Table of Contents

Terms and Acronyms .................................................................................................................. 3

About This Document .................................................................................................................. 4

Zscaler Overview.......................................................................................................................... 4
Microsoft Overview ..................................................................................................................... 4
Audience ....................................................................................................................................... 4
Software Versions ......................................................................................................................... 4
Request for Comments ................................................................................................................ 4

Zscaler and Microsoft SharePoint Introduction ............................................................................. 5

Zscaler Overview .......................................................................................................................... 5
  Zscaler Internet Access (ZIA) Overview .................................................................................... 5
  Zscaler Private Access (ZPA) Overview .................................................................................... 5
SharePoint Overview .................................................................................................................... 7

Zscaler Data Protection and Digital Experience for SharePoint.com .............................................. 8

Overview ...................................................................................................................................... 8
  Zscaler Internet Access CASB Data and Malware Protection for SharePoint ............................. 9
  Zscaler Internet Access SSL Inspection for SharePoint ............................................................. 10
  Zscaler Internet Access Cloud Application Control ................................................................. 11
  Zscaler Digital Experience SharePoint User Experience ......................................................... 12

Configuring SharePoint SaaS Security ......................................................................................... 13

Adding the SharePoint Tenant ...................................................................................................... 14
  SaaS Tenant Configuration Wizard ......................................................................................... 15
Configuring the Zscaler Tenant on SharePoint ............................................................................ 16
  Finishing the Zscaler Tenant on Zscaler .................................................................................. 17
  The Completed and Active SharePoint API connector ............................................................ 18

Configuring SharePoint SaaS Data Loss Prevention ..................................................................... 19

Creating a DLP Policy .................................................................................................................. 19
  Creating a DLP Engine ............................................................................................................ 20
Configure a SaaS DLP Policy ....................................................................................................... 22
  SaaS DLP Policy Details .......................................................................................................... 23
  SaaS DLP Policy Wizard ......................................................................................................... 24

Configuring SharePoint SaaS Malware Detection ...................................................................... 26
### Appendix A: Requesting Zscaler Support

- **Gather Support Information** ......................................................................................... 64
- **Save Company ID** ........................................................................................................... 64
- **Enter Support Section** .................................................................................................... 65

---

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Malware Detection Policy</td>
<td>26</td>
</tr>
<tr>
<td>Configuring SharePoint Security Scan for DLP and Malware</td>
<td>28</td>
</tr>
<tr>
<td>The Scan Schedule Configuration</td>
<td>28</td>
</tr>
<tr>
<td><strong>SaaS Security Reporting and Visibility</strong></td>
<td>31</td>
</tr>
<tr>
<td>SaaS Assets and SaaS Assets Summary Report</td>
<td>32</td>
</tr>
<tr>
<td>SaaS Security Insights</td>
<td>33</td>
</tr>
<tr>
<td><strong>Configuring SSL Inspection for SharePoint</strong></td>
<td>34</td>
</tr>
<tr>
<td>Configuring SSL Inspection for SharePoint</td>
<td>35</td>
</tr>
<tr>
<td>Configuring an SSL Inspection rule</td>
<td>36</td>
</tr>
<tr>
<td>Verify SSL Inspection</td>
<td>38</td>
</tr>
<tr>
<td><strong>Zscaler Internet Access Cloud Application Control</strong></td>
<td>39</td>
</tr>
<tr>
<td>Zscaler Internet Access Cloud Application Control Policy</td>
<td>40</td>
</tr>
<tr>
<td>Zscaler Internet Access Cloud Application Control</td>
<td>41</td>
</tr>
<tr>
<td><strong>Zscaler Digital Exchange (ZDX) for SharePoint</strong></td>
<td>44</td>
</tr>
<tr>
<td>Configure ZDX for SharePoint</td>
<td>45</td>
</tr>
<tr>
<td>Configure ZDX for SharePoint</td>
<td>46</td>
</tr>
<tr>
<td>Configure Probes for SharePoint Monitoring</td>
<td>47</td>
</tr>
<tr>
<td>The ZDX Enabled SharePoint Application</td>
<td>48</td>
</tr>
<tr>
<td>Create an Alert for the SharePoint Service</td>
<td>49</td>
</tr>
<tr>
<td>The Triggered Alert for the SharePoint Service</td>
<td>55</td>
</tr>
<tr>
<td>Alert Detail for the SharePoint Service</td>
<td>56</td>
</tr>
<tr>
<td>The Sent Alert Email for the SharePoint Service</td>
<td>57</td>
</tr>
<tr>
<td>Using ZDX: The Dashboard</td>
<td>58</td>
</tr>
<tr>
<td>Application Overview</td>
<td>59</td>
</tr>
<tr>
<td>SharePoint Application Performance Detail</td>
<td>60</td>
</tr>
<tr>
<td>User Overview</td>
<td>62</td>
</tr>
<tr>
<td>SharePoint User Detail</td>
<td>63</td>
</tr>
</tbody>
</table>

