Visualizing User Connectivity with Zscaler Digital Experience

Reference Architecture

Contents

About Zscaler Reference Architecture Guides

The Zscaler™ Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who Is This Guide For?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A Note for Federal Cloud Customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler Account team on feature availability and configuration requirements.

Conventions Used in This Guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding Out More

You can find our guides on the Zscaler website at Reference Architectures (https://www.zscaler.com/resources?type=reference-architectures).

You can join our user and partner community and get answers to your questions in the Zenith Community (https://community.zscaler.com/).

Terms and Acronyms Used in This Guide

Acronym	Definition
AI	Artificial Intelligence
AP	Access Point
API	Application Programming Interface
BYOD	Bring Your Own Device
CLI	Command Line Interface
DC	Data Center
DEM	Digital Experience Monitoring
I/O	Input/Output
ICMP	Internet Control Message Protocol
JSON	JavaScript Object Notation
JWT	JSON Web Token
ML	Machine Learning
MTTD	Mean Time to Discovery
MTTR	Mean Time to Resolution
OS	Operating System
OT	Operational Technology
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SSE	Secure Service Edge
SSL	Secure Socket Layer (superseded by TLS)
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UCaaS	Unified Communication as a Service
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
ZDX	Zscaler Digital Experience™
ZIA	Zscaler Internet Access™
ZPA	Zscaler Private Access™

Icons Used in This Guide

The following icons are used in the diagrams contained in this guide.

Zscaler Zero Trust Exchange


Zscaler App Connector


Laptop with Zscaler Client Connector Installed


Zscaler Client Connector on Phone


Internet

Data Tunnel


API Gateway


Headquarters Location


Branch Office Location


Hybrid and Remote Users


Cloud Identify Provider


Generic Cloud Application or Workload


Router


Generic Application or Workload

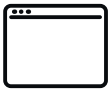

Administrator


Gateway


Wired


Wi-Fi


Egress


Website


Expand View


Positive / True Badge


Negative / False Badge

Introduction

As your applications and work locations continue to evolve, so must your ability to monitor and diagnose application access and performance. Traditional monitoring tools for application performance and user experience relied on the ability to control and instrument the network and applications. Using synthetic probes, users could be simulated to test access to applications, latency, and jitter. When a user experienced an issue accessing an application from their IT-issued device, IT staff worked with the user to diagnose the issue.

The ongoing migration to cloud-based applications, remote and hybrid work locations, and bring your own device (BYOD) initiatives have made this model obsolete. To effectively understand performance issues, your IT team needs visibility into more than the cloud application. When a user calls in, your team needs to determine if it is an issue with the user's device, their home Wi-Fi router, their ISP, or your cloud application. Understanding what the issue is and where it is occurring ensures that the correct troubleshooting procedures can be taken.

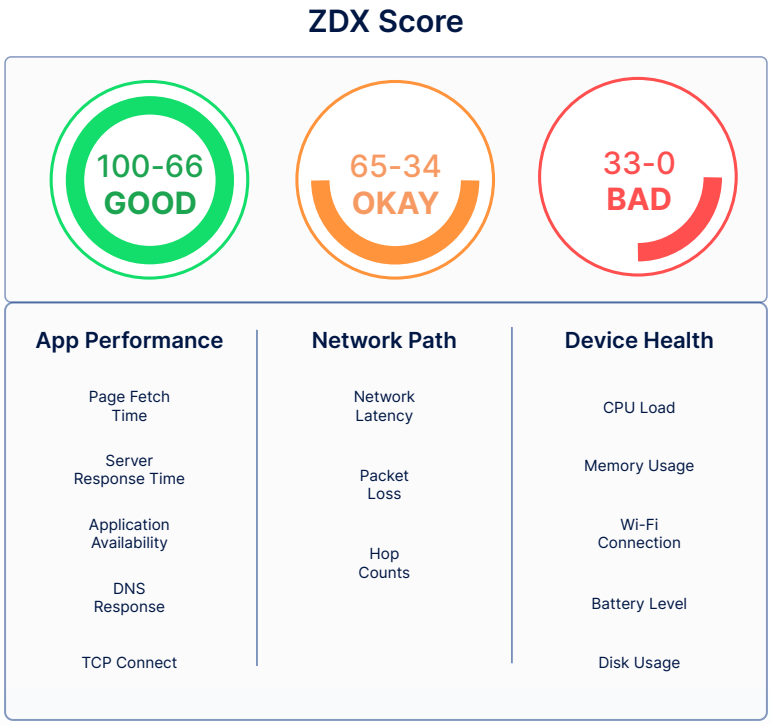


Figure 1: Digital experience monitoring provides end-to-end visibility from the user's perspective

Zscaler Digital Experience (ZDX) provides visibility into the experience for your end user. ZDX delivers Digital Experience Monitoring (DEM) via Zscaler Client Connector, a small agent that probes the device itself. Zscaler Client Connector sends probes to cloud applications you define and performs network health checks from your client devices. ZDX also proactively alerts you to problems that are occurring. You define the rules that tell ZDX when an issue exists and who to alert without waiting for a user ticket.

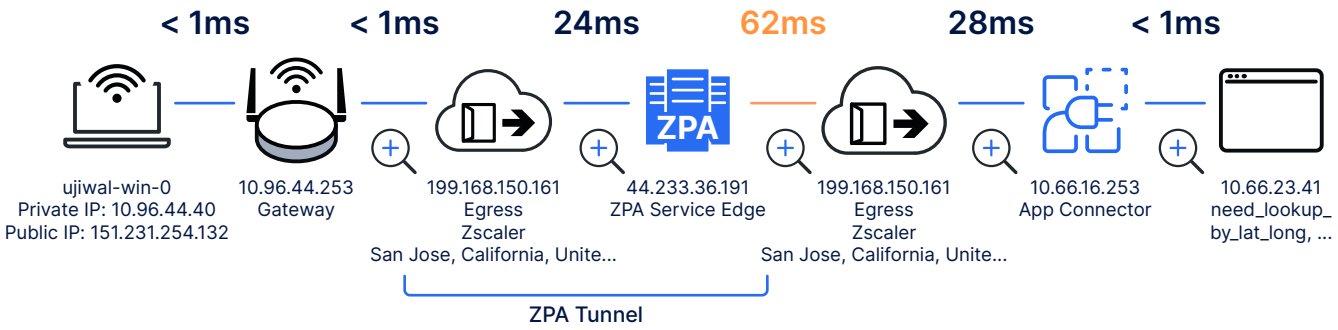


Figure 2: ZDX gives you visibility into your device and the network between your user and the application they are using

ZDX enables your help desk to quickly pinpoint where issues are occurring without having to do complex troubleshooting with the end user. Your help desk gets an end-to-end view of the network, with the most problematic segment highlighted. This includes the user's device and Wi-Fi network strength.

ZDX goes a step further with automated root cause analysis. This feature looks for the primary causes of a user's issue, from their local connection to the application itself. This gives first- and second-level support the ability to resolve more tickets without escalation. Together these tools speed your mean time to detection (MTTD) and mean time to resolution (MTTR), reducing your overall support costs.

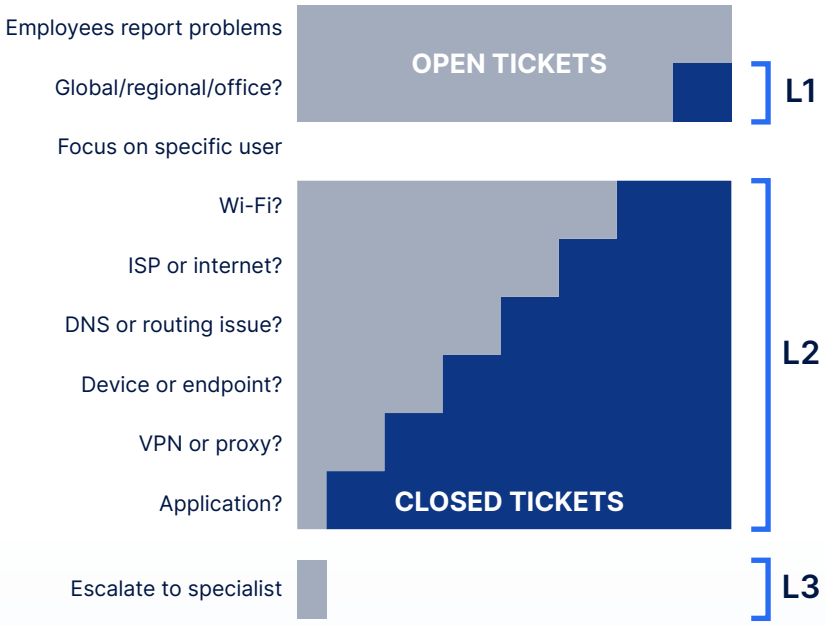


Figure 3: Providing more visibility into issues reduces escalations and speeds MTTR

Zscaler Client Connector polls applications with a small bit of data every 5 minutes, noting the response code and the time the transaction took to complete. Zscaler Client Connector also monitors points along the path to the application, reporting on the status of each link in the network.

This data is sent to the Zscaler Zero Trust Exchange, collecting and reporting on the conditions as seen for your user's view. ZDX takes in all the information and generates a ZDX Score for each user from 0 to 100. The higher a user's score, the better their overall experience is interacting with cloud applications. The score gives you a rapid way to assess a user's current experience.

Zscaler Cloud Path Analytics allows you to view a dashboard that shows your users' overall throughput and at individual steps along the path. You can see latency and packet loss information for each network hop

along the path the user is taking to reach the application. At a macro level, you can see your application performance and availability, and where users are having issues connecting.

When a user is experiencing a problem and you want more details, your help desk can launch a Deep Tracing session. When a session is started, your help desk selects a user, a device, and an application. Zscaler Client Connector on the user's device starts sending web and Cloud Path probes to the application at an accelerated rate. Information such as Wi-Fi signal strength and the processes running on the user's machine is also collected. Your help desk can then review the information without the user being involved in the troubleshooting.

ZDX also supports alerting based on triggers to proactively notify your team about issues affecting your end users. These alerts show up on the ZDX Alerts page, but they can also be configured to send email notifications or use webhooks to trigger your existing security information and event management (SIEM) system.

If you subscribe to Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), Zscaler Client Connector is used to connect your users to those services. It can also be deployed as a standalone monitoring tool for ZDX access only. By giving your help desk and application monitoring teams direct access to your users' experience, they can rapidly diagnosis the source of performance issues and suggest remediations.

Key Features and Benefits

- Increase agility and collaboration among desktop, security, network, and help desk teams while triaging and resolving user experience issues.
- Improve productivity with better user experience and fast, secure, and reliable connectivity through the Zscaler Zero Trust Exchange.
- Reduce complexity and cost of point monitoring solutions with a single location to review and rapidly troubleshoot application performance issues for your users.
- Simplify operations using the same lightweight agent for all Zscaler services.

In this guide, we discuss different aspects of ZDX and provide recommendations for you to get the most out of the ZDX service. At each step, we link to appropriate Zscaler Help articles for detailed configuration steps.

We start with understanding your applications and updating network and host security to allow ZDX to function properly. We discuss how web probes function and how to determine which probes each user group should use. Next, we talk about alerting and using the system's analytics.

We discuss when to use Deep Tracing to resolve user issues. We cover the rollout of ZDX to your environment, and touch briefly on what is available for the ZDX API. Finally, we explore approaches to leveraging ZDX through three use cases: ZDX and ZIA, ZDX and ZPA, and ZDX as a standalone DEM solution.

New to ZDX?

If this is your first time learning about ZDX, you can read overviews and watch video demonstrations of the ZDX technology with the following links:

- Zscaler Digital Experience (https://www.zscaler.com/products/zscaler-digital-experience)
- Cloud Path Analytics (https://www.zscaler.com/products/zdx/cloudpath-analytics)
- Zscaler Digital Experience at a glance (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience-benefits.pdf)
- Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf)
- Digital Experience Monitoring (ZDX) Help (help.zscaler.com/zdx)

Understanding ZDX Probes

For many years, traditional network monitoring tools existed with cloud applications by monitoring connections from fixed sites. Remote work was limited and often entailed a VPN connection to a central site for access to applications. The realities of newly remote and hybrid work have made that monitoring style of limited value.

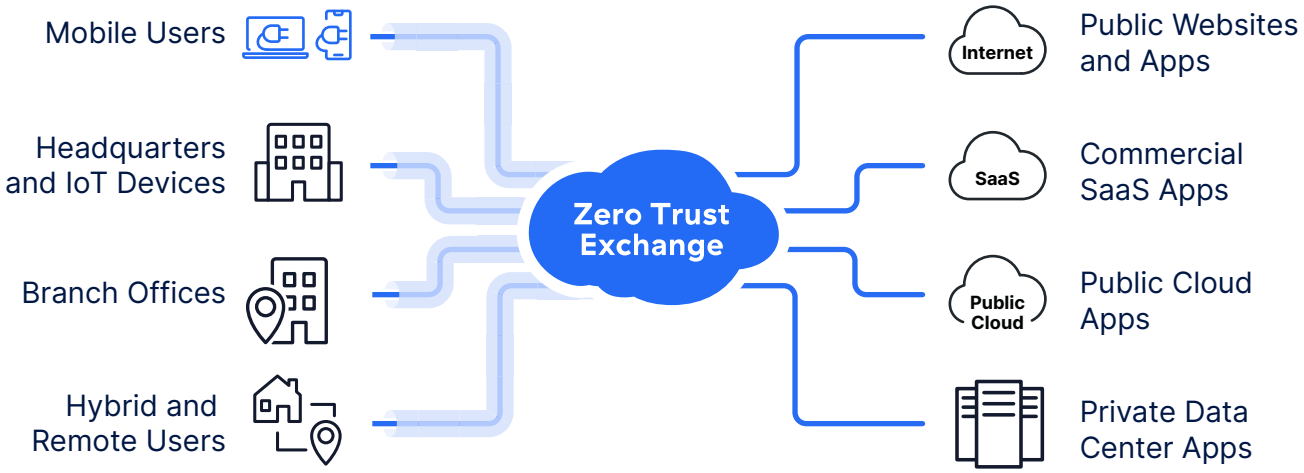


Figure 4: The number of locations where users and applications are located continues to shift and increase

ZDX instead monitors application availability from every user's device via Zscaler Client Connector. This is the same software that allows users to connect directly to applications using ZPA, or to a ZIA Public Service Edge for internet access. The ZDX feature of Zscaler Client Connector enables probes to be sent to configured web-based applications.

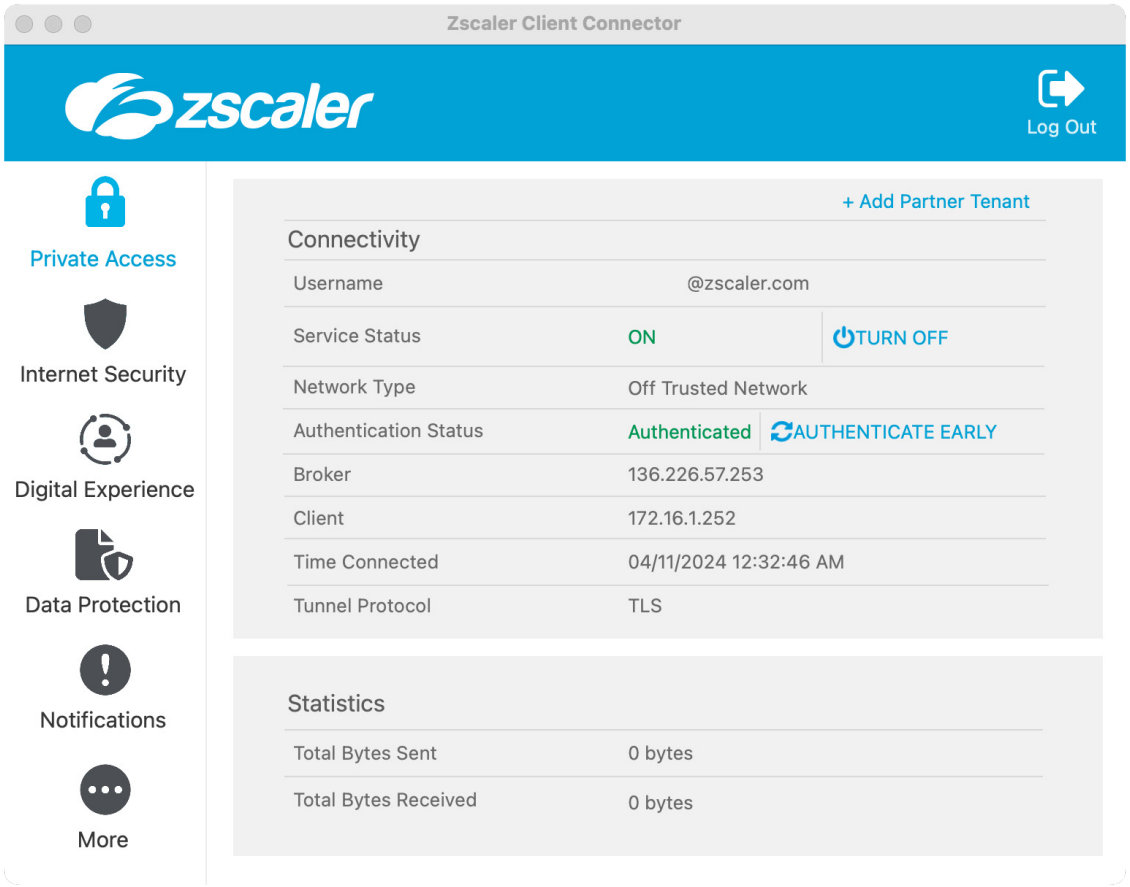


Figure 5: ZDX runs on the user's machine as a part of Zscaler Client Connector

ZDX probes exist as part of an application you select. ZDX provides several preconfigured applications depending on your subscription level, and you can always define custom applications and probes. The probes check that your application is responding appropriately, and record latency and jitter statistics along the network path. These two functions are handled using two probe types:

- Web probes that check for application availability.
- Cloud Path probes that record hop-by-hop network performance information between the user and the application.

The data from these probes is combined with information about the user's device. This includes items such as CPU and memory usage, network usage, and Wi-Fi signal strength. This information is sent to the ZDX cloud. The data is aggregated and presented as a series of dashboards that allow you to see your organization's application performance. ZDX also supports configurable alerts, allowing your operations team to proactively address issues as they begin, not after they are reported.

Learn more at About Probes (https://help.zscaler.com/zdx/about-probes).

ZDX Web Probes

The ZDX web probe makes an HTTP or HTTPS GET request to an application to check its service availability and responsiveness. When the application receives the request, it responds with an HTTP Status Code, such as a redirect to a login page. ZDX sends the probe and looks for the correct response code in return based on its configuration to mark the status as available or down.

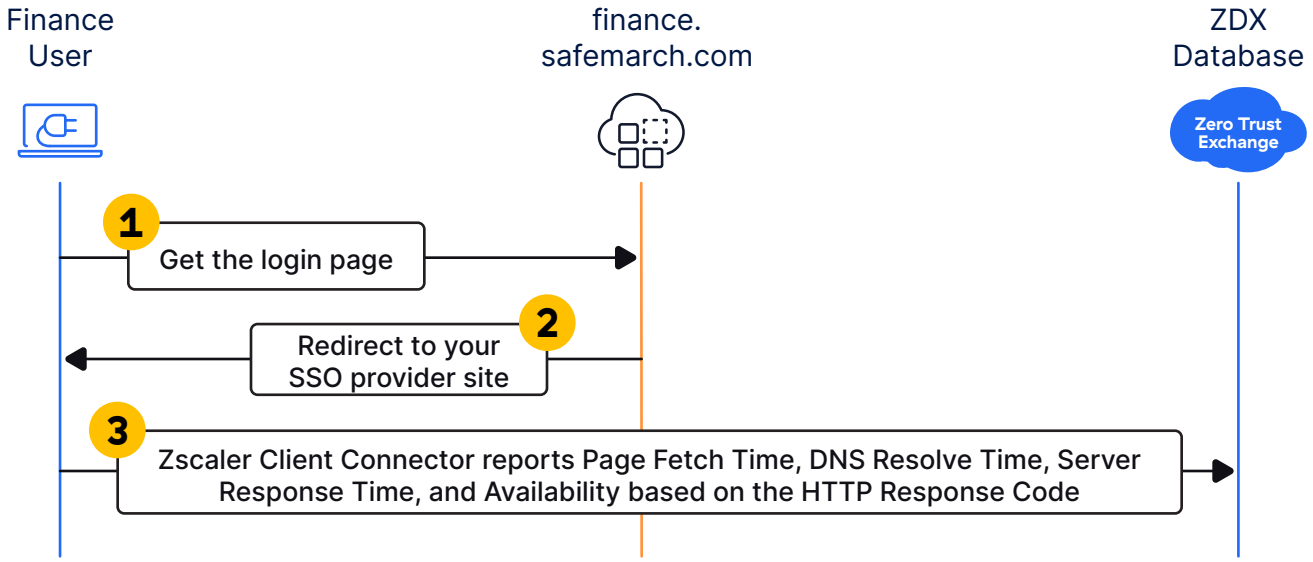


Figure 6: Web probes send HTTP/HTTPS GET requests to your application and monitor the HTTP Status Code that is returned

1. A member of the finance team has Zscaler Client Connector installed. Zscaler Client Connector is configured to check that the finance application is running for anyone in the finance group. To do this, Zscaler Client Connector sends an HTTPS probe to the login page for finance.safemarch.com.
2. Finance.safemarch.com responds with a redirect to the organization's single sign-on (SSO) provider to authenticate.
3. The server response and the data around the response is sent to ZDX, which is configured to consider the redirect response as a sign that the service is operational.

The ZDX web probes collect the following information about the application:

- **Page Fetch Time** – This metric collects the network fetch time of the web page from the URL-specified web probe. It requests only the top-level page document and does not request all embedded links within the web page.
- **DNS Resolve Time** – This metric represents the time it took to resolve the DNS name for the hostname specified in the web probe URL.
- **Server Response Time** – Time to First Byte (TTFB).
- **Availability based on the HTTP Response code** – If a success code is returned, the availability is either 1 or 0. If the probe times out, the availability defaults to 0.

Web probe requests are always TLS/SSL terminated. Any configured policies for TLS/SSL bypass are overridden for ZDX web probes. The ZIA Public Service Edge must intercept and instrument the probe, which requires TLS/SSL termination. When using Deep Tracing during a live troubleshooting session, session probe requests are logged in ZIA web logs. This provides an additional level of detail when troubleshooting internet-related issues.

ZDX Cloud Path Probes

Cloud Path probes work by sending packets with reduced time-to-live (TTL) values to map the path between the user-installed Zscaler Client Connector and the web application. Cloud Path probes can use ICMP, UDP, or TCP, and can change these segment by segment. The system records the statistics as the probes come back or fail to come back.

