Zscaler Digital Experience Administrator

STUDY GUIDE:

Zscaler Digital Experience Administrator (ZDXA)

Zscaler Digital Experience Administrator

How to Use This Study Guide

Welcome to the Zscaler ZDXA Study Guide, which will serve as your go-to resource in preparing for the ZDXA exam and receiving your ZDXA certification.

About the ZDXA Exam

The Zscaler Digital Experience Administrator (ZDXA) is a formal, third-party proctored certification that indicates that those who have achieved it possess the in-depth knowledge to design, install, configure, maintain, and troubleshoot most ZDX implementations.

Exam Format

Certification name: Zscaler Digital Experience Administrator (ZDXA)
Delivered through: Online Proctored via Certiverse
Exam series: Administrator
Seat time: 90 minutes
Number of items: 60
Format: Multiple Choice, Scenarios with Graphics, and Matching
Languages: English

Exam Domain	Weight (%)
Zscaler Digital Experience (ZDX) Overview	20 %
Monitoring ZDX	20 %
Configuring ZDX	20 %
Troubleshoot User Experience Issues with ZDX	25 %
Best Practices for Operalization of ZDX	15 %

*refer to the extended blueprint in the learning path to identify subdomains included in each domain.

Audience & Qualifications

The ZDXA exam is for Zscaler customers as well as all who sell and support the Zscaler platform. By taking the exam, you are demonstrating your deep understanding and knowledge needed to sufficiently drive operational success.

Candidates should have a:

- Minimum of 5 years working in both IT networks and cybersecurity
- Minimum of 1 year experience with the Zscaler platform

Skills Required

- Ability to professionally design, implement, operate, and troubleshoot the Zscaler platform.
- Ability to adapt legacy on-premises technologies and legacy hub-and-spoke network designs to modern cloud architectures.

Required Training

Zscaler requires that you have first completed the Zscaler Digital Experience Operalization (EDU-310) course and hands-on lab, and it is recommended to have solid hands-on experience with ZIA, ZPA and ZDX.

Overview

Learning Objectives

By the end of this chapter, you will be able to

1. **Describe** what Zscaler Digital Experience (ZDX) is and why it was created
2. **Describe** the core components that make up ZDX and the important aspects of each component
3. **Navigate** the various dashboards, graphs and widgets within the ZDX Administrator Portal
4. **Understand** and interpret the presented data
5. **Configure** ZDX components and functions
6. **Analyze** ZDX dashboards and metrics to troubleshoot user experience issues

What's in it for me?

You might be asking yourself “How is ZDX going to help me in my day-to-day job?”

Do you experience an abundance of trouble tickets coming through your inbox everyday? Do a lot of those trouble tickets require escalation? Is it taking days or weeks to detect and solve these tickets with poor collaboration among your helpdesk, network, desktop, application, and security teams?

These are all problems which ZDX was built to eliminate, to make your job easier by decreasing the total number of trouble tickets, improving the mean time to detection (MTTD), mean time to resolution (MTTR) and mean time to innocence (MTTI), and improving cross-functional collaboration between your teams. You no longer have to struggle to find out what's wrong where. You can now pinpoint what is happening and why, gaining a unified view into user experiences - user device, network path, and application all within one ZDX Administrator Portal.

Sounds too good to be true? Let's start by gaining an overview of ZDX and then we'll dive into the capabilities that ZDX has in place to make your day-to-day job easier.

ZDX OVERVIEW

Introduction to Zscaler Digital Experience

Zscaler Digital Experience (ZDX) is a cloud-native service that's part of the world's largest security cloud, for analyzing, troubleshooting, and resolving user experience issues. It was built as a multi-tenant Digital Experience Monitoring (DEM) platform to probe, benchmark, and measure the digital experiences for every single user within an organization, including their global remote workforce.

ZDX is an integrated service on top of the Zscaler Zero Trust Exchange. Instrumentation starts at Zscaler Client Connector, a unified agent for cloud security, zero-trust application access, and digital experience monitoring. As a result, setup is frictionless and quick – there is no need to deploy new hardware, software agents, or probes.

Monitoring Requirements have changed in a Mobile-First World

The rapid adoption of cloud and mobility initiatives within organizations and a shift to work-from-anywhere have introduced new monitoring challenges for IT teams.

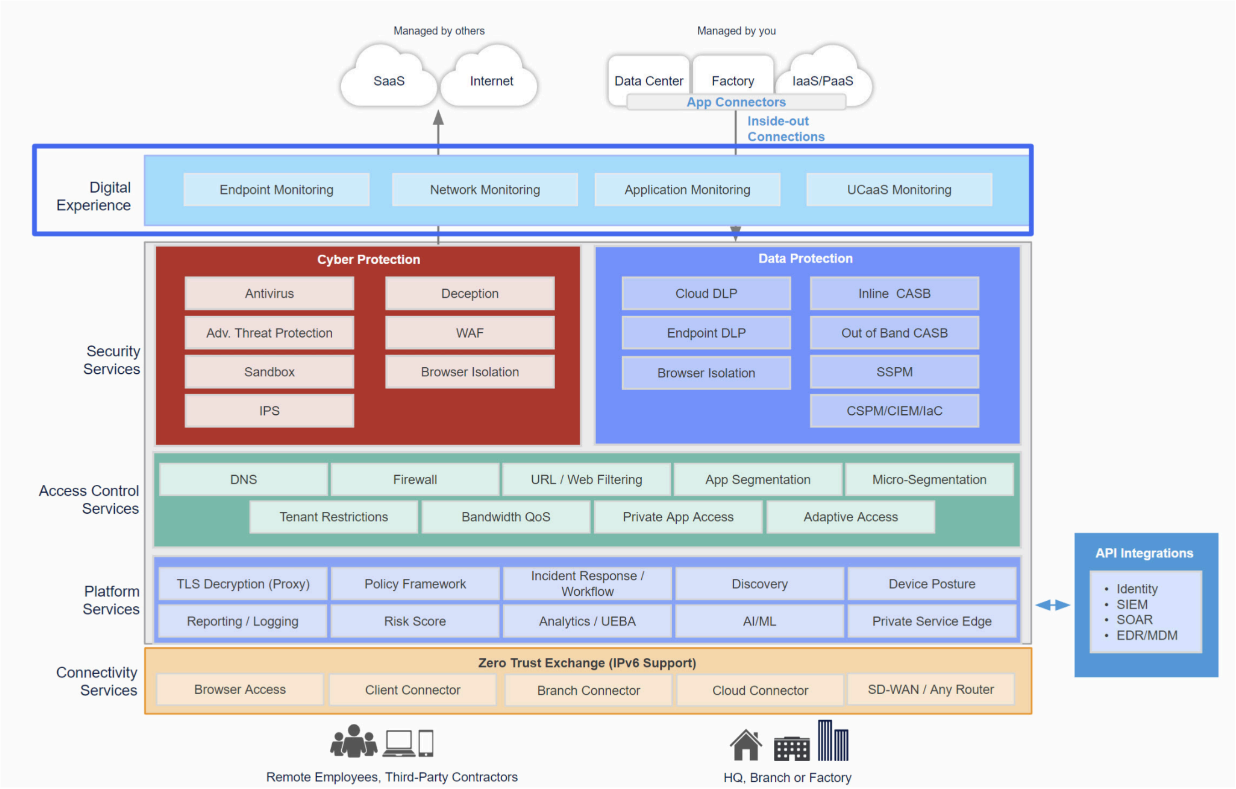
Digital experience monitoring for a hybrid workforce requires a modern and dynamic approach. IT teams need to continuously monitor and measure the digital experience for each user from the user perspective, regardless of their location.

Traditional monitoring tools take a data center-centric approach to monitoring and collecting metrics from fixed sites rather than directly from the user device. This approach does not provide a unified view of performance based on a user device, network path, or application.

Zscaler provides this unified view through our Digital Experience monitoring solution that sits on top of the Zero Trust Exchange. Zscaler Digital Experience (ZDX) helps IT teams proactively monitor digital experiences from the end user perspective, optimize performance and rapidly troubleshoot and resolve application, network, and device issues.

ZDX is a cloud native service, built on the world's largest security cloud, focusing on analyzing troubleshooting, and resolving IT and user experience issues. It is an integrated product line built on top of Zscaler Zero Trust Exchange, leveraging the scale of the globally distributed Zscaler cloud and integrations with existing product lines, including both Internet Access and

Private Access, to continuously monitor SaaS and private application performance for every single user from every device they're coming from.



But how did we get here? Why was ZDX created?

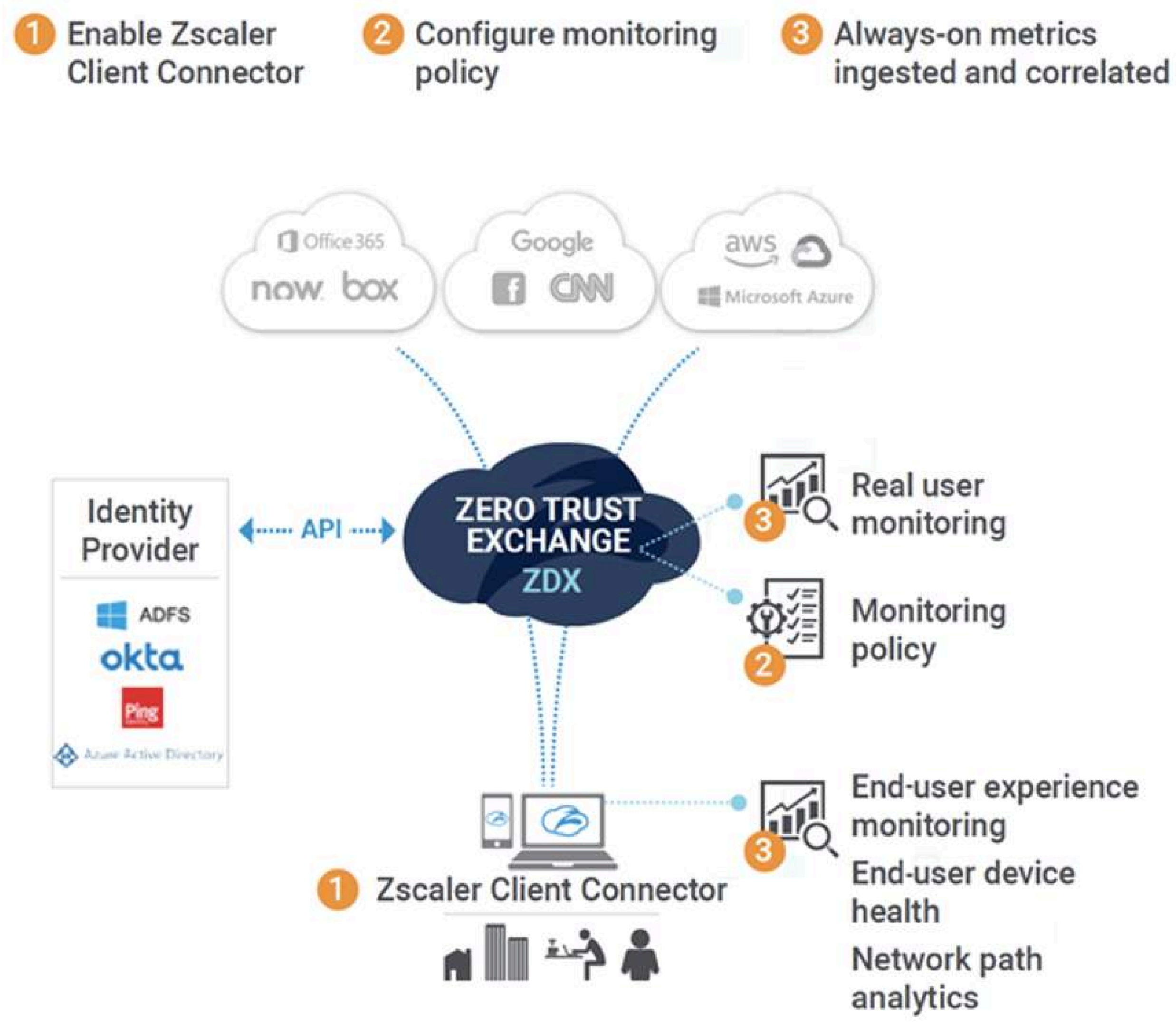
Digital transformation as we know creates monitoring gaps. And as we move more apps to SaaS, such as Microsoft 365 and Salesforce, or to the public cloud, such as Azure or AWS, we are relying more and more on the public internet to provide us desired performance and connectivity.

Moreover, users are everywhere, not sitting in a corporate office. This leads to a big problem for IT organizations, as infrastructure that was typically in full control is now all over the map. Every user who works from a home office or a coffee shop is seen as an extension of the corporate network and that of the corporate footprint.

SaaS apps cannot be instrumented with monitoring scripts. Instead, there's reliance on SaaS provider’s monitoring tools and SLA reports, further highlighting that you do not own the infrastructure and applications anymore.

ZDX Architecture

The ZDX platform is a highly sophisticated design, incorporating advanced technologies at both the client/endpoint level and within the ZDX Cloud platform. While the ZDX Cloud Platform is independent of Zscaler's other Cloud platforms (Internet Access, Private Access, etc.) and can be deployed as a standalone product, it's often best thought of as a companion to those products. All of the Zscaler products share some key design philosophies, concepts, and complement each other being part of the same Zscaler Zero Trust Exchange Platform.

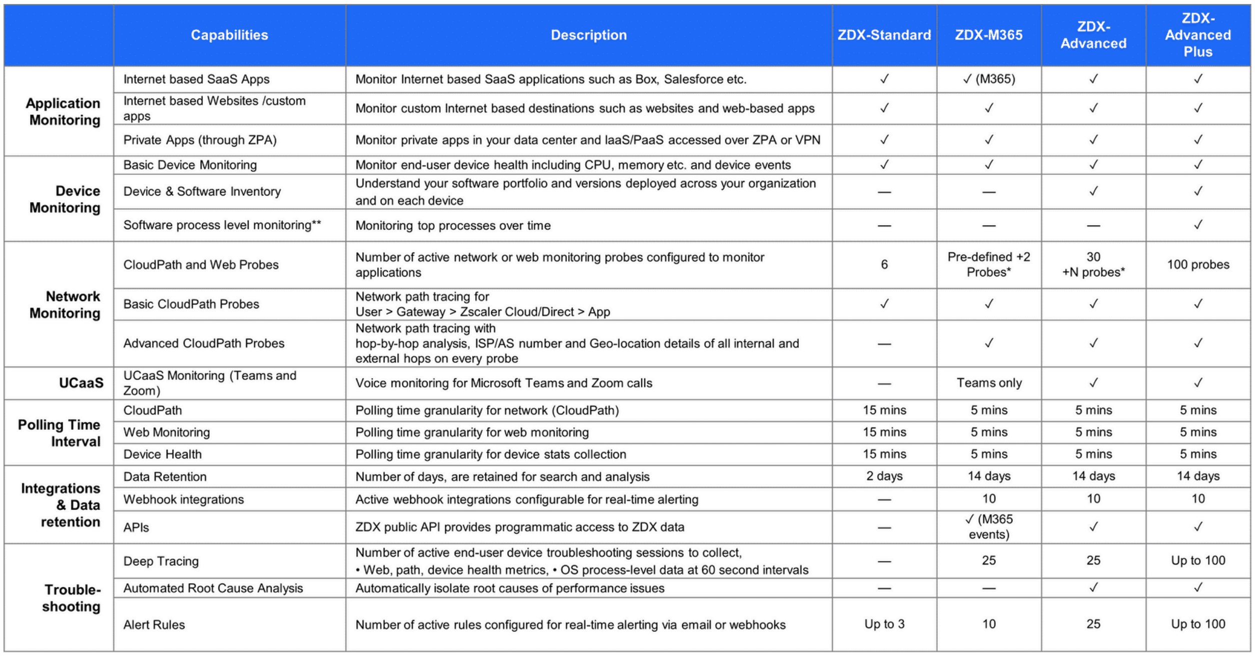


The ZDX service is primarily comprised of two major components: the Zscaler Client Connector and the ZDX Cloud.

Zscaler Client Connector	The Zscaler Client Connector is a **lightweight, tamper-resistant endpoint agent which is deployed to a user's endpoint**, where it can play a number of roles relating to Zscaler Internet Access, Zscaler Private Access, and more. In the case of Zscaler Digital Experience, the Client Connector's primary purpose is to **gather and forward critical telemetry data from the device to the cloud, along with validating user identity via authentication.**
ZDX Cloud	Looking "behind the scenes," there are some components of the platform which play a critical role in providing the user experience insights that organizations find so valuable: **Telemetry and Policy Gateway (TPG):** The TPG is an application running within the ZDX Cloud infrastructure, which performs two important functions: 1. Gathers telemetry data (which can include information about the endpoint itself, along with the results of probes from an endpoint to configured cloud applications) from the Client Connector, and forwards that data to the ZDX Analytics system noted below. 2. Responds to the Client Connector with the latest policy updates designed by the customer organization, whether those updates are changes to the Client Connector configuration or new application probes. **ZDX Central Authority (CA):** The Central Authority essentially oversees the entire ZDX Cloud and provides a central location for software and database updates, policy and configuration settings, and general intelligence. It communicates with Central Authorities in the individual Zscaler clouds to get user configuration information, for example group/department membership, and device ID and also caches that user information. The collection of ZDX Central Authority instances together act as the "brain" of the cloud, and they are geographically distributed for redundancy and performance. **ZDX Analytics:** In essence, raw telemetry data is fed out of the core ZDX Cloud and into the ZDX Analytics sub-cloud, where it is processed and aggregated back out again, in the reports, charts, and graphs that a customer interacts with while in the ZDX Administrator Portal. It's also important to note that the ZDX Analytics system is the only place where telemetry data is written to disk—at all other stages of ZDX, user activity and telemetry are processed in RAM. The Client Connector writes telemetry data to disk before being uploaded to the ZDX platform, typically several times per hour. Additionally, any potentially-sensitive Zscaler Private Access telemetry data being written to disk is encrypted before being uploaded to the ZDX platform.

ZDX Plans

ZDX is available in different plans: **ZDX-Standard, ZDX-M365, ZDX-Advanced** and **ZDX-Advanced Plus**. As you can see in the table below, some features, for example the ability to run Deep Tracing sessions, use Webhooks, or provide more granular probing are only available in the ZDX-Advanced, ZDX-Advanced Plus and ZDX-M365 plans. There are also differences in the number of applications, probes, and alerts that can be used.



	Capabilities	Description	ZDX-Standard	ZDX-M365	ZDX-Advanced	ZDX-Advanced Plus
Application Monitoring	Internet based SaaS Apps	Monitor Internet based SaaS applications such as Box, Salesforce etc.	✓	✓ (M365)	✓	✓
	Internet based Websites /custom apps	Monitor custom Internet based destinations such as websites and web-based apps	✓	✓	✓	✓
	Private Apps (through ZPA)	Monitor private apps in your data center and IaaS/PaaS accessed over ZPA or VPN	✓	✓	✓	✓
Device Monitoring	Basic Device Monitoring	Monitor end-user device health including CPU, memory etc. and device events	✓	✓	✓	✓
	Device & Software Inventory	Understand your software portfolio and versions deployed across your organization and on each device	—	—	✓	✓
	Software process level monitoring**	Monitoring top processes over time	—	—	—	✓
Network Monitoring	CloudPath and Web Probes	Number of active network or web monitoring probes configured to monitor applications	6	Pre-defined +2 Probes*	30 +N probes*	100 probes
	Basic CloudPath Probes	Network path tracing for User > Gateway > Zscaler Cloud/Direct > App	✓	✓	✓	✓
	Advanced CloudPath Probes	Network path tracing with hop-by-hop analysis, ISP/AS number and Geo-location details of all internal and external hops on every probe	—	✓	✓	✓
UCaaS	UCaaS Monitoring (Teams and Zoom)	Voice monitoring for Microsoft Teams and Zoom calls	—	Teams only	✓	✓
Polling Time Interval	CloudPath	Polling time granularity for network (CloudPath)	15 mins	5 mins	5 mins	5 mins
	Web Monitoring	Polling time granularity for web monitoring	15 mins	5 mins	5 mins	5 mins
	Device Health	Polling time granularity for device stats collection	15 mins	5 mins	5 mins	5 mins
Integrations & Data retention	Data Retention	Number of days, are retained for search and analysis	2 days	14 days	14 days	14 days
	Webhook integrations	Active webhook integrations configurable for real-time alerting	—	10	10	10
	APIs	ZDX public API provides programmatic access to ZDX data	—	✓ (M365 events)	✓	✓
Trouble-shooting	Deep Tracing	Number of active end-user device troubleshooting sessions to collect, • Web, path, device health metrics, • OS process-level data at 60 second intervals	—	25	25	Up to 100
	Automated Root Cause Analysis	Automatically isolate root causes of performance issues	—	—	✓	✓
	Alert Rules	Number of active rules configured for real-time alerting via email or webhooks	Up to 3	10	25	Up to 100

ZDX Metrics

How ZDX Score Works

The ZDX Score is **calculated by observing the Page Fetch Time and availability of an application for a given user.** This is then baselined across all the users in that geolocation (country) accessing that particular application.

25
BAD
65
OKAY
100
GOOD

ZDX periodically sends a probe to an application, by default, every 5 minutes. For each 5-minute period, measurements are taken and given a numerical value from 1 to 100. The lowest value within an hour becomes the ZDX Score for that hour.

This is done for every defined application, across all users, their devices, and their locations. Click each marker below to see how the score is calculated for each of these areas.

Applications	Departments, Locations, and Cities	Organizations	Users
Find the lowest value of each user that accessed the application during the selected time range.	Find the lowest value of users accessing the application during the time intervals, based on the selected time range.	Identify the lowest value of each application for time intervals, based on the selected time range.	Compare values of all accessed applications.
ZDX Score = sum of low value/ **number of users.**	ZDX Score = sum of low value/ **number of time intervals.**	ZDX Score = sum of low value/ **number of time intervals.**	ZDX Score = Lowest value **during the selected time range**.

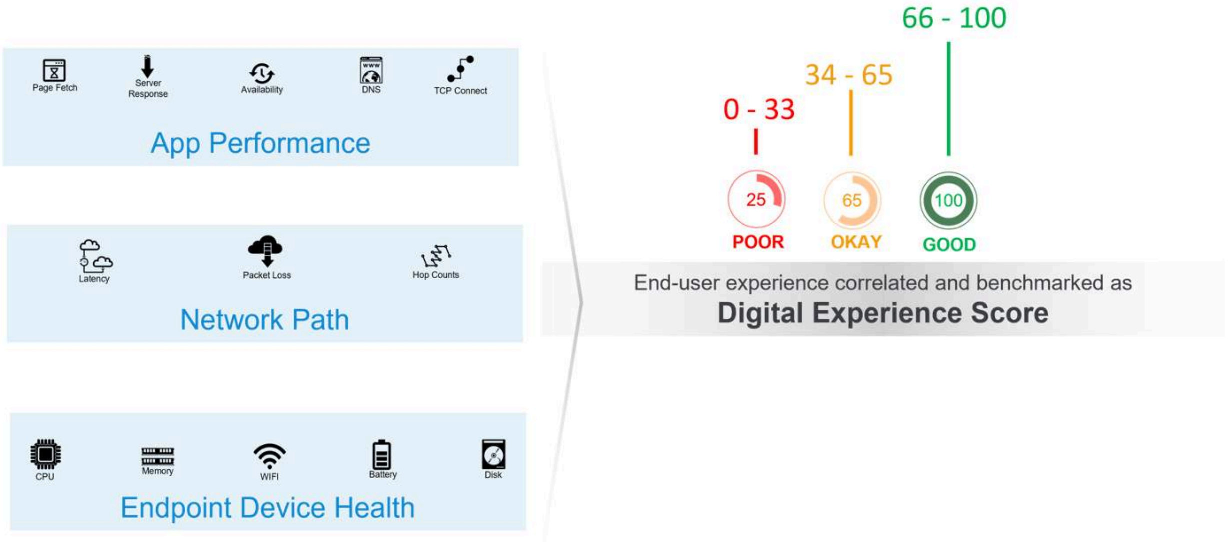
The power of ZDX is being able to use these calculated scores in order to drill into issues when a score seems to be visibly low. What, however, might cause a good score to go down?

App Issues	App issues would typically be seen in the 'PFT' (Page Fetch Time) and 'SRT' (Server Response Time) metrics
DNS	Many customers still use sub-optimal DNS that could result in higher overall latency
App Availability	App availability is impacted, and users are seeing 5xx errors
Local WiFi	Local WiFi based signal strength or WiFi <-> egress latency. Example: 2.4Ghz instead of 5Ghz
Egress Latency	Traffic being backhauled through a VPN or too many hops before traffic hits the egress IP Address
Network Latency	Latency up to Zscaler: Sub-optimal routing or ISP issues Latency at Zscaler: High CPU/traffic on ZEN or ISP issues
Network Congestion	Network congestion would surface as latency, WiFi, or high bandwidth utilization
Device Metrics	CPU/memory spikes translate into slower client (ex. browser) response time and leads to bad user experience, or CPU at 100%
Device Events	Check for device events for bad score triggers: Example: VPN tun interface, WiFi change, system restart, etc.

ZDX Score Overview

> ZDX generates an incredible quantity of performance data at multiple levels—at the client's endpoint device, along the path between the client and their applications, and from the application servers themselves. Of course, performance data alone isn't worth very much—it's only as useful as its ability to be analyzed and acted upon where needed. With this in mind, ZDX is built around a powerful concept called the ZDX Score. In short, the **ZDX Score** compiles key performance metrics and represents or summarizes the digital experience for all users in an organization, across all their applications, and from all their managed devices, locations, and/or cities.

The ZDX Score is a scale ranging from 1 to 100, where lower numbers indicate a poor user experience, and higher numbers represent a better (and thus more productive) user experience. A score of 0 means that the application was not reachable, pointing to a network connectivity problem or to the application not being available.



Factors that might commonly contribute to a low ZDX Score include:

- Problems at the endpoint level, such as a fully saturated CPU.
- Problems along the path between the client and an application, such as congested WiFi at the user's location, or an Internet Service Provider (ISP) which is overly congested.
- Problems with the application itself, such as a server that is taking unusually long to respond to a request, or which has gone offline and stopped responding altogether.

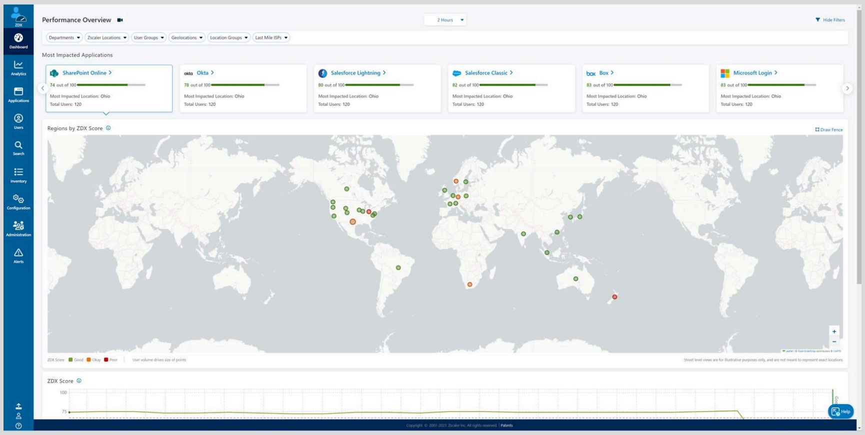
ZDX Score Measurements

Zscaler sends a probe from the Zscaler Client Connector to an application every 5 minutes. For each 5-minute period, measurements are taken and given a numerical value from 1 to 100.

This is done for every defined application in the ZDX Administrator Portal across all users, their devices, and their locations. From there, Zscaler calculates the score based on what is measured, across the following categories:

Applications

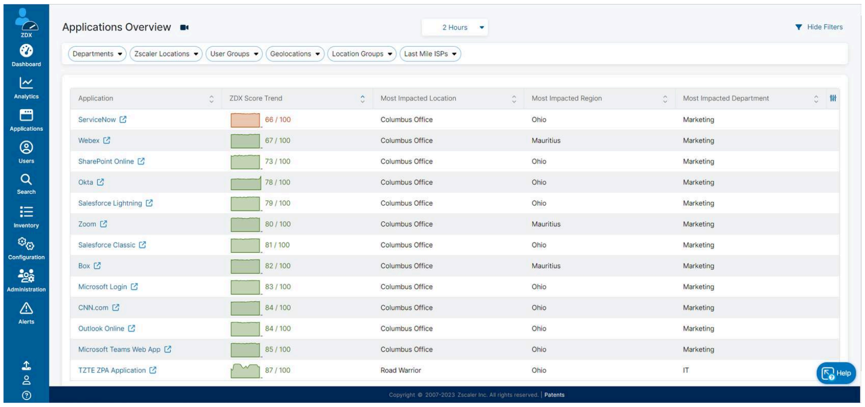
To determine the score for an application, Zscaler takes all the users that accessed the application for the selected time period and finds the average value each user would have experienced for the application. ZDX also measures the "Availability" of an application. If probes fail due to underlying reasons it will be reflected in the score.



Departments, Defined Locations, and Geolocations

The ZDX Score for variables like departments, organizationally defined locations, and cities identifies the lowest value for users accessing the applications from those places and groups during time intervals based on the selected time range. The lowest value represents the department's, location's, or city's score for each time interval. An average of all the time intervals for the selected time period is calculated to provide the score for the time range.

For example, the time interval for the 24 hour time range is one hour. Each hour's score is added together and divided by 25 (24 hours + 1 for the starting score) to provide the ZDX Score. Also, if the user has location services enabled on their endpoint, ZDX will incorporate their actual location (based on longitude and latitude). Alternatively, if the user has disabled location services on their endpoint, the ZDX service will fall back to geolocating the user based on their current egress IP address—while this isn't as accurate as longitude and latitude, it is accurate enough for the purposes of ZDX Scoring.



Applications Overview

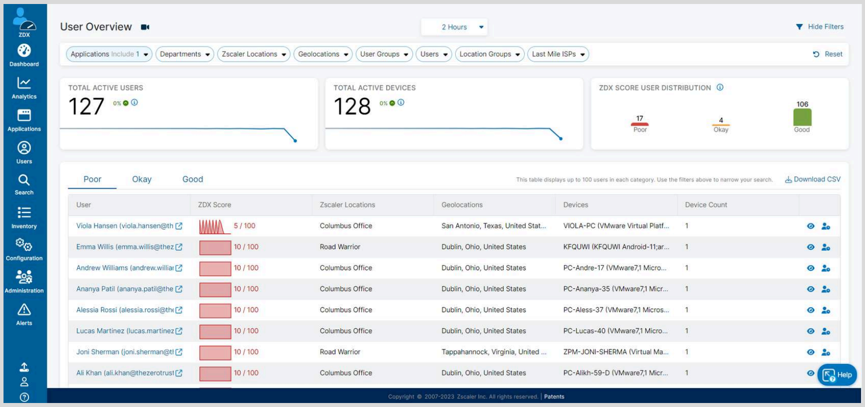
2 Hours

Application	ZDX Score Trend	Most Impacted Location	Most Impacted Region	Most Impacted Department
ServiceNow	66 / 100	Columbus Office	Ohio	Marketing
Webex	67 / 100	Columbus Office	Mauritius	Marketing
SharePoint Online	73 / 100	Columbus Office	Ohio	Marketing
Okta	78 / 100	Columbus Office	Ohio	Marketing
Salesforce Lightning	79 / 100	Columbus Office	Ohio	Marketing
Zoom	80 / 100	Columbus Office	Mauritius	Marketing
Salesforce Classic	81 / 100	Columbus Office	Ohio	Marketing
Box	82 / 100	Columbus Office	Mauritius	Marketing
Microsoft Login	83 / 100	Columbus Office	Ohio	Marketing
CNN.com	84 / 100	Columbus Office	Ohio	Marketing
Outlook Online	84 / 100	Columbus Office	Ohio	Marketing
Microsoft Teams Web App	85 / 100	Columbus Office	Ohio	Marketing
TZTE ZPA Application	87 / 100	Road Warrior	Ohio	IT

Copyright © 2007-2023 Zscaler Inc. All rights reserved. | Patents

Users

For a user's ZDX Score, a comparison of the values across each application they accessed is done for the selected time period. The application with the lowest value is the user's score since it represents the user's poorest digital experience for the selected time range. Note that in situations where a user is working on multiple managed devices (in other words, devices running the Zscaler Client Connector), the user’s score is computed as an average of all user devices.



User Overview

2 Hours

Applications Include 1

TOTAL ACTIVE USERS
127 0%

TOTAL ACTIVE DEVICES
128 0%

ZDX SCORE USER DISTRIBUTION

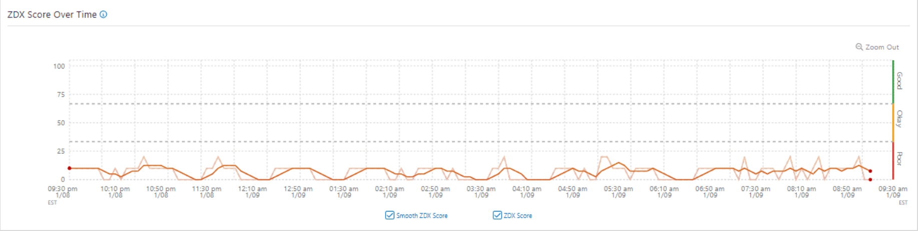
Poor Okay Good

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

User	ZDX Score	Zscaler Locations	Geolocations	Devices	Device Count
Viola Hansen (viola.hansen@th	5 / 100	Columbus Office	San Antonio, Texas, United Stat...	VIOLA-PC (VMware Virtual Platf...	1
Emma Willis (emma.willis@thez	10 / 100	Road Warrior	Dublin, Ohio, United States	KFQUWI (KFQUWI Android-11;ar...	1
Andrew Williams (andrew.williar	10 / 100	Columbus Office	Dublin, Ohio, United States	PC-Andre-17 (VMware7,1 Micro...	1
Ananya Patil (ananya.patil@the	10 / 100	Columbus Office	Dublin, Ohio, United States	PC-Ananya-35 (VMware7,1 Micr...	1
Alessia Rossi (alessia.rossi@the	10 / 100	Columbus Office	Dublin, Ohio, United States	PC-Aless-37 (VMware7,1 Micros...	1
Lucas Martinez (lucas.martinez	10 / 100	Columbus Office	Dublin, Ohio, United States	PC-Lucas-40 (VMware7,1 Micro...	1
Joni Sherman (joni.sherman@tl	10 / 100	Road Warrior	Tappahannock, Virginia, United ...	ZPM-JONI-SHERMA (Virtual Ma...	1
Ali Khan (ali.khan@thezerotrust	10 / 100	Columbus Office	Dublin, Ohio, United States	PC-Alikh-59-D (VMware7,1 Micr...	1

Copyright © 2007-2023 Zscaler Inc. All rights reserved. | Patents

When looking at the ZDX Score for a user, you will see a toggle option for “**Smooth ZDX Score.**” Occasionally, the ZDX Score can become noisy and hard to interpret due to a high degree of variance. The Smooth ZDX feature provides easier interpretation and visualization of the trendline. It does this by acting as a moving average, adding weight to previous scores in the past 30 minutes to smoothen the variations in the “point in time” ZDX Score.



Page Fetch Time (PFT)

There are a wide range of factors that contribute to a ZDX Score. However, the most significant metric factored in the computation of a ZDX Score is **Page Fetch Time**. PFT is the single most important metric available when determining a user's experience of using a web application because a poor PFT can ruin their experience even when all other metrics are great.

ZDX Score Baselining

Baseline vs Threshold

In order to fully understand the concepts at play in ZDX Scoring, it’s useful to understand two key terms: “baseline” and “threshold."

- Baseline represents the normal operating parameters for the activity that is being monitored—in this case, user activity across applications defined in the ZDX Administrator Portal

- Threshold defines the high (or low) values for whatever data is being collected

BASELINE VS THRESHOLDING	ZDX SCORE & BASELINING
For the kinds of performance measurements that ZDX is generating, we have found that baselining is more effective than thresholding, in part because creating useful threshold data requires advanced knowledge of the performance of all applications being measured, and those performance metrics change constantly.	Computing a ZDX Score using baselining is incredibly powerful. ZDX Score baseline values are calculated every day, for each application that a customer has defined or configured in their ZDX Administrator Portal, whether a given application is **custom** or **pre-defined**.

Those values are calculated in a rolling 7-day window of time. A 7-day window was chosen to ensure that the score can:

- Reflect the complete activity of a typical week

- Ensure that any performance or connectivity issues with a given application will be incorporated into the score and won’t be missed

- Incorporate that data in the form of percentile values across all applications the organization uses

Additional ZDX Score Factors

In addition to what we already discussed, recognizing these additional ZDX Score factors will be useful in case questions arise.

- The score indicated as part of the Application Tile is computed as the average score over the selected period of time.

- The User Score in the Users Page when multiple applications are selected corresponds to the score of the worst application during the selected time frame.

- Every device will probe and have its associated score. The User Score is the average of devices score.

- The Application Tile in the User Details page is the average score for the user in the selected time frame.

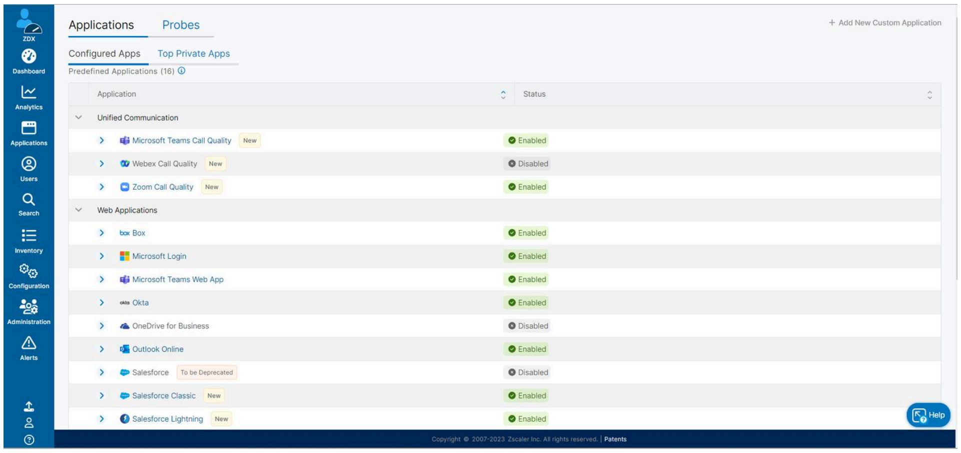
- The Application Score Over Time in the ZDX Dashboard or Application's Dashboard is the average score of all users at every point in time. The Application Score in the Application Tile is the average of all users for that selected period of time.

Applications

There are two types of applications that can be configured for monitoring with ZDX.

Predefined Applications

Predefined applications are templates for commonly used SaaS applications, such as SharePoint Online, Box, Salesforce and others. After you initially onboard a predefined application, ZDX will automatically create probes for it. In addition to these predefined probes, you can create your own custom probes for the application.



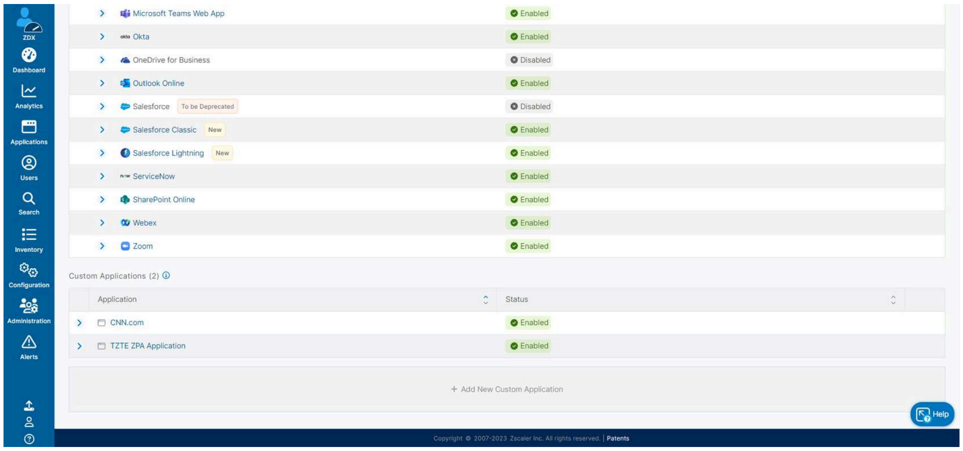
Predefined Applications (16)

Application	Status
Unified Communication	
Microsoft Teams Call Quality New	Enabled
Webex Call Quality New	Disabled
Zoom Call Quality New	Enabled
Web Applications	
Box	Enabled
Microsoft Login	Enabled
Microsoft Teams Web App	Enabled
Okta	Enabled
OneDrive for Business	Disabled
Outlook Online	Enabled
Salesforce To be Deprecated	Disabled
Salesforce Classic New	Enabled
Salesforce Lightning New	Enabled

Copyright © 2007-2023 Zscaler Inc. All rights reserved. | Patents

Custom Applications

Custom applications are used to monitor **any** internal or external application. In order to enable a custom application, you must configure at least one Web Probe.



Microsoft Teams Web App	Enabled
Okta	Enabled
OneDrive for Business	Disabled
Outlook Online	Enabled
Salesforce To be Deprecated	Disabled
Salesforce Classic New	Enabled
Salesforce Lightning New	Enabled
ServiceNow	Enabled
SharePoint Online	Enabled
Webex	Enabled
Zoom	Enabled

Custom Applications (2)

Application	Status
CNN.com	Enabled
TZTE ZPA Application	Enabled

Copyright © 2007-2023 Zscaler Inc. All rights reserved. | Patents

Integration with UCaaS Applications

ZDX provides integrations with UCaaS Applications such as Microsoft Teams, Zoom and Webex to make monitoring and troubleshooting meetings easy.

Microsoft Teams Integration with ZDX

ZDX's Integration with Microsoft Teams is made possible through an integration with the Microsoft Graph API, providing a call quality dashboard for immediate insight into issues that may occur during a Teams meeting.

The integration works by gathering data coming from that API, and is then put in context alongside everything ZDX is already measuring. This provides two major benefits:

1. **A Single Pane of Glass** for call quality information, end-to-end network metrics and Cloud Path details, and device metrics

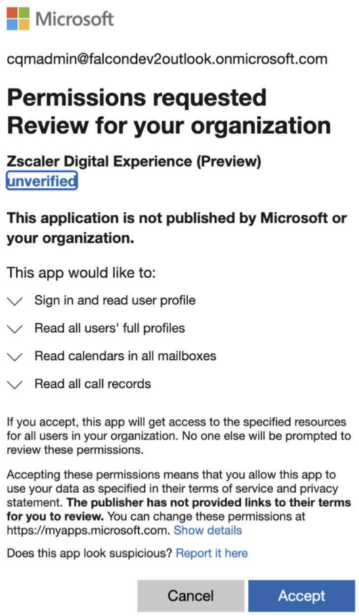
2. **Troubleshooting exactly where the problem happens** including what Teams meetings participants were affected and where in the network path the issues are being observed

"Unified Communications as a Service or (UCaaS), is a cloud-delivered unified communications model that supports six communications functions: Enterprise telephony, meetings (audio/video/web conferencing), unified messaging, instant messaging, and presence (personal and team), mobility, and communications-enabled business processes."

-Gartner

Microsoft Teams Integration Requirements

The Microsoft Teams Call Quality application leverages the integration with the Microsoft Graph API to retrieve information about users' call records within an organization. In order to read those records, an administrator will be initially redirected to Microsoft and asked to authenticate. Zscaler then requires consent to a set of permissions.



Microsoft

cqmadmin@falcondev2outlook.onmicrosoft.com

Permissions requested
Review for your organization

Zscaler Digital Experience (Preview)
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- Sign in and read user profile
- Read all users' full profiles
- Read calendars in all mailboxes
- Read all call records

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

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

Does this app look suspicious? Report it here

How to Monitor Microsoft Teams With ZDX’s integration with Microsoft Teams there are two applications to configure that are continuously being monitored:	
Microsoft Teams Application	● Probes signaling endpoint to teams.microsoft.com ● ZDX Score based on Page Fetch Time to teams.microsoft.com
Microsoft Teams Call Quality Application	● Probes to the transport relay worldaz.tr.teams.microsoft.com and a ZDX Autosense probe, which detects and probes endpoints dynamically rather than probing fixed endpoints at fixed intervals ● Extracts meeting information from a tenant's users, including a history of meetings with participants' metrics that are displayed on the User Details page ● The ZDX Score is based on Mean Opinion Score (MOS) that drills down into thresholds such as jitter, loss, and latency. MOS uses a transmission rating factor (R-Factor) that generates range levels it derives from those particular metrics. MOS rates call quality on a scale from 1 to 5 (worst to best). The range levels help determine the ZDX Score for Call Quality as Poor (MOS is between 0 and 3.6) , Okay (MOS >3.6<4.34), or Good (MOS > 4.34).

