



# Best Practices for Implementing Access to Microsoft 365 with Zscaler™

Authors:

**Naresh Kumar,**

Director Product Management, Zscaler

**Misha Kuperman,**

Sr. VP Cloud Operations, Zscaler



This document was authored by Zscaler. All best practices and technical recommendations have been developed based on Microsoft's recommended principles for Microsoft 365 connectivity (<https://aka.ms/pnc>) in close collaboration and review with Microsoft product groups.

## Table of contents

<b>Introduction</b>	<b>4</b>
Purpose	4
Intended audience	4
What is Microsoft 365?	4
Microsoft connectivity principles	4
What is Zscaler Internet Access?	5
Microsoft-recommended one-click	5
Benefits of using Zscaler with Microsoft 365	6
<b>Network transformation</b>	<b>7</b>
Local internet breakouts	7
Peering optimization with Microsoft	7
Verify local internet breakout coverage on Zscaler	7
<b>Network deployment options for Microsoft 365</b>	<b>8</b>
Microsoft 365 networking goals	9
<b>Deployment best practices with Zscaler</b>	<b>9</b>
Traffic forwarding	9
Configuring Microsoft-recommended one-click	15
Recommended firewall policy	16
All ports and protocols traffic forwarding	17
<b>Value-added services with Zscaler</b>	<b>18</b>
Tenancy restrictions	18
Blocking personal tenants	19
Bandwidth control	22
<b>Summary</b>	<b>22</b>

## Introduction

### **Purpose**

This paper discusses best practices and recommendations for customers on how to configure their Zscaler Internet Access™ (ZIA™) solution for the optimal Microsoft 365 performance, security, and user experience. These recommendations have been developed based on Microsoft's recommended principles for Microsoft 365 connectivity (<https://aka.ms/pnc>).

### **Intended audience**

This document is intended for IT administrators who want to use ZIA with Microsoft 365 solutions. Familiarity with ZIA is assumed, as is familiarity with other technologies, including web security and network security, Active Directory, identity management, and directory services.

### **What is Microsoft 365?**

Microsoft 365 (formerly known as Office 365) is a suite of cloud-based services designed to help meet your organization's needs for robust security, reliability, and user productivity. Instead of buying and installing a new version of the suite whenever you need to upgrade, the products are updated automatically so that users always work with the most current versions. Microsoft 365 provides its suite of applications from the cloud through the browser. The license follows each user across devices, providing a consistent experience offline or online, across all supported devices. In addition to the familiar suite of Office products—Word, Excel, PowerPoint, and Outlook—Microsoft 365 includes OneDrive, Microsoft Teams, SharePoint, Yammer, and OneNote.

For more information, see [What is Microsoft 365?](#) and [Microsoft 365 Support](#).

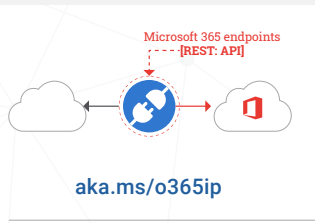
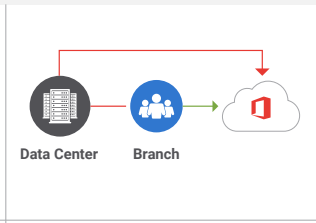
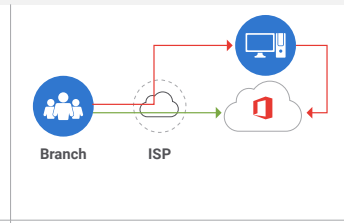
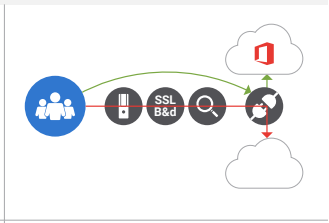
Note: Microsoft 365 is delivered to customers across several clouds, including World-Wide Commercial Cloud, U.S. Government Cloud, Germany Cloud, and China Cloud. The information in this paper applies to Zscaler for Microsoft 365 World-Wide Commercial Cloud.

### **Microsoft connectivity principles**

Microsoft 365 has become the standard productivity platform for the majority of organizations, large and small, around the world. It is an easy-to-use, cost-effective solution with flexible collaboration features, making it a compelling choice for many organizations.

Microsoft recommends the following principles to achieve optimal Microsoft 365 connectivity and performance. Use the Microsoft 365 connectivity principles described in this document to manage your traffic and get the best performance when connecting to Microsoft 365.

## Microsoft 365 Network Connectivity Principles

 <p>Microsoft 365 endpoints [REST: API]</p> <p>aka.ms/o365ip</p>	 <p>Data Center Branch</p>	 <p>Branch ISP</p>	
<p><b>Optimize Microsoft 365 traffic</b></p> <p>Use the endpoint categories to differentiate Microsoft 365 traffic for more efficient routing.</p>	<p><b>Enable local egress</b></p> <p>Egress Microsoft 365 data connections through internet as close to the user a practical with matching DNS resolution.</p>	<p><b>Enable direct connectivity</b></p> <p>Enable direct egress for Microsoft 365 connections. Avoid network hairpins and minimize network latency (RTT) to Microsoft global network.</p>	<p><b>Modernize security for SaaS</b></p> <p>Avoid intrusive network security for Microsoft 365 connections. Assess bypassing proxies, traffic inspection devices, and duplicate security already available in Microsoft 365.</p>

### Microsoft 365 Networking Partner Program

Zscaler Internet Access (ZIA) has been validated to work with Microsoft 365. ZIA's qualification under this program provides several preset performance and operational optimizations that—in combination with the best practices outlined in this document—allow you to make the right deployment choices for an optimal configuration. You can learn more about the Microsoft 365 Networking Partner Program [here](#).

### What is Zscaler Internet Access (ZIA)?

ZIA is a secure internet and web gateway delivered as a service from the world's largest, purpose-built security cloud. ZIA provides a full security stack with all the in-depth protection needed by enterprises of any size. ZIA is a key component of the Zscaler Zero Trust Exchange™, a cloud-native platform that securely connects users, apps, and devices over any network, in any location using business policies to increase user productivity, reduce business risk, slash costs, and simplify IT.

Zscaler has partnered with Microsoft to help enterprises migrate from on-premises deployments to the Microsoft 365 cloud. Our deep integration adopts the network principles recommended by Microsoft for an optimal user experience and secure connectivity, enabled through a simple one-click configuration.