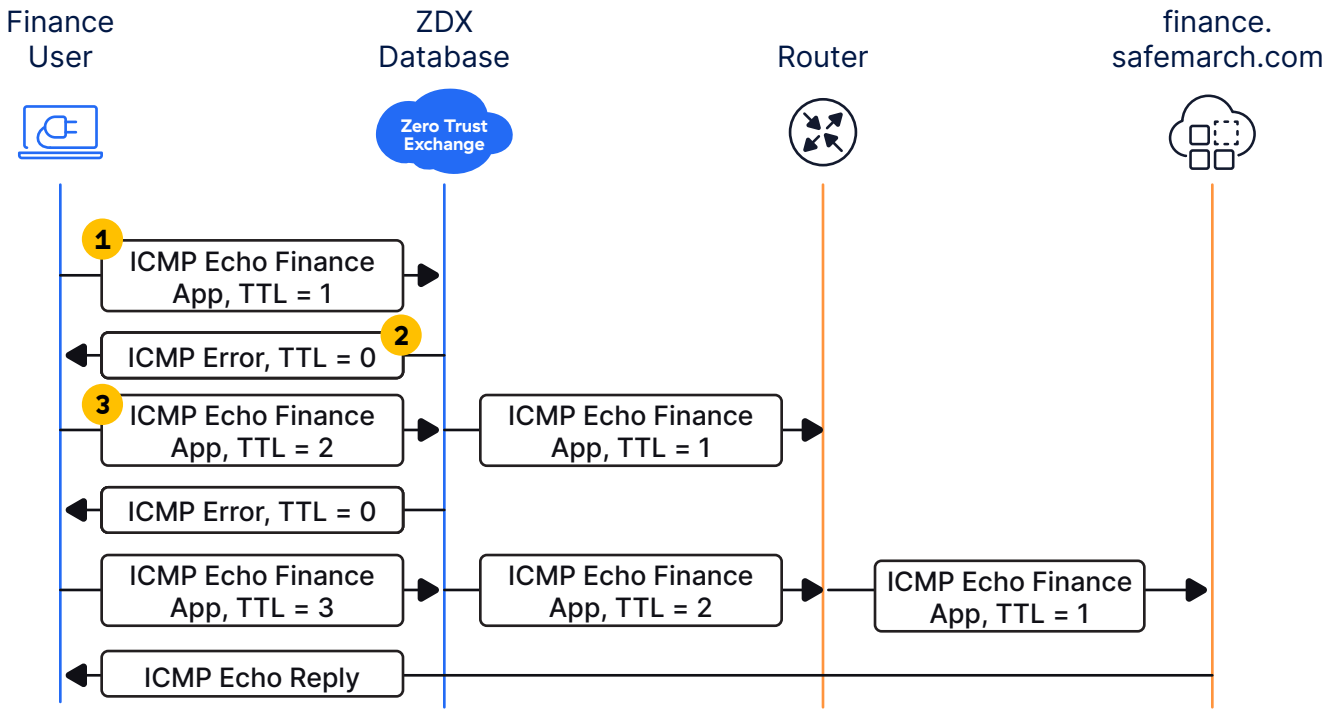


Figure 7: Cloud Path probes send requests with incremental TTL settings to probe each hop in the network path

1. The same finance user with Zscaler Client Connector installed, the agent begins sending probe packets out with a time to live (TTL) of 1, or 1 network hop away. The probes are sent 5 times with the same TTL.
2. At each hop, the router decrements the TTL by 1, dropping any probes that reach 0. Typically, a router sends a notification back to the sender that the TTL has expired, and that the packet has been dropped. Zscaler Client Connector records this data for each set of probes.
3. After the 5 sets of packets, Zscaler Client Connector increases the Cloud Path probe TTL by 1 and sends another series of 5 probes. This increase continues until the application is reached or the number of hops exceeds the systems limits.

Cloud Path probes are used to collect the following metrics:

- **Hop Count** – The number of hops between each hop point on the path.
- **Packet Loss** – The percentage of packet loss at each hop point on the path.
- **Latency (Average, Minimum, Maximum, and Standard Deviation)** – The roundtrip path time measured in milliseconds.

Probe Smart Caching

One of the optimizations performed by ZDX is probe smart caching. When several of your users sit in the same location, many probes will come from the same location, bound for the same destination applications, effectively reporting the same metrics. With smart caching, ZDX aggregates multiple probes to the same application with a single probe, and then replicates that data in the user's dashboard.

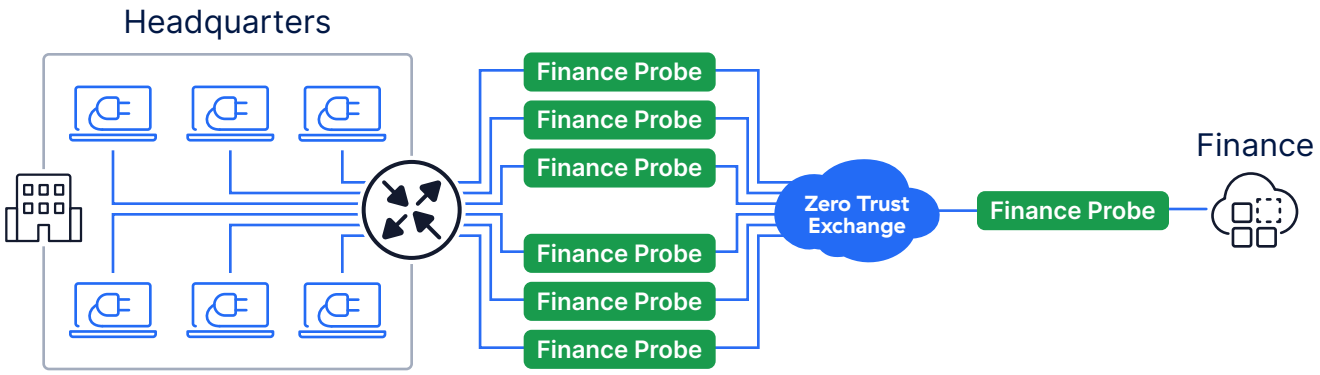


Figure 8: Smart caching prevents applications from being flooded with probe requests

This service is handled automatically in the Zero Trust Exchange to protect applications from dealing with a flood of probe requests. Smart caching helps preserve bandwidth and CPU cycles for your application instances. For public services, smart caching helps to prevent network defense countermeasures such as IP blacklisting from being triggered due to a high probe volume.

Zscaler Hosted Monitoring

In addition to probes configured and run from Zscaler Client Connector, Zscaler also runs workloads in our data centers around the world that send out their own probes. The Hosted Monitoring service enables organizations to probe applications and services continuously. This provides continuous monitoring and reporting to identify service interruptions. Hosted Monitoring uses Web and Cloud Path probes to monitor both predefined and custom applications.

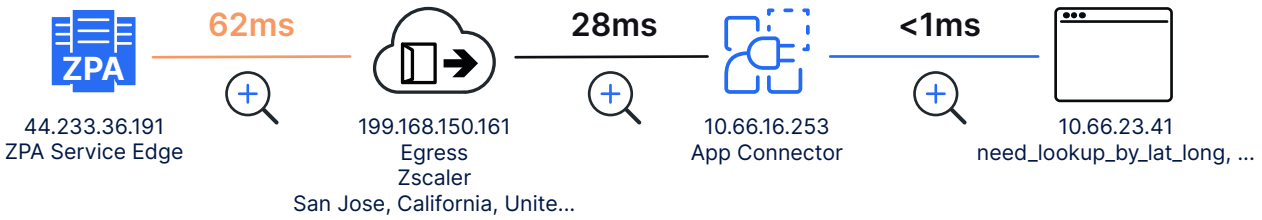


Figure 9: Zscaler Hosted Monitoring sends Web and Cloud Path probes from hosts located in Zscaler data centers

When configuring Hosted Monitoring, you can choose the data centers nearest your organizations, users, or locations as the probe source. After configuring, your probes will record the Web and Cloud Path data that you can then examine.

Learn more at Understanding Hosted Monitoring (https://help.zscaler.com/zdx/understanding-zscaler-hosted-monitoring).

Hosted Monitoring Web Probe Metrics

Web probes provide metrics on the performance of web-based applications. This information includes site availability and page fetch times. The charts show performance metrics for the last 30 days, the current month to date, or in a selectable time range of 2 to 48 hours.

Availability represents the site being active and responding to the probe requests. This is shown as a percentage. Page fetch time is the time it takes to receive a response to a web request. You can further examine the details including:

- **Redirect Time** – The time measurement of traffic redirects.
- **DNS** – The resolution time for the DNS name.
- **TCP** – The time measurement of the Transmission Control Protocol.
- **TLS/SSL Handshake** – The communication time to the device.
- **Server Response Time** – The Time to First Byte (TTFB).
- **Page Fetch Time** – The time it takes the application to load a page for the user.

Hosted Monitoring Cloud Path Probe Metrics

Cloud Path probes monitor the performance from the Hosted Monitoring environment and display the End-to-End latency as the default. Cloud Path probes provide information on each hop in the network connections. This provides information to discover network bottlenecks, such as slow devices or missed cache events. The Cloud Path graph shows the following metrics:

- **End-to-End Latency** – The time to send a data packet from source to destination, including hops between legs in the Cloud Path.
- **Packet Loss** – When data packets that travel across a network fail to reach their destination.
- **Jitter** – The variance in time delay between data packets over a network.

Learn more at Evaluating the Cloud Path (https://help.zscaler.com/zdx/evaluating-cloud-path).

Hosted Monitoring Alerts

Hosted Monitoring is integrated into the ZDX alerts module. Alerts can be configured to send an alert based on application and network performance issues from the viewpoint of the Zscaler data center. Hosted Monitoring alerts appear along with any configured alerts for Zscaler Client Connector probes.

Hosted Monitoring alerts require ZDX Advanced, ZDX Advanced Plus, or Hosted Monitoring licenses.

Learn more at About Alerts (https://help.zscaler.com/zdx/about-alerts).

Getting Started with ZDX

With the highly distributed nature of both users and applications in organizations today, monitoring and ensuring fast access to applications continues to increase in importance. ZDX gives your organization the ability to see into users' work experience, no matter where they work or where the applications they access are located. ZDX does this by instrumenting your users' devices to gather network and application performance data. ZDX provides the following set of features and capabilities:

- Proactively monitors every user device in your organization to detect user experience and productivity issues.
- Grades your digital experience by referencing the ZDX Score over time for your organization. A ZDX Score is also generated for each application, location, department, and user.
- Triages performance issues and pinpoints whether the issue is in the local network, a user's device, the ISP provider, or within the Zscaler policy.
- Uses Zscaler's unified client, Zscaler Client Connector, to implement ZDX on Windows and macOS devices.
- Monitors general data center information and your key SaaS applications (i.e., Office365 Online, Salesforce, Box, etc.) using HTTP, ICMP, or UDP probes running on user devices in near real-time.
- Collects real-time health information from your user's devices, including CPU usage, memory usage, Network I/O, Disk I/O, Wi-Fi signal strength, and more.
- Hop-by-hop network path visualization from the client device to the destination device.
- Threshold-based alerting for SLA monitoring and proactive remediation.
- Remote troubleshooting capabilities to perform detailed analysis of problematic devices.
- Executive insight reports and digital experience analytics aggregated at organization, location, and application levels to simplify reporting requirements.

Using the ZDX Setup Wizard for ZIA Customers

If your organization subscribes to ZIA to protect your users' access to the internet, you can take advantage of the ZDX setup wizard. This tool leverages the existing authentication and administration accounts in your ZIA tenant.

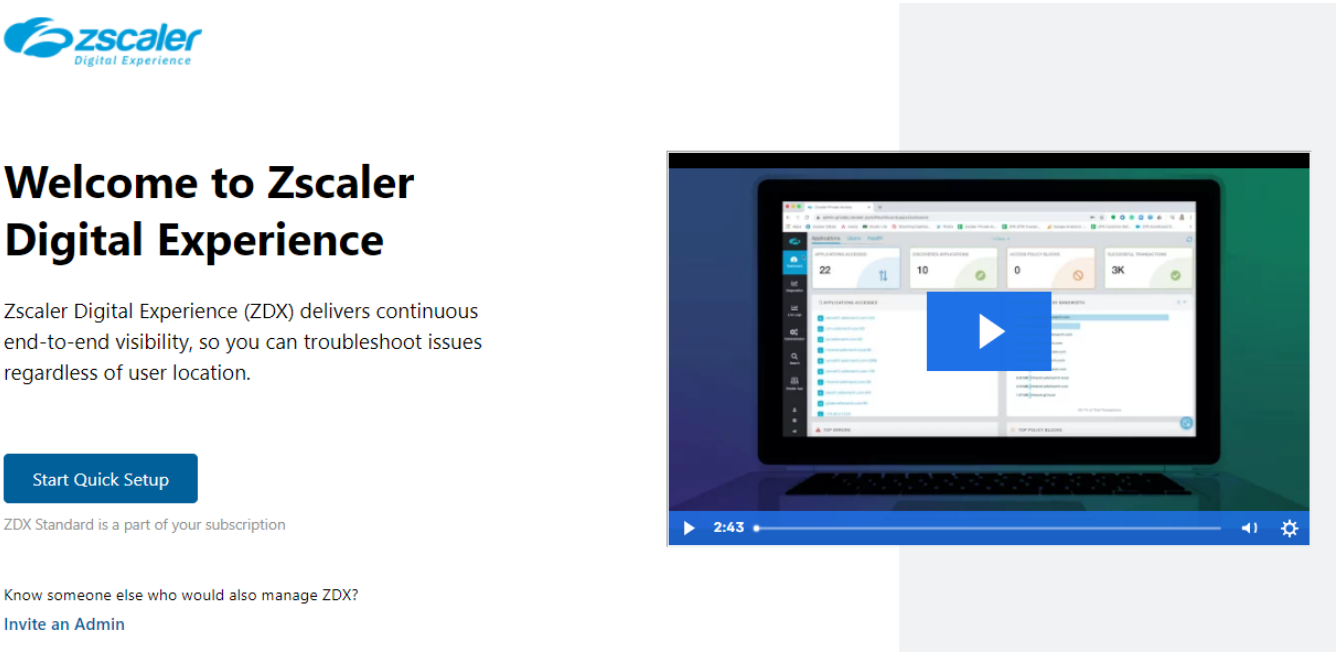


Figure 10: The ZDX Quick Setup wizard

The wizard allows you to perform the following actions in a guided series of steps:

- Watch an introductory video on ZDX.
- Invite existing or new admins to manage ZDX.
- Enable the ZDX service for all users or select user groups.
- Select up to three predefined or custom applications, including tenant IDs as required.

By using the wizard and leveraging your existing configurations, you can quickly get your organization running with ZDX. Zscaler recommends ZIA users leverage the wizard when first enabling ZDX. Learn more about Using the ZDX Setup Wizard (https://help.zscaler.com/zdx/using-zdx-setup-wizard).

Administrator Accounts

Administrator accounts in ZDX allow you the flexibility of assigning different permissions to members of your operations team. You can define different roles with permissions assigned to them based on the needs of users in that role. These roles are then associated with administrator accounts you create in the ZDX Admin Portal. ZDX supports both local password accounts and security assertion markup language (SAML)-initiated authentication.

You will initially receive a password reset notification for the default administrator account from the Zscaler support team. You should use this account to create another local account for one or more of your top admins, giving them full permissions to administer your ZDX tenant. By creating administrator accounts from the beginning, you will have more complete audit logs should it become necessary to review changes later.

Zscaler recommends the use of SAML as the authentication method for admins. This allows you to leverage your existing single sign-on (SSO) infrastructure and any existing two-factor authentication. The default account should then be used only for emergencies where other administrators are unable to log in to the system. Learn more at First Time Provisioning for ZDX Admins (https://help.zscaler.com/zdx/first-time-provisioning-zdx-admins).

When using SAML authentication, it is best practice to have one account that is still password based in the event of a SAML interruption. Ideally the default administrator account would be used for this purpose.

Administrator permissions offer flexibility and granular control over what actions an administrator can perform. ZDX has three preconfigured roles, and you can build custom roles as needed:

- **ZDX Super Admin** – An admin with this role has read, add, edit, delete, and manage permissions in the ZDX Admin Portal. The default admin account uses this role.
- **ZDX Read-Only Admin** – An admin with this role only has read-only permissions in the ZDX Admin Portal.
- **ZDX Service Desk Tier 1** – An admin with this role has read-only permissions to the User Dashboard and access to the User Search portal.

Learn more at About Administrators (https://help.zscaler.com/zdx/about-administrators).

Updating Network and Host Allow Lists

For ZDX to function properly, you need to add a set of domains through your gateway firewall or any non-Zscaler proxy you have in operation. This includes allowing probes from Zscaler Client Connector. If you are an existing ZIA subscriber, you also need to allow specific hosts on your ZIA cloud.

You can find your ZIA cloud by viewing the URL of your Admin Portal, or by visiting https://ip.zscaler.com while logged in to the ZIA service.

To view a complete list of hostnames that must be bypassed, see Allowlist Domains for ZDX (https://help.zscaler.com/zdx/allowlist-domains-zdx).

Defining Applications

Application definitions allow you to build web and Cloud Path probes to the application for monitoring. ZDX comes with a set of predefined applications as well as the ability to build custom applications. When using a predefined application, you enable the application and enter your tenant information for your organization. With a custom application, you need to build the web and Cloud Path probes to support that application.

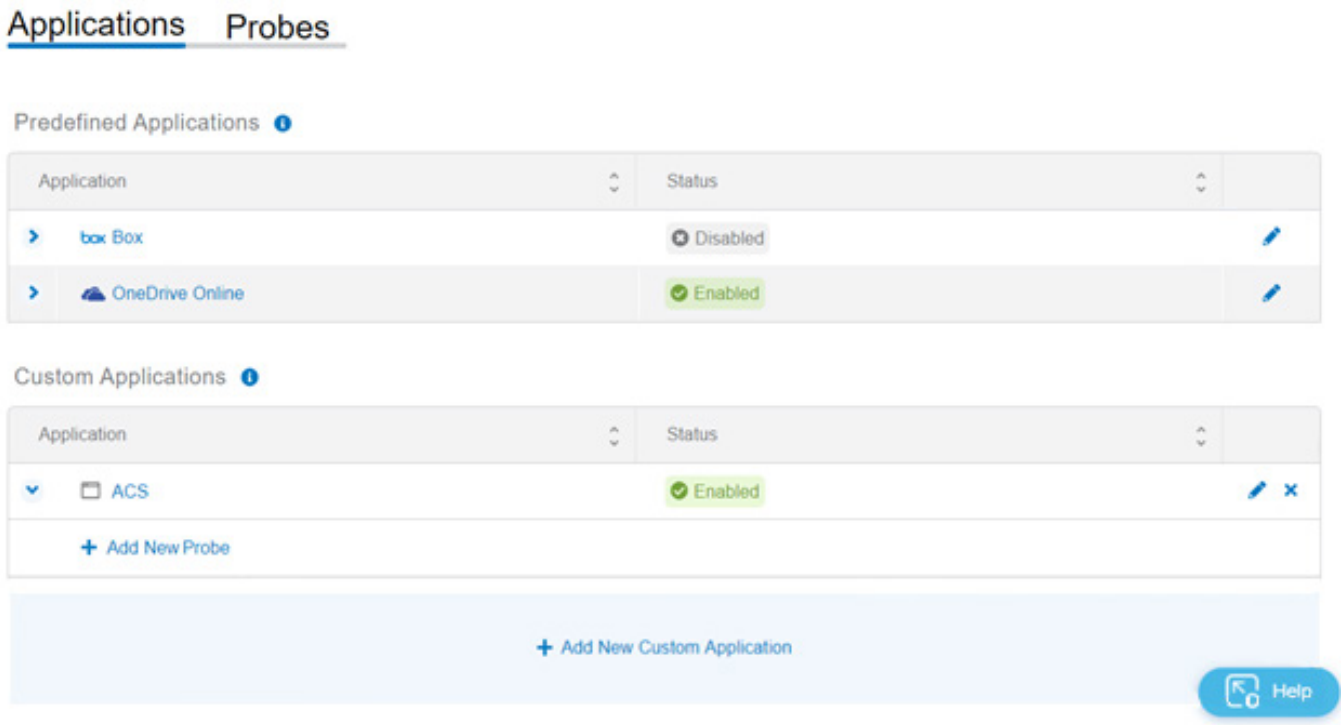


Figure 11: The Applications page lists both predefined and custom applications

Learn more at About Applications (https://help.zscaler.com/zdx/about-applications).

Predefined Applications

ZDX has predefined support for common large enterprise applications. Because these applications are already understood by ZDX, you only need to do minimal configuration before using them. The exact applications that are available to your organization depend on your ZDX subscription level. The following list includes all supported applications:

- Unified Communication
  - Microsoft Teams Call Quality
  - WebEx Call Quality
  - Zoom Call Quality
- Web Applications
  - Box
  - Microsoft Login
  - Microsoft Teams Web App
  - Okta

- OneDrive for Business
- Outlook Online
- Salesforce
- Salesforce Classic
- Salesforce Lightning
- ServiceNow
- SharePoint Online
- Webex
- Zoom

To learn more about which applications are included in each subscription level, see Predefined Applications for ZDX (https://help.zscaler.com/zdx/predefined-applications-zdx).

Defining Custom Applications and Probes for ZDX

Custom applications allow you to apply ZDX monitoring to applications that you run in your private data center or that are hosted in the cloud. These can be custom-built applications, privately hosted instances of applications, or cloud services. When you add a custom application, you must also add the associated probes to monitor the application.

There are two types of probes you will build: a web probe and a Cloud Path probe. For each application, you will configure each probe type. It is recommended that you build your web probes first, as the Cloud Path probe can follow the web probe and simplify configuration. Each probe has a frequency timer determining how often the probe should run.

The frequency at which probes are sent varies based on your subscription. To learn more, see Ranges & Limitations (https://help.zscaler.com/zdx/ranges-limitations).

Each application requires some basic information such as the name of the probe and the name of the application. It's recommended that you relate the probes and application names to ease configuration management in the future. The initial setup also requires that you select Probing Criteria and Exclusion Criteria. These two settings determine which devices run the probes. Your options include user groups, departments, specific users, locations, or device types. Follow the strategies discussed in Developing a Probe Monitoring Strategy when setting your criteria.

Configuring Web Probes for Custom Applications

To complete setting up your web probe, you must determine what constitutes a successful web probe request for that application. The probes send HTTP or HTTPS GET requests to your application, based on the URL you provide. If you are required to pass a request header, such as a security token to your application, you can add multiple pairs consisting of names and values. It's best to work with your operations and applications developers to understand what the requirements are for these fields.

For predefined applications, many of these values will not be available for configuration.