- There are three additional UCaaS metrics added to the User Details page:
    - Audio: Latency, jitter, average, and max loss
    - Video: Latency, jitter, average, and max loss
    - Screen Sharing: Latency, jitter, average, and max loss

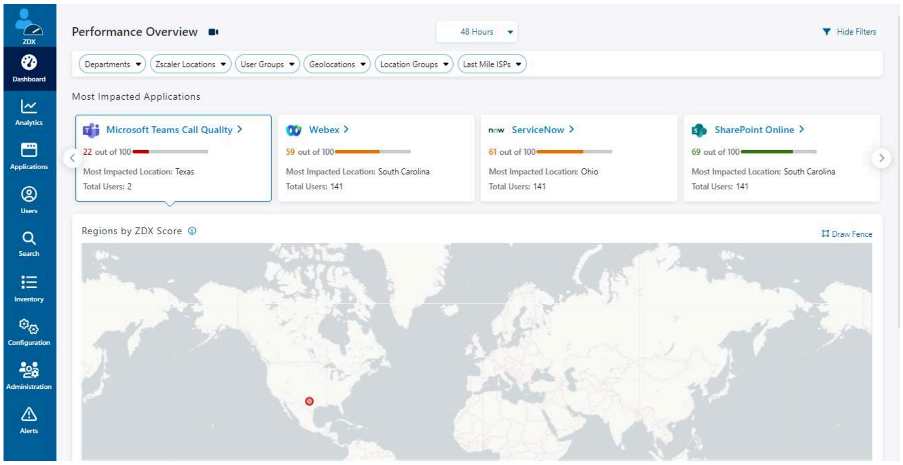
Viewing Call Quality Metrics

Below, view the following four areas as they relate to the Microsoft Teams Call Quality Application on the ZDX Administrator Portal: **ZDX Dashboard, Applications Dashboard, Meetings Tab, and Meeting Metrics.**

– The ZDX dashboard views for Zoom & Webex are similar to Microsoft Teams Call Quality.

ZDX Dashboard

Once configured, the Teams Call Quality Application will appear on the ZDX Dashboard. On the map, you can view where meetings have taken place and filter down from there. Also presented is the ZDX Score that shows the score for all users and meetings happening in the allotted time frame selected.



Microsoft Teams Call Quality
22 out of 100
Most Impacted Location: Texas
Total Users: 2

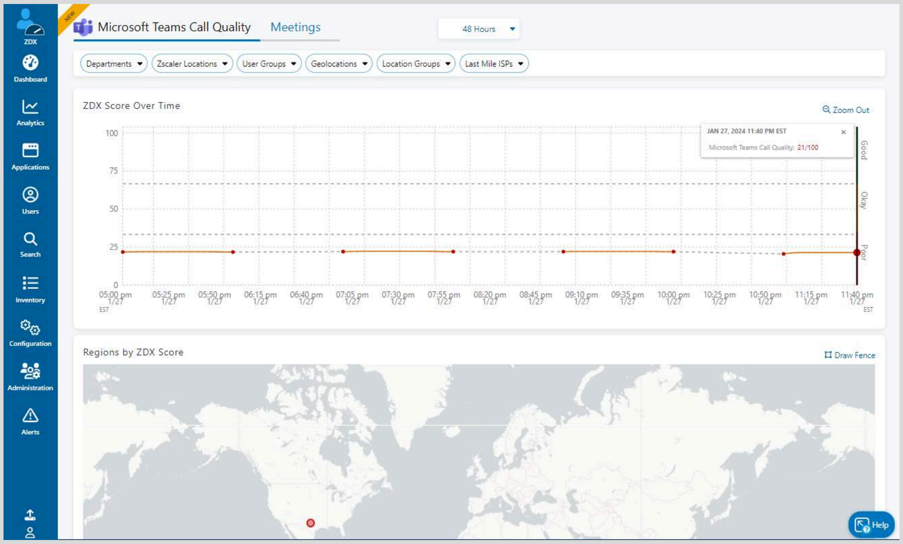
Webex
59 out of 100
Most Impacted Location: South Carolina
Total Users: 141

ServiceNow
61 out of 100
Most Impacted Location: Ohio
Total Users: 141

SharePoint Online
69 out of 100
Most Impacted Location: South Carolina
Total Users: 141

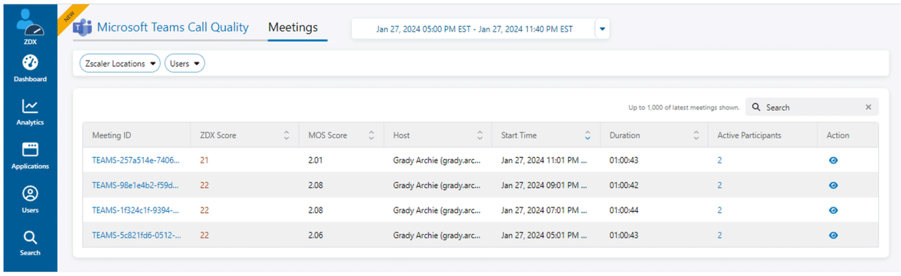
Applications Dashboard

The ZDX Score Over Time and Map View are shown on the Applications Dashboard. In addition, there is a widget showcasing the top meetings by meeting ID and/or name. At the top of the Applications Dashboard, one can also toggle to view “Meetings”.



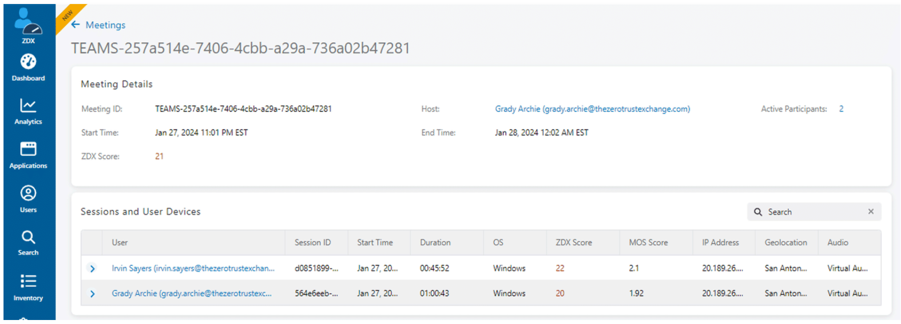
Meetings Tab

This is where all meetings are listed and where you can view the high-level ZDX Score, MOS Score, start and end time of a meeting, and the number of participants. You can also drill down further to troubleshoot issues happening within that particular meeting. This tab may show different types of users, for example authenticated users with Client Connector running, or external guests.



Up to 1,000 of latest meetings shown.

Meeting ID	ZDX Score	MOS Score	Host	Start Time	Duration	Active Participants	Action
TEAMS-257a514e-7406...	21	2.01	Grady Archie (grady.arc...	Jan 27, 2024 11:01 PM ...	01:00:43	2	👁
TEAMS-98e1e4b2-f59d...	22	2.08	Grady Archie (grady.arc...	Jan 27, 2024 09:01 PM ...	01:00:42	2	👁
TEAMS-1f324c1f-9394-...	22	2.08	Grady Archie (grady.arc...	Jan 27, 2024 07:01 PM ...	01:00:44	2	👁
TEAMS-5c821fd6-0512-...	22	2.06	Grady Archie (grady.arc...	Jan 27, 2024 05:01 PM ...	01:00:43	2	👁



TEAMS-257a514e-7406-4cbb-a29a-736a02b47281

Meeting Details

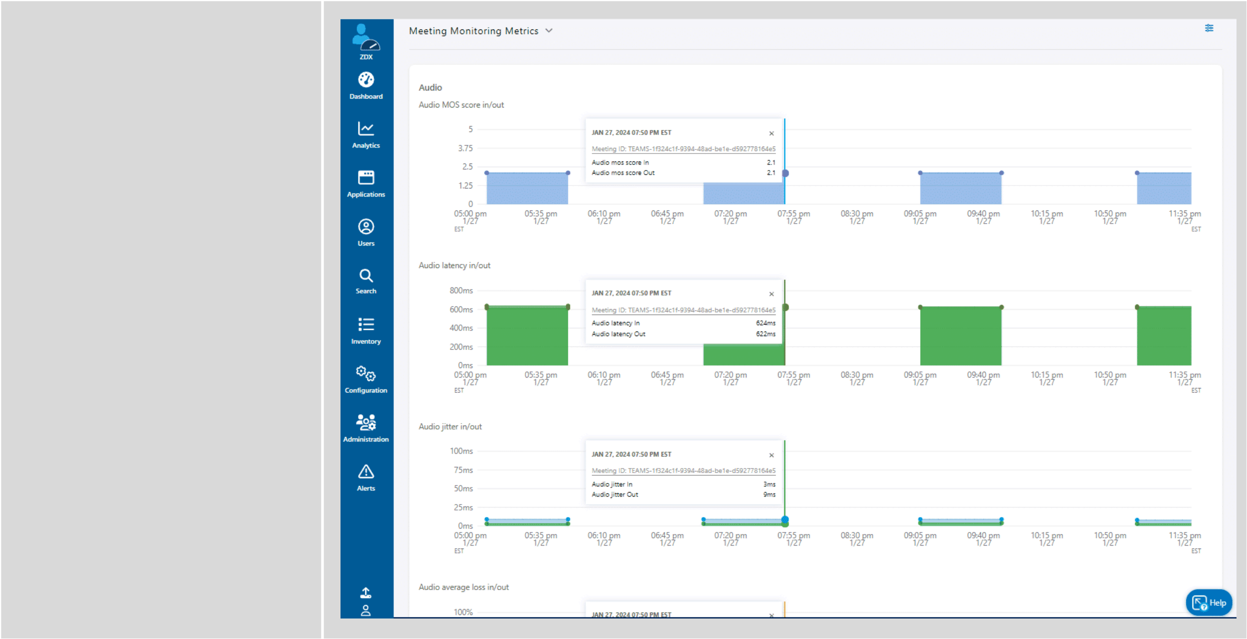
Meeting ID: TEAMS-257a514e-7406-4cbb-a29a-736a02b47281
Host: Grady Archie (grady.archie@thezerotrustexchange.com)
Active Participants: 2
Start Time: Jan 27, 2024 11:01 PM EST
End Time: Jan 28, 2024 12:02 AM EST
ZDX Score: 21

Sessions and User Devices

	User	Session ID	Start Time	Duration	OS	ZDX Score	MOS Score	IP Address	Geolocation	Audio
>	Irvin Sayers (irvin.sayers@thezerotrustexchan...	d0851899-...	Jan 27, 20...	00:45:52	Windows	22	2.1	20.189.26....	San Anton...	Virtual Au...
>	Grady Archie (grady.archie@thezerotrustexc...	564e6eeb-...	Jan 27, 20...	01:00:43	Windows	20	1.92	20.189.26....	San Anton...	Virtual Au...

Meeting Metrics

Clicking on a username instrumented with ZDX will direct you to the User Details page, which is where you can drill down to determine an issue within a meeting, and view the meeting metrics for that user.



JAN 27, 2024 07:50 PM EST

Meeting ID: TEAMS-1f324c1f-9394-48ad-be1e-d592778164e5

Audio mos score In 2.1

Audio mos score Out 2.1

JAN 27, 2024 07:50 PM EST

Meeting ID: TEAMS-1f324c1f-9394-48ad-be1e-d592778164e5

Audio latency In 624ms

Audio latency Out 622ms

JAN 27, 2024 07:50 PM EST

Meeting ID: TEAMS-1f324c1f-9394-48ad-be1e-d592778164e5

Audio jitter In 3ms

Audio jitter Out 9ms

JAN 27, 2024 07:50 PM EST

Zoom Integration with ZDX

ZDX's Integration with Zoom allows data to be captured in real time as a meeting is in progress. User and device information garnered from the API for call participants is mapped to ZDX users and devices. It supports two methods to collect Zoom call quality metrics:

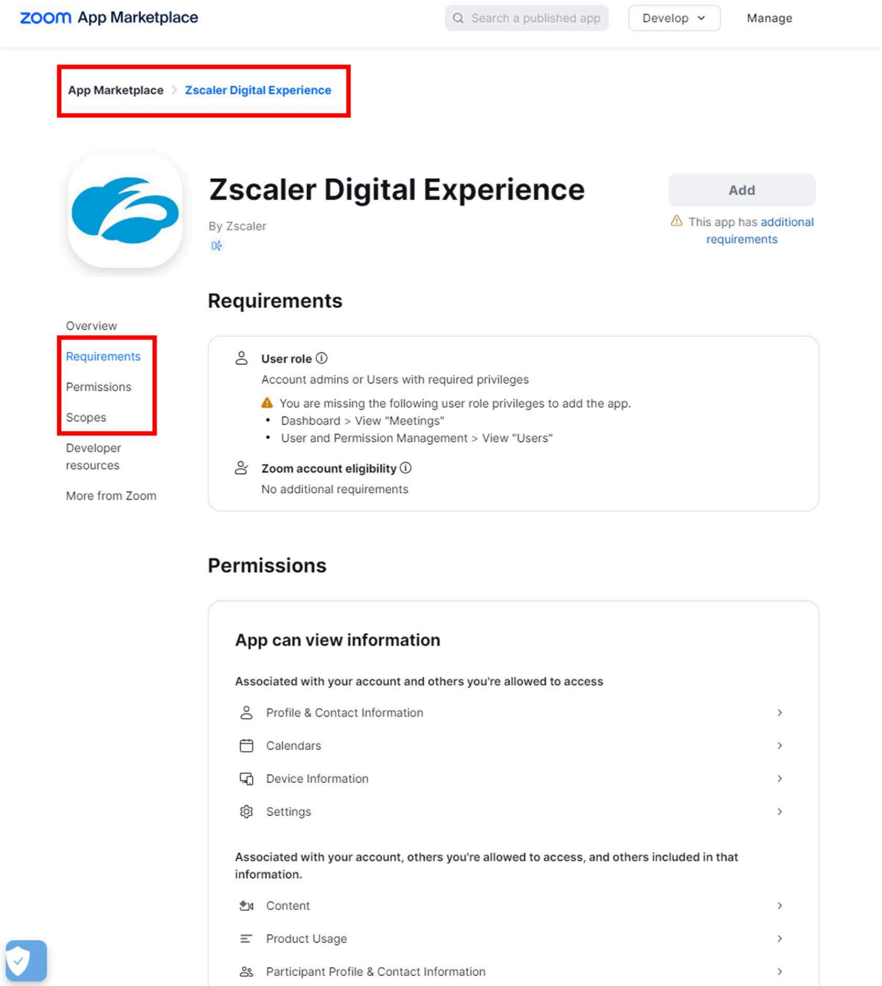
1. Default API: ZDX receives webhook notifications from Zoom for your tenant when a meeting starts or stops. ZDX then makes periodic API calls to retrieve meeting QoS data and makes the data available via APIs to display on the ZDX Admin portal.

2. Quality of Service Subscription (QSS) API: was introduced by Zoom to overcome challenges with rate limits of the default API. With QSS, Zoom will periodically push call quality information to ZDX.

Zoom Integration Requirements

For required permissions and API scope settings, check the Zoom Marketplace.

The Zscaler Help documentation provides details on the required ZDX and Client Connector versions, subscription levels, etc. and step-by-step guides for onboarding a new Zoom tenant.



⚠ This app has additional requirements

Requirements

User role ⓘ
Account admins or Users with required privileges
⚠ You are missing the following user role privileges to add the app.
- Dashboard > View "Meetings"
- User and Permission Management > View "Users"

Zoom account eligibility ⓘ
No additional requirements

Permissions

App can view information

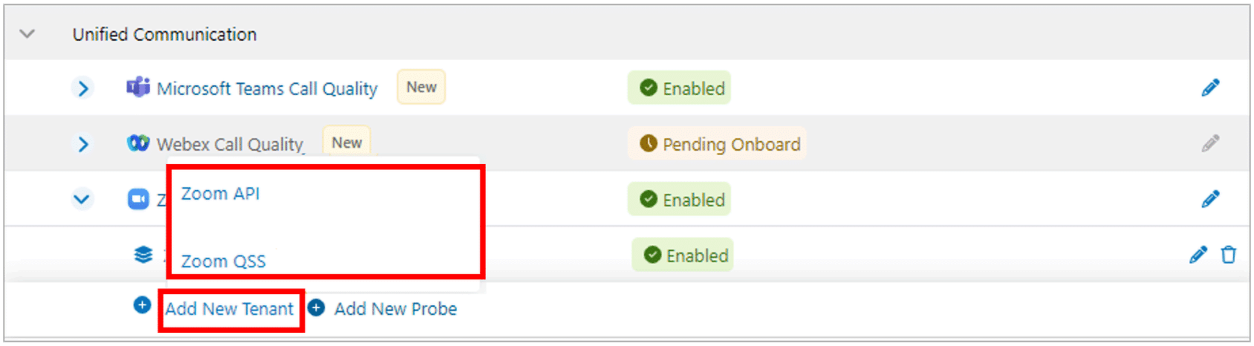
Associated with your account and others you're allowed to access

- Profile & Contact Information
- Calendars
- Device Information
- Settings

Associated with your account, others you're allowed to access, and others included in that information.

- Content
- Product Usage
- Participant Profile & Contact Information

You can onboard either a Zoom API Tenant or a Zoom QSS tenant. You cannot onboard both at one time.



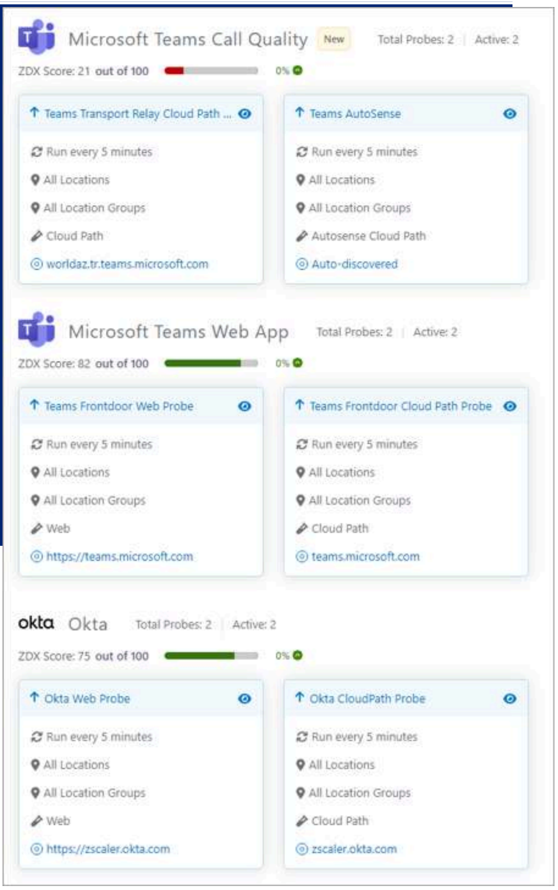
Unified Communication

Microsoft Teams Call Quality New	Enabled	
Webex Call Quality New	Pending Onboard	
Z	Enabled	
	Enabled	

Probes

What is a Probe?

As a Digital Experience Monitoring platform, ZDX needs to gather accurate, relevant, and recent metrics about critical applications, in addition to the endpoint details being gathered by the Client Connector. Bearing in mind that there are two types of applications supported (predefined and custom), ZDX uses a concept called “probes”.



Microsoft Teams Call Quality New Total Probes: 2 | Active: 2
ZDX Score: 21 out of 100 0%

Teams Transport Relay Cloud Path ...
Run every 5 minutes
All Locations
All Location Groups
Cloud Path
worldaz.tr.teams.microsoft.com

Teams AutoSense
Run every 5 minutes
All Locations
All Location Groups
Autosense Cloud Path
Auto-discovered

Microsoft Teams Web App Total Probes: 2 | Active: 2
ZDX Score: 82 out of 100 0%

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

Teams Frontdoor Cloud Path Probe
Run every 5 minutes
All Locations
All Location Groups
Cloud Path
teams.microsoft.com

okta Okta Total Probes: 2 | Active: 2
ZDX Score: 75 out of 100 0%

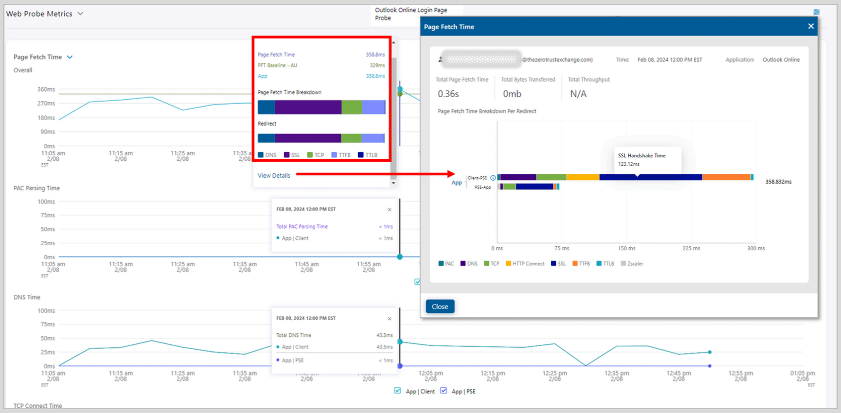
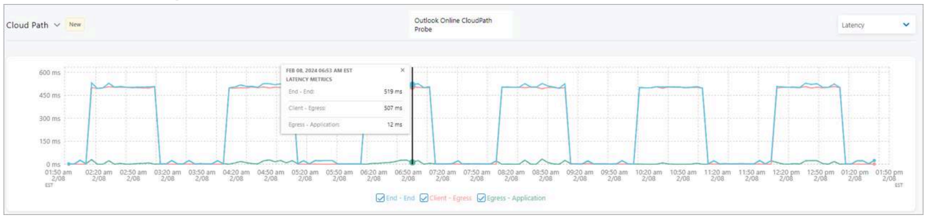
Okta Web Probe
Run every 5 minutes
All Locations
All Location Groups
Web
https://zscaler.okta.com

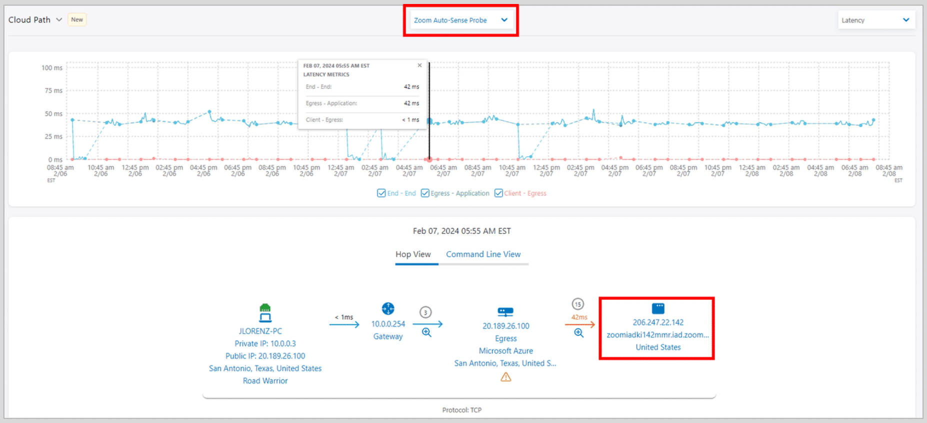
Okta CloudPath Probe
Run every 5 minutes
All Locations
All Location Groups
Cloud Path
zscaler.okta.com

A probe is an automated process through which ZDX logs metrics related to the performance and availability of applications, and this data can then be used to determine the ZDX Score for a given application. **Predefined Applications** have preconfigured probes associated with them by default, while **Custom Applications** require probes to be manually created.

There are three types of probes; Web Probe, Cloud Path Probe and Autosense Cloud Path Probe.

Web Probe	**With a Web Probe, ZDX gathers metrics like:** **Page Fetch Time:** This metric collects the time it takes to pull down (or “fetch") a web page from the specified URL. It requests only the top-level page document and does not request all embedded links within the web page. In short, the primary purpose of Page Fetch Time is to essentially simulate the web browsing experience of the user, in a way that can be precisely quantified. With this in mind, the Page Fetch Time metric generates up to 8 requests in parallel, in much the same way that a typical browser would. Also, Page Fetch Time leverages caching, which will be described later. When a connection to the server is not successful, error codes indicating the reason are displayed. Depending on your ZDX subscription, you may have access to a tooltip on the PFT graph with DNS, SSL, TCP, TTFB (Time to First Byte), and TTLB (Time to Last Byte) metrics that comprise the total Page Fetch Time.

	 Web Probe Metrics Outlook Online Login Page Probe Page Fetch Time Overall Page Fetch Time 358.8ms PFT Baseline - AU 329ms App 358.8ms Page Fetch Time Breakdown Redirect DNS SSL TCP TTFB TTLB View Details PAC Parsing Time FEB 08, 2024 12:00 PM EST Total PAC Parsing Time < 1ms App | Client < 1ms DNS Time Total DNS Time 43.5ms App | Client 43.5ms App | PSE < 1ms ☑ App | Client ☑ App | PSE TCP Connect Time Page Fetch Time [redacted]@thezerotrustexchange.com) Time: Feb 08, 2024 12:00 PM EST Application: Outlook Online Total Page Fetch Time 0.36s Total Bytes Transferred 0mb Total Throughput N/A Page Fetch Time Breakdown Per Redirect SSL Handshake Time 123.12ms App Client-PSE PSE-App 358.832ms 0 ms 75 ms 150 ms 225 ms 300 ms PAC DNS TCP HTTP Connect SSL TTFB TTLB Zscaler Close Additional PFT-related graphs are displayed for PAC parsing, DNS, TCP Connect, SSL handshake, HTTP Connect time. These graphs help identify which portion of the page load contributed disproportionate to the total transaction time. **DNS 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:** This metric measures the interval between requesting a resource and the first byte of data received back from the server. This metric is sometimes referred to as the “Time To First Byte” or “TTFB.” **Availability:** If a successful HTTP response code is received in response to a fetch request, the response code will be either 1 or 0, with 0 indicating that the probe timed out without ever receiving a response from the server.
Cloud Path Probe	Cloud Path Probes are a very sophisticated and innovative aspect of the ZDX service. Cloud Path Probes are **built around a highly optimized traceroute algorithm which allows ZDX to parallelize traceroute execution.** In other words, this allows a Cloud Path Probe to **gather performance metrics on all the hops between a client and the configured application simultaneously,** rather than in sequence. For every application discovery, there will be multiple runs (as per the configured packet count) with packets paced evenly over time to avoid peaks of traffic.  Cloud Path New Outlook Online CloudPath Probe Latency 600 ms 450 ms 300 ms 150 ms 0 ms FEB 08, 2024 06:53 AM EST LATENCY METRICS End - End 519 ms Client - Egress 507 ms Egress - Application 12 ms 01:50 am 02:20 am 02:50 am 03:20 am 03:50 am 04:20 am 04:50 am 05:20 am 05:50 am 06:20 am 06:50 am 07:20 am 07:50 am 08:20 am 08:50 am 09:20 am 09:50 am 10:20 am 10:50 am 11:20 am 11:50 am 12:20 pm 12:50 pm 01:20 pm 01:50 pm 2/08 EST ☑ End - End ☑ Client - Egress ☑ Egress - Application

Autosense Cloud Path Probe	For UCaaS applications, the endpoint of the cloud path e.g. Zoom Multimedia Router (MMR) will likely change, based on the server a call gets connected to. That limits the usefulness of regular, synthetic cloud path probes for network analysis, because they are "hard-coded" to a specific cloud path host. A driver installed in Client Connector dynamically detects the destination IP address and port of the server a call gets connected to and will start probing the cloud path to that server for the duration of the call. This provides a more precise correlation between the UCaaS metrics and cloud path probe data.  Cloud Path New Zoom Auto-Sense Probe Latency FEB 07, 2024 05:55 AM EST LATENCY METRICS End - End: 42 ms Egress - Application: 42 ms Client - Egress: < 1 ms 100 ms 75 ms 50 ms 25 ms 0 ms 08:45 am 2/06 EST 10:45 am 2/06 12:45 pm 2/06 02:45 pm 2/06 04:45 pm 2/06 06:45 pm 2/06 08:45 pm 2/06 10:45 pm 2/06 12:45 am 2/07 02:45 am 2/07 04:45 am 2/07 06:45 am 2/07 08:45 am 2/07 10:45 am 2/07 12:45 pm 2/07 02:45 pm 2/07 04:45 pm 2/07 06:45 pm 2/07 08:45 pm 2/07 10:45 pm 2/07 12:45 am 2/08 02:45 am 2/08 04:45 am 2/08 06:45 am 2/08 08:45 am 2/08 EST ☑ End - End ☑ Egress - Application ☑ Client - Egress Feb 07, 2024 05:55 AM EST Hop View Command Line View JLORENZ-PC Private IP: 10.0.0.3 Public IP: 20.189.26.100 San Antonio, Texas, United States Road Warrior < 1ms 10.0.0.254 Gateway 3 20.189.26.100 Egress Microsoft Azure San Antonio, Texas, United S... 15 42ms 206.247.22.142 zoomiadki142mmr.iad.zoom... United States Protocol: TCP Example Cloud Path with Zoom Autosense probe, which detected the specific Zoom MMR server the end user’s meeting is hosted on

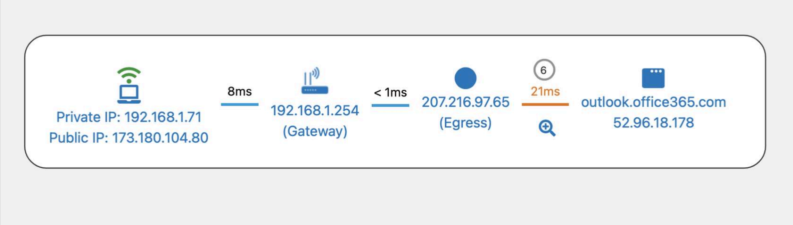
Cloud Path

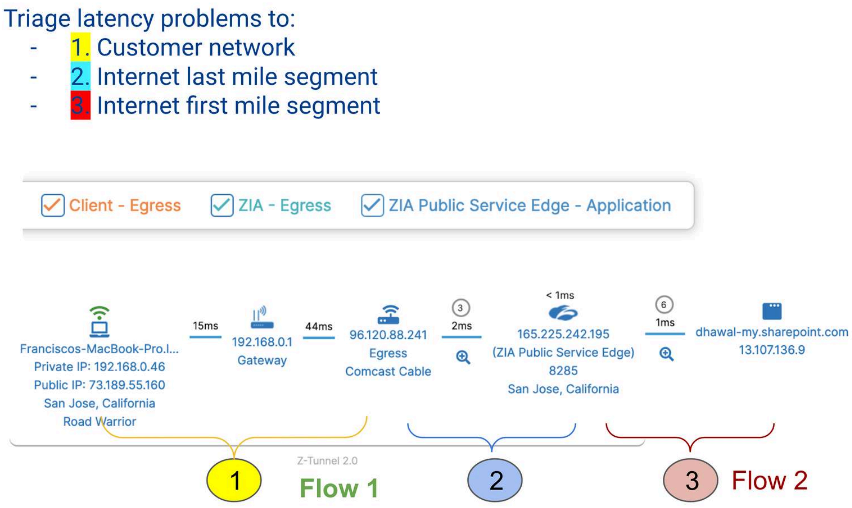
> **“Cloud Path”** is used to help visualize the journey that network data will take between the client and whatever application is being accessed.

Cloud Path Legs

Cloud Path Probes use a traceroute algorithm to discover the network path with all hops along the path, and measure the network performance, including latency and packet loss.

There are three different paths that provide visualization from the client to the application: Direct, through Zscaler Internet Access (ZIA), and through Zscaler Private Access (ZPA). Let's look at all three in order to understand the significant segments along each path and how the **Hop View** in the ZDX Administrator Portal visualizes the different legs.

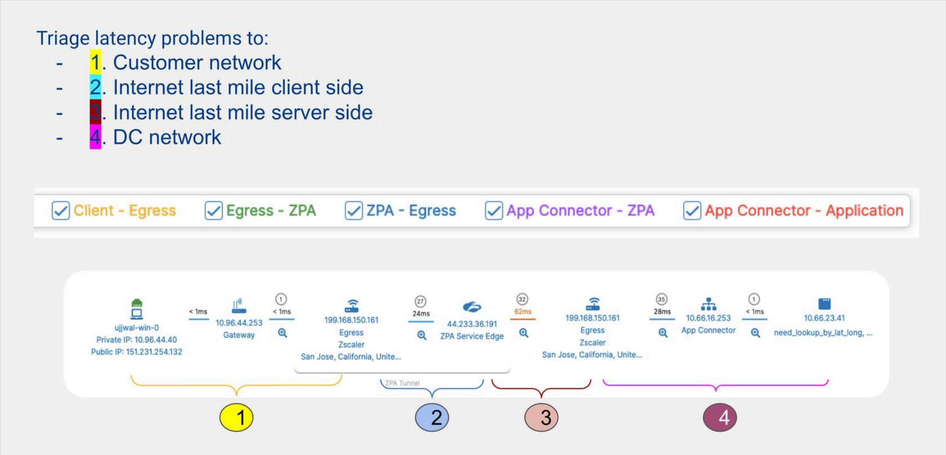
Direct Cloud Path	 Private IP: 192.168.1.71 Public IP: 173.180.104.80 8ms 192.168.1.254 (Gateway) < 1ms 207.216.97.65 (Egress) 6 21ms outlook.office365.com 52.96.18.178 Cloud Path Probes can provide visualization cases where traffic will follow a direct traffic path: **Zscaler Client Connector > Local Egress > Application**
Cloud Path Through ZIA	Cloud Path Probes provide visualization in cases where a client’s traffic is passing through a Zscaler Internet Access (ZIA) Public Service Edge: **Zscaler Client Connector > Local Egress > ZIA Public Service Edge > Application** In this image, you can see the path, each leg on the path, and where to triage latency problems.



Triage latency problems to:

- 1. Customer network
- 2. Internet last mile segment
- 3. Internet first mile segment

☑ Client - Egress ☑ ZIA - Egress ☑ ZIA Public Service Edge - Application

<table>
<tr>
<td><b>Cloud Path Through ZPA</b></td>
<td>
Cloud Path Probes provide visualization in cases where a client’s traffic is passing through Zscaler Private Access (ZPA) Service Edge:
<b>Zscaler Client Connector > Local Egress > ZPA Service Edge &gt;</b> Application
In this image, you can see the path, each leg on the path, and where to triage latency problems.

Triage latency problems to:
- 1. Customer network
- 2. Internet last mile client side
- 3. Internet last mile server side
- 4. DC network
☑ Client - Egress ☑ Egress - ZPA ☑ ZPA - Egress ☑ App Connector - ZPA ☑ App Connector - Application

</td>
</tr>
</table>

Cloud Path Probes are used to collect the following metrics:

- **Hop Count:** The number of hops between each hop point on the path between client and application.

- **Packet Loss:** The % of packet loss at each hop point on the path between client and application.

- **Latency** (Average, Minimum, Maximum, and Standard Deviation): This is the roundtrip path time, measured in milliseconds. Standard Deviation can also be considered as jitter.

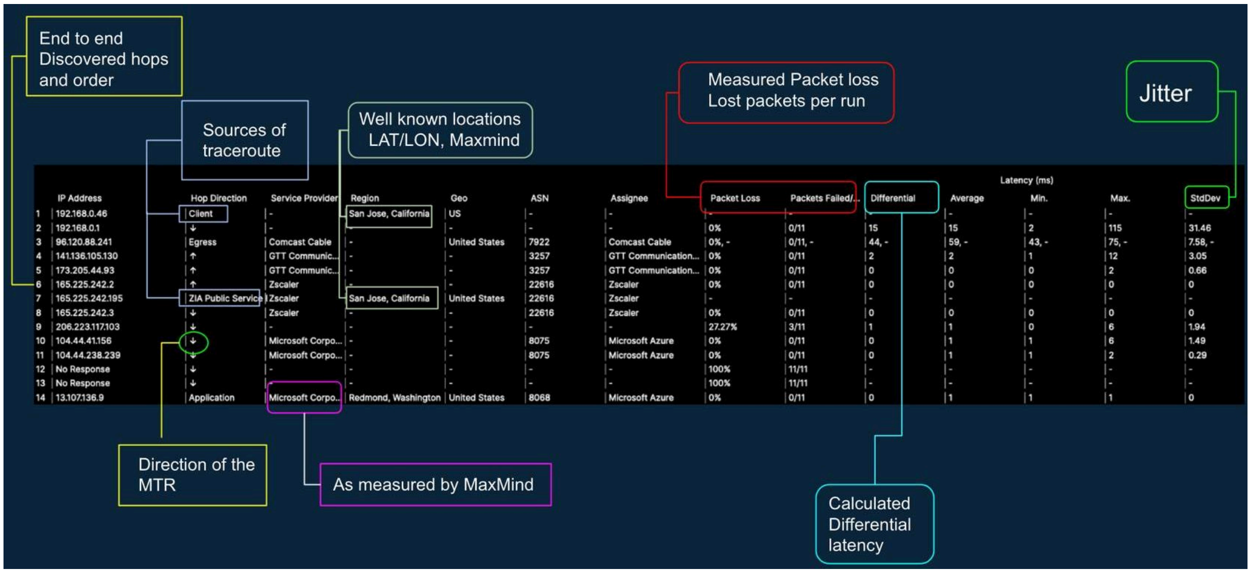
Cloud Path Probes support ICMP, UDP-based traceroutes, TCP traceroutes, and Adaptive protocol that will discover the best option per leg segment.

Command Line View

You can also review all Cloud Path data and parameters by switching to Command Line View. The first column on the left shows the IP addresses of all hops. The Hop Direction (from the client to your egress IP, from ZIA Public or Private Service Edges to your egress IP, and from Service Edges to destination) is indicated by Up and Down arrows.

Then there is Geo information, ISP names, Regions, and Zscaler locations that are derived from device location information and from an extensive MaxMind database. Other parameters displayed in this view include Packet Loss (%) and PacketsFailed, as well as Latency metrics.

Here's a tip when reading the Cloud Path: The loss that matters the most is the one on the destination. Routers on the Internet usually rate limit ICMP. Sometimes you might see that the Packet Loss on some of the intermediate hops is high, but there is no packet loss at the destination. It's always a good idea to look at other metrics like the page fetch time, DNS response times when troubleshooting slowness.



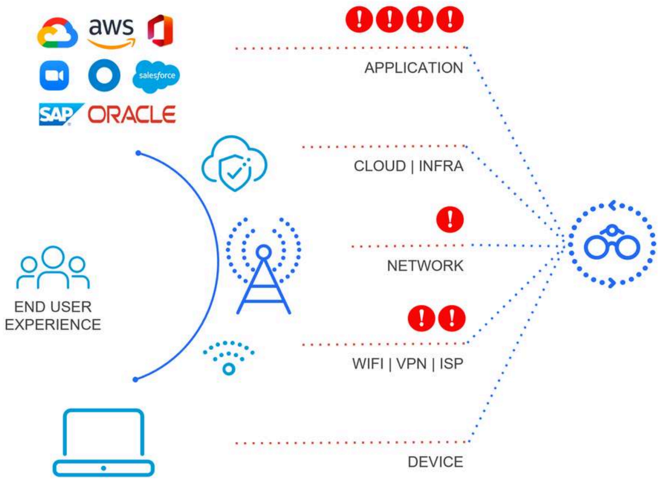
	IP Address	Hop Direction	Service Provider	Region	Geo	ASN	Assignee	Packet Loss	Packets Failed/...	Latency (ms) Differential	Average	Min.	Max.	StdDev
1	192.168.0.46	Client	-	San Jose, California	US	-	-	-	-	-	-	-	-	-
2	192.168.0.1	↓	-	-	-	-	-	0%	0/11	15	15	2	115	31.46
3	96.120.88.241	Egress	Comcast Cable	-	United States	7922	Comcast Cable	0%, -	0/11, -	44, -	59, -	43, -	75, -	7.58, -
4	141.136.105.130	↑	GTT Communic...	-	-	3257	GTT Communication...	0%	0/11	2	2	1	12	3.05
5	173.205.44.93	↑	GTT Communic...	-	-	3257	GTT Communication...	0%	0/11	0	0	0	2	0.66
6	165.225.242.2	↑	Zscaler	-	-	22616	Zscaler	0%	0/11	0	0	0	0	0
7	165.225.242.195	ZIA Public Service	Zscaler	San Jose, California	United States	22616	Zscaler	-	-	-	-	-	-	-
8	165.225.242.3	↓	Zscaler	-	-	22616	Zscaler	0%	0/11	0	0	0	0	0
9	206.223.117.103	↓	-	-	-	-	-	27.27%	3/11	1	1	0	6	1.94
10	104.44.41.156	↓	Microsoft Corpo...	-	-	8075	Microsoft Azure	0%	0/11	0	1	1	6	1.49
11	104.44.238.239	↓	Microsoft Corpo...	-	-	8075	Microsoft Azure	0%	0/11	0	1	1	2	0.29
12	No Response	↓	-	-	-	-	-	100%	11/11	-	-	-	-	-
13	No Response	↓	-	-	-	-	-	100%	11/11	-	-	-	-	-
14	13.107.136.9	Application	Microsoft Corpo...	Redmond, Washington	United States	8068	Microsoft Azure	0%	0/11	0	1	1	1	0

End to end Discovered hops and order
Sources of traceroute
Well known locations LAT/LON, Maxmind
Measured Packet loss Lost packets per run
Jitter
Direction of the MTR
As measured by MaxMind
Calculated Differential latency

Automated Root Cause Analysis

With many employees now working from home, the office, or a combination of the two, IT needs to ensure optimal digital experiences across a wider range of networks, even those not in their control. This is why IT operations and service desk teams often struggle to pinpoint the exact root cause of application issues, system failures, latency, or poor user experience.

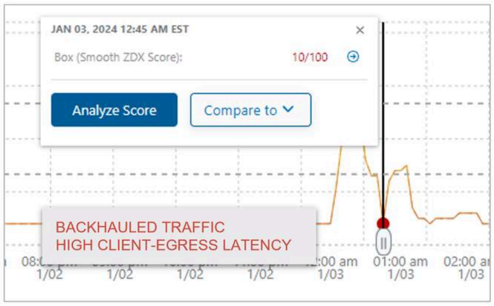
ZDX can quickly identify the root cause of user experience issues with its AI-powered analysis capability (called Y-Engine). It spares IT teams the labor of sifting through fragmented data and troubleshooting, thereby accelerating resolution and keeping employees productive.



Automate Root Causes Analysis

across
apps, services, users, regions, time, etc.

due to
ISP, wifi, backhaul, VPN, internet, egress, etc.



JAN 03, 2024 12:45 AM EST

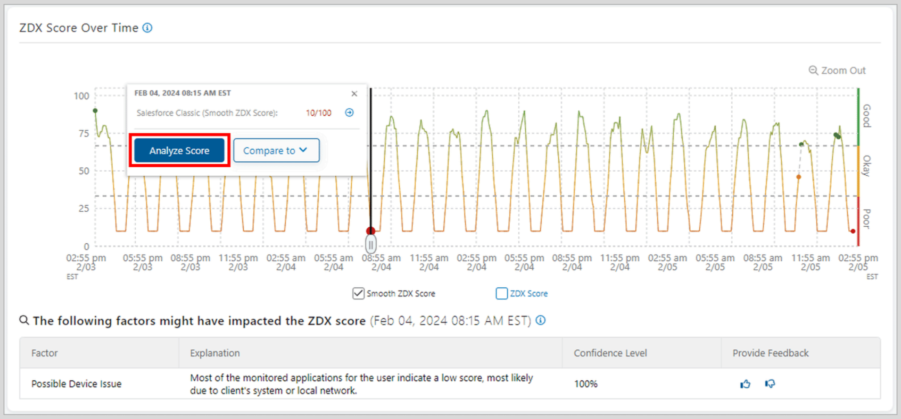
Box (Smooth ZDX Score): 10/100

Identifying root cause in ZDX is simple: pick a point in time where user experience is impacted and click **Analyze Score**.

Automated Root Cause Analysis can be used to evaluate a poor (0–33) score for a **single date and time**, for a **time range** and **compare** the current score with a previous score.

Single Date and Time

In this mode, the ZDX Score Over Time graph includes a feature to help identify reasons for the low score. The application tile with the **lowest Poor score is preselected**, and ZDX runs root cause analysis automatically on the most recent Poor score. As a result of the analysis, potential factors are provided that might have contributed to the score.



FEB 04, 2024 08:15 AM EST

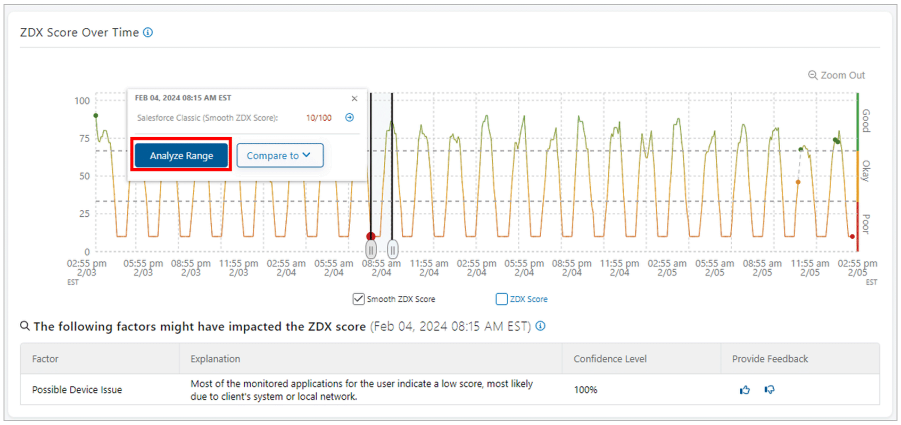
Salesforce Classic (Smooth ZDX Score): 10/100

The following factors might have impacted the ZDX score (Feb 04, 2024 08:15 AM EST)

Factor	Explanation	Confidence Level	Provide Feedback
Possible Device Issue	Most of the monitored applications for the user indicate a low score, most likely due to client's system or local network.	100%	👍 👎

Time Range

The ZDX Score Over Time graph also includes an option to analyze scores within a time range. After you select a point on the graph for a Poor score at a specific date and time, you can drag a slider to specify the end of the time range.