### Zscaler one-click configuration for Microsoft 365

Zscaler simplifies administration, improves control, and increases visibility into Microsoft 365 activity with one-click configuration.

## Zscaler One Click Configuration

Simplify day-to-day Microsoft 365 administration

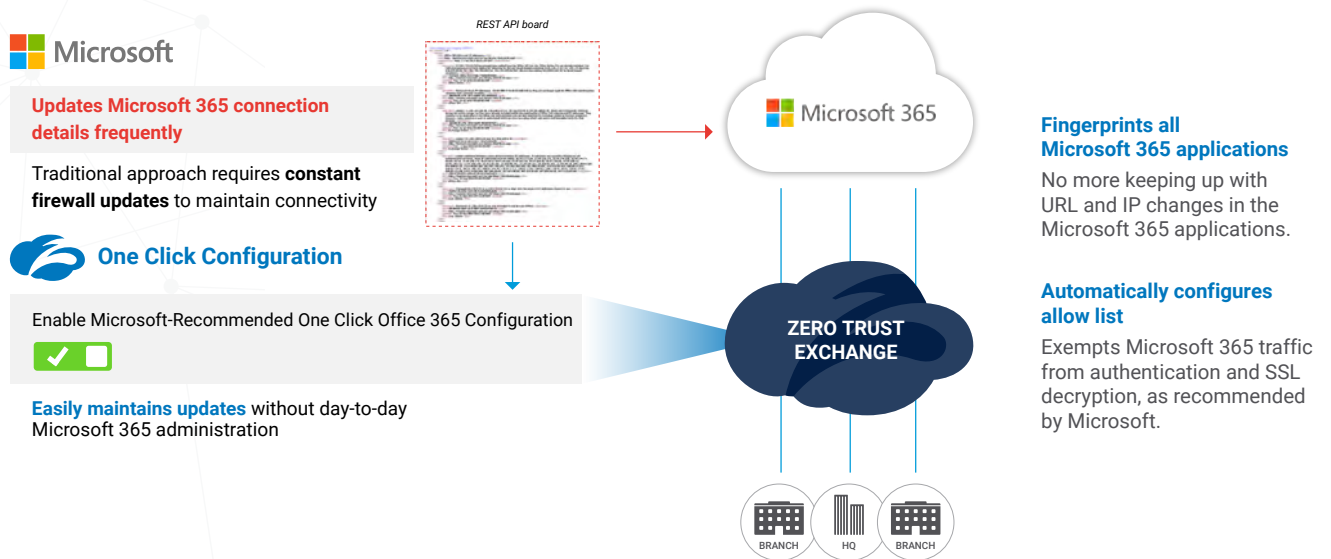


Figure 2 – Zscaler one-click configuration for Microsoft 365

### Benefits of using Zscaler with Microsoft 365

Zscaler's one-click configuration for Microsoft 365 provides many benefits:

#### 1. Deployment

- Access Microsoft 365 & internet traffic locally, at any location, without any on-premises network security hardware to deploy & manage.

#### 2. Management

- Automate administration of Microsoft 365 IP & URL changes to ensure connections are not blocked or inspected in compliance with M365 connectivity principles.

#### 3. Optimization

- The Zscaler cloud peers with Microsoft's global network, as well as major ISPs around the world, to optimize end user-traffic to the Microsoft 365 front door.
- Reduce latency with Zscaler's fast & local DNS services to connect users to the closest Microsoft 365 front door.

There are additional benefits Zscaler provides with features such as Bandwidth Control, Zscaler Client Connector, TCP Window Shaping, UDP support, and dashboard visibility, all of which enhance the experience for end-users.

## Network transformation

### Local internet breakouts

While the popularity of Microsoft 365 is at an all-time high, many companies new to Microsoft 365 do not have the proper network architecture to fully take advantage of its cloud-native apps and services.

Many organizations rely on a hub-and-spoke network to route traffic from branch offices through a central data center, where applications are hosted and security controls are applied. This architecture vastly increases latency and denigrates the overall user experience for applications like Microsoft 365. Microsoft 365 is a distributed cloud service with distributed front doors in close geographical/network proximity to users; in this context, hub-and-spoke networks add significant latency, impacting user experience and application performance.

Both Microsoft and Zscaler recommend establishing a local network egress as close as possible to the user. One of the core **connectivity tenets of Office 365**, also known as “Egress network connections locally,” helps minimize latency on user traffic by means of enabling local egress and DNS for users inside or outside the corporate network. Reducing latency yields the best Microsoft 365 user experience, so the quicker you can get your user to egress—avoiding the corporate network, VPN, or DNS hairpins—the better.

### Local internet breakout considerations

- Zscaler has globally deployed data centers for low latency and resilient connectivity with local end-user populations.
- Customers should consider not only the geographical location of its data center(s), but also round-trip delay and packet loss metrics during business hours.

To best assess the optimal locations, customers should consult <https://config.zscaler.com/> and collect latency and loss data during local business hours to primary, backup, and tertiary sites. For more details, please contact support or your account team. Zscaler also supports a self-provisioning capability for setting up GRE tunnels through the admin portal.

To ensure optimal connectivity, it's important that customers set up connectivity at every branch office to the Zscaler cloud.

### Routing/peering optimization with Microsoft

Zscaler peers with Microsoft in major data centers globally.

As part of the standard rollout for any customer that expresses a need or desire for peering, Zscaler works to identify the data centers that are connected to the internet exchanges, which are then directly peered with the Microsoft Network.