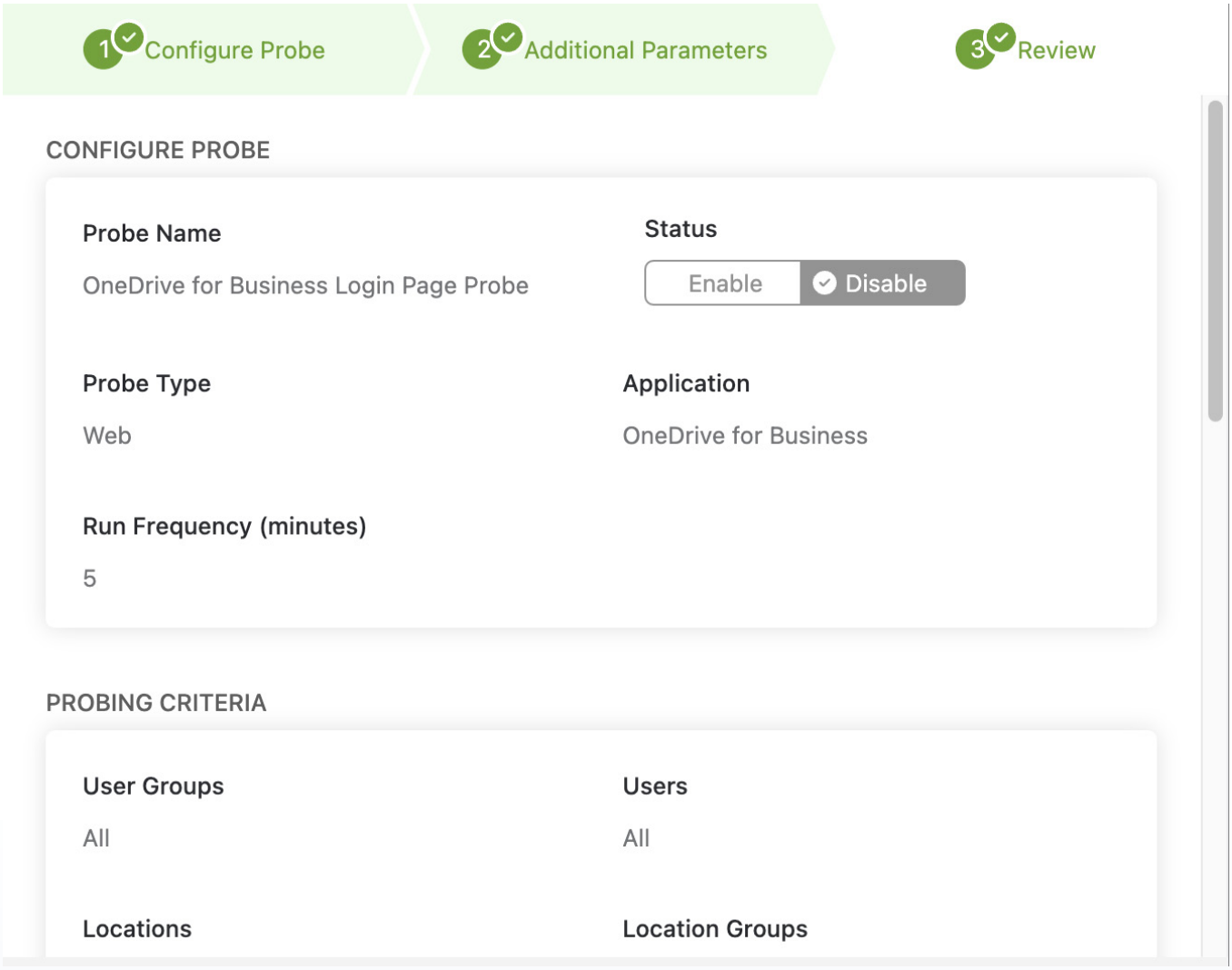


Figure 12: ZDX web probe configuration wizard

When the application responds to the probe, it provides an HTTP Status Code (e.g., "404 page not found"). Every web transaction you initiate receives a response code from the server. For a complete list of HTTP Status Codes, see Hypertext Transfer Protocol (HTTP) Status Code Registry (https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml).

Initially ZDX monitors the following 1xx (Informational), 2xx (Success), and 3xx (Redirection) codes, which can be removed individually if not needed:

- 100 Continue
- 101 Switching Protocol
- 102 Processing
- 103 Early Hints
- 200 OK
- 201 Created
- 202 Accepted
- 203 Non-Authoritative Information
- 204 No Content
- 205 Reset Content
- 206 Partial Content
- 207 Multi-Status
- 208 Already Reported
- 226 IM Used
- 300 Multiple Choices
- 301 Moved Permanently
- 302 Found
- 303 See Other
- 304 Not Modified
- 307 Temporary Redirect
- 308 Permanent Redirect

Continuing with your configuration choices, you must decide what success looks like. Removing response codes that don't match your criteria for success is a good way to remove false positives. The initial number of attempts is set at 1 but can be increased if needed. Timeout is set to a default of 60 seconds but can be modified. Unless there is a technical reason to modify these values, Zscaler recommends leaving them at the default settings.

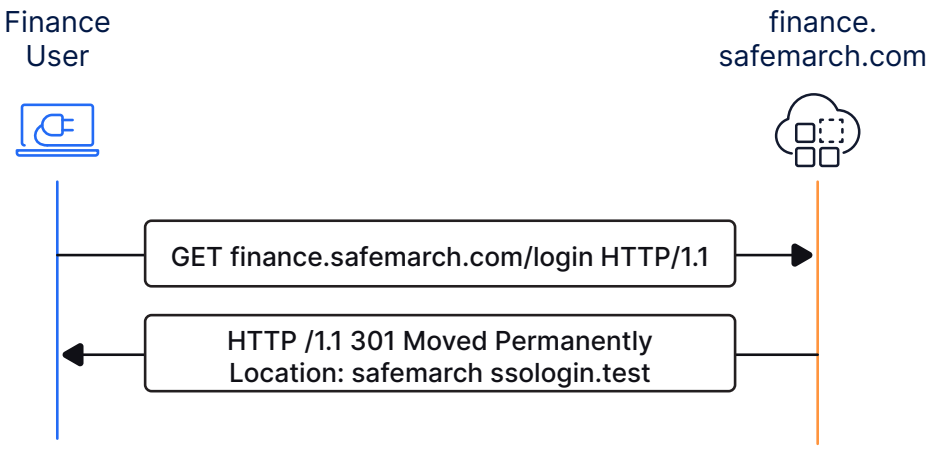


Figure 13: It's important that you monitor the correct service and response codes

It is important that you monitor the correct URL for your application and the correct response. As in the previous example, when you reach your application tenant's landing page or "front door" multiple times, it redirects you to the authentication service. The authentication service then responds with its own code. In this case, you would monitor for the original application sending a redirect code. This tells you that the application is up and responding appropriately to unauthenticated users.

Zscaler also provides a feature setting to enable following redirects. If the feature is enabled, you can further set the maximum number of redirects to follow before the application is considered failed. The default for this setting is 5.

To learn more about configuring web probes, see Configuring a Probe – Additional Parameters (https://help.zscaler.com/zdx/configuring-probe#Additional_Parameters).

Configuring Cloud Path Probes for Custom Applications

Cloud Path probes operate as a diagnostic tool looking at each segment of the network path. Cloud Path can leverage TCP, UDP, and ICMP when sending probes. If you select Adaptive mode, ZDX tries all three protocols and uses the one that is best suited to each hop in the network. Using Adaptive mode requires you to specify the TCP and UDP ports for your application. If you choose TCP or UDP instead, you only need to specify that protocol's port number. ICMP does not require configuration. Zscaler recommends using Adaptive mode in most cases.

Learn more at About Adaptive Mode (https://help.zscaler.com/zdx/about-adaptive-mode).

Timing between probes (when a timeout occurs) and the number of probes sent are also configurable. It is recommended to leave the probe settings at the default values unless you experience issues with slow outage reporting or false outage notifications. You might also need to adjust probe frequency or timing to avoid triggering automated blacklisting actions by your application vendor or host.

The interval between probes being sent is configurable from 1,000 to 10,000 milliseconds. This is also used as the spacing between the last probe with a TTL value and the next probe with an incremented TTL value. The timeout for probe response is configurable from 500 to 5,000 milliseconds. The number of probes sent per TTL level is configurable from 3 to 20, with 5 being the default. The number of probes sent is a balance between the need to see jitter and latency in the network and not triggering host defensive mechanisms.

To learn more about configuring Cloud Path probes, see Configuring a Probe – Additional Parameters (https://help.zscaler.com/zdx/configuring-probe#Additional_Parameters).

Defining Locations

A location in ZDX is a network from which your organization sends traffic to the internet. Your organization likely has multiple locations with each network identified. Locations are primarily used as a criteria for ZDX probes to ensure users are probing the applications that are hosted locally to them.

Learn more at About Locations (https://help.zscaler.com/zdx/about-locations).

Developing a Probe Monitoring Strategy

When a user logs in to Zscaler Client Connector, the software downloads its list of assigned applications to probe. Each user can be assigned a maximum of 30 applications to probe. The applications assigned are based on a combination of criteria such as the user's group membership or their current location.

In this section, we explore a monitoring strategy for applications. We discuss categorizing and assigning applications to users, and how to organize your applications so that your monitoring reflects accurately on the service. Finally, we cover best practices for handling web redirects and protocols.

Categorizing Applications

Assigning applications to users requires some thought to which applications are accessed by which user populations. If your organization has 30 or fewer monitored applications, the simplest approach is to assign all applications to all users. If you exceed the 30 monitored applications, you will need to start assigning applications more discriminately.

A useful framework is to break your applications into three categories:

- **Organization-wide critical applications** – These applications are important to the entire organization, such as your file share or business communication platform.
- **Group-specific critical applications** – These are applications that are critical to a smaller number of users, such as a GitHub for your development team.
- **Noisy applications** – These are applications that generate help desk tickets. They might also be new applications that you bring online. Applications come and go from this list as needed.

Probe and Application Arrangement

Keeping your applications and probes dedicated to a single service is important to ensure that you are receiving correct information. Putting multiple services into the same application, such as instances of a service located in multiple regions, can impact your reporting and troubleshooting.

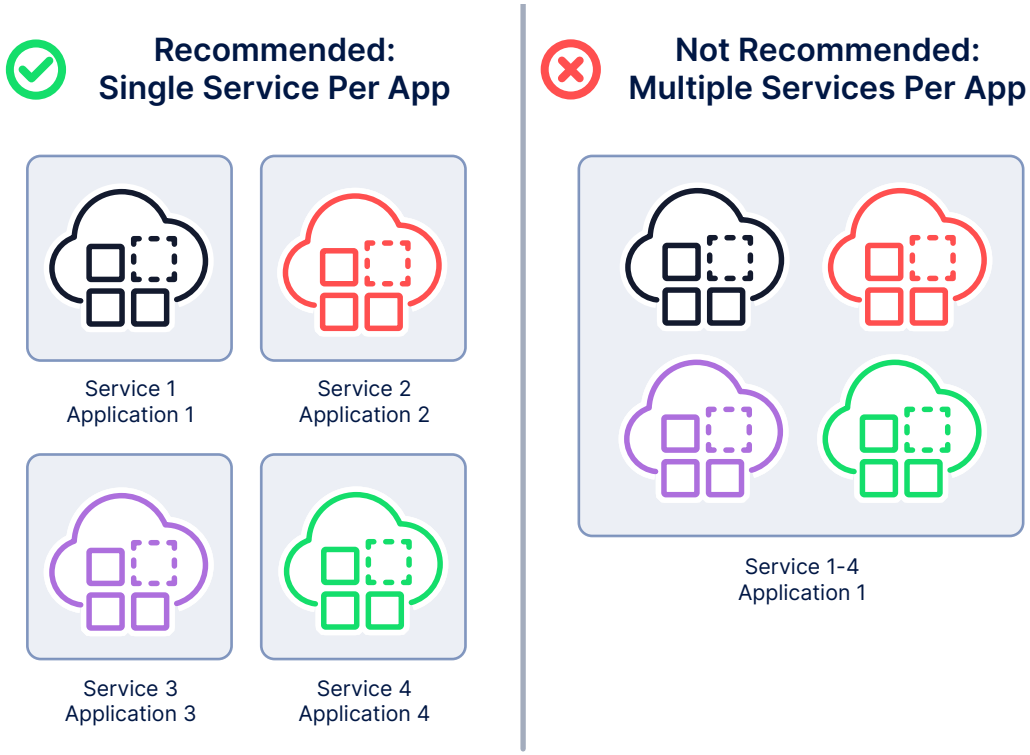


Figure 14: Keep applications focused on a single service for best reporting and eliminate false positives

If you run regional instances of your applications, consider splitting those services up as well. For example, having your finance servers that exist in the US, EMEA, and Asia in a single application can skew results for users and lead to unnecessary probing. By keeping your applications and services simplified, you ensure better reporting for your end users.

ZDX Dashboards and Analytics

Now that your applications have been defined and assigned to your users, you can begin to explore the various dashboards and inventory lists available to you. Using these tools, you can integrate ZDX into your operations workflow.

Some features mentioned in this section are not available on the standard plan. This can include changes to the amount of data available and data retention time. To view the supported range and feature availability by subscription level, see the Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf).

Learn more at About Analytics (https://help.zscaler.com/zdx/analytics).

Understanding the ZDX Score

ZDX takes in web and Cloud Path probe data from all your organization's users and combines the information to create a ZDX Score. The ZDX Score is generated for your applications, locations, groups, and individual users. Using this data, you can find out what the overall experience is for your users, and drill down to details for a specific user.

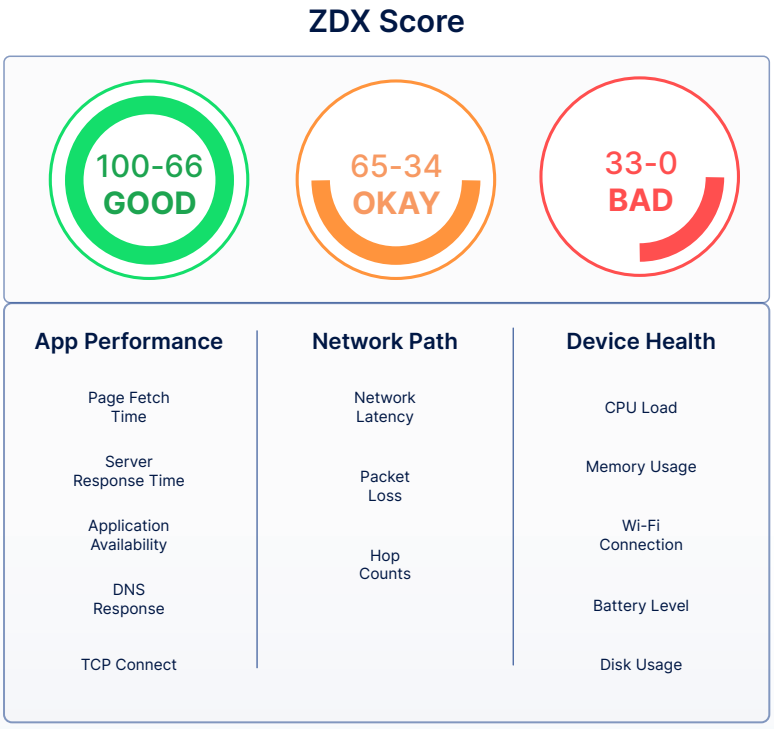


Figure 15: The ZDX Score takes in multiple inputs and reports at the organization, region, site, and user level

The generated ZDX Score ranges from 0 to 100, with 0 being the worst and 100 the best experience. The score is classed into one of three categories with a corresponding color code used on dashboards:

- **Good (Green)** – The score is above an acceptable threshold and ranges from 66 to 100.
- **Okay (Amber)** – The score is acceptable and ranges from 34 to 65.
- **Poor (Red)** – The score is below an acceptable threshold and ranges from 0 to 33.

ZDX Scores are calculated after probing an application. For most plans, probes are sent every 5 minutes. This occurs for every defined application in ZDX. When viewing the dashboard, note that the lowest score for the course of a one-hour period is used for the hours score that is displayed on dashboards. The meaning of the score varies by usage for applications, locations, cities, departments, organizations, and users.

The user's ZDX Score is the basis for all other scores. The scores are computed by looking at the users who are in the group (locations, cities, and departments) or accessing a particular application. The lowest ZDX Score for each user over the time frame is taken, and the scores are averaged to derive the ZDX Score for the group or application.

Learn more at About the ZDX Score (https://help.zscaler.com/products/zdx/zdx-score).

ZDX Dashboard

The ZDX dashboard provides information focused on impacted application performance across your organization. The goal of this dashboard is to quickly view your overall application performance and drill down to impacted users and locations. Note that this dashboard always displays the applications with the lowest ZDX Score, even if the low scores are still in the good range.

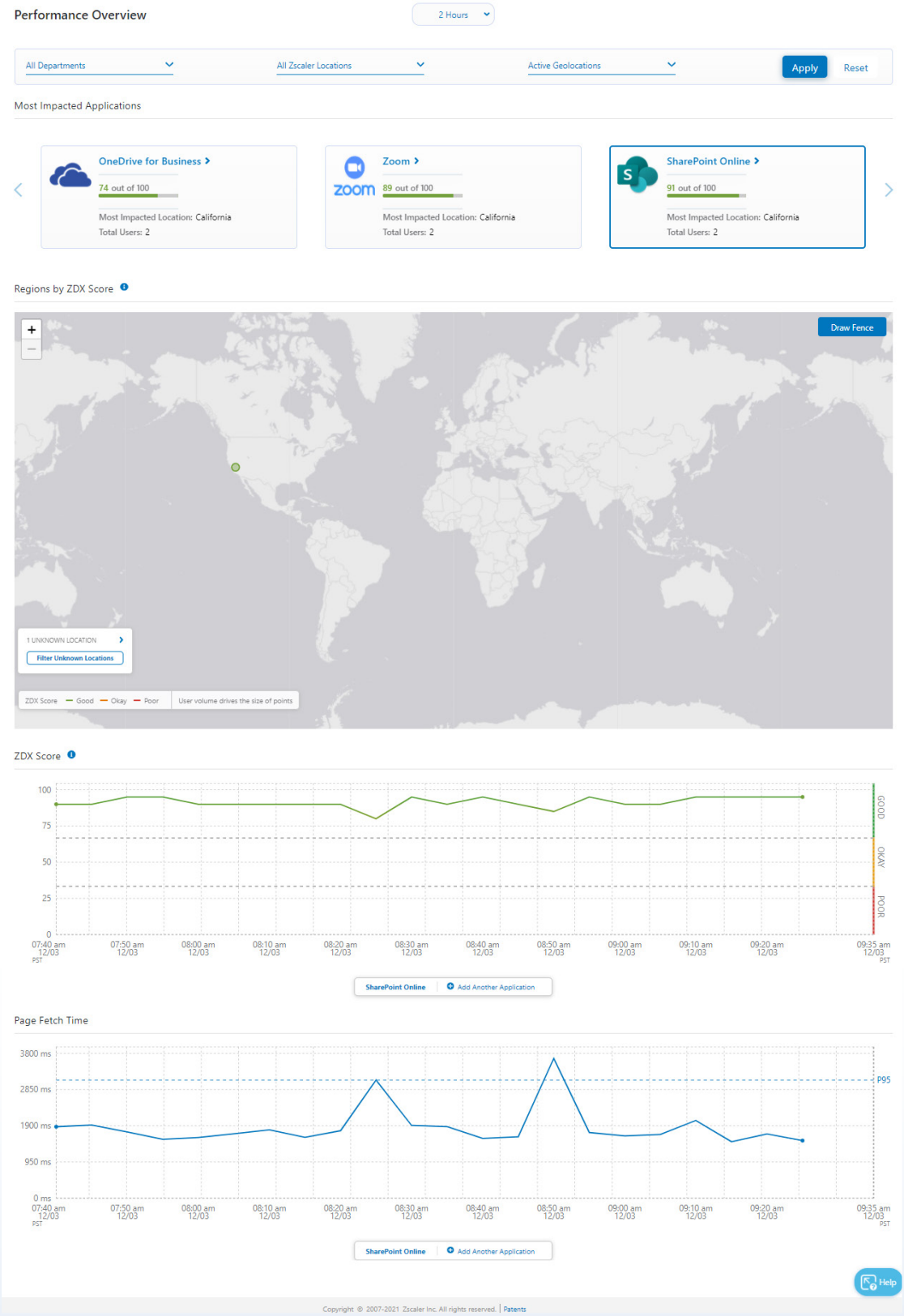


Figure 16: The ZDX dashboard

The dashboard provides filters that allow you to narrow your results by selecting Departments, Zscaler Locations, and Geolocations, as well as more advanced options. The reporting time frame is also adjustable. By default, the dashboard shows the last 30 minutes of activity, but can be set to view specific times up to 14 days in the past.

The dashboard provides 4 widgets to quickly view the impact of applications:

- **Most Impacted Applications** – Shows the applications with the lowest ZDX Score across the selected time frame. The lowest three applications are shown on the front page of the dashboard. The application with the lowest score is preselected when you open the dashboard. Clicking on the name of the application takes you to the Applications Overview Dashboard with that application selected.
- **Regions by ZDX Score Map** – An interactive map that shows where your users are who are accessing the selected impacted application. Each city receives a ZDX Score based on the users in that region accessing the selected application. The Regions by ZDX Score Map also allows you to select multiple locations as a filter by drawing a custom fence around the locations that you can use to filter the Applications Overview Dashboard and the User Overview Dashboard.
- **ZDX Score Graph** – Shows a ZDX Score trend line over the selected time frame. You can add up to 4 additional applications to the graph, which can be used to help you see a more widespread network congestion or hosting provider outage by viewing a range of applications.
- **Page Fetch Time** – Shows a graph that tracks how long in milliseconds it takes for the application to transfer the requested page. An overlay line is drawn to indicate where 95% of the page load times are at or below, allowing you to focus on outliers. You can add up to 4 additional applications to the graph for comparison across the same time frame.

The ZDX dashboard allows you to get a sense of your overall organization's ability to access your applications. You can use it to see which applications are impacted and which users are experiencing poor performance.

Learn more at Monitoring the Performance Dashboard (https://help.zscaler.com/zdx/monitoring-performance-dashboard).

Applications Overview Dashboard

The Applications Overview dashboard is designed to give you visibility into the applications your organization is using and how they impact your users. This dashboard presents an overview of all applications defined in ZDX, including any disabled applications. This dashboard has a filterable list of your applications that can be sorted by Application Name, ZDX Score Trend, Most Impacted Location, Most Impacted Region, and Most Impacted Department.

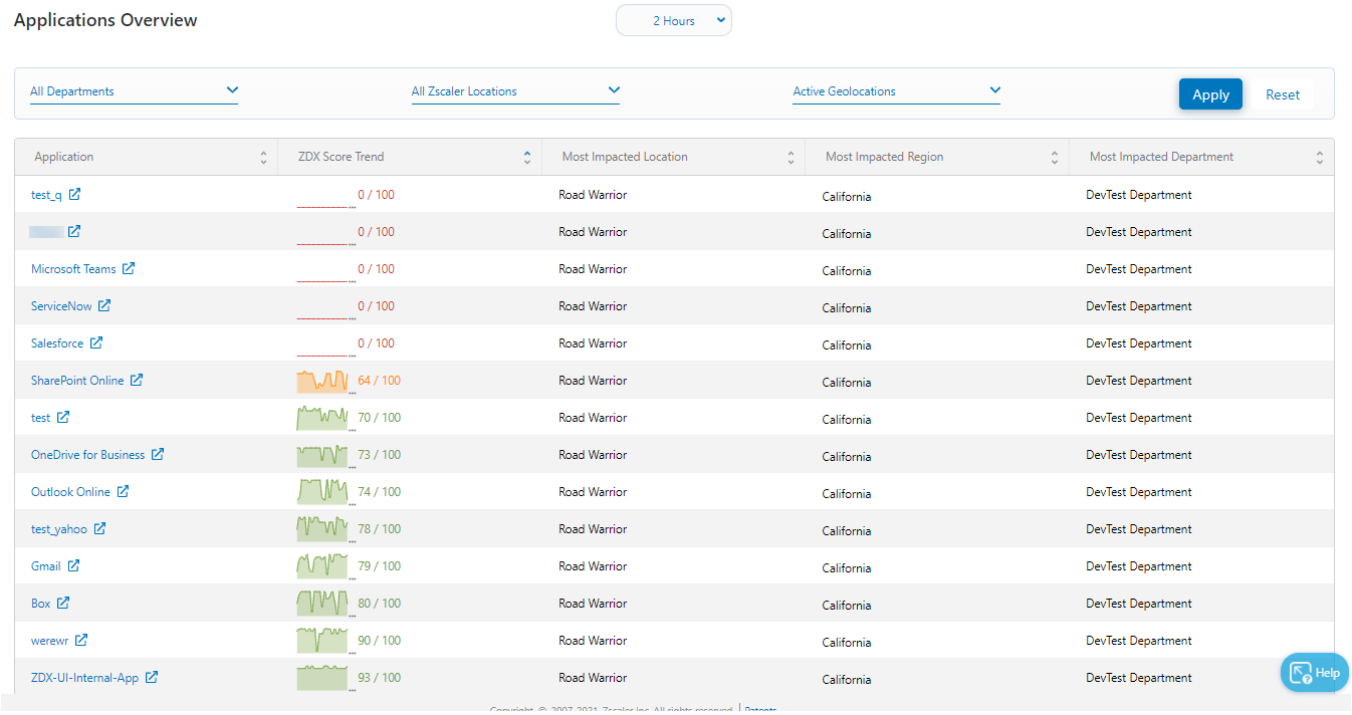


Figure 17: The ZDX Applications Overview dashboard

Using these filters, you can narrow the table results to identify performance issues related to your applications, users, and sites. When you find an application requiring more investigation, click the application to open a more detailed view of the application and its performance.