FEB 04, 2024 08:15 AM EST

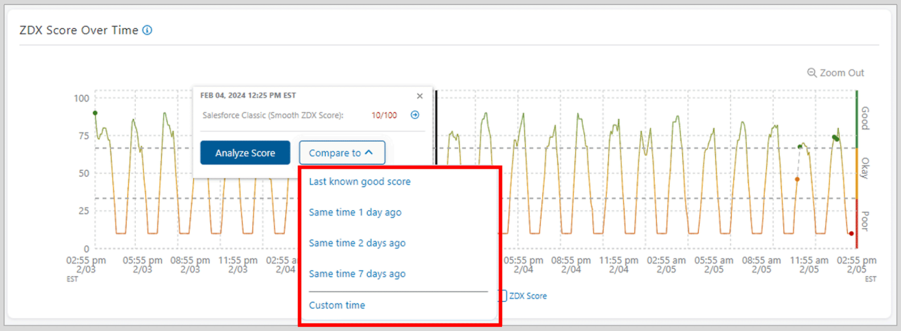
Salesforce Classic (Smooth ZDX Score): 10/100

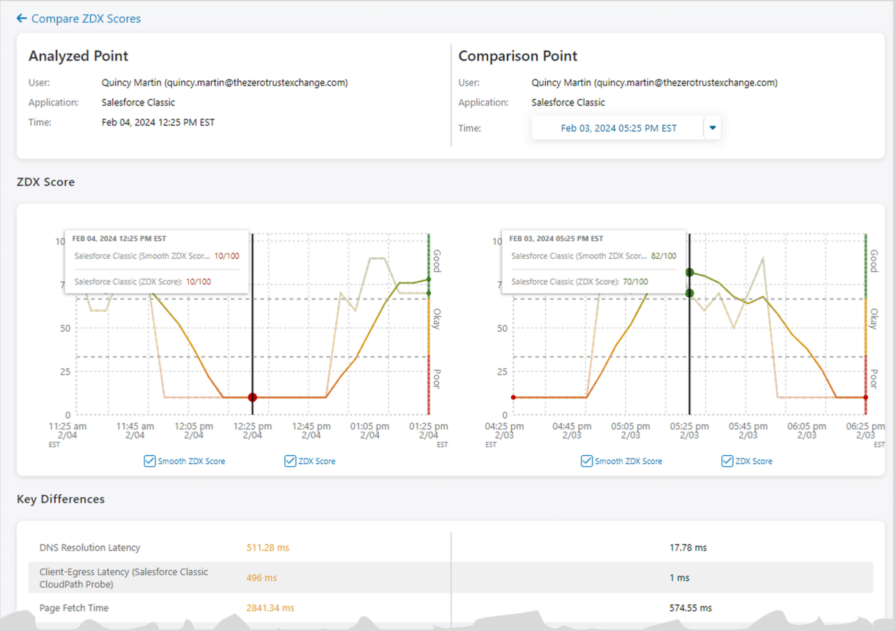
The following factors might have impacted the ZDX score (Feb 04, 2024 08:15 AM EST)

Factor	Explanation	Confidence Level	Provide Feedback
Possible Device Issue	Most of the monitored applications for the user indicate a low score, most likely due to client's system or local network.	100%	👍 👎

Compare

You can also compare ZDX Scores for an application to understand why they might vary at different points in time. A score comparison can highlight why a current score might be considerably different from a previous score. This option shows a side-by-side comparison of web, device, and Cloud Path metrics to help determine differences in scoring. You can select a predefined comparison point, e.g. Last known good score, or select a specific date/time.




← Compare ZDX Scores

Analyzed Point

User: Quincy Martin (quincy.martin@thezerotrustexchange.com)
Application: Salesforce Classic
Time: Feb 04, 2024 12:25 PM EST

Comparison Point

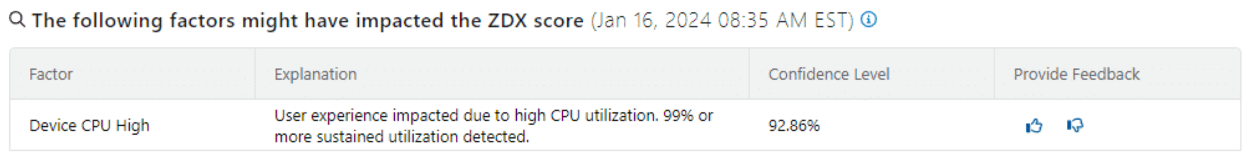
User: Quincy Martin (quincy.martin@thezerotrustexchange.com)
Application: Salesforce Classic
Time: Feb 03, 2024 05:25 PM EST

ZDX Score

Key Differences

DNS Resolution Latency	511.28 ms	17.78 ms
Client-Egress Latency (Salesforce Classic CloudPath Probe)	496 ms	1 ms
Page Fetch Time	2841.34 ms	574.55 ms

Example analysis output, showing a probable cause for a poor ZDX score.


The following factors might have impacted the ZDX score (Jan 16, 2024 08:35 AM EST) ⓘ

Factor	Explanation	Confidence Level	Provide Feedback
Device CPU High	User experience impacted due to high CPU utilization. 99% or more sustained utilization detected.	92.86%	👍 👎

Deep Tracing

For most day-to-day activities and situations, the perspective provided by the dashboards in the ZDX Administrator Portal will suffice. However, when additional detail is needed, ZDX can provide deeper granularity into process-level information for a user, via the functionality called Deep Tracing. During a Deep Tracing session, information is collected every minute for the Web Probe, Cloud Path Probe, as well as device statistics.

Because Deep Tracing is providing a wealth of highly-granular information relating to both the endpoint and the application, it is typically engaged for short ‘bursts’ of time. While Deep Tracing can be engaged for up to 60 minutes (maximum), a 5-minute Deep Tracing session can be enough to provide the necessary information to uncover the cause of a poor user experience.

Running a Deep Tracing Session

An administrator can start a Deep Tracing session in the ZDX Administrator Portal to analyze issues that users may be facing. An administrator can select a user, a device, and an application that they are experiencing issues on to troubleshoot, and can choose to run the Deep Tracing session from 5 minutes for up to 60 minutes to monitor issues. The administrator can then view session information in the Deep Tracing page and also export it in PDF format for reference, archiving, or sharing.

Deep Tracing also allows an administrator to quickly evaluate the user experience to any previously-defined application which already has probes enabled, or to simply enter an arbitrary URL, even if it has not been explicitly configured as an application elsewhere in ZDX. If the administrator performs a Deep Tracing session against an arbitrarily-entered URL, this is not counted towards their organizational probe quota.

There are two additional options that are available with Deep Tracing:

1. **Packet Capture Probing** allows you to run a remote packet capture on a device without the need to install any additional software on the device. The resulting pcap file is stored locally on the user's device and can be attached to a support ticket.

2. **Bandwidth Test** runs a bandwidth test from the user to the Zscaler data center and collects upload/download bandwidth metrics, basic diagnostics and cloud path details.

Alerts & Rules

Alerts

Alerts enable you to monitor your device, application, network performance, and ZDX Score. Alert rules can be configured so that alerts are triggered when a preset threshold is reached for different types of events.

Administrators cannot only gain a high-level overview of ZDX alerts but can also review every detail on a per-alert basis through the ZDX Administrator Portal.

Alert Rules

Alert Rules form the foundation that ensures IT teams can prioritize alerts and quickly identify issues, which is achieved through the very granular end-to-end performance parameters made available through ZDX. This provides powerful rule and alerting capabilities that can differentiate between issues on a device, network, or application, with configurable thresholds around parameters like response time, device performance, network latency, or packet loss.

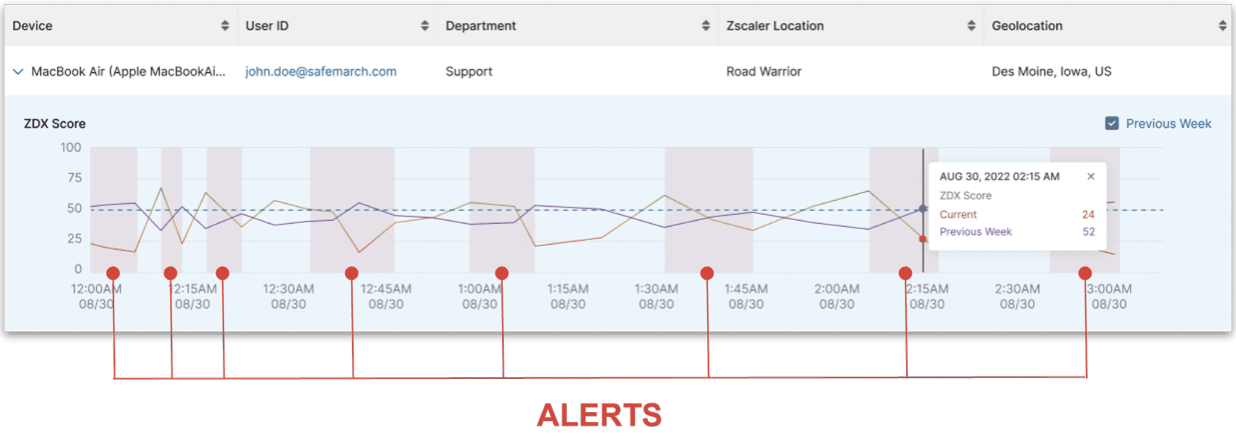
Defining an Alert Rule	An administrator will first determine what **type** of event will trigger an alert, which will inform the threshold criteria available later in the rule-definition process: **Application** Example parameters: DNS Time, Page Fetch Time, Server Response Time **Device** Example parameters: Bandwidth throughput, Battery, CPU and Memory utilization, WiFi signal Strength **Network** Example parameters: Latency, Packet Count, Number of Hops, Packet Loss
Add Filters	Regardless of rule type, granular filters can be applied to Locations, Location Groups, Zscaler Locations, Geolocations, Departments, User Groups, Users, and Devices.
Configure Criteria	For each available criteria, thresholds can be configured around these parameters for determining whether a rule will trigger, based on parameters being higher or lower than the desired value. Additionally,

	multiple criteria can be defined, where a rule can be configured to trigger only if **all** parameters match the defined criteria, or if **any** match the defined criteria. An example is a rule that may only trigger a high-severity alert if device CPU Utilization exceeds 90% **and** Packet Loss exceeds 10%.
Define Alerting Actions	Once the rule type, filters, and threshold criteria are configured, an administrator can define several alerting **actions**, when triggered, on a per-rule basis: **Muted:** No alerts will be sent via email or Webhook, but would be available in the ZDX Administrator portal **Email:** Sends details of an alert to a specific email address **Webhook:** Sends details of an alert to a third-party incident management application

Dynamic Alerts

Imagine a server located in the US is accessed by users in South America and users in the US. Because these users go through different paths, their "normal" ZDX Score will be different. Creating an alert based on a fixed ZDX Score threshold alone would not accurately reflect the different, yet acceptable user experience in these locations.

ZDX adaptively baselines ‘normal’ scores over time and accurately detects anomalies. Dynamic alerts are triggered based on the **deviations** from a baseline ZDX Score. This results in more meaningful alerts, less noise and simpler administration.

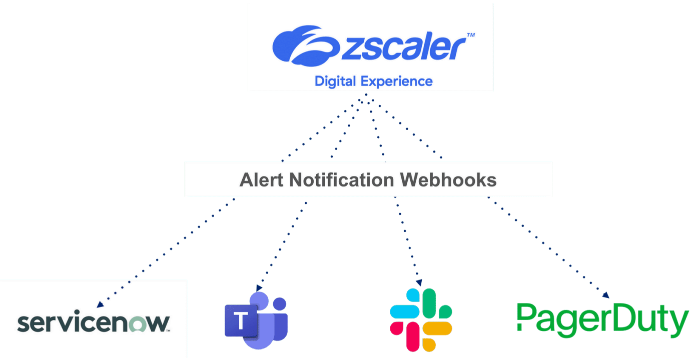


Device	User ID	Department	Zscaler Location	Geolocation
MacBook Air (Apple MacBookAi...	john.doe@safemarch.com	Support	Road Warrior	Des Moine, Iowa, US

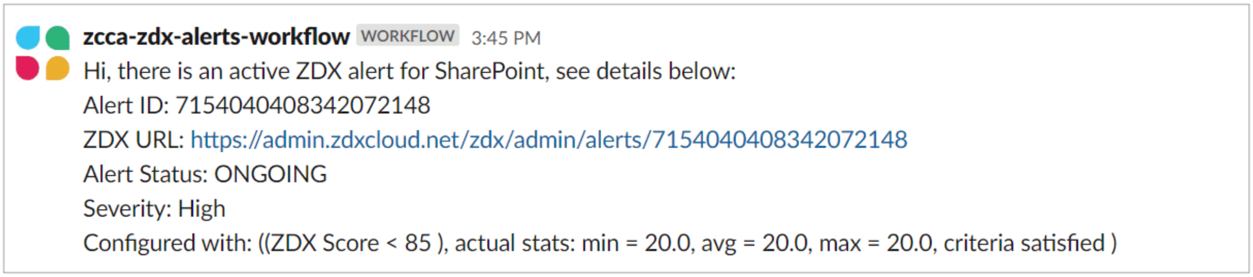
Red-shaded background on the graph identifies periods with threshold violations

Webhooks

Many IT teams handle incident management and internal communication within applications such as ServiceNow, Slack, and PagerDuty, and ZDX can, through Webhooks, deliver alerts directly into these applications.



For example, with a Webhook integration between ServiceNow and ZDX, a triggered rule in ZDX can result in a ServiceNow HelpDesk ticket being logged, while integration with Slack could message a specific Slack channel with details of an alert.


zcca-zdx-alerts-workflow WORKFLOW 3:45 PM

Hi, there is an active ZDX alert for SharePoint, see details below:

Alert ID: 7154040408342072148

ZDX URL: https://admin.zdxcloud.net/zdx/admin/alerts/7154040408342072148

Alert Status: ONGOING

Severity: High

Configured with: ((ZDX Score < 85), actual stats: min = 20.0, avg = 20.0, max = 20.0, criteria satisfied)

Integration is achieved by configuring the incident management application to receive alerts from ZDX and how to handle these alerts, which will generate an endpoint API and in some cases a security token. This information is copied into the ZDX Administrator Portal as a Webhook alert destination, and the Webhook is defined as an alert mechanism within a rule.

Alerts sent via a Webhook can contain information such as ZDX rule name, alert details URL, affected location, users, alert status, and alert severity, providing at-a-glance information per-alert, while providing the URL for quickly drilling into the details of an alert.

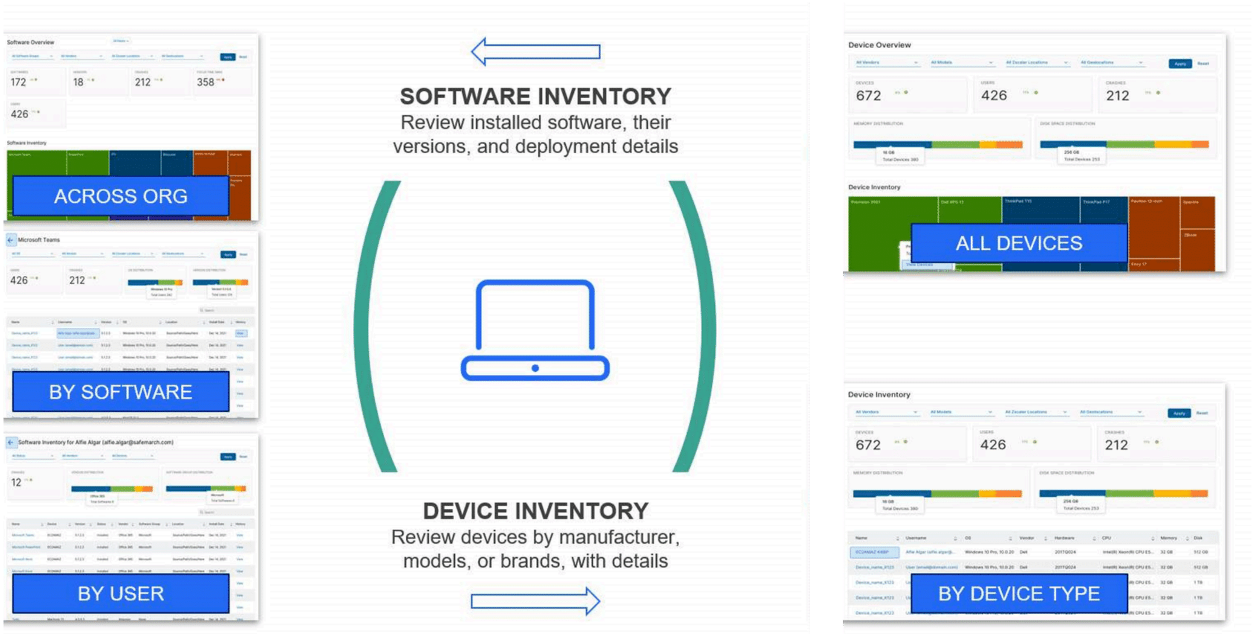
Device, Software & Process Inventory

A user’s computer/device performance plays a major role in user experience. It’s helpful to know if devices in the organization are running the latest OS, Patch or Software version. And understanding resources utilization allows you to profile devices that may need upgrades.

That's where ZDX Inventory Analytics comes in:

Software Inventory allows you to view current and historical information about software versions and updates on your users' devices.

Device Inventory allows you to view current information about your organization's devices and their associated users.



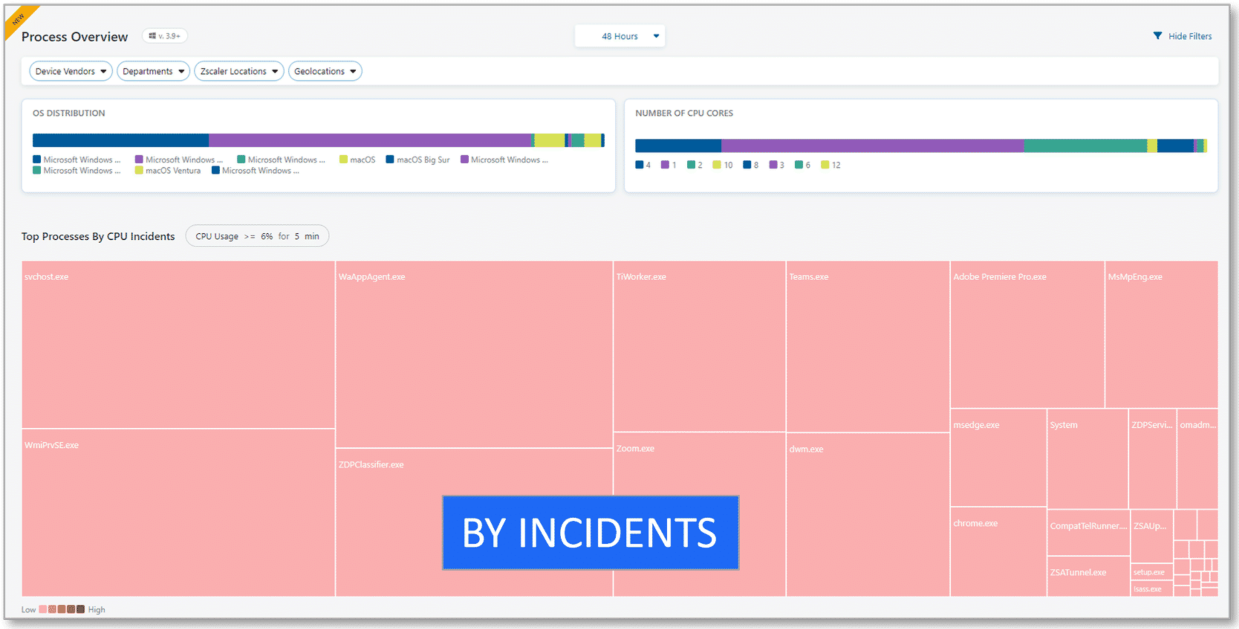
SOFTWARE INVENTORY
Review installed software, their versions, and deployment details

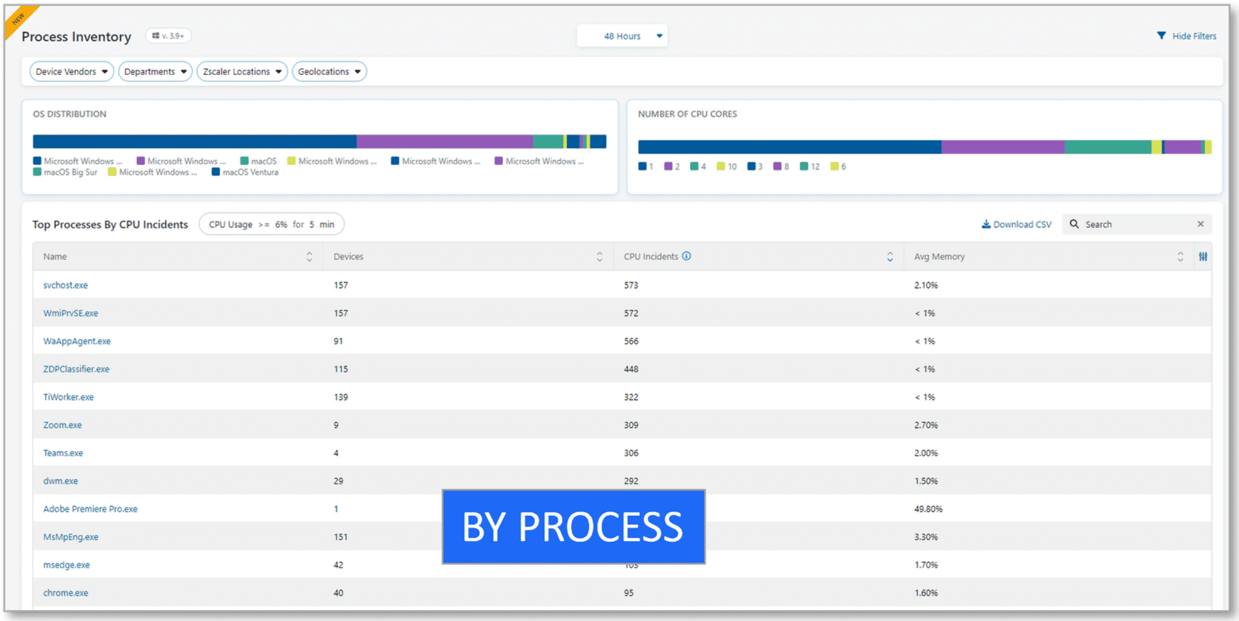
DEVICE INVENTORY
Review devices by manufacturer, models, or brands, with details

In addition to performance metrics, Client Connector can also collect information about an end user's hardware and software configuration.

—

The inventory data collected by Client Connector are organized into high-level overview graphs and detailed lists that provide user-specific insights.





Top Processes By CPU Incidents CPU Usage >= 6% for 5 min

Name	Devices	CPU Incidents	Avg Memory
svchost.exe	157	573	2.10%
WmiPrvSE.exe	157	572	< 1%
WaAppAgent.exe	91	566	< 1%
ZDPClassifier.exe	115	448	< 1%
TiWorker.exe	139	322	< 1%
Zoom.exe	9	309	2.70%
Teams.exe	4	306	2.00%
dwm.exe	29	292	1.50%
Adobe Premiere Pro.exe	1	[illegible]	49.80%
MsMpEng.exe	151	[illegible]	3.30%
msedge.exe	42	[illegible]	1.70%
chrome.exe	40	95	1.60%

Process Inventory

Process Inventory lets you monitor processes that might be impacting the behavior of your users' devices. Process calculations are updated in one-minute rolling intervals, and the top processes are displayed every five minutes.

Integration with Microsoft Intune

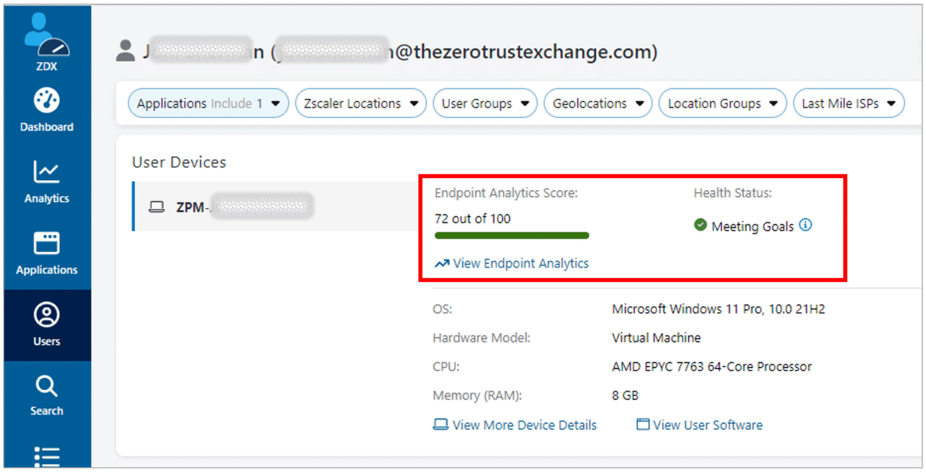
Microsoft Endpoint Analytics helps identify issues with user software or devices that might be impacting performance and reliability. Metrics pulled from the Microsoft Intune API are mapped to individual ZDX users and devices to provide Endpoint Analytics scores and data.

Through the integration with Intune, ZDX can provide deeper insights into the health and performance of end user devices. This allows ServiceDesk teams to review crash statistics, boot and startup times across Microsoft devices, and fix issues from within ZDX.

- **Startup Performance** lets you assess the health and performance of a user's device over time, based on Endpoint Analytics scores, boot and sign-in times, and processes that might affect device startup.

- **Software Reliability** can help identify potential problems with software and applications on user devices so you can troubleshoot the cause of the issues. The Software Reliability Score, history of software events, and details of those software events can collectively provide insight into the health status of individual devices.

The **User Details** page provides Endpoint Analytics information for a specified user device.



J[redacted]n ([redacted]@thezerotrustexchange.com)

User Devices

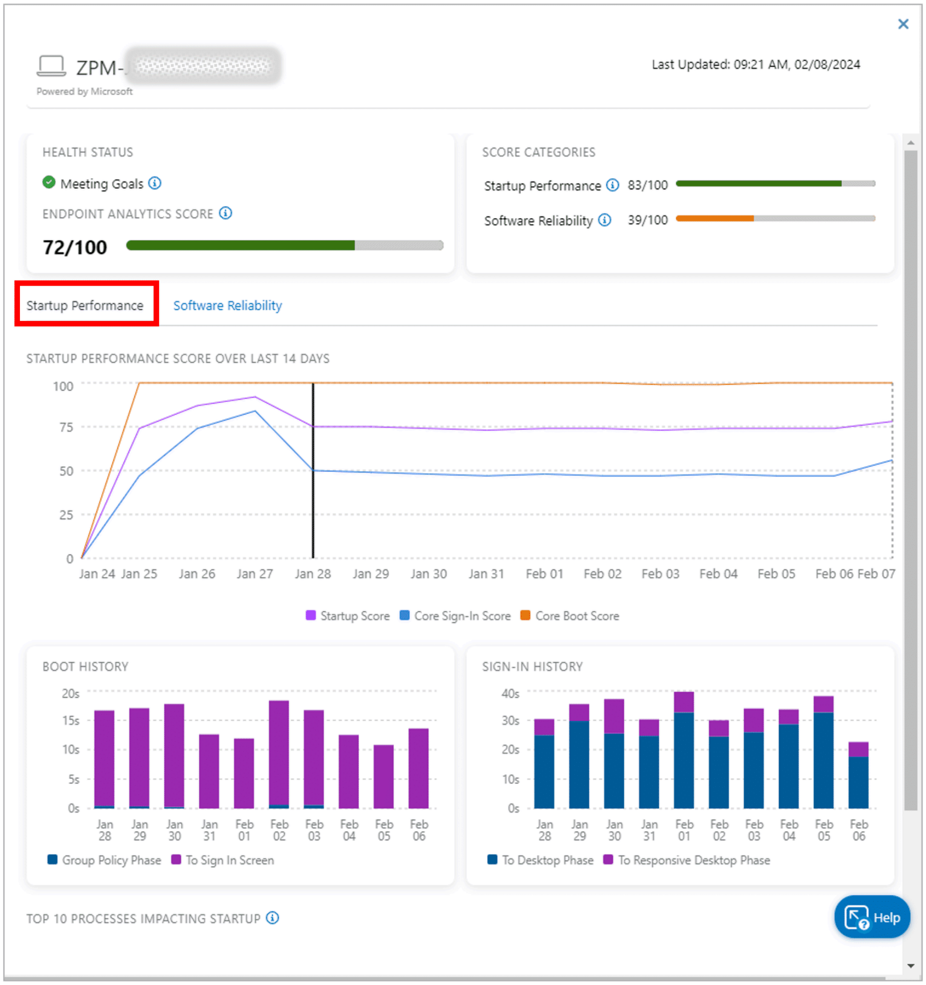
ZPM-[redacted]

Endpoint Analytics Score: 72 out of 100

Health Status: Meeting Goals

OS:	Microsoft Windows 11 Pro, 10.0 21H2
Hardware Model:	Virtual Machine
CPU:	AMD EPYC 7763 64-Core Processor
Memory (RAM):	8 GB

The **Startup Performance** tab shows the Health Status of the device, the Startup Performance, and other metrics.



ZPM-[redacted]

Powered by Microsoft

Last Updated: 09:21 AM, 02/08/2024

HEALTH STATUS

Meeting Goals ⓘ

ENDPOINT ANALYTICS SCORE ⓘ

72/100

SCORE CATEGORIES

Startup Performance ⓘ 83/100

Software Reliability ⓘ 39/100

Startup Performance | Software Reliability

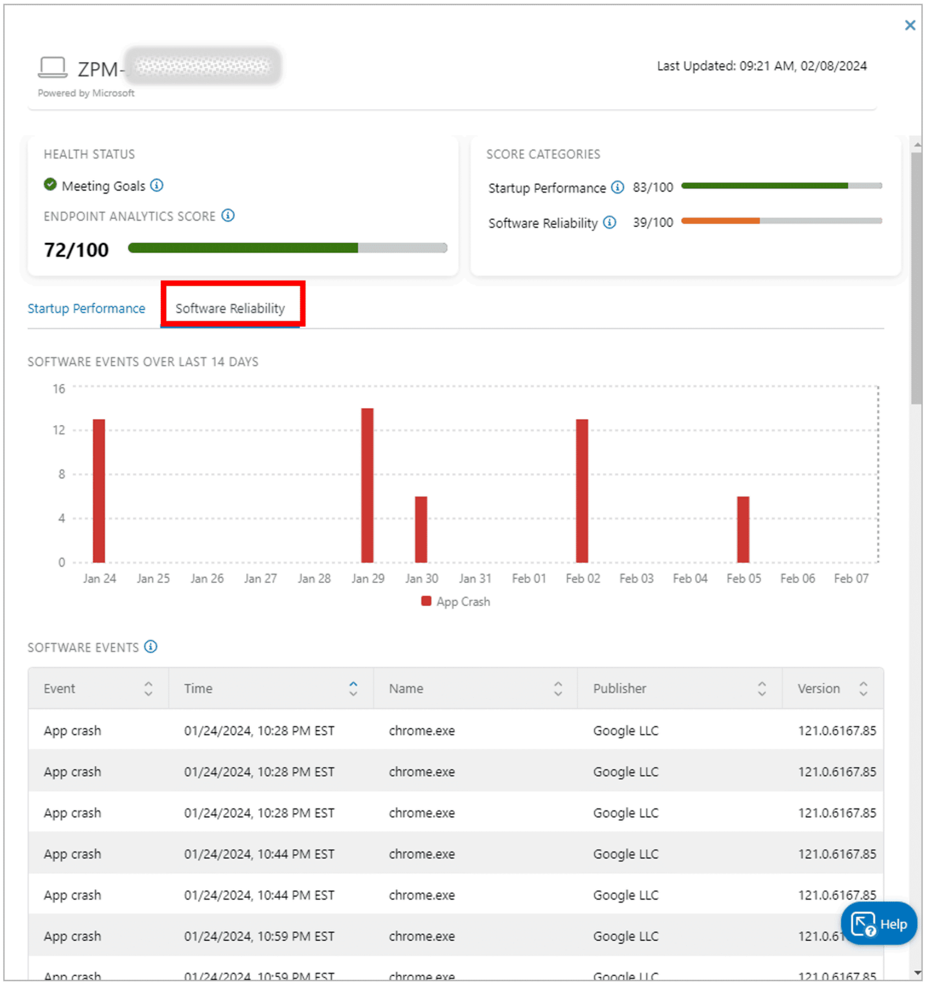
STARTUP PERFORMANCE SCORE OVER LAST 14 DAYS

BOOT HISTORY

SIGN-IN HISTORY

TOP 10 PROCESSES IMPACTING STARTUP ⓘ

The **Software Reliability** tab shows events like application crashes.



ZPM-[redacted]

Powered by Microsoft

Last Updated: 09:21 AM, 02/08/2024

HEALTH STATUS

Meeting Goals

ENDPOINT ANALYTICS SCORE

72/100

SCORE CATEGORIES

Startup Performance 83/100

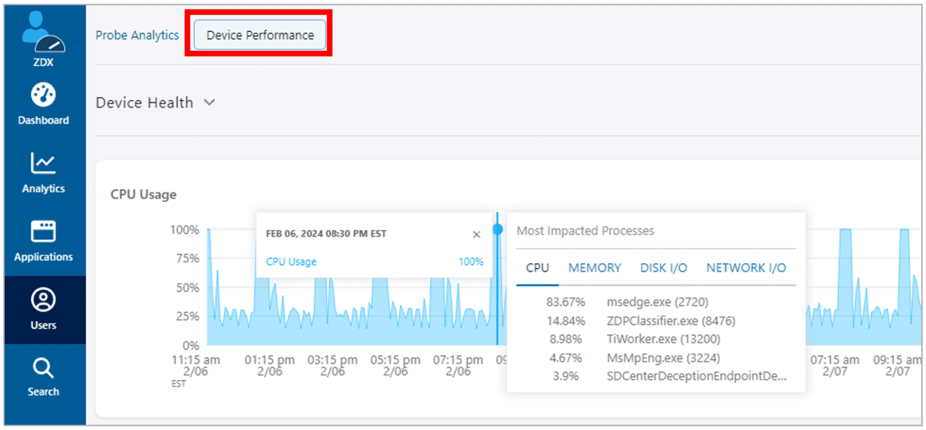
Software Reliability 39/100

SOFTWARE EVENTS OVER LAST 14 DAYS

SOFTWARE EVENTS

Event	Time	Name	Publisher	Version
App crash	01/24/2024, 10:28 PM EST	chrome.exe	Google LLC	121.0.6167.85
App crash	01/24/2024, 10:28 PM EST	chrome.exe	Google LLC	121.0.6167.85
App crash	01/24/2024, 10:28 PM EST	chrome.exe	Google LLC	121.0.6167.85
App crash	01/24/2024, 10:44 PM EST	chrome.exe	Google LLC	121.0.6167.85
App crash	01/24/2024, 10:44 PM EST	chrome.exe	Google LLC	121.0.6167.85
App crash	01/24/2024, 10:59 PM EST	chrome.exe	Google LLC	121.0.61
App crash	01/24/2024, 10:59 PM EST	chrome.exe	Google LLC	121.0.6167.85

You can also check the **Device Performance** section in a User Details page to get details of most impacted processes by CPU usage, memory utilization, disk and network I/O.



CPU Usage

FEB 06, 2024 08:30 PM EST

CPU Usage 100%

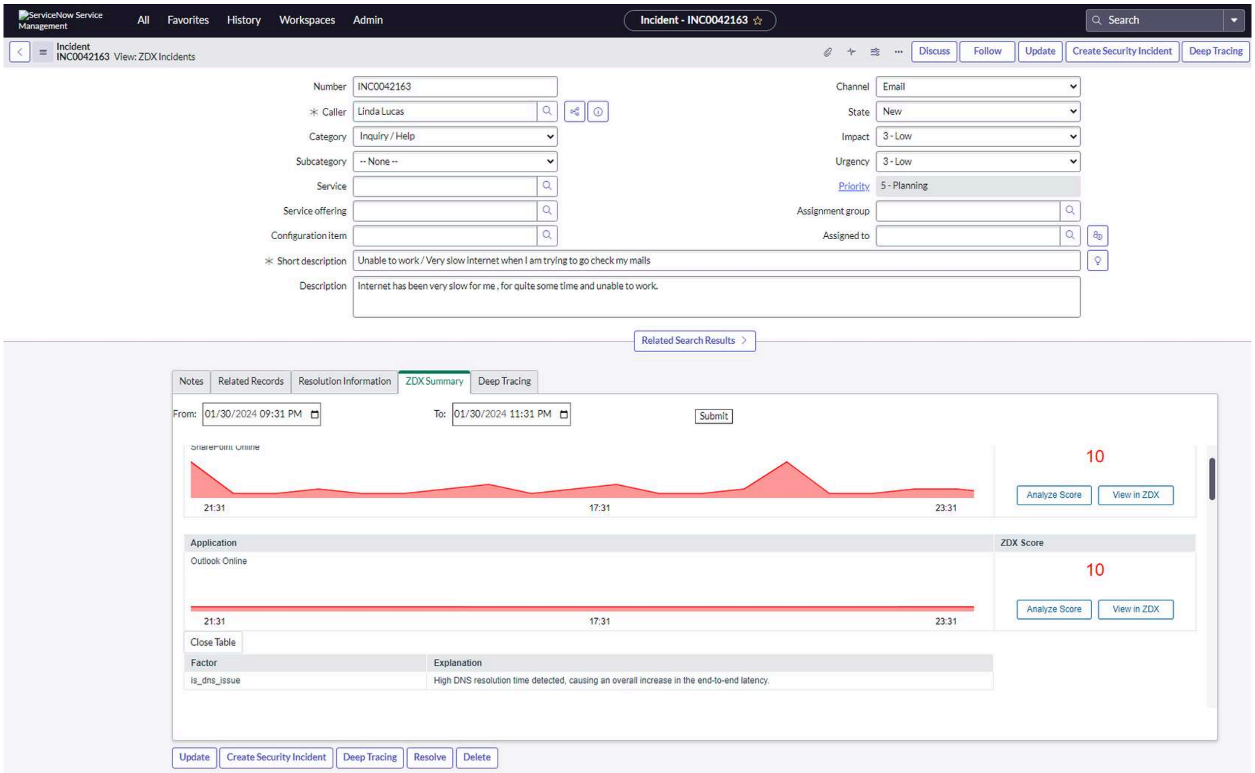
Most Impacted Processes

83.67%	msedge.exe (2720)
14.84%	ZDPClassifier.exe (8476)
8.98%	TiWorker.exe (13200)
4.67%	MsMpEng.exe (3224)
3.9%	SDCenterDeceptionEndpointDe...

Integration with ServiceNow

Switching between multiple tools slows down the work of ServiceDesk teams, which leads to longer MTTR. With the ServiceNow integration, ZDX alerts and metrics are available right in the ServiceNow console. ServiceDesk teams can also run Depp Tracing sessions and automated root cause analysis directly from ServiceNow, without having to switch to the ZDX Admin portal.

When ZDX detects an issue related to the end user device, application, or the underlying network infrastructure, API calls can forward the full alert details into ServiceNow, including impacted departments, geolocations, Zscaler locations, and users. With incidents consolidated in the ServiceNow dashboard, ServiceDesk staff can drill down into the incident's details provided by ZDX. This enables proactive incident management and simplifies the process of triaging and diagnosing the problem.



Number	INC0042163	Channel	Email
* Caller	Linda Lucas	State	New
Category	Inquiry / Help	Impact	3 - Low
Subcategory	-- None --	Urgency	3 - Low
Service		Priority	5 - Planning
Service offering		Assignment group	
Configuration item		Assigned to	
* Short description	Unable to work / Very slow internet when I am trying to go check my mails		
Description	Internet has been very slow for me , for quite some time and unable to work.		

From: 01/30/2024 09:31 PM To: 01/30/2024 11:31 PM

Application	ZDX Score
SharePoint Online	10
Outlook Online	10

Factor	Explanation
is_dns_issue	High DNS resolution time detected, causing an overall increase in the end-to-end latency.

With incidents consolidated in the ServiceNow dashboard, you can drill down into the incident's details provided by ZDX. Let's look at the most recent incident, and review basic ZDX-related data directly from within the ServiceNow console.

And the Alert Impact and Impacted Users tab provide the alert details, without needing to login to the ZDX Admin portal.

As the ServiceDesk analyst assigned to a ticket, you can click on the incident and then click on ZDX Summary, which shows application details for the user are populated right within the tab. From there you can launch a Y-Engine analysis by clicking Analyze Score, where you will see an explanation for what is causing the poor performance for Outlook Online for the user.

You can drill down even further and launch a deep tracing session for the user. Once that session completes, a hyperlink is available in the Deep Tracing tab, which takes you to the Deep Tracing results in the ZDX Admin portal.

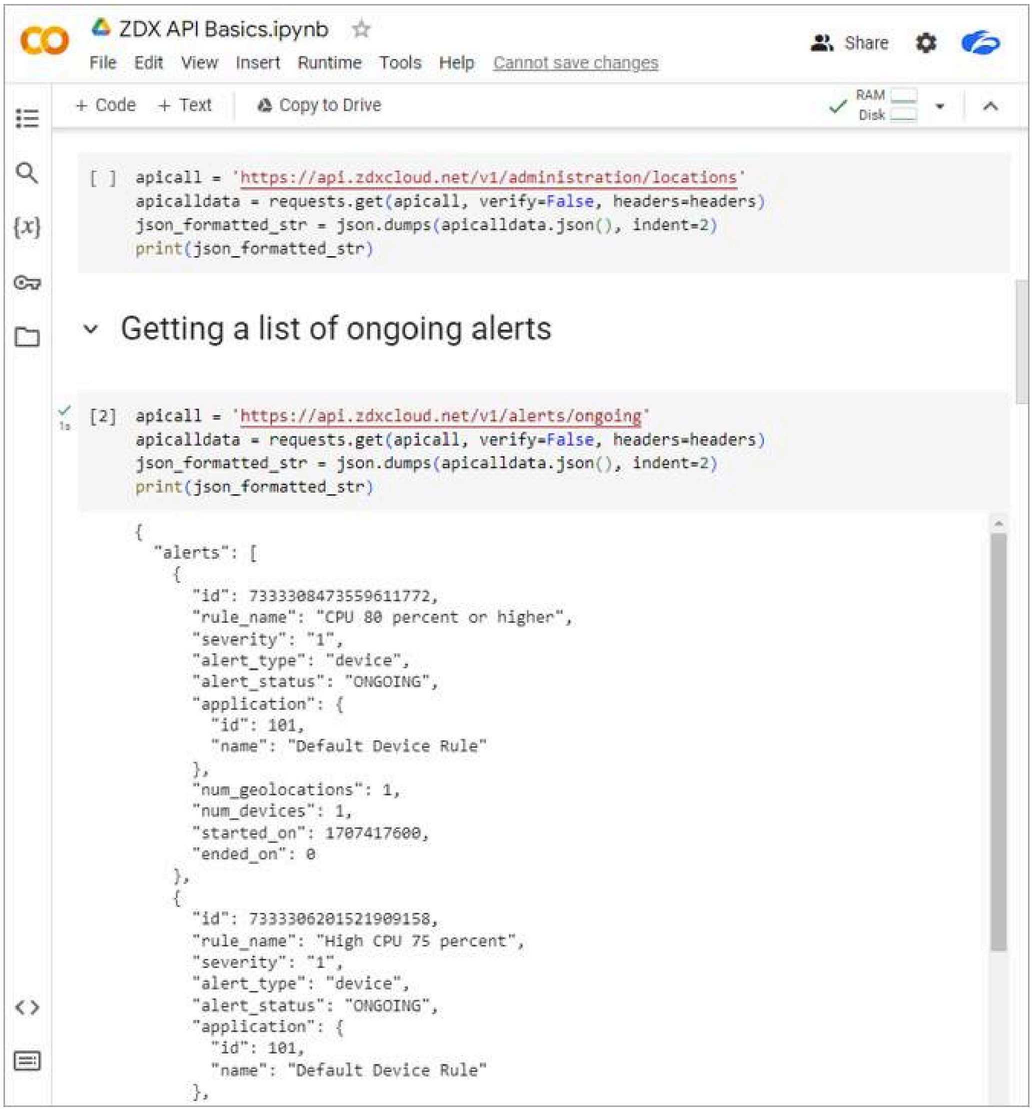
To recap, ServiceNow integrates with ZDX Alerting to provide near real-time alerts that are pushed to the ServiceNow Incident Management system and provides the ability to create Deep Tracing sessions right from the ServiceNow console.

ZDX API

The API gives you programmatic access to ZDX features. There are multiple API Endpoints available, such as Configuration, Reporting, and Troubleshooting endpoints.

Once you create an API key and an admin role in ZDX, you can use API calls to authenticate and pull ZDX data into some other system, for example your organization's business intelligence platform, an ITSM solution, a SIEM system or a developer tool like Postman. This data can then be processed further into enterprise-specific graphs, reports and dashboards. You can even use a POST call to run a Deep Tracing or start a ZDX Score analysis on a device for a specific application.

