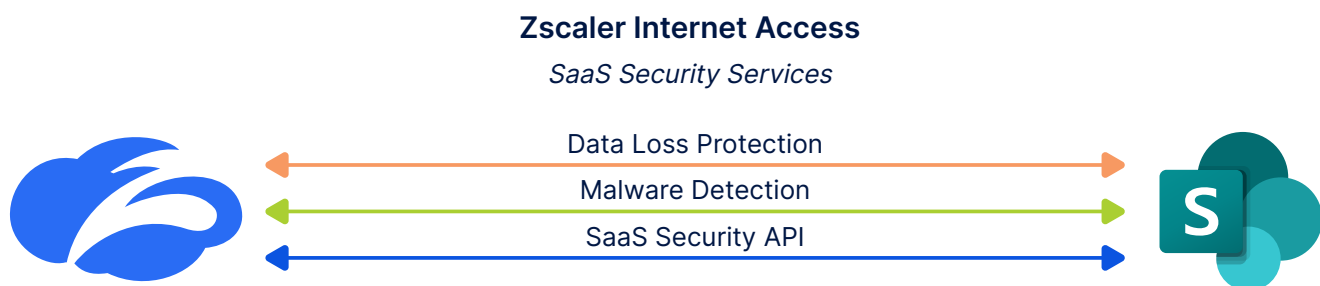


Figure 2. Zscaler SaaS Security API in use with SharePoint

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.

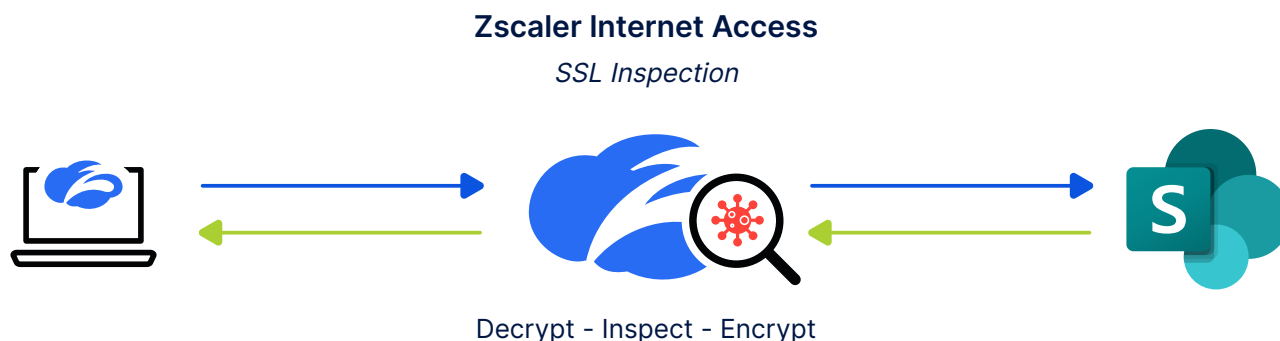


Figure 3. SSL decryption

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.

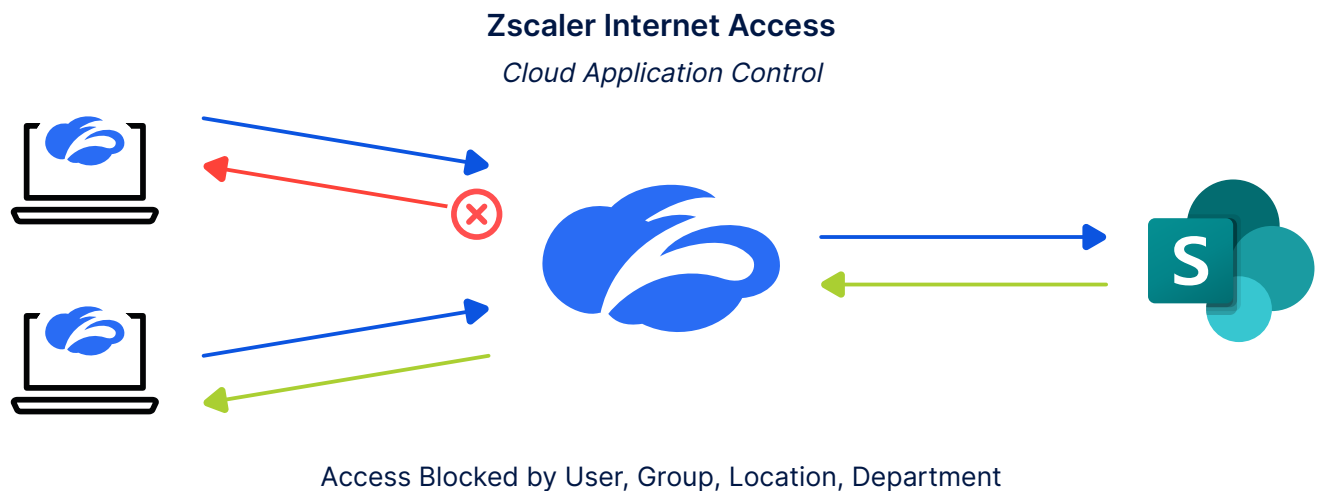


Figure 4. Cloud app control

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.

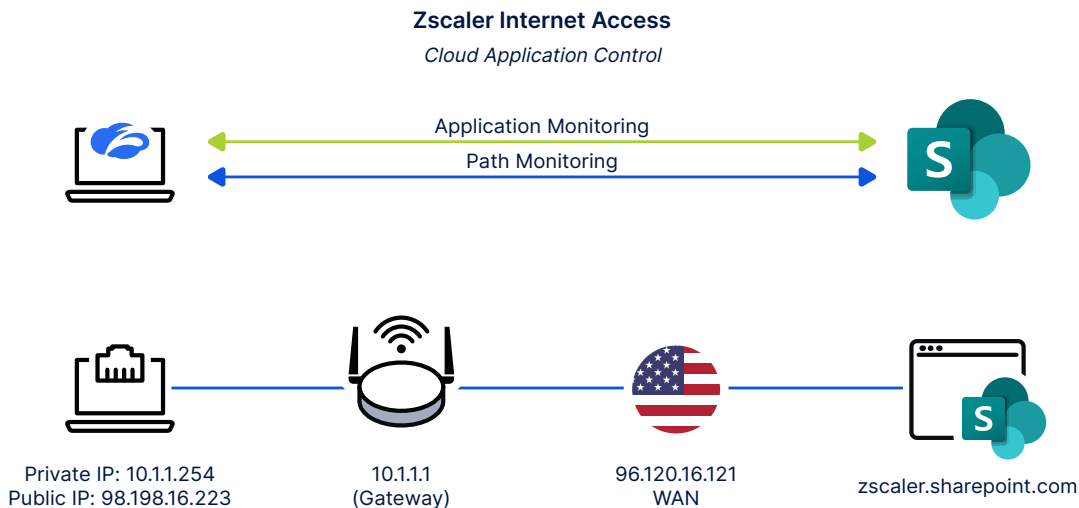


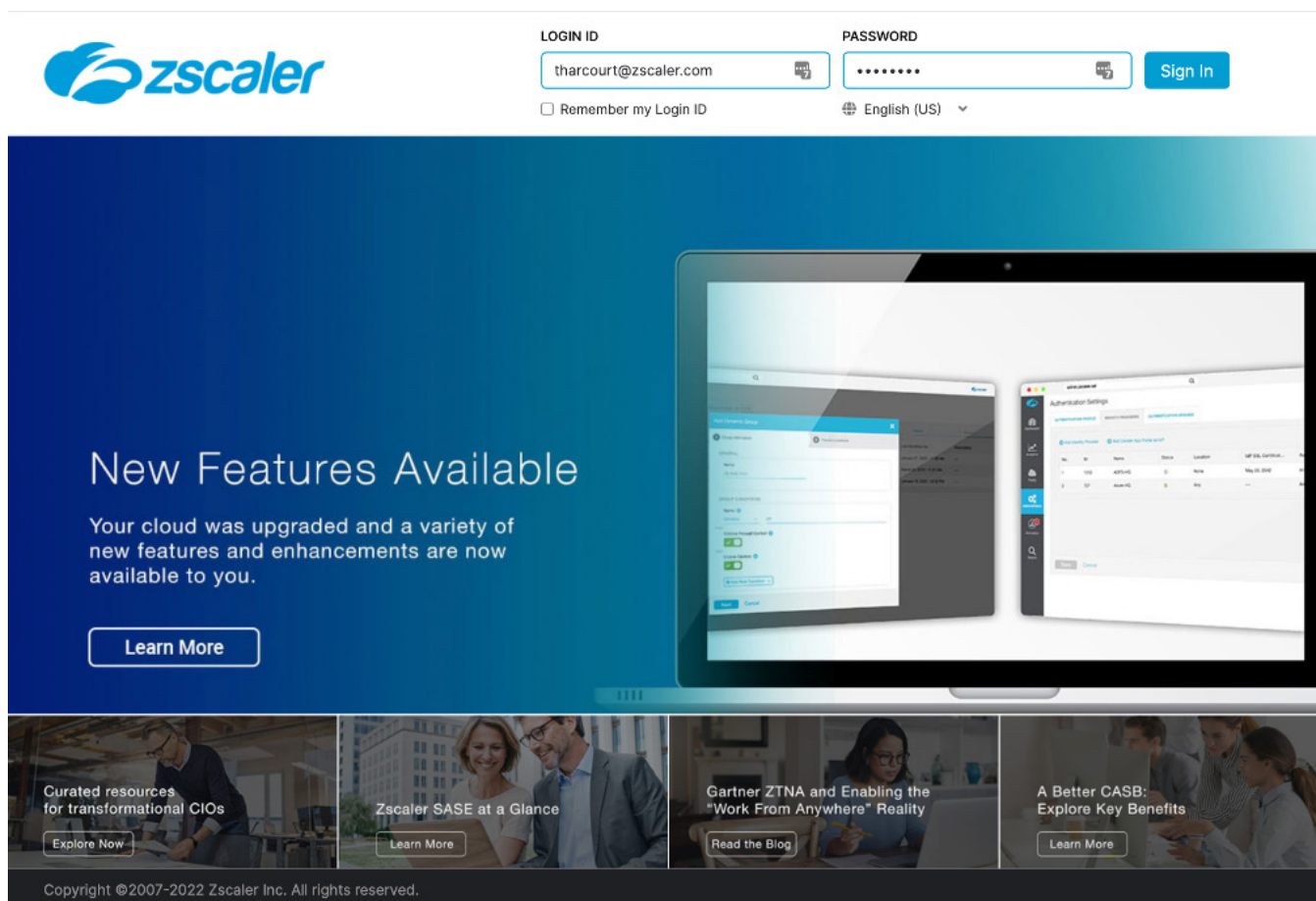
Figure 5. ZDX for user experience monitoring for SharePoint

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.



The image shows the Zscaler ZIA Admin Portal login page. At the top left is the Zscaler logo. To its right are two input fields: 'LOGIN ID' with the email 'tharcourt@zscaler.com' and 'PASSWORD' with masked characters. Below the login ID field is a checkbox for 'Remember my Login ID'. To the right of the password field is a language dropdown menu set to 'English (US)' and a blue 'Sign In' button. Below the login section is a large blue banner with the text 'New Features Available' and a sub-message: 'Your cloud was upgraded and a variety of new features and enhancements are now available to you.' A 'Learn More' button is positioned below this text. To the right of the text is a tablet displaying two screenshots of the ZIA Admin Portal interface. At the bottom of the page is a horizontal row of four promotional tiles, each with a background image and a title: 'Curated resources for transformational CIOs' (with an 'Explore Now' button), 'Zscaler SASE at a Glance' (with a 'Learn More' button), 'Gartner ZTNA and Enabling the "Work From Anywhere" Reality' (with a 'Read the Blog' button), and 'A Better CASB: Explore Key Benefits' (with a 'Learn More' button). The footer contains the copyright notice: 'Copyright ©2007-2022 Zscaler Inc. All rights reserved.'

LOGIN ID
tharcourt@zscaler.com

PASSWORD

☐ Remember my Login ID

English (US)

Sign In

New Features Available

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

Learn More

Curated resources for transformational CIOs
Explore Now

Zscaler SASE at a Glance
Learn More

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

A Better CASB: Explore Key Benefits
Learn More

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

Figure 6. ZIA Admin Portal login

Adding the SharePoint Tenant

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

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

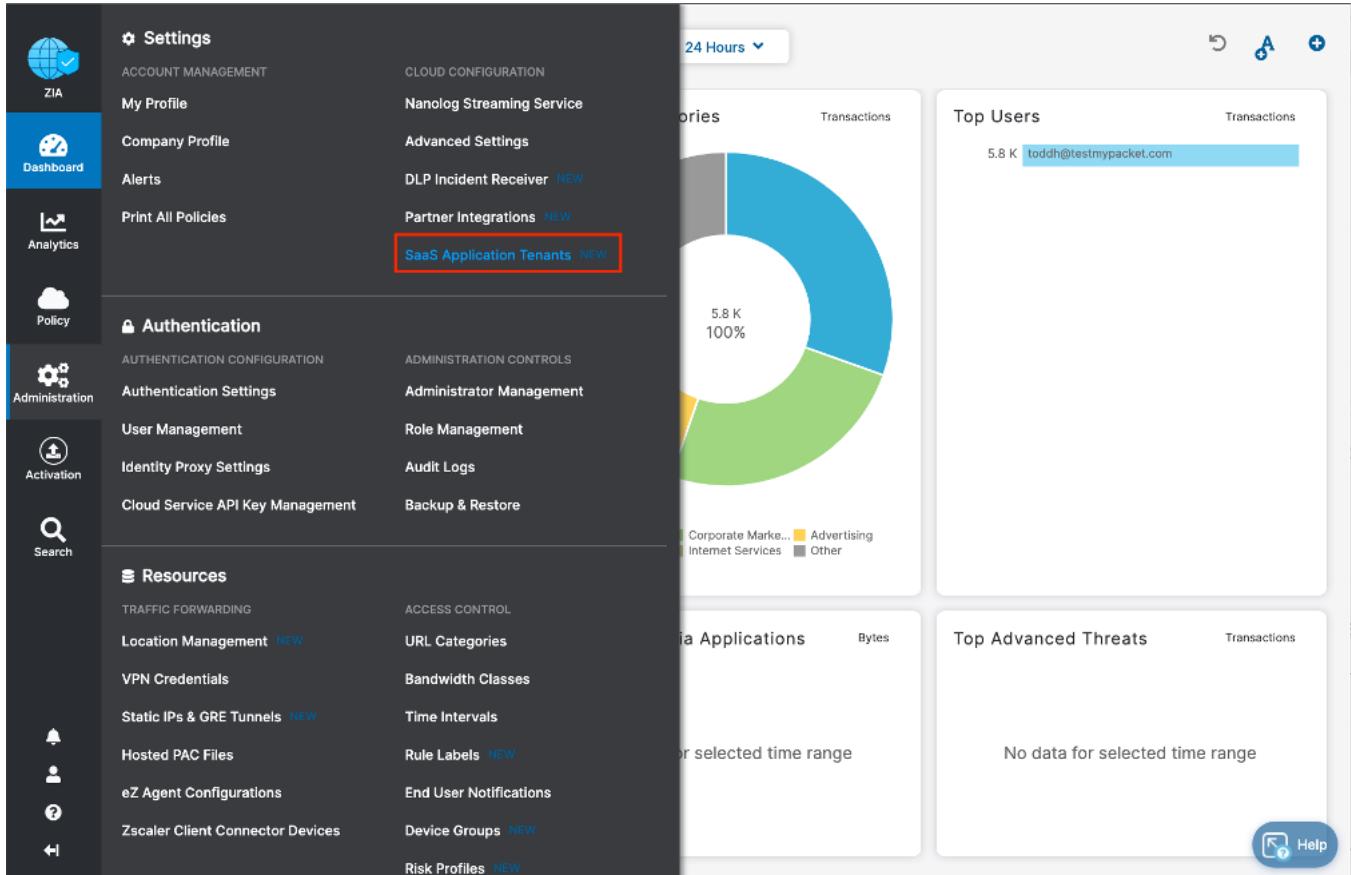


Figure 7. SaaS Application Tenant

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.