When the detailed view is opened, you see similar widgets to the ZDX Dashboard page with much greater detail about the application:

- **ZDX Score Graph** – Shows a ZDX Score trend line over the selected time frame. You can add up to 4 additional applications to the graph, which can be used to help you see a more widespread network congestion or hosting provider outage by viewing a range of applications.
- **Page Fetch Time** – Shows a graph that tracks how long in milliseconds it takes for the application to transfer the requested page. An overlay line is drawn to indicate where 95% of the page load times are at or below, allowing you to focus on outliers. You can add up to 4 additional applications to the graph for comparison across the same time frame.
- **Regions by ZDX Score Map** – An interactive map that shows where your users are who are accessing the selected impacted application. Each city receives a ZDX Score based on the users in that region accessing the selected application. The Regions by ZDX Score Map also allows you to select multiple locations as a filter by drawing a custom fence around the locations that you can use to filter on this dashboard and the User Dashboard.
- **Impacted Departments** – A list of the departments with the lowest ZDX Scores reported by that department's users' ZDX probes.
- **Impacted Regions** – A list of the regions with the lowest ZDX Scores reported by users' ZDX probes from the region.
- **Impacted Zscaler Locations** – A list of the defined Zscaler locations, typically large sites, with the lowest ZDX Scores reported by users' ZDX probes from those sites.

- **Probe Status** – The results from your web probe and Cloud Path probes. Each displays information relevant to that probe, including minimum, average, and max values for each data type it displays.
  - **Web probe** – Applications performance and availability details including the URL address, Page Fetch Time, Server Response Time, DNS Response Time, and Availability as a percentage.
  - **Cloud Path probe** – Network information details between the users and the application including the URL address, Packet Loss percentage, Total Latency time, Packet Count, and Total Number of Hops.

This dashboard focuses on giving you visibility into the state of all the applications your organization is monitoring. You can find out how performance is for different groups and locations across your organization quickly by setting filters. You can see all the applications that are in use, and how performance is over time for all of them in a single view.

Learn more at Monitoring the Applications Overview (https://help.zscaler.com/zdx/monitoring-applications-overview).

User Overview Dashboard

The User Overview dashboard provides a view of your organization's digital experience from the perspective of your user population. The dashboard provides you with a view of your current users and devices, and a bar graph with all users placed into the categories of Good, OK, and Poor as discussed in Understanding the ZDX Score.

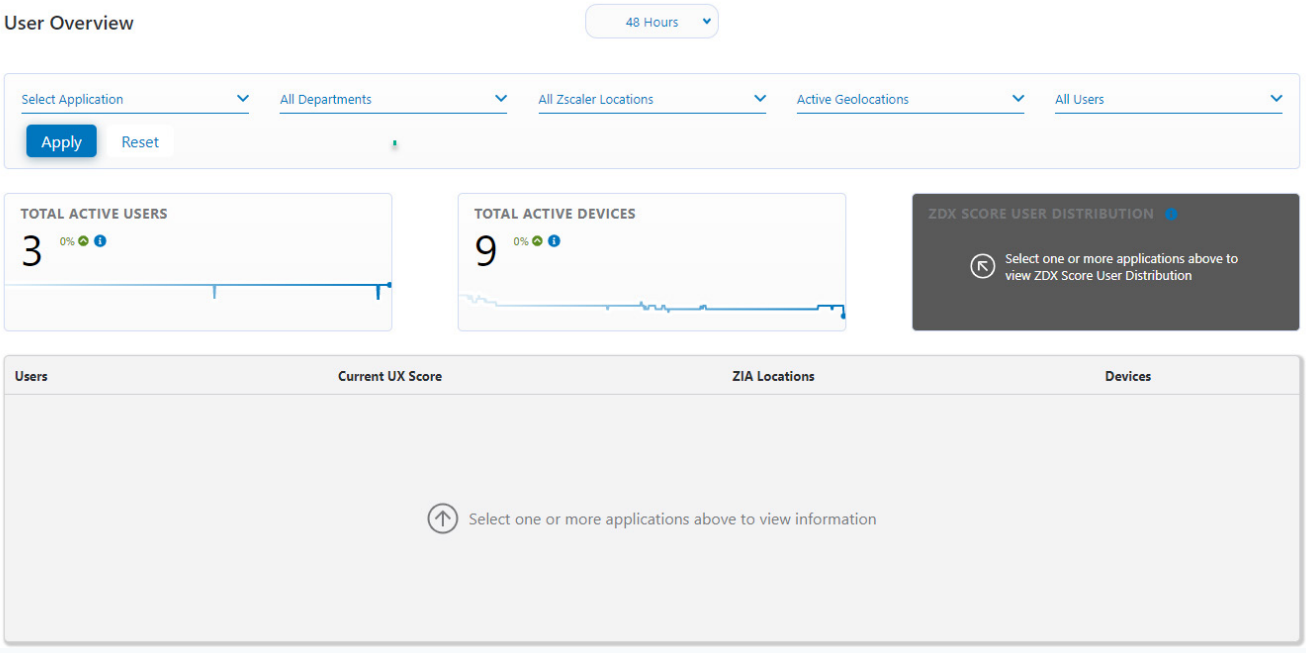


Figure 18: The User Overview dashboard

Three tables appear at the bottom of the page, one for each category, containing up to 100 users with a ZDX score matching that category. The available filters are:

- **Applications** – The applications used by users.
- **Departments** – Your departments, as defined in ZIA.
- **Zscaler Locations** – Your locations, as defined in ZIA.
- **Cities** – The cities where your users are located.
- **Users** – The names of your users.

The user information tables show information about the individual users, and each has a link to the User Details Page discussed later in this chapter. This view also provides access to start a Deep Tracing session for advanced troubleshooting of a single user. The table displays the following information about individual users, and the users shown in the table are subject to the previously mentioned filters:

- **Name** – The users name as provided by your IdP.
- **ZDX Score** – The user's ZDX score overall.
- **Zscaler Locations** – A list of locations where a user has used their device during the selected time frame.
- **Geolocations** – Areas where a user used their device during the selected time frame.
- **Devices** – All of the user's devices used during the selected time frame.

Using the filters, you can narrow down your results to focus on users who are having the most issues with their digital experience. You can also download the current table view as a CSV file for each of the three score categories should you need to share information outside of the dashboard view.

Learn more at Monitoring the Users Overview (https://help.zscaler.com/zdx/monitoring-users-overview).

Reducing MTTR with Automated Root Cause Analysis

The user details page focuses on a single user and their digital experience. In this view, you can examine the details of what is happening as the user tries to access their applications. Using this information, it is possible to narrow down where an issue is occurring for a user when they open a help desk ticket.

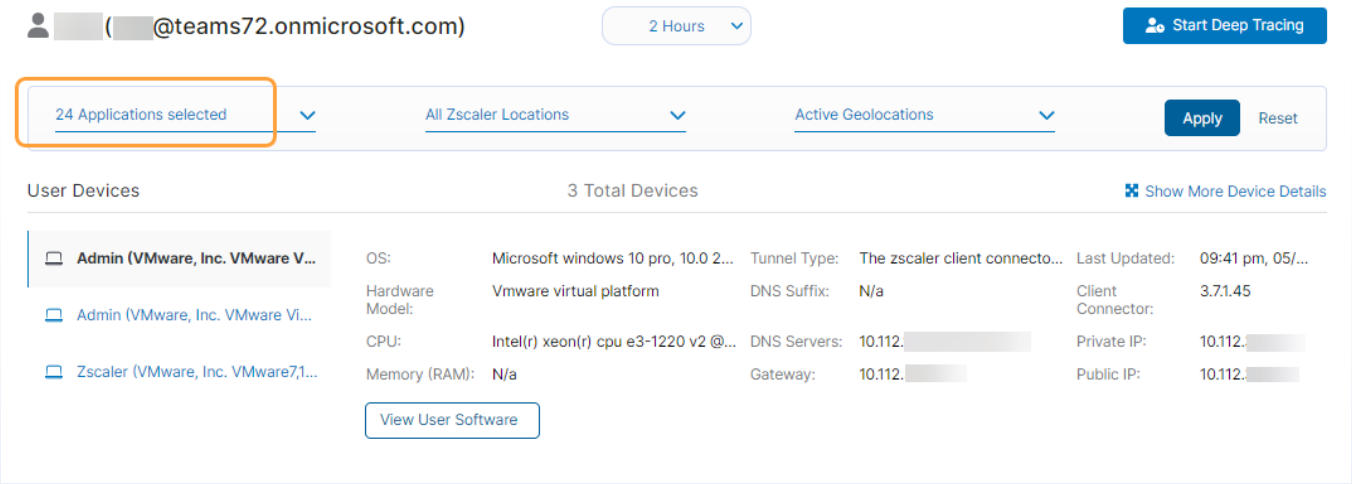


Figure 19: The user details page

As with the other dashboards, the filters you select here determine what data is visible on this dashboard. You can select from Applications, Zscaler Locations, and Active Geolocations. Time filters are also available to narrow down to the relevant data.

One of the first things displayed on the dashboard is a list of all devices in use by the user during the selected time frame. By selecting more information, you see a detailed view into the device including hardware, software, and network information. Each tab gives you more information on the device, such as hardware memory, disk, and processor. You can also view the versions of ZDX and Zscaler Client Connector installed on the device.

The next section includes the selected applications in a scrollable frame along with their ZDX Score. By default, the application with the lowest ZDX Score is selected. The application you select from this menu updates all other information fields on the dashboard.

Learn more at Evaluating User Details (https://help.zscaler.com/zdx/evaluating-user-details).

Investigating the ZDX Score

The user's ZDX Score for a particular application can be viewed both currently and historically. Data about the user's experience is available in almost real time, giving you the ability to see what is happening for the user as it is occurring. The ability to look back into probe data for 14 days is especially helpful when the help desk receives a ticket about an event that happened in the past.

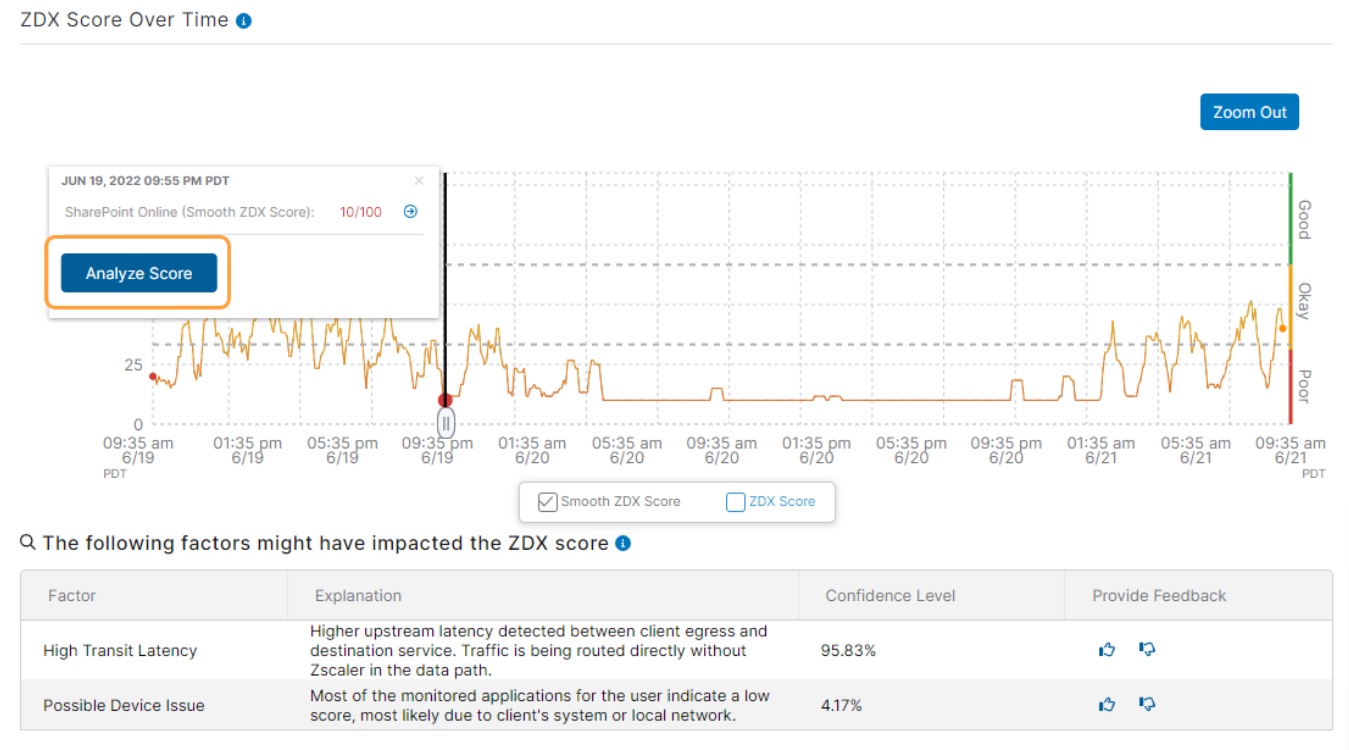


Figure 20: The user's ZDX Score Over Time graph

The following views are available to help you understand a user's ZDX Score:

- **Viewing the ZDX Score Over Time** – The ZDX Score Graph shows a ZDX Score trend line over the selected time frame. You can add up to 4 additional applications to the graph, which can be used to help you see a more widespread network congestion or hosting provider outage by viewing a range of applications.
- **Analyzing the ZDX Score for a single date and time** – When you hover over an area within the ZDX Score Over Time graph in an area with a poor ZDX Score, a tool tip appears. Click Analyze Score on the tool tip that opens. This displays a probable cause for the low score, an explanation of the issue, and a confidence level based on probes that encountered similar issues.
- **Analyzing the ZDX Score over a time range** – Similar to the previous single date and time, you can also specify a range for ZDX Score analysis. This provides a similar output over the given time frame.
- **Compare ZDX Scores** – This allows you to select a single point to a previous time. This can be the last known good score, or the same time on a previous day. The result highlights key differences in the current ZDX Score and status versus the selected comparison point.

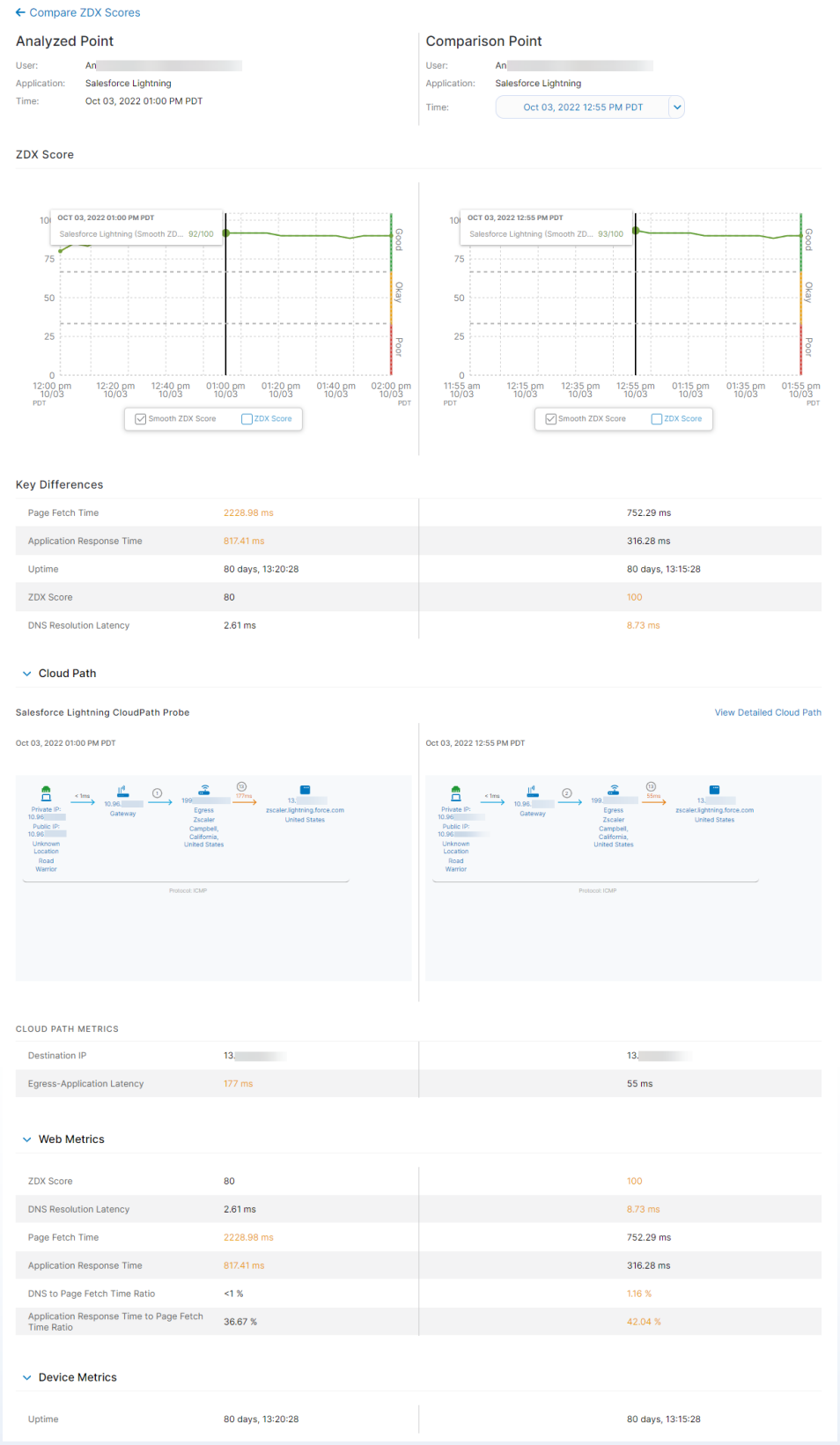


Figure 21: Comparing ZDX Scores for different users against each other

By using the ZDX Score, you can begin to narrow down the issues facing the end user. Comparing ZDX Scores allows your help desk to understand how a user's condition has degraded since a known good datapoint. ZDX also attempts to analyze and guide the help desk toward potential solutions based on the user scores.

Reducing Mean Time to Resolution with Automated Root Cause Analysis

Using the ZDX user dashboard and user details page, you can look at different data points to discover the cause of the issue. While useful, this often requires a senior support engineer to do the root cause analysis. To shorten the mean time to resolution (MTTR) of your user tickets, ZDX can automatically provide a root cause analysis for a user.

The analysis leverages artificial intelligence (AI) and machine learning (ML) capabilities of the Zscaler cloud. The system starts by comparing the different aspects of the user's experience, looking for issues with services and internet links. Because ZDX has a cloud-level view, the experience of other users accessing the same services also plays a part in determining the root cause.

Based on the cause of the low ZDX Score and other inputs, ZDX makes recommendations if the issue is within the user's control. This could include moving closer to their Wi-Fi router, updating software, or contacting their local ISP. It can also alert the help desk to an issue related to a service provider or application outage.

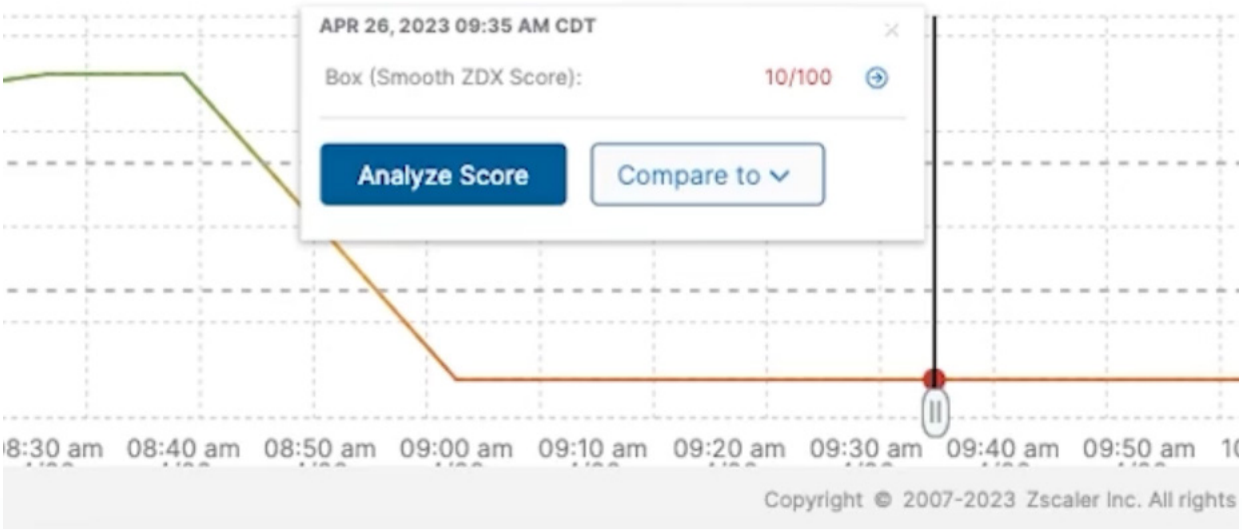


Figure 22: Hover over a data point to access additional automated analysis

To analyze the user's score, click a low ZDX Score in the graph and then select Analyze Score. This gives you a breakdown of the issue facing the user and the likely cause of the issue, such as a low Wi-Fi signal. Select the Compare to drop-down menu to select a time when the ZDX Score was good and compare the differences. You can set this to up to 14 days in the past.

As an example, when we analyze a user's ZDX Score, we see a low Wi-Fi signal was the main cause of the low score. But what changed from the previous good signal? Did the user move, did they switch Wi-Fi networks, or did they roam to a new access point (AP) in a centralized wireless local area network (WLAN)? With the compare function, we can see all the changes that have occurred.

To view a video demonstration of this feature, see ZDX Demo: AI-Powered Root Cause Analysis with Zscaler Digital Experience (https://www.zscaler.com/resources/videos/zdx-demo-ai-powered-root-cause-analysis-zscaler-digital-experience).

Investigating Web Probe Metrics

Web probe metrics are available for the application based on the user's probes. ZDX web probes collect the following information:

- **Page Fetch Time** – This metric collects the network fetch time of the web page from the URL-specified web probe. It requests only the top-level page document and does not request all embedded links within the web page.
- **DNS Resolve Time** – This metric represents the time it took to resolve the DNS name for the hostname specified in the web probe URL.
- **Server Response Time** – Time to First Byte (TTFB).
- **Availability based on the HTTP Response code** – If a success code is returned, the availability is either 1 or 0. If the probe times out, the availability defaults to 0.