Example alert data


ZDX API Basics.ipynb
File Edit View Insert Runtime Tools Help Cannot save changes
Share
+ Code + Text Copy to Drive
RAM
Disk

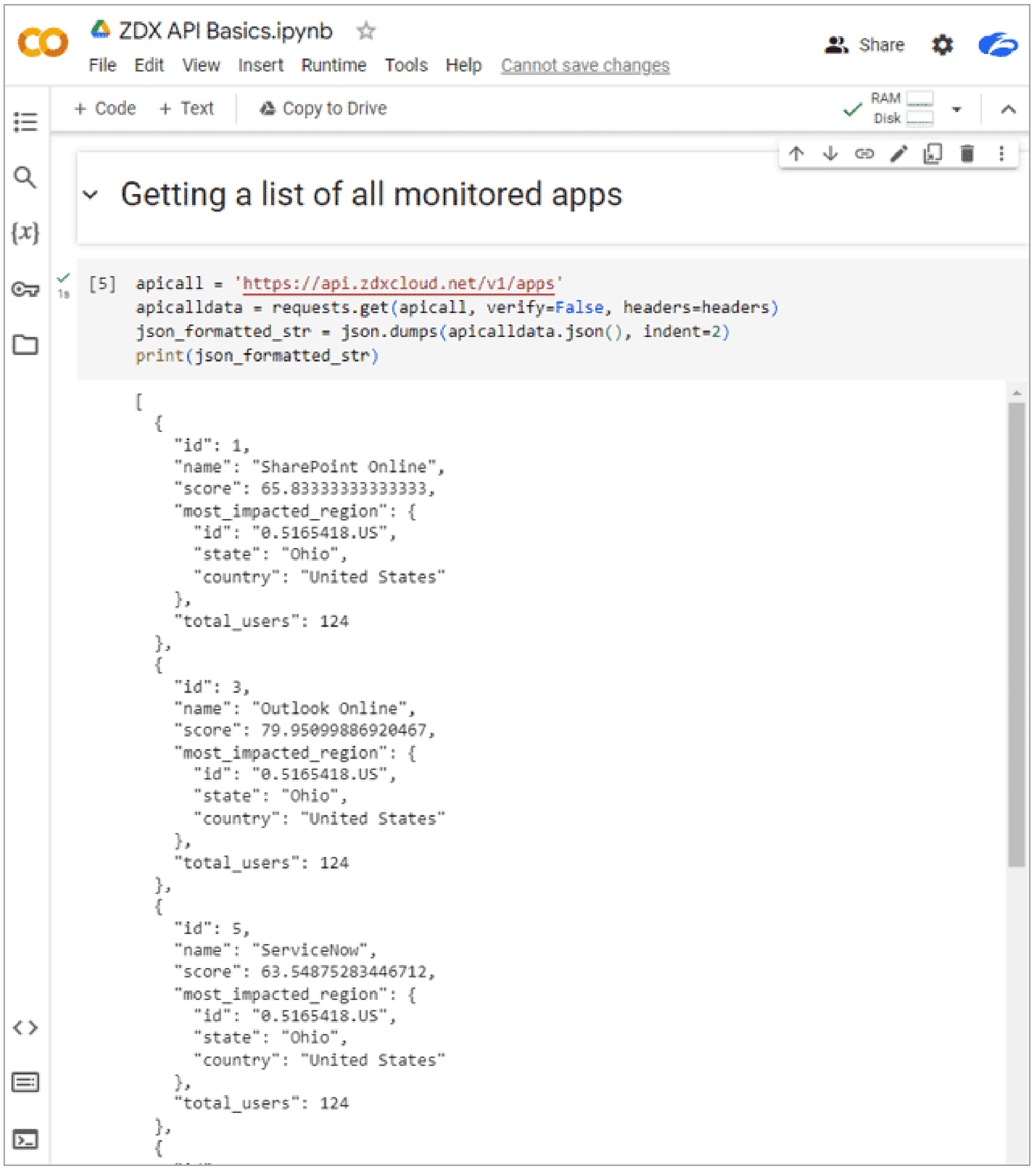
```
[ ] apicall = 'https://api.zdxcloud.net/v1/administration/locations'
    apicalldata = requests.get(apicall, verify=False, headers=headers)
    json_formatted_str = json.dumps(apicalldata.json(), indent=2)
    print(json_formatted_str)
```

Getting a list of ongoing alerts

```
[2] apicall = 'https://api.zdxcloud.net/v1/alerts/ongoing'
    apicalldata = requests.get(apicall, verify=False, headers=headers)
    json_formatted_str = json.dumps(apicalldata.json(), indent=2)
    print(json_formatted_str)
```

```
{
  "alerts": [
    {
      "id": 7333308473559611772,
      "rule_name": "CPU 80 percent or higher",
      "severity": "1",
      "alert_type": "device",
      "alert_status": "ONGOING",
      "application": {
        "id": 101,
        "name": "Default Device Rule"
      },
      "num_geolocations": 1,
      "num_devices": 1,
      "started_on": 1707417600,
      "ended_on": 0
    },
    {
      "id": 7333306201521909158,
      "rule_name": "High CPU 75 percent",
      "severity": "1",
      "alert_type": "device",
      "alert_status": "ONGOING",
      "application": {
        "id": 101,
        "name": "Default Device Rule"
      },
```

Example Application Data

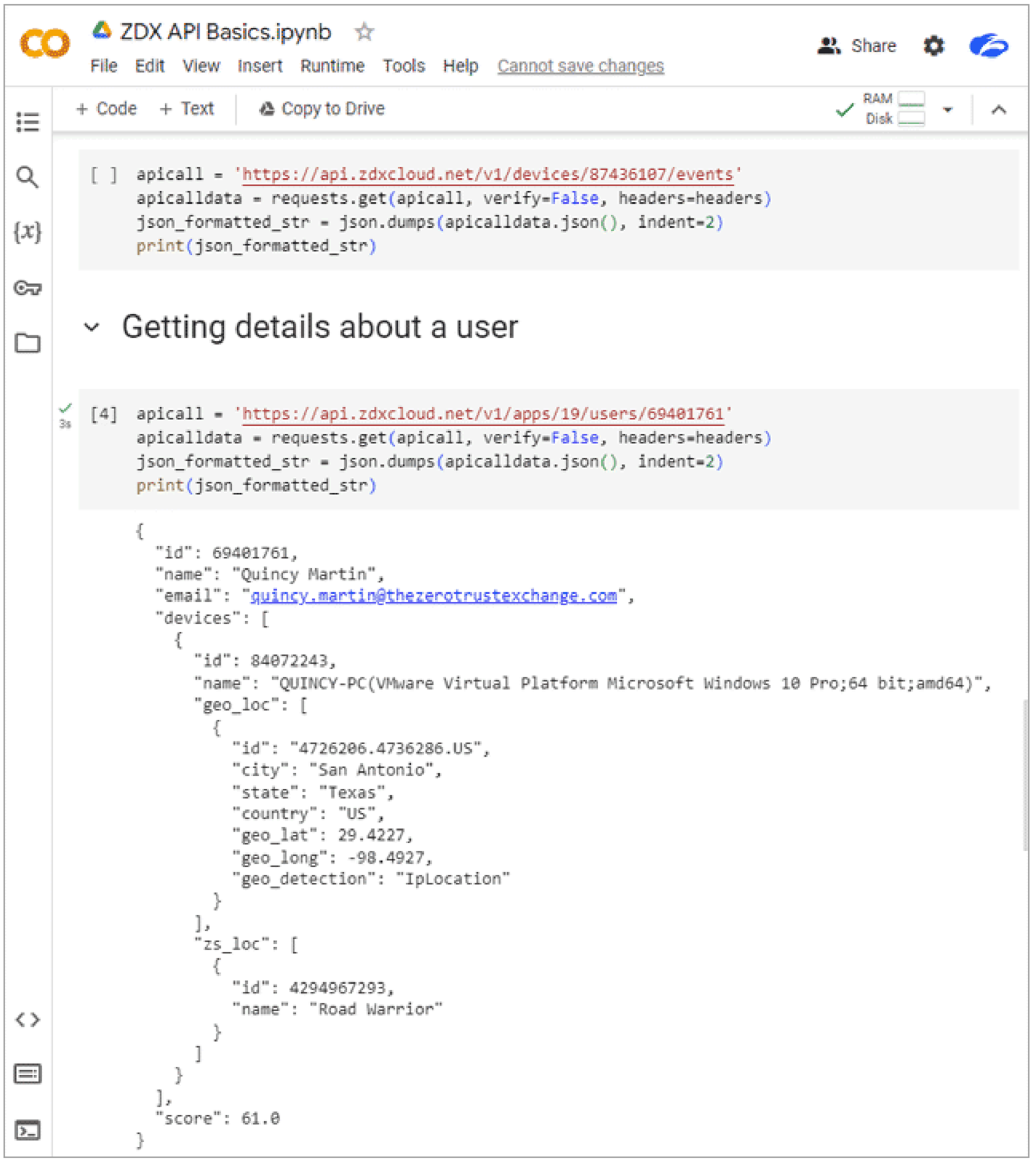


Getting a list of all monitored apps

```
[5] apicall = 'https://api.zdxcloud.net/v1/apps'
    apicalldata = requests.get(apicall, verify=False, headers=headers)
    json_formatted_str = json.dumps(apicalldata.json(), indent=2)
    print(json_formatted_str)
```

```
[
  {
    "id": 1,
    "name": "SharePoint Online",
    "score": 65.83333333333333,
    "most_impacted_region": {
      "id": "0.5165418.US",
      "state": "Ohio",
      "country": "United States"
    },
    "total_users": 124
  },
  {
    "id": 3,
    "name": "Outlook Online",
    "score": 79.95099886920467,
    "most_impacted_region": {
      "id": "0.5165418.US",
      "state": "Ohio",
      "country": "United States"
    },
    "total_users": 124
  },
  {
    "id": 5,
    "name": "ServiceNow",
    "score": 63.54875283446712,
    "most_impacted_region": {
      "id": "0.5165418.US",
      "state": "Ohio",
      "country": "United States"
    },
    "total_users": 124
  },
  {
```

Example User Details


ZDX API Basics.ipynb
File Edit View Insert Runtime Tools Help Cannot save changes
Share
+ Code + Text
Copy to Drive
RAM
Disk

```
[ ] apicall = 'https://api.zdxcloud.net/v1/devices/87436107/events'
    apicalldata = requests.get(apicall, verify=False, headers=headers)
    json_formatted_str = json.dumps(apicalldata.json(), indent=2)
    print(json_formatted_str)
```

Getting details about a user

```
[4] apicall = 'https://api.zdxcloud.net/v1/apps/19/users/69401761'
    apicalldata = requests.get(apicall, verify=False, headers=headers)
    json_formatted_str = json.dumps(apicalldata.json(), indent=2)
    print(json_formatted_str)
```

```
{
  "id": 69401761,
  "name": "Quincy Martin",
  "email": "quincy.martin@thezerotrustexchange.com",
  "devices": [
    {
      "id": 84072243,
      "name": "QUINCY-PC(VMware Virtual Platform Microsoft Windows 10 Pro;64 bit;amd64)",
      "geo_loc": [
        {
          "id": "4726206.4736286.US",
          "city": "San Antonio",
          "state": "Texas",
          "country": "US",
          "geo_lat": 29.4227,
          "geo_long": -98.4927,
          "geo_detection": "IpLocation"
        }
      ],
      "zs_loc": [
        {
          "id": 4294967293,
          "name": "Road Warrior"
        }
      ]
    }
  ],
  "score": 61.0
}
```

Role-Based Administration

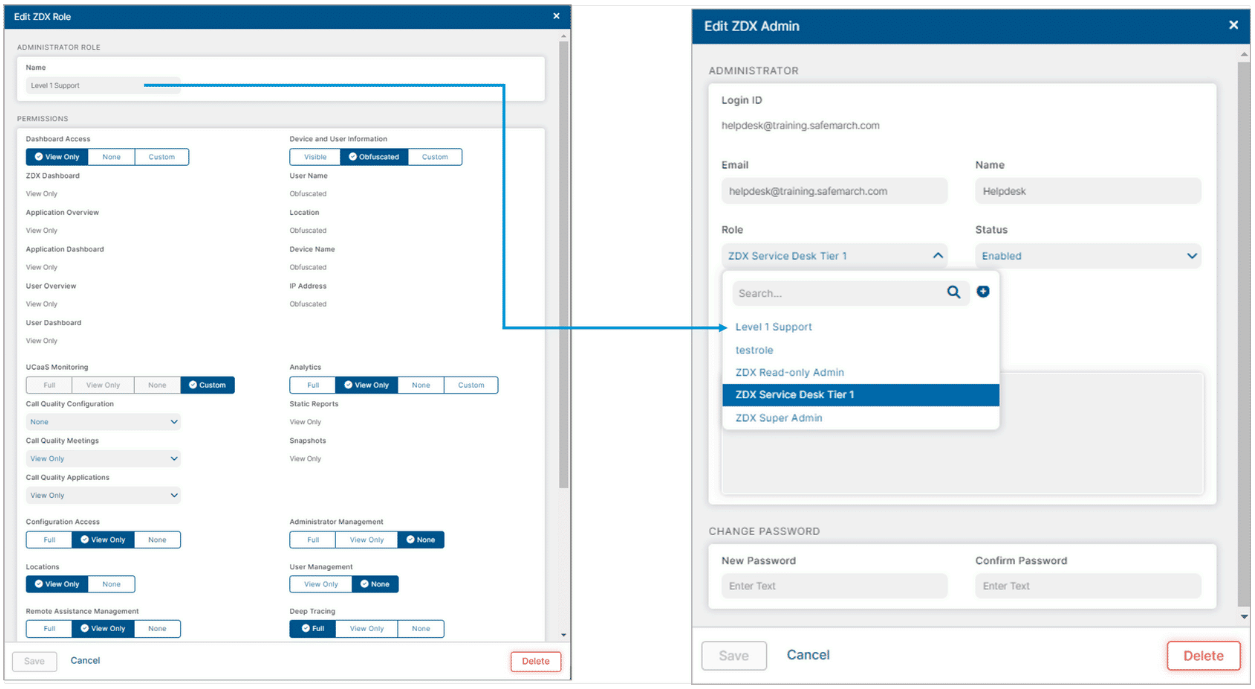
Role-Based Access Control

ZDX has been built with the understanding that multiple users and roles may need access to the ZDX Administrator Portal and that this access should be tailored to each administrator's needs and interests.

Role-Based Access Control (RBAC), otherwise known as Role-Based Administration, is a mechanism for granting not only access to different features within the ZDX Administrator Portal, but differentiating the level of access granted, i.e. read-write or read-only access per feature.

Areas of Access

As an example, access can be granted to areas of the Administrator Portal such as **Dashboard Access, UCaaS Monitoring, Configuration Access, Administrator Management, Deep Tracing, Alerts, Webhooks,** and many others. In each of these areas, granular control can be granted as **Full** (read-write access), **View Only, Custom** and **None**. Additionally, for roles where exposing user and device details may present a privacy concern, this information can be obfuscated.



Edit ZDX Role

ADMINISTRATOR ROLE

Name: Level 1 Support

PERMISSIONS

Dashboard Access: [✓ View Only] None Custom
- ZDX Dashboard: View Only
- Application Overview: View Only
- Application Dashboard: View Only
- User Overview: View Only
- User Dashboard: View Only

Device and User Information: Visible [✓ Obfuscated] Custom
- User Name: Obfuscated
- Location: Obfuscated
- Device Name: Obfuscated
- IP Address: Obfuscated

UCaaS Monitoring: Full View Only None [✓ Custom]
- Call Quality Configuration: None
- Call Quality Meetings: View Only
- Call Quality Applications: View Only

Analytics: Full [✓ View Only] None Custom
- Static Reports: View Only
- Snapshots: View Only

Configuration Access: Full [✓ View Only] None

Administrator Management: Full View Only [✓ None]

Locations: [✓ View Only] None

User Management: View Only [✓ None]

Remote Assistance Management: Full [✓ View Only] None

Deep Tracing: [✓ Full] View Only None

Edit ZDX Admin

ADMINISTRATOR

Login ID: helpdesk@training.safemarch.com

Email: helpdesk@training.safemarch.com

Name: Helpdesk

Role: ZDX Service Desk Tier 1

Status: Enabled

CHANGE PASSWORD

New Password: Enter Text

Confirm Password: Enter Text

Identity Provider Integration

ZDX supports two authentication methods for granting administrator access to the ZDX Administrator Portal:

1. Admin users are manually provisioned in the ZDX Administrator Portal with their email address and a secure password.

2. Admin users are added to the ZDX Administrator Portal with authentication handled by an organization's Identity Provider (IdP), also known as Single Sign-On (SSO). Common Identity Providers include Azure AD, ADFS, Okta, etc.

Single Sign On (SSO) for Administration

Administrator integration with an organization's SSO solution can be quickly configured, prevents management of multiple credentials, supports two-factor authentication, and improves the administrator experience.

ZDX Administrator integration with an SSO leverages Identity Provider (IdP)-initiated SAML, where the SSO solution is configured with Zscaler's SAML certificate and authentication endpoint. Once configured, all user authentication occurs by clicking the ZDX Administrator Portal icon or link in the SSO user portal, and as the user is already authenticated with the SSO solution, authentication into the ZDX Administrator Portal will be seamless, with no need to re-enter or maintain a separate set of credentials.

Audit Logs

Whether auditing access for compliance or having a need to revert a configuration to a prior state, the ZDX Administrator Portal provides exclusive insight into all administrator actions, providing a digital trail of who did what and when.

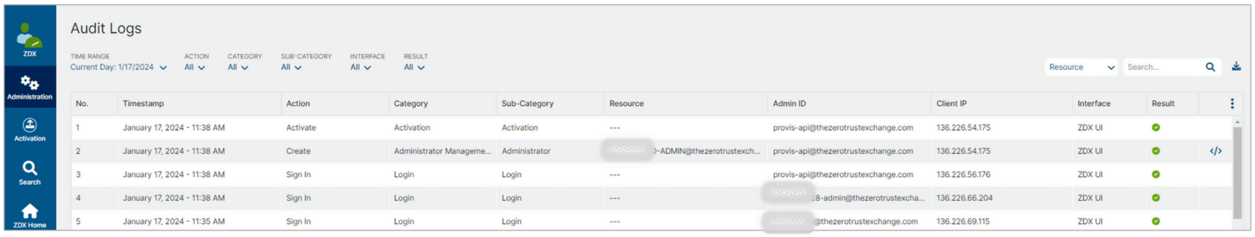
Audit Log Functionality

At its highest level, the Audit Logs functionality logs the username and IP address of every administrator. This includes both their successful and unsuccessful login attempts, any configuration changes made once logged in, which can be filtered in several useful ways, such as:

- **Time Range:** Filter logs to only display administrator actions that occur within a specific period of time
- **Action:** Logs shown can be the result of a Create, Update, or Delete action

- **Category:** Logs with changes in specific sections of the ZDX Administrator Portal like Alert, Configuration, Administrator Management, Role Management etc.
- **Sub-Category:** Feature specific logging filters, e.g. differentiate logs shown between Probe and Application changes in the Configuration category
- **Admin ID:** The user responsible for the logged event

Additionally, any change in configuration is logged, with Audit Logs providing a side-by-side Pre-Configuration/Post-Configuration view, so that any change can be quickly identified.



Audit Logs

TIME RANGE: Current Day: 1/17/2024 · ACTION: All · CATEGORY: All · SUB-CATEGORY: All · INTERFACE: All · RESULT: All

Resource · Search...

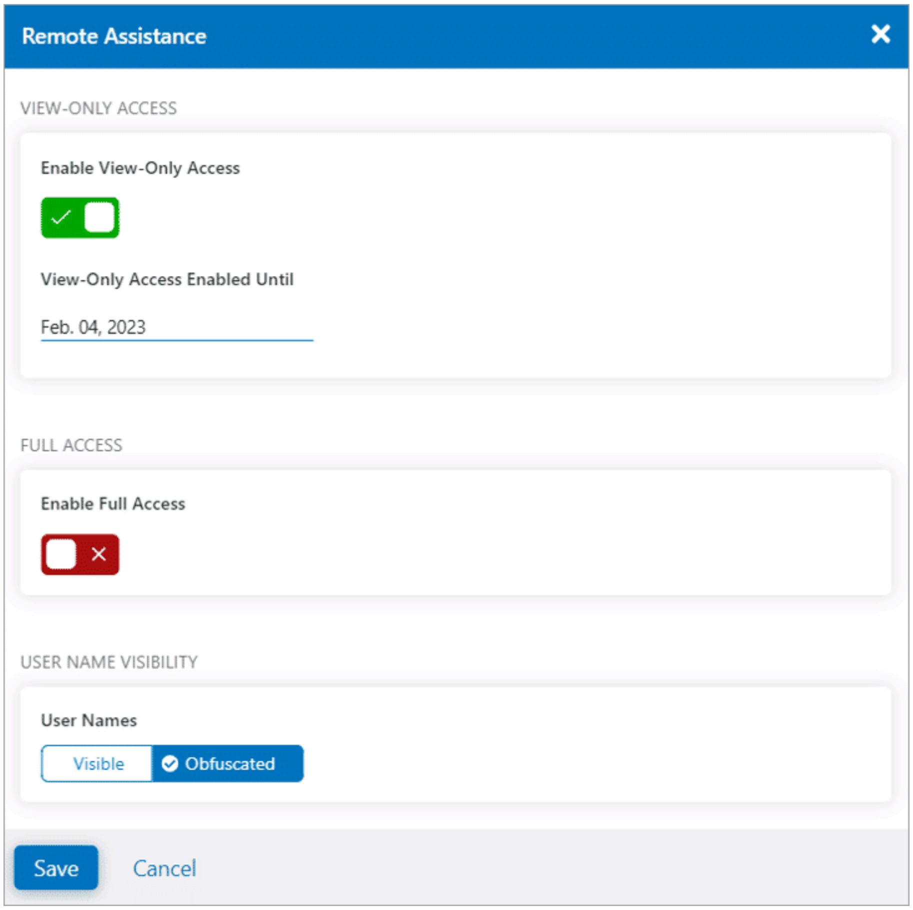
No.	Timestamp	Action	Category	Sub-Category	Resource	Admin ID	Client IP	Interface	Result	
1	January 17, 2024 - 11:38 AM	Activate	Activation	Activation	---	provis-api@thezerotrustexchange.com	136.226.54.175	ZDX UI	✓	
2	January 17, 2024 - 11:38 AM	Create	Administrator Manageme...	Administrator	[redacted]-ADMIN@thezerotrustexch...	provis-api@thezerotrustexchange.com	136.226.54.175	ZDX UI	✓	</>
3	January 17, 2024 - 11:38 AM	Sign In	Login	Login	---	provis-api@thezerotrustexchange.com	136.226.56.176	ZDX UI	✓	
4	January 17, 2024 - 11:38 AM	Sign In	Login	Login	---	[redacted]8-admin@thezerotrustexcha...	136.226.66.204	ZDX UI	✓	
5	January 17, 2024 - 11:35 AM	Sign In	Login	Login	---	[redacted]@thezerotrustexchange.com	136.226.69.115	ZDX UI	✓	

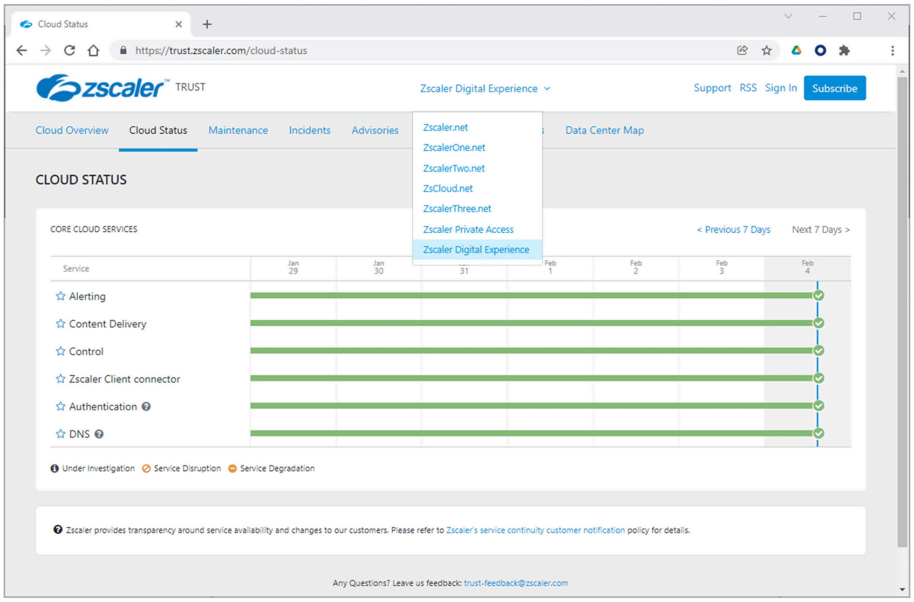
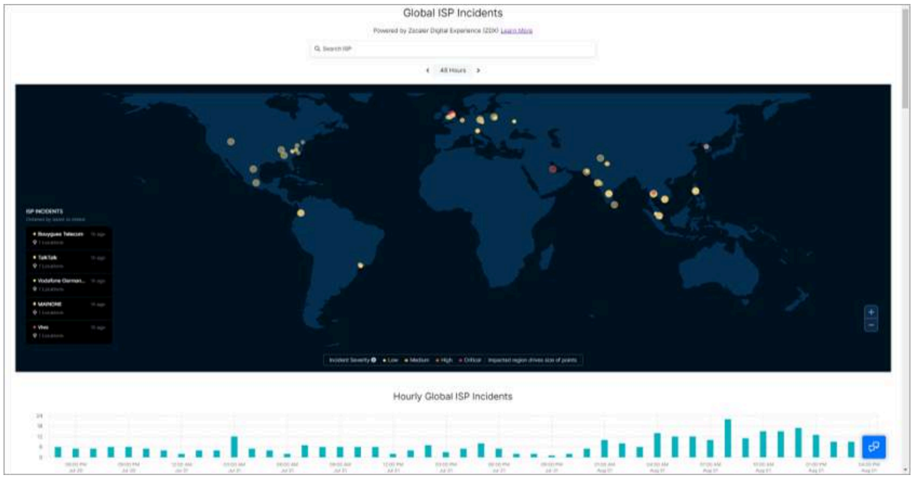
Getting Help from Zscaler

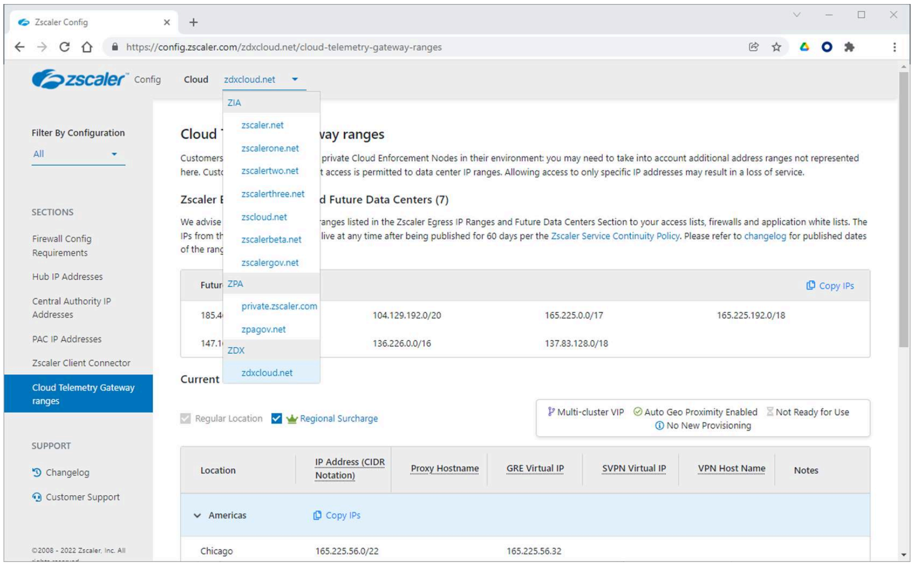
Need more information about the details of a dashboard, or a reminder on how to configure alert rules? No problem, the ZDX Online Help documentation is just a mouse click away!

In the ZDX Administrator Portal, click the ? menu, and then select **Zscaler Help Portal**. Or, go directly to the Help Portal at https://help.zscaler.com.

Remote Assistance	The **Remote Assistance** option on the ZDX Administrator Portal **?** menu allows Zscaler Support to review or even adjust your configurations. You may be asked by Zscaler Support to enable Remote Assistance to allow them either: ● **View-only Access** to simply review your connectivity or policy settings as part of their troubleshooting process ● **Full Access** to give them the ability to change settings. When enabling remote assistance, you must also specify the date that it will expire by, which prevents your system being accessed by Zscaler Support beyond that date.

	 Remote Assistance VIEW-ONLY ACCESS Enable View-Only Access: ✓ View-Only Access Enabled Until Feb. 04, 2023 FULL ACCESS Enable Full Access: ✕ USER NAME VISIBILITY User Names Visible ● Obfuscated Save Cancel
Cloud Trust Pages	The Trust Pages provide an indication of the current status of each of the Clouds and shows availability over time. This page is accessible either from the Help Portal, or at **https://trust.zscaler.com**. Make sure that you select the **Zscaler Digital Experience** cloud from the dropdown list at the top of the page. On this page, Zscaler posts notices for all scheduled maintenance, any recent incidents, security advisories and more. The Trust pages should be one of the first places to check if you suspect an issue may be Zscaler-related.

	 Cloud Status https://trust.zscaler.com/cloud-status zscaler TRUST Zscaler Digital Experience Support RSS Sign In Subscribe Cloud Overview Cloud Status Maintenance Incidents Advisories Data Center Map Zscaler.net ZscalerOne.net ZscalerTwo.net ZsCloud.net ZscalerThree.net Zscaler Private Access Zscaler Digital Experience CLOUD STATUS CORE CLOUD SERVICES < Previous 7 Days Next 7 Days > Service: Jan 29, Jan 30, Jan 31, Feb 1, Feb 2, Feb 3, Feb 4 ☆ Alerting ☆ Content Delivery ☆ Control ☆ Zscaler Client connector ☆ Authentication ☆ DNS Under Investigation · Service Disruption · Service Degradation Zscaler provides transparency around service availability and changes to our customers. Please refer to Zscaler's service continuity customer notification policy for details. Any Questions? Leave us feedback: trust-feedback@zscaler.com
Global ISP Incidents Dashboard	The Global ISP Incidents Dashboard is available at: **https://www.zscaler.com/threatlabz/global-isp-incidents**. The dashboard lets you review the health of the internet in real time. You can instantly see ISP incidents mapped by severity around the world.  Global ISP Incidents Powered by Zscaler Digital Experience (ZDX) Learn More Search ISP 48 Hours ISP INCIDENTS Bouygues Telecom TalkTalk Vodafone German... MAINONE Vivo 1 Locations Incident Severity Low Medium High Critical Impacted region drives size of points Hourly Global ISP Incidents 24 18 12 6 0
Cloud Configuration Pages	The Cloud Configuration Requirements pages accessible from the Help Portal Tools page, or at **https://config.zscaler.com**, provide reference data that is most useful during the implementation phase of your ZDX service. However, it can also be used as a reference when troubleshooting, to confirm that settings are correct.

<table>
<tr>
<td></td>
<td>


Cloud
…way ranges

Customers … private Cloud Enforcement Nodes in their environment: you may need to take into account additional address ranges not represented here. Custo… t access is permitted to data center IP ranges. Allowing access to only specific IP addresses may result in a loss of service.

Zscaler E… d Future Data Centers (7)

We advise … ranges listed in the Zscaler Egress IP Ranges and Future Data Centers Section to your access lists, firewalls and application white lists. The IPs from th… live at any time after being published for 60 days per the Zscaler Service Continuity Policy. Please refer to changelog for published dates of the rang…

Futur… Copy IPs
185.4… 104.129.192.0/20 165.225.0.0/17 165.225.192.0/18
147.1… 136.226.0.0/16 137.83.128.0/18

Current

☑ Regular Location ☑ Regional Surcharge

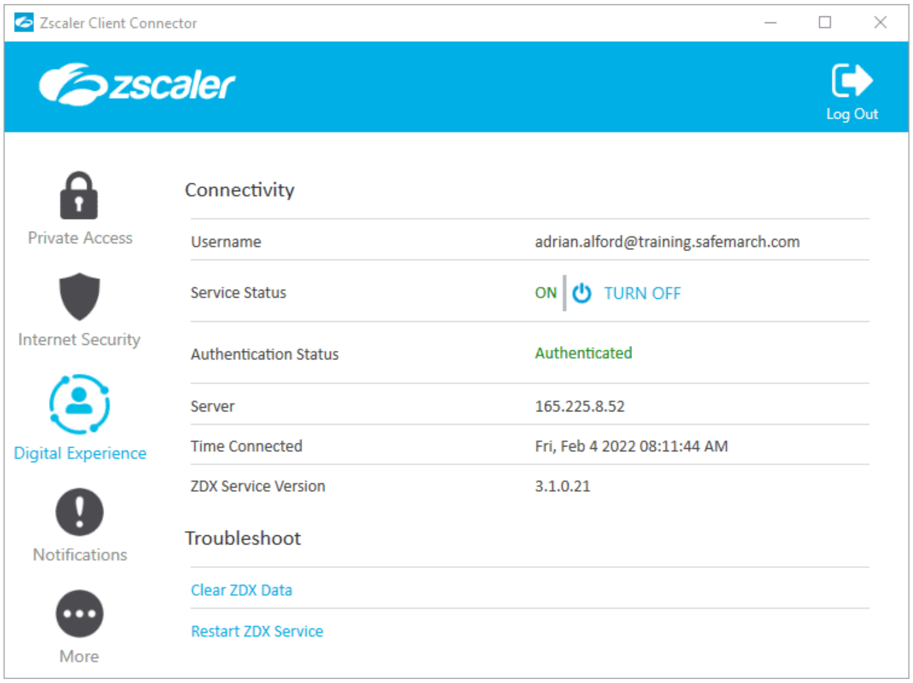
Multi-cluster VIP ✓ Auto Geo Proximity Enabled Not Ready for Use ⓘ No New Provisioning

Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	SVPN Virtual IP	VPN Host Name	Notes
Americas	Copy IPs					
Chicago	165.225.56.0/22		165.225.56.32			
</td>
</tr>
<tr>
<td><b>Client Connector</b></td>
<td>

The **Digital Experience** tab on the Client Connector provides information about ZDX connectivity and authentication status.

For basic troubleshooting, you can ask a user to:

- **Clear ZDX Data**: Click to clear the ZDX data that Zscaler Client Connector stored
- **Restart ZDX Service:** Click to restart the ZDX service



Connectivity

Username	adrian.alford@training.safemarch.com
Service Status	ON TURN OFF
Authentication Status	Authenticated
Server	165.225.8.52
Time Connected	Fri, Feb 4 2022 08:11:44 AM
ZDX Service Version	3.1.0.21

Troubleshoot

Clear ZDX Data

Restart ZDX Service
</td>
</tr>
</table>

MONITORING WITH ZDX

ZDX Dashboard

The Admin Portal's Dashboard menu function provides access to the following ZDX Dashboards:

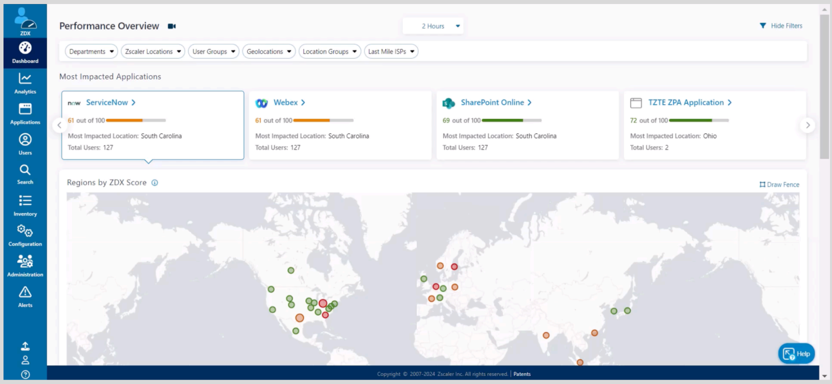
- **Performance Overview** shows an overview of the application performance and user experience for your organization.
- **Incidents Overview** displays information about issues that impact the device performance of multiple users.
- **Self Service Overview** displays an overview of data pulled from user notifications.

ZDX Dashboard: Performance Overview

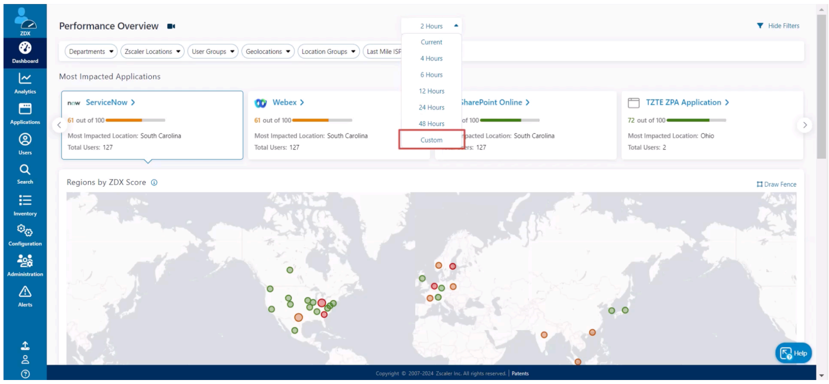
Gaining an overview of application performance and user experience allows you to easily and quickly detect performance issues. Within this dashboard, you will find the following widgets and graphs to help in identifying issues: Most Impacted Applications, Regions by ZDX Score Map, ZDX Score Graph, and Page Fetch Time Graph.

Scores are all relative and making sense of the values is a bit of an art, rather than an exact science. For example, a low ZDX Score for a user on a slow satellite link may be normal because of high Page Fetch Time. Careful interpretation of these values is key! Look for significant score changes, rather than absolute values.

The ZDX dashboard provides an overview of the application performance and user experience for your organization. Think of this dashboard as a thirty thousand foot overview of how your organization's applications are performing. Along the top of this page, there are several filters to zero in on issues reported by users.

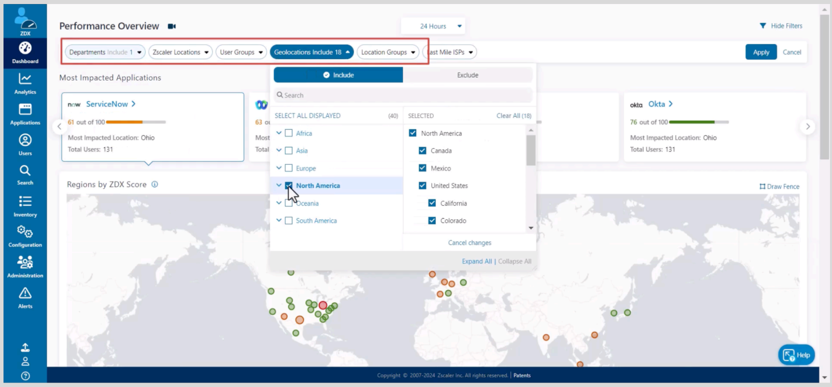


First, there is the time range filter. This can be used to view performance data over a period between 2 and 48 hours for the advanced ZDX plan, or for between 2 and 24 hours for the standard plan. You can also specify a custom time frame. The current option allows you to view the previous thirty minutes captured in the ZDX score.



The available options under the departments, Zscaler locations, user groups, location groups, last mile ISPs, and geolocations filters represent your organization's departments and office locations as they are defined in your ZIA tenant.

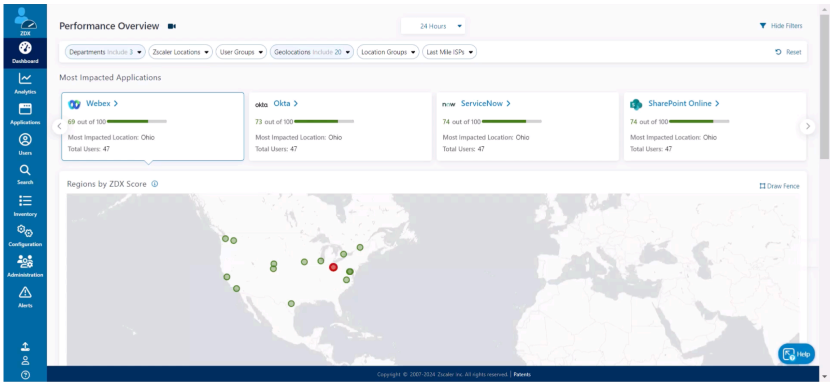
Active geo-locations represent the cities where users are located based on user device longitude and latitude information.



Then apply these filters to update the dashboard view.

You'll see that each application displays the following:

The **ZDX score**, which represents the total experience of all users in your organization for all locations during the selected time period. The score is based on a scale of one to one hundred.



Performance Overview

24 Hours

Departments Include 3 · Zscaler Locations · User Groups · Geolocations Include 20 · Location Groups · Last Mile ISPs

Most Impacted Applications

Webex	Okta	ServiceNow	SharePoint Online
69 out of 100	73 out of 100	74 out of 100	74 out of 100
Most Impacted Location: Ohio	Most Impacted Location: Ohio	Most Impacted Location: Ohio	Most Impacted Location: Ohio
Total Users: 47	Total Users: 47	Total Users: 47	Total Users: 47

Regions by ZDX Score

Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

Most impacted location, which is the location with the worst digital experience for that application during the selected time period. And the **number of users** during the selected time period.

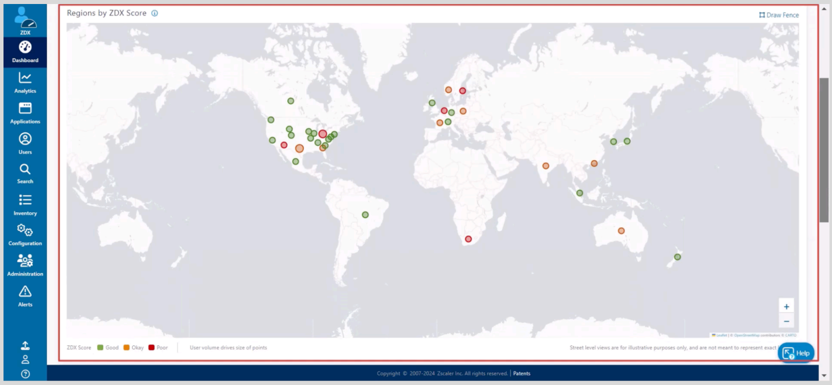
Since the Zscaler Client Connector uses synthetic probes, they are sent out as long as the user devices are active. There is no need for a user to actually interact with an application for probes to be sent.

You can use the navigation buttons to scroll left or right to see more applications.

And if needed, you can adjust the filters or remove all of them by clicking reset.

The regions by ZDX score widget displays a map with the locations for all users for the selected application.

You can zoom in or out of the map to better view regions that you're interested in.



Regions by ZDX Score

ZDX Score 🟩 Good 🟧 Okay 🟥 Poor | User volume drives size of points

Street level views are for illustrative purposes only, and are not meant to represent exact

Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

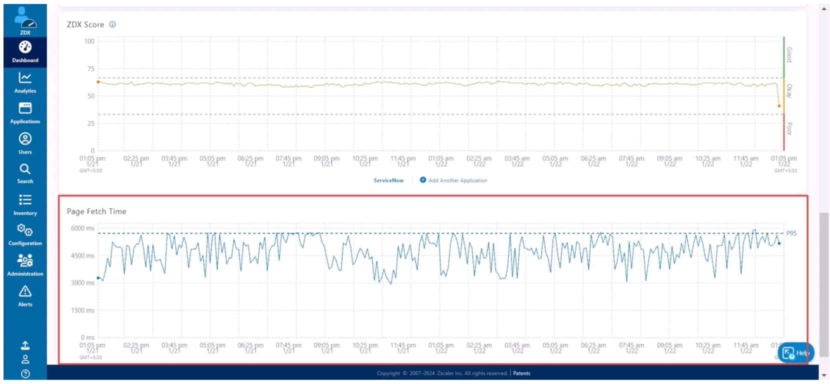
For example, tech support can use this map to quickly identify a regional outage of an application by zooming in on the map. Having this overview helps identify a problem before a bunch of support tickets from users come in.

You can also zero in on a specific region by drawing a fence around an area on the map.

When you scroll down you'll see a couple of ZDX dashboard graphs.

The ZDX score graph shows how the ZDX score changed over the selected time period.

And the page fetch time graph tracks how long it takes the selected application to transfer the fetched page to users.



Page fetch time, or PFT, for short, is the single most important metric when determining a user's experience when using a web application. Because a poor PFT can ruin their experience even when all other metrics look good.

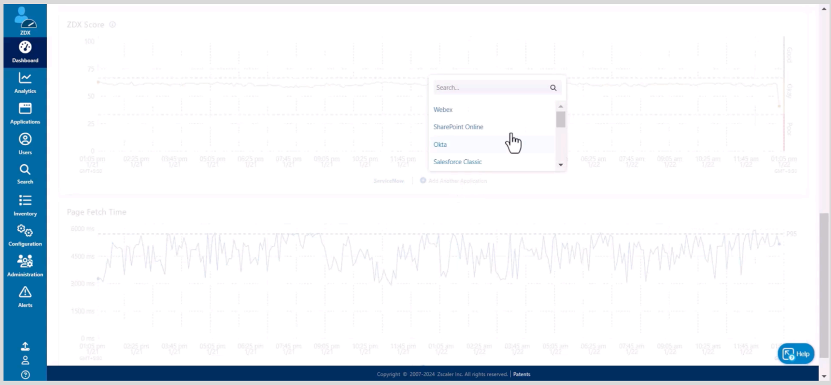
Also, notice a line that runs across the graph as identified by P95. This indicates the ninety fifth percentile as calculated for the page fetch time. While the actual PFT curve represents the average for all users at that point in time.