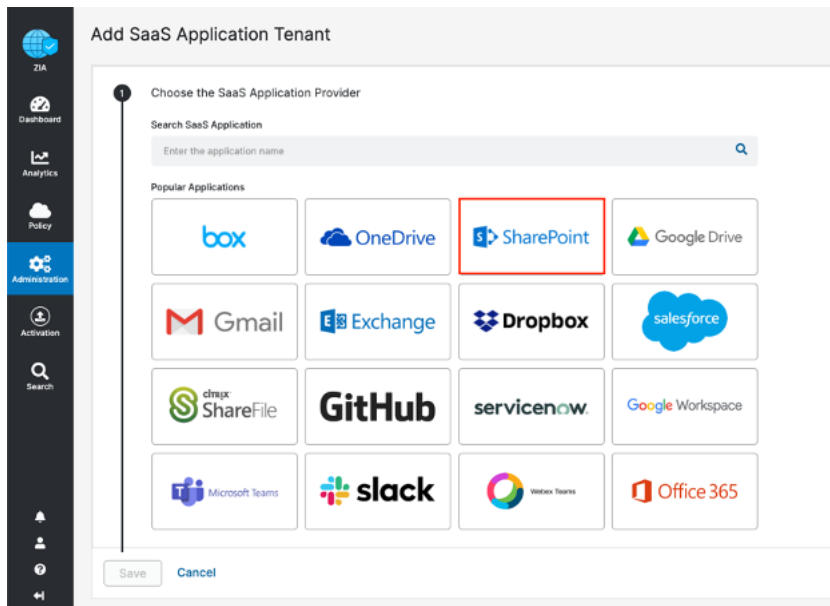


Figure 8. The SaaS tenant configuration wizard

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**.

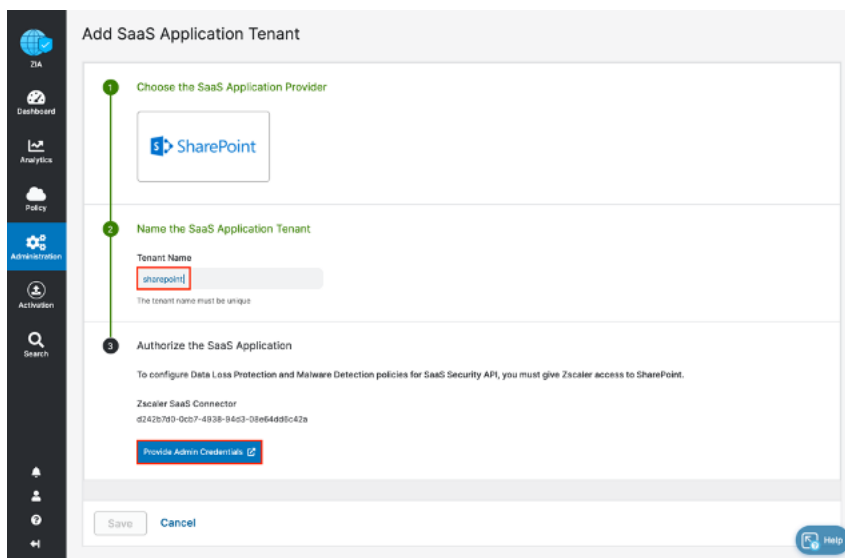


Figure 9. Open the SharePoint tenant

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.

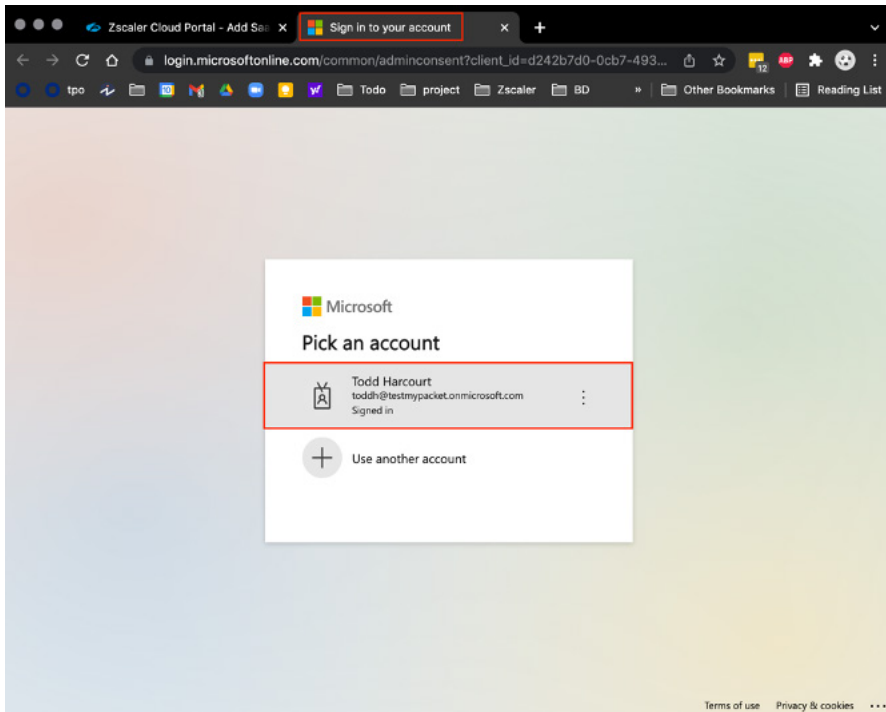


Figure 10. Log in to the SharePoint tenant

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

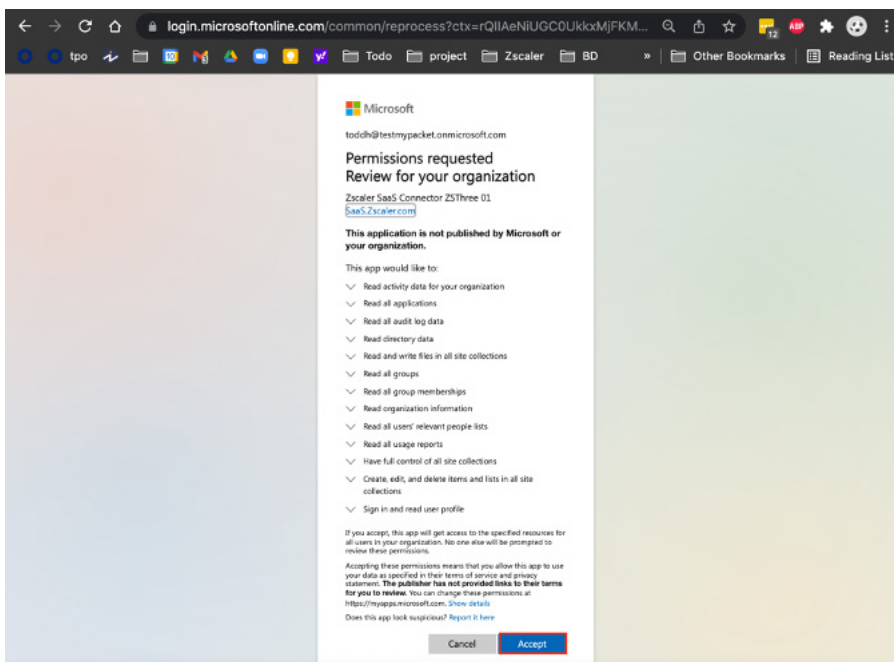


Figure 11. Accept SharePoint permissions

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: c242b7d0-0cb7-4938-94d3-08e64dd6c42a
Tenant ID: 045989c5-04a4-431b-8c19-e3e9371823ad

Provide Admin Credentials

Save Cancel

Help

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

Search...

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

Help

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](#)

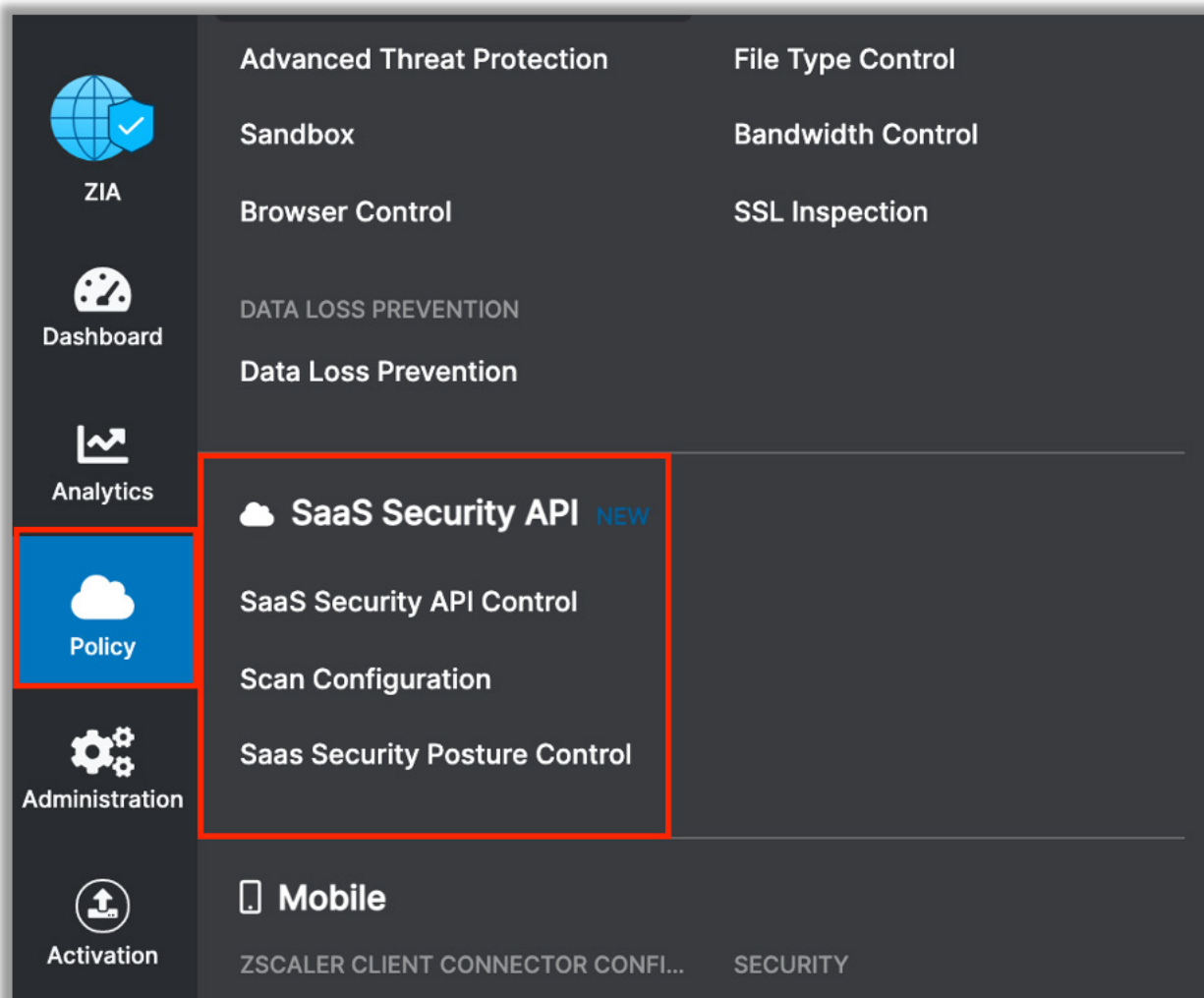


Figure 14. Zscaler policy configuration

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.

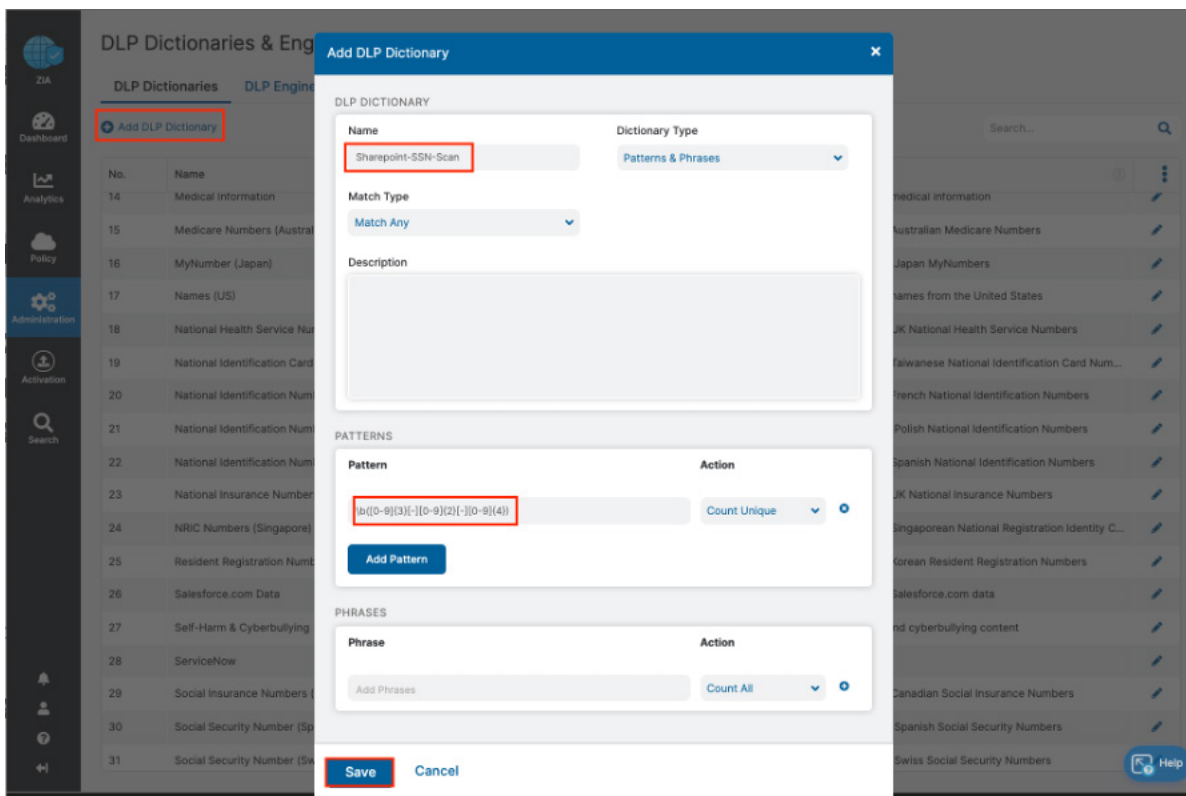


Figure 15. Creating a DLP dictionary

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**.

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.

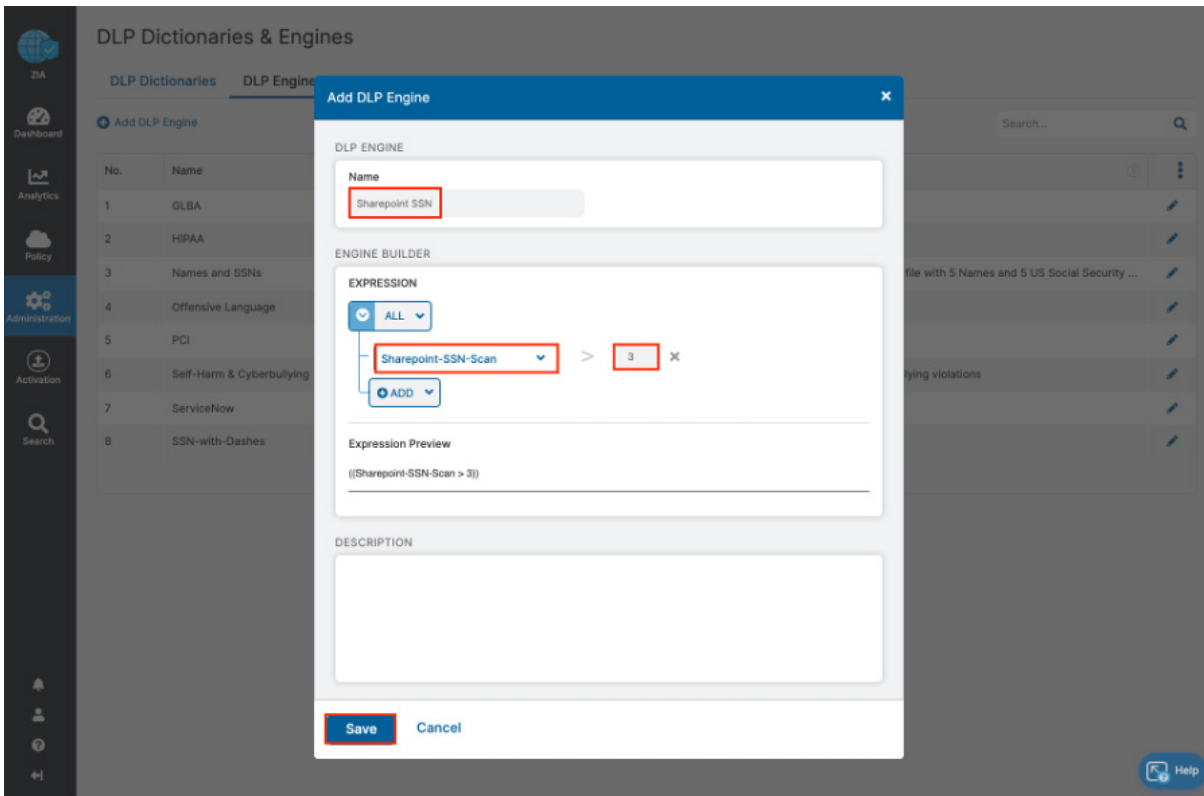


Figure 17. The DLP engine wizard



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**.