---

Copyright 2022, Zscaler, Inc.
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Central Authority (Zscaler)</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC2409)</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security (RFC2411)</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Share Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (RFC6101)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC7239)</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
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 on Zscaler, visit www.zscaler.com or follow Zscaler on Twitter @zscaler.

Microsoft Overview

Microsoft (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 additional product and company resources, refer to:

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

Software Versions

This document was authored using Zscaler Internet Access and Zscaler Private Access (with Zscaler Client Connector) along with SharePoint Online Microsoft 365.

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Please 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.

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (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 our lightweight Zscaler Client Connector or PAC file (for mobile employees).

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

You get full protection from web and Internet threats. The Zscaler cloud platform supports cloud Firewall, IPS, sandboxing, data loss prevention (DLP), cloud access security broker (CASB), and browser isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides secure remote access to internal applications running on 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, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user’s device posture and extends a secure micro-tunnel 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZDX Help Portal</td>
<td>Help articles for ZDX.</td>
</tr>
<tr>
<td>Adding SaaS Application Tenant</td>
<td>ZIA help article for adding SaaS application tenants.</td>
</tr>
<tr>
<td>SaaS Security API DLP Policy</td>
<td>ZIA help article for creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications.</td>
</tr>
<tr>
<td>SaaS Security Insights</td>
<td>ZIA help article for viewing and defining information that you want to view when analyzing files scanned through charts.</td>
</tr>
<tr>
<td>SaaS Posture Security</td>
<td>ZIA help article on recommended security policies to decrease security risks for your organization’s SaaS applications.</td>
</tr>
<tr>
<td>SaaS Identity Proxy</td>
<td>ZIA help article for configuring Zscaler as an Identity Provider (IdP) for the following cloud apps.</td>
</tr>
<tr>
<td>About Data Loss Prevention</td>
<td>ZIA help article on different types of DLP policy rules.</td>
</tr>
<tr>
<td>About DLP Dictionaries</td>
<td>ZIA help article on creating custom dictionaries for DLP content.</td>
</tr>
<tr>
<td>About DLP Engines</td>
<td>ZIA help article on adding a custom DLP engine.</td>
</tr>
<tr>
<td>Cloud Application Access Control</td>
<td>ZIA help article on providing granular control over popular websites and applications.</td>
</tr>
<tr>
<td>ZDX Predefined Applications</td>
<td>ZIA help article on providing quick and seamless application onboarding for admins.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
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, Internet Explorer, Chrome, or 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. And it offers additional features and capabilities, such as modern site pages, modern web parts and authoring, modern lists and libraries, modern search, integration with PowerApps, Power BI and MS Flow, and SharePoint home page.

- **SharePoint Designer 2013.** A free program last released in 2013. Used to build powerful, workflow-enabled solutions. And used to 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>About SharePoint</td>
<td>Quick video on SharePoint uses, features, and applications.</td>
</tr>
<tr>
<td>SharePoint Community</td>
<td>A SharePoint community for news, announcements, and best practices.</td>
</tr>
<tr>
<td>SharePoint Support</td>
<td>Microsoft SharePoint support portal.</td>
</tr>
</tbody>
</table>
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, ease of use, and the ease of sharing they enable globally. But 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. Especially in today’s work from anywhere corporate infrastructures. Zscaler provides a complete SharePoint solution using our Zscaler Internet Services (ZIA) for security of SharePoint and our Zscaler Digital Access Exchange Service (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 our SaaS 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 ZIA SaaS security and ZDX SaaS monitoring operate as separate stand-alone services and are not dependent on one or the other. However, the two services working together provide a comprehensive solution for both security and operations of Microsoft’s SharePoint services.