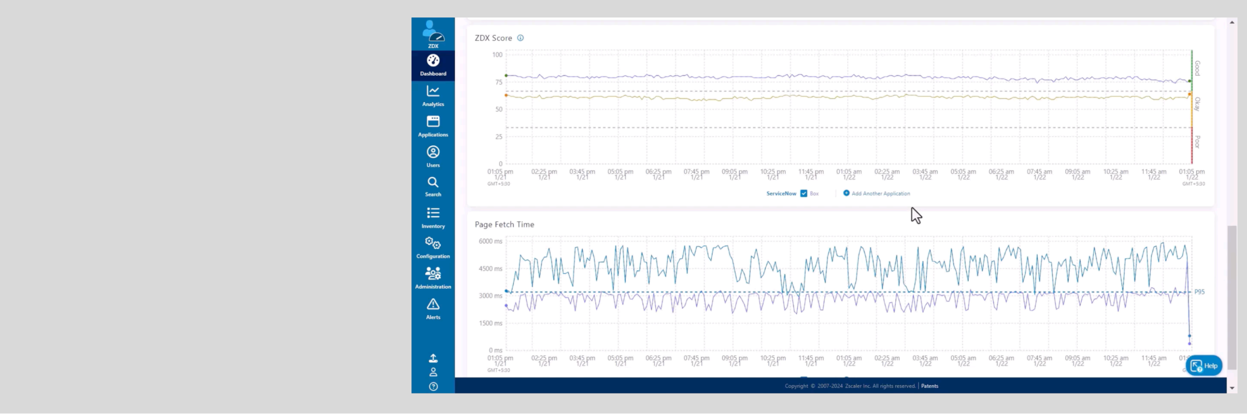
While looking at PFT trends for globally distributed or organizations, you may see PFT changes based on users in different time zones becoming active.

For comparison, you can select up to four additional applications by clicking add another application below the graph then selecting the additional applications to view. Let's select the box application.

If you want to take a closer look at the significant drop in ZDX score, or a spike in page fetch time, you can simply click on that point in the graph and display metrics for the selected applications at that time.

From here, you can click on the arrow to go to that applications page and drill down further to find the root cause of the issue.



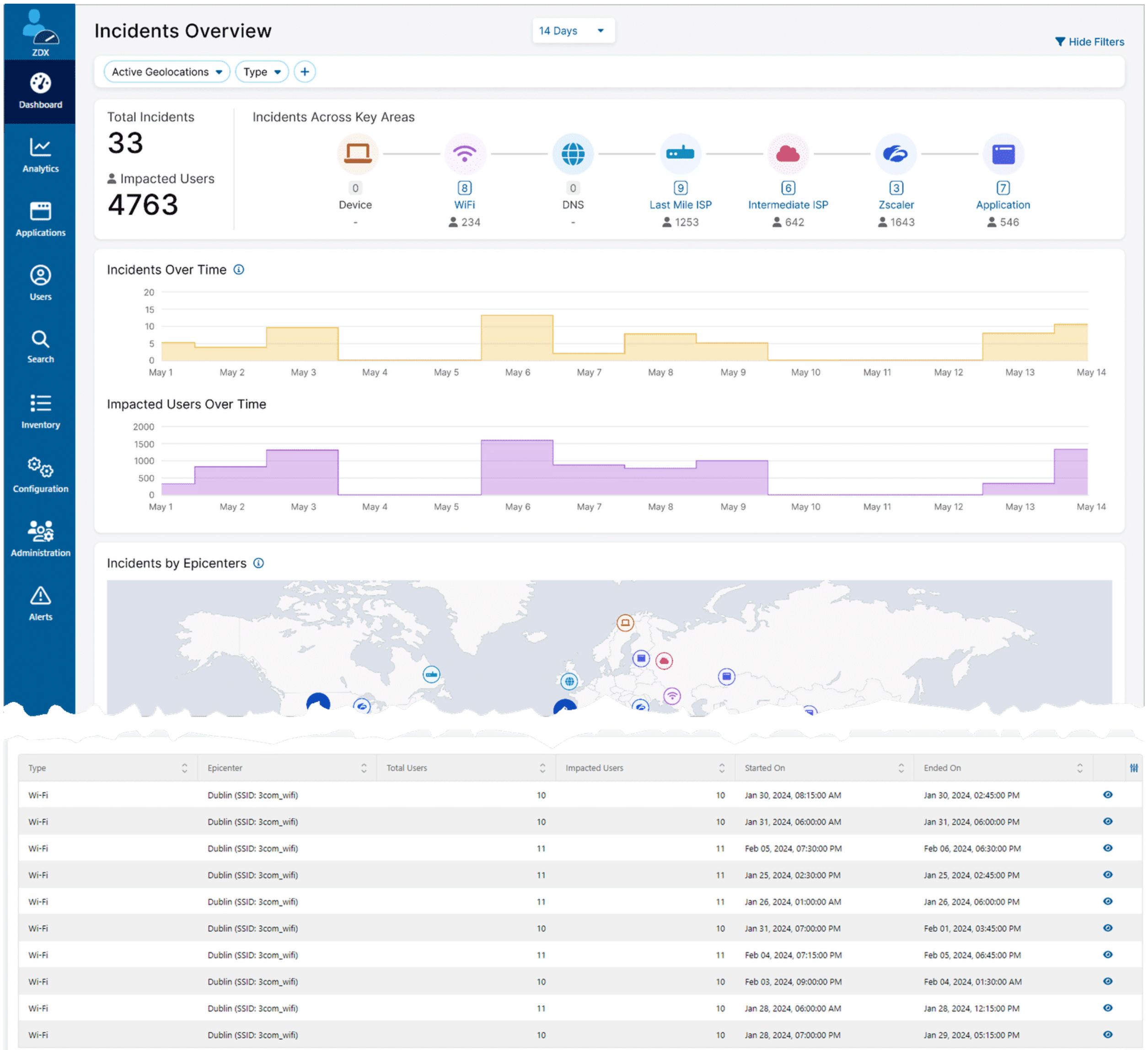


To recap, the ZDX dashboard is a good starting point when it comes to troubleshooting user experience issues. It provides a high level overview of your organization's applications and their impact on users in their geographic regions and office locations.

Incidents Overview

When a user opens a ticket, ServiceDesk teams need to quickly decide if this is an individual problem or a bigger incident that affects many users. Understanding the source of the problem often requires a lot of time and effort. ZDX uses artificial intelligence and machine learning (AI/ML) to triage issues quickly, and notify you about outages and brownouts, so that you can **proactively** resolve developing application, network or device issues **before** users complain.

The Incidents Overview dashboard helps you prioritize issues by showing incidents in four area types: WiFi, Last Mile ISP (Internet Service Provider), Zscaler Data Center, and Application.



Incidents Overview

Total Incidents
33

Impacted Users
4763

	Device	WiFi	DNS	Last Mile ISP	Intermediate ISP	Zscaler	Application
Incidents	0	8	0	9	6	3	7
Impacted Users	-	234	-	1253	642	1643	546

Type	Epicenter	Total Users	Impacted Users	Started On	Ended On	
Wi-Fi	Dublin (SSID: 3com_wifi)	10	10	Jan 30, 2024, 08:15:00 AM	Jan 30, 2024, 02:45:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	10	10	Jan 31, 2024, 06:00:00 AM	Jan 31, 2024, 06:00:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	11	11	Feb 05, 2024, 07:30:00 PM	Feb 06, 2024, 06:30:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	11	11	Jan 25, 2024, 02:30:00 PM	Jan 25, 2024, 02:45:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	11	11	Jan 26, 2024, 01:00:00 AM	Jan 26, 2024, 06:00:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	10	10	Jan 31, 2024, 07:00:00 PM	Feb 01, 2024, 03:45:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	11	11	Feb 04, 2024, 07:15:00 PM	Feb 05, 2024, 06:45:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	10	10	Feb 03, 2024, 09:00:00 PM	Feb 04, 2024, 01:30:00 AM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	11	10	Jan 28, 2024, 06:00:00 AM	Jan 28, 2024, 12:15:00 PM	👁
Wi-Fi	Dublin (SSID: 3com_wifi)	10	10	Jan 28, 2024, 07:00:00 PM	Jan 29, 2024, 05:15:00 PM	👁

Within the Incidents Overview page, you can see:

- **Filters:** Use the filters to select the type for incidents and a time range to view when incidents occurred. The default is 14 days.
- **Incident Summary:** This shows you what type of incidents have occurred. View the total incidents and the total counts across the key metrics and impacted users.
- **Incidents Over Time:** These graphs show you when incidents have occurred. Review the number of incidents that have occurred based on the impacted devices within a time range, and the number of impacted users from the incident over time.
- **Incidents by Epicenter map:** View where incidents have occurred within the time range on a map. Click on any incident to view more details.
- **Incident Details:** View a full list of incidents for the selected location and drill down further to see which users were affected.

Example:

With all the available reports, graphs and alerts in ZDX, it may be a bit challenging to separate isolated incidents from problems that affect a large number of users. With the ZDX, AI and machine learning capabilities, we are looking at many of these common issues across an organization’s tenant and categorize them to provide ServiceDesk teams a starting point when it comes to prioritizing incidents.

The Incidents Dashboard is perfect for troubleshooting.

For this example, perhaps we want to focus on Wifi issues, where we might encounter a number of Wifi Incidents and impacted users in the selected time range. Scrolling down, we would see the Epicenters of Incidents and where they are located on a map. Below the map, there is also a full list of the incidents.

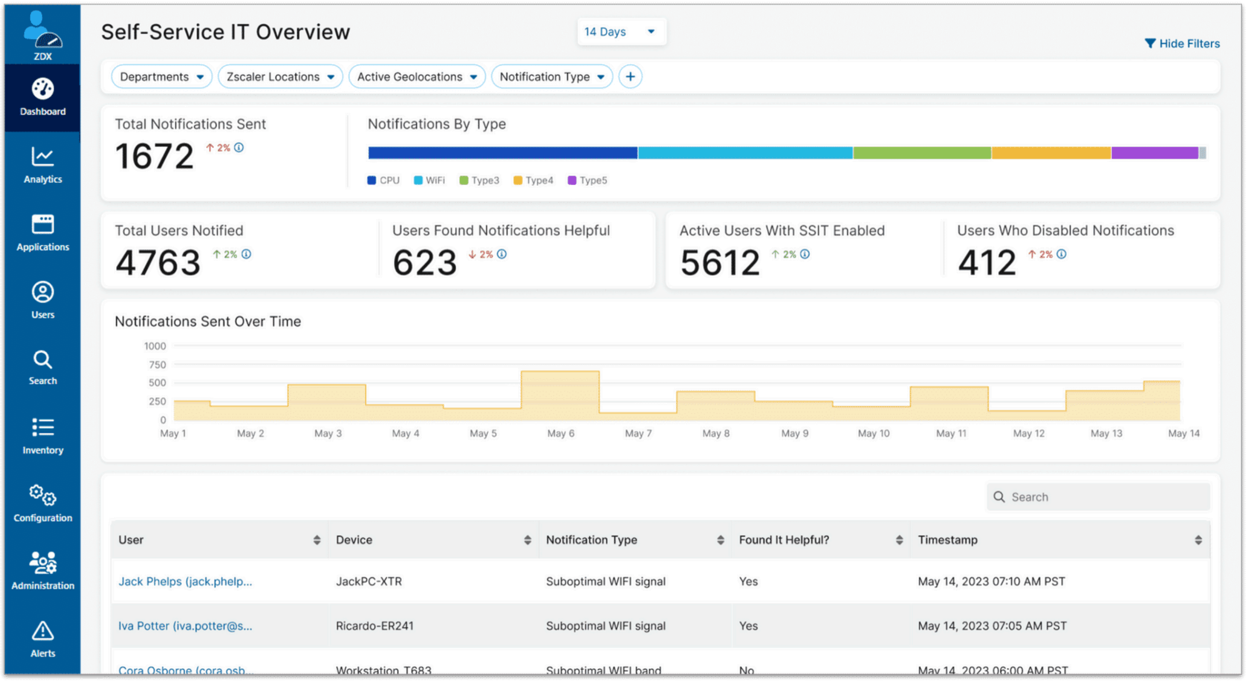
Simply clicking on one of the Incidents would reveal more information, such as Start and End times. Clicking on View Incident Details and it will take you to more details about the incident where you can see the Impacted Users, the Wifi SSID, the access point and other metrics about the Wifi Connectivity. You can also drill down into the details for an affected user. Perhaps the Wifi Signal strength is degraded as well and there is a lot of fluctuation in the Wifi signal strength.

To recap, the Incidents Overview dashboard is a great starting point for a troubleshooting workflow that starts with AI-generated incident categories. From there you can drill down into the details, all the way down to the user level.

Self Service Overview

An AI-engine running on Zscaler Client Connector is able to quickly detect device issues and provide suggestions to fix them. This AI assistant runs on the user's device, even in offline scenarios. When enabled for your users, ZDX can provide notifications when issues related to device performance, like CPU usage and WiFi performance are detected. Users can then investigate potential solutions **without the need to contact customer support**.

The Self Service Overview dashboard consolidates the data from user notifications and lets you drill down into the details of an incident.



Self-Service IT Overview

14 Days

Total Notifications Sent 1672 ↑ 2%

Notifications By Type

Total Users Notified 4763 ↑ 2%

Users Found Notifications Helpful 623 ↓ 2%

Active Users With SSIT Enabled 5612 ↑ 2%

Users Who Disabled Notifications 412 ↑ 2%

Notifications Sent Over Time

User	Device	Notification Type	Found It Helpful?	Timestamp
Jack Phelps (jack.phelp...	JackPC-XTR	Suboptimal WIFI signal	Yes	May 14, 2023 07:10 AM PST
Iva Potter (iva.potter@s...	Ricardo-ER241	Suboptimal WIFI signal	Yes	May 14, 2023 07:05 AM PST
Cora Osborne (cora.osb...	Workstation_T683	Suboptimal WIFI band	No	May 14, 2023 06:00 AM PST

Within the Incidents Overview page, you can see:

- **Filters:** Narrow the scope of notification by selecting filters for time range, departments, locations and notification types
- **Notification & User Counts:** View summary information about notifications and users, based on your selected time range.
- **Notifications Sent Over Time:** Review the number of user notifications that were generated during your selected time range.
- **User Details:** For any user listed in the table, click the username to view the User Details page, incl. the related event in the User Device Events graph. Notification icons indicate the dates and times when a notification was sent to the user.

Analytics

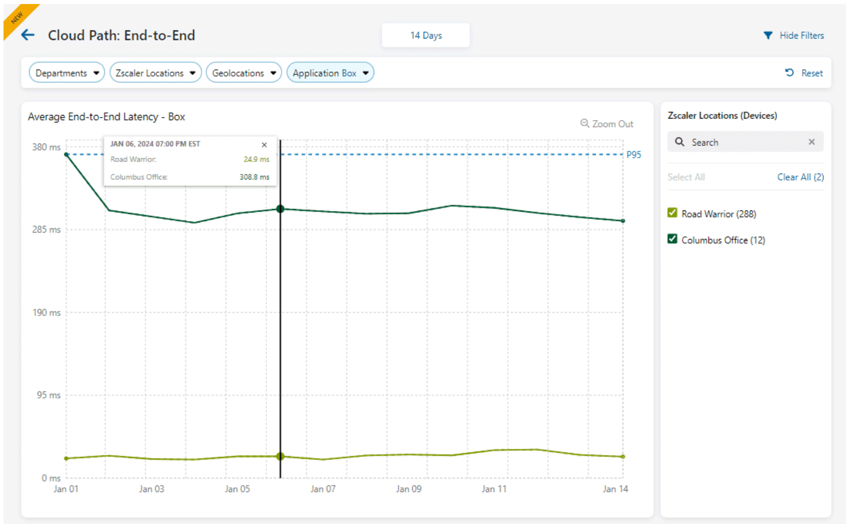
The Admin Portal's *Analytics* menu provides reports that go beyond day-to-day monitoring and troubleshooting. These reports offer insights into general trends, which may be useful for capacity planning or identifying patterns with application or network performance.

System Generated Reports

System-generated reports allow you to view user data across your organization that can reveal distinctive patterns among various metrics, for example Device Distribution by WiFi Bands, DNS Performance, Application Performance and more. Details for each report are aggregated day-to-day and captured in a rolling 14-day cycle.

Available Reports Include:

Cloud Path: End-to-End: The End-to-End Latency report captures the average latency in the Cloud Path within a 14-day time range.



Cloud Path: End-to-End

14 Days

Average End-to-End Latency - Box

JAN 06, 2024 07:00 PM EST

Road Warrior: 24.9 ms

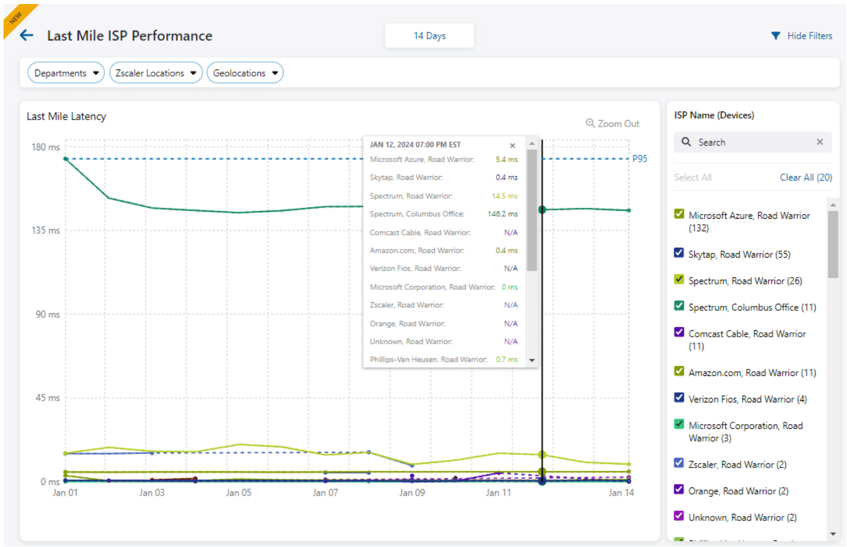
Columbus Office: 308.8 ms

Zscaler Locations (Devices)

☑ Road Warrior (288)

☑ Columbus Office (12)

Last Mile ISP Performance: The Last Mile ISP Performance report captures ISP latency within a 14-day time range.

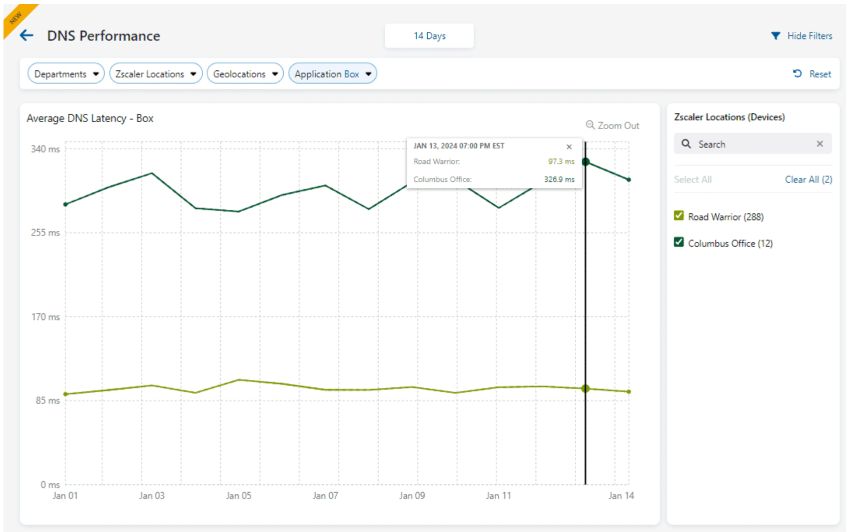


JAN 12, 2024 07:00 PM EST

Microsoft Azure, Road Warrior: 5.4 ms
Skytap, Road Warrior: 0.4 ms
Spectrum, Road Warrior: 14.5 ms
Spectrum, Columbus Office: 146.2 ms
Comcast Cable, Road Warrior: N/A
Amazon.com, Road Warrior: 0.4 ms
Verizon Fios, Road Warrior: N/A
Microsoft Corporation, Road Warrior: 0 ms
Zscaler, Road Warrior: N/A
Orange, Road Warrior: N/A
Unknown, Road Warrior: N/A
Phillips-Van Heusen, Road Warrior: 0.7 ms

☑ Microsoft Azure, Road Warrior (132)
☑ Skytap, Road Warrior (55)
☑ Spectrum, Road Warrior (26)
☑ Spectrum, Columbus Office (11)
☑ Comcast Cable, Road Warrior (11)
☑ Amazon.com, Road Warrior (11)
☑ Verizon Fios, Road Warrior (4)
☑ Microsoft Corporation, Road Warrior (3)
☑ Zscaler, Road Warrior (2)
☑ Orange, Road Warrior (2)
☑ Unknown, Road Warrior (2)

DNS Performance: The DNS Performance report captures the average DNS latency within a 14-day time range.

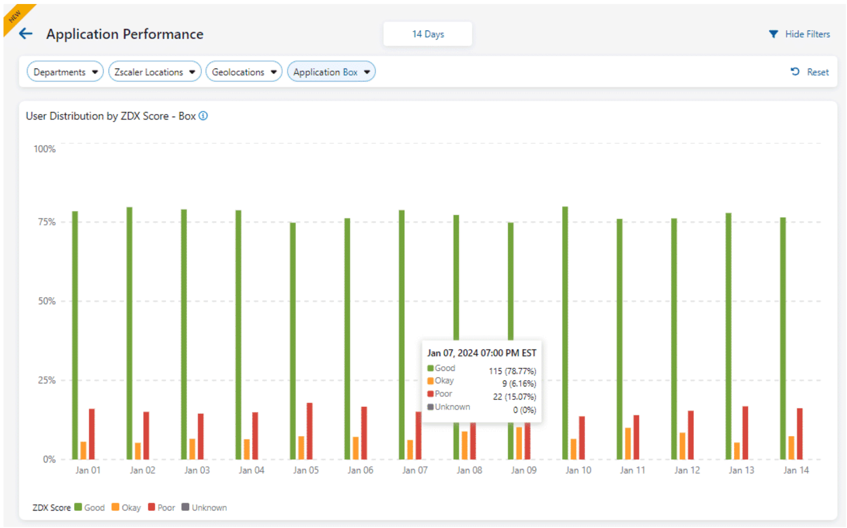


JAN 13, 2024 07:00 PM EST

Road Warrior: 97.3 ms
Columbus Office: 326.9 ms

☑ Road Warrior (288)
☑ Columbus Office (12)

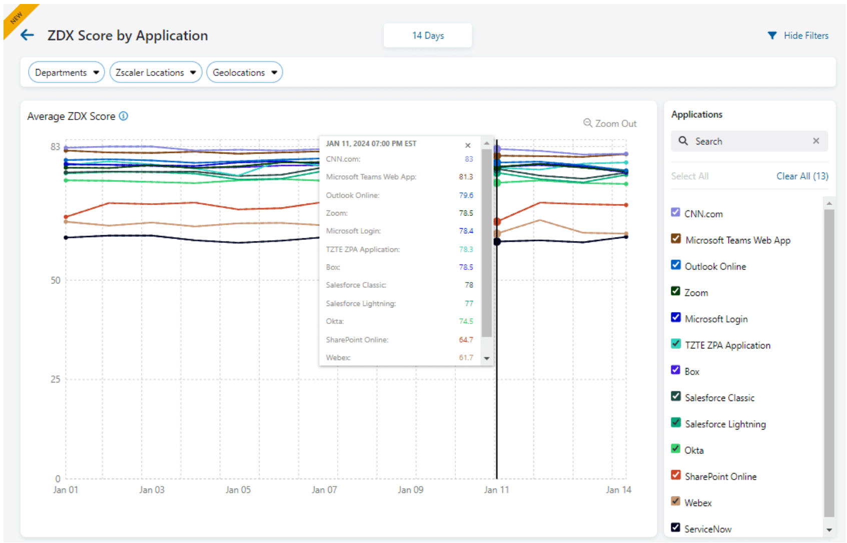
Application Performance: The Application Performance report captures the daily distribution of ZDX Scores within a 14-day time range.



Jan 07, 2024 07:00 PM EST

🟩 Good 115 (78.77%)
🟧 Okay 9 (6.16%)
🟥 Poor 22 (15.07%)
⬛ Unknown 0 (0%)

ZDX Score By Application: The ZDX Score by Application report captures the average ZDX Score per application within a 14-day time range.

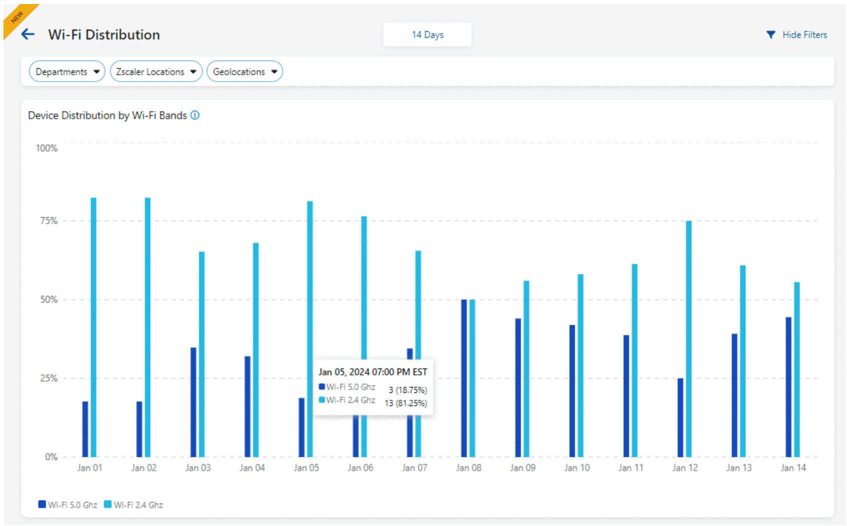


JAN 11, 2024 07:00 PM EST

CNN.com:	83
Microsoft Teams Web App:	81.3
Outlook Online:	79.6
Zoom:	78.5
Microsoft Login:	78.4
TZTE ZPA Application:	78.3
Box:	78.5
Salesforce Classic:	78
Salesforce Lightning:	77
Okta:	74.5
SharePoint Online:	64.7
Webex:	61.7

☑ CNN.com
☑ Microsoft Teams Web App
☑ Outlook Online
☑ Zoom
☑ Microsoft Login
☑ TZTE ZPA Application
☑ Box
☑ Salesforce Classic
☑ Salesforce Lightning
☑ Okta
☑ SharePoint Online
☑ Webex
☑ ServiceNow

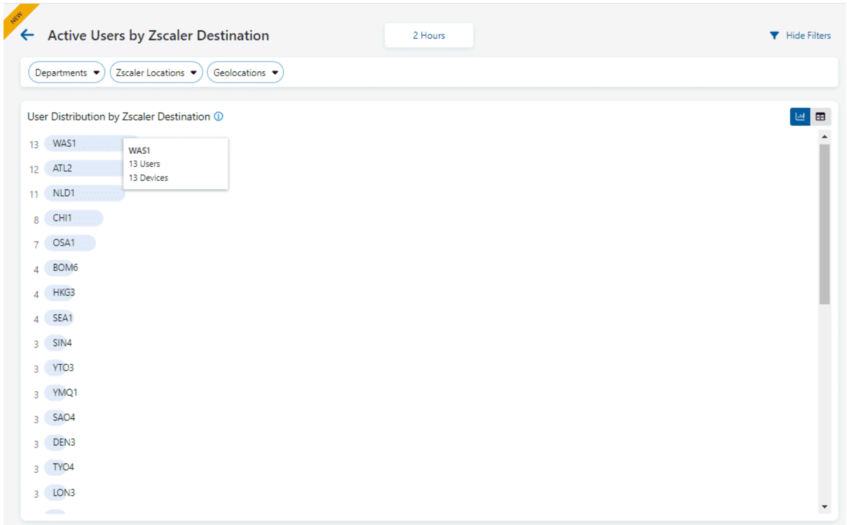
WiFi Distribution: The WiFi Distribution report captures the daily distribution of ZDX Scores within a 14-day time range.



Jan 05, 2024 07:00 PM EST

Wi-Fi 5.0 Ghz	3 (18.75%)
Wi-Fi 2.4 Ghz	13 (81.25%)

Active Users by Zscaler Destination: Show the user and device counts per Zscaler data center within a 2 hour time range.

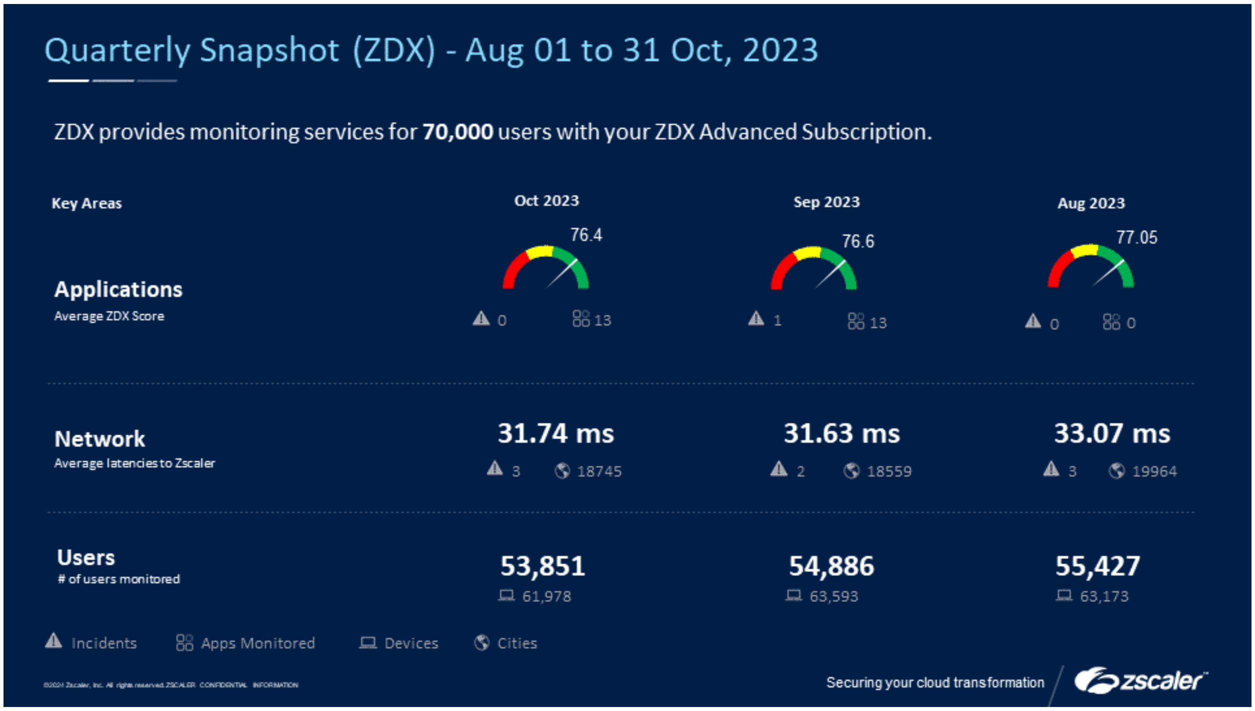

NEW
Active Users by Zscaler Destination
2 Hours
Hide Filters
Departments
Zscaler Locations
Geolocations
User Distribution by Zscaler Destination

13	WAS1
12	ATL2
11	NLD1
8	CHI1
7	OSA1
4	BOM6
4	HKG3
4	SEA1
3	SIN4
3	YTO3
3	YMQ1
3	SAO4
3	DEN3
3	TYO4
3	LON3

WAS1
13 Users
13 Devices

Quarterly Business Reviews

Quarterly Business Review (QBR) reports help provide insight into emerging traffic trends, such as a quarterly snapshot of your Application ZDX Score, Network Average Latency, and Users. Once a new report is generated, it is securely stored as a PowerPoint file in the Zscaler cloud and can be downloaded from the ZDX Admin portal.



Quarterly Snapshot (ZDX) - Aug 01 to 31 Oct, 2023

ZDX provides monitoring services for **70,000** users with your ZDX Advanced Subscription.

Key Areas	Oct 2023	Sep 2023	Aug 2023
Applications Average ZDX Score	76.4 ⚠ 0 88 13	76.6 ⚠ 1 88 13	77.05 ⚠ 0 88 0
Network Average latencies to Zscaler	**31.74 ms** ⚠ 3 🌐 18745	**31.63 ms** ⚠ 2 🌐 18559	**33.07 ms** ⚠ 3 🌐 19964
Users # of users monitored	**53,851** 💻 61,978	**54,886** 💻 63,593	**55,427** 💻 63,173

⚠ Incidents   88 Apps Monitored   💻 Devices   🌐 Cities

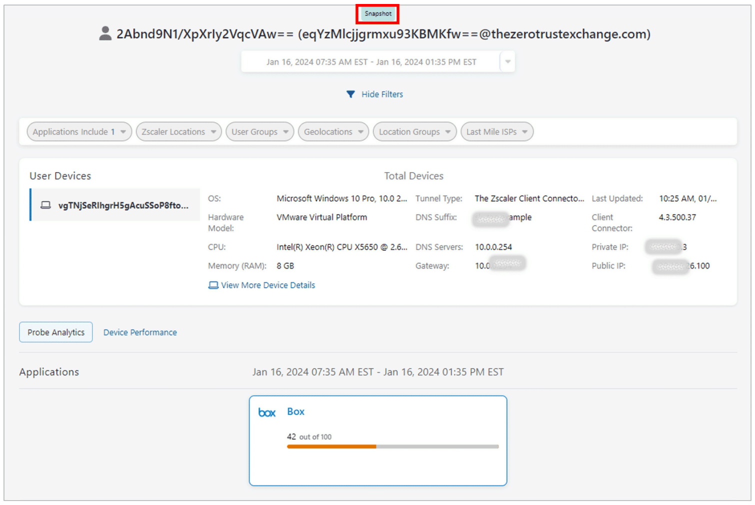
©2024 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation

ZDX Snapshots

Imagine you need to escalate a support ticket for further investigation to a Level 3 application specialist. Adding screenshots of the User Details page to a Word document or printing to pdf may be cumbersome.

That's where the ZDX Snapshot feature comes in. It captures the current state of a UI page, and provides a URL that admins can share with ZDX users or other admins for view-only access; with no Admin portal login required. The recipient can access the URL and browse the page with limited interactivity.



Snapshot

2Abnd9N1/XpXrly2VqcVAw== (eqYzMlcjjgrmxu93KBMKfw==@thezerotrustexchange.com)

Jan 16, 2024 07:35 AM EST - Jan 16, 2024 01:35 PM EST

User Devices

Total Devices

vgTNjSeRlhgrH5gAcuSSoP8fto...

OS:	Microsoft Windows 10 Pro, 10.0 2...	Tunnel Type:	The Zscaler Client Connecto...	Last Updated:	10:25 AM, 01/...
Hardware Model:	VMware Virtual Platform	DNS Suffix:	[redacted]ample	Client Connector:	4.3.500.37
CPU:	Intel(R) Xeon(R) CPU X5650 @ 2.6...	DNS Servers:	10.0.0.254	Private IP:	[redacted].3
Memory (RAM):	8 GB	Gateway:	10.0[redacted]	Public IP:	[redacted]6.100

Applications

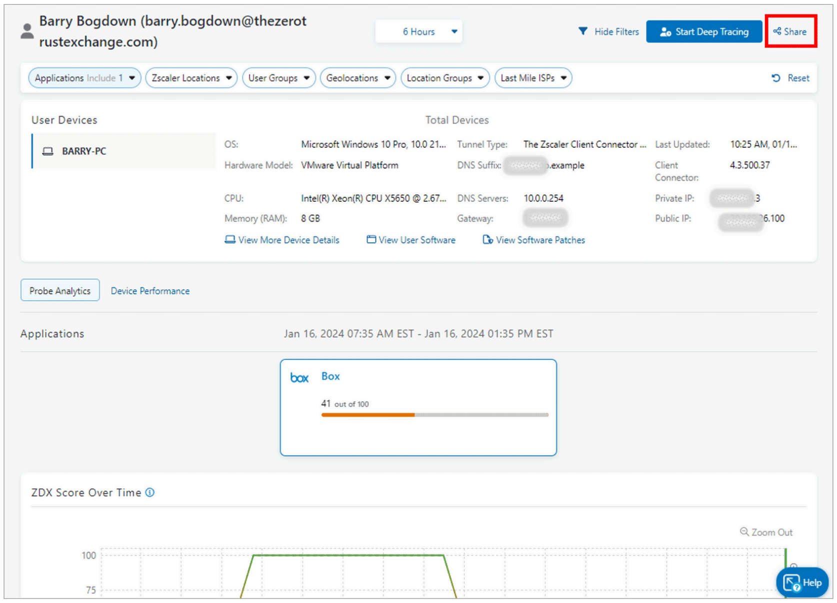
Jan 16, 2024 07:35 AM EST - Jan 16, 2024 01:35 PM EST

Box

42 out of 100

Here's how you **create and share a ZDX snapshot:**

On the User Details page, run Root Cause Analysis for a particular point, so that the analysis is included in the snapshot. Then, click the **Share** button.



Barry Bogdown (barry.bogdown@thezerot rustexchange.com)

User Devices — Total Devices

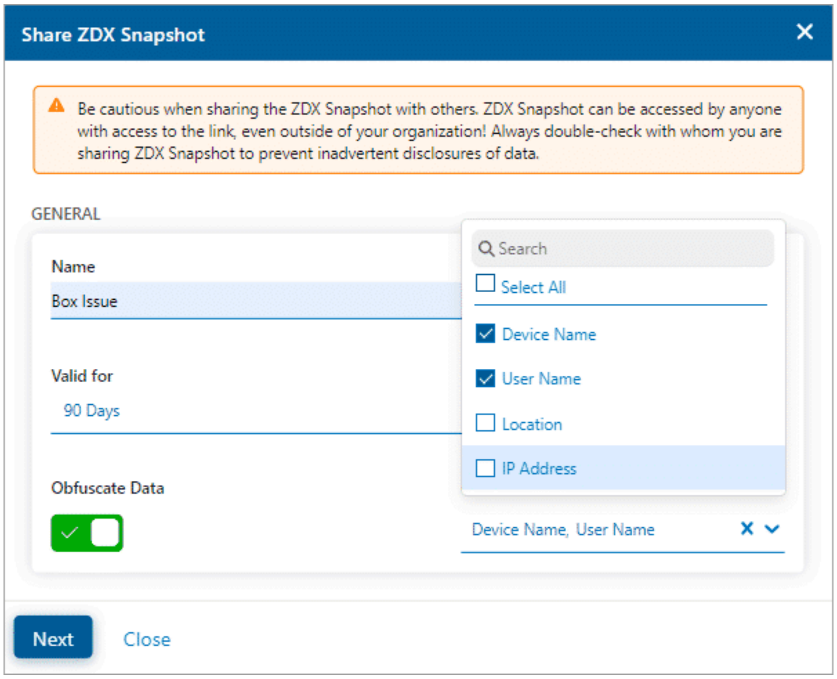
BARRY-PC

OS: Microsoft Windows 10 Pro, 10.0 21...
Hardware Model: VMware Virtual Platform
CPU: Intel(R) Xeon(R) CPU X5650 @ 2.67...
Memory (RAM): 8 GB
Tunnel Type: The Zscaler Client Connector ...
DNS Suffix: [redacted].example
DNS Servers: 10.0.0.254
Gateway: [redacted]
Last Updated: 10:25 AM, 01/1...
Client Connector: 4.3.500.37
Private IP: [redacted]3
Public IP: [redacted]6.100

Applications — Jan 16, 2024 07:35 AM EST - Jan 16, 2024 01:35 PM EST

Box — 41 out of 100

Configure some simple parameters. For example, specify how long the snapshot should be available and, as required, if you want to obfuscate user-specific details.



Share ZDX Snapshot

Be cautious when sharing the ZDX Snapshot with others. ZDX Snapshot can be accessed by anyone with access to the link, even outside of your organization! Always double-check with whom you are sharing ZDX Snapshot to prevent inadvertent disclosures of data.

GENERAL

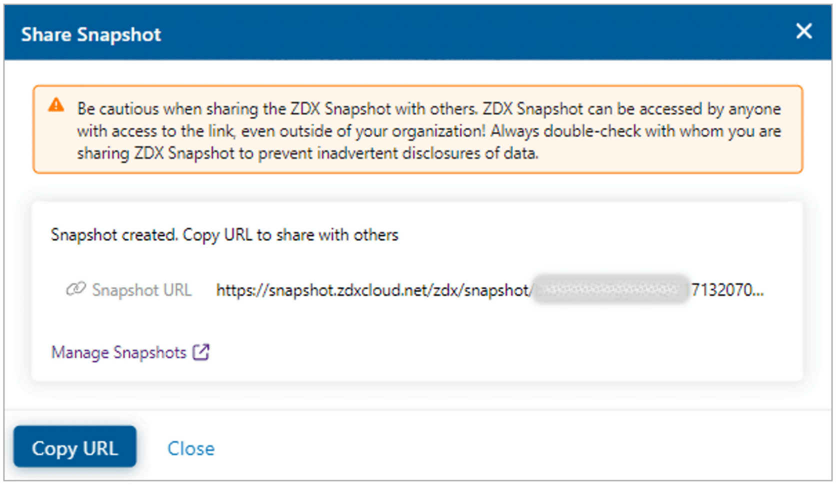
Name: Box Issue

Valid for: 90 Days

Obfuscate Data: on — Device Name, User Name

- ☐ Select All
- ☑ Device Name
- ☑ User Name
- ☐ Location
- ☐ IP Address

Copy the URL here, or close the dialog and get the URL from the ZDX Snapshots page.



⚠ Be cautious when sharing the ZDX Snapshot with others. ZDX Snapshot can be accessed by anyone with access to the link, even outside of your organization! Always double-check with whom you are sharing ZDX Snapshot to prevent inadvertent disclosures of data.

Snapshot created. Copy URL to share with others

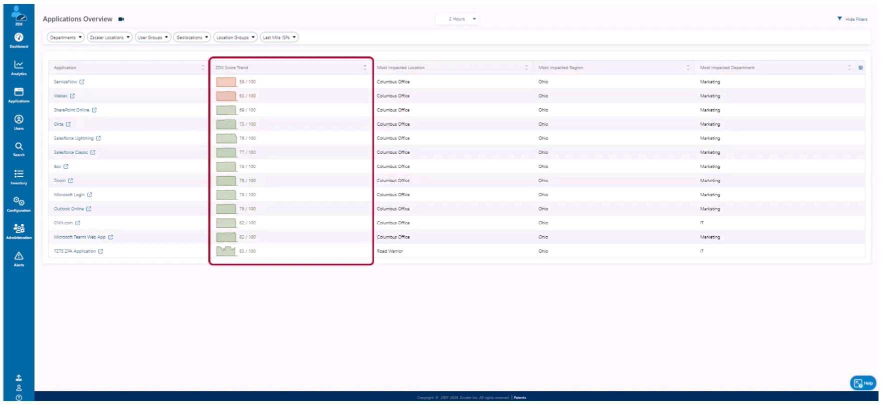
Snapshot URL https://snapshot.zdxcloud.net/zdx/snapshot/[redacted]7132070...

Applications Dashboard

The Applications Overview Dashboard displays information about the applications users are accessing and the impact these applications have on your organization’s digital experience.

The applications dashboard provides a great starting point for troubleshooting application issues. It provides a simple one page summary view of your predefined and custom applications.

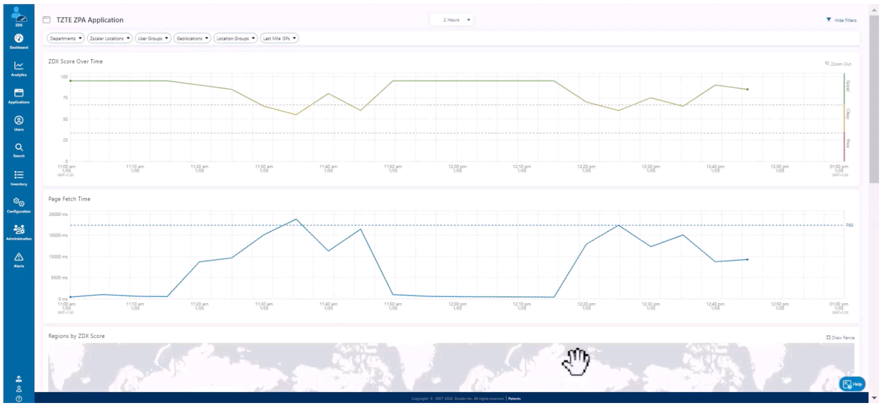
At the top of the page, there are filters for time range departments, Zscaler locations, user groups, geographic locations, location groups, and last mile ISPs.