## Zscaler Cloud Platform - Simple, Fast and Reliable

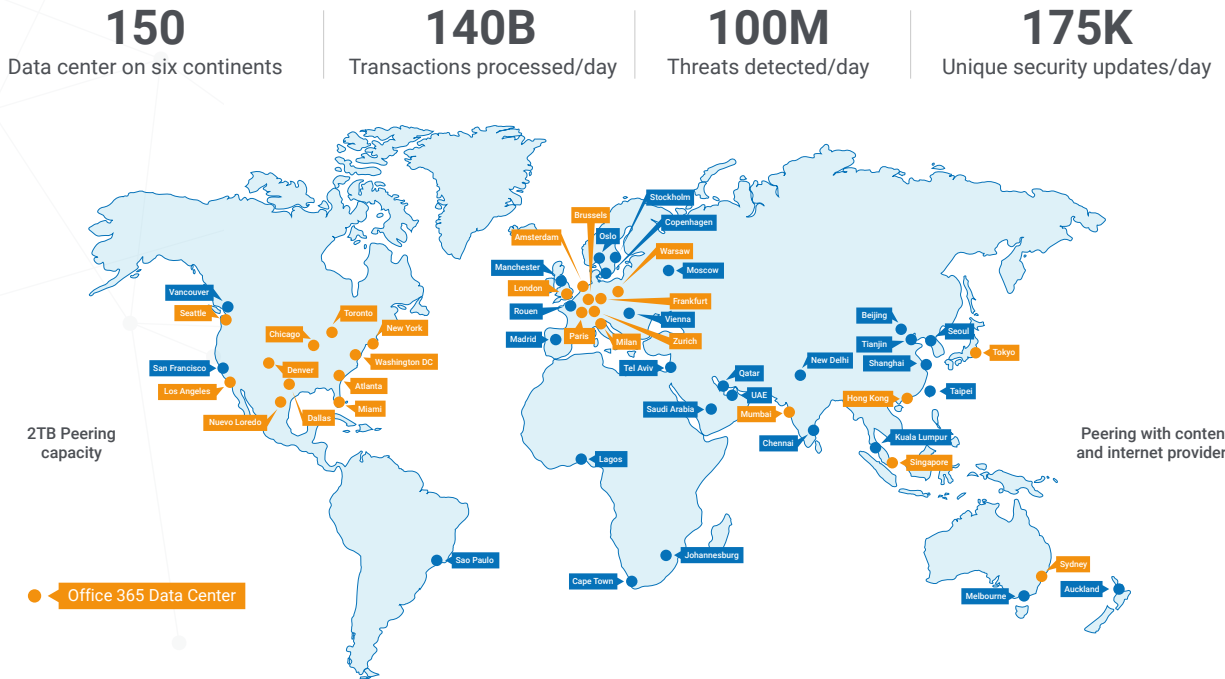


Figure 3 – Zscaler global cloud footprint

And since Zscaler has an open peering policy (meaning Zscaler will peer with any content or service provider), this performance may be extended to other key services as well.

There are three key recommendations for enabling local internet breakouts:

- Identifying the locations/sites: Many enterprise customers have architected their networks in hub-and-spoke models with a limited number of locations egressing traffic directly to the internet. As you plan for local internet breakouts, prioritize locations with the largest volumes of traffic and the greatest backhauling distance over the private network.
- Choose the right traffic-forwarding method to Zscaler.
- Enable Microsoft 365 one-click configuration to have recommended and dependable connectivity to Microsoft 365 applications and services.

### Network deployment options for Microsoft 365

Microsoft 365 is a distributed software-as-a-service (SaaS) cloud that provides productivity and collaboration services through a diverse set of applications and microservices. Many of the applications and services interact between the end-user and data center in a unique way to accomplish the application or service's intended goal. With this in mind, deployment tactics may vary to maintain end-user experience standards for reliability and speed.



## Microsoft 365 networking goals

The ultimate goal of Microsoft 365 networking is to optimize the end-user experience by enabling the fastest, most direct connections between clients and the closest Microsoft 365 front doors via the nearest Microsoft Network POP. The quality of the end-user experience is directly related to the performance and responsiveness of the connection supporting the cloud app. For example, Microsoft Teams relies on low latency so that user phone calls, conferences, and shared-screen collaborations are glitch-free, while Outlook relies on great networking connectivity for instant search features that leverage server-side indexing and AI capabilities.

Therefore, the primary goal in the network design should be to minimize latency by reducing the round-trip time (RTT) from client machines to the Microsoft Global Network, Microsoft's public network backbone that interconnects all of Microsoft's data centers with low-latency, high-availability cloud application entry points spread around the world.

To achieve this goal of low latency, **Microsoft has established Microsoft 365 Networking Connectivity Principles**. Furthermore, the Microsoft 365 Networking Partner Program helps facilitate a customer's ability to improve its Microsoft 365 experience through the easy discovery of validated partner solutions that consistently demonstrate alignment to the key principles for optimal Microsoft 365 connectivity in customer deployments. Zscaler is one of a very select number of security vendors in the Microsoft 365 Networking Partner Program.

## Deployment best practices with Zscaler for Microsoft 365

### Traffic forwarding:

There are four primary ways to forward traffic to Zscaler Internet Access:

- GRE tunnels
- IPsec tunnels
- Zscaler Client Connector
- PAC file

Forwarding traffic from a corporate location (data center, branch, etc.)

To send traffic to the Zscaler service, either the originating client or an intermediary node (gateway) must communicate directly with Zscaler data centers (either ZIA Public Service Edge or ZIA Private Service Edge) for policy enforcement.

A corporate location should build diverse tunnels to Zscaler data centers to carry internet-bound traffic through the Zscaler security platform. GRE and IPsec are supported VPN tunneling options at locations for forwarding traffic to the Zscaler platform. Zscaler recommends GRE tunnels, especially for larger corporate locations.

To learn more, visit <https://help.zscaler.com/zia/best-practices-deploying-gre-tunnels>.

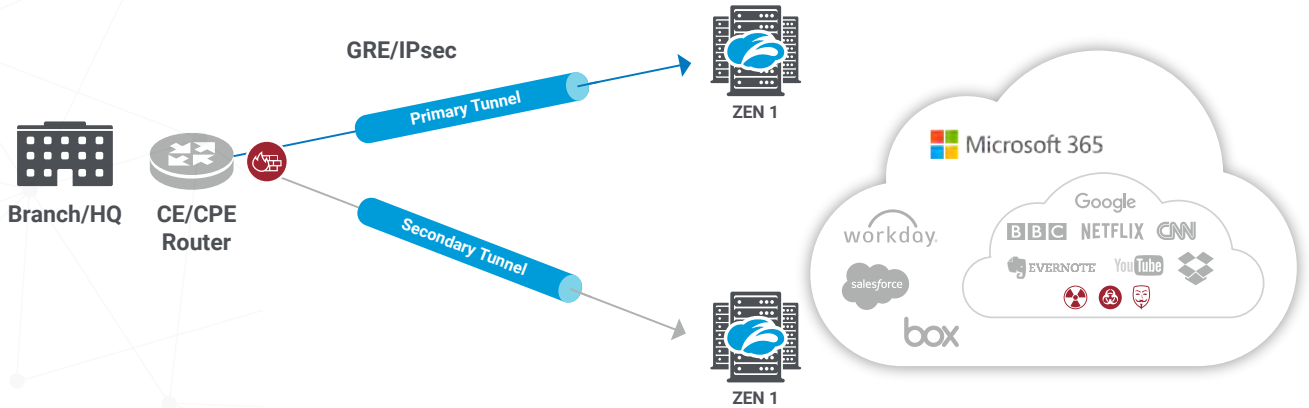


Figure 4 – Traffic forwarding

Typically, it is recommended that a client-based method of traffic forwarding, such as the Zscaler Client Connector (formerly known as Zscaler App), coexist with the tunnel configuration at a site for the purposes of granular traffic steering. This provides control mechanisms for such items as source-IP-restricted applications and the reduction of redundant DNS resolution when possible.