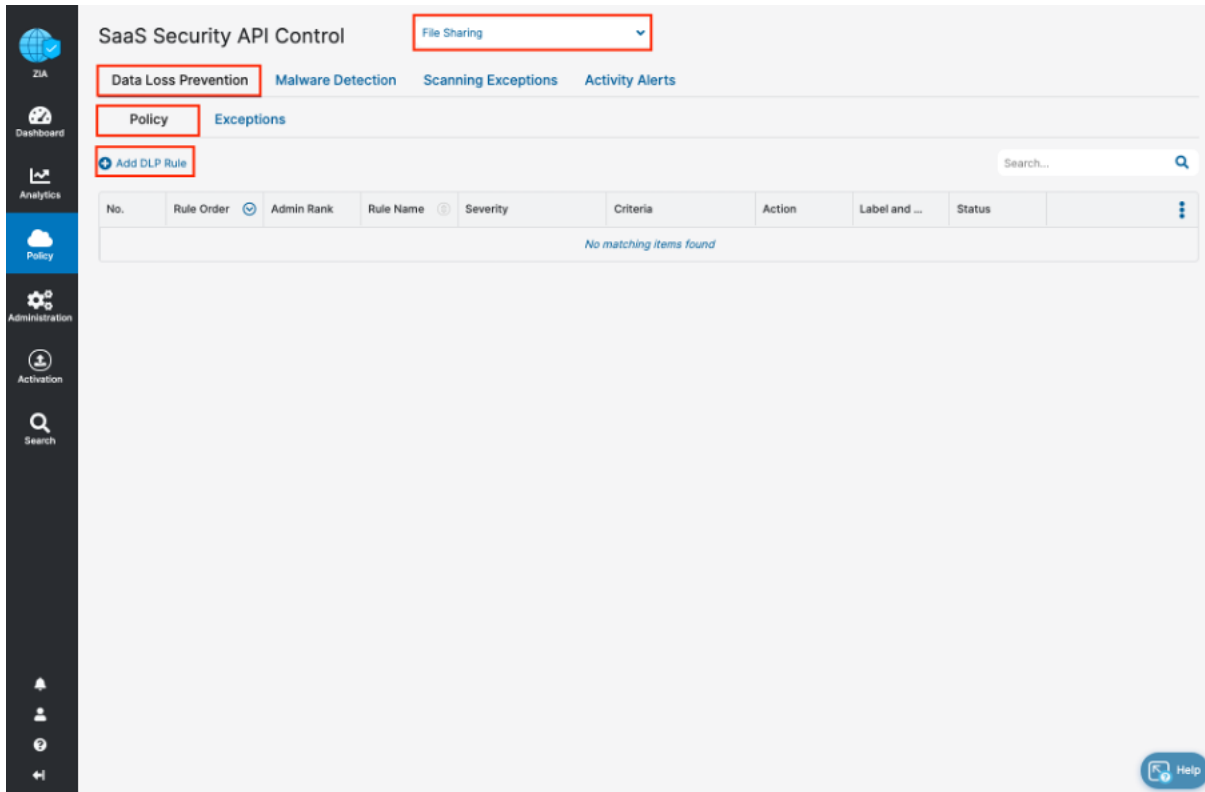


Figure 18. Launch the SaaS DLP policy configuration wizard

This launches the **DLP Policy Wizard**.

SaaS DLP Policy Details

The SaaS DLP policy is like all Zscaler policies 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**.

SaaS Security API Control

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: N/A

ACTION

Action: Remove Sharing | Severity: Medium

NOTIFICATION

Auditor Type: Internal | External

Auditor: auditor@zscaler.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.

The screenshot displays the Zscaler SaaS Security API Control interface. The left sidebar contains navigation icons for ZIA, Dashboard, Analytics, Policy, Administration, and Activation (highlighted with a red box and a red circle with the number 1). The main content area is titled "SaaS Security API Control" and features a dropdown menu set to "File Sharing". Below this, there are tabs for "Data Loss Prevention", "Malware Detection", "Scanning Exceptions", and "Activity Alerts". The "Data Loss Prevention" tab is active, showing a "Policy" and "Exceptions" sub-tab. A "+ Add DLP Rule" button and a search bar are visible. A table lists the DLP rules:

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

A "Help" button is located in the bottom right corner of the main content area.

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**.

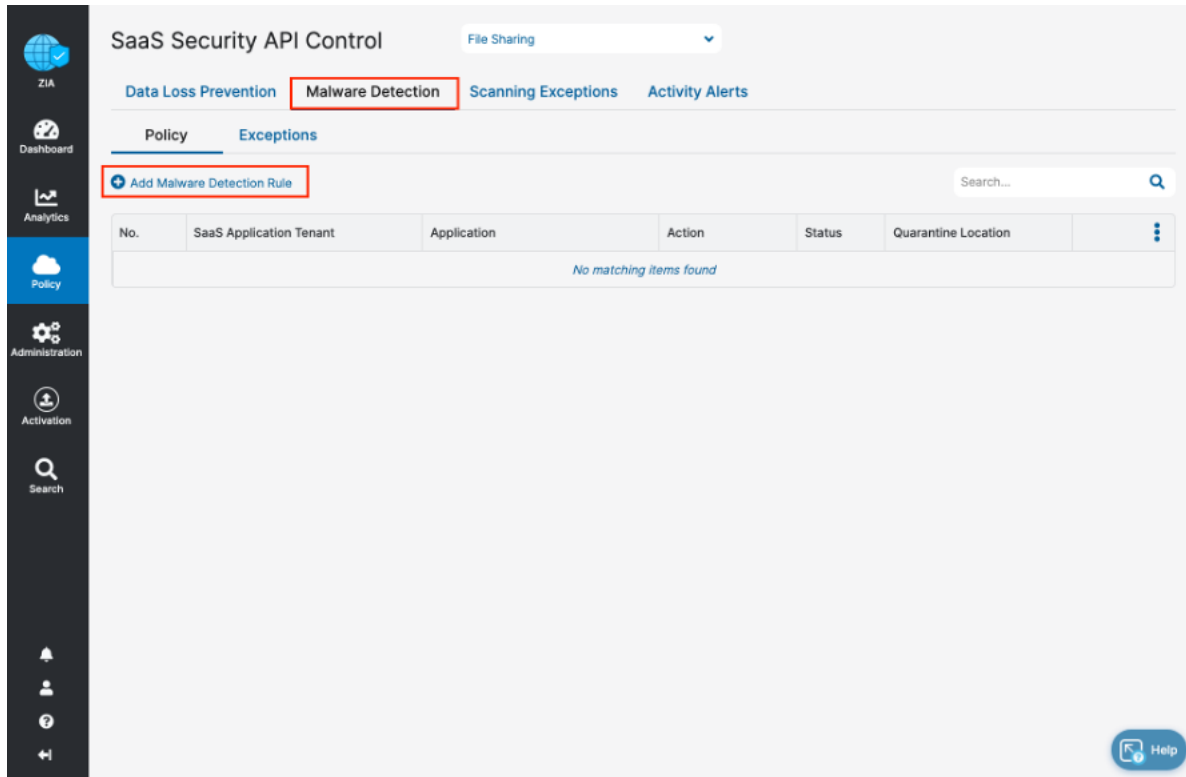


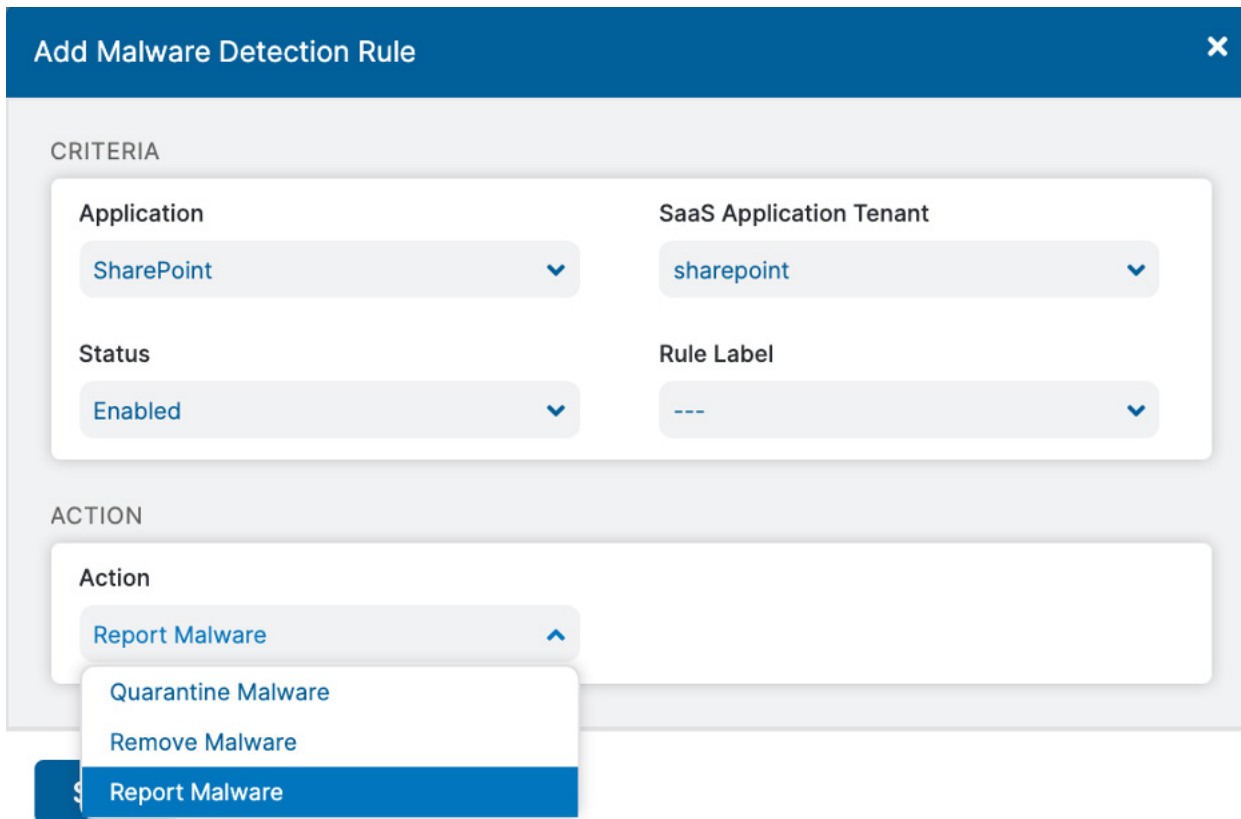
Figure 21. Adding a SaaS malware detection policy

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	SaaS Application Tenant
SharePoint	sharepoint
Status	Rule Label
Enabled	---

ACTION

Action

Report Malware

- Quarantine Malware
- Remove Malware
- 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**.

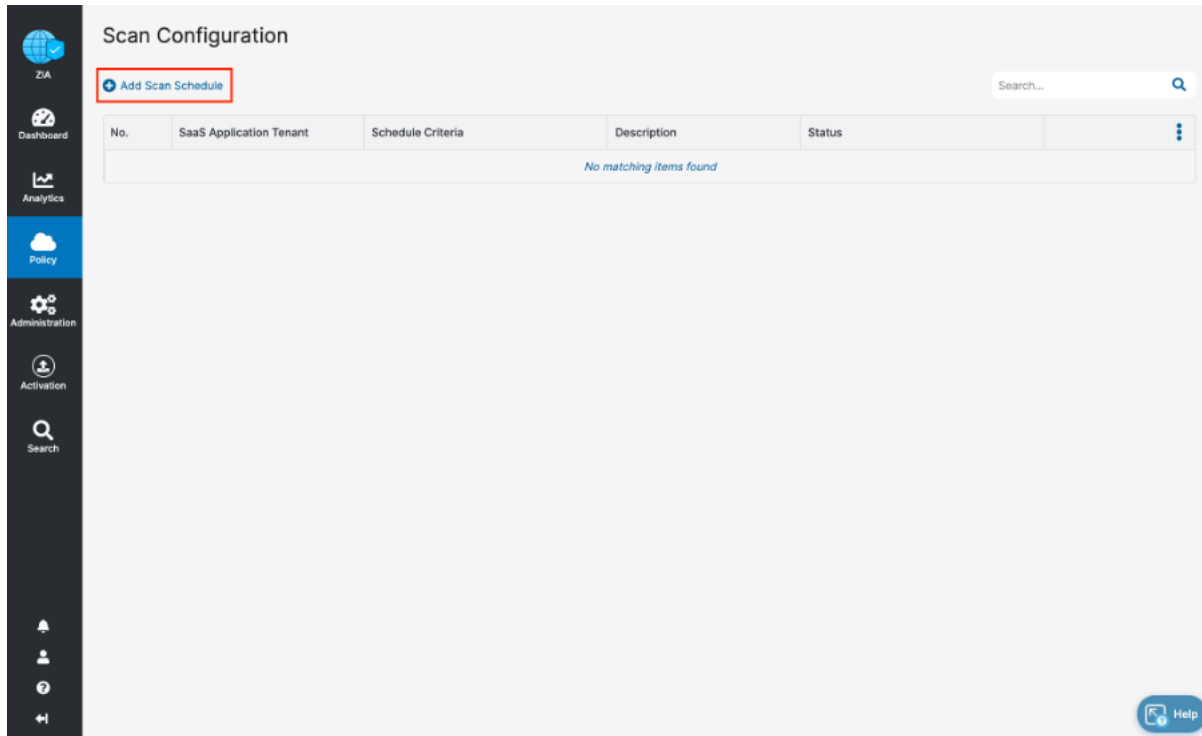


Figure 23. Configure the scan

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**.