This guide covers the following Zscaler Internet Access features for SharePoint Security, and the Zscaler Digital Experience 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
- Zscaler Internet Access Cloud Application Control
- Zscaler Digital Exchange (ZDX) for SharePoint

**Zscaler Internet Access CASB Data and Malware Protection for SharePoint**

The Zscaler CASB (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 our file collaboration SaaS partners by preventing data exposure and ensure compliance across the SaaS application.

*Figure 2. ZIA CASB SaaS security in use with SharePoint*

The Zscaler SaaS Security enables organizations to securely adopt and govern the use of multiple SaaS applications. It provides real-time visibility and controls access and user activity across sanctioned and unsanctioned applications. The fully integrated platform eliminates overlay architectures and simplifies policy creation and administration, ensuring data is protected and compliance is maintained.
What makes our SaaS Security unique?

- **Data exposure reporting and remediation.** Zscaler SaaS Security checks SaaS applications and cloud providers' configurations and compares them to industry and organizational benchmarks to report on violations and automate remediation.
- **Threat identification and remediation.** Zscaler SaaS Security checks SaaS applications for hidden threats being exchanged and prevents their propagation.
- **Compliance assurance.** Zscaler SaaS Security provides compliance visibility across SaaS and cloud providers and can mitigate violations automatically.
- **Part of a larger data protection platform.** The Zscaler Cloud Security Platform provides unified data protection with DLP and malware scanning capabilities for internet, data center, and SaaS applications, and ensures that public cloud applications are configured to prevent data exposure and maintain compliance. Zscaler also offers 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, please see Zscaler Resources.

**Zscaler Internet Access 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. This is where SSL decryption (also referred to as SSL visibility) comes in. 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. But 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 visibility for all inspectable destinations and enable security that provides cloud application control, DLP, file protection, sandbox, and malware protection.

This guide walks through enabling SSL inspection for SharePoint, allowing us to control and secure access and the data between organizations and the SharePoint Online site.

**Zscaler Internet Access Cloud Application Control**

The Zscaler Internet Access security cloud is a fully integrated cloud-based security stack that sits in-line between users and the internet, inspecting all traffic (including SSL) flowing between them. As part of the platform, Zscaler’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. While SaaS tenant security is referred to as out-of-band CASB for data-at-rest, Zscaler cloud application security is in-line CASB.

![Zscaler Internet Access Cloud Application Control](image)

**Figure 4. Cloud app control**

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

ZDX is the missing link needed for our customers and their SaaS applications. 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 ZIA SaaS security and can run with or without SaaS security 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 current ZIA clouds include zscaler.net, zscalerone.net, zcalerhtwo.net, zscalerthree.net, zscloud.net, zscalergbeta.net, and zscalergov.net.
Adding the SharePoint Tenant

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

- Select Administration
- Select SaaS Application Tenants
- On the SaaS Applications Tenants page select Add SaaS Application Tenant

Figure 7. ZIA SaaS application tenant
**SaaS Tenant Configuration Wizard**

To start the Wizard select **Add SaaS Application Tenant.** This opens the wizard. Select the SharePoint tile under popular applications to move to the next step in the wizard.

1. Select Add SaaS Application Tenant on the Tenant page.
2. Select the SharePoint tile on the wizard.

![Add SaaS Application Tenant](image)

**Figure 8. The SaaS tenant configuration wizard**

3. Give the SharePoint tenant a name. This is the name that is selected when assigning a policy for the Zscaler security features.
4. Enter a name for the **Tenant Name.**
5. Click on **Provide Admin Credentials.**

![Add SaaS Application Tenant](image)

**Figure 9. Open the SharePoint tenant**

This opens a new tab in your browser that asks to select an account.
Configuring the Zscaler Tenant on SharePoint

To configure the Zscaler tenant from your SharePoint Admin account.

1. Log in to SharePoint with administrator credentials.

![Login to the SharePoint tenant](image1.png)

**Figure 10. Login to the SharePoint tenant**

2. Verify and accept the requested permissions.

3. Select Accept.

![Accept SharePoint permissions](image2.png)

**Figure 11. Accept SharePoint permissions**
Finishing the Zscaler Tenant on Zscaler

Save and activate the configuration changes.