### MTU/MSS settings:

With GRE or IPsec, it is important to understand the underlying transport mechanism when sending traffic to the Zscaler service. Settings, such as the MTU (maximum transmission unit—the largest packet size) and MSS (maximum segment size—essentially the amount of data sent in a packet), become more relevant when sending traffic over a tunnel. If the packets are too big in either case, TCP will usually still work but will fragment packets unnecessarily.

It is important that, when creating tunnels to the Zscaler service, these values be calculated properly for the organization. Zscaler provides example configurations and calculations, which can be found at: <https://help.zscaler.com/zia/determining-the-optimal-mtu-for-gre-or-ipsec-tunnels>. But these should still be calculated at the time of tunnel creation to ensure the optimal TCP experience for the organization.

### Monitoring tunnels:

It is natural and desirable to monitor the tunnels. The tunnels should be monitored at Layer 7; this is due to the nature of a cloud service. Monitoring by IP address is ineffective, as particular machines that comprise the cloud architecture may go in and out of service without affecting the overall service. IP checks against these machines may erroneously show something down when the service is operating normally.

Zscaler recommends a Layer 7 health check through the tunnel to <http://gateway.zscalerone.net/vpntest> in addition to any IP SLA checks for the tunnel itself. Please see the following link for additional information: <https://help.zscaler.com/zia/best-practices-deploying-gre-tunnels>.

It is also possible to forward using only client-based methods from small sites, but tunnels are preferred and recommended. Some best practices recommendations are below for internet-bound traffic in general.

### **Locations with tunneling:**

- All TCP/UDP/ICMP traffic from all client devices at a corporate office should be forwarded through a GRE or IPsec tunnel to Zscaler.
- Enable authentication, SSL decryption, bandwidth control.
- Enable surrogate IP for the location.
- Intelligent devices, such as laptops that will move in and out of the corporate environment, should use Zscaler Client Connector for trusted network detection and traffic-forwarding control.

**Locations that CANNOT support tunneling:** At offices where tunneling is not an option, Zscaler Client Connector should be used to forward traffic to Zscaler. If Client Connector is not a feasible option, a standalone PAC file can be used as an alternative (but is not recommended).

### **Remote user traffic forwarding**

As users take advantage of mobile technology, whether using laptops or iOS/Android devices, Zscaler Client Connector is the recommended approach to ensure traffic is forwarded to the Zscaler cloud regardless of device location.

Zscaler Client Connector will detect the trusted network status and forward traffic to Zscaler appropriately based on whether the user is on the corporate network, on a traditional VPN, or completely off the corporate infrastructure. Zscaler Client Connector provides a few benefits over a PAC file that should be considered:

- Captive portal detection
- Trusted network detection
- User identification and authentication is handled by Zscaler Client Connector rather than the browser

If Client Connector is not a feasible option, then a standalone PAC file can be used as an alternative (but is not recommended)

### **On VPN:**

Full tunnel:

- Full tunnel without Zscaler split: If it is desired to force internet traffic through the tunnel, then Client Connector should be configured to behave as it does on a trusted network such that all traffic is routed back to the data center for forwarding as if attached to the corporate network. Of course, if a PAC file is used instead of Client Connector, then that PAC file would continue to operate over the tunnel.
- Full tunnel with Zscaler split: If it is desired, Client Connector traffic can be excluded from forwarding through the tunnel by exempting Zscaler subnets from the tunnel configuration. This will allow Client Connector to enforce policy control directly at the nearest Zscaler data center to the end-user, rather than hauling the internet traffic back to the data center. In this case, if a PAC file is used, it could operate in a similar fashion to Client Connector.

Split tunnel:

- If split tunneling is already allowed, then Client Connector should be used to forward traffic to Zscaler. If Client Connector is not a feasible option, then a standalone PAC file can be used as an alternative.

**Off VPN:** Client Connector should be used to forward traffic to Zscaler.

### **Microsoft 365 and Teams with Zscaler Client Connector for mobile/remote users:**

Microsoft published guidelines for work-from-anywhere (WFA) users and a strategy to split the most performance-sensitive Microsoft 365 applications, which need optimized connectivity from VPN tunnels. These applications include Microsoft Teams, Exchange Online, and SharePoint Online.

(<https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide>).

For an optimal user experience, Zscaler recommends split tunneling IP ranges for Teams traffic from Zscaler Client Connector for work-from-anywhere users only. For location traffic, the best practice is to forward traffic via tunnels configured to Zscaler Public Edge Connectors.

Steps to split specific traffic for WFA users:

- Deploy Zscaler Client Connector (Ver 2.0 or later with Z-Tunnel 2.0) for all WFA users. To learn more about deployment, go to: <https://help.zscaler.com/z-app/best-practices-deploying-z-tunnel-2.0>
- Login to the Zscaler admin portal and go to the Zscaler Client Connector portal: Policy->Zscaler Client Connector portal
- Add Microsoft Teams under Application bypass as shown below: App Profile->Windows->Add Windows Policy ( modify existing profile as needed) Under Z-Tunnel 2.0 configuration ->Application bypass ->selected

Add Microsoft Teams as shown below:

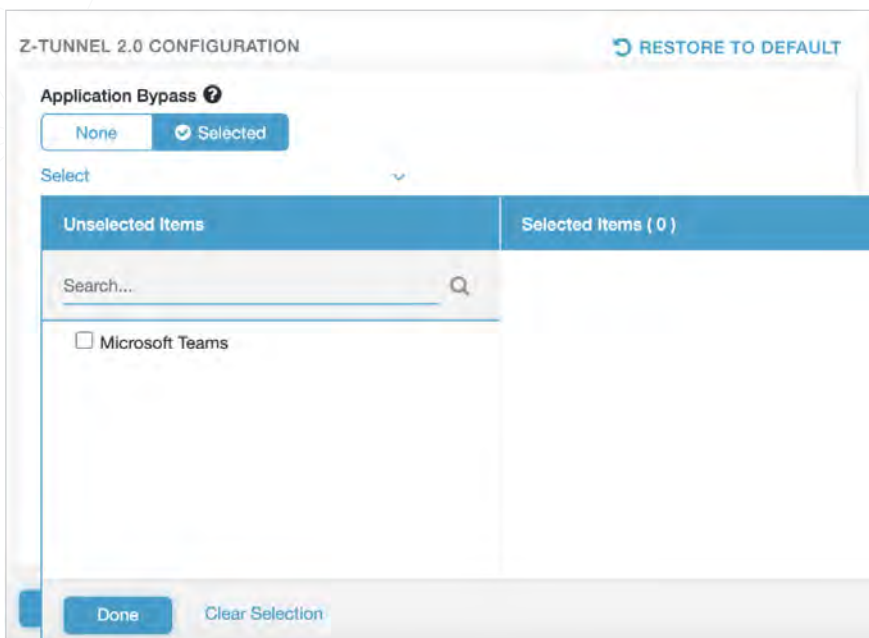


Figure 5 – Add Microsoft Teams to Client Connector

Note: Zscaler maintains the IP ranges and ports for the Microsoft Teams service. Here is the list of dedicated Microsoft 365 IP ranges and UDP ports covered under the above bypass selection:

13.107.64.0/18

52.112.0.0/14

52.120.0.0/14

UDP 3478, 3479, 3480, and 3481

If customers choose to bypass more than the Microsoft Teams service, the below configuration can be used to add more optimized endpoint IP ranges and ports manually.

Please note: customers that do this should also plan to maintain the related exclusion lists regularly.

App Profile->Windows->Add Windows Policy ( modify existing profile as needed)

Under Z-Tunnel 2.0 configuration ->Destination exclusion, add IP ranges

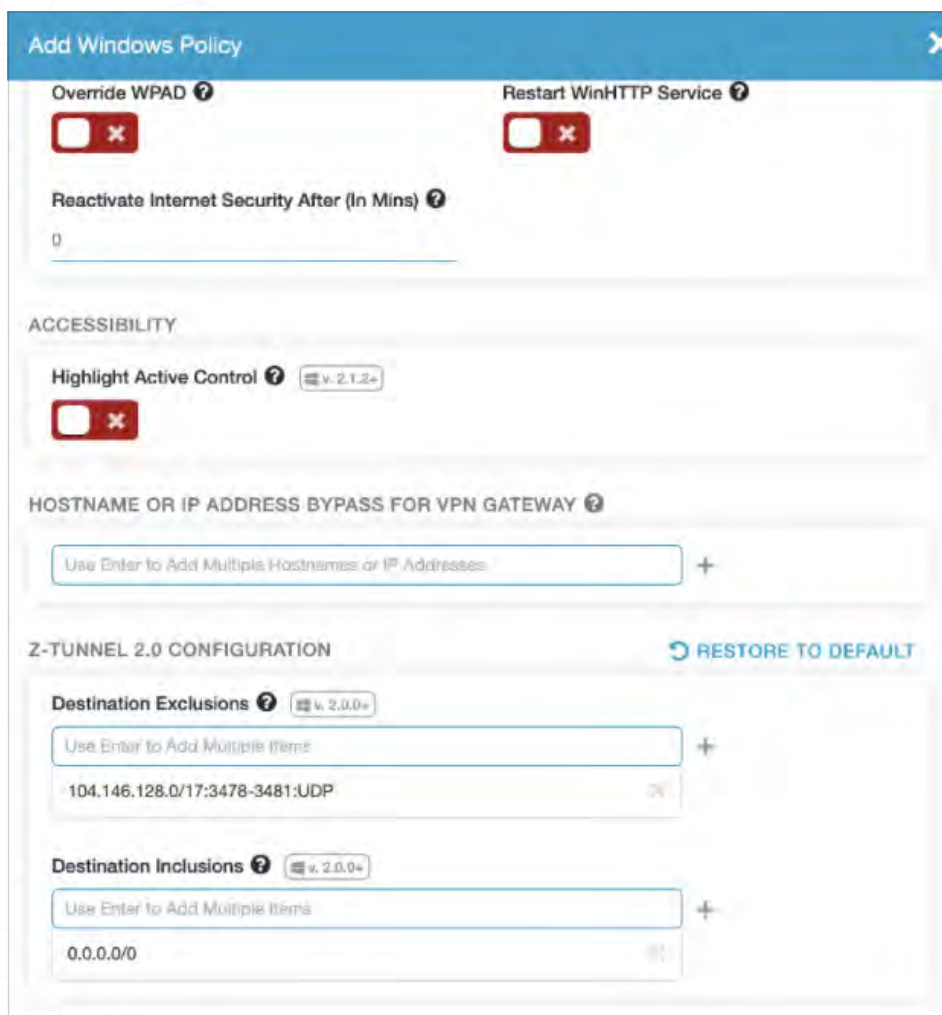


Figure 6 – Add IP ranges

For more details on optimized endpoint IP ranges, check here:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide>

### **PAC file challenges:**

PAC file deployment has many limitations with both visibility and secure access controls. Zscaler strongly recommends against forwarding traffic using PAC files. Challenges with PAC files include:

- PAC file management is often very complex due to exception handling and updates.
- PAC file errors are hard to troubleshoot.
- PAC files only affect web traffic and can have a performance impact if not handled properly for collaboration applications.
- Improper handling of PAC files (DIRECT) can introduce security risks.

PAC files hinder usability and management while decreasing security. To get the best performance and security with Zscaler Internet Access and Microsoft 365, Zscaler Client Connector is recommended.

### **Zscaler Private Service Edge considerations**

From an architectural point of view, there is no technological difference between Zscaler Private Service Edge except for the organizational restrictions. Customers that have deployed a hybrid environment should make the same consideration for Zscaler Private Service Edge and add it to the trusted IP ranges.