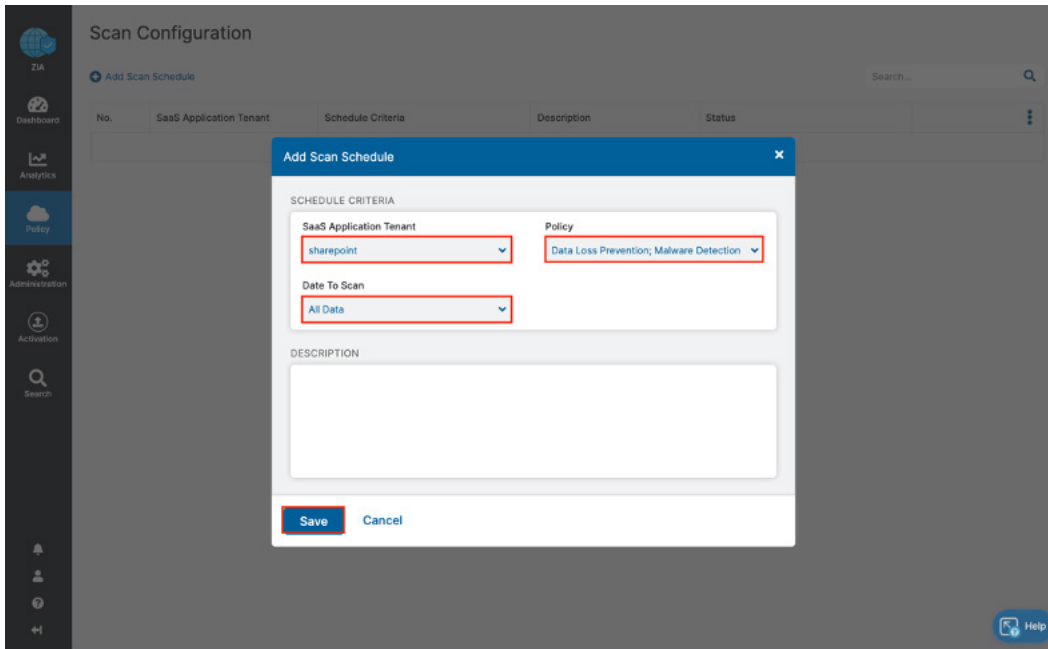


Figure 24. Scan configuration details

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

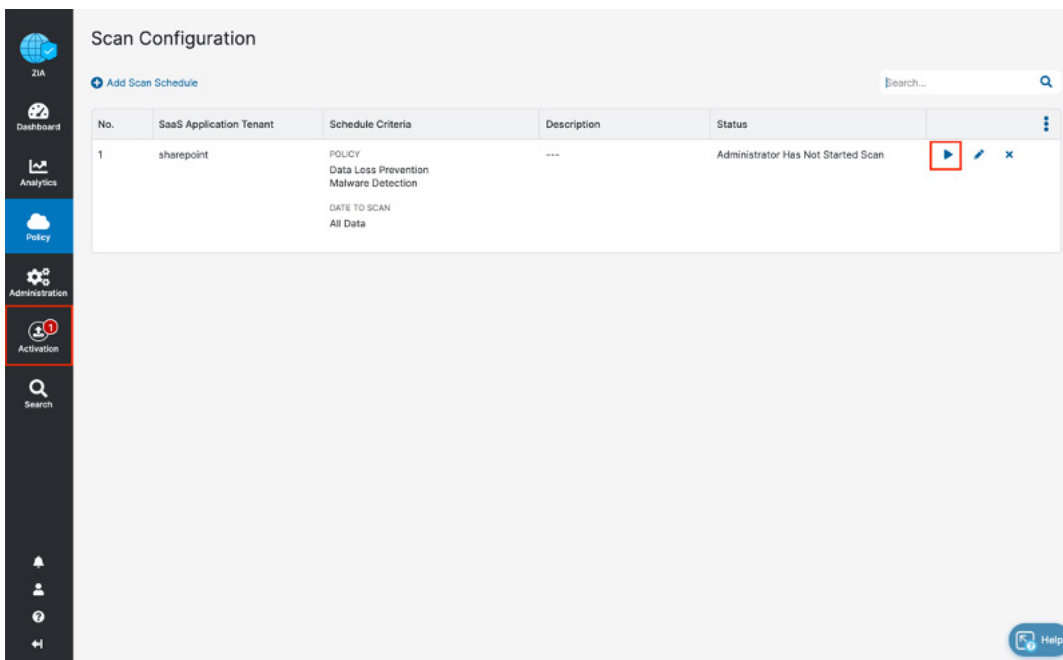


Figure 25. Start the scan

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

The screenshot displays the 'Scan Configuration' interface in the ZIA console. On the left is a dark sidebar with navigation icons for ZIA, Dashboard, Analytics, Policy (highlighted), Administration, Activation, and Search. The main content area has a title 'Scan Configuration' and a '+ Add Scan Schedule' button. A search bar is located in the top right. Below is a table with the following data:

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

A red rectangle highlights the 'Status' column for the first row, which shows 'Running' in green text, followed by 'Scan Started on January 10, 2022 06:10 PM' and 'Latest Scan: ---'. A 'Help' button is visible in the bottom right corner of the main area.

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 [Dashboard & Analytics](#) (government agencies, see [Dashboard & Analytics](#)).

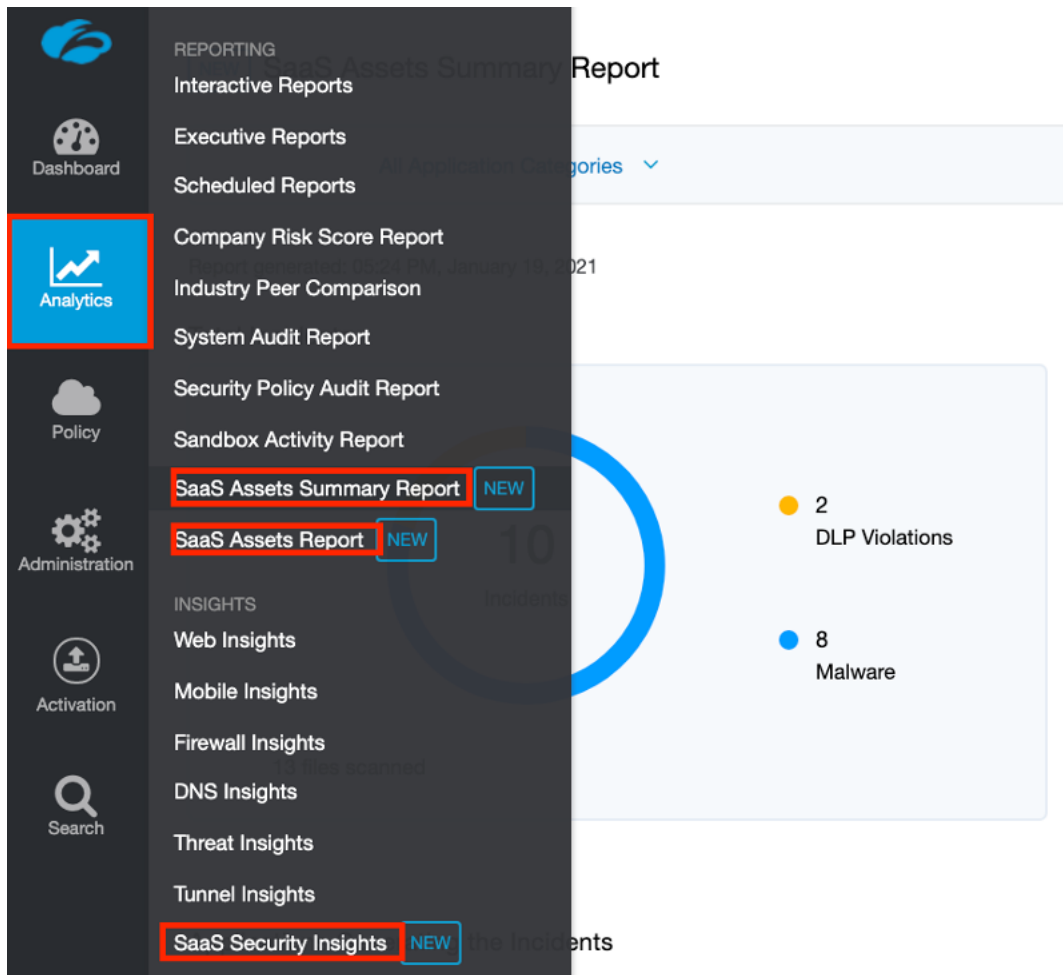


Figure 27. SaaS security visibility

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.

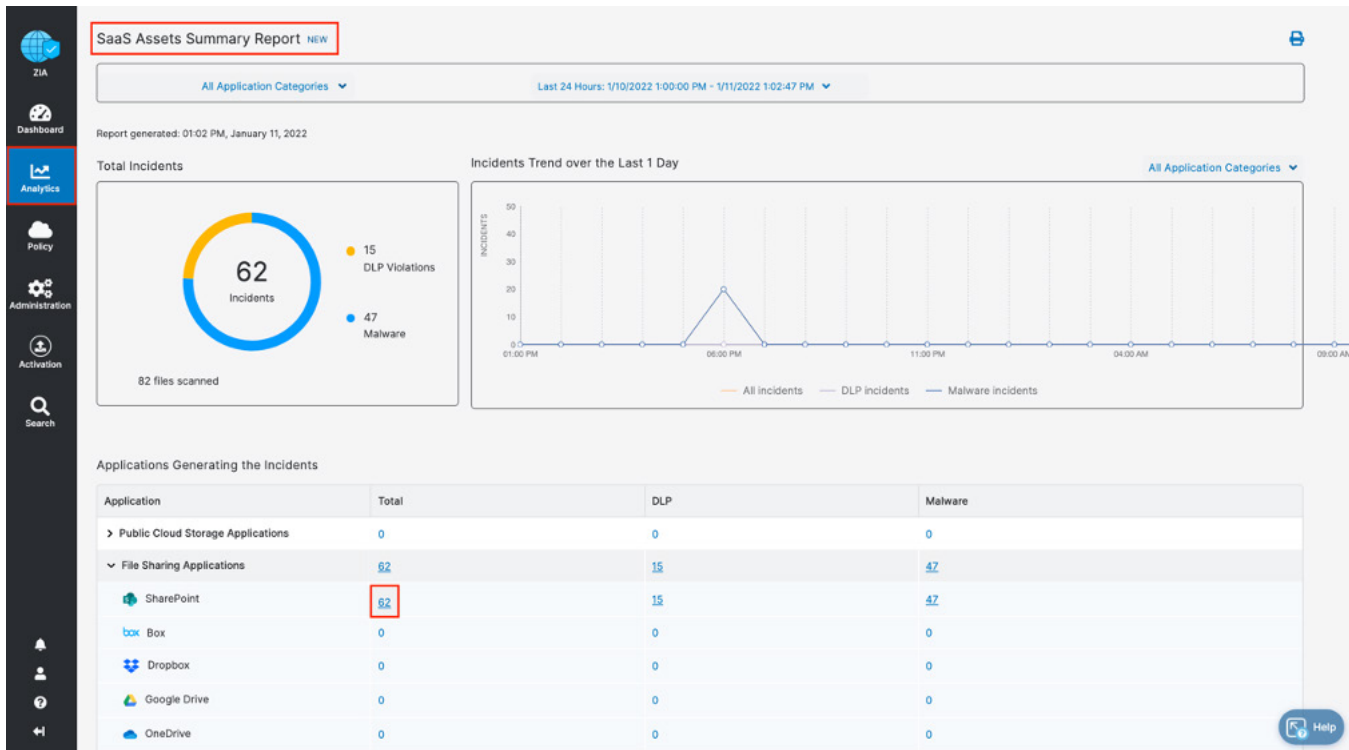


Figure 28. Summary reports

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

The screenshot shows the 'Insights Logs' page in the Zscaler console. The left sidebar contains navigation links: ZIA, Dashboard, Analytics, Policy, Administration, and Activation. The main content area is titled 'Insights Logs' and shows a table of log entries for the period 'Jan 10, 2022 06:11:37 PM - Jan 11, 2022 11:57:55 AM'. The table has columns: Logged Time, Application, File Name, File Source Location, Policy Type, Rule Name, Action, File MD5, and Severity. One log entry is highlighted with a red border: Tuesday, January 11, 2022, SharePo..., 15252.exe, /Shared%20Documents, Malware Detect..., sharepoint, Report Malware, a7f4f9996d4586c72c6..., None. Below the table, there are filters for Application Category (File), Application (SharePoint), and Event (Incidents). A 'Help' button is visible in the bottom right corner of the table area.

Logged Time	Application	File Name	File Source Location	Policy Type	Rule Name	Action	File MD5	Severity
Tuesday, January 11, 2022	SharePo...	15252.exe	/Shared%20Documents	Malware Detect...	sharepoint	Report Malware	a7f4f9996d4586c72c6...	None
Tuesday, January 11, 2022	SharePo...	ssn-records.csv	/Shared%20Documents	DLP	Sharpoin S...	Remove Sharing	71c56967e5d0e0544d...	Medium
Tuesday, January 11, 2022	SharePo...	eicar_com.zip	/Shared%20Documents	None	None	no action	---	None
Tuesday, January 11, 2022	SharePo...	eicar_com.zip	/Shared%20Documents	None	None	no action	---	None
Tuesday, January 11, 2022	SharePo...	eicar.com.txt	/Shared%20Documents	None	None	no action	---	None
Tuesday, January 11, 2022	SharePo...	eicar.com	/Shared%20Documents	None	None	no action	---	None
Tuesday, January 11, 2022	SharePo...	ssn-records.csv	/Shared%20Documents	DLP	Sharpoin S...	Remove Sharing	71c56967e5d0e0544d...	Medium
Tuesday, January 11, 2022	SharePo...	Customer.csv	/Shared%20Documents	DLP	Sharpoin S...	Remove Sharing	71c56967e5d0e0544d...	Medium
Tuesday, January 11, 2022	SharePo...	eicarcom2.zip	/Shared%20Documents	None	None	no action	---	None
Tuesday, January 11, 2022	SharePo...	Medical-Record...	/sites/Testmypacket/Shared%	DLP	Sharpoin S...	Remove Sharing	5f36c6820843d3d33d...	Medium
Tuesday, January 11, 2022	SharePo...	ssn-records.csv	/sites/Testmypacket/Shared%	DLP	Sharpoin S...	Remove Sharing	71c56967e5d0e0544d...	Medium
Tuesday, January 11, 2022	SharePo...	Customer.csv	/sites/Testmypacket/Shared%	DLP	Sharpoin S...	Remove Sharing	71c56967e5d0e0544d...	Medium
Tuesday, January 11, 2022	SharePo...	Medical-Record...	/sites/Testmypacket/Shared%	DLP	Sharpoin S...	Remove Sharing	5f36c6820843d3d33d...	Medium
Tuesday, January 11, 2022	SharePo...	3974.exe	/Shared%20Documents	None	None	no action	---	None
Tuesday, January 11, 2022	SharePo...	Medical-Record...	/sites/Testmypacket/Shared%	DLP	Sharpoin 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.

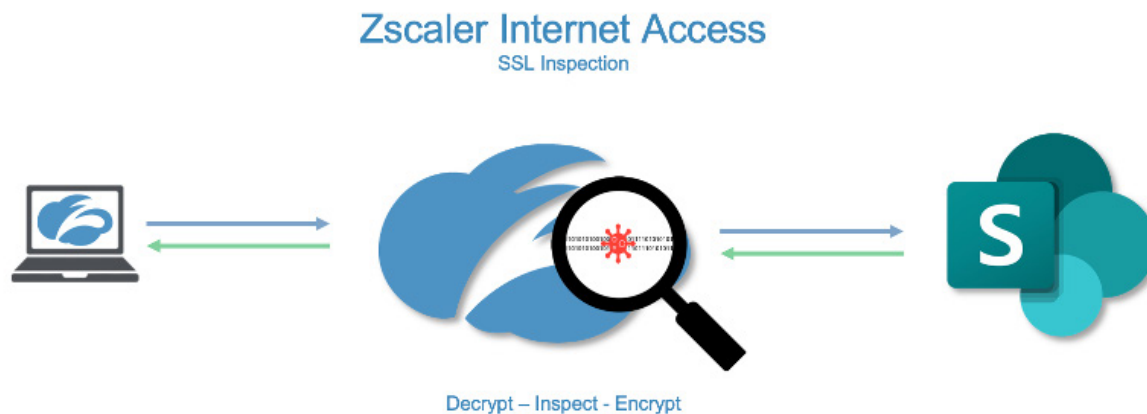


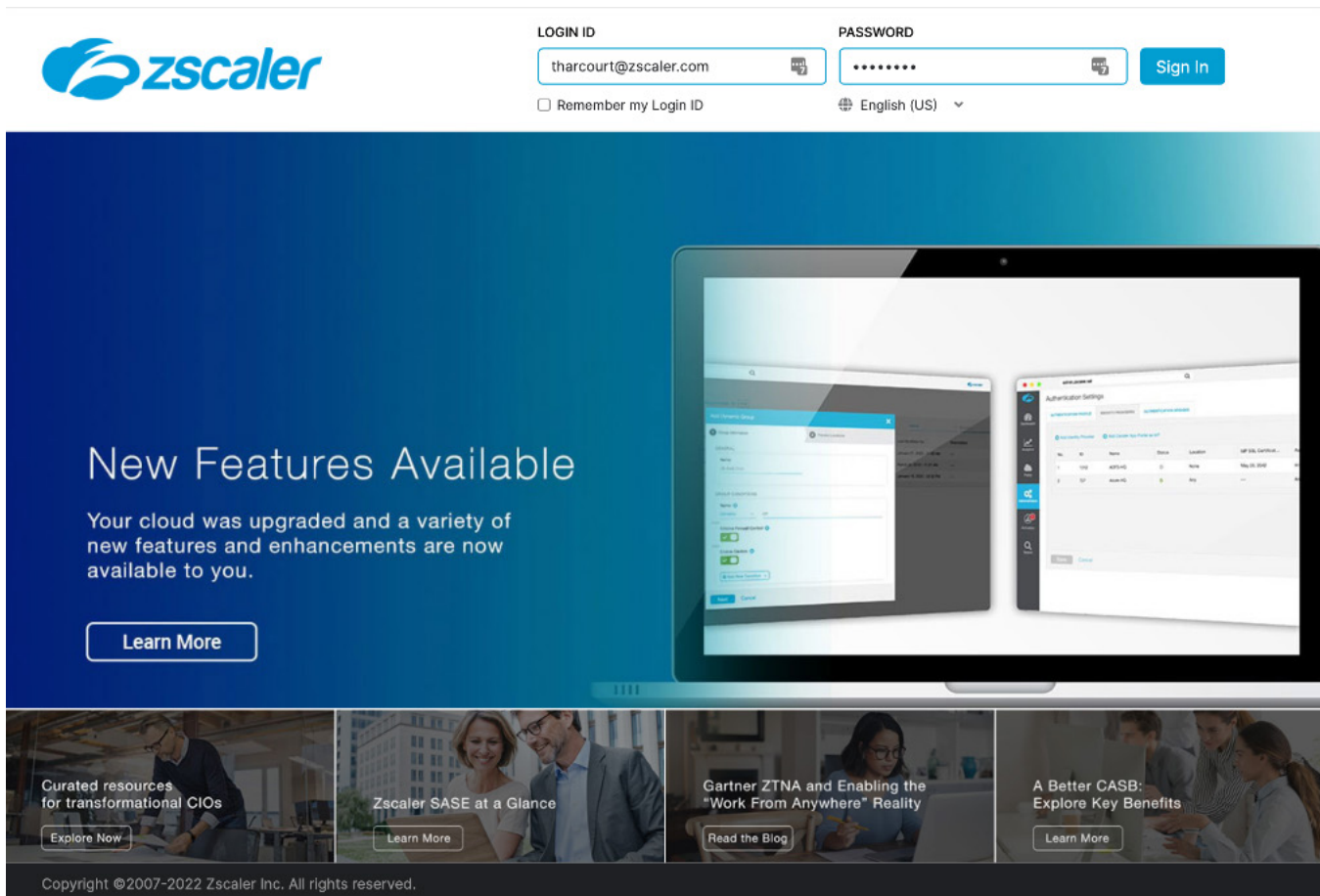
Figure 30. SSL decryption

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.