Application	ZDX Score Trend	Most Impacted Location	Most Impacted Region	Most Impacted Department
ServiceNow	59 / 100	Columbus Office	Ohio	Marketing
Webex	63 / 100	Columbus Office	Ohio	Marketing
SharePoint Online	69 / 100	Columbus Office	Ohio	Marketing
Okta	75 / 100	Columbus Office	Ohio	Marketing
Salesforce Lightning	76 / 100	Columbus Office	Ohio	Marketing
Salesforce Classic	77 / 100	Columbus Office	Ohio	Marketing
Box	78 / 100	Columbus Office	Ohio	Marketing
Zoom	78 / 100	Columbus Office	Ohio	Marketing
Microsoft Login	79 / 100	Columbus Office	Ohio	Marketing
Outlook Online	79 / 100	Columbus Office	Ohio	Marketing
CNN.com	82 / 100	Columbus Office	Ohio	IT
Microsoft Teams Web App	82 / 100	Columbus Office	Ohio	Marketing
TZTE ZPA Application	83 / 100	Road Warrior	Ohio	IT

The table below lists your applications, their ZDX scores, and a small graph showing the rise and fall of the application score over time.

The other columns show the most impacted locations, regions, and departments.



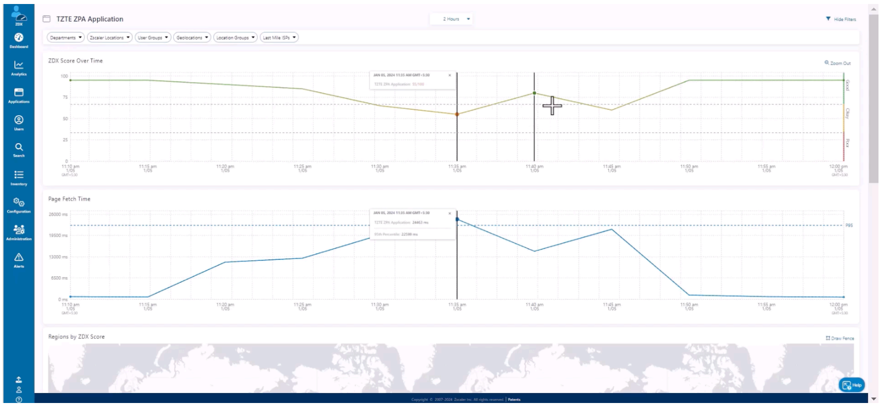
From here, you can quickly drill down into a more detailed view of an application needing your attention.

Simply click on the application's name or click the link next to it to open the details in a new browser window.

At the top of the application details page, there are graphs that show the ZDX score and page fetch time over the selected time range. Let's zoom in on a time span where the ZDX score graph shows a significant drop. Simply click on a point on the zoomed in graph to see more details. This is super helpful in a workflow you should get used to.

When you see a drop in the graph, zoom in on the drop and see which metrics were affected.

When you scroll down, there's a regions by ZDX Score map. That shows the geographic locations, their ZDX score, and the number of users at each location.



TZTE ZPA Application

ZDX Score Over Time

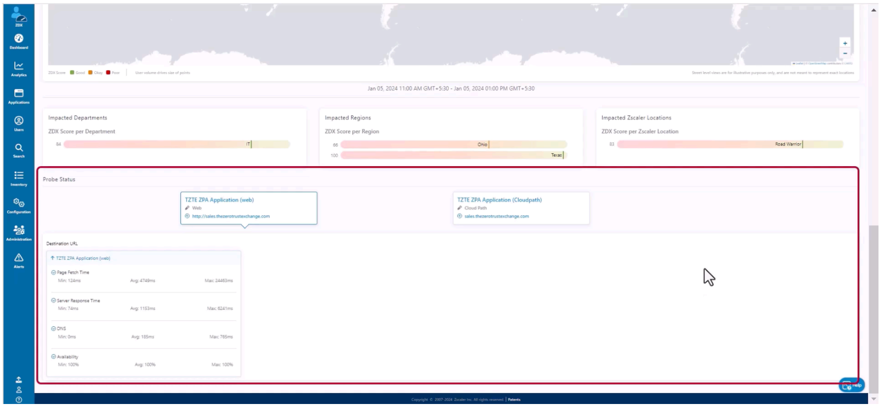
JAN 05, 2024 11:35 AM GMT+5:30
TZTE ZPA Application: 55/100

Page Fetch Time

JAN 05, 2024 11:35 AM GMT+5:30
TZTE ZPA Application: 24463 ms
95th Percentile: 22599 ms

Regions by ZDX Score

Below the map, there are widgets that show the top affected departments, regions, and Zscaler locations. And when you scroll down all the way to the bottom of the page, you'll see details about the probes that have been configured for the application and what metrics the probes are tracking.



Street level views are for illustrative purposes only, and are not meant to represent exact locations

Jan 05, 2024 11:00 AM GMT+5:30 - Jan 05, 2024 01:00 PM GMT+5:30

Impacted Departments
ZDX Score per Department

Impacted Regions
ZDX Score per Region

Impacted Zscaler Locations
ZDX Score per Zscaler Location

Probe Status

TZTE ZPA Application (web)
Web
http://sales.thezerotrustexchange.com

TZTE ZPA Application (Cloudpath)
Cloud Path
sales.thezerotrustexchange.com

Destination URL

TZTE ZPA Application (web)

Page Fetch Time
Min: 124ms Avg: 4749ms Max: 24463ms

Server Response Time
Min: 74ms Avg: 1153ms Max: 6241ms

DNS
Min: 0ms Avg: 185ms Max: 765ms

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

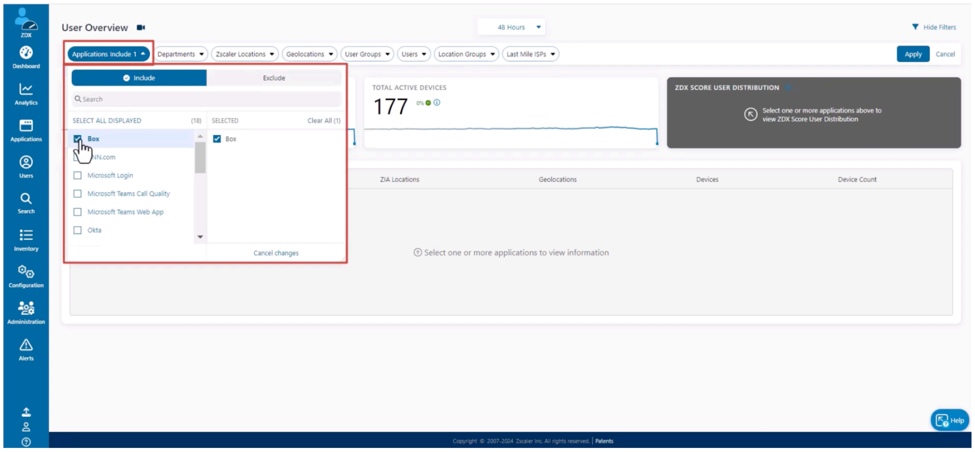
Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

Users Dashboard

Viewing the Users Dashboard

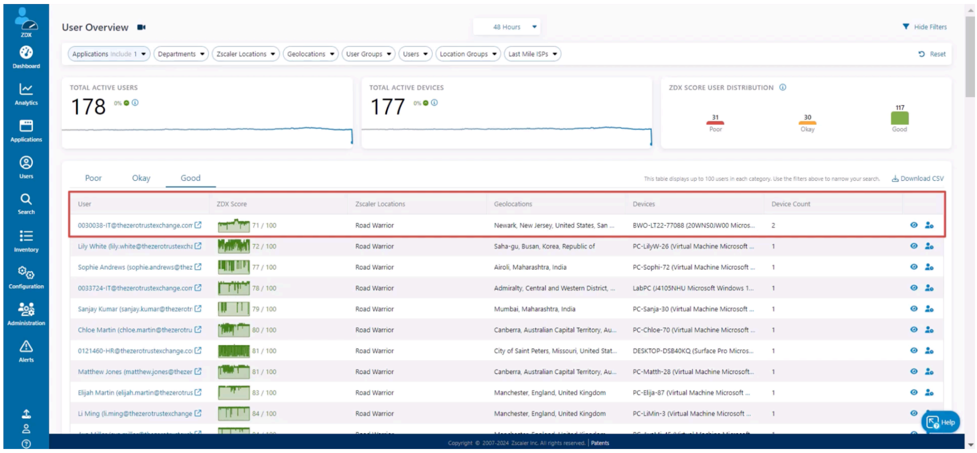
Troubleshooting an issue that was reported by one specific user can be quite tricky. With many employees now working from home, where do you even begin to narrow down the root cause of the problem? Is it the user's laptop or home WiFi? Their ISP? Some internet backbone node or the application itself? The ZDX user's dashboard helps you answer these questions and reduce the time it takes to close a support ticket.

Let's take a tour of the dashboard and a user details page. To populate data in the user's dashboard, you first need to select one or more applications from the drop down list.



Here is a tip for you. When selecting multiple applications, the graph will then display aggregated metrics. Which may show lower scores compared to choosing only one application. That's because ZDX shows the lowest score among all selected applications. Once you've selected an application, you can adjust and apply any additional filters.

Below the filter section are several widgets that give an overview of your user's digital experience.



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

User	ZDX Score	Zscaler Locations	Geolocations	Devices	Device Count
0030038-IT@thezerotrustexchange.com	71 / 100	Road Warrior	Newark, New Jersey, United States, San ...	BWO-LT22-77088 (20WNS0JW00 Micros...	2
Lily White (lily.white@thezerotrustexcha	72 / 100	Road Warrior	Saha-gu, Busan, Korea, Republic of	PC-LilyW-26 (Virtual Machine Microsoft ...	1
Sophie Andrews (sophie.andrews@thez	77 / 100	Road Warrior	Airoli, Maharashtra, India	PC-Sophi-72 (Virtual Machine Microsoft ...	1
0033724-IT@thezerotrustexchange.com	78 / 100	Road Warrior	Admiralty, Central and Western District, ...	LabPC (J4105NHU Microsoft Windows 1...	1
Sanjay Kumar (sanjay.kumar@thezerotr	79 / 100	Road Warrior	Mumbai, Maharashtra, India	PC-Sanja-30 (Virtual Machine Microsoft ...	1
Chloe Martin (chloe.martin@thezerotru	80 / 100	Road Warrior	Canberra, Australian Capital Territory, Au...	PC-Chloe-70 (Virtual Machine Microsoft ...	1
0121460-HR@thezerotrustexchange.co	81 / 100	Road Warrior	City of Saint Peters, Missouri, United Stat...	DESKTOP-DSB40KQ (Surface Pro Micros...	1
Matthew Jones (matthew.jones@thezer	81 / 100	Road Warrior	Canberra, Australian Capital Territory, Au...	PC-Matth-28 (Virtual Machine Microsoft...	1
Elijah Martin (elijah.martin@thezerotrus	83 / 100	Road Warrior	Manchester, England, United Kingdom	PC-Elija-87 (Virtual Machine Microsoft ...	1
Li Ming (li.ming@thezerotrustexchange	84 / 100	Road Warrior	Manchester, England, United Kingdom	PC-LiMin-3 (Virtual Machine Microsoft ...	1

Total active users shows the number of users that are active for the selected time range. There is a percentage indicating how much the number of users has gone up or down over time. And the trend line below tracks how the number rose and fell during that time.

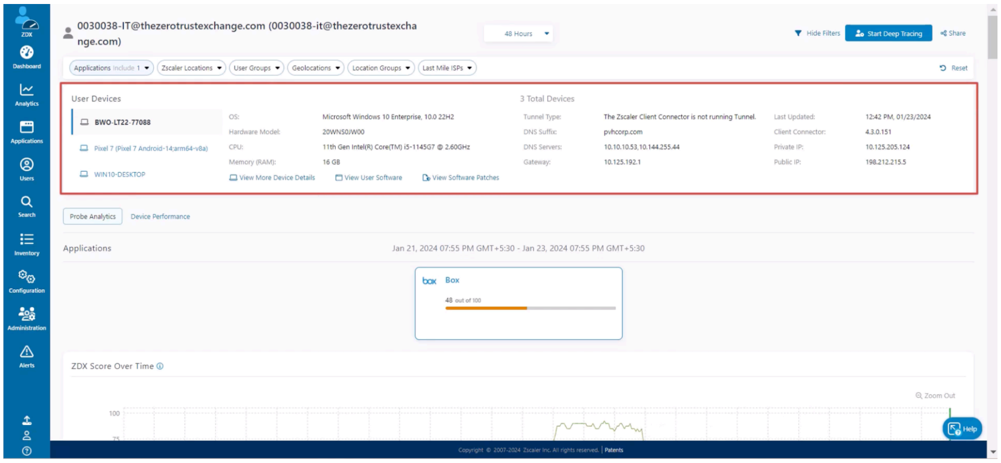
Total active devices show similar information about the number of devices. Note, in this screen, the number of active users is different from the number of active devices. That's because ZDX can track more than one device per user.

Also, looking at the trend lines, you may see a drop in the active users and device count towards the end of the trend line. That's because ZDX updates the widgets periodically in batches, which may slightly skew the displayed values.

And the ZDX score user distribution widget shows how many users have a poor, okay, or good ZDX score over the selected time range? Remember that the ZDX score is based on a scale of one to one hundred. You can also look at the users list, which displays it to one hundred users ZDX scores for the poor, okay, and good categories. For each user, the list shows the ZDX score The scores change over time, the Zscaler location, the geographic location, as well as the device information. You can also download this list as a CSV file.

And there are clickable icons to view the user details or to start a deep tracing session.

Let's have a closer look at the information provided on the user details page by selecting one of our users.



0030038-IT@thezerotrustexchange.com (0030038-it@thezerotrustexchange.com)

User Devices

3 Total Devices

BWO-LT22-77088

Pixel 7 (Pixel 7 Android-14;arm64-v8a)

WIN10-DESKTOP

OS: Microsoft Windows 10 Enterprise, 10.0 22H2

Hardware Model: 20WNS0JW00

CPU: 11th Gen Intel(R) Core(TM) i5-1145G7 @ 2.60GHz

Memory (RAM): 16 GB

View More Device Details | View User Software | View Software Patches

Tunnel Type: The Zscaler Client Connector is not running Tunnel.

DNS Suffix: pvhcorp.com

DNS Servers: 10.10.10.53,10.144.255.44

Gateway: 10.125.192.1

Last Updated: 12:42 PM, 01/23/2024

Client Connector: 4.3.0.151

Private IP: 10.125.205.124

Public IP: 198.212.215.5

Applications

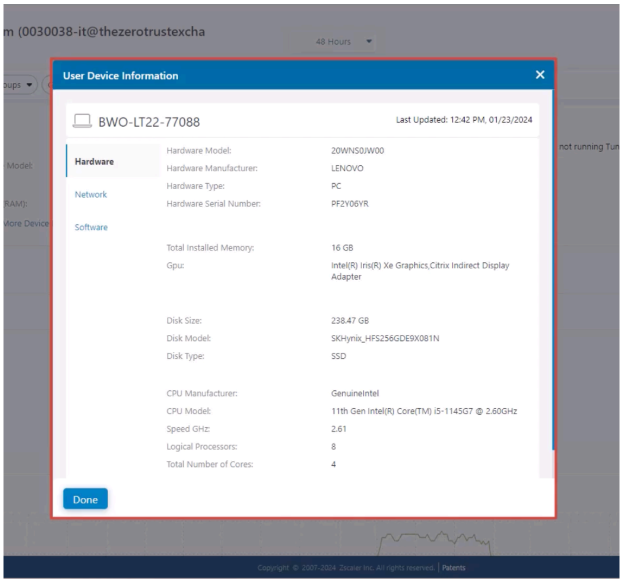
Jan 21, 2024 07:55 PM GMT+5:30 - Jan 23, 2024 07:55 PM GMT+5:30

Box

48 out of 100

ZDX Score Over Time

The graphs and metrics in the user details page really help you drill down to the root cause of an issue. And remember, all of these metrics are automatically collected by the client connector. There's nothing else to configure. At the top, you'll see the devices in use and specific device information such as OS type, version, CPU, memory, private and public IP, and more. If there is more than one device, the first device in the list is automatically selected.


48 Hours
Done
Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

User Device Information

BWO-LT22-77088

Last Updated: 12:42 PM, 01/23/2024

Hardware

Network

Software

Hardware Model: 20WNS0JW00

Hardware Manufacturer: LENOVO

Hardware Type: PC

Hardware Serial Number: PF2Y06YR

Total Installed Memory: 16 GB

Gpu: Intel(R) Iris(R) Xe Graphics,Citrix Indirect Display Adapter

Disk Size: 238.47 GB

Disk Model: SKHynix_HFS256GDE9X081N

Disk Type: SSD

CPU Manufacturer: GenuineIntel

CPU Model: 11th Gen Intel(R) Core(TM) i5-1145G7 @ 2.60GHz

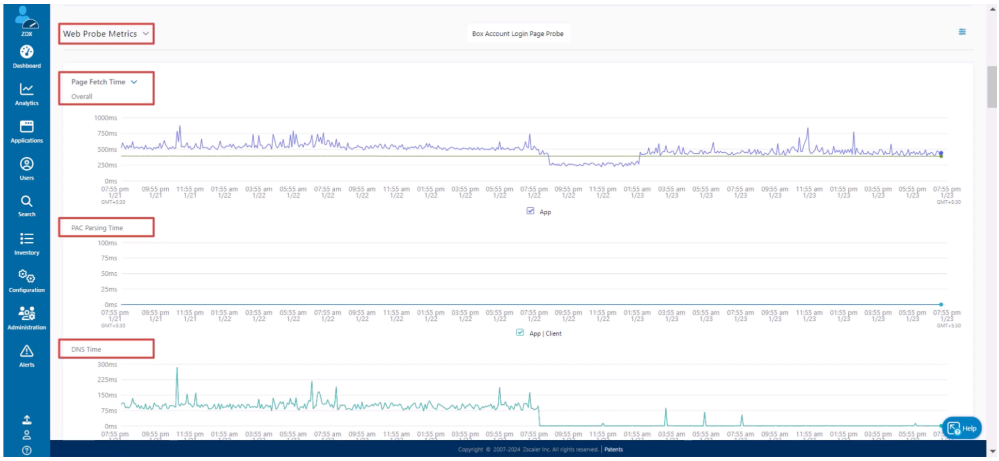
Speed GHz: 2.61

Logical Processors: 8

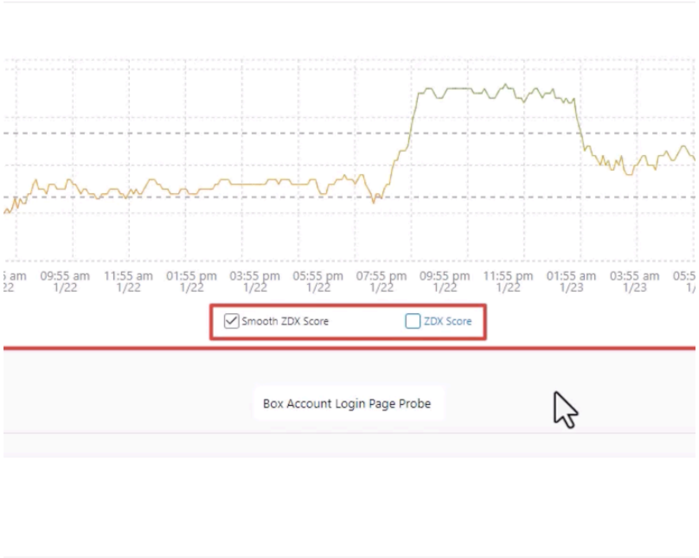
Total Number of Cores: 4

Let's look at more device details. This window displays additional device details organized under the hardware, network, and software tabs. For example, under the network tab you can review details about a user's WiFi setup, including WiFi type, SSID, and WiFi channel.

Next, there is a ZDX score over time graph which shows how the application's ZDX score changed over the selected time period for this user and device.



At the bottom of the graph, you have toggle options for smooth ZDX score and ZDX score. So what's the difference?



Sometimes brief ups and downs in the ZDX score can make it difficult to cut through the noise and figure out what's really going on.

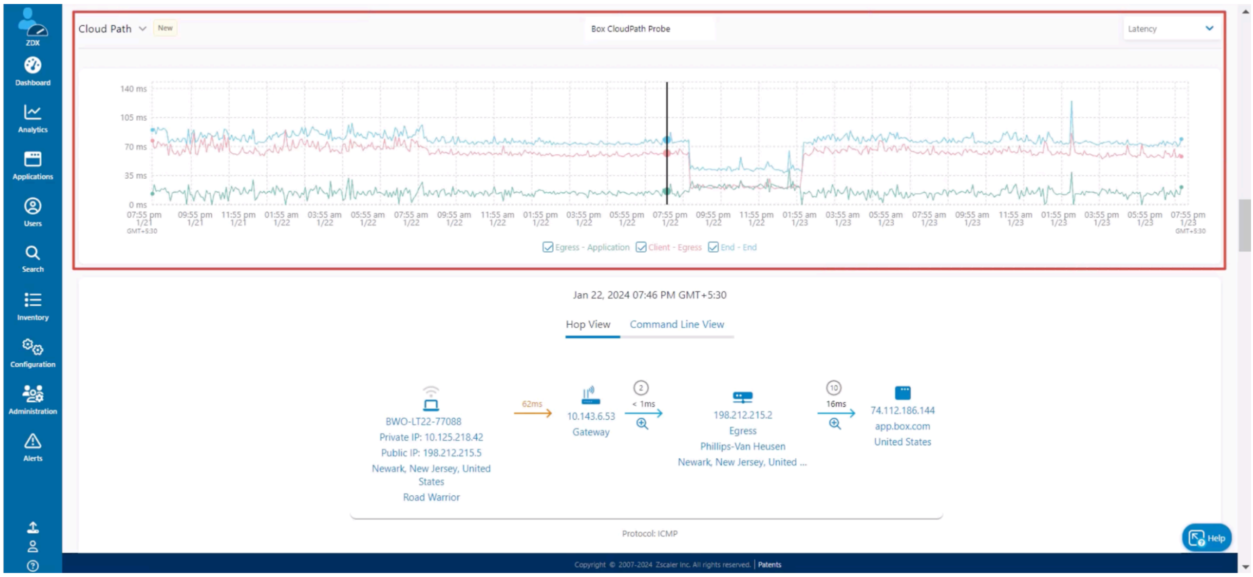
That's where the default smooth ZDX score option comes in handy. Because it aggregates historical data to reuse short term variations in the ZDX score and provides a clear picture of the overall trend. When you scroll down further, you'll see a section for web probe metrics with graphs for page fetch time, server response time, DNS resolve time, and availability.

These graphs are shown by default, but you can use the menu on the right and deselect any of the graphs you're not interested in.

As always, you can click a point on one graph and all other graphs will show their values for that same point in time.

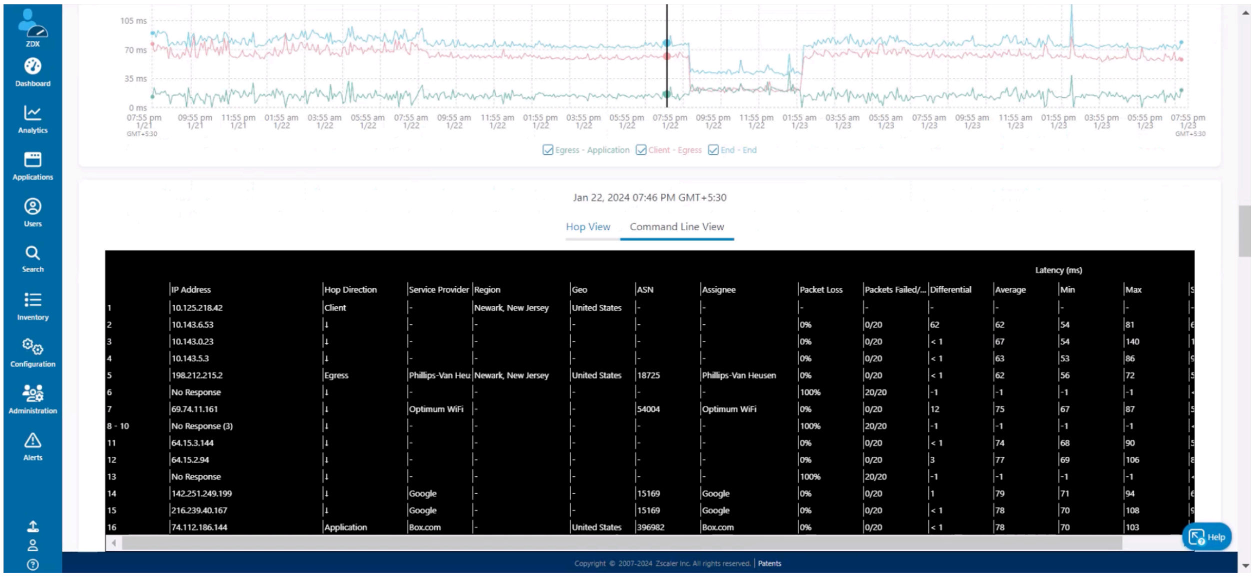
Further down we can see the next set of graphs.

At the top of the Cloud Path section, there's a graph that shows either latency or packet loss for various segments of the data path between user and application.



Below that, you'll see Hop View, which shows a graphical representation of the path from the user's device to the application's front door.

The HopView is a great troubleshooting tool to quickly identify the source of packet loss or latency along the data path.



Jan 22, 2024 07:46 PM GMT+5:30

Hop View | Command Line View

											Latency (ms)		
	IP Address	Hop Direction	Service Provider	Region	Geo	ASN	Assignee	Packet Loss	Packets Failed/...	Differential	Average	Min	Max
1	10.125.218.42	Client	-	Newark, New Jersey	United States	-	-	-	-	-	-	-	-
2	10.143.6.53	↓	-	-	-	-	-	0%	0/20	62	62	54	81
3	10.143.0.23	↓	-	-	-	-	-	0%	0/20	< 1	67	54	140
4	10.143.5.3	↓	-	-	-	-	-	0%	0/20	< 1	63	53	86
5	198.212.215.2	Egress	Phillips-Van Heu:	Newark, New Jersey	United States	18725	Phillips-Van Heusen	0%	0/20	< 1	62	56	72
6	No Response	↓	-	-	-	-	-	100%	20/20	-1	-1	-1	-1
7	69.74.11.161	↓	Optimum WiFi	-	-	54004	Optimum WiFi	0%	0/20	12	75	67	87
8 - 10	No Response (3)	↓	-	-	-	-	-	100%	20/20	-1	-1	-1	-1
11	64.15.3.144	↓	-	-	-	-	-	0%	0/20	< 1	74	68	90
12	64.15.2.94	↓	-	-	-	-	-	0%	0/20	3	77	69	106
13	No Response	↓	-	-	-	-	-	100%	20/20	-1	-1	-1	-1
14	142.251.249.199	↓	Google	-	-	15169	Google	0%	0/20	1	79	71	94
15	216.239.40.167	↓	Google	-	-	15169	Google	0%	0/20	< 1	78	70	108
16	74.112.186.144	Application	Box.com	-	United States	396982	Box.com	0%	0/20	< 1	78	70	103

And the command line view shows similar details in a table format.

Drilling down even deeper we can look at the device health section.

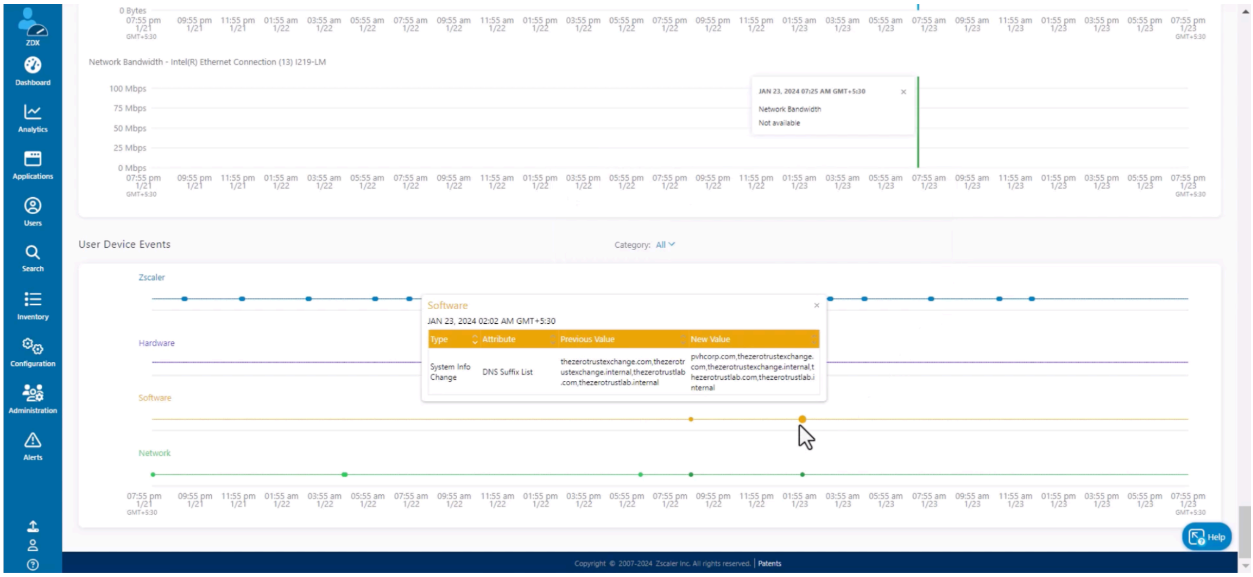
The graphs in this section are based on metrics that client connector collects on the end user device. There's a set of common graphs for things like CPU, memory, and disk usage.

And depending on the device the user was on at the time, additional metrics may be available. For example, for a Windows laptop, you'll see graphs for wifi signal strength, wifi network adapters, and battery usage.

Of course, you can customize which graphs you want to see and click on any graph point to correlate a change in one graph with all others.

And finally, there is the user device events section which tracks changes for the device, like restarts or changes in network activity.

These events are displayed in categories for Zscaler hardware, software, and network related events.



JAN 23, 2024 07:25 AM GMT+5:30

Network Bandwidth

Not available

Software

JAN 23, 2024 02:02 AM GMT+5:30

Type	Attribute	Previous Value	New Value
System Info Change	DNS Suffix List	thezerotrustexchange.com,thezerotrustexchange.internal,thezerotrustlab.com,thezerotrustlab.internal	pvhcorp.com,thezerotrustexchange.com,thezerotrustexchange.internal,thezerotrustlab.com,thezerotrustlab.internal

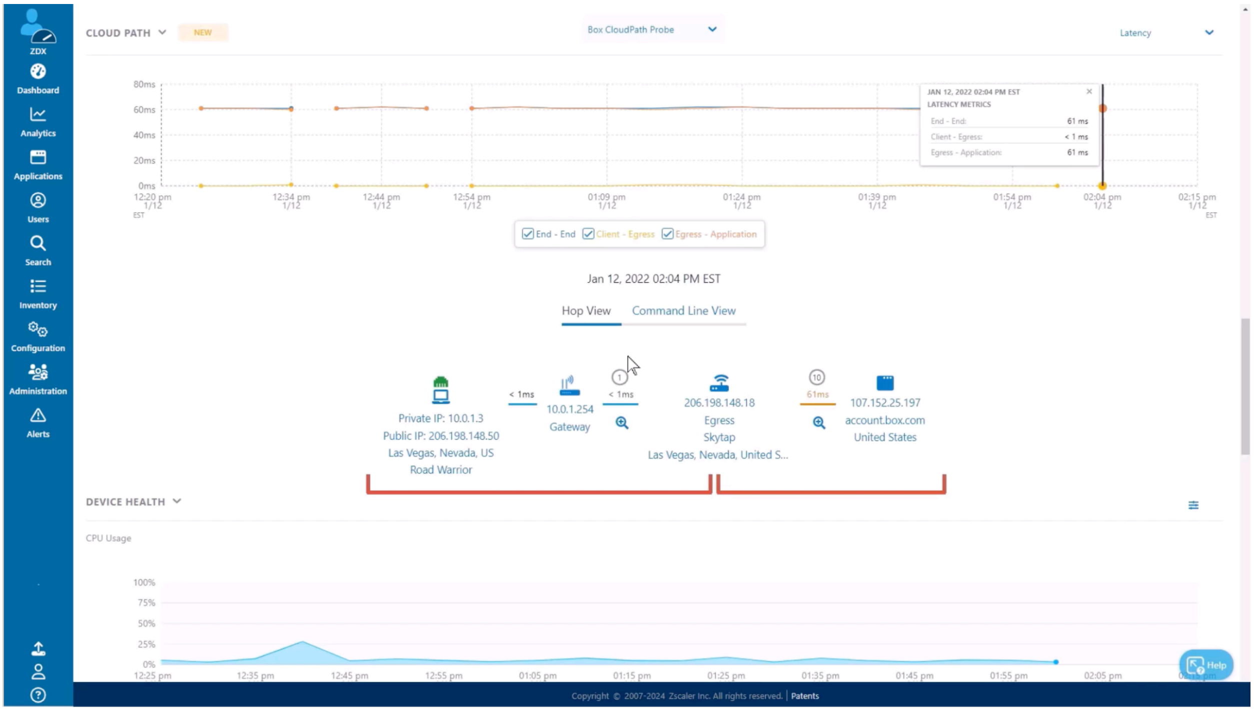
Simply move your mouse over an event to see more details.

Note that device attribute changes are tracked every five minutes. So if an attribute changed, and then reverted back within the five minutes, that change would not be displayed in this section.

To recap, the user's dashboard and user details page are full of information that help you decide if a user reported issue was caused by the application, a network problem, or the user's device.

Viewing Cloud Path Details

Back at the user details page we can take a closer look at the cloud path section.



JAN 12, 2022 02:04 PM EST
LATENCY METRICS
End - End: 61 ms
Client - Egress: < 1 ms
Egress - Application: 61 ms

Jan 12, 2022 02:04 PM EST

Private IP: 10.0.1.3
Public IP: 206.198.148.50
Las Vegas, Nevada, US
Road Warrior

10.0.1.254
Gateway

206.198.148.18
Egress
Skytap
Las Vegas, Nevada, United S...

107.152.25.197
account.box.com
United States

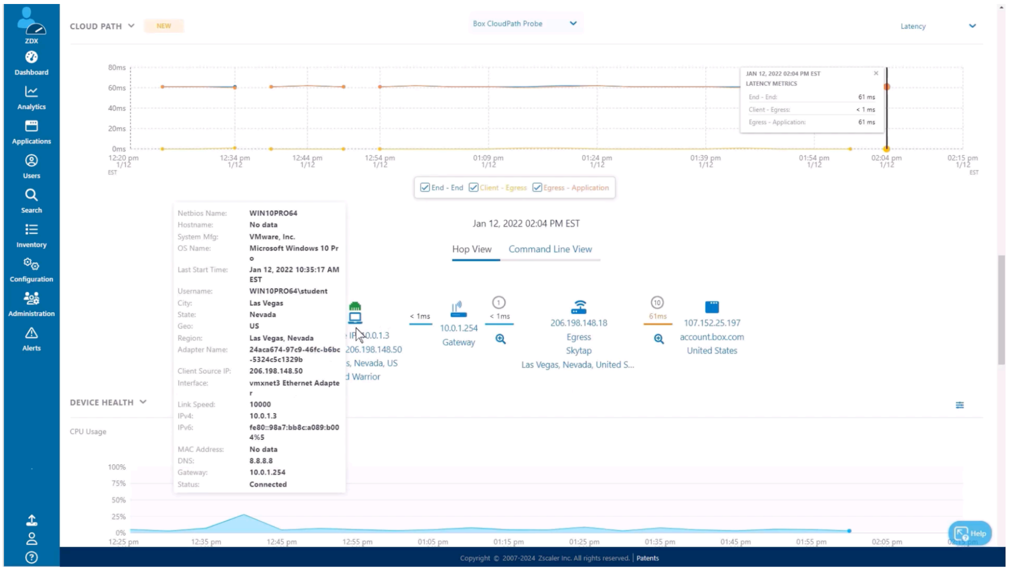
Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

First, there's the Cloud Path graph that shows latency or packet loss measure for the various legs of the data path between the end user device and application.

Then there is the Hop View that shows a graphical representation of the complete data path and all hops along the way. This view will differ depending on a user's traffic either going direct or through zscaler's zero trust exchange.

Let's first look at an example of a user accessing a SaaS application directly.

From the Zscaler client connector to the egress point, and from there to the application.



JAN 12, 2022 02:04 PM EST
LATENCY METRICS
End - End: 61 ms
Client - Egress: < 1 ms
Egress - Application: 61 ms

Jan 12, 2022 02:04 PM EST

Netbios Name: WIN10PRO64
Hostname: No data
System Mfg: VMware, Inc.
OS Name: Microsoft Windows 10 Pro
Last Start Time: Jan 12, 2022 10:35:17 AM EST
Username: WIN10PRO64\student
City: Las Vegas
State: Nevada
Geo: US
Region: Las Vegas, Nevada
Adapter Name: 24aca674-97c9-46fc-b6bc-5324c5c1329b
Client Source IP: 206.198.148.50
Interface: vmxnet3 Ethernet Adapter
Link Speed: 10000
IPv4: 10.0.1.3
IPv6: fe80::98a7:bb8c:a089:b004%5
MAC Address: No data
DNS: 8.8.8.8
Gateway: 10.0.1.254
Status: Connected

IP: 10.0.1.3
206.198.148.50
s, Nevada, US
d Warrior

10.0.1.254
Gateway

206.198.148.18
Egress
Skytap
Las Vegas, Nevada, United S...

107.152.25.197
account.box.com
United States

Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

When you hover your mouse over any of the individual hops, you'll get details such as device information, the service provider, latency, and packet loss metrics.

Differential latency is shown over the different legs of the cloud path, and the leg with the highest latency is displayed in orange.

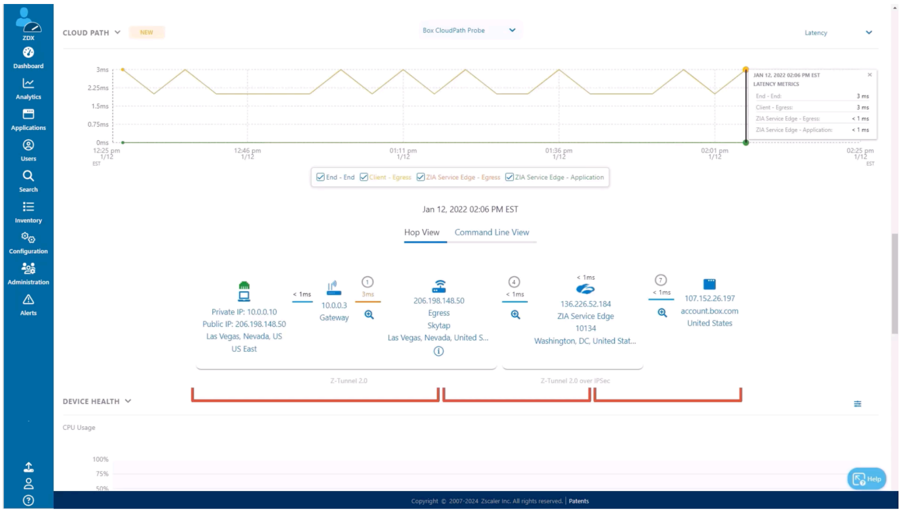
You can expand the view of each leg and quickly identify the hop with the highest latency.

Connections from ZIA are displayed in three legs:

1. From the user device to the egress point.
2. From the egress point to the ZIA public service edge.
3. From the ZIA public service edge to the application.

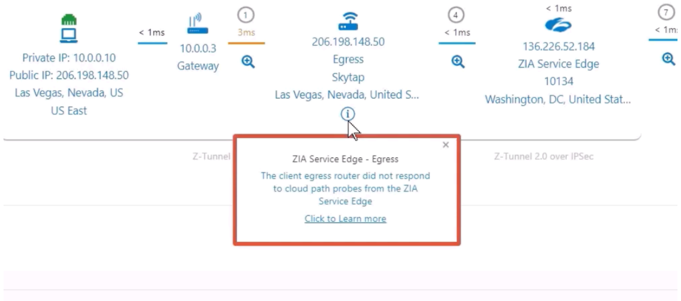
For each ZIA public service edge, Hop View also displays an internal hash value that will help Zscaler support, locate and troubleshoot any issues with the Zscaler cloud itself.

If there are any errors in the cloud path, you will see icons below a hop that indicate informational messages, warnings, or critical errors.



JAN 12, 2022 02:06 PM EST
LATENCY METRICS

End - End:	3 ms
Client - Egress:	3 ms
ZIA Service Edge - Egress:	< 1 ms
ZIA Service Edge - Application:	< 1 ms



ZIA Service Edge - Egress

The client egress router did not respond to cloud path probes from the ZIA Service Edge

Click to Learn more

Clicking the icon will display a message. The ZDX help portal provides an extensive list of these messages, including a description and suggested actions.

Nex is the command line view. This view is similar to the output from a traceroute command. The column on the left shows the IP address of all hops.

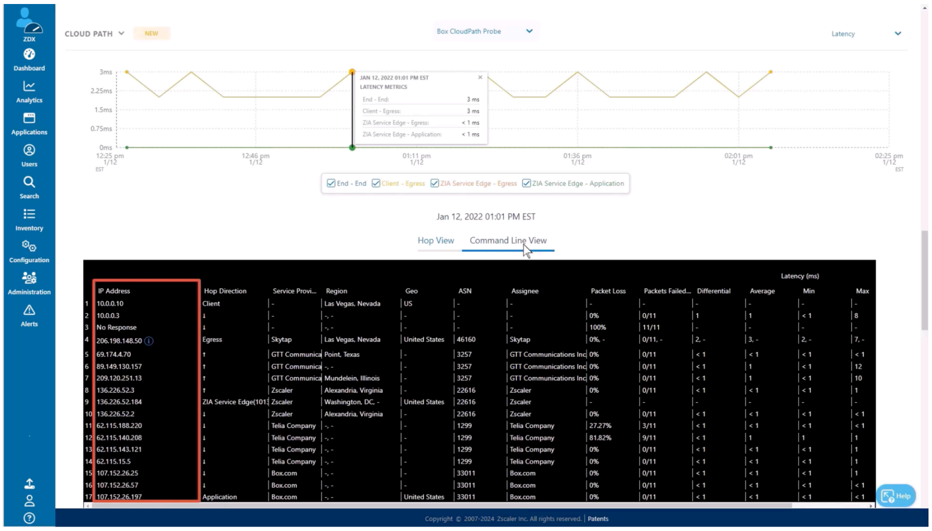
Similar to Hop View, any error or warning icons are displayed next to the IP address.

The hop direction, from the client to your egress IP, from ZIA public or private service edges to your egress IP, and from service edges to destination is indicated by up and down arrows.

Then there is geo information, ISP names, regions, and zscaler locations, which are derived from device location information and from an extensive database.

Other parameters displayed in this view include packet loss, packets failed, as well as latency metrics.

One thing to note here is packet loss metrics on intermediate nodes. For example, Internet backbone nodes should be used carefully because they may depend on how these nodes handle traceroute packets.



Jan 12, 2022 01:01 PM EST

											Latency (ms)	
	IP Address	Hop Direction	Service Provi...	Region	Geo	ASN	Assignee	Packet Loss	Packets Failed...	Differential	Average	Min	Max
1	10.0.0.10	Client	-	Las Vegas, Nevada	US	-	-	-	-	-	-	-	-
2	10.0.0.3	↓	-	-, -	-	-	-	0%	0/11	1	1	< 1	8
3	No Response	↓	-	-, -	-	-	-	100%	11/11	-	-	-	-
4	206.198.148.50 ⓘ	Egress	Skytap	Las Vegas, Nevada	United States	46160	Skytap	0%, -	0/11, -	2, -	3, -	2, -	7, -
5	69.174.4.70	↑	GTT Communica	Point, Texas	-	3257	GTT Communications Inc	0%	0/11	< 1	< 1	< 1	< 1
6	89.149.130.157	↑	GTT Communica	-, -	-	3257	GTT Communications Inc	0%	0/11	< 1	1	< 1	12
7	209.120.251.13	↑	GTT Communica	Mundelein, Illinois	-	3257	GTT Communications Inc	0%	0/11	< 1	1	< 1	10
8	136.226.52.3	↑	Zscaler	Alexandria, Virginia	-	22616	Zscaler	0%	0/11	< 1	< 1	< 1	1
9	136.226.52.184	ZIA Service Edge(101	Zscaler	Washington, DC, -	United States	22616	Zscaler	-	-	-	-	-	-
10	136.226.52.2	↓	Zscaler	Alexandria, Virginia	-	22616	Zscaler	0%	0/11	< 1	< 1	< 1	< 1
11	62.115.188.220	↓	Telia Company	-, -	-	1299	Telia Company	27.27%	3/11	< 1	< 1	< 1	< 1
12	62.115.140.208	↓	Telia Company	-, -	-	1299	Telia Company	81.82%	9/11	< 1	1	1	1
13	62.115.143.121	↓	Telia Company	-, -	-	1299	Telia Company	0%	0/11	< 1	< 1	< 1	1
14	62.115.15.5	↓	Telia Company	-, -	-	1299	Telia Company	0%	0/11	< 1	< 1	< 1	1
15	107.152.26.25	↓	Box.com	-, -	-	33011	Box.com	0%	0/11	< 1	< 1	< 1	1
16	107.152.26.57	↓	Box.com	-, -	-	33011	Box.com	0%	0/11	< 1	< 1	< 1	< 1
17	107.152.26.197	Application	Box.com	-, -	United States	33011	Box.com	0%	0/11	< 1	< 1	< 1	< 1

And this example shows what Hop View is like when accessing an internal application via Zscaler private access, the cloud path will show information about the tunnel, ZPA service edge, and app connector details, but with additional legs:

1. From the user device to the egress point of the customer network.
2. From the egress point to the ZPA service edge.
3. From ZPA service edge to an app connector, and four from the app connector to the application.