### **Configure Microsoft-recommended one-click configuration**

To provide the best-performing and most secure user experience, Microsoft 365 applications use a wide variety of protocols, connection optimizations, strong in-transit encryption technologies, and advanced security checks for their connections and traffic going to Microsoft 365. Many of these connections are also sensitive to inline network protocol and data processing, inspection, and pre-authentication actions. For these reasons Microsoft does not recommend and does not offer support for inline network decryption and inspection of Microsoft 365 traffic (more information at <https://docs.microsoft.com/en-us/office365/troubleshoot/miscellaneous/office-365-third-party-network-devices>).

Zscaler Internet Access fully complies with these Microsoft recommendations for Microsoft 365 traffic by implementing “One-click Microsoft 365 configuration.” When one-click configuration is enabled (on by default), Microsoft 365 traffic is optimized through the Zscaler systems and bypasses SSL inspection and pre-authentication layers for the fastest performance and best interoperability.

Enable the setting under Policy->URL and Cloud App policy->Advanced Policy Settings in the admin portal:

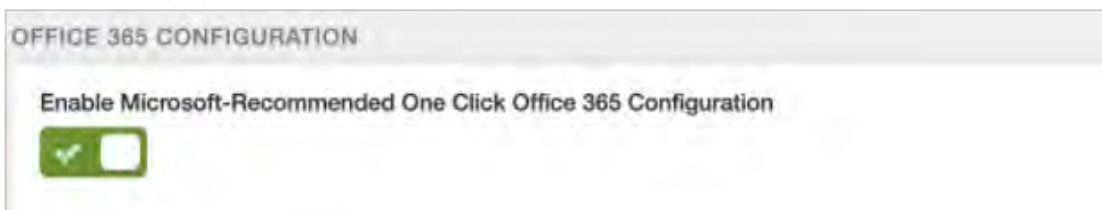


Figure 7 – Enabling one-click configuration

Once this setting is enabled and activated, two automated policies get created in the Zscaler firewall:

1. Policy to identify (based on REST API) and bypass SSL and authentication, avoiding security stack to minimize latency:

Rule Order	Rule Name	Criteria	Action
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow

Figure 8 – SSL bypass policy

2. DNS policy to optimize the path and connect to the nearest front door application endpoint:

Rule Order	Rule Name	Criteria	Action
1	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow

Figure 9 – DNS policy

### Recommended firewall policy

As many customers leverage ZIA for forwarding all web application traffic, below is the recommended firewall policy under Policy->Firewall Control as one-click configuration automatically ingests a default policy to handle Microsoft 365 traffic.

Note: Rule No. 1 below is not required. Microsoft 365 will work without that, but it is the recommended policy for firewall today for other web traffic to work.

### Recommended policy

Scenario: Location connected using GRE/IPSec with Auth, SSL, FW enabled. Microsoft Office365 One click enabled, NO URL policies specific to M365 and ONLY Firewall Policies like below.

Rule Order	Rule Name	Criteria	Action
1	Zscaler Proxy Traffic	DESTINATION IP CATEGORIES Zscaler Proxy IPs  NETWORK SERVICES Zscaler Proxy Network Services	Allow
2	Allow_HTTP_HTTPS_TRAFFIC	NETWORK SERVICES HTTP; HTTPS	Allow
3	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow
Default	Default Firewall Filtering Rule	Any	Block/Reset

Figure 10 – Recommended firewall policy

Note: We don't need to add 9440 to Rule 1 because ZEN will automatically forward all 9440 traffic to Proxy. So no need to configure explicitly.



Result: Able to login into S4B and able to make audio/video calls, desktop sharing. Since HTTP/HTTPS able to login into outlook-2016, word, put etc.

### Verify local internet breakouts with Zscaler

To understand an organization’s local internet breakouts, take the following steps:

Step 1: In the ZIA admin portal, go to Administration->Location Management->Locations to find the total number of locations.

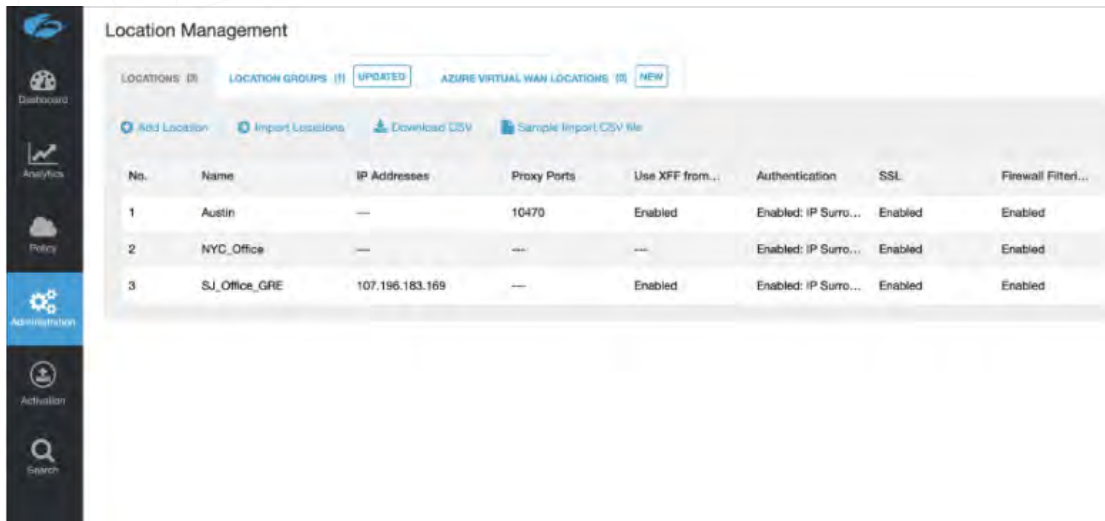


Figure 11 – Local internet breakouts shown in admin portal

Step 2: Go to Dashboard->Microsoft 365 dashboard to look for the “Top Office 365 Locations” widget to identify the number of locations with local breakouts enabled.



Figure 12 – Locations with local breakouts

### All port and protocol traffic forwarding

Microsoft 365 is the major driver for local internet breakouts for many enterprises. Customers can take the advantage of direct-to-internet access at branch and regional locations for all SaaS applications and internet destinations with the Zscaler cloud security platform.

For a better user experience and call quality with applications such as Skype for Business and Microsoft Teams, it is important to send all audio and media traffic (UDP) from locations through the local internet egress as well.