zscaler

LOGIN ID:

PASSWORD:

☐ Remember my Login ID

English (US) ▼

[Sign In](#)

New Features Available

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

[Learn More](#)

Curated resources for transformational CIOs [Explore Now](#)

Zscaler SASE at a Glance [Learn More](#)

Gartner ZTNA and Enabling the "Work From Anywhere" Reality [Read the Blog](#)

A Better CASB: Explore Key Benefits [Learn More](#)

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

Figure 31. ZIA tenant

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**.

The screenshot shows the Zscaler Policy configuration interface. The left sidebar contains navigation icons for ZIA, Dashboard, Analytics, Policy (highlighted), Administration, Activation, and Search. The main content area is titled "SSL Inspection" and includes a "Configure SSL Inspection Policy" section with the note: "Rules are evaluated in the order specified. Rule evaluation stops at the first match." Below this, there are tabs for "SSL Inspection Policy" and "Advanced SSL Inspection Settings". A button "Add SSL Inspection Rule" is visible. The main table lists the following rules:

Rule Order	Rule Name	Criteria	Action	Label and Descripti...
1	SSL_1	CLOUD APPLICATIONS ServiceNow URL CATEGORIES Other Adult Material; Adult Themes; Lingerie/Bikini;...	Inspect Untrusted Server Certificates Block OCSP Revocation Check Enabled Block Undecryptable Traffic Disable Minimum Client TLS Version TLS 1.0 Minimum Server TLS Version TLS 1.1	
2	Zscaler Recommended...	URL CATEGORIES Recommended SSL Exemptions	Do Not Inspect Bypass Other Policies	
3	Office 365 One Click	URL CATEGORIES Office 365; Zscaler Recommended Exemptions Off...	Do Not Inspect Bypass Other Policies	
4	UCaaS One Click	CLOUD APPLICATIONS Zoom; RingCentral; LogMeIn	Do Not Inspect Bypass Other Policies	DESCRIPTION Recommended exempt...
5	SSL Bypass	CLOUD APPLICATIONS Apple Developer; Gmail; iCloud IP & FQDN GROUPS NoSSL_NoOtherPolicies_Domains	Do Not Inspect Bypass Other Policies	DESCRIPTION (Auto-generated) Whit...
6	Inspect CItCon on SSL ...	DEVICE GROUPS Mac; Windows	Inspect Untrusted Server Certificates Pass OCSP Revocation Check Disabled	DESCRIPTION (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.

The screenshot shows the 'Add SSL Inspection Rule' wizard in the Zscaler interface. The wizard is configured with the following details:

- Rule Order:** 1
- Rule Name:** SharePoint
- Rule Status:** Enabled
- Cloud Applications:** SharePoint Online
- Device Groups:** Mac, Windows
- Action:** Inspect

The 'Save' button is highlighted in red at the bottom of the wizard. The background shows a list of existing SSL inspection rules.

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](#) (government agencies, see [SSL Inspection Using a Custom Intermediate Root Certificate](#)).

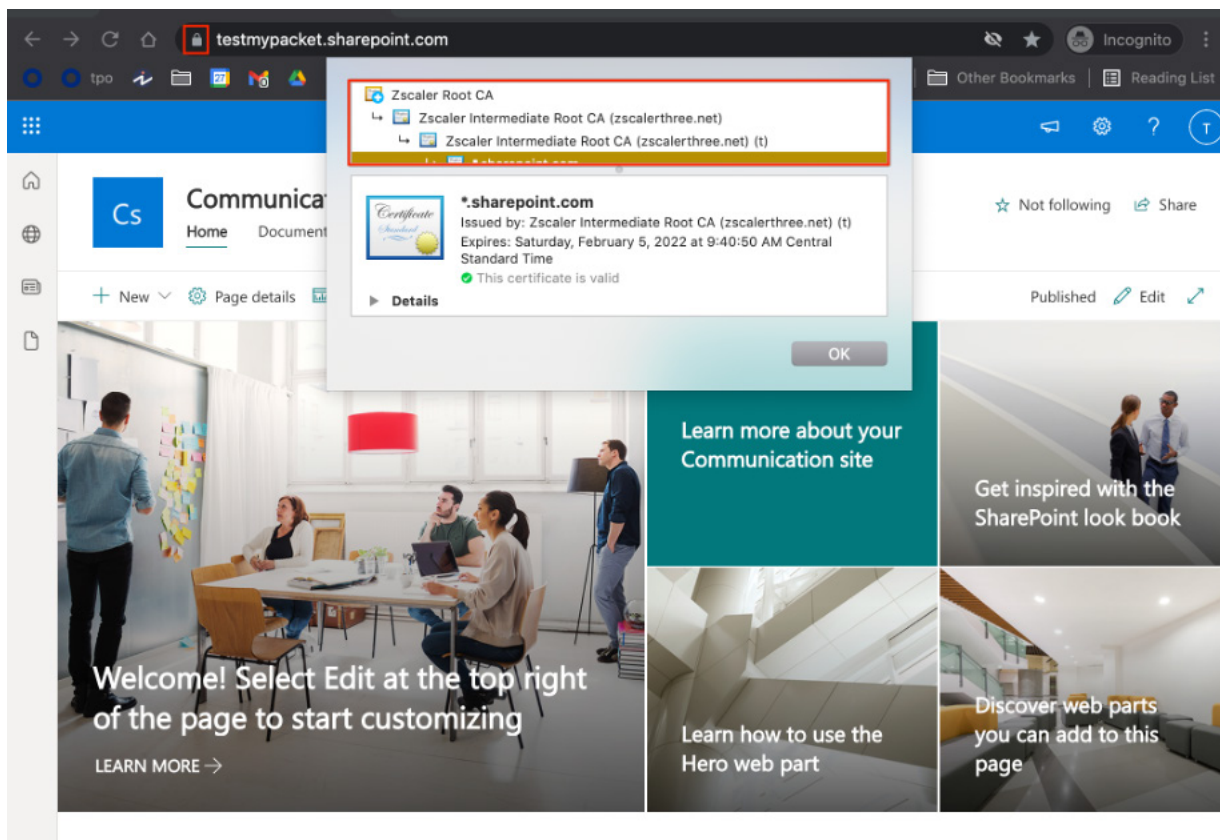


Figure 34. Verifying SSL inspection for SharePoint

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.

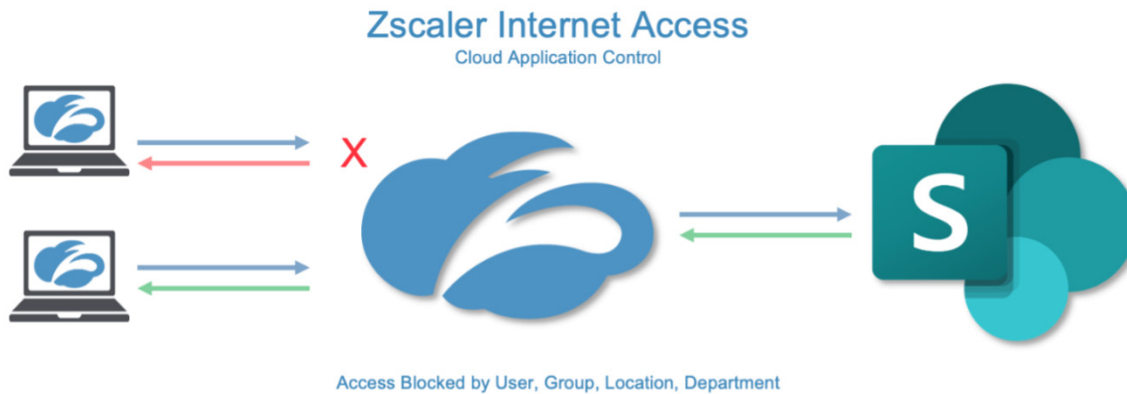


Figure 35. Cloud app control

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**.

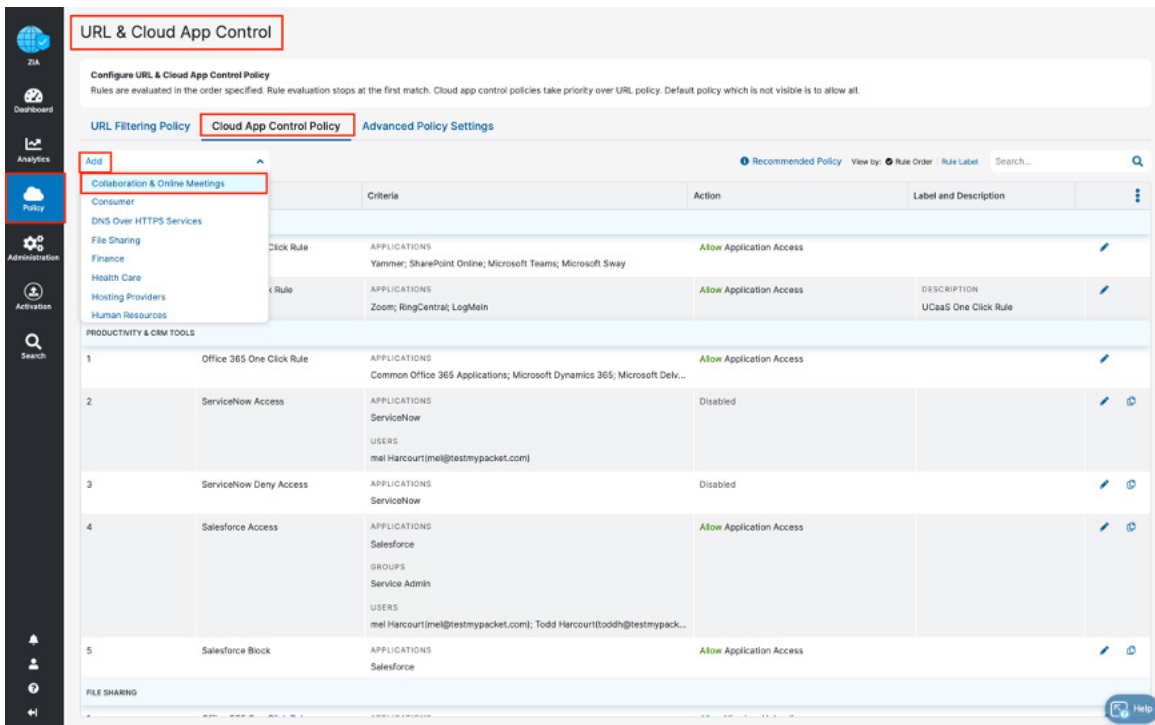


Figure 36. Cloud app control

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.

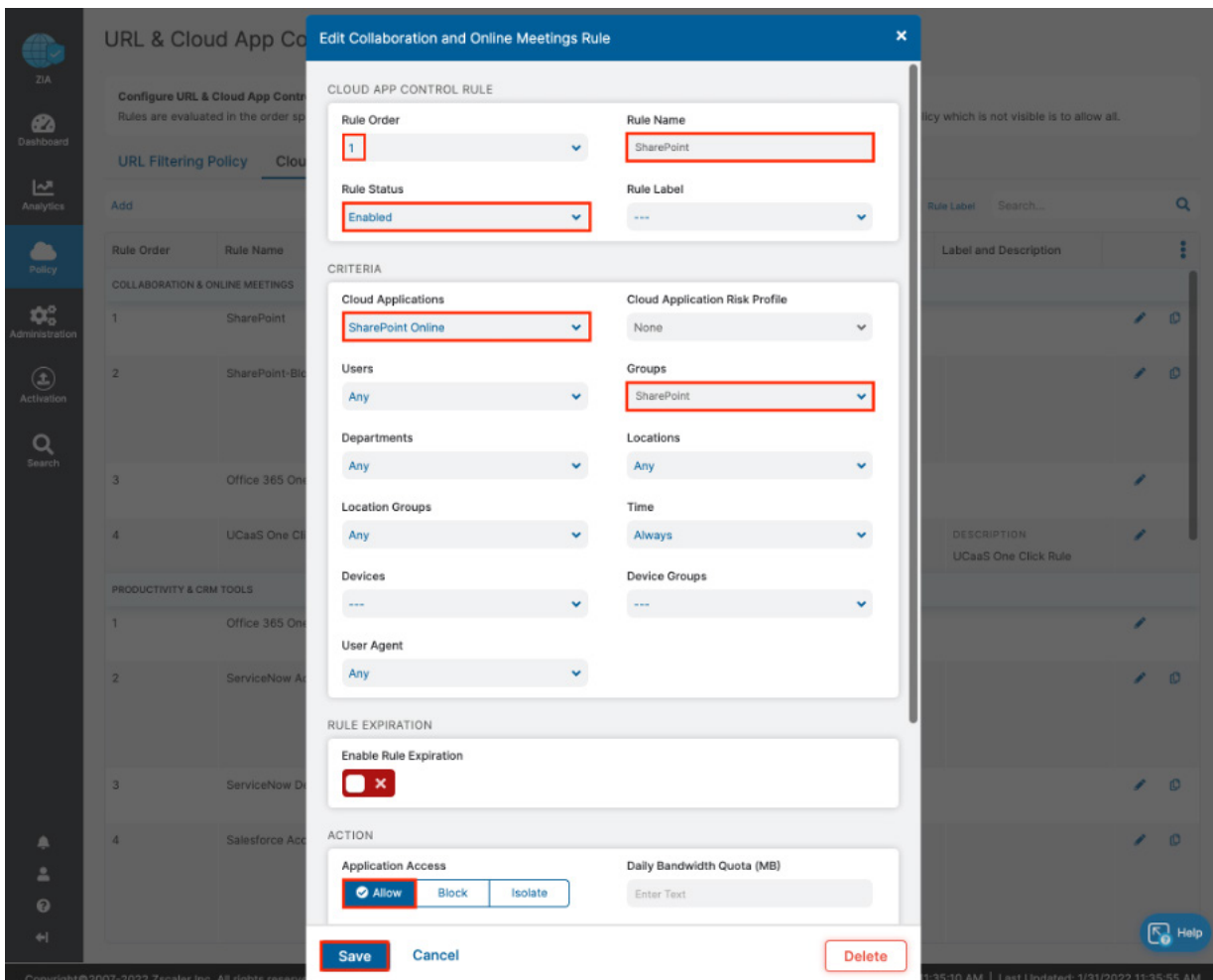


Figure 37. Cloud app control rule 1

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.