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

![Add SaaS Application Tenant](image)

**Figure 12. Finish the Zscaler tenant**

3. Verify the SharePoint tenant is **Active**.

![SaaS Application Tenants](image)

**Figure 13. The completed and active SharePoint tenant**
The Completed and Active SharePoint API connector

After adding and configuring the SharePoint tenant, you can configure the SaaS Security API Control DLP and malware policies and then Scan Configuration for the policies. You can also view reports and data for SharePoint in Analytics, SaaS Security Insights, and Logs.

![Zscaler policy configuration](image)

*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, but you could use one of the predefined libraries as well.

Then an engine is created that is the logical template for adding expressions and additional data. This is where you would specify the SharePoint-SSN-Scan Dictionary AND any other criteria for the policy. The engine precisely adds or removes data to match our violation and eliminates false positives.

Creating a DLP Policy

A SaaS security DLP policy is created that allows us to specify the detail about where, when, the action taken, and whom to inform about violations. Finally, the DLP policy is applied to our SharePoint tenant.

Let’s create our DLP dictionary as next steps. 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(\d{3}\d{2}\d{4}) ]
6. Select Save to save the dictionary

Figure 15. Creating a DLP dictionary
Creating a DLP Engine

A DLP engine needs to be created to provide the logic for the DLP library. This provides a template 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](image)

*Figure 16. Creating a DLP engine*
3. Give the DLP Engine a **Name**
4. In the **Engine Builder** under **Expression** select our 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. Select **Save** to save the configuration
8. **Activate** the configuration

**Figure 17. The DLP engine wizard**

**NOTE**
This policy triggers when we see the fourth Social Security number. Again, this is a demonstration, and the criteria is too general to be a production DLP rule.
Configure a SaaS DLP Policy

Now let’s apply the engine to a DLP policy that is used for our 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. And then select Add DLP Rule

![Figure 18. Launch the SaaS DLP policy configuration wizard](image)

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 which are processed in a specific order.

The first rule that matches is the applied rule. We specify the DLP engine we have defined, any file owners, groups, departments, and the file types to inspect. For our policy we 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 takes upon detecting 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, follow the steps below.

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 (or 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. Select **Save** and **Activate** to save and activate the policy

![Add DLP Rule](image)

*Figure 19. Completing the SaaS DLP policy configuration wizard*
The completed, activated, and enabled DLP policy.

**Figure 20.** Completing the SaaS DLP policy configuration wizard
Configuring SharePoint SaaS Malware Detection

Configuring the Malware Detection Policy

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

- Select Policy > SaaS Security API > Malware Detection
- Select Filesharing
- 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.
Once the malware detection rule wizard is visible:

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. Save and Activate the policy

![Add Malware Detection Rule](image)

*Figure 22. Adding a SaaS malware detection policy*
Configuring SharePoint Security Scan for DLP and Malware

The final configuration step for SaaS data scanning is to create the scan configuration. We 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 we select “All Data”. However, if this is a POV or a Trial, the only option available is New Data Only. To add a scan schedule.

- Select Policy > Scan Configuration > Add Scan Schedule

![Figure 23. Configure the scan](image)
In the wizard:

1. Select the SharePoint SaaS Tenant for 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 POV
4. Select Save to save the scan schedule

Figure 24. Scan configuration details

5. **Activate** the configuration
6. Start the scan by selecting the start arrow

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](image)

**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 our SaaS partners Zscaler provides reports and SaaS security insights. This provides visibility from a high-level overview to management of the individual logs and violations.

We will take a brief look at the tools, but for detailed information of the SaaS security analytics tools visit the Zscaler 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](image)

**Figure 28. Summary reports**

This opens SaaS Security Insights and the log data for each violation containing over 30 meta-data 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

---

**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. This is where SSL decryption (also referred to as SSL visibility) comes in. 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. But inspecting encrypted traffic is nontrivial and it requires a proxy architecture.

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 walks through the process of enabling SSL inspection for SharePoint, allowing us to control access and securing the data between our 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 Zcaler Cloud Instance may be different from the example.