Recommendation: Zscaler recommends sending all internet-bound traffic leveraging Cloud Firewall functionality to protect all web and non-web application traffic.

## Value-added services with Zscaler

### Tenancy restriction controls

Microsoft's tenant restrictions give organizations the ability to specify the list of tenants that their users are permitted to access. Azure AD then grants access only to these permitted tenants.

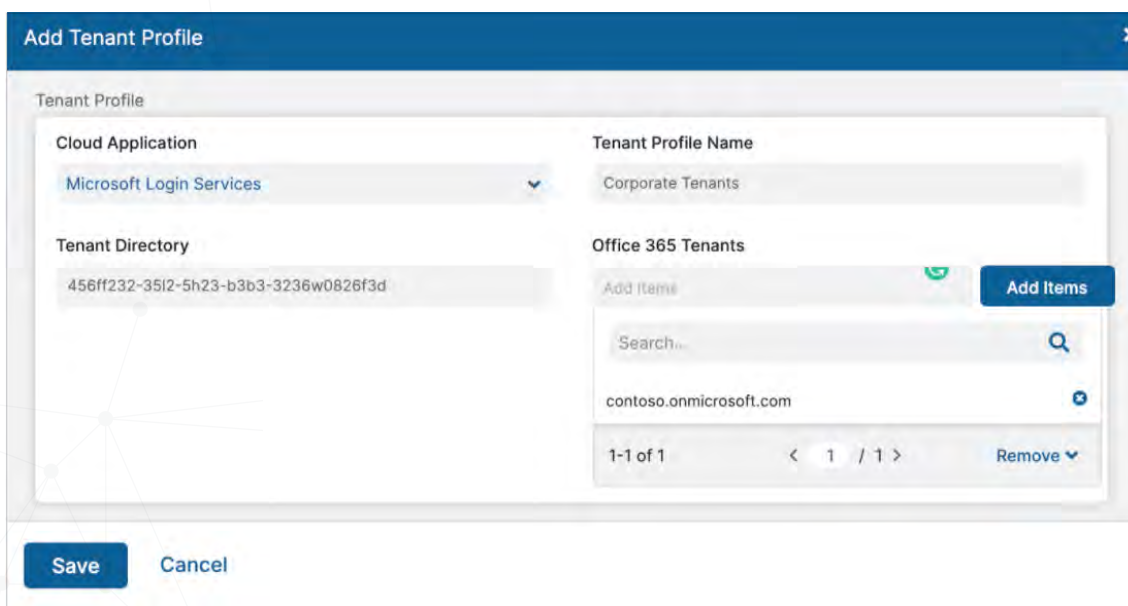
For each incoming request to the below domains, the ZIA Public Service Edge inserts two HTTP headers: Restrict-Access-To-Tenants and Restrict-Access-Context.

- login.microsoftonline.com
- login.microsoft.com
- login.windows.net

Apart from these three domains, Zscaler will not insert restrictive headers to any other domain.

To enable tenant restriction on admin portal, follow the below steps:

1. Create tenant profile under Administration ->Tenant Profiles in the admin portal:



The screenshot shows a dialog box titled "Add Tenant Profile" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Tenant Profile**: A sub-header for the main form.
- Cloud Application**: A dropdown menu currently showing "Microsoft Login Services".
- Tenant Profile Name**: A text input field containing "Corporate Tenants".
- Tenant Directory**: A text input field containing the GUID "456ff232-35f2-5h23-b3b3-3236w0826f3d".
- Office 365 Tenants**: A section for adding tenants, featuring an "Add Items" button with a green checkmark, a search input field with "Search..." and a magnifying glass icon, and a list of tenants. One tenant, "contoso.onmicrosoft.com", is listed with a blue plus icon to its right. Below the list is a pagination indicator "1-1 of 1" and a "Remove" button with a dropdown arrow.

At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Figure 13 – Tenancy restriction controls

2. Enable tenant restrictions within cloud app policies Policy->URL and Cloud App policy->IT services (category) ->Microsoft Login Services

### Add IT Services Rule

Tenant restrictions corporate Enabled

**CRITERIA**

<b>Cloud Applications</b> Microsoft Login Services	<b>Users</b> Any
<b>Groups</b> Any	<b>Departments</b> Manufacturing; Product Mgmt; Servic...
<b>Locations</b> Any	<b>Location Groups</b> Any
<b>Time</b> Always	<b>User Agent</b> Any

**RULE EXPIRATION**

Enable Rule Expiration

**ACTION**

<b>Application Access</b> Allow Block	<b>Daily Bandwidth Quota (MB)</b> Enter Text
<b>Daily Time Quota (min)</b> Enter Text	<b>Tenant Profile</b> corporate

SSL Inspection Required

Save Cancel

## Blocking personal tenants

Zscaler provides tenant restriction controls to handle personal Outlook and personal OneDrive accounts to protect enterprises from data exfiltration and advanced threats. Zscaler can inspect the personal Outlook and OneDrive traffic and protect against phishing attacks.

In the Zscaler admin UI, configure as follows:

Policy->URL and Cloud app policy->cloud app policy->File hosting ( OneDrive)

Policy->URL and Cloud app policy->cloud app policy->Webmail ( Outlook)

**Add File Sharing Rule** [X]

**CLOUD APP CONTROL RULE**

Rule Order: 2 [v]  
Rule Name: File\_Sharing\_2 [v]  
Rule Status: Enabled [v]

**CRITERIA**

Cloud Applications: Any [v]    Users: Any [v]

Unselected Items	Selected Items ( 1 )
onedrive [x] [Q]	OneDrive (Personal)
<input type="checkbox"/> OneDrive	
<input checked="" type="checkbox"/> OneDrive (Personal)	

AC [v]

Done    Cancel    Clear Selection

Daily Bandwidth Quota (MB) [v]    Daily Time Quota (min) [v]

Figure 14 – Blocking personal tenants

## Conditional access with Zscaler

By forwarding Microsoft 365 traffic via the Zscaler cloud, Microsoft's network sees all the traffic originating from Zscaler's public IP addresses. As these IP addresses can be used by other Zscaler customers, applying specific controls to access Microsoft 365 applications based on users' location is not applicable.

Microsoft conditional access uses specific hostnames to perform its security controls:

- login.microsoftonline.com
- login.windows.net

If the IP address reaching Microsoft 365 is the organization's public IP address, then seamless authentication can be applied. Otherwise, multifactor authentication is enforced.