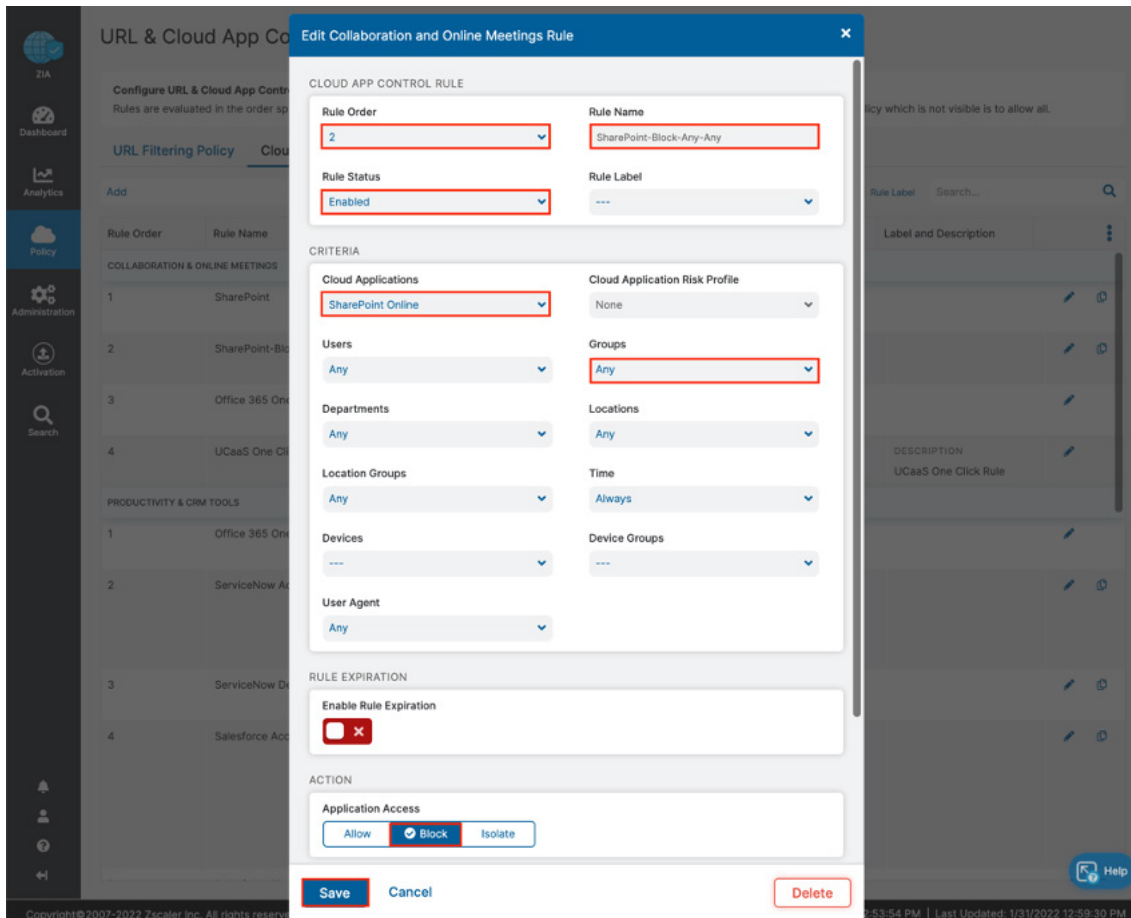


Figure 38. Cloud app control rule 2

The completed policies are displayed.

The screenshot displays the Zscaler management console interface for URL & Cloud App Control. The left sidebar contains navigation icons for ZIA, Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled "URL & Cloud App Control" and includes a sub-header "Configure URL & Cloud App Control Policy" with a note: "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". Below this are three tabs: "URL Filtering Policy", "Cloud App Control Policy" (which is selected), and "Advanced Policy Settings". A "Add" button is visible. The interface shows a list of policies under the heading "COLLABORATION & ONLINE MEETINGS". The policies are listed in a table with columns: Rule Order, Rule Name, Criteria, Action, and a partially visible "L" column. The first two rules are highlighted with a red border.

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

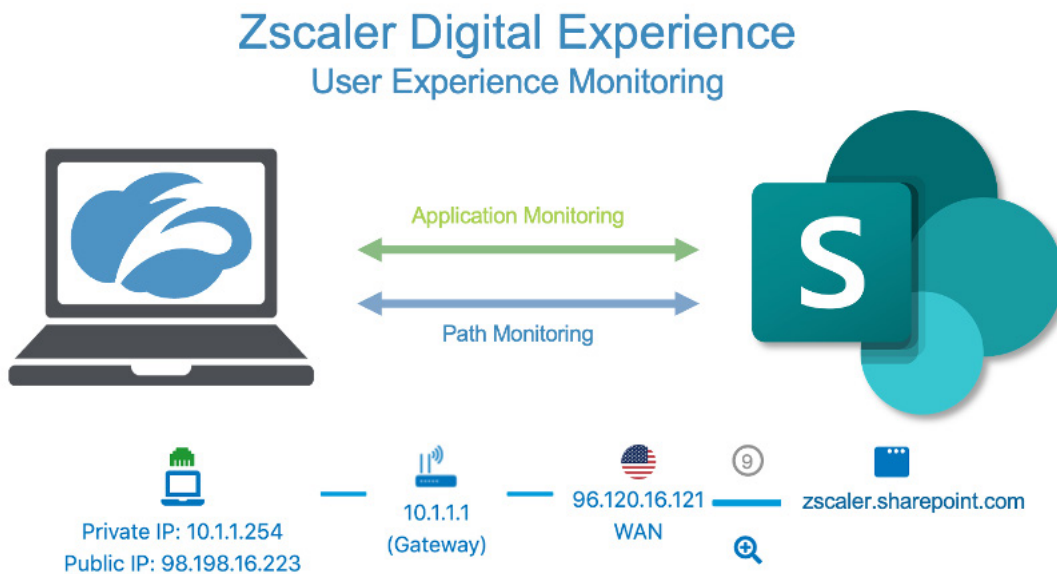


Figure 40. ZDX for user experience monitoring for SharePoint

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.



The image shows the Zscaler ZDX Admin Portal login page. At the top left is the Zscaler logo with the tagline "Digital Experience". To the right of the logo are two input fields: "LOGIN ID" and "PASSWORD". The "LOGIN ID" field contains the text "zdx-admin@10656179.zscalerthree.net". The "PASSWORD" field contains a series of dots. Below the "LOGIN ID" field is a checkbox labeled "Remember my Login ID". To the right of the "PASSWORD" field is a dropdown menu showing "English (US)". A blue "Sign In" button is located to the right of the "PASSWORD" field. Below the login fields is a large banner image of a man working on a laptop. Overlaid on the banner is the text "Empower employees to work safely and productively from anywhere" and a "Get Started" button. Below the banner are four smaller images with text and "Learn More" buttons: "Zscaler Cloud Upgrade: New Features Available", "Zscaler SASE at a Glance", "Gartner ZTNA and Enabling the 'Work From Anywhere' Reality", and "A Better CASB: Explore Key Benefits". At the bottom of the page is a copyright notice: "Copyright ©2007-2022 Zscaler Inc. All rights reserved."

zscaler
Digital Experience

LOGIN ID
zdx-admin@10656179.zscalerthree.net

PASSWORD
.....

☒ Remember my Login ID

English (US)

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.

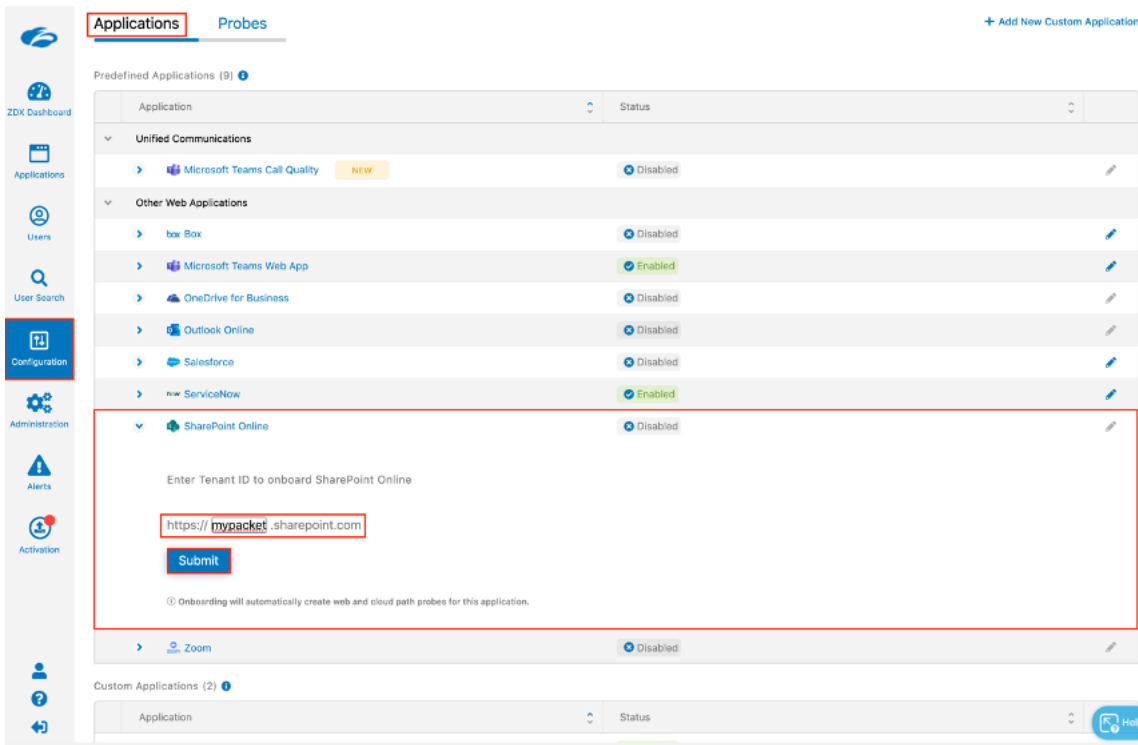


Figure 42. Onboard the SharePoint Online app

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.

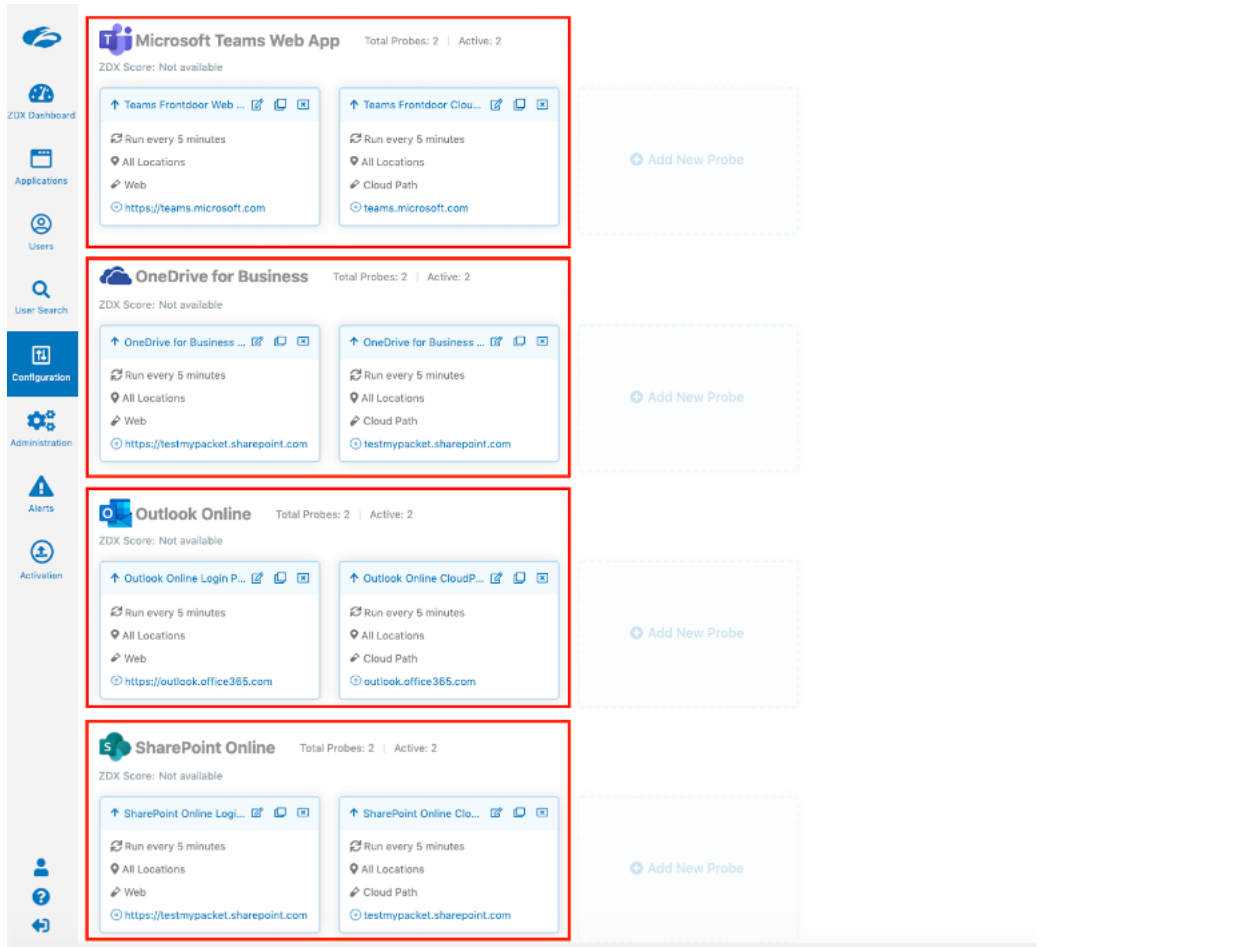


Figure 43. ZDX for user experience monitoring for SharePoint

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.

Applications **Probes** [+ Add New Custom Application](#)

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**.

The screenshot displays the Zscaler ZDX Dashboard interface. On the left sidebar, the 'Alerts' icon is highlighted with a red box. The main content area shows the 'Rules' tab selected and highlighted with a red box. Below the tabs, there are filter dropdowns for 'All Applications & Probes', 'All Severities', 'All Locations', and 'All Geolocations', along with 'Apply' and 'Reset' buttons. A table below these filters shows 'No data'. At the bottom of the main content area, a button labeled '+ Add New Alert Rule' is highlighted with a red box.

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 [X]

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

* **Name**
SharePoint Degradation Alert

* **Status**
☒ Enabled ☐ Disabled

* **Severity**
High

* **Type**
Application

Next Cancel

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**.

The screenshot shows the 'Add New Alert Rule' wizard with five steps: 1. Configure Rule, 2. Filters, 3. Criteria, 4. Action, and 5. Review. Step 2, 'Filters', is the active step. It contains two dropdown menus: '* Application' and '* Web Probe'. The '* Application' dropdown is set to 'SharePoint Online' and the '* Web Probe' dropdown is set to 'SharePoint Online Login Page Probe'. Below these dropdowns is a button labeled '+ Add Filter'. At the bottom of the wizard, there are three buttons: 'Next', 'Previous', and 'Cancel'. The 'Next' button is highlighted with a red border.

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**.

The screenshot shows the 'Add New Alert Rule' wizard with five steps: 1. Configure Rule, 2. Filters, 3. Criteria, 4. Action, and 5. Review. The 'Criteria' step is currently active. The rule is configured as follows:

- Scope: ALL
- Condition: Page Fetch Time >= 5000 ms
- Buttons: Add, Expression, Show Preview

At the bottom of the wizard, there are three buttons: **Next** (highlighted with a red box), Previous, and Cancel.

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

1 **Configure Rule**

2 **Filters**

3 **Criteria**

4 **Action**

5 **Review**

THROTTLING

* Alert Only if Repeated Times in a Row

* Minimum Devices Impacted

Number

☒ Percentage

* In Group

Cities

ACTION

Muted

☐ ☒

* Alert Delivery Method

Email

* Alert Recipients

Next

Previous

Cancel

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

©2024 Zscaler, Inc. All rights reserved. 54

The following is the completed rule set for the alert.