The web probe metrics also display baselines for the user based on a rolling timeline of the previous 7 days. This allows you to quickly evaluate the current performance against the longer-term baseline.

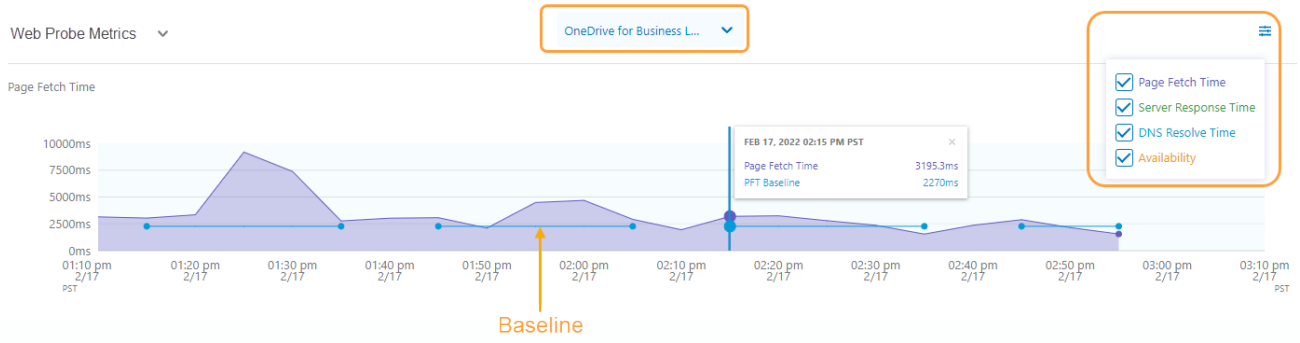


Figure 23: Web probe metrics over time

There will be times when an error is displayed for the web probes. This can be a notification that the probes are being rate limited, a warning that something might need to be updated, or that a critical error has occurred and should be investigated.

Learn more at Web Probe Errors (https://help.zscaler.com/zdx/web-probe-errors).

Cloud Path Probe Metrics

Cloud Path gives you the visibility to see into the device's data path and what is happening on the internet. When viewing Cloud Path probe data, there are two views: latency or packet loss, and a hop-by-hop view of the user's network experience between their device and the application.

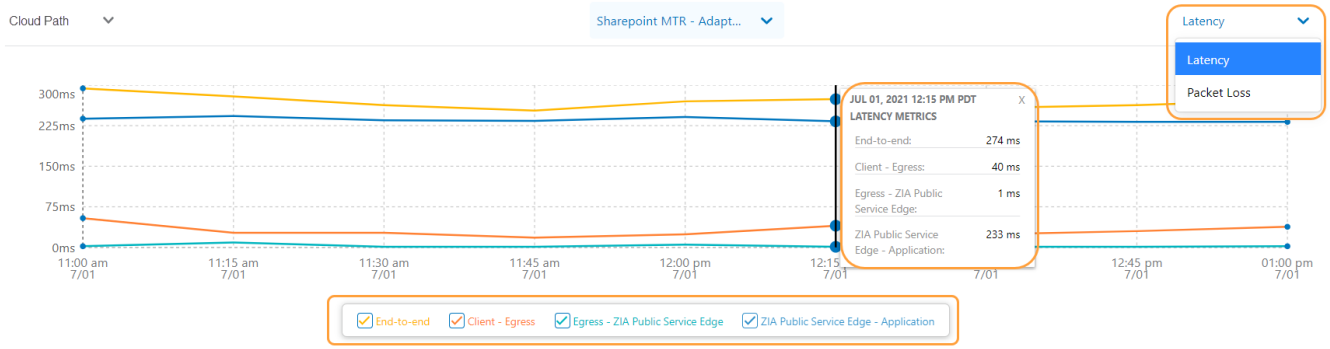


Figure 24: Cloud Path metrics over time

In the Latency or Packet Loss graph, you can select one of the two metrics to display. The graph allows you to hover to discover details about that point in time including the total end-to-end time. You can also view different parts of the path including how long it takes from the ZIA Public Service Edge to the application.

The view that most users find extremely helpful in narrowing down issues is the hop view showing the various hops in the network path from end-user device to application. In this view, you can quickly see the latency between each hop in the network path. The hop with the highest latency is displayed in orange. If a ZIA Service Edge or ZPA Service Edge sits in the network path, it shows the latency between the user and the application on each side of the ZIA Service Edge or ZPA Service Edge.

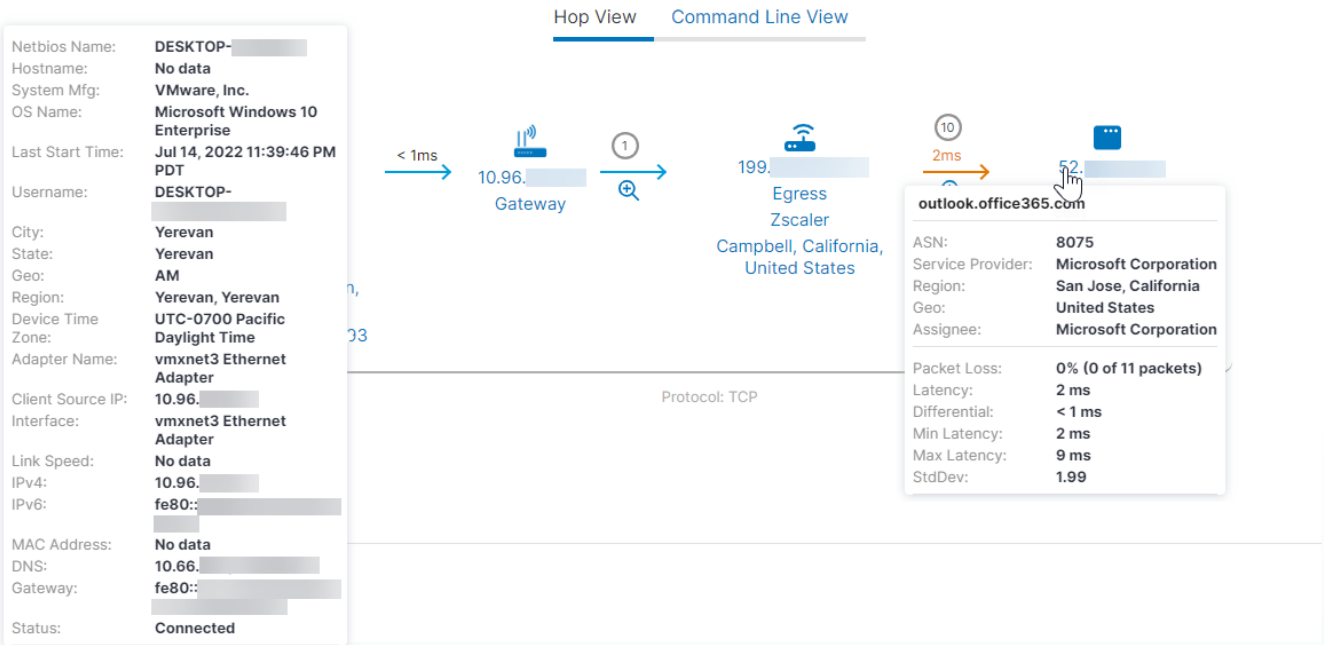
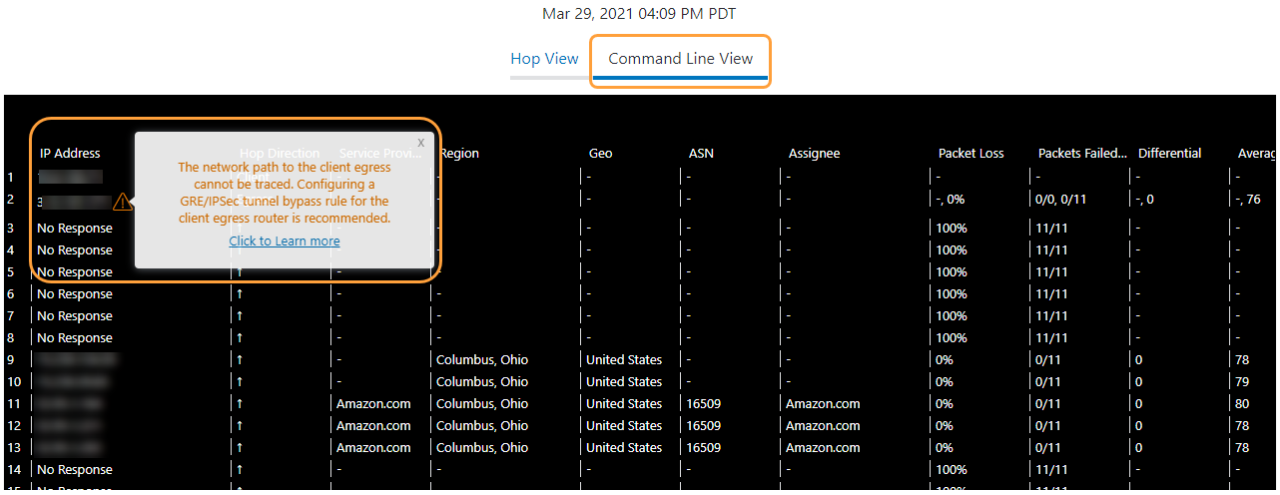


Figure 25: Hop view gives you details about the path from your user to an application

You can hover over components in the path to see the details ZDX has collected about that hop. This data varies by device and can include information such as device identification and information, the service provider, latency details, packet loss, hop count, IP addressing, Zscaler location, and geolocation. ZDX also attempts to show the path that exists when tunnels such as GRE or IPSec are in use.



	IP Address	Region	Geo	ASN	Assignee	Packet Loss	Packets Failed...	Differential	Averag
1		-	-	-	-	-	-	-	-
2		-	-	-	-	-, 0%	0/0, 0/11	-, 0	-, 76
3	No Response	-	-	-	-	100%	11/11	-	-
4	No Response	-	-	-	-	100%	11/11	-	-
5	No Response	-	-	-	-	100%	11/11	-	-
6	No Response	-	-	-	-	100%	11/11	-	-
7	No Response	-	-	-	-	100%	11/11	-	-
8	No Response	-	-	-	-	100%	11/11	-	-
9		Columbus, Ohio	United States	-	-	0%	0/11	0	78
10		Columbus, Ohio	United States	-	-	0%	0/11	0	79
11		Columbus, Ohio	United States	16509	Amazon.com	0%	0/11	0	80
12		Columbus, Ohio	United States	16509	Amazon.com	0%	0/11	0	78
13		Columbus, Ohio	United States	16509	Amazon.com	0%	0/11	0	78
14	No Response	-	-	-	-	100%	11/11	-	-

Figure 26: Command line view of network hops

Using this information, you can quickly narrow down where issues are occurring for the user and act to remediate the situation. Being able to quickly spot network path issues is critical to troubleshooting and ensuring that the correct issue is being addressed.

There will be times when an error is displayed for the Cloud Path probes. This can be a notification that is informational only, a warning that something might need to be updated, or that a critical error has occurred and should be investigated.

Learn more at Cloud Path Errors (https://help.zscaler.com/zdx/cloud-path-errors).

Examining Device Health and Events

ZDX also assists your help desk in understanding the state of the user's machine over time by recording both Device Health information and Device Events that have occurred. By examining this information, you can see where device performance or a recent change to the device configuration created a user experience issue.

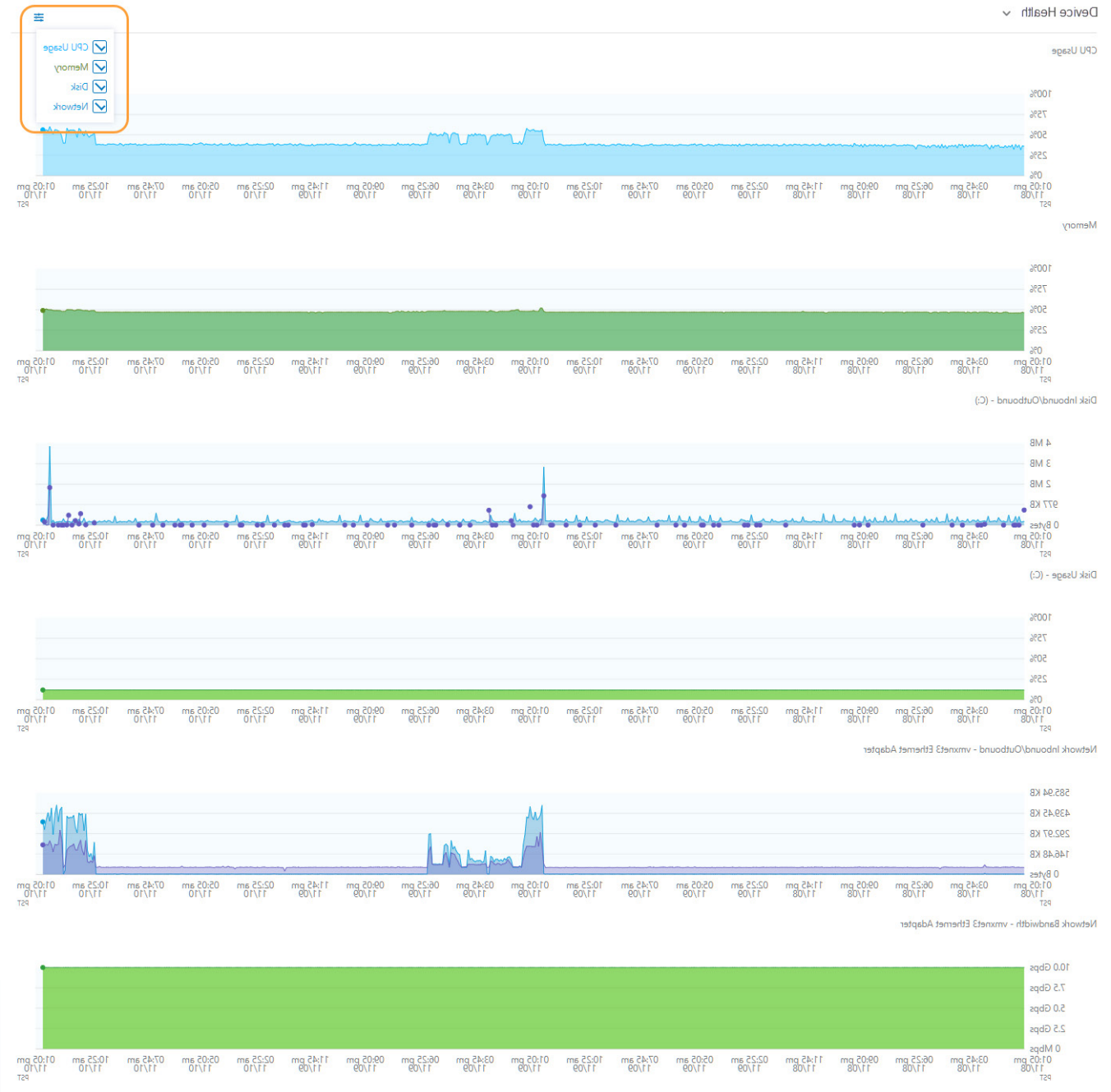


Figure 27: The Device Health dashboard gives you a look at the user's machine and its performance

The Device Health dashboard shows the following information about the state of the device for the selected time frame:

- CPU usage displayed as a percentage
- Memory usage displayed as a percentage
- Disk Inbound/Outbound (I/O) traffic
- Disk usage displayed as a percentage
- Network Inbound/Outbound traffic and the name of the network adapter
- Network bandwidth and the name of the network adapter

From these statistics, you can tell if the user device is potentially causing the experience issues. For a more detailed view, you can click any of the graphs and see the top 5 processes across CPU, Memory, Disk (I/O), and Network (I/O).

The User Device Events are used to track changes in a device configuration over the selected time frame. You can see when things changed, such as a network adapter connecting to a new network and receiving new DNS information, or when a device has gone to sleep. Together these indicators can help you discover where a device has become impacted and any changes that might have led to the event.

Software Inventory

Software Inventory is an advanced feature that allows you to view the installed software across your organization. The inventory shows the number of software packages, number of software versions, total number of users leveraging that software, and the number of software vendors currently in use. The software is displayed as a set of color-coded tiles. Each vendor has its own color, and the size of its tile is related to the number of installations in your organization.

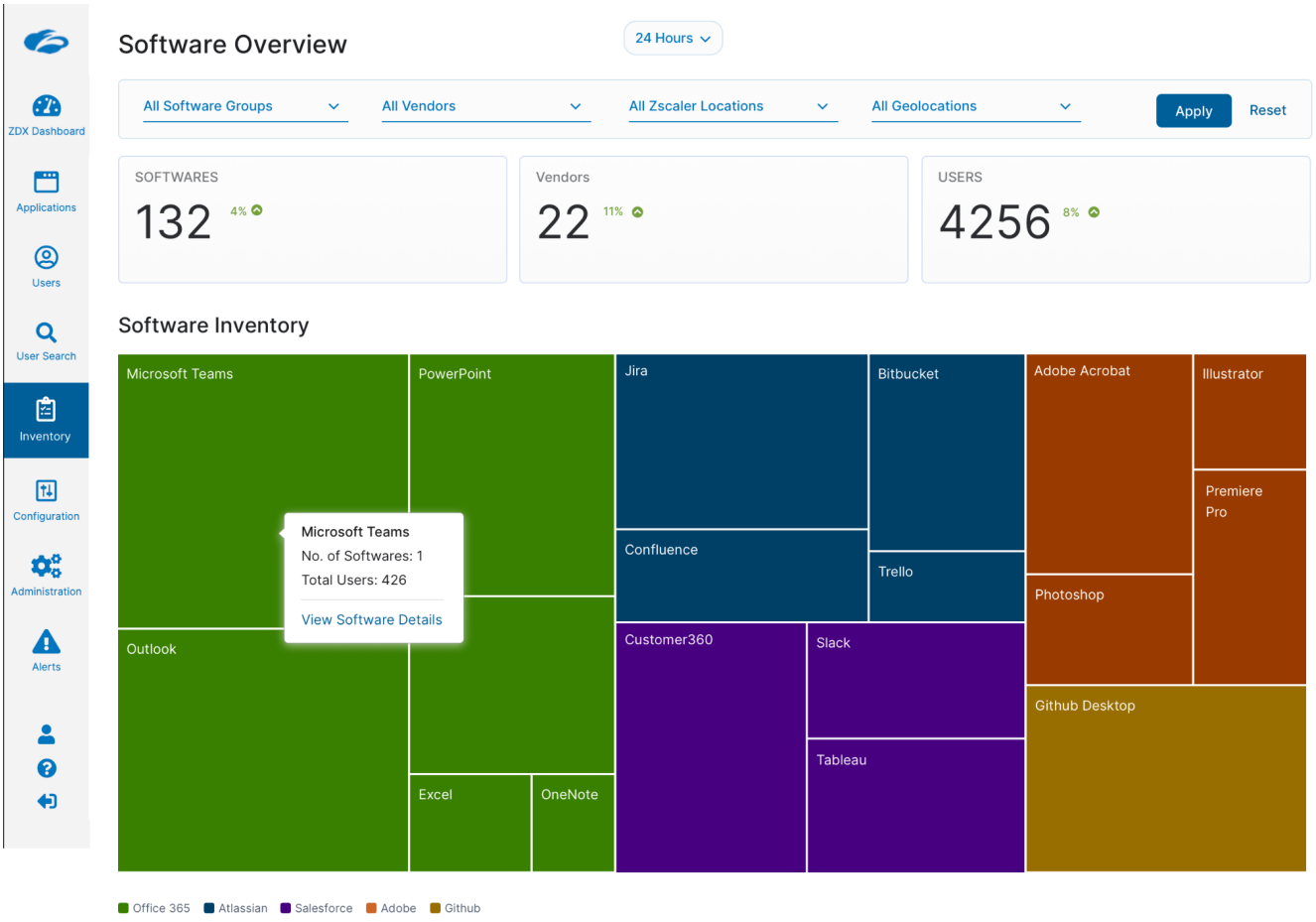


Figure 28: The Software Inventory page with applications grouped by vendor and scaled by user count, with hover-over details showing the number of versions and users

As with other dashboards, you can use filters to narrow the results of your search. The following filters are available for software inventory:

- **Software App Groups** – Supported vendor software or individual applications, grouped by name.
- **Vendors** – Software or application vendors.
- **Zscaler Locations** – The list of locations where a user accessed a device, as defined in ZIA.
- **Geolocations** – The geographic areas where users accessed their devices.

When you locate the software package you are interested in investigating, hover over the application to see the number of ZDX applications and user installations for that package. To view the details, click any software package. If there is more than one version available, you are presented with a table in the Software Inventory page and asked to click the version you want to see. If only one version is available, you are taken immediately to the software details page.

The Software Inventory page presents a table structure with information about the software and versions in use in your organization. This table summarizes the details with the following values:

- **Name** – The software or application version name.
- **Vendor** – The software or application provider.
- **Software Group** – The group name to which the software or application belongs.
- **Users** – The number of software or application users.
- **OS** – The operating system on which the software or application is run.
- **Software Version** – The numbered version of the software or application.
- **Install Type**:
  - **32-bit** – Installed for all users.
  - **64-bit** – Installed for all users.
  - **Current User** – Either 32-bit or 64-bit installed only for the current user.

When you click the application or the software details, you see granular information about a specific version of an application or software. The high level at the top of the page gives you an overview of the software. It includes the number of users who have the software version installed, the distribution of operating systems running the software, and how many users are running each of the different versions currently in use in your organization.

Below the dashboard is a table of installed users. This table can be filtered to help you discover who is running a particular version of software and its history on that machine. The table includes the following fields:

- **Device** – The hardware device on which the software or application is running.
- **User** – The name of the user running the software or application.
- **Software Version** – The numbered version of the software or application.
- **OS** – The operating system on which the software or application is run.
- **Location** – The folder on the user's system where the software or application can be found.
- **Install Date** – The date when the software or application was originally installed.
- **Version History** – Launches a window that displays the date when the software or application was last updated.

This can help you gain insights into when applications are updated and performance changes for the end user. You can also use the report to view users with a problematic or outdated version of the software in question.

Software Inventory is not available on the standard plan. To view the supported range and feature availability by subscription level, see the Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf).

Learn more at Viewing Software Inventory (https://help.zscaler.com/zdx/viewing-software-inventory).

Device Inventory

Device Inventory is an advanced feature that allows you to view the devices in use across your organization. The inventory shows the OS and hardware models of devices connected to ZDX. Like other dashboards, you can filter based on Device Vendor, Device Model, Zscaler Locations, and Geolocations.