The payload traffic, being the vast majority of the traffic, goes via Zscaler and is optimized as described above.

The following diagram presents the high-level design.

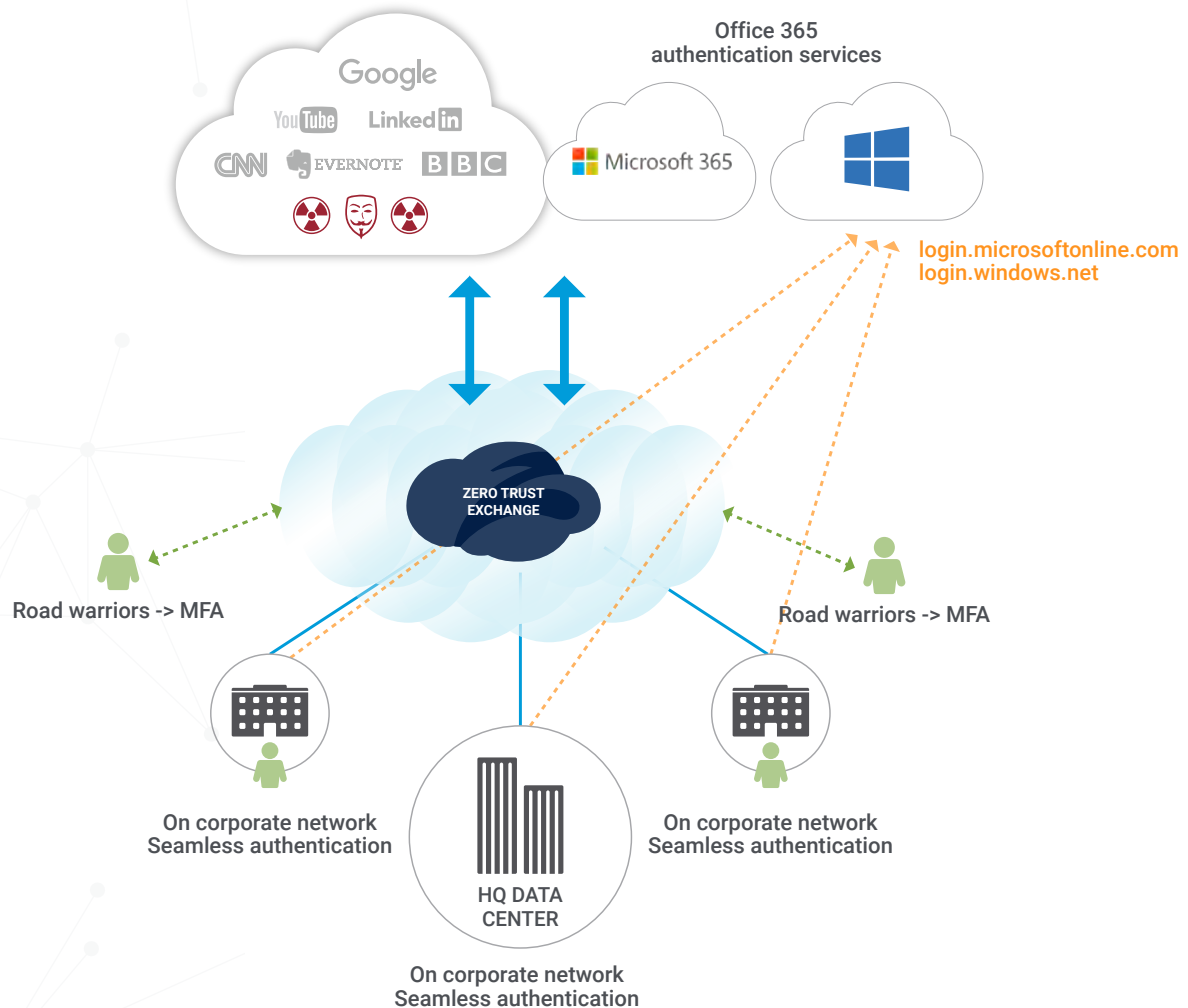


Figure 15 – Integrating Zscaler with conditional access

## Adding Zscaler IP addresses to the trusted IP

As all traffic is presented with Zscaler's IP addresses, those can be added to the list of trusted networks. Those addresses are documented here: <https://config.zscaler.com>.

While this makes access simple and provides non-MFA for roaming users as well, it also means that we do not recognize whether users are on the corporate network vs. remote/mobile.

## PAC file approach

Zscaler Client Connector uses PAC files in the forwarding profile and app profile to determine which traffic should be allowed to Zscaler and which should bypass. With a PAC file, it is simple to bypass specific destinations using Zscaler Client Connector. To send traffic direct for deciding if MFA should occur or not, the following statement needs to be added to the PAC file:

```
if (dnsDomainIs(host, "login.microsoftonline.com")) ||
dnsDomainIs(host, "login.microsoft.com") ||
dnsDomainIs(host, "login.windows.net"))
{return "DIRECT";}
```

These hostnames test the client's public IP address for conditional access.

## Bandwidth control

Figure 16 – Defining access policy

## BEST PRACTICES FOR IMPLEMENTING ACCESS TO MICROSOFT 365 WITH ZSCALER™

Zscaler Bandwidth Control allows you to preserve access to your business-critical Microsoft 365 applications regardless of your internet pipe consumption. This enables you to maintain greater control of all traffic flows, such as adding more restrictive rules around social media and streaming. For example, you could allocate a maximum of 10 percent of the bandwidth to streaming and social media. When bandwidth is restricted, this traffic will not be guaranteed any bandwidth during times of contention with business-critical traffic. This way, business-critical applications such as Microsoft 365 Teams, SharePoint, and OneDrive always have access to enough of your bandwidth to perform their best.

### Summary

Zscaler enables direct-to-cloud access for internet-based applications like Microsoft 365. Organizations can send traffic directly to application servers over the internet, instead of backhauling traffic over costly MPLS circuits. Zscaler simplifies Microsoft 365 deployment by taking advantage of our global direct-to-cloud network, which improves user experience and application performance.



**About Zscaler:** Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

**Zscaler, Inc.**  
120 Holger Way  
San Jose, CA 95134  
+1 408.533.0288  
[www.zscaler.com](https://www.zscaler.com)