![Login Page](image)

**Figure 31. ZIA tenant**

The current ZIA clouds include zscaler.net, zcalerone.net, scalertwo.net, scalertthree.net, zcloud.net, zscalerbeta.net, and zscaler.gov.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. **SSL Inspection**
3. **SSL Inspection Policy**
4. Click **Add SSL Inspection Rule**

![SSL Inspection](image)

*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 will be visited in another guide)
10. Select **Inspect** for the **Action**
11. **Save** and **Activate** the configuration changes

![Figure 33. SSL inspection rule wizard](image-url)
Verify SSL Inspection

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

NOTE

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

- Click the lock next to the SharePoint URL
- Select **Connection is secure**
- Select **Certificate is Valid**

Validate that you’re using the Zscaler Intermediate Root CA certificate instead of the SharePoint site certificate. This could be a custom certificate for your installation if it had been setup. See section [SSL Inspection Using a Custom Intermediate Root Certificate](#) in the ZIA online help portal for more detail if you believe this may be the case.

![Figure 34. Verifying SSL inspection for SharePoint](image.png)

We are now ready to configure and enable feature that require deep packet inspection now that we can see inside the packet to inspect the data.
Zscaler Internet Access Cloud Application Control

The Zscaler Internet Access security cloud is a fully integrated cloud-based security stack that sits in-line between users and the internet, inspecting all traffic (including SSL) flowing between them. As part of the platform, Zscaler Cloud Application Visibility and Control delivers full visibility into application usage, and granular policies ensure the proper use of both sanctioned and unsanctioned applications. While SaaS tenant security is referred to as out-of-band CASB for data-at-rest, Zscaler Cloud Application security is in-line CASB.

![Zscaler Internet Access Cloud Application Control](image)

**Figure 35. Cloud app control**

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

For most Microsoft 365 installations, the Zscaler OneClick configuration is enabled by default. The OneClick 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, we must re-enable SSL inspection as a first step. For this section we will enable SSL inspection and then enable cloud application policies controlling access and cloud app control for SharePoint.
Zscaler Internet Access Cloud Application Control Policy

To configure Zscaler Cloud Application access policies we will configure 2 rules. We will configure 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**

![Cloud App Control Policy](image)

*Figure 36. Cloud app control*

This starts the rule wizard.
Zscaler Internet Access 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. Save and Activate the configuration changes

![Figure 37. Cloud app control](image-url)
To create the SharePoint **Block Any Any** policy.

8. Select 2 for the **Rule Order**
9. Give the rule an intuitive name
10. Select **Enabled** for **Rule Status**
11. Select **SharePoint Online** for the **Cloud Application**
12. Select **Any User** and **Any Security Group**
13. Select **Block** for **Application Access**
14. Save and Activate the configuration changes

![Figure 38. Cloud app control](image-url)
The completed policies are shown.

![URL & Cloud App Control](image)

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 will be applied if no Match is found.

<table>
<thead>
<tr>
<th>Rule Order</th>
<th>Rule Name</th>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SharePoint</td>
<td>APPLICATIONS, SharePoint Online</td>
<td>Allow Application Access</td>
</tr>
<tr>
<td>2</td>
<td>SharePoint-Block-Any-Any</td>
<td>APPLICATIONS, SharePoint Online</td>
<td>Block Application Access</td>
</tr>
<tr>
<td>3</td>
<td>Office 365 One Click Rule</td>
<td>APPLICATIONS, Yammer, SharePoint Online, Microsoft Teams, Microsoft ...</td>
<td>Allow Application Access</td>
</tr>
<tr>
<td>4</td>
<td>UCaaS One Click Rule</td>
<td>APPLICATIONS, Zoom, RingCentral, LogMeIn</td>
<td>Allow Application Access</td>
</tr>
</tbody>
</table>

*Figure 39. Cloud app control*
Zscaler Digital Exchange (ZDX) for SharePoint

ZDX is the missing link our customers need for their SaaS applications. 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 ZIA SaaS Security 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 Into your organizations ZDX Admin Portal

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

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

1. Select Configuration
2. Select Applications
3. Select the blue arrow next to the SharePoint App
4. Enter the URL for your SharePoint Tenant Login
5. Select Submit to Onboard SharePoint

![Configuration Screen]

Figure 42. Onboard the SharePoint app
Configure Probes for SharePoint Monitoring

Clicking the Submit button enables the SharePoint app for monitoring, and the pre-configured probes are displayed. The probes consist of a CloudPath Probe which uses ICMP Trace Route, and a Landing Page Probe to the testmypacket.sharepoint.com location to monitor page load times.