Depending on how traffic is being forwarded, you may see additional legs. For example, if you have configured a path for internal application traffic through the ZIA public service edge, then both the ZIA and ZPA public service edges will be shown in Hop View.

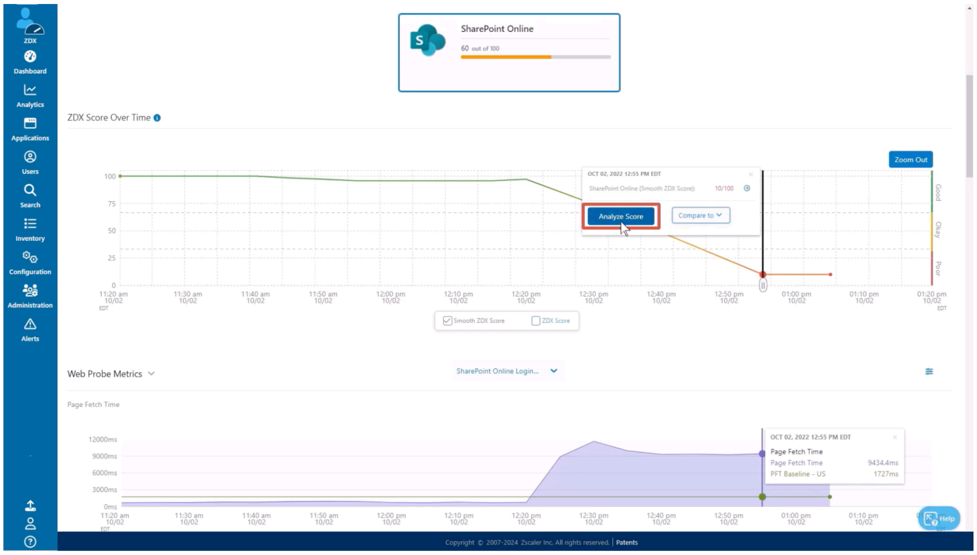
To recap, the Cloud Path graph, Hop View and command line view are powerful tools to help you quickly identify if a reported issue is at the user local network, their ISP, or the internet, the application they're accessing or even within the Zscaler cloud itself.

Viewing Automated Root Cause Analysis Data

ZDX collects a tremendous amount of data for a user's experience with business critical applications. But sifting through all this data can be quite time consuming, and time is the one thing that's crucial when it comes to troubleshooting problems.

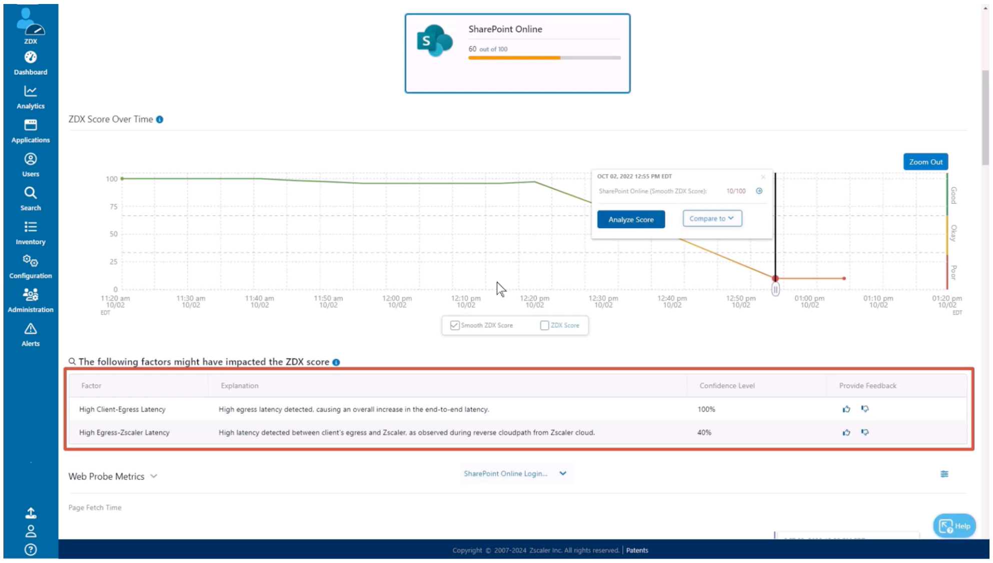
With **AI powered root cause analysis**, ZDX speeds up analysis from hours to seconds by instantly exposing the root cause of poor user experience.

Let's see how this works. In the ZDX score over time graph, on a user detail page, select a point in the graph with a poor score, and then simply click **analyze score**.



ZDX processes multiple signals to identify the root cause and lists factors that may have contributed to the poor score.

For each of the factors, you also get an explanation, and the confidence level quantifies the accuracy of the analysis based on probes with similar issues.



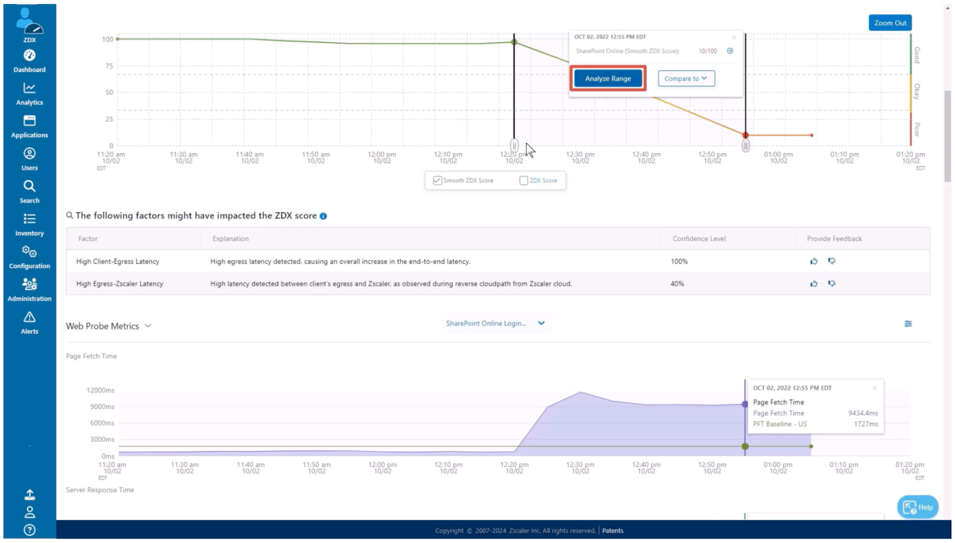
The following factors might have impacted the ZDX score

Factor	Explanation	Confidence Level	Provide Feedback
High Client-Egress Latency	High egress latency detected, causing an overall increase in the end-to-end latency.	100%	👍 👎
High Egress-Zscaler Latency	High latency detected between client's egress and Zscaler, as observed during reverse cloudpath from Zscaler cloud.	40%	👍 👎

You can now scan the other graphs on this page to confirm the suggested root cause. In this example, the automated root cause analysis for the poor SharePoint score, suggests high latency somewhere between the user's network and the Zscaler public service edge. A closer look at the latency values in the Cloud Path graph, and Hop View confirm the likely cause. The spike in the end to end latency is almost entirely caused by one hop.

Back of the root cause analysis pop up, you can now provide feedback and let Zscaler know if the analysis for the low score was helpful, or if the analysis was not accurate and the low scores related to a different issue.

In addition to analyzing the score for one specific point in time, the ZDX score over time graph also includes an option to analyze scores within a time range. Simply move the slider to specify a time frame. And then click analyze range.

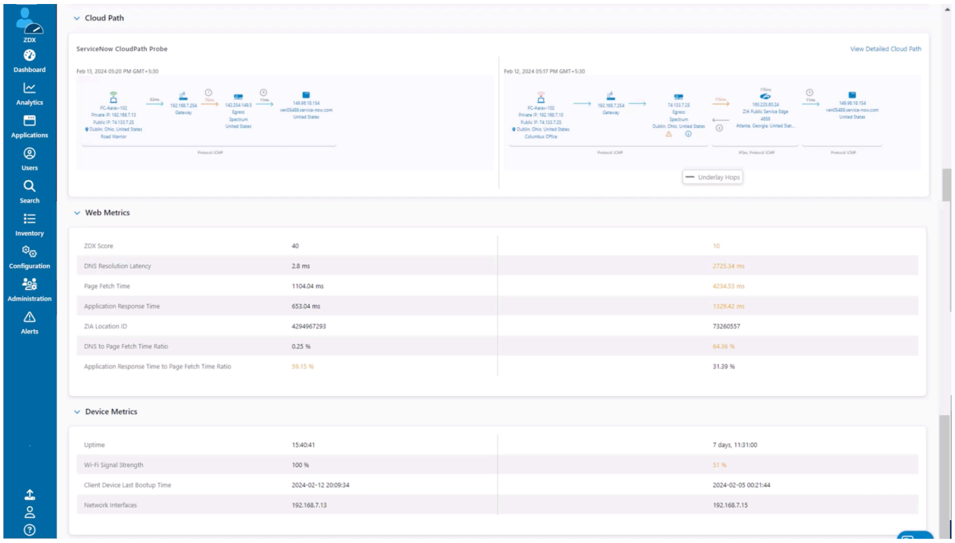


The following factors might have impacted the ZDX score

Factor	Explanation	Confidence Level	Provide Feedback
High Client-Egress Latency	High egress latency detected, causing an overall increase in the end-to-end latency.	100%	👍 👎
High Egress-Zscaler Latency	High latency detected between client's egress and Zscaler, as observed during reverse cloudpath from Zscaler cloud.	40%	👍 👎

As before, the automated root cause analysis will display potential factors that may have contributed to the low scores within your specified time range.

And the third option is to compare ZDX Scores for an application to understand why they might vary at different points in time. A score comparison can highlight why a current score might be considerably different from a previous score. As always, you can review web, device, and cloud path metrics to help determine differences in scoring. This way, you can quickly identify what changed from when everything was working fine.



Web Metrics

ZDX Score	40	10
DNS Resolution Latency	2.8 ms	2725.34 ms
Page Fetch Time	1104.04 ms	4234.53 ms
Application Response Time	653.04 ms	1329.42 ms
ZIA Location ID	4294967293	73260557
DNS to Page Fetch Time Ratio	0.25 %	64.36 %
Application Response Time to Page Fetch Time Ratio	59.15 %	31.39 %

Device Metrics

Uptime	15:40:41	7 days, 11:31:00
Wi-Fi Signal Strength	100 %	51 %
Client Device Last Bootup Time	2024-02-12 20:09:34	2024-02-05 00:21:44
Network Interfaces	192.168.7.13	192.168.7.15

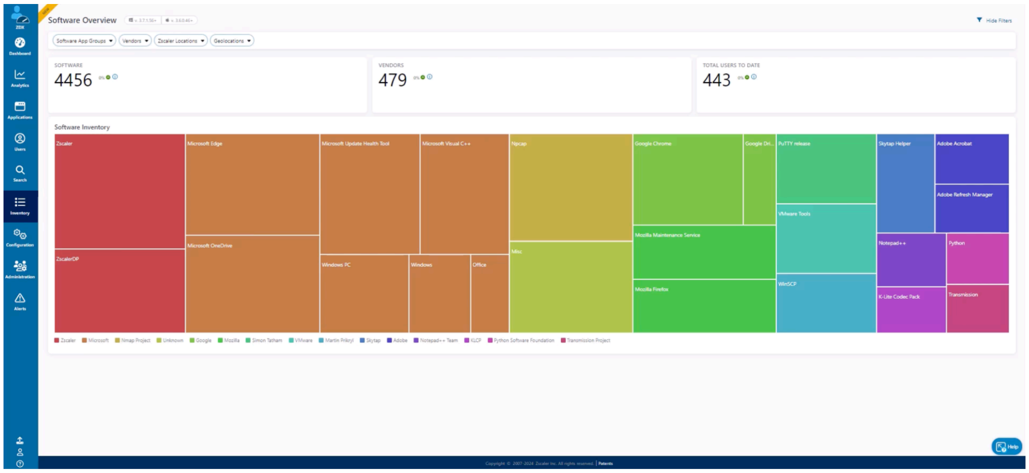
To recap, ZDX uses machine learning to process multiple signals from past experiences, predict the root cause of an issue, and offers IT teams the ability to provide feedback on its conclusions.

Device, Software & Process Inventory Information

With hundreds or even thousands of end users in your organization, it can be difficult to keep track of all the software and hardware deployed on their devices. That's where ZDX inventory comes in. It helps you fully understand your software port and versions deployed across your organization and on each device.

Software Inventory

Let's start with a closer look at the **software inventory**, which allows you to view current and historical information about software versions and updates on your user's devices.



Software Overview

Software App Groups ▾ | Vendors ▾ | Zscaler Locations ▾ | Geolocations ▾

SOFTWARE 4456 0%

VENDORS 479 0%

TOTAL USERS TO DATE 443 0%

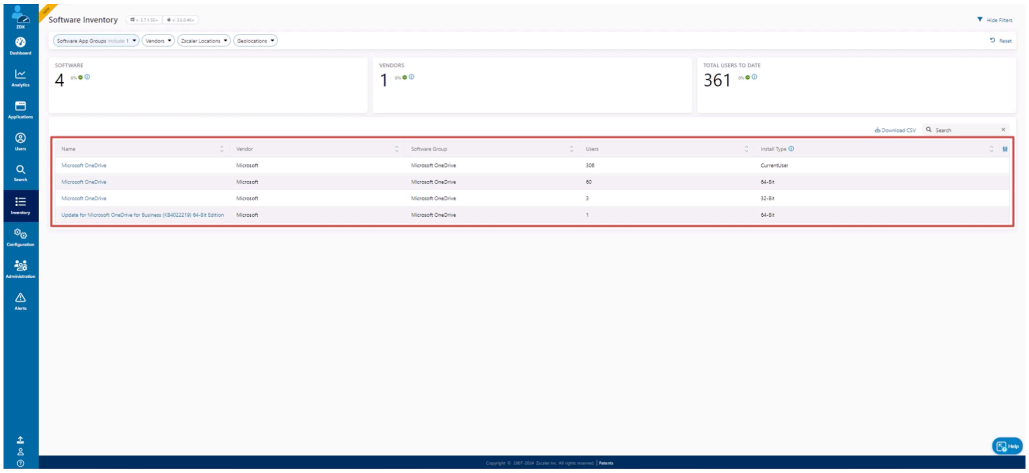
Software Inventory

The software overview page provides a high level summary of your organization's software inventory.

The filters along the top help you to quickly find specific software or applications and select the associated color coded tile. The widgets below show the current count for installed software, vendors, and users. And the percentage in each card indicates how the count has increased or decreased over the past twenty four hours.

Installed software and applications are grouped and color coded according to their vendors. With the size of each tile visually indicating the number of installations per software or application relative to other software or applications installed on user devices.

Clicking one of these tiles will display a detailed inventory list for that software.



Software Inventory

Software App Groups Include 1 ▾ | Vendors ▾ | Zscaler Locations ▾ | Geolocations ▾

SOFTWARE 4 0%

VENDORS 1 0%

TOTAL USERS TO DATE 361 0%

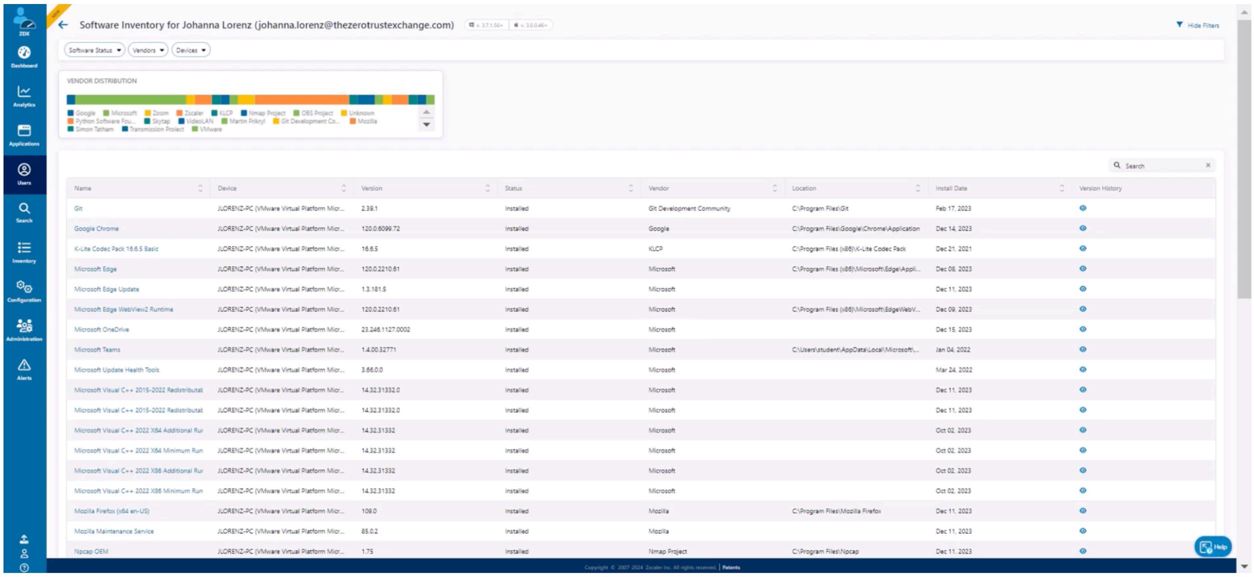
Name	Vendor	Software Group	Users	Install Type
Microsoft OneDrive	Microsoft	Microsoft OneDrive	306	CurrentUser
Microsoft OneDrive	Microsoft	Microsoft OneDrive	60	64-Bit
Microsoft OneDrive	Microsoft	Microsoft OneDrive	3	32-Bit
Update for Microsoft OneDrive for Business (KB4022219) 64-Bit Edition	Microsoft	Microsoft OneDrive	1	64-Bit

The software inventory page provides a current snapshot of your users, installed applications and software, including details like Vendor, Software Group, Users, and install type.

You can drill down further simply by selecting an application in the table. The software details page lists all the users and devices that have this software installed.

And you can even zoom in on one specific user and display a detailed list of the installed software on the user's device.

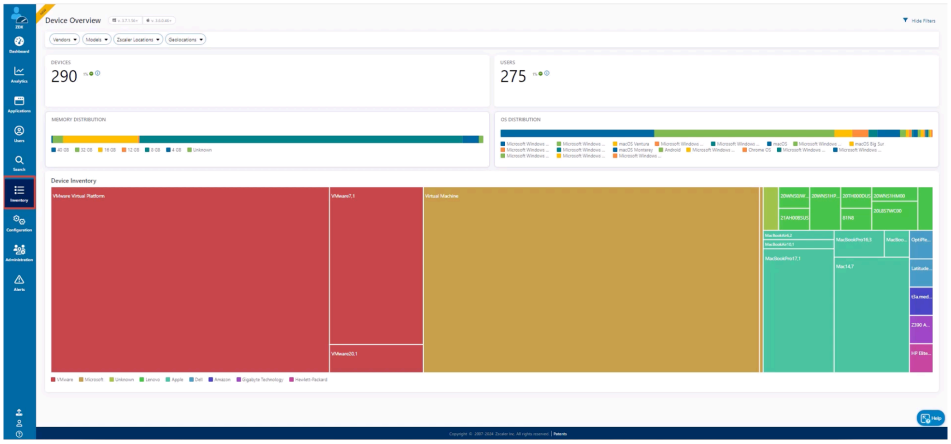
Clicking the version history column displays the date when the software version was last updated.



Software Inventory for Johanna Lorenz (johanna.lorenz@thezerotrustexchange.com)

Name	Device	Version	Status	Vendor	Location	Install Date	Version History
Git	JLORENZ-PC (VMware Virtual Platform Micr...	2.39.1	Installed	Git Development Community	C:\Program Files\Git	Feb 17, 2023	●
Google Chrome	JLORENZ-PC (VMware Virtual Platform Micr...	120.0.6099.72	Installed	Google	C:\Program Files\Google\Chrome\Application	Dec 14, 2023	●
K-Lite Codec Pack 16.6.5 Basic	JLORENZ-PC (VMware Virtual Platform Micr...	16.6.5	Installed	KLCP	C:\Program Files (x86)\K-Lite Codec Pack	Dec 21, 2021	●
Microsoft Edge	JLORENZ-PC (VMware Virtual Platform Micr...	120.0.2210.61	Installed	Microsoft	C:\Program Files (x86)\Microsoft\Edge\Appli...	Dec 08, 2023	●
Microsoft Edge Update	JLORENZ-PC (VMware Virtual Platform Micr...	1.3.181.5	Installed	Microsoft		Dec 11, 2023	●
Microsoft Edge WebView2 Runtime	JLORENZ-PC (VMware Virtual Platform Micr...	120.0.2210.61	Installed	Microsoft	C:\Program Files (x86)\Microsoft\EdgeWebV...	Dec 09, 2023	●
Microsoft OneDrive	JLORENZ-PC (VMware Virtual Platform Micr...	23.246.1127.0002	Installed	Microsoft		Dec 15, 2023	●
Microsoft Teams	JLORENZ-PC (VMware Virtual Platform Micr...	1.4.00.32771	Installed	Microsoft	C:\Users\student\AppData\Local\Microsoft\...	Jan 04, 2022	●
Microsoft Update Health Tools	JLORENZ-PC (VMware Virtual Platform Micr...	3.66.0.0	Installed	Microsoft		Mar 24, 2022	●
Microsoft Visual C++ 2015-2022 Redistributat	JLORENZ-PC (VMware Virtual Platform Micr...	14.32.31332.0	Installed	Microsoft		Dec 11, 2023	●
Microsoft Visual C++ 2015-2022 Redistributat	JLORENZ-PC (VMware Virtual Platform Micr...	14.32.31332.0	Installed	Microsoft		Dec 11, 2023	●
Microsoft Visual C++ 2022 X64 Additional Rur	JLORENZ-PC (VMware Virtual Platform Micr...	14.32.31332	Installed	Microsoft		Oct 02, 2023	●
Microsoft Visual C++ 2022 X64 Minimum Run	JLORENZ-PC (VMware Virtual Platform Micr...	14.32.31332	Installed	Microsoft		Oct 02, 2023	●
Microsoft Visual C++ 2022 X86 Additional Rur	JLORENZ-PC (VMware Virtual Platform Micr...	14.32.31332	Installed	Microsoft		Oct 02, 2023	●
Microsoft Visual C++ 2022 X86 Minimum Run	JLORENZ-PC (VMware Virtual Platform Micr...	14.32.31332	Installed	Microsoft		Oct 02, 2023	●
Mozilla Firefox (x64 en-US)	JLORENZ-PC (VMware Virtual Platform Micr...	109.0	Installed	Mozilla	C:\Program Files\Mozilla Firefox	Dec 11, 2023	●
Mozilla Maintenance Service	JLORENZ-PC (VMware Virtual Platform Micr...	85.0.2	Installed	Mozilla		Dec 11, 2023	●
Npcap OEM	JLORENZ-PC (VMware Virtual Platform Micr...	1.75	Installed	Nmap Project	C:\Program Files\Npcap	Dec 11, 2023	●

Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents



Device Inventory

The **device inventory** shows similar summary and detail pages for your organization's devices and their associated users. Here is a look at the device inventory page with filter options, summary widgets, and tiles representing operating systems and their associated devices.

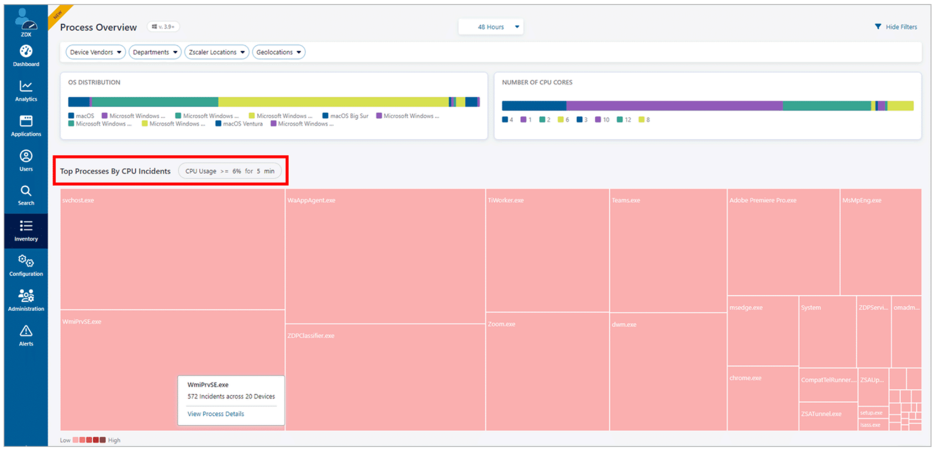
As before, you can click on any of the tiles to go to the device inventory page that provides a current snapshot of your user's devices, including hardware details like processed models and the amount of RAM installed on the device. Clicking on the device name lets you view hardware, network, and software details for the device.

To recap, ZDX inventory data collection gives you easy to navigate snapshots of your organization's software and hardware inventory.

Process Inventory

Similar to the overview and inventory graphs for software and hardware, the Process Overview page shows summary information about software processes, specifically incidents when a configurable CPU usage threshold was exceeded. Clicking a tile on the Overview page shows details about a specific process. The Process Inventory page lists the number of CPU Incidents that exceed the CPU Usage threshold (e.g., CPU Usage > 10%) for a duration of 5 minutes. Clicking any of the top processes drills down into the process details page, which provides a graph that shows the CPU usage percentage in conjunction with the number of associated user devices.

View the top processes for CPU usage incidents based on the configured threshold. These processes have exceeded the threshold within a 5-minute interval, and are color-coded according to the number of incidents.



Process Overview

48 Hours

Top Processes By CPU Incidents

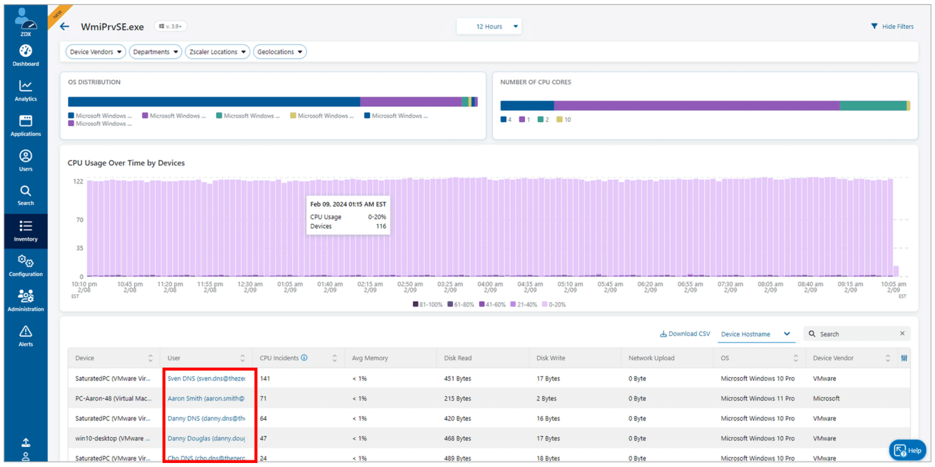
CPU Usage >= 6% for 5 min

WmiPrvSE.exe

572 Incidents across 20 Devices

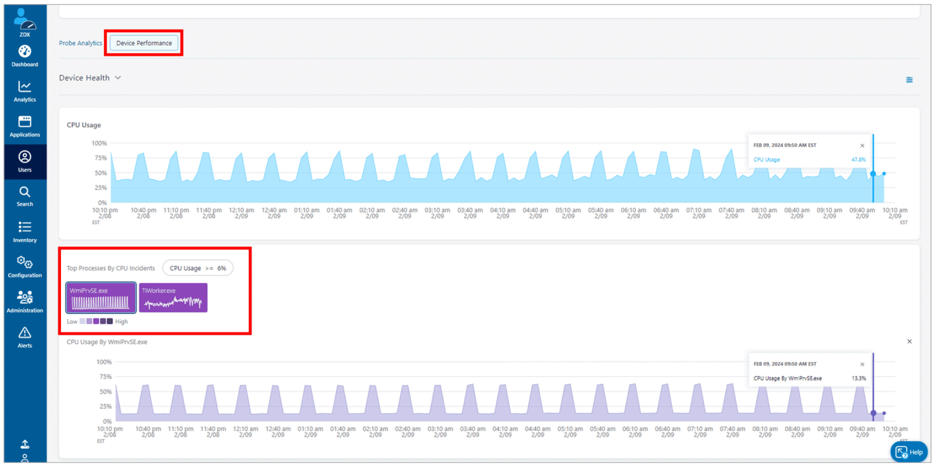
View Process Details

The Process Details page provides a graph that shows the CPU usage percentage in conjunction with the number of associated user devices. From here, you can zero in on a specific user.

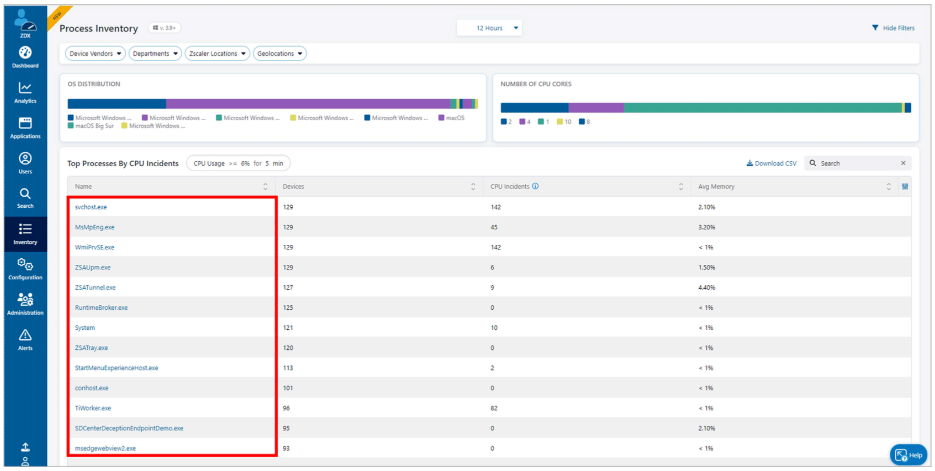


Device	User	CPU Incidents	Avg Memory	Disk Read	Disk Write	Network Upload	OS	Device Vendor
SaturatedPC (VMware Vir...	Sven DNS (sven.dns@thezei	141	< 1%	451 Bytes	17 Bytes	0 Byte	Microsoft Windows 10 Pro	VMware
PC-Aaron-48 (Virtual Mac...	Aaron Smith (aaron.smith@	71	< 1%	215 Bytes	2 Bytes	0 Byte	Microsoft Windows 11 Pro	Microsoft
SaturatedPC (VMware Vir...	Danny DNS (danny.dns@th	64	< 1%	420 Bytes	16 Bytes	0 Byte	Microsoft Windows 10 Pro	VMware
win10-desktop (VMware ...	Danny Douglas (danny.dou	47	< 1%	468 Bytes	17 Bytes	0 Byte	Microsoft Windows 10 Pro	VMware
SaturatedPC (VMware Vir...	Cho DNS (cho.dns@thezerc	24	< 1%	489 Bytes	18 Bytes	0 Byte	Microsoft Windows 10 Pro	VMware

On the User Details page, Click Device Performance to view Device Health metrics for the selected device. If more than one process is shown for the device, you can select a process to view its percentage of CPU usage within your set time range.



The Process Inventory page provides a current snapshot of CPU usage that has exceeded the threshold on user devices.



Name	Devices	CPU Incidents	Avg Memory
svchost.exe	129	142	2.10%
MsMpEng.exe	129	45	3.20%
WmiPrvSE.exe	129	142	< 1%
ZSAUpm.exe	129	6	1.50%
ZSATunnel.exe	127	9	4.40%
RuntimeBroker.exe	125	0	< 1%
System	121	10	< 1%
ZSATray.exe	120	0	< 1%
StartMenuExperienceHost.exe	113	2	< 1%
conhost.exe	101	0	< 1%
TiWorker.exe	96	82	< 1%
SDCenterDeceptionEndpointDemo.exe	95	0	2.10%
msedgewebview2.exe	93	0	< 1%

Deep Tracing Session Results

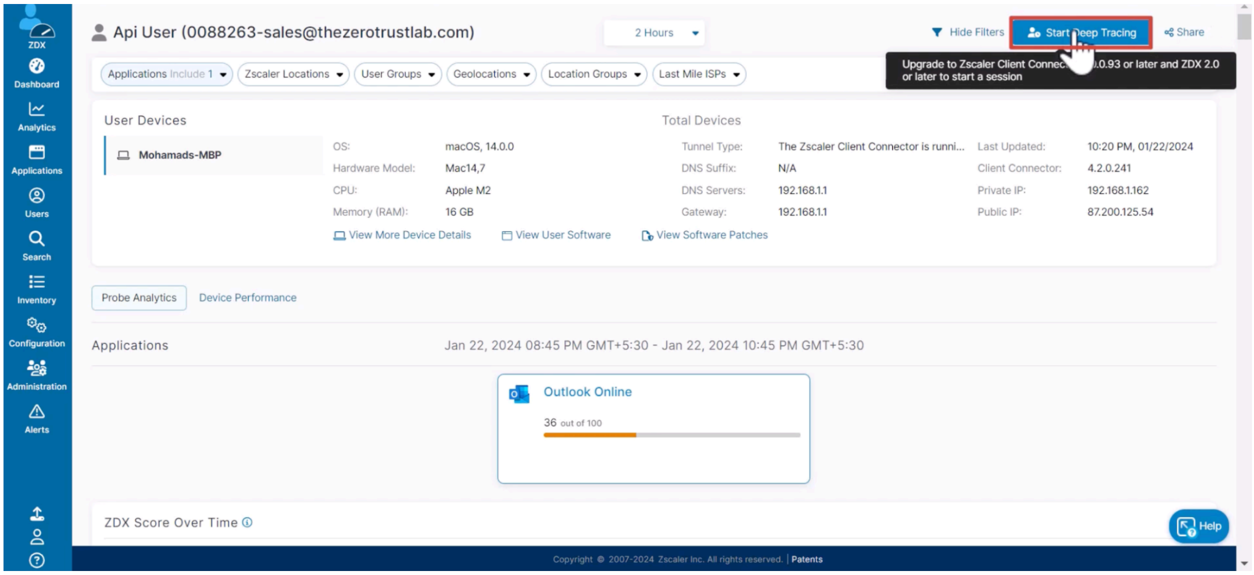
During a Deep Tracing session, metrics are collected every minute for Web and Cloud Path Probes, and every 5 minutes for device statistics. In this section, we will look at the results of a Deep Tracing session, which provides much **more granular information to analyze end user issues**. The biggest benefit of a Deep Tracing session is that it also collects process-level information for a user.

Imagine that an employee in your company's finance department contacts the IT help desk to complain about poor performance when trying to access Outlook online.

A quick check of the ZDX dashboard confirms that this is not a global or regional issue. That's good news for all other users, but you still have to find out what causes the one employed to have a poor experience.

Now what?

To start, you can filter the user overview page to zero in on Outlook and the employee that reported the issue. Scrolling through the user details page is a good first step when trying to troubleshoot the issue. But you also have the option to start a deep tracing session and collect more granular information.



Api User (0088263-sales@thezerotrustlab.com)

Upgrade to Zscaler Client Connec .0.93 or later and ZDX 2.0 or later to start a session

User Devices

Mohamads-MBP

OS: macOS, 14.0.0
Hardware Model: Mac14,7
CPU: Apple M2
Memory (RAM): 16 GB

Total Devices

Tunnel Type: The Zscaler Client Connector is runni...
DNS Suffix: N/A
DNS Servers: 192.168.1.1
Gateway: 192.168.1.1

Last Updated: 10:20 PM, 01/22/2024
Client Connector: 4.2.0.241
Private IP: 192.168.1.162
Public IP: 87.200.125.54

View More Device Details
View User Software
View Software Patches

Applications Jan 22, 2024 08:45 PM GMT+5:30 - Jan 22, 2024 10:45 PM GMT+5:30

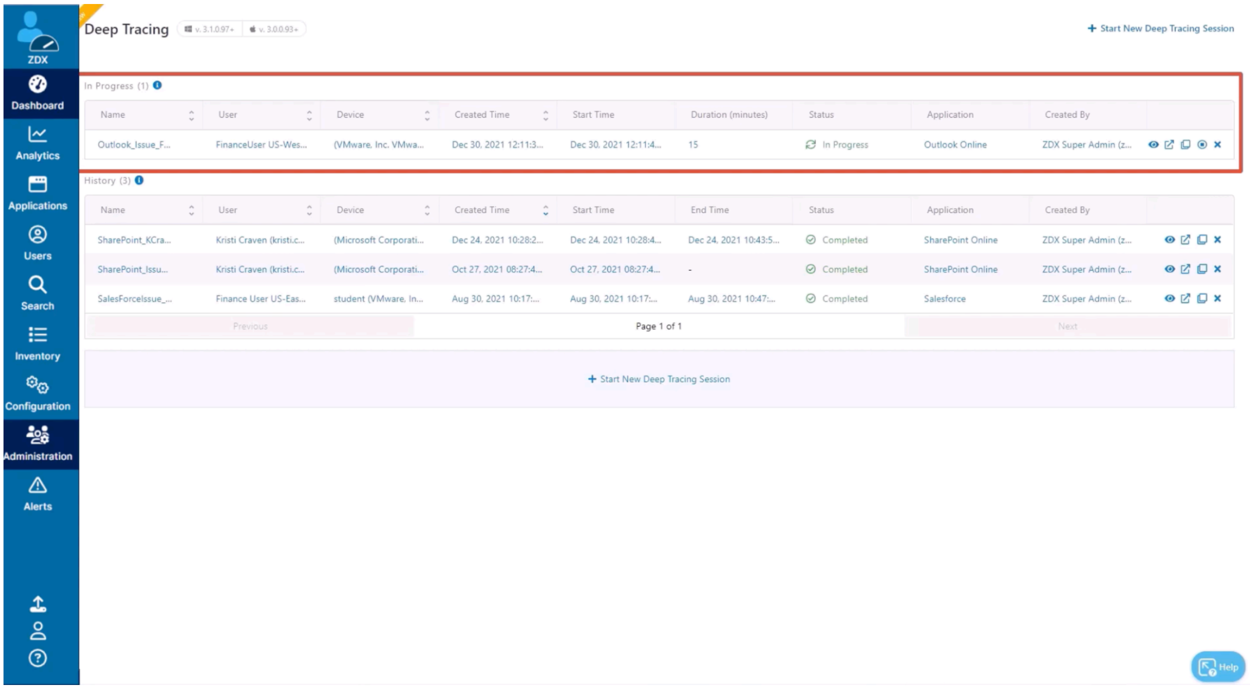
Outlook Online
36 out of 100

ZDX Score Over Time

Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

Once started, the session is shown in the in progress table on the deep tracing page, where data forward in progress sessions is updated every minute and can be viewed by clicking on the eye icon.

After the session is completed, it will be listed in the history tab From here, you can select one session to view the captured data.



In Progress (1)

Name	User	Device	Created Time	Start Time	Duration (minutes)	Status	Application	Created By
Outlook_Issue_F...	FinanceUser US-Wes...	(VMware, Inc. VMwa...	Dec 30, 2021 12:11:3...	Dec 30, 2021 12:11:4...	15	In Progress	Outlook Online	ZDX Super Admin (z...

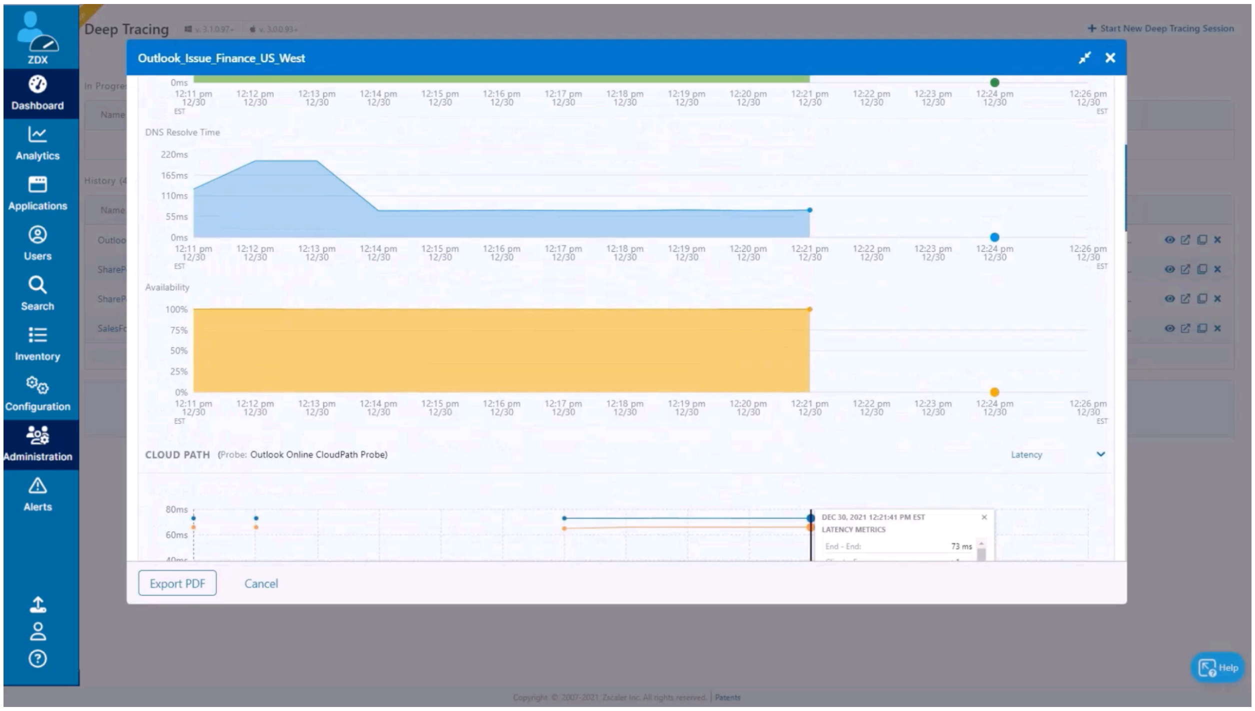
History (3)

Name	User	Device	Created Time	Start Time	End Time	Status	Application	Created By
SharePoint_KCra...	Kristi Craven (kristi.c...	(Microsoft Corporati...	Dec 24, 2021 10:28:2...	Dec 24, 2021 10:28:4...	Dec 24, 2021 10:43:5...	Completed	SharePoint Online	ZDX Super Admin (z...
SharePoint_Issu...	Kristi Craven (kristi.c...	(Microsoft Corporati...	Oct 27, 2021 08:27:4...	Oct 27, 2021 08:27:4...	-	Completed	SharePoint Online	ZDX Super Admin (z...
SalesForceIssue_...	Finance User US-Eas...	student (VMware, In...	Aug 30, 2021 10:17:...	Aug 30, 2021 10:17:...	Aug 30, 2021 10:47:...	Completed	Salesforce	ZDX Super Admin (z...

Previous Page 1 of 1 Next

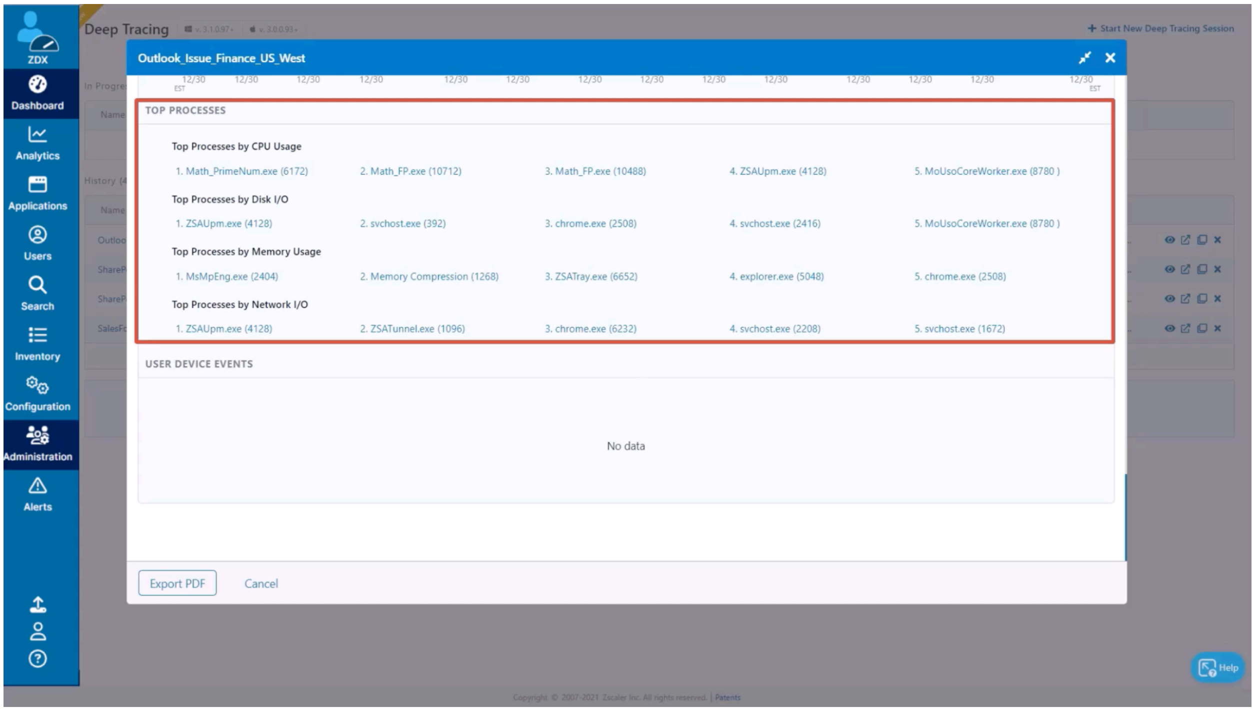
+ Start New Deep Tracing Session

Scrolling through the various graphs, you'll see that the session results show web probe, cloud path, and device health metrics similar to the graphs in the user details page. You can also zero in on one specific graph point. For example, a spike in CPU utilization.