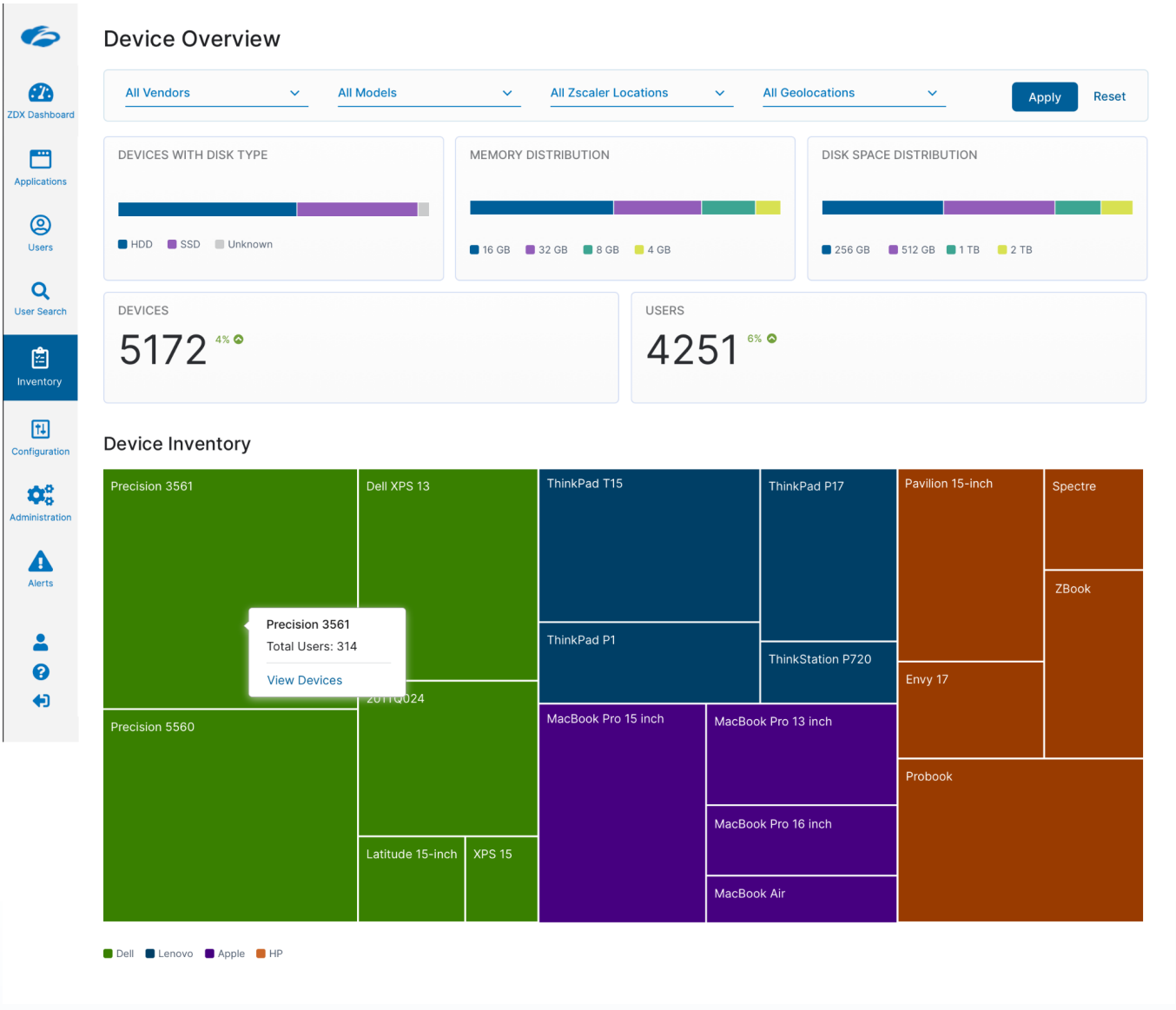


Figure 29: The Device Overview page with applications grouped by vendor and scaled by user count

The initial view gives you a look at the numbers of devices and users, the memory installed on devices, and the OS version. A set of tiles representing each detected OS allows you to quickly view the distribution of devices in your network. The tiles are scaled to represent the number of devices with that OS operating, and you can hover over each to see how many users are on a particular OS.

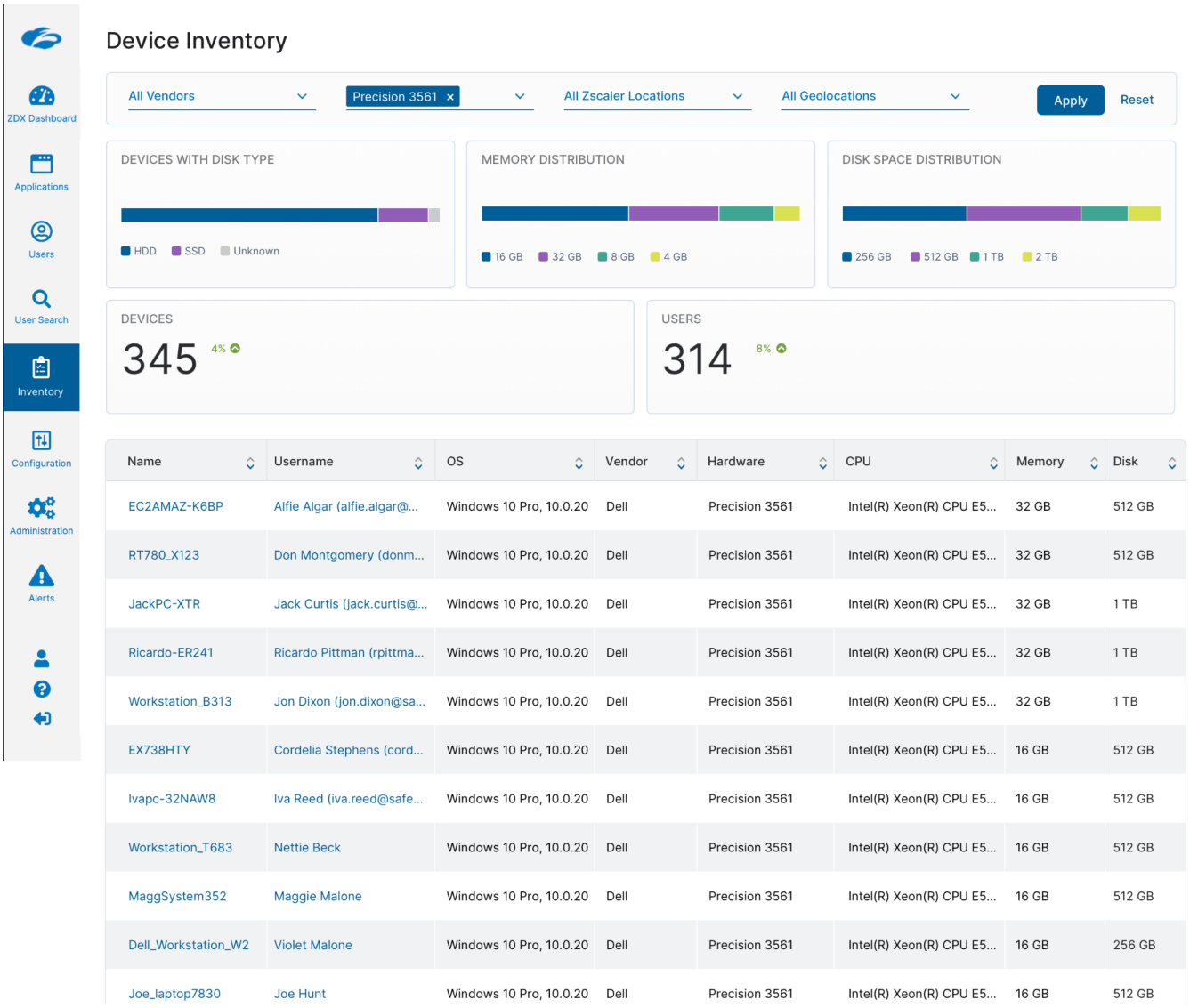


Figure 30: The Device Inventory page displays your devices with details

The table displays the following fields:

- **Name** – The vendor device name, with model and OS.
- **User** – The device user.
- **OS** – The operating system running on the device.
- **Vendor** – The name of the device provider.
- **Hardware Model** – The specific model name of the device.
- **CPU** – The processor model.
- **Memory (RAM)** – The amount of memory installed on the device.

When you click one of the tiles, you are taken to the Device Inventory page, where you see the devices with that OS installed and more details about the devices themselves. The tabular view of the Device Inventory page provides more comprehensive details about individual machines. Click a device on the Device Inventory page to open a more detailed view of the device, with tabs for hardware, network, and software information.

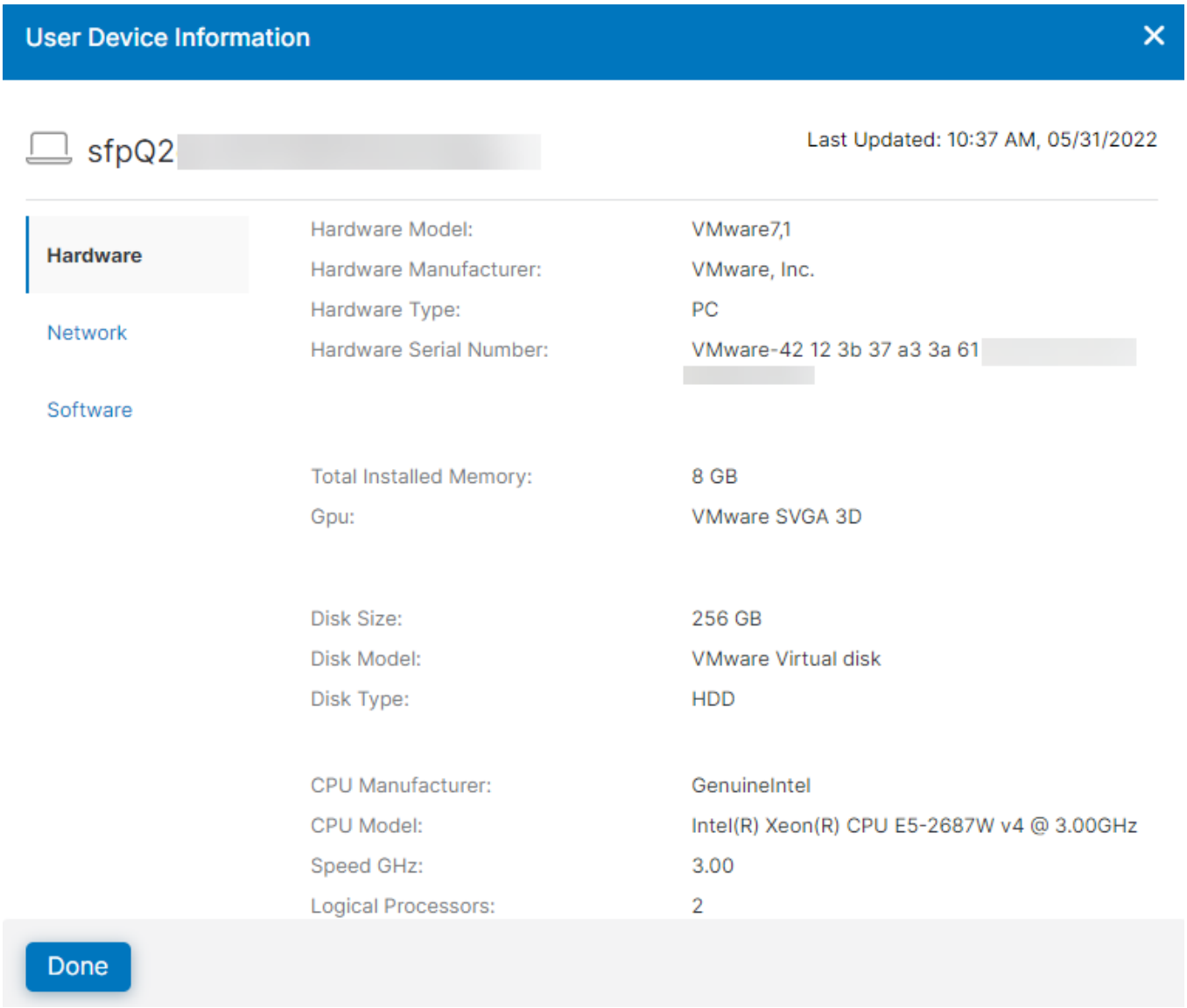


Figure 31: The User Device Information page gives you more information on how the device is operating and any incidents that have occurred

This detailed view of devices can be helpful when looking for outdated software or hardware still in use. This is useful for organizations to quickly locate users holding on to outdated hardware or software. This table is also useful if your organization operates in a BYOD model. You can quickly find out which devices your users are bringing into your organization and evaluate their use and software compliance.

Device Inventory is not available on the standard plan. To view the supported range and feature availability by subscription level, see the Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf).

Learn more at Viewing Device Inventory (https://help.zscaler.com/zdx/viewing-device-inventory).

Understanding ZDX Alerts

ZDX alerts allow you to take a proactive approach to monitoring your users' digital experience. Instead of waiting for a ticket or call, your operations team can be notified when an issue starts to affect multiple users or regions, or if an application becomes unavailable. Alerts are based on rules you create, allowing you to be flexible about report criteria and notification.

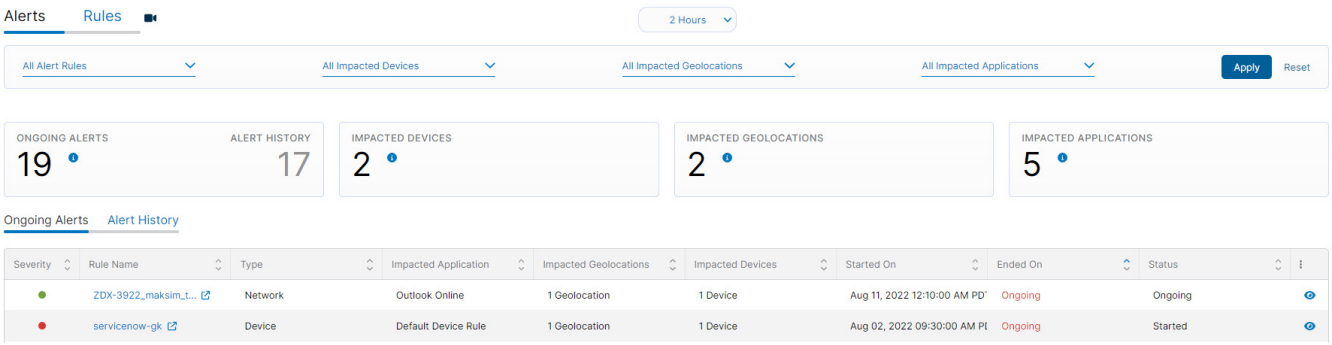


Figure 32: The ZDX Alerts page

The Alerts page in the ZDX Admin Portal allows you to view the status of your organization by summarizing the status of any ongoing alerts. The top of the page shows a count of Ongoing Alerts, along with an Alert History going back 14 days. The summary also shows how many devices, geolocations, and impacted applications are related to the current alerts. Filters are available for each of these fields so that you can quickly triage events and route tickets appropriately.

Below the summary tiles is a table listing alerts that you can quickly view and filter, with tabs for current and historical alerts. The alert table shows the following fields:

- **Severity** – The severity level of the event. Red indicates high severity, orange is medium severity, and green indicates low severity.
- **Rule Name** – The name entered for the rule at configuration.
- **Type** – The type is Application, Network, Device, or ZDX Score.
- **Impacted Application** – The application impacted by the alert.
- **Impacted Geolocation** – The geolocation impacted by the alert.
- **Impacted Devices** – The devices impacted by the alert.
- **Started On** – The date and time the alert was triggered.
- **Ended On** – The date and time the alert ended. If it is an ongoing alert, then the column indicates Ongoing.
- **Status** – The status of the alert.

By default, the alerts are shown in a table sorted based on the Ended On field, but any of the fields can be used as a filter. Alerts are hyperlinked and open in a new tab when clicked. This allows you to open multiple alerts at the same time for comparison.

Learn more at About Alerts (https://help.zscaler.com/zdx/about-alerts).

Rules for Alerts and Triggering an Alert

ZDX offers a flexible framework to build alerting rules. New rules are configured via a wizard in the interface that allows you to build rules based on previous configurations. ZDX uses these configurations to decide when an alert should be sent.

Before you configure a rule, it's important to know what it is you want to be notified about proactively. Ideally this would be based on a past event, and the details of that event can help inform the rule design. The details we are looking for are parameter values that describe a poor experience for your users.

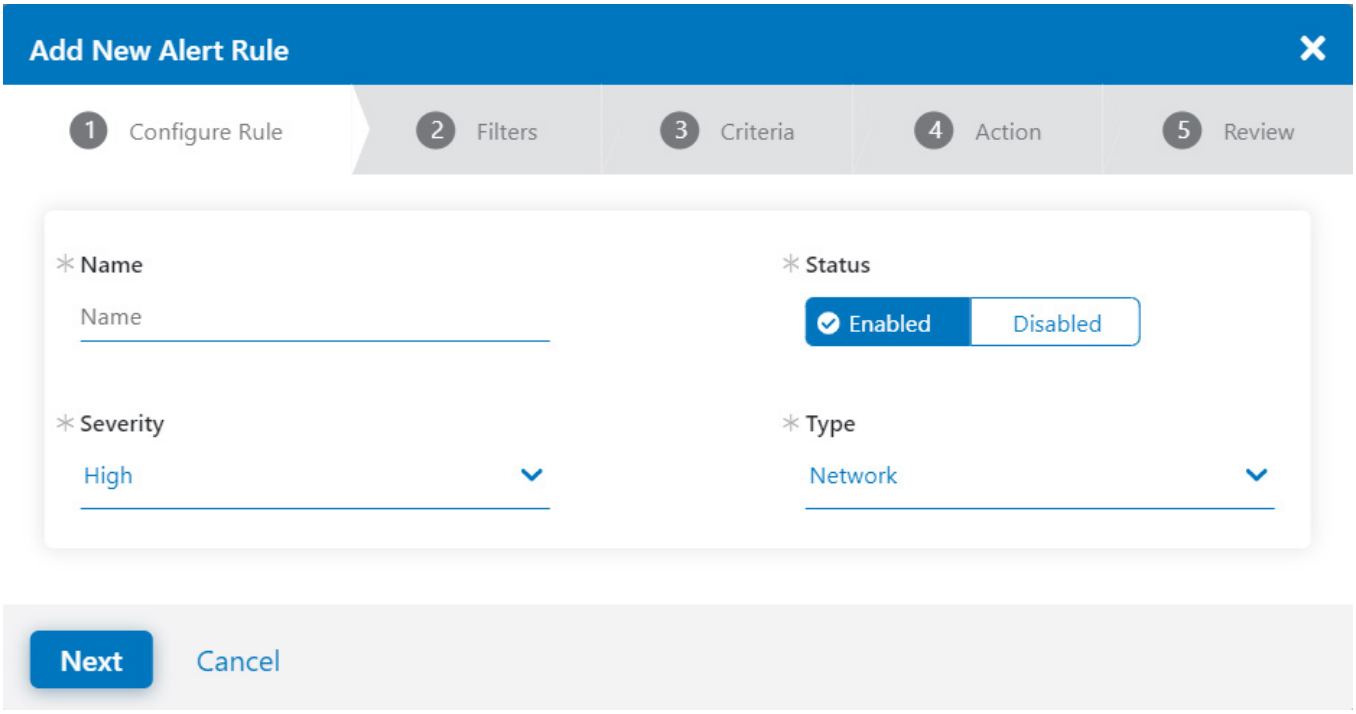


Figure 33: The ZDX alert rule configuration wizard

For example, if you know that an application you deployed has been experiencing stability issues, you want your operations team to be notified when an outage is occurring so that they can troubleshoot the issue in real time. For this, you can create an alert rule to trigger an action when the outage is occurring. The settings you choose for the rule should be based on your actual experience with the application. You might use a rule to alert when more than 20 users in the same city experience loss of an application.

There are 4 rule types for alerts, and you should pick the one that best matches your goal and the data that indicates a degradation in service:

- **ZDX Score** – You are asked to group your ZDX Score for the alert by Departments, Cities, Organization, Region, or Zscaler Locations.
- **Applications** – These are the applications you have configured for monitoring by ZDX.
- **Devices** – These are devices that are connected.
- **Zscaler Locations** – Any configured ZIA locations can be used.

Based on the rule type, you are presented with a set of choices and filters related to that rule type. This also affects your criteria matches, as those also relate to the alert type you selected. As an example, an application rule type would require you to select the application and its associated web probe. You can select Locations, Geolocations, Departments, User Groups, Users, and Devices as filters, which allows you to specifically target locations or user populations to monitor.

The criteria section allows you to select values to monitor and alert on, and are dependent on the error you are trying to capture. This could be poor network performance at a branch or campus location, or low ZDX Scores across a region or city. Your criteria options are based on your alert type and change with that selection. You can add any or all the criteria available for that alert type when defining your alert rule. Depending on the criteria type, you can specify your values as a percentage or in milliseconds as appropriate.

However, triggering on any single user with a poor digital experience can lead to a lot of noise in the system. For a single user, it is often better to let the help desk handle the routine query. To avoid seeing too many alerts, ZDX provides a throttling section to the rule to suppress alerts until some critical mass has been achieved. This system is flexible and can be adjusted after the rule is created if you see too many false positives or miss alerts due to values being too high.

When defining your alert throttling, there are three values you need to specify, and all of these values must be matched for an alert to be triggered:

- **Alert Only if Repeated [Numerical Value] Times in a Row** – For an alert to trigger, the same error must be repeated some number of times. Zscaler recommends starting with a value of 3 and adjusting from there.
- **In Group** – Determine what group of users the alert is related to from Departments, Cities, Organization, or Regions.
- **Minimum Devices Impacted** – This value can be either a number or a percentage of your devices in the group you select.

Finally, you must select an action to take when the rule is matched. First, you can choose to be notified or to mute notifications. Muted notifications are still visible on the Alerts page but do not trigger any additional action by the ZDX Alert rule. This is useful when you are building out new rules so that you can monitor their frequency and effectiveness. It is also useful in cases where you are interested in monitoring a particular aspect of your users' digital experience over time but do not require immediate notification of an event.

If you choose to enable actions, you have two choices: email notification or webhooks integration. If you select email notification, you need to specify an email address to receive the notification. You can also view a preview of the email, which can be helpful if you plan to automate email parsing in a third-party platform.

Webhooks allow you to set up an integration with a third-party platform such as a ticketing or automation system. Webhooks require that you provide a name and URL to receive the notification. You also need to specify an authentication method. ZDX supports both simple (username and password) and bearer token (alphanumeric string) authentication. The choice will be determined by your automation platform's support.

Webhook integration is not available on the standard plan. To view the supported range and feature availability by subscription level, see the Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf).

Learn more at:

- About Rules (https://help.zscaler.com/zdx/about-rules)
- Triggering an Alert (https://help.zscaler.com/zdx/triggering-alert)
- Configuring Webhooks (https://help.zscaler.com/zdx/configuring-webhooks)

Webhook Integration Guides

Zscaler partners with leading technology vendors in the operations space. Zscaler's help site contains vendor configuration guides for Slack, PagerDuty, Splunk, and ServiceNow. For example, you can set up a webhook to integrate with the ZDX application in ServiceNow. This integration allows you automatically generate tickets in your ServiceNow instance. By installing and integrating the ZDX application in ServiceNow, you can be alerted to network conditions affecting the user before the need to generate a ticket. Troubleshooting integration allows your help desk agents to begin Diagnostics sessions directly from the ServiceNow interface.

- Learn more about configuring a ServiceNow integration in our guide Zscaler and ServiceNow Deployment Guide (https://help.zscaler.com/downloads/zscaler-technology-partners/data/zscaler-and-servicenow-deployment-guide/Zscaler-ServiceNow-Deployment-Guide-FINAL.pdf).
- You can view a video of the steps required to integrate ZDX with ServiceNow at Zscaler Digital Experience and ServiceNow (https://www.youtube.com/watch?v=5DMrNB8jCWY).
- Learn more at Webhook Configuration Guides for Supported Platforms (https://help.zscaler.com/zdx/alerts/webhook-configuration-guides-supported-platforms).
- Find out more about Zscaler's integration ecosystem at Zscaler Technology Partners (https://www.zscaler.com/partners/technology).