The screenshot shows the Zscaler Alerts configuration interface. The 'Rules' tab is selected, displaying a table of alert rules. A single rule, 'SharePoint Degrad...', is listed with a status of 'Enabled'. The sidebar on the left contains navigation icons for ZDX Dashboard, Applications, Users, User Search, Configuration, Administration, Alerts, and Activation. The 'Activation' icon is highlighted with a red box.

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.

The screenshot displays the Zscaler Alerts dashboard. On the left is a sidebar with navigation icons for ZDX Dashboard, Applications, Users, User Search, Configuration, Administration, Alerts (highlighted with a red box), and Activation. The main content area has tabs for 'Alerts' and 'Rules'. Below the tabs is a filter bar with dropdowns for 'All Alert Rules', 'All Impacted Devices', 'All Impacted Geolocations', and 'All Impacted Applications', along with 'Apply' and 'Reset' buttons. A '48 Hours' time range selector is also present. Below the filter bar are five summary cards: 'ONGOING ALERTS' (1), 'HISTORICAL' (0), 'TOTAL IMPACTED DEVICES' (1), 'TOTAL IMPACTED GEOLOCATIONS' (1), and 'TOTAL IMPACTED APPLICATIONS' (1). Under the 'Ongoing Alerts' tab, a table lists the active alerts. The first row, highlighted with a red border, shows a 'SharePoint Degra...' alert of severity 'Critical' (red dot), type 'Application', impacted by 'SharePoint Online', affecting '1 Geolocations' and '1 Devices', started on 'Jan 31, 2022 11:40:00 AM', and currently 'Ongoing'. A 'View' icon is visible at the end of the row.

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

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.

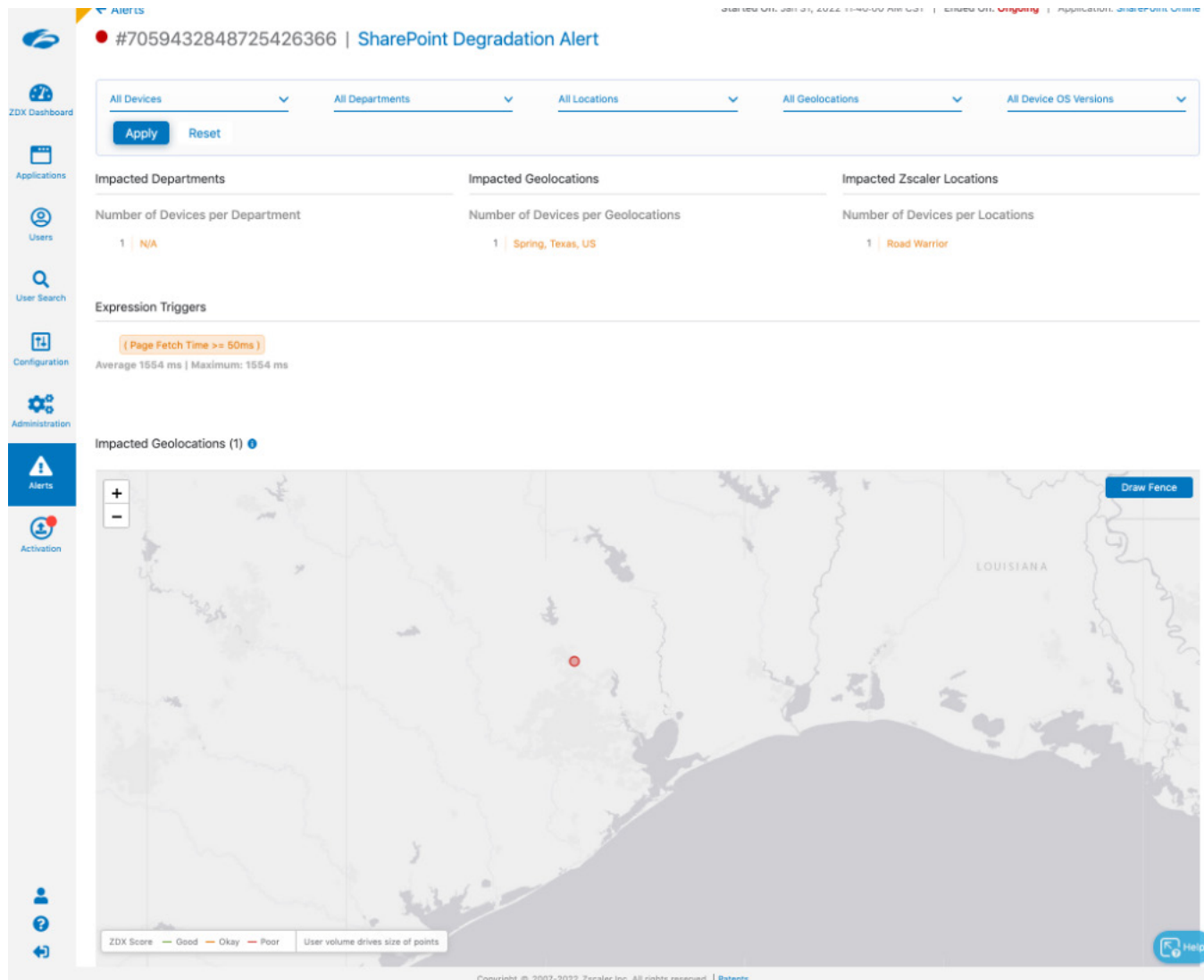


Figure 52. Alert details

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

Inbox - Zscaler 12:04 PM

N

ZDX Alert# 7059432848725426366 Started 1 Devices Affected

To: Todd Harcourt


 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

View Alert 

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.

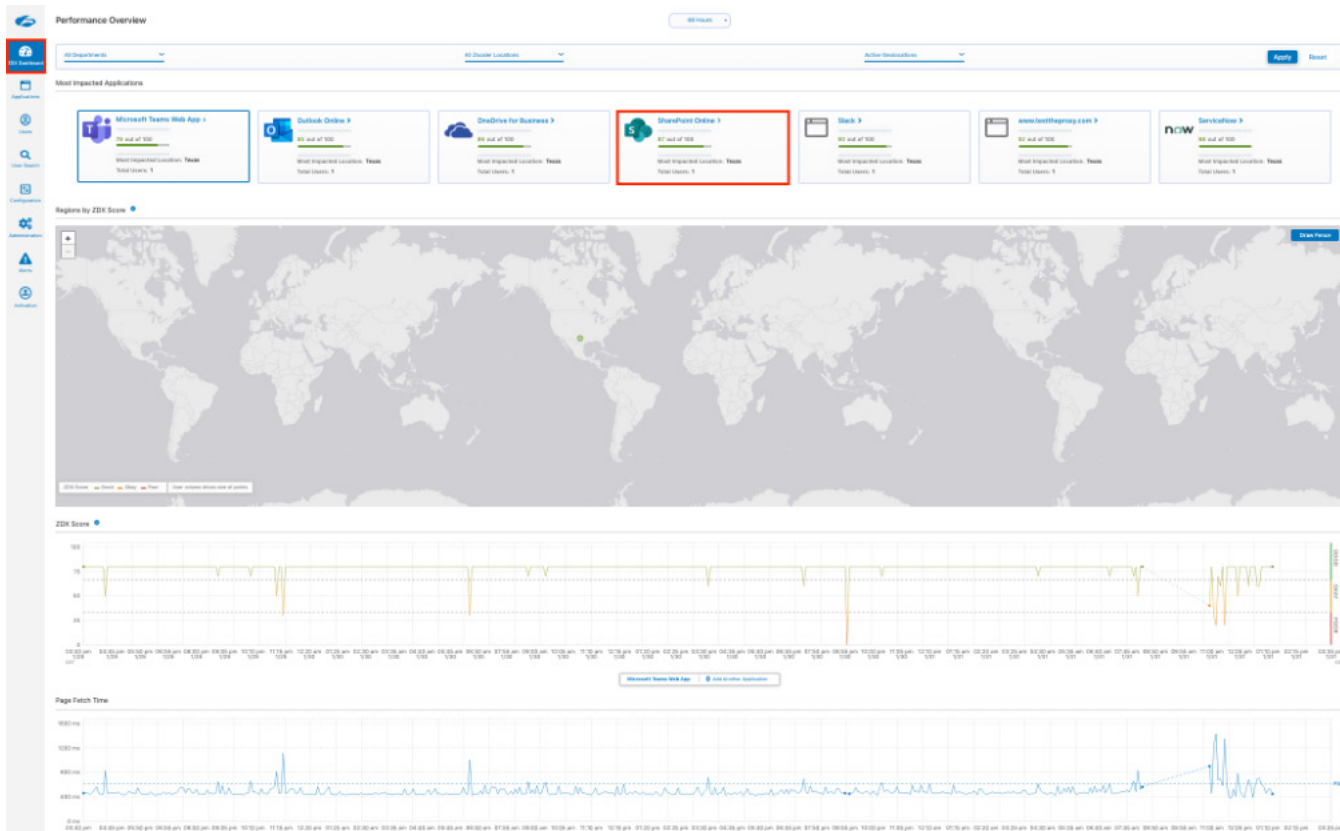


Figure 54. The dashboard

Application Overview

Selecting Applications on the left-hand navigation pane of the ZDX Admin Portal displays the Applications Overview, which 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**.

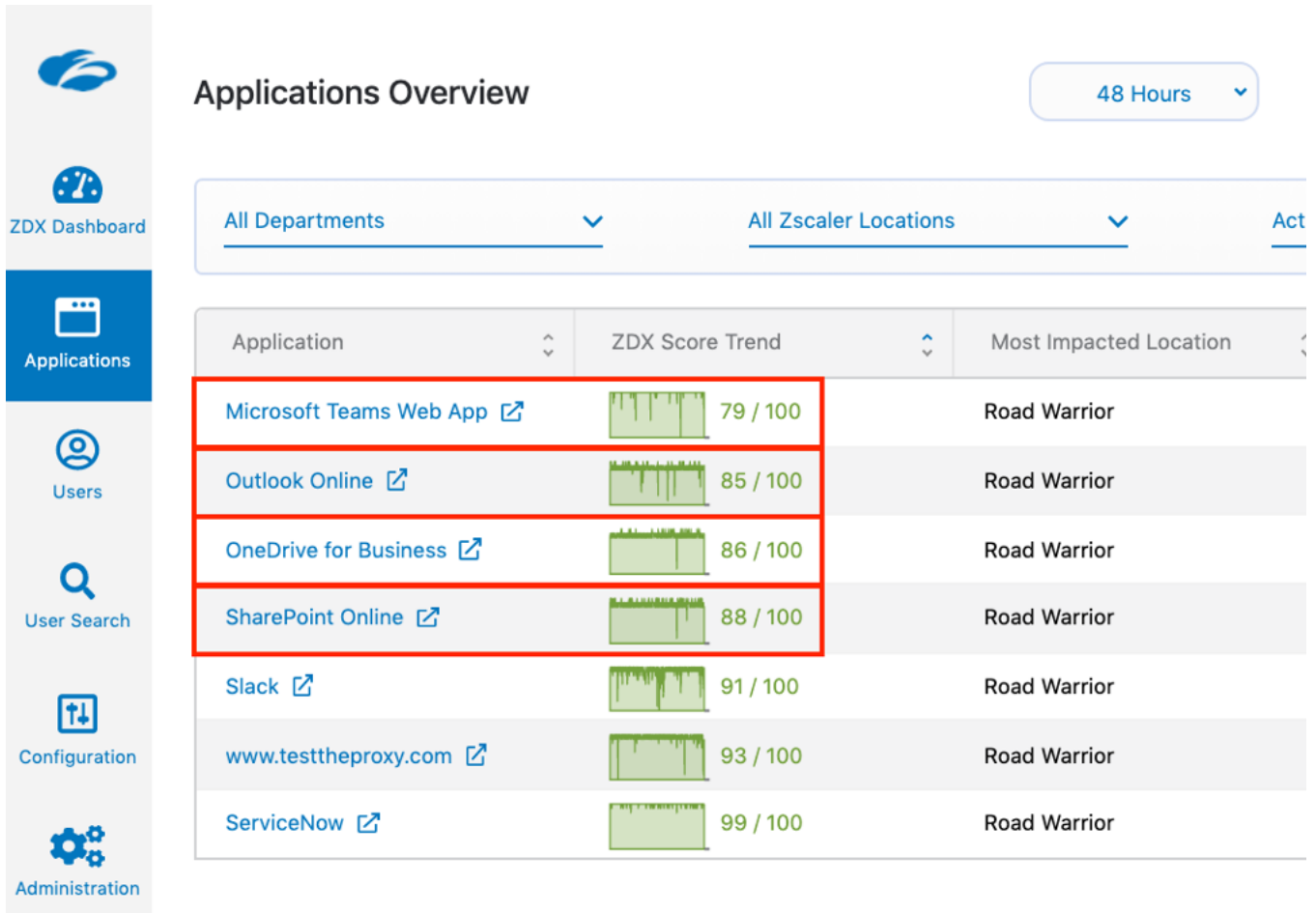


Figure 55. Application overview

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.

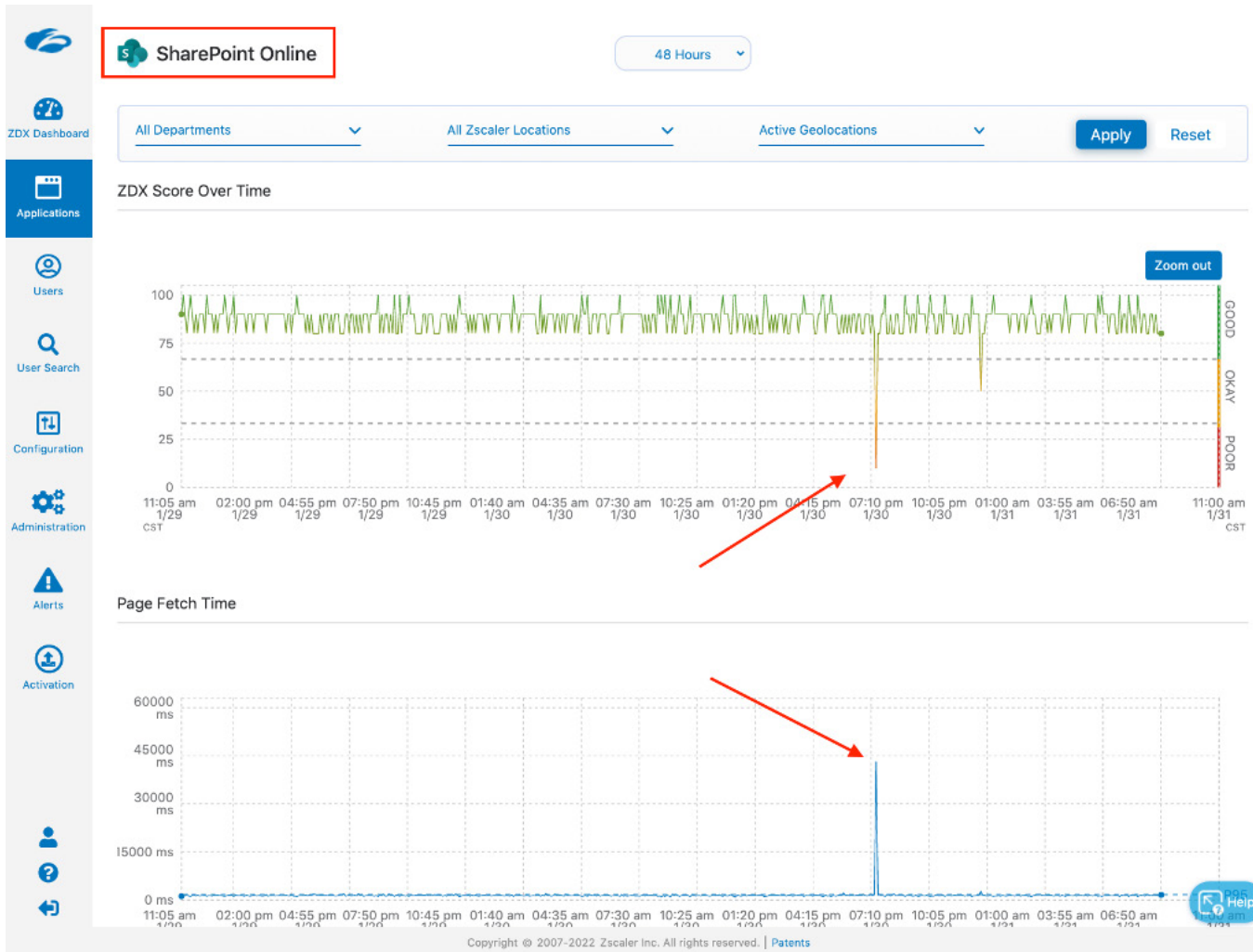


Figure 56. Application detail

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.