This will display an additional pop up showing the top software processes that are consuming resources by memory usage, CPU usage, disk usage, and network usage.

When you scroll down to the bottom of the page, you'll get a similar listing of the top processes with their process IDs shown in brackets.



Outlook_Issue_Finance_US_West

TOP PROCESSES

Top Processes by CPU Usage

1. Math_PrimeNum.exe (6172) 2. Math_FP.exe (10712) 3. Math_FP.exe (10488) 4. ZSAUpm.exe (4128) 5. MoUsoCoreWorker.exe (8780)

Top Processes by Disk I/O

1. ZSAUpm.exe (4128) 2. svchost.exe (392) 3. chrome.exe (2508) 4. svchost.exe (2416) 5. MoUsoCoreWorker.exe (8780)

Top Processes by Memory Usage

1. MsMpEng.exe (2404) 2. Memory Compression (1268) 3. ZSATray.exe (6652) 4. explorer.exe (5048) 5. chrome.exe (2508)

Top Processes by Network I/O

1. ZSAUpm.exe (4128) 2. ZSATunnel.exe (1096) 3. chrome.exe (6232) 4. svchost.exe (2208) 5. svchost.exe (1672)

USER DEVICE EVENTS

No data

Finally, you can export the results of your session to a PDF file and download it for further analysis.

To recap, deep tracing results provide granular web probe and cloud metrics along with device health, device events, and a list of top processes. Reviewing this data simplifies your troubleshooting process and reduces the time needed to close support tickets.

Alerts Page

The dashboards and graphs we looked at so far are powerful tools to troubleshoot user-reported problems. Alerts on the other hand allow you to be proactive and get notifications of potential service degradations **before** users start opening support tickets.

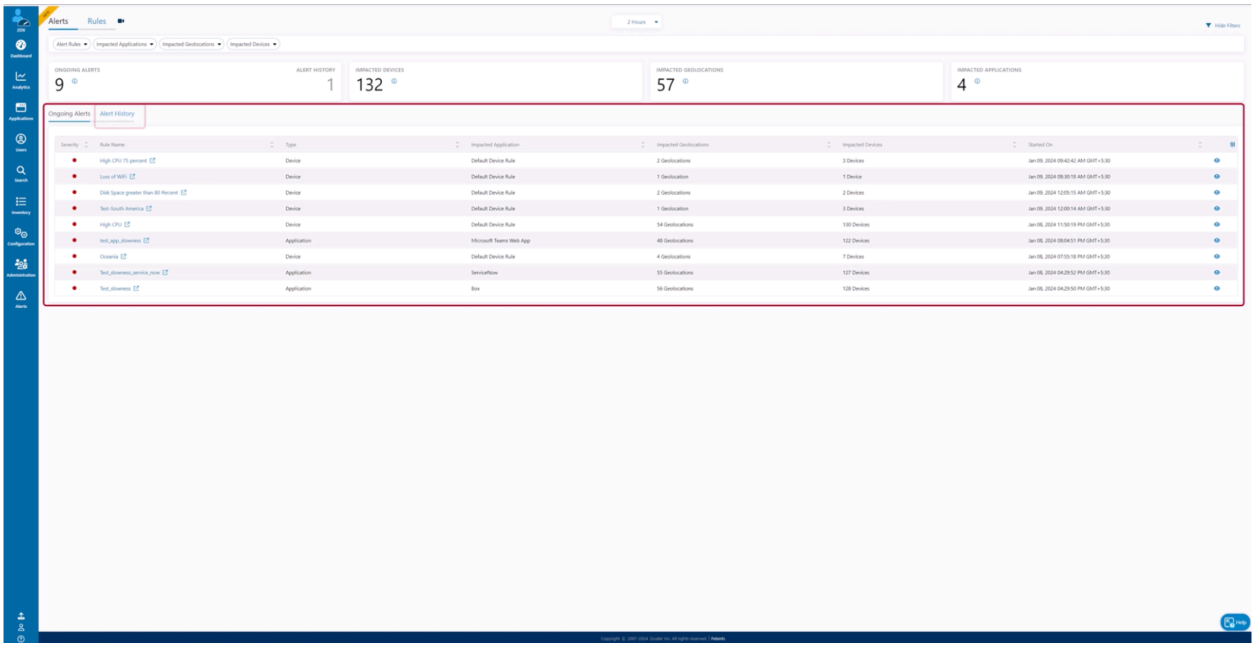
For example, you could create an alert that is triggered whenever the ZDX Score for a business-critical application drops below 40.

The Alerts Page lists both active and historical alerts, and lets you manage alert rules; **all in one place**.

In their day to day operations, IT support teams will get ZDX alert modifications via webhooks or email. But you can always view alerts in the ZDX admin portal by selecting alerts from the main menu. Similar to other ZDX dashboards, there are filters at the top of the page that allow you to zero in on a subset of alerts.

Next, there are overview widgets that show the number of ongoing and historical alerts, as well as the number of impacted devices, geolocations, and applications.

And the information in the table below is organized into ongoing alerts and alert history.



ONGOING ALERTS 9 ALERT HISTORY 1

IMPACTED DEVICES 132

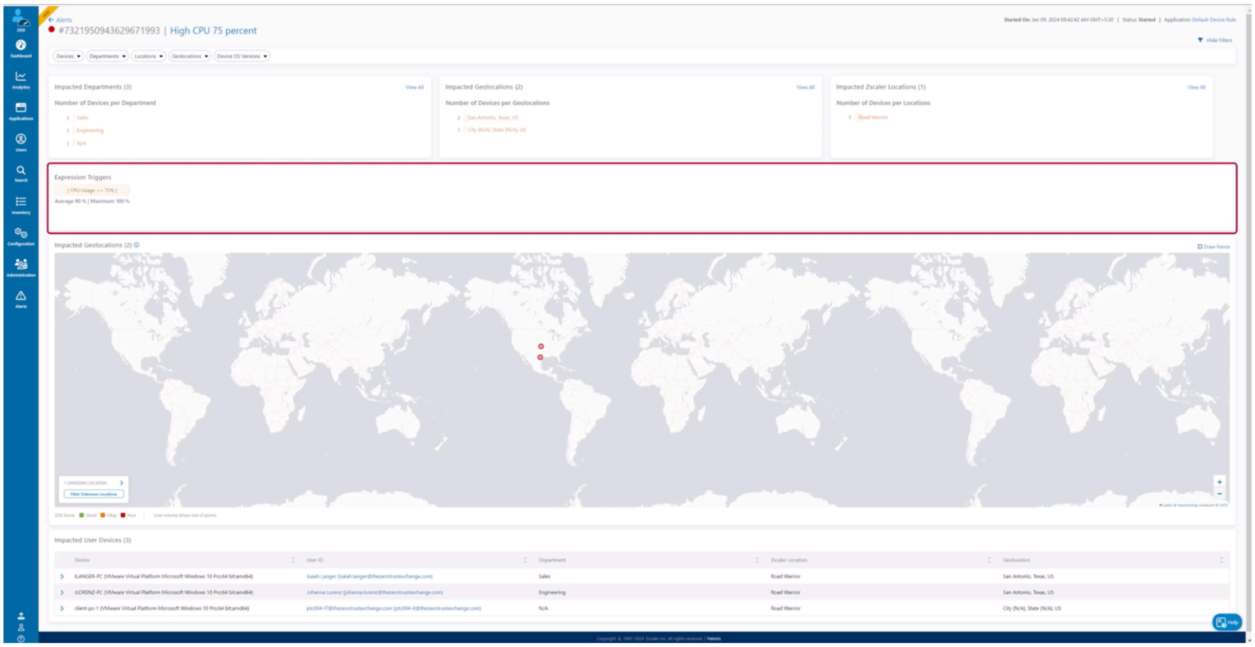
IMPACTED GEOLOCATIONS 57

IMPACTED APPLICATIONS 4

Severity	Rule Name	Type	Impacted Application	Impacted Geolocations	Impacted Devices	Started On	
●	High CPU 75 percent	Device	Default Device Rule	2 Geolocations	3 Devices	Jan 09, 2024 09:42:42 AM GMT+5:30	👁
●	Loss of WiFi	Device	Default Device Rule	1 Geolocation	1 Device	Jan 09, 2024 08:30:18 AM GMT+5:30	👁
●	Disk Space greater than 80 Percent	Device	Default Device Rule	2 Geolocations	2 Devices	Jan 09, 2024 12:05:15 AM GMT+5:30	👁
●	Test-South America	Device	Default Device Rule	1 Geolocation	3 Devices	Jan 09, 2024 12:00:14 AM GMT+5:30	👁
●	High CPU	Device	Default Device Rule	54 Geolocations	130 Devices	Jan 08, 2024 11:50:19 PM GMT+5:30	👁
●	test_app_slowness	Application	Microsoft Teams Web App	48 Geolocations	122 Devices	Jan 08, 2024 08:04:51 PM GMT+5:30	👁
●	Oceania	Device	Default Device Rule	4 Geolocations	7 Devices	Jan 08, 2024 07:55:18 PM GMT+5:30	👁
●	Test_slowness_service_now	Application	ServiceNow	55 Geolocations	127 Devices	Jan 08, 2024 04:29:52 PM GMT+5:30	👁
●	Test_slowness	Application	Box	56 Geolocations	128 Devices	Jan 08, 2024 04:29:50 PM GMT+5:30	👁

For each alert, the table shows the type of alert, impacted application, geolocation, and devices, as well as the start and end time. To investigate further and view the details of an ongoing alert, you can simply click the eye icon.

The alert details page shows the number of impact devices by department, geolocation, and Zscaler location. You can also review the threshold settings that trigger the alert as well as the average and maximum values for the time period. The impacted geolocations map displays the location of the impacted devices. The table at the bottom displays all impacted devices.



#7321950943629671993 | High CPU 75 percent

Started On: Jan 09, 2024 09:42:42 AM GMT+5:30 | Status: Started | Application: Default Device Rule

Impacted Departments (3)

Number of Devices per Department

1	Sales
1	Engineering
1	N/A

Impacted Geolocations (2)

Number of Devices per Geolocations

2	San Antonio, Texas, US
1	City (N/A), State (N/A), US

Impacted Zscaler Locations (1)

Number of Devices per Locations

3	Road Warrior

Expression Triggers

(CPU Usage >= 75%)

Average 90 % | Maximum: 100 %

Impacted Geolocations (2)

Impacted User Devices (3)

Device	User ID	Department	Zscaler Location	Geolocation
ILANGER-PC (VMware Virtual Platform Microsoft Windows 10 Pro;64 bit;amd64)	Isaiah Langer (isaiah.langer@thezerotrustexchange.com)	Sales	Road Warrior	San Antonio, Texas, US
JLORENZ-PC (VMware Virtual Platform Microsoft Windows 10 Pro;64 bit;amd64)	Johanna Lorenz (johanna.lorenz@thezerotrustexchange.com)	Engineering	Road Warrior	San Antonio, Texas, US
client-pc-1 (VMware Virtual Platform Microsoft Windows 10 Pro;64 bit;amd64)	ptc004-IT@thezerotrustexchange.com (ptc004-it@thezerotrustexchange.com)	N/A	Road Warrior	City (N/A), State (N/A), US

You can also click the drop down arrow to the left of the device name and view details for that individual device.

And finally, you can use the alert history to view a list of alerts that have ended up fourteen days in the past.

To recap alerts can be a useful tool for your support team, such that they can be notified and quickly respond to performance issues with applications, networks and devices.

CONFIGURING ZDX

Configuring Applications

To get started with Zscaler Digital Experience, you need to decide which applications you want to monitor. ZDX provides several **predefined applications** for popular SaaS applications, such as SharePoint Online, Box, Salesforce and others. Additionally, you can configure **custom applications** to monitor your organization’s internal or external applications. Remember that an application needs at least a Web Probe configured.

In this chapter, we will have a detailed look at the steps required to configure both types of applications.

Predefined and Custom Applications are an important place to start when configuring a ZDX tenant, so that you can monitor the applications that are critical to your organization.

One of the first things to do in configuring a new tenant is to define a list of applications that you want to monitor with ZDX.

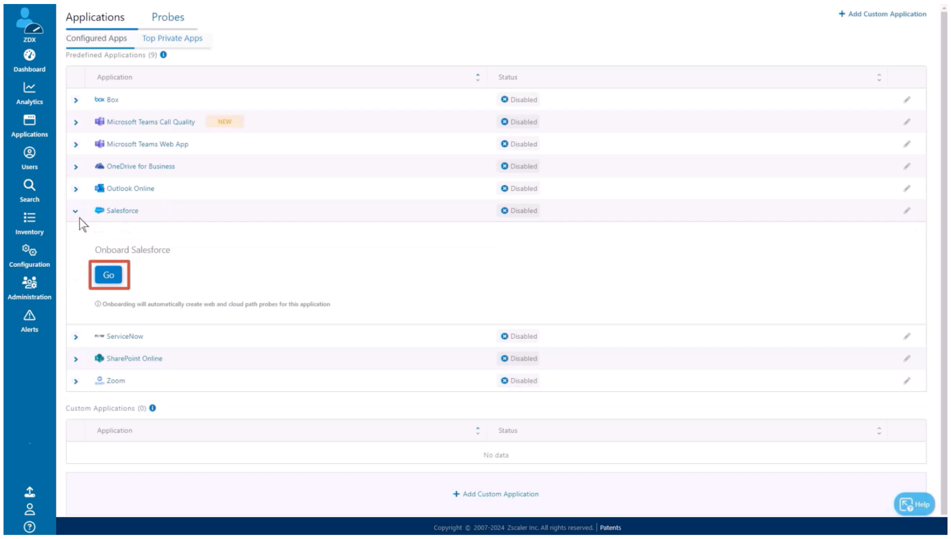
Enabling Predefined Applications

First, let's look at how easy it is to get started with predefined applications.

Think of predefined applications as templates that already include a web and cloud path probe to collect metrics. All you need to do is enable them. The applications tab in the configuration menu shows a list of all predefined applications.

The applications you see on this page depend on your ZDX plan. For example, with the ZDX-M365 plan, you'll only see Microsoft applications like Teams, OneDrive, Outlook, and SharePoint.

Most predefined applications can be enabled with the click



Predefined Applications (9)

Application	Status
Box	Disabled
Microsoft Teams Call Quality NEW	Disabled
Microsoft Teams Web App	Disabled
OneDrive for Business	Disabled
Outlook Online	Disabled
Salesforce	Disabled
ServiceNow	Disabled
SharePoint Online	Disabled
Zoom	Disabled

Onboard Salesforce

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

Custom Applications (0)

Application	Status
No data	

Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Patents

of a button. Let's use Salesforce as an example.

Simply expand the listing and click go.

ZDX automatically created a web probe and a cloud path probe for you. It's that simple.

Some of your applications, for example, SharePoint require you to enter your organization's tenant ID. Once you are done, activate your changes. And you would repeat these steps to enable any other predefined applications that are critical to your organization.

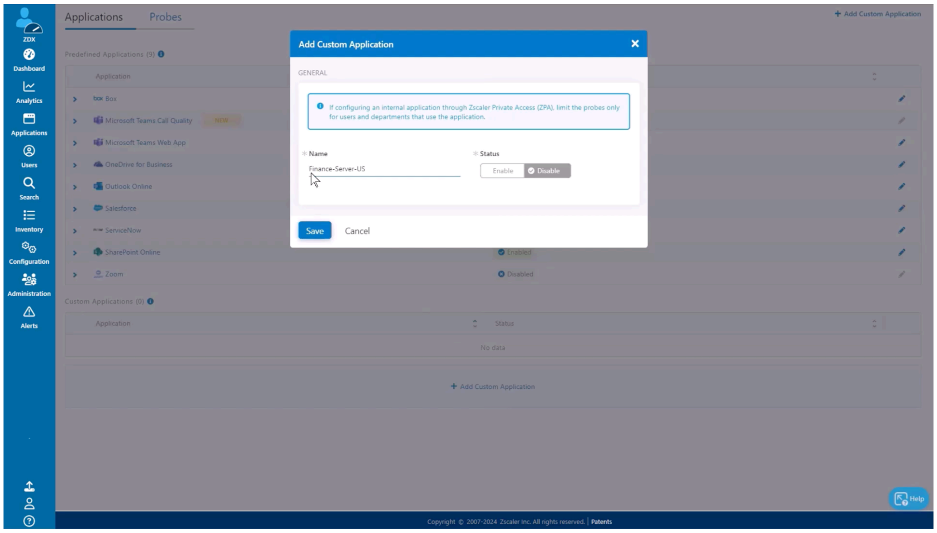
The ZDX score and performance metrics for these applications will, over time, be displayed in the various dashboards and graphs.

Adding Custom Applications

Now let's take a quick look at the steps required to add a custom application.

Remember, that a custom application allows you to monitor any SaaS or web application.

Back on the configuration page, select add custom application. Simply enter a descriptive name for the application, then click save. As always, activate the changes.



Add Custom Application

GENERAL

If configuring an internal application through Zscaler Private Access (ZPA), limit the probes only for users and departments that use the application.

* Name: Finance-Server-US

* Status: Enable [✓ Disable]

Save Cancel

Again, it's that simple to get started. The new application is now added to the list of custom applications, but it is still disabled. That's because you need to manually configure at least a web probe. We will cover configuring probes in a later chapter.

Configuring Call Quality Monitoring

One of the most dreaded calls that IT support can receive is from a user complaining about poor call quality. These problems are usually highly visible, highly disruptive, hard to isolate, and are fleeting. To pinpoint call quality issues, ZDX integrates with the Microsoft Teams Call Quality API and Zoom API to pull in call, video, and sharing quality statistics for every meeting. This data is then made available in ZDX graphs, along with Cloud Path and endpoint device metrics that ZDX has been collecting during the meeting.

Configuring Microsoft Teams Call Quality Monitoring

Similar to other predefined applications, Microsoft Team's call quality monitoring is available under the ZDX configuration menu and can be configured with just a few mouse clicks. Here are the steps you need to complete for the initial configuration.

1. With the call quality application already enabled, you can now set up a connection between your ZDX tenant and the Microsoft Graph API. To do that, simply expand Microsoft Team's call quality and click add new tenant.Next, accept the application permissions that allow ZDX to pull user and call record data from the Microsoft Graph API.

2. From there, you can enter the tenant name and then click Microsoft Office 365 authentication. Remember that you need to sign in with credentials for a user with administrator privileges. Otherwise, you'll see an error message. You want to save these changes back in the new tenant window and then validate that the API set up to Microsoft was successful.

And that's it. The Microsoft Teams call quality cloud path probe now starts collecting metrics. Now whenever a team's call has ended, call quality data is retrieved using the Microsoft Graph API and is displayed in the applications page.

Configuring Zoom Call Quality Monitoring

Zoom call quality monitoring is available under the ZDX configuration menu and can be configured with just a few mouse clicks. Here are the steps you need to complete for the initial configuration.

1. To set up a connection between your ZDX tenant and the zoom API, click authenticate. Sign in with your Zoom email address and password. Remember that you need to sign in with credentials for a user with administrator privileges. Next, accept the application permissions that allow ZDX to pull user and call record data from the Zoom API.

2. Back in the new tenant window, you can rename the tenant and ensure that the status is set to enable. If needed, you can use filters under monitoring criteria to identify users who are meeting hosts.Only meetings hosted by these users are monitored.

3. Click validate to verify that your setup was Zoom successful and save the setup.

4. The last step is to configure a cloud path probe for zoom.

And that's it. The Zoom call quality cloud path probe now starts collecting metrics as a meeting is in progress and displays ZDX score data in the applications page. From here, you can drill down further and view meeting specific metrics.

Configuring Probes

ZDX Probes periodically generate synthetic traffic and collect metrics for your applications. There are different types of probes that each collect a different set of metrics; **Web Probes, Cloud Path Probes** and **Autosense Cloud Path Probes**.

While predefined applications already have preconfigured probes, custom applications require you to create at least one Web Probe. Probe traffic that goes through a Zscaler Internet Access (ZIA) cloud will be cached. However, probe traffic that goes **directly** to a SaaS application or a private application runs the risk of DDOS mitigation if the probe frequency is too high and/or too many probes are being generated by employees that may not even use an application.

Let's first look at the steps for configuring a Web Probe.

Configuring a Web Probe

Remember that for a custom application to be enabled, you need to configure a web probe.

To get started, you can either go to the probes tab in the configuration menu or select add a new probe for an application. Setting up a new probe is a simple three step process:

1. In the first step, you'll configure general probe settings starting with a descriptive name. There is no need for any other changes here, as the application name is already selected and the web probe type is set by default. You can configure the probe to monitor multiple user groups, users in particular locations or departments, or a combination of these.
    - For example, the custom application you had selected earlier is only being used by the finance department, so it makes sense to limit the probe only to users in that department. Along the same lines, you also have the option to select user groups, locations, or departments that you do not want to monitor. Reducing unnecessary probe traffic is always good practice. This is especially important when configuring web probes for internal applications through Zscaler private access. Since web probes for ZPA are currently not cached, you should probe only for users, user groups, and departments that actually use that application.

2. In the second configuration step, you need to specify the destination URL. This is the web address the probe will request. There are a few advanced settings that are not commonly changed and only apply to special use cases. First, there is the option to customize the HTTP request header that is passed as part of the probe.

    - If the target website wires an authentication token, you could use an authentication header and include the token value.
    - You can add or delete HTTP response status codes that will be considered as success codes for the probe. If the configured URL returns HTTP code that is not in this list, then the probe is considered failed, and that will lower the ZDX score.
    - By default, we use 2xx and 3xx HTTP response codes, but there may be cases where you want to accept some HTTP error codes as success. For example, if a web application returns a code not in the 2xx and 3xx range, even though the request is valid, you can add it here.
    - When you scroll down, you can, if needed, change any of the remaining default values. For example, if the application being probed is expected to be slow, you can increase the number of attempts and time out threshold to reduce probe errors. This may be useful when probing a file download URL, which is expected to take much longer than a simple web page.
    - If you want to only measure response time to the first URL, Without redirection, you can disable “follow redirects”.
    - And in the case of an application that has a lot of redirects, you can increase the default number.

3. And in the third step, you can review the web probe configuration and then click submit. Once you activate the changes, the new web probe is listed on the probes page. After a few minutes, you will then see performance metrics for the application.

Configuring a Cloud Path Probe

A Cloud Path Probe collects metrics for each hop along the data path, from the end user all the way to the application. These probes help to identify the source of a performance issue. When it comes to troubleshooting user issues, cloud path probes help you answer an important question: Which hop along the path between user and application caused the highest latency?

Let's now take a look at the steps for configuring a Cloud Path Probe.

The setup process is very similar to a web probe.

1. To get started, you can either go to the probes tab in the configuration menu or select Add New Probe for an application. As before, enter a descriptive name for the probe and then select cloud path as the probe type. Selecting a web probe for the cloud path probe to follow is **recommended best practice** and is required for use with Z-tunnel version 1. Because Z-tunnel version 1 is only for HTTP-based connections, the cloud path probe needs to be explicitly configured to follow the path of a web probe.

2. As we saw earlier, with the web probe, you have the options to configure probing and exclusion criteria. Again, limiting the number of probes is especially important for internal

applications through Zscaler private access.You should only probe for users, user groups, and departments that actually use that application.

3. You now have the option to configure additional parameters for the probe. Remember that the available protocol options are ICMP, TCP, UDP, and Adaptive. Depending on the protocol you select, you'll get slightly different options. For example, with UDP selected, there is a default UDP port number that can be changed. Also, keep in mind that TCP and adaptive mode generate numerous syn packets to initiate connections. And that may cause problems with remote access boxes that are typically used in small offices or home offices.
   - Packet count, interval, and timeout are advanced options, which are really changed. For example, increasing the pack account or reducing the interval will increase the fidelity of the cloud path probe, but will also generate more network traffic.
4. Finally you will need to enter the tenant name or fully qualified domain name for the target host. Review the cloud path probe configuration to make sure everything is correct and then click submit. You will now see the new cloud path probe displayed for the custom application. As always, activate the changes. The metrics collected by probe will be displayed in the user details page.

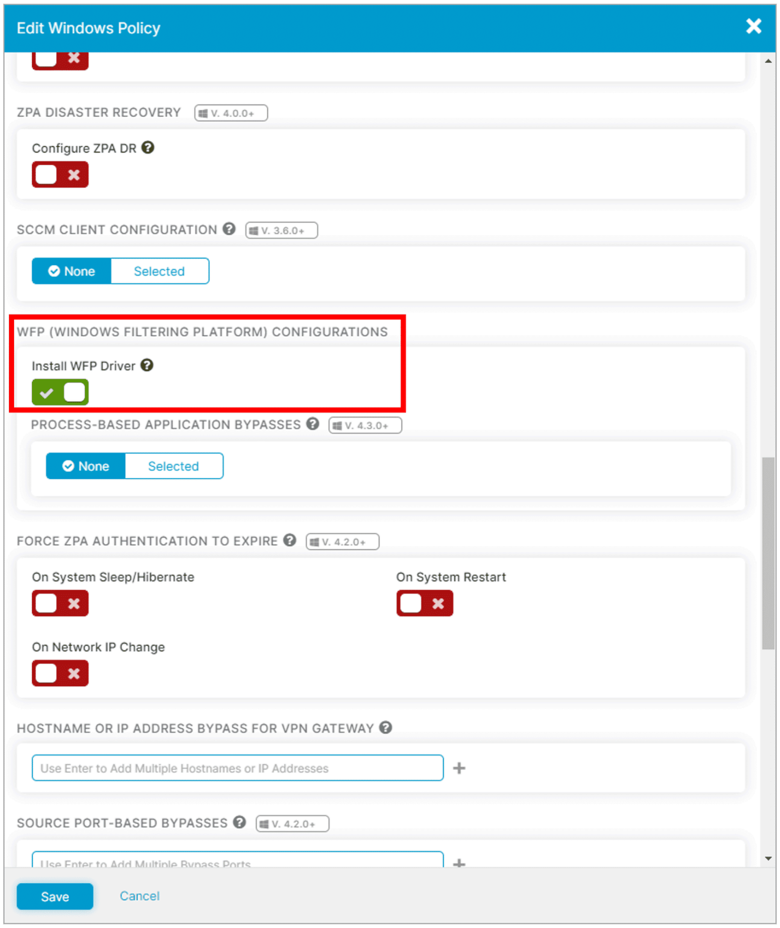
To recap, cloud path probes collect packet loss, latency metric, and details for each hop along the path from the user to the application.

Configuring an Authosense Cloud Path Probe

Remember that an Autosense probe detects and probes endpoints dynamically rather than probing fixed endpoints at fixed intervals. The configuration steps for an Autosense probe are similar to what you saw in the previous configuration, with a few caveats.

Meet Minimum Requirements

In addition to minimum versions for ZDX and Client Connector, Autosense probes require the installation of a Windows Filtering Platform (WFP) driver on Client Connector. Make sure that in the Zscaler Client Connector Portal, the **Install WFP Driver** option is enabled in Application Profiles.



Edit Windows Policy

ZPA DISASTER RECOVERY V. 4.0.0+

Configure ZPA DR ☒

SCCM CLIENT CONFIGURATION V. 3.6.0+

[✓ None] Selected

WFP (WINDOWS FILTERING PLATFORM) CONFIGURATIONS

Install WFP Driver ✓

PROCESS-BASED APPLICATION BYPASSES V. 4.3.0+

[✓ None] Selected

FORCE ZPA AUTHENTICATION TO EXPIRE V. 4.2.0+

On System Sleep/Hibernate ☒

On System Restart ☒

On Network IP Change ☒

HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY

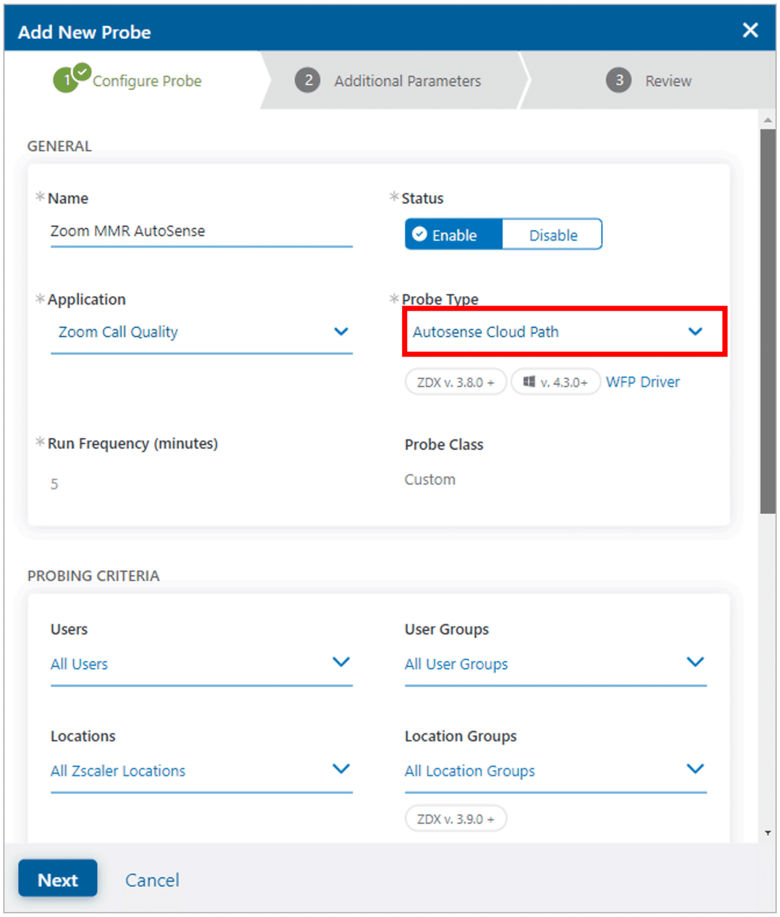
Use Enter to Add Multiple Hostnames or IP Addresses +

SOURCE PORT-BASED BYPASSES V. 4.2.0+

Use Enter to Add Multiple Bypass Ports +

Configure Probe Type and Criteria

Select the **Autosense Cloud Path** type and configure any other criteria.



GENERAL

*Name: Zoom MMR AutoSense

*Status: ● Enable | Disable

*Application: Zoom Call Quality

*Probe Type: Autosense Cloud Path

*Run Frequency (minutes): 5

Probe Class: Custom

PROBING CRITERIA

Users: All Users

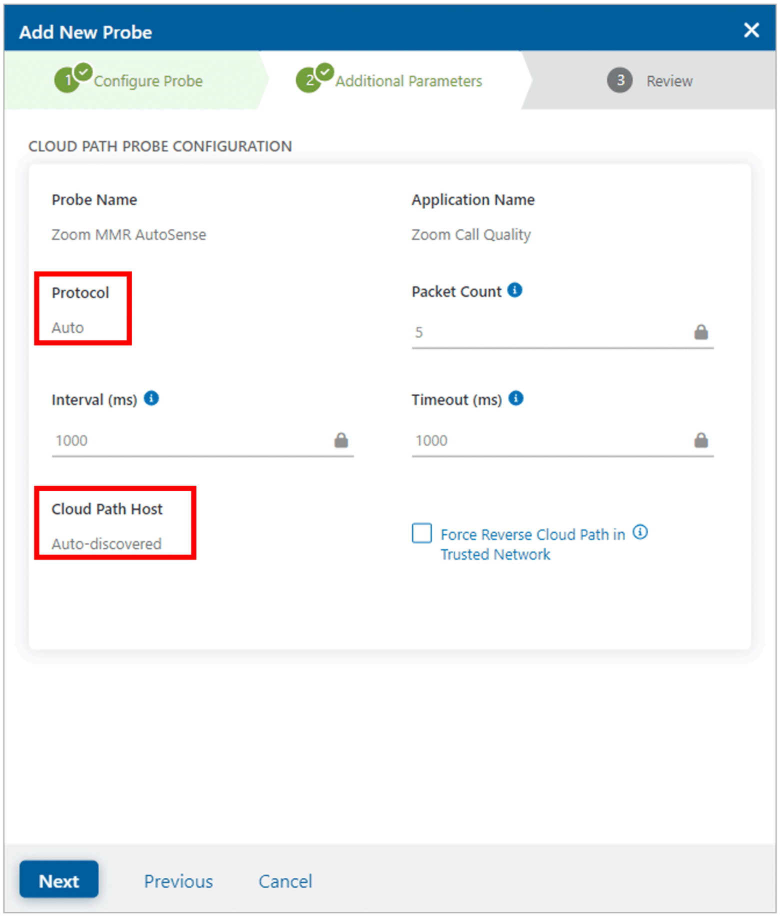
User Groups: All User Groups

Locations: All Zscaler Locations

Location Groups: All Location Groups

Configure Additional Parameters

Configure additional parameters Since Autosense probes detect and probe endpoints dynamically, the options for **Protocol** selection and **Cloud Path Host** are grayed out.



Add New Probe

1 Configure Probe — 2 Additional Parameters — 3 Review

CLOUD PATH PROBE CONFIGURATION

Probe Name: Zoom MMR AutoSense

Application Name: Zoom Call Quality

Protocol: Auto

Packet Count: 5

Interval (ms): 1000

Timeout (ms): 1000

Cloud Path Host: Auto-discovered

□ Force Reverse Cloud Path in Trusted Network

Configuring Deep Tracing

Deep Tracing in ZDX can provide deeper insights into process-level information for a user. During a Deep Tracing session, information is collected **every minute** for the Web Probe, Cloud Path Probe, as well as device statistics.

Deep tracing is a powerful tool to quickly identify end user issues. With a few mouse clicks, you can select a user, a device, and an application they are experiencing issues with, and then start collecting data. Let's see how this works.

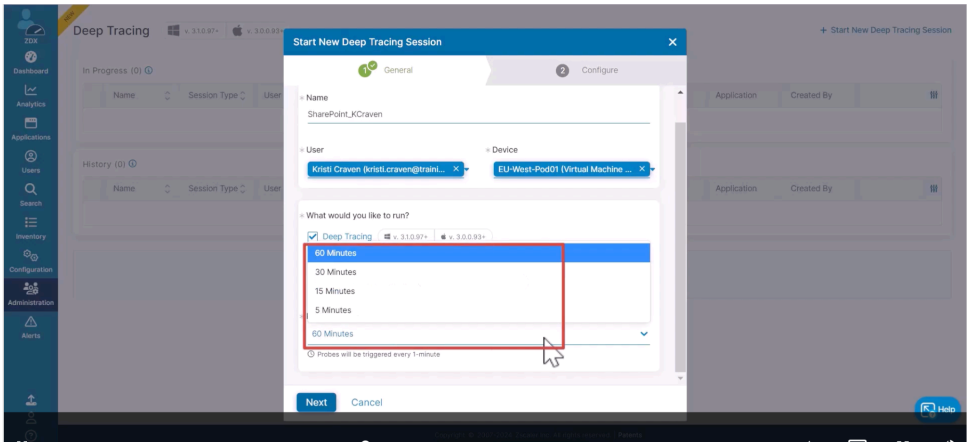
In the ZDX admin portal, there are three options to configure a deep tracing session.

1. The default is to select deep tracing **from the administration menu**.
2. Then there is a shortcut for each user **in the user overview page**. Clicking this link already fills in the username and application in the deep tracing configuration window.
3. And the third option is to use the start deep tracing button **on a user's details page**. With this option, username, application, probes, and device details are already preselected.

Next, select what you want to run. Besides Deep Tracing, you can also choose to run a bandwidth test, or perform a packet capture. If you select Packet Capture Probing, you'll see slightly different options on the next screen that allow you to configure IP addresses or ports to filter packet capture, network interfaces and a packet size limit.

In this example, we select the Deep Tracing option.

All you need to do now is enter a descriptive name for the session and specify how long the session should run for.


Start New Deep Tracing Session

1 General — 2 Configure

* Name: SharePoint_KCraven

* User: Kristi Craven (kristi.craven@traini...

* Device: EU-West-Pod01 (Virtual Machine ...

* What would you like to run?

☑ Deep Tracing v. 3.1.0.97+ v. 3.0.0.93+

60 Minutes
30 Minutes
15 Minutes
5 Minutes

60 Minutes

Probes will be triggered every 1-minute

Remember that a deep tracing session can slightly increase the processing load on an end user device. So it makes sense to only collect metrics for a few minutes.

Next, you'll have the option to also collect device statistics. It's good practice to include device stats because they help with identifying device problems by viewing details such as the top processes that are consuming the most system resources.

Here is an option that's often overlooked. When you select add a special application from the drop down list, you can add any URL without an existing probe. So if a user has issues with a site that's not on your list of predefined custom applications, you can still start a deep tracing session for it.

All that's left to do now is to click save.

The new session is listed in the in progress table on the deep tracing page. Wait a few minutes and then click the I icon to view the data that has been collected so far.

Once a deep tracing session ends, it'll be listed in the history table.

From there, you can dig into the web probe and cloud path metrics, device health information, top processes, and device events.

To recap, deep tracing is easy to configure, and it helps you troubleshoot user issues in near real time.

Configuring Alerts

Alerts allow you to be proactive and monitor your organization’s device, application, and network performance, and ZDX Score. An alert is triggered based on a threshold that is configured as part of an **Alert Rule**.

Alerts can be configured to send notifications either by email or webhooks. If your organization already uses Slack or ServiceNow, then integrating ZDX alerts directly into these SaaS applications via webhooks is recommended best practice. The setup details depend on the application you want to integrate with, but the ZDX help portal provides step-by-step guides and sample configurations to simplify the process.

Configuring Alerts is important, so that IT teams such as HelpDesk can be notified about ZDX Score drops for their key applications before users submit tickets.

Here are the alert types and what can be configured as thresholds:

For an **Application**-type alert rule, the available criteria are:

- DNS Time
- Page Fetch Time
- Server Response Time
- Web Request Availability
- ZDX Score Drops

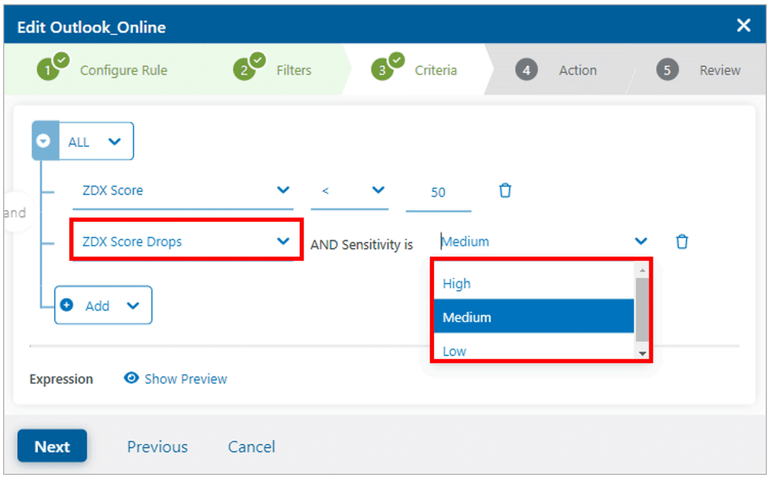
For a **Device**-type alert rule, the available criteria are:

- Bandwidth in Mbps
- Battery Level
- CPU Idle
- CPU Kernel Usage
- CPU Usage
- CPU User Usage
- Disk Reads in bps
- Disk Usage
- Disk Writes in bps
- Memory Usage
- Memory Used
- Received Bits in Mbps
- Sent Bits in Mbps
- WiFi Signal

For a **Network**-type alert rule, the available criteria are:

- Latency
- Packet Count
- Number of Hops
- Packet Loss
- ZDX Score Drops

Configuring Dynamic Alerts



Edit Outlook_Online

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

ALL

ZDX Score < 50

and

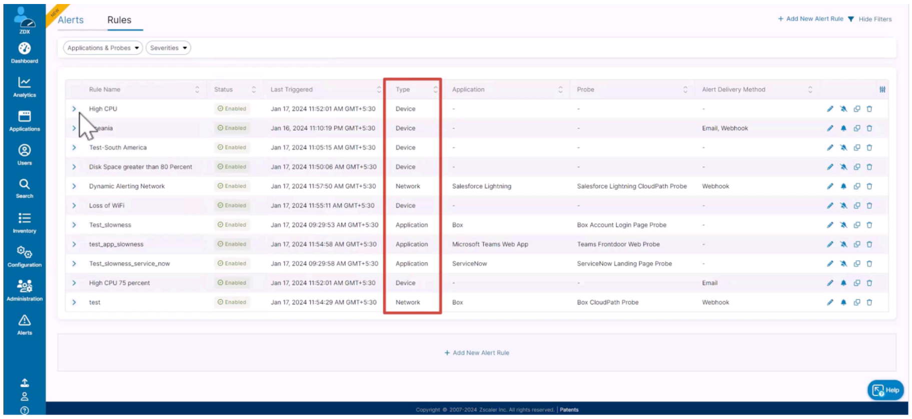
ZDX Score Drops AND Sensitivity is Medium

To configure a dynamic alert, you'll use the **ZDX Score Drops** criteria and specify a sensitivity threshold that reflects your organization's tolerance for performance degradations.

You probably have more important things to do than to stare at ZDX dashboards all day. So alerts are a great way to have ZDX keep an eye on your organization's applications, networks, and end users and notify you when an event requires attention.

To configure and manage alert rules, simply select alerts from the main menu and then go to the rules tab.

1. First, let's take a closer look at what's included on the alert rules page. Along the top are several filter options. For example, you can filter the page to only list rules for a specific application and probe. The table below shows details for each of the existing rules including their status, the alert rule type, application and probe, and their alert delivery method. There are also options to edit, delete, mute, or unmute a rule. If a rule is muted, the alerts can still be viewed in the ZDX admin portal, but no notifications will be sent via email or webhook. And you can quickly check the rules criteria details.



Rule Name	Status	Last Triggered	Type	Application	Probe	Alert Delivery Method
High CPU	Enabled	Jan 17, 2024 11:52:01 AM GMT+5:30	Device	-	-	-
Oceania	Enabled	Jan 16, 2024 11:10:19 PM GMT+5:30	Device	-	-	Email, Webhook
Test-South America	Enabled	Jan 17, 2024 11:05:15 AM GMT+5:30	Device	-	-	-
Disk Space greater than 80 Percent	Enabled	Jan 17, 2024 11:50:06 AM GMT+5:30	Device	-	-	-
Dynamic Alerting Network	Enabled	Jan 17, 2024 11:57:50 AM GMT+5:30	Network	Salesforce Lightning	Salesforce Lightning CloudPath Probe	Webhook
Loss of WiFi	Enabled	Jan 17, 2024 11:55:11 AM GMT+5:30	Device	-	-	-
Test_slowness	Enabled	Jan 17, 2024 09:29:53 AM GMT+5:30	Application	Box	Box Account Login Page Probe	-
test_app_slowness	Enabled	Jan 17, 2024 11:54:58 AM GMT+5:30	Application	Microsoft Teams Web App	Teams Frontdoor Web Probe	-
Test_slowness_service_now	Enabled	Jan 17, 2024 09:29:58 AM GMT+5:30	Application	ServiceNow	ServiceNow Landing Page Probe	-
High CPU 75 percent	Enabled	Jan 17, 2024 11:52:01 AM GMT+5:30	Device	-	-	Email
test	Enabled	Jan 17, 2024 11:54:29 AM GMT+5:30	Network	Box	Box CloudPath Probe	Webhook

2. Next, let's have a look at how easy it is to add a new alert rule. The alert rule configuration wizard walks you through the required steps.

a. First, you'll need to configure some basic settings starting with the alert rule name.
b. Next, select the severity level. The options here are high, medium, or low depending on the impact of this event to your users,
c. Next, you'll need to select the alert type. The available type options are pretty self explanatory and include application, device, network, or ZDX score.
d. We configured an application alert in the previous step, so you now need to select an application, for example, OneDrive and its web probe.
e. You then have the option to configure filters. For example, you could limit the alert rule to a specific Zscaler location and department. Depending on the alert type you configured in the first step, there are different criteria options available. Since we configured an application alert earlier, the criteria here will be application related. For example, page fetch time and DNS time. You can combine several criteria with logical and or combinations.
f. In the next step, you can change the default throttling options that make sure that help desk doesn't get swamped with notifications about one off or minor issues. Nobody needs alert fatigue.
g. And finally, you'll select the delivery method for the alert, for example, email.
h. Review the final alert rule configuration And if everything looks good, click submit. And as always, activate the changes.