Tuning Alerts to Reduce False Positives

As you build up your alert rules, you'll want to monitor their effectiveness to reduce false positives and ensure you are capturing real events. ZDX allows you to adjust the operation of your alerting rule by modifying the rule. Depending on the alert type you selected, you can modify fields in the rule.

The most common change is to modify the throttling values for the rule. Often the values are initially too lax or strict and need to be adjusted. As an example, you might find that your rule is triggering too often at 3 repeated alerts, and you need to adjust the value to 5.

Criteria changes are also possible in the rule. The criteria changes are made to modify, replace, remove, or add criteria to a rule to reduce excessive or incorrect matches for the rule. As an example, you might find that matching a region is too broad for the alert type you selected, and city would be a better gauge.

Learn more at Editing an Alert Rule (https://help.zscaler.com/zdx/editing-alert-rule).

Advanced Call Quality Reporting for Microsoft Teams, Zoom, and Webex

Monitoring your unified communications platforms has taken on greater importance as remote and hybrid work become the norm. ZDX supports monitoring direct calls and meetings between two or more participants using Microsoft Teams, Zoom, or Webex. The ZDX Score for Call Quality can reflect either a Mean Opinion Score (MOS) average, or metric thresholds for latency, jitter, and packet loss.

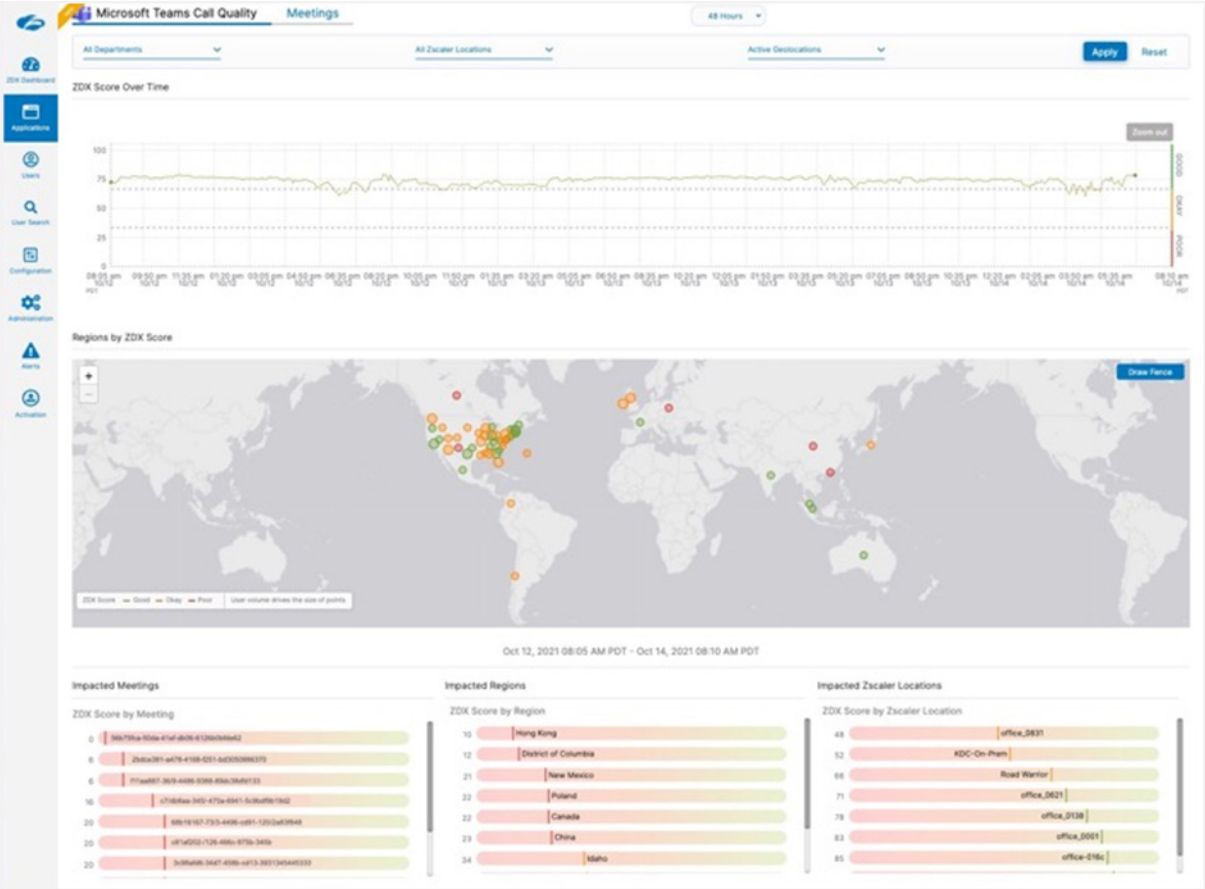


Figure 34: The Microsoft Teams Call Quality page

The ZDX Microsoft Teams, Zoom, and Webex dashboards have the following benefits:

- Find all relevant telemetry data in one place and gain insights starting with a scoring framework (ZDX Score).
- Gain operational efficiencies by allowing network, application, and service or help desk to gain common context and collaborate.
- Triage Microsoft Teams, Zoom, and Webex performance issues quickly, decrease resolution times, and optimize user productivity.

Call monitoring is reported after the call completes. Currently, call quality metrics are only reported after a call by both Microsoft Teams, Zoom, and Webex.

Call Quality reporting allows you to gain a deeper insight into trends with your unified communications calling. When your help desk receives a ticket, they can diagnose reasons for poor call quality and take the appropriate steps to remediate the issue in the future.

Call Quality works in parallel with Cloud Path probes, device metrics, and device events to help you identify issues that are unique to a device or the network. The Call Quality report is a part of the Applications Overview page, under Microsoft Teams Call Quality, Zoom Call Quality, or Webex Call Quality.

UCaaS monitoring is not available on the standard plan. To view the supported range and feature availability by subscription level, see the Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf).

Learn more at:

- Understanding Microsoft Teams Call Quality for ZDX (https://help.zscaler.com/zdx/understanding-microsoft-teams-call-quality-zdx).
- Understanding Zoom Call Quality for ZDX (https://help.zscaler.com/zdx/understanding-zoom-call-quality-zdx).
- Understanding Webex Call Quality for ZDX (https://help.zscaler.com/zdx/understanding-webex-call-quality-zdx).

Viewing Call Quality Data

Call Quality data is related to calls between two participants. You can specify date ranges up to 14 days in the past, and filter by departments, Zscaler locations, and Geolocations.

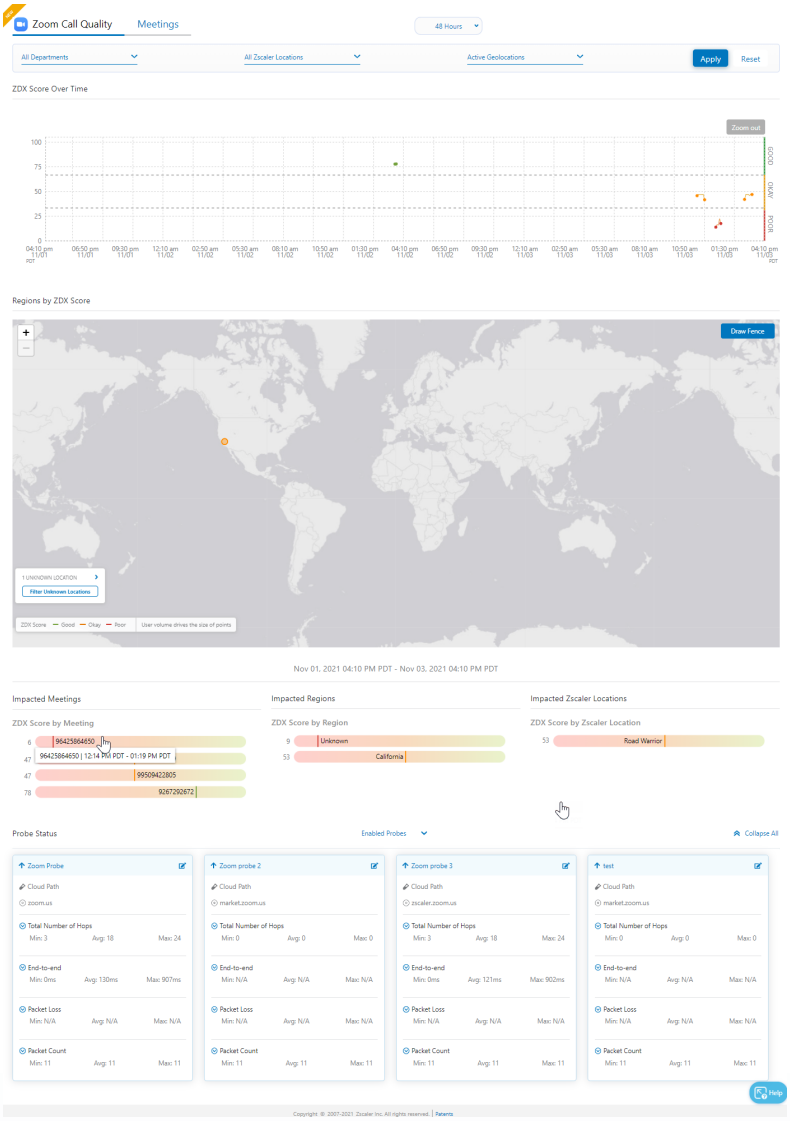


Figure 35: Call quality can be displayed for Zoom (above), Microsoft Teams, and Webex

This dashboard gives you a view of the following call data:

- **ZDX Score Over Time** – The ZDX Score for Call Quality reflects the entire duration of a call for all users. The score is based on the MOS or metric thresholds.
- **Regions by ZDX Score** – The call meeting participant locations.
- **Impacted Meetings** – The meetings with low ZDX Scores, with the lowest ZDX Score at the top. Hover over any Meeting ID to view the time and length of that meeting.
- **Probe Status** – The metrics for Cloud Path probes configured as part of the Call Quality application. Web probes are not allowed for the Microsoft Teams application.

Viewing Meeting Data

The Meetings page shows a list of meetings that have occurred and information about them. It also shows one-to-one calls that appear on the Call Quality dashboard. This tabular list can be filtered by Zscaler locations and Users who participated in meetings or calls.

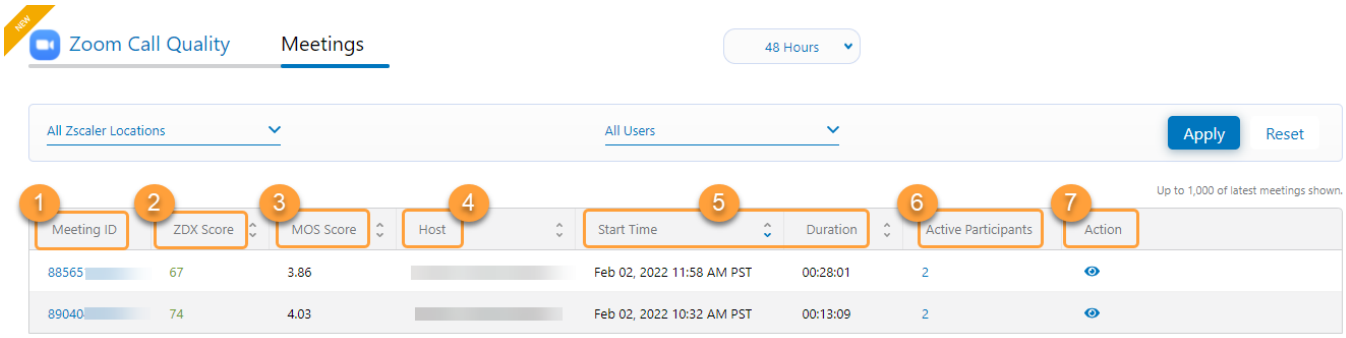


Figure 36: View specific meeting data for Zoom (above), Microsoft Teams, and Webex

- **Meeting ID** – Click any meeting ID to view meeting details. For confidentiality, the internal meeting ID is displayed, and not the actual meeting topic name.
- **ZDX Score** – The ZDX Score for Call Quality reflects the entire duration of a call for all users. The score is based on the MOS or metric thresholds.
- **MOS Score** – The MOS average might be integrated into the ZDX Score to rate a call's quality.
- **Host** – The name of the meeting host.
- **Start Time and Duration** – The length of the entire call. Partial data for meetings in progress is not captured. Ongoing calls are shown as In Progress to indicate the call has not ended. Call data for meetings in progress is captured every 5 minutes.
- **Active Participants** – The number of participants as reflected in the session data. Participants who join a call from multiple devices or who leave and rejoin a call are counted per session. This number might differ from Active Participants in the Meeting Details summary, which shows the number of participants derived from the Microsoft Graph API, the Zoom API, or the Webex API.
- **Action** – Click the View icon to view meeting details.

Clicking on a meeting ID or the View icon brings up the meeting details for that call. Metrics for your meetings are included within the user details page.

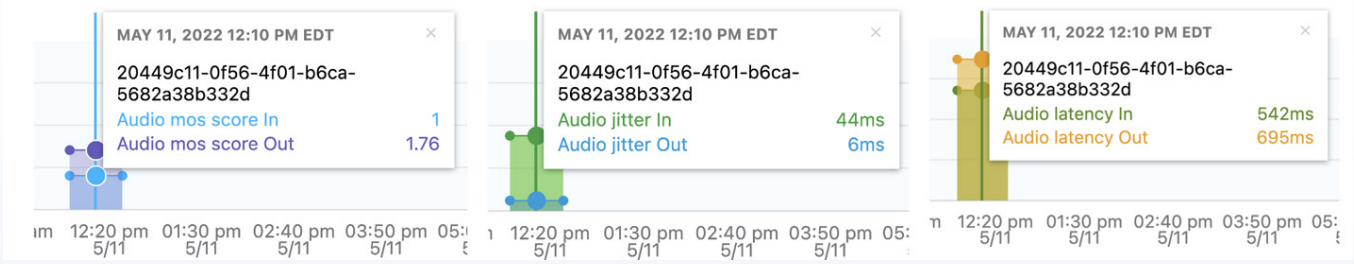


Figure 37: Meeting details allow you to quickly scan key metrics related to meeting quality

The values for Audio, Video, and Sharing Quality are displayed with the following values:

- **Latency** – Range starts at 0ms, lower is better.
- **Jitter** – Range starts at 0ms, lower is better.
- **MOS** – Audio quality score, with brackets for Good (4.34+), OKAY (3.6 to 4.33), and Poor (0 to 3.59).

Using these scores, you can see over the course of the call where the issues are occurring to take corrective action.

- Learn more at Understanding Microsoft Teams Call Quality for ZDX (https://help.zscaler.com/zdx/understanding-microsoft-teams-call-quality-zdx).
- Learn more at Understanding Zoom Call Quality for ZDX (https://help.zscaler.com/zdx/understanding-zoom-call-quality-zdx).
- Learn more at Understanding Webex Call Quality for ZDX (https://help.zscaler.com/zdx/understanding-webex-call-quality-zdx).

Advanced Troubleshooting with Deep Tracing

Deep Tracing involves a much more granular approach to troubleshooting end user issues. This is the ideal tool to leverage when users are experiencing a persistent but difficult to diagnose issue. To gain more data, Deep Tracing enables and collects information from web probes, Cloud Path probes, and device statistics every minute.

Currently, Deep Tracing is only supported on the following desktop versions of Zscaler Client Connector:

- For Windows devices, Zscaler Client Connector 3.1.0.97 (or later) and ZDX 2.0.0.14 (or later) are required.
- For macOS devices, Zscaler Client Connector 3.0.0.93 (or later) and ZDX 2.0.0.2 (or later) are required.

Both ZDX and ZIA use Deep Tracing, which provides additional, detailed diagnostic reporting on network path conditions. Because the goals of the two services are not identical, the information returned is not the same. ZDX probes will not report information including policy matches or categories.

The data is captured on a per-user basis for a specific application. The session must be manually started to enable a capture by a ZDX admin. The collection can be enabled from 5 to 60 minutes to capture data about the issue. When captured for analysis, the data is made available on the Diagnostics page and can be exported as a PDF for data sharing.

Learn more at About Diagnostics (https://help.zscaler.com/zdx/about-diagnostics).

When you start a Deep Tracing session, you name the session and select the options you need to monitor. You can also clone an existing session with the same settings if you were unable to capture the information in the first session. This might be necessary with some transient issues such as congestion. This can include:

- **Session name** – Something that is easily recalled so that you can find your session again to examine the results.
- **The user you want to monitor** – If you start a session from the Diagnostics page, you need to select a user from the drop-down menu. You can also launch a session from the user details or User Overview pages which will automatically select the user.
- **The device you want to monitor** – Select the device from a drop-down menu. If the device is grayed out, it is due to a compatibility issue with the device's Zscaler Client Connector version.
- **The session duration in 5-minute increments** – Select a time from 5 to 60 minutes to run the Diagnostics session.
- **Device probing** – When enabled on the device, statistics are captured as a part of a deep capture session. If you suspect the user's device might be related to the problem, enable this setting.
- **Application** – Select one of the applications you have configured for ZDX. There are two options for Application selection:
  - Leverage the existing Application configuration for an existing monitored application.
  - Deep Tracing also supports the concept of a Special Application. This allows you to add a URL or a tenant URL when you need to monitor an application that is not configured in your ZDX instance.

- **Select a probe to enable** – One or both probe types must be selected:
  - **Web probe** – Choose the web probe you previously configured for your selected application from the drop-down menu.
  - **Cloud Path probe** – Choose the configured Cloud Path probe for this application from the drop-down menu. If you add a Cloud Path probe, you can optionally enter thresholds for Packet Loss as a percentage and Latency in milliseconds. When you view the results of the Deep Tracing session, the Packet Loss and Latency are shown on the graph as a dotted red line, allowing you to view the data against your expectations.
  - If you select a Cloud Path probe that has been configured to follow a web probe, the web probe is also selected.

Deep Tracing can also be restricted by the ZDX admin to prevent unauthorized users from capturing and examining end user data. For more on admin roles, see Administrator Accounts in this guide.

Deep Tracing is not available on the standard plan. To view the supported range and feature availability by subscription level, see the Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf).

The Diagnostics page shows a tabular format of existing sessions. The table can be filtered by Name, User, Device, and Created Time.

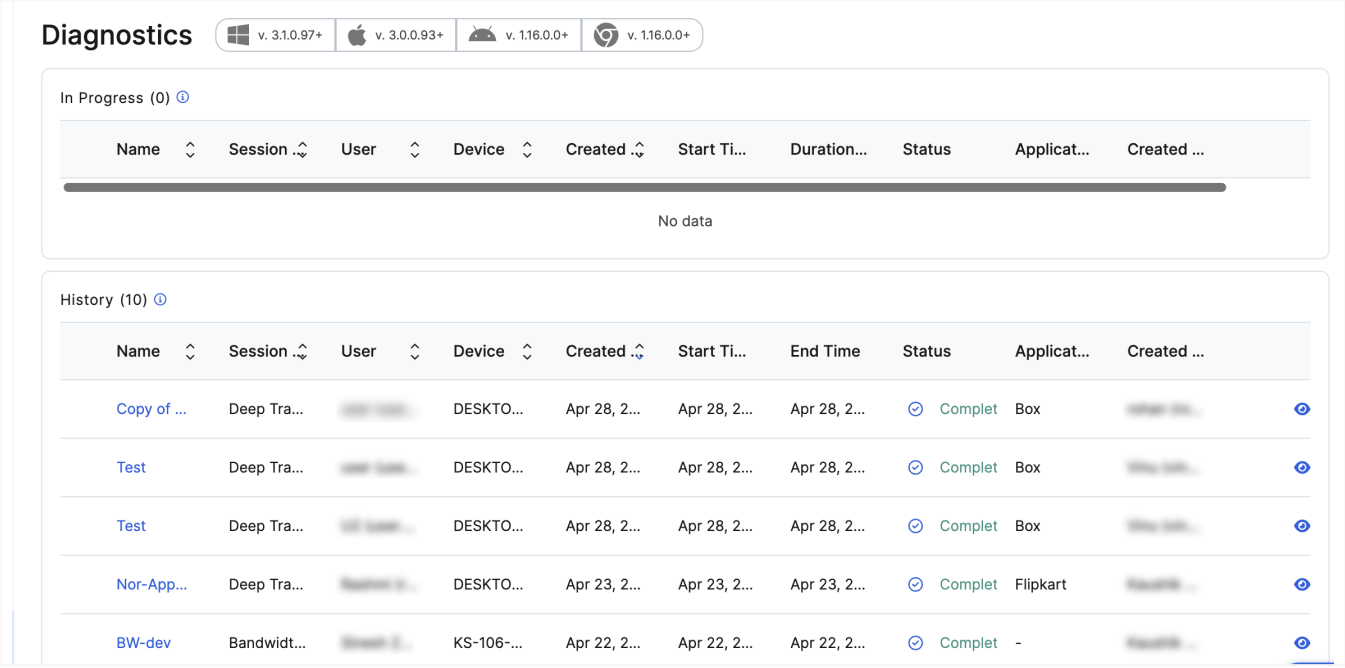


Figure 38: The Diagnostics page shows you recent sessions and their statuses

The following fields are available in the tabular format to help you quickly locate a session:

- **Name** – The name entered for the session during initiation of a session. Click the Name to open session results information in the same tab.
- **User** – The name and email address of the user.
- **Device** – The device being analyzed for the session.
- **Created Time** – The time the session was created by the ZDX admin.
- **Start Time** – The time that Zscaler Client Connector accepted the request and started collecting data.
- **End Time** – The time the session ended.
- **Status** – Session status differs depending on which table the session is listed in.
- **Application** – The application being monitored for the session.
- **Created By** – The name and email address of the admin who created the session.

Learn more at Starting a New Diagnostics Session (https://help.zscaler.com/zdx/starting-new-diagnostics-session).

Viewing Deep Tracing Details

When you view a Deep Tracing session, you are presented with the results based on your configuration selections. The start and stop times for the graphs reflect the length of the Deep Tracing session. The page is broken up into sections displaying the results of the session. The session info contains the general information about the configured session including the name of the user, session status, application if selected, device if Device Probing was enabled, and the session end time.