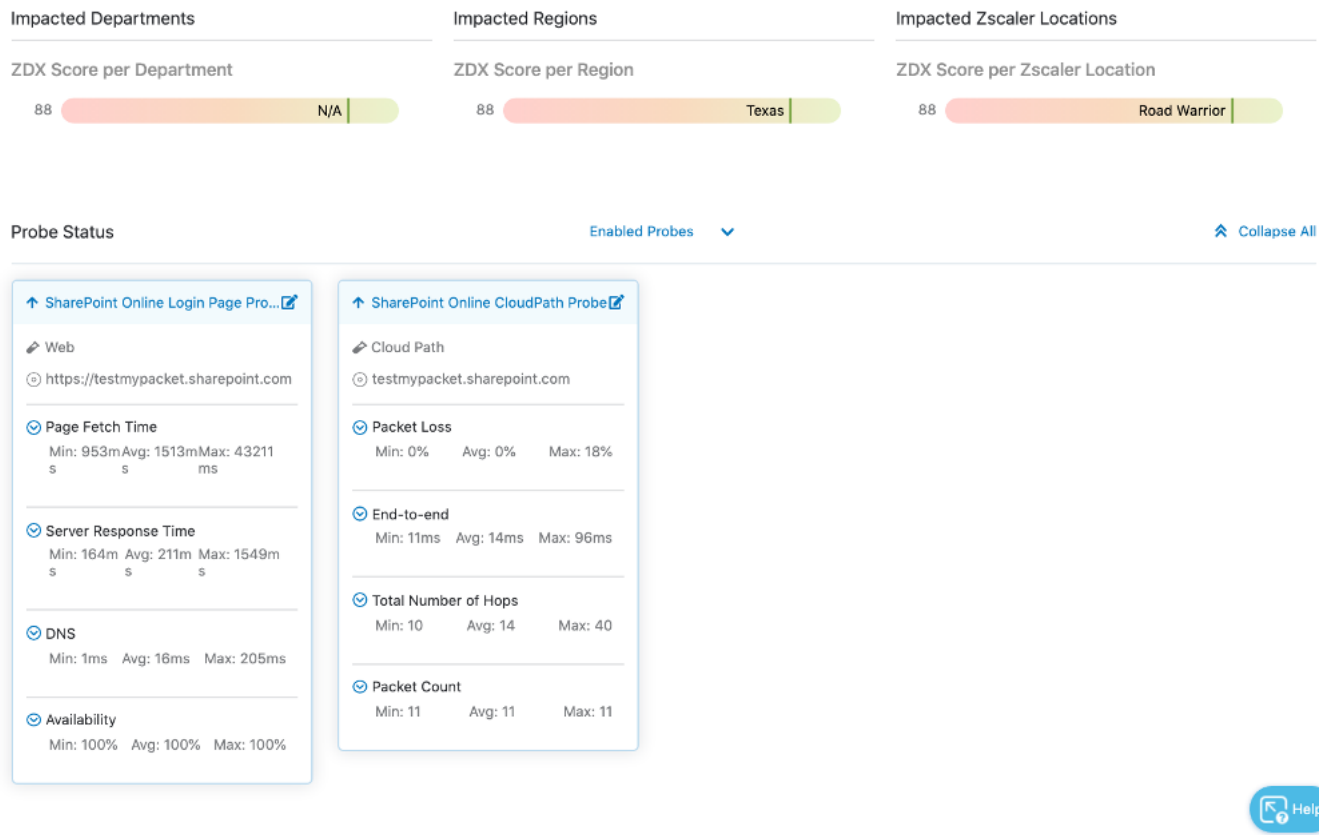


Figure 57. Application detail

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.

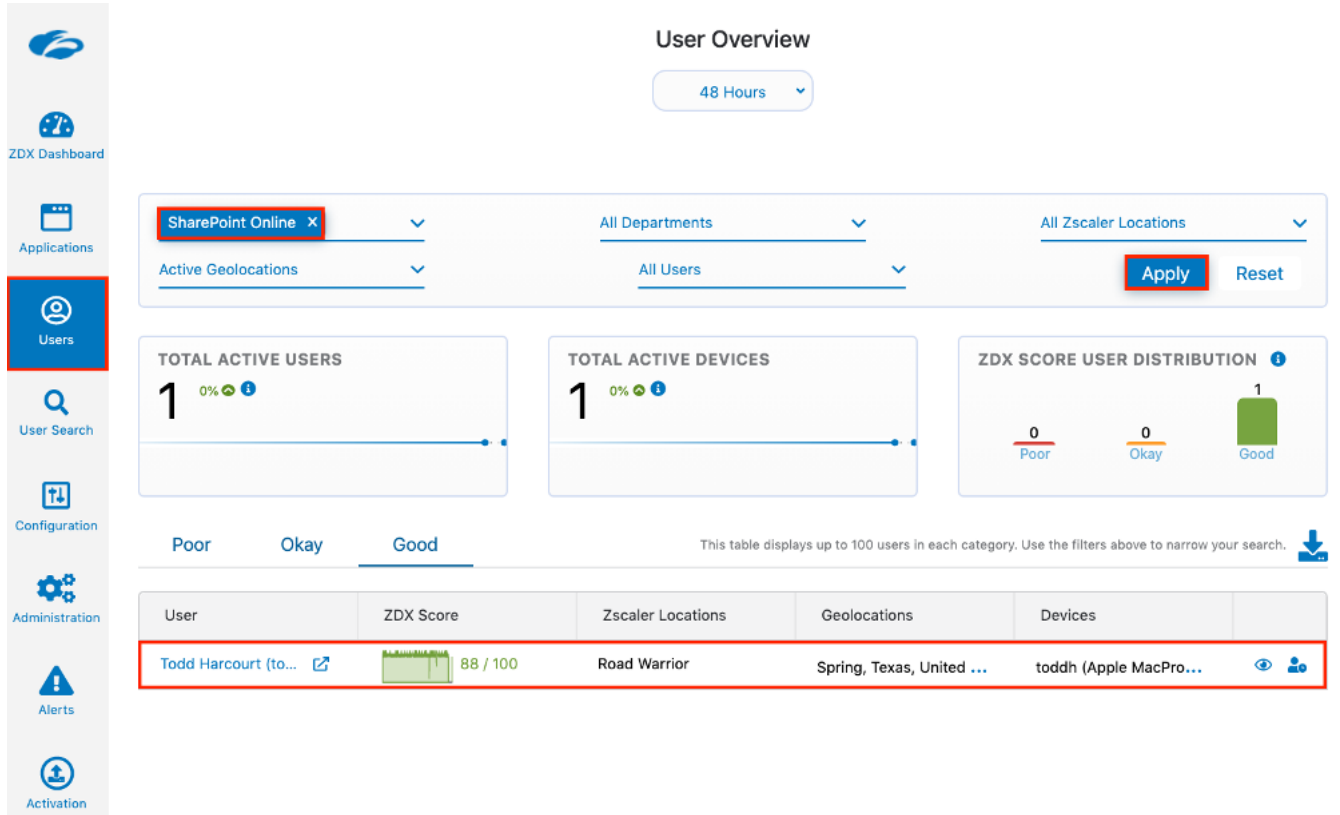


Figure 58. User overview

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.

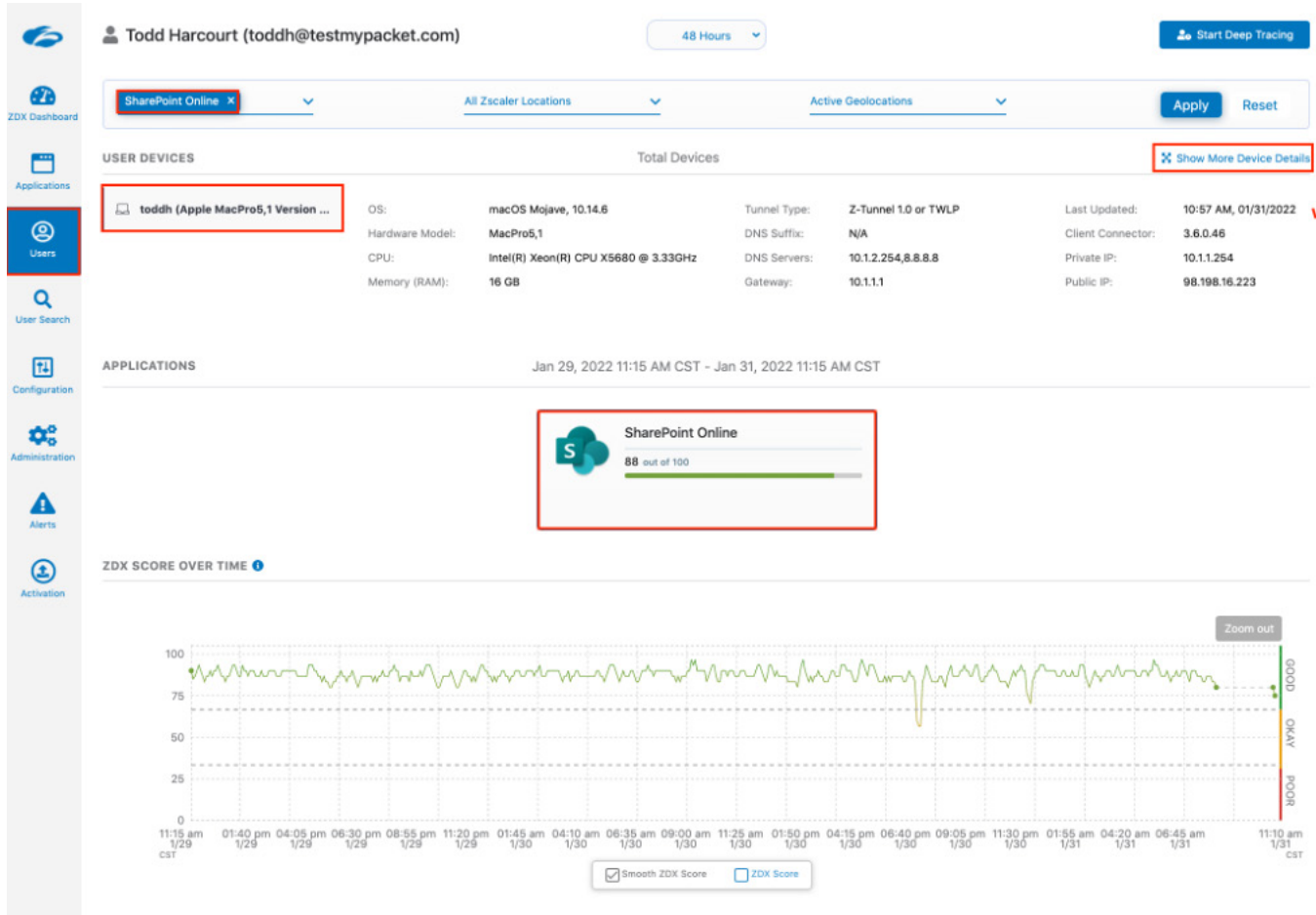


Figure 59. User detail

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.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > and then click **Company Profile**.

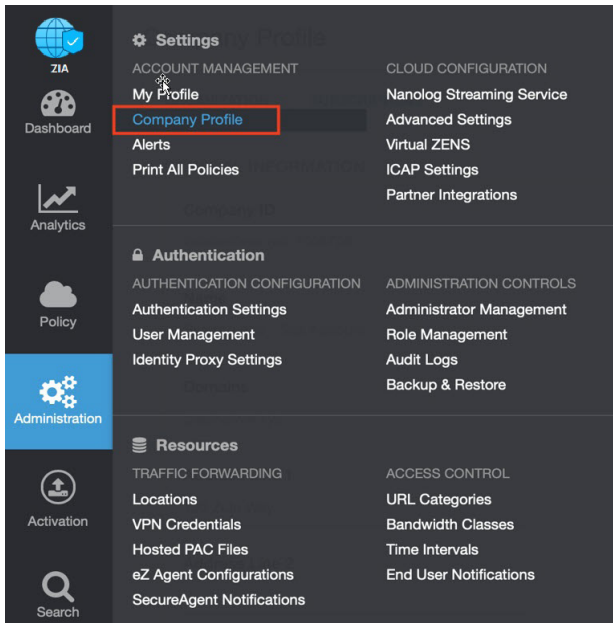


Figure 60. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

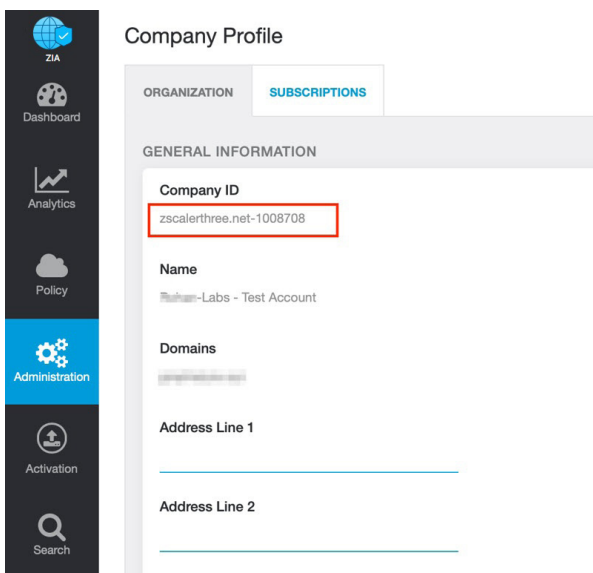


Figure 61. Company ID

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

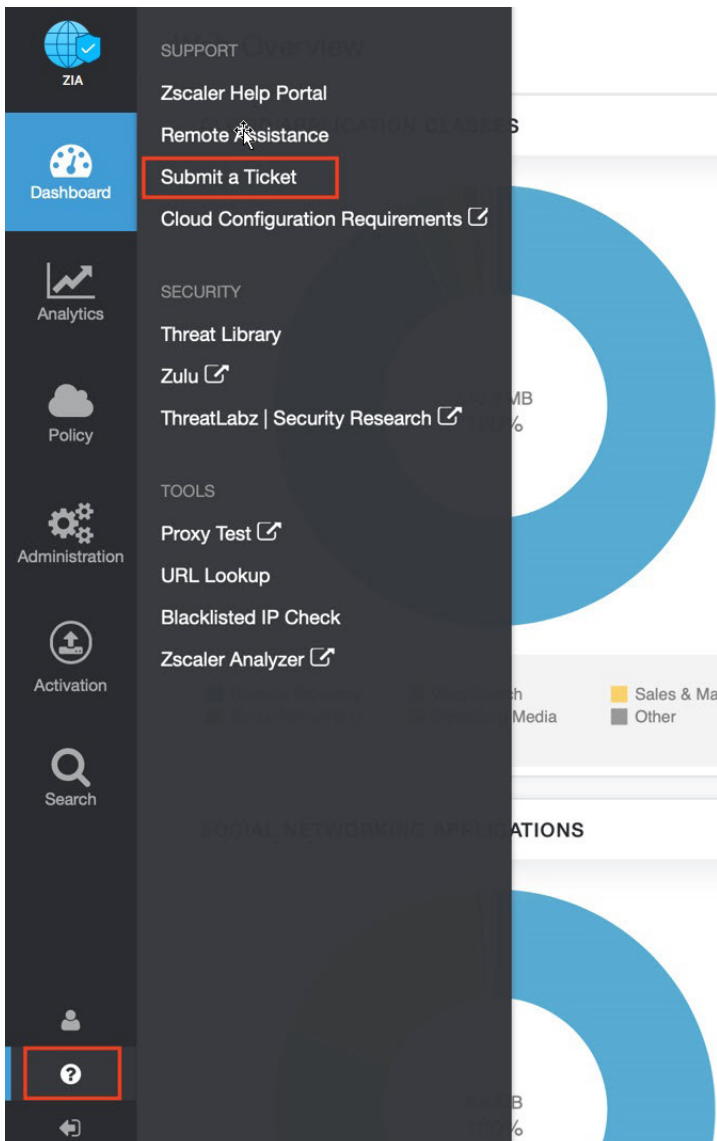


Figure 62. Submit a Ticket