We are going to make one change to the CloudPath 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. Select the blue pencil to edit the probe

*Figure 43. ZDX for user experience monitoring for SharePoint*
The ZDX Enabled SharePoint Application

The SharePoint application monitoring has now been activated, and our probes begin to monitor all our users that are using the Zscaler Client Connector. You can see Zscaler Client Connector running the ZDX with the service On.

![Figure 44. Active SharePoint monitoring](image)

*Figure 44. Active SharePoint monitoring*
Create an Alert for the SharePoint Service

As a final configuration step, let’s create an alert to email us when there is service degradation of the SharePoint application. An alert can be configured for **Network**, **Application**, or **Device** thresholds. An alert rule can be created with any of the below information:

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

To create our alert on page fetch times:

- Select **Alerts > Rules > Add New Alert Rule**

![Alerts and Rules Interface](image)

*Figure 45. Creating an alert*

This starts the **Add New Rule Alert** wizard
Step One of the Add New Rule Alert wizard:

- Name the Rule
- Select Enable Under Status
- Give the Alert an appropriate Severity
- Select a Type of Application
- Select Next

Figure 46. The alert creation wizard
Step Two of the Add New Rule Alert wizard.

- Select SharePoint as the application
- Select SharePoint Landing Page Probe
- Select Next

*Figure 47. The alert creation wizard*
**Step Three** of the Add New Rule Alert wizard creates the criteria for that triggers the alert by exceeding the threshold. We can use multiple variables here to eliminate false positive:

- Select Page Fetch Time
- Select the time to exceed 5000ms (5 Seconds)
- Select Next

![Add New Alert Rule](image)

*Figure 48. The alert creation wizard*
Step Four of the Add New Rule Alert wizard adds throttling to control the scope of the alert. We then define the Action as Email. The action can also be defined as an authenticated Webhook, which could be used to send the alert to a Slack channel:

- Enter “10” for the number of times the probe time must exceed our threshold
- Select 10 percent for the Minimum Number of Devices that must be impacted
- Select Email as the Delivery Method
- Enter the Alert Recipients email address separated by commas

![Add New Alert Rule Wizard](image)

*Figure 49. The alert creation wizard*
Our completed rule set for the alert.

![Completed Rule Set](image)

*Figure 50. The completed rule set*
The Triggered Alert for the SharePoint Service

You can see the triggered alert generated by our threshold settings in our rule set being exceeded. You can click on the **Rule Name** or click the eye to see more detail about the alert.

![Alerts and Rules](image)

**Figure 51. The alert**
Alert Detail for the SharePoint Service

You can see the triggered alert detail for our triggered alert 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 once our threshold was exceeded. Another email is sent when the threshold returns to normal values if the alert was an ongoing or continuous alert.

Figure 53. The alert email
Using ZDX: The Dashboard

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

*Figure 54. The dashboard*
Application Overview

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

- Select Applications
- Select the SharePoint App

![Applications Overview](image)

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 briefly. We also see our probe data, with minimum, maximum, and average response times.

<table>
<thead>
<tr>
<th>Impacted Departments</th>
<th>Impacted Regions</th>
<th>Impacted Zscaler Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZDX Score per Department</td>
<td>ZDX Score per Region</td>
<td>ZDX Score per Zscaler Location</td>
</tr>
<tr>
<td>88</td>
<td>88 Texas</td>
<td>88 Road Warrior</td>
</tr>
</tbody>
</table>

**Probe Status**

- SharePoint Online Login Page
- SharePoint Online CloudPath Probe
- Cloud Path
- Packet Loss
  - Min: 0% Avg: 0% Max: 18%
- End-to-end
  - Min: 1ms 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 and then Apply to see all SharePoint users. The ZDX score is provided, and users can be selected by a Poor, Okay, or a Good ZDX score. You can get more detail on the user by clicking the name or the eye on the right. Select a user to bring up more detail.

Figure 58. User overview
SharePoint User Detail

The User Detail shows an incredible amount of useful 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 on 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.

Gather Support Information

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

![Company Profile](image)

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

**Save Company ID**

Copy your Company ID.

![Company Profile](image)

*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*