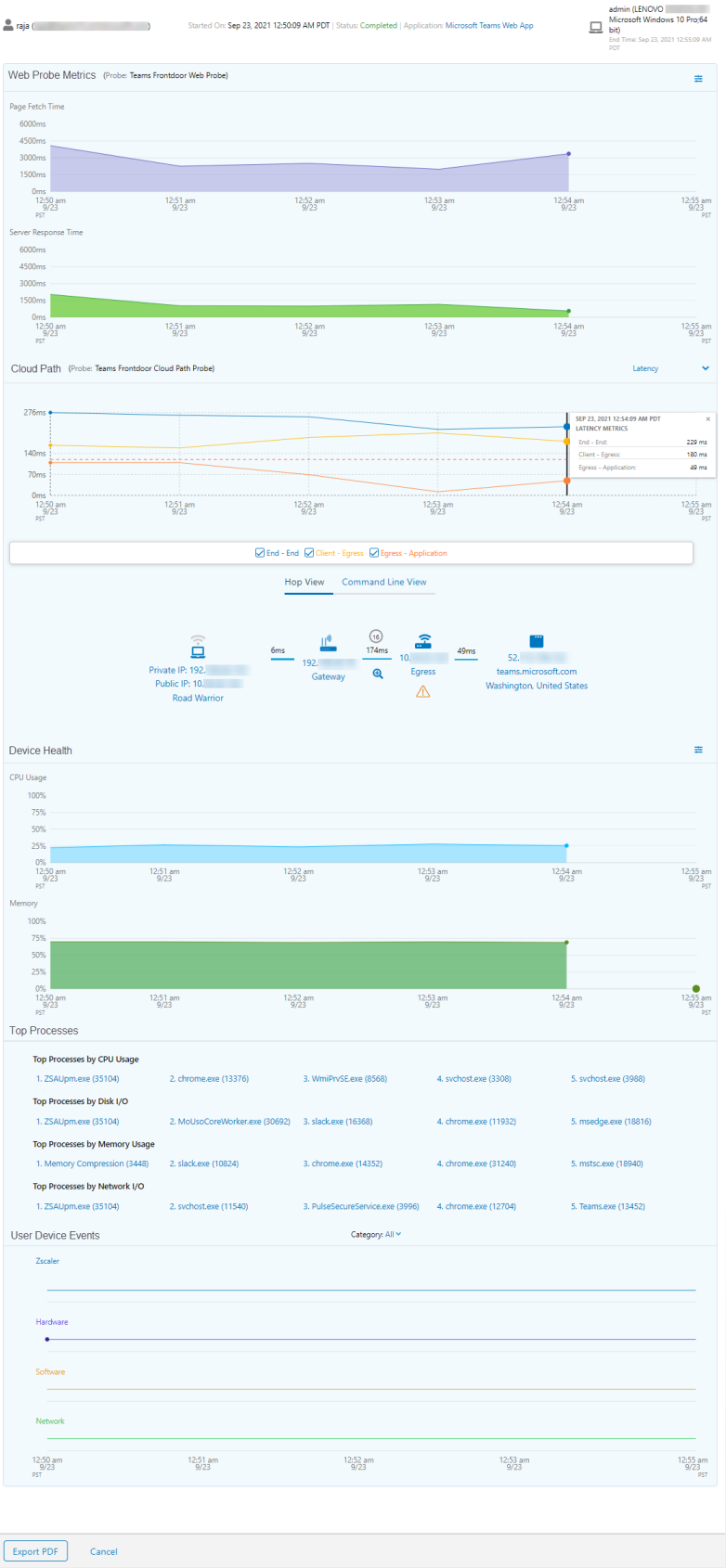


Figure 39: The Deep Tracing session results display information with options chosen during configuration

If you didn't enable Device Probing, didn't select an Application, or didn't configure either a web probe or a Cloud Path probe, those sections do not appear in the data.

If you selected an application, the following data is displayed:

- **Web Probe Metrics** – If you enabled a web probe, this section shows data for the Page Fetch Time, Server Response Time, DNS Resolve Time, and Availability. It also displays the probe name that was used during the session.
- **Cloud Path Probe** – If you enabled a Cloud Path probe, it is displayed in two sections:
  - **Graph section** – You can switch between Packet Loss and Latency metric views, and if configured, it shows a red dashed line at the level you specified for each metric.
  - **Hop View and Command Line View** – Displays icons with latency information or as a text view with Region and Geolocation, Packet Loss (%) and Packets Failed, and Latency metrics.

If you enabled the Device Probe for the Deep Tracing session, the following data is displayed in three sections:

- **Device Health** – Hardware utilization metrics as a time-based graph:
  - **CPU Usage** – Percentage of CPU used during the session.
  - **Memory** – Percentage of memory used during the session.
- **Top Processes** – Lists the top 4 processes in the following categories:
  - Top Processes by CPU Usage
  - Top Processes by Disk I/O
  - Top Processes by Memory Usage
  - Top Processes by Network I/O
- **User Device Events** – Tracks the following changes on the device itself and is displayed as a graph over time:
  - Zscaler
  - Hardware
  - Software
  - Network

As with all ZDX information, storage time is limited to a maximum of 14 days. Zscaler recommends backing up your Deep Tracing session by exporting the session as a PDF. The same dashboard view is exported to allow you to keep a copy of the information, or to add to a ticketing system when a ticket moves to a higher level of support.

If an admin has View Only access to Diagnostics as a part of their Admin Account, the export to PDF option is disabled. For more on admin roles, see Administrator Accounts in this guide.

Learn more at Viewing Diagnostics Session Results (https://help.zscaler.com/zdx/viewing-diagnostics-session-results).

Understanding the ZDX API

The ZDX API allows you to integrate with partner or custom solutions to leverage the application, network, and user data discovered by ZDX.

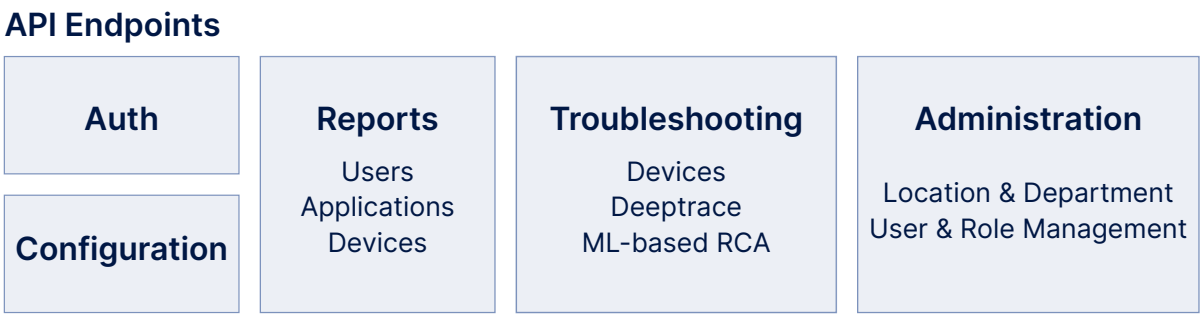


Figure 40: The ZDX API endpoints

The ZDX API supports the following functions:

Authentication

- Returns the authentication token for access to ZDX API.

Reports

- Retrieves ZDX Scores for applications and specific device health metrics and events.
- Reports allow you to pull information about users, applications, and devices.
- These reports are typically for a single application, user, or device.
- When it comes to the user details report, the endpoints are designed to allow you to pull specific information.

Administration

- Lists the active locations and departments for a tenant.
- Locations & Departments
- Users & Role Management

Troubleshooting

- Start Deep Tracing on a specific user and their respective device.
- A deep trace can be initiated using the API for a specific timeframe (for example, 5 minutes). A unique trace ID is generated for each request. Users can then access the result after the trace is complete.

Configuration

- Configuration of ZDX applications and probes.

ZDX API integration is not available on the standard plan. To view the supported range and feature availability by subscription level, see the Zscaler Digital Experience Data Sheet (https://www.zscaler.com/resources/data-sheets/zscaler-digital-experience.pdf).

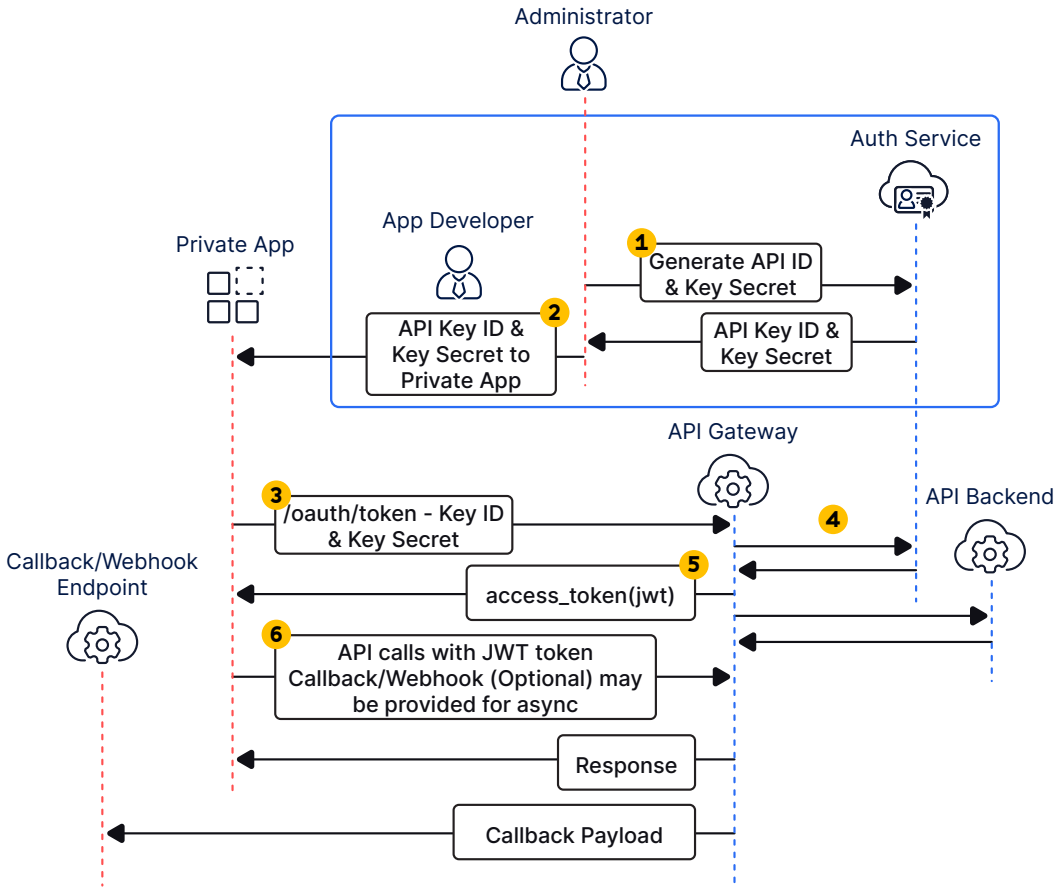


Figure 41: The ZDX API access flow

1. Your admins generate a per application API Key ID and API Key Secret in the ZDX Admin Portal.
2. The API Key ID and API Key Secret are added to your client application.
3. Your application requests access to the ZDX API.
4. If the API Key ID and API Key Secret are valid, the application is granted a JSON web token (JWT) access token.
5. API calls are made with the JWT token, and callbacks can also be configured for asynchronous operation.
6. Callbacks are made to the callback or webhook endpoint.

The Zscaler API gives you access to the information collected by probes and device data. There are two caveats to be aware of with regards to the data accuracy:

- **Inconsistency in data** – The data returned by the ZDX API might not exactly match the data on the ZDX UI. The difference between the data is a marginal 2% because the aggregated metrics compute using approximate functions. The ZDX API does this to maximize performance.
- **Delay in data** – Zscaler Client Connector collects all telemetry and reporting. This can cause a delay from collection to reporting, which is estimated to be 20 minutes. To get the full data for one hour, ensure that you use the right timestamp and adjust for this delay.

API calls are subject to rate limiting based on your subscription tier. It's important that you design your applications and integrations with your rate limits in mind. The system also provides rate limiting headers about the requests remaining and reset time. The following limits apply:

Tier Level	Number of Licenses	API Calls/ Second	API Calls/ Minute	API Calls/ Hour	API Calls/ Day
1	5,000	5	30	1,000	10,000
2	20,000	5	60	3,000	15,000
3	100,000	5	120	6,000	30,000
4	More than 100,000	5	180	9,000	60,000

Table 1: Rate limits for the ZDX API

Learn more at Understanding the ZDX API (https://help.zscaler.com/zdx/understanding-zdx-api).

Learn more at About API Key Management (https://help.zscaler.com/zdx/about-api-key-management).

Learn more about Zscaler technology partners at the Zero Trust Exchange Partner Ecosystem (https://www.zscaler.com/partners/technology).

Recommendations for Deploying ZDX in Your Organization

Deploying ZDX successfully in your organization is typically done in stages. By starting small, you can test your monitoring rules before rolling them out to the rest of your organization. This gives you time to tune the rules to ensure they are alerting you as expected and not overwhelming your help desk with false positives.

ZDX requires the use of Zscaler Client Connector. This lightweight agent is used by ZDX to send out probes and monitor client machines. It can also be used by ZIA to direct your users' internet-bound traffic to a ZIA Private Service Edge or inspection. If you have ZPA, Zscaler Client Connector provides access to your private applications. If you are already a subscriber to either ZIA or ZPA, you might have already rolled out Zscaler Client Connector to your endpoints. This is a required step for ZDX to operate in your organization. To learn more about Zscaler Client Connector, see What Is Zscaler Client Connector? (https://help.zscaler.com/zscaler-client-connector/what-is-zscaler-client-connector).

If you have not yet deployed Zscaler Client Connector, you need to consider any adjustments that need to be made to any antivirus or client monitoring solutions. Your network firewall also needs to be adjusted to allow the ZDX probes to function. For more information, see Updating Network and Host Allow Lists in this guide.

As with any new tool, it can be useful to test with your own IT staff as your first users. These users are best able to articulate any issues that occur and can troubleshoot with you as required. You must ensure that your staff is aware of the testing, and what you need from them in terms of feedback and reporting. Zscaler recommends rolling out in the following populations first:

1. Your level 3 help desk.
2. The rest of your help desk staff.
3. Network and operations teams.

As each of these teams comes on board, you'll want to baseline their digital experience to applications in their location. You'll find that some regions have faster or slower response times to applications or the internet generally. What is considered acceptable in one region might trigger matches in another, and the probes need to be tuned accordingly. For more on tuning your action rules, see Tuning Alerts to Reduce False Positives in this guide.

After you've tuned your rule sets for alerts, you can begin to bring the rest of your users into ZDX. Zscaler recommends doing this in controlled groups depending on the size of your organization and number of probes. This allows you to tune the rules with the users who actively use the application, and to get a better understanding of the application's performance in the real world.

Defining your groups is primarily based on the number of applications your organization plans to monitor, and the 30 probe per user limit. This can be all users that match a particular profile such as finance or development, or it can be users in a local region. By keeping your groups small, you can quickly adjust rule settings should you receive too many notifications.

If you have 30 or fewer probes, Zscaler recommends assigning all probes to all users. In this model, Zscaler recommends bringing groups on by location and region, giving you the ability to baseline your notifications for the new group. Continue this pattern with the rest of the users in your organization.

If you have more than 30 applications, you are required to build different mixes of applications based on the user's role. In this case, you assign probes for applications based on the user's role in the organization. As you identify the application mix for each role or group of users, they can have ZDX enabled, and you can then baseline this new group.

ZIA and Internet-Accessible Applications

ZIA provides safe, fast internet and SaaS access with the industry's most comprehensive cloud-native security service edge (SSE) platform. ZIA contains multiple tools to secure your user's internet access including full TLS/SSL inspection of all traffic. When working with ZDX, ZIA allows you to leverage your existing authentication configuration, administrative accounts, and defined locations.

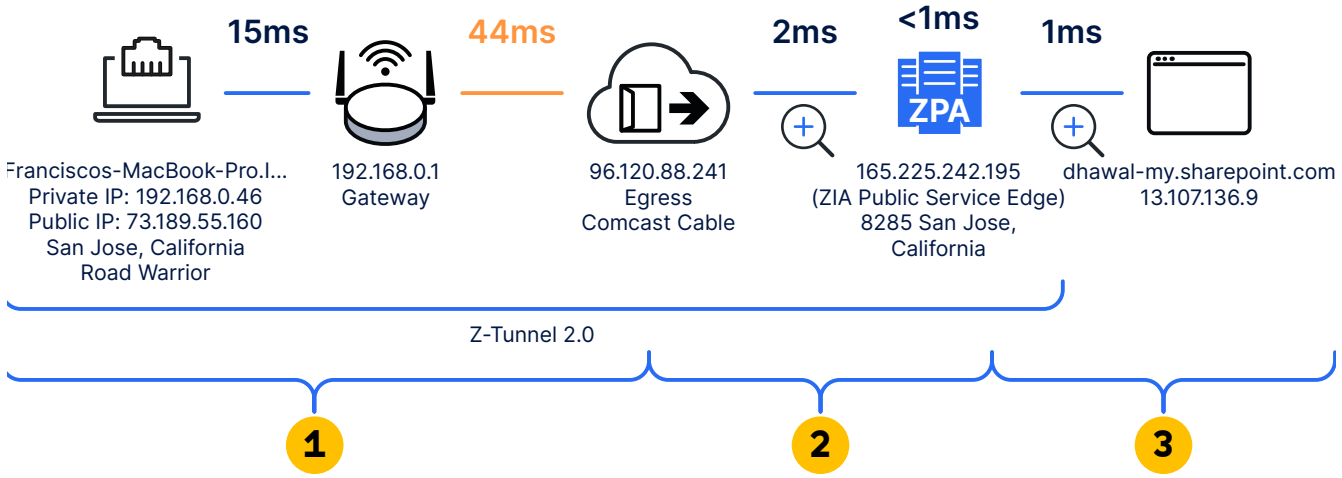


Figure 42: Defined segment groups in the ZIA path

When you examine a user's path using ZDX with ZIA, there are three groupings of segments to consider as you begin your analysis:

1. **User Device to Egress Point** – This segment covers your user's device and the network gateway, up to the service provider edge.
2. **Egress Point to ZIA Public Service Edge** – This segment is the ISP network between your end user and the ZIA Public Service Edge.
3. **ZIA Public Service Edge to Application** – This segment is the network between the ZIA Public Service Edge and the intended application.

ZPA and Private Applications

ZPA offers the fastest, most secure access to private applications, services, and operational technology (OT) devices with the industry's only next-gen Zero Trust Network Access (ZTNA) platform. ZPA allows you to make applications and OT devices invisible on the internet, reachable only through the ZPA service for authenticated and authorized users. When working with ZDX, ZPA allows you to leverage your existing authentication configuration and administrative accounts.

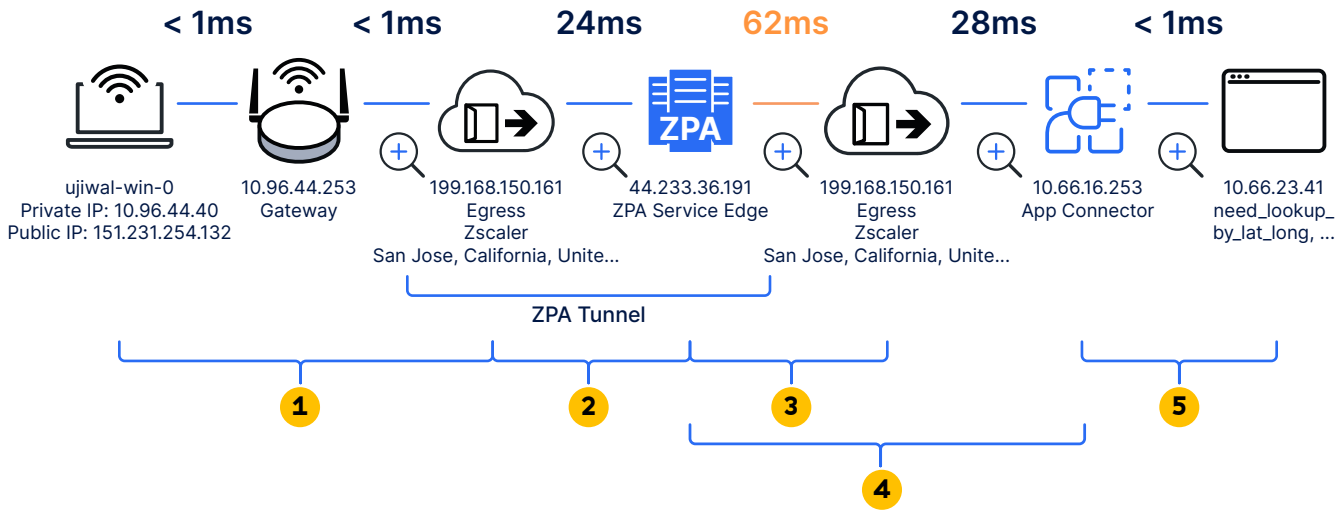


Figure 43: Defined segment groups in the ZPA path

When you examine a user's path using ZDX with ZPA, there are 5 groupings of segments to consider as you begin your analysis:

1. **User Device to Egress Point** – This segment covers your user's device and the network gateway, up to the service provider edge.
2. **Egress Point to ZPA Public Service Edge** – This segment is the ISP network between your end user and the ZPA Public Service Edge.
3. **ZPA Public Service Edge to Application Egress Point** – This is the segment between the ZPA Public Service Edge and the egress point from the application's point of view.
4. **ZPA App Connector to ZPA Public Service Edge** – This segment contains segment 3, as well as the internal network between the ZPA App Connector and the ZPA Public Service Edge.
5. **ZPA App Connector to Application** – This segment is the internal network between the ZPA App Connector and the private application the user is trying to reach.

Standalone ZDX Deployments

ZDX can be used without either ZIA or ZPA, however the detail and segments reported in the overview are more limited. With ZIA or ZPA, there are more Zscaler segments reporting in and displayed on the dashboard. Standalone ZDX relies only on the information collected by ZDX probes. Your users install Zscaler Client Connector on their devices for monitoring, and you need to configure authentication and administration for your ZDX instance.

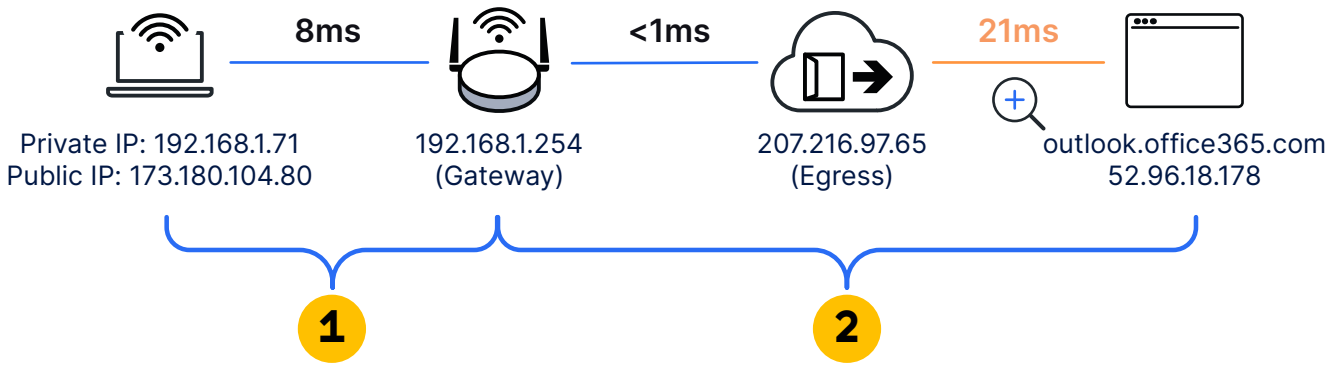


Figure 44: Defined segment groups in the ZDX standalone path

When you examine a user's path using a standalone ZDX deployment, there are two groupings of segments to consider as you begin your analysis:

1. **User Device to Egress Point** – This segment covers your user's device and the network gateway, up to **the service provider edge.**
2. **Egress Point to Application** – This segment covers the network between the egress point and the final application destination.

Summary

Zscaler Digital Experience (ZDX) is a digital experience monitoring solution delivered as a service from the Zscaler cloud. ZDX provides end-to-end visibility and troubleshooting of end user performance issues for any user or application, regardless of location. In addition, it enables continuous monitoring for network, security, application, and help desk teams with insight into the end user device, network, and application performance issues.

ZDX leverages Zscaler Client Connector and the Zscaler Zero Trust Exchange to actively monitor applications from an end user perspective. It continuously collects and analyzes various performance metrics, including application availability, response times, network hop-by-hop performance metrics, and end user device health metrics such as device configuration, CPU, memory usage, process information, and device events. As a result, IT teams get uninterrupted visibility and can save time with proactive identification and resolution of end user experience issues.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so 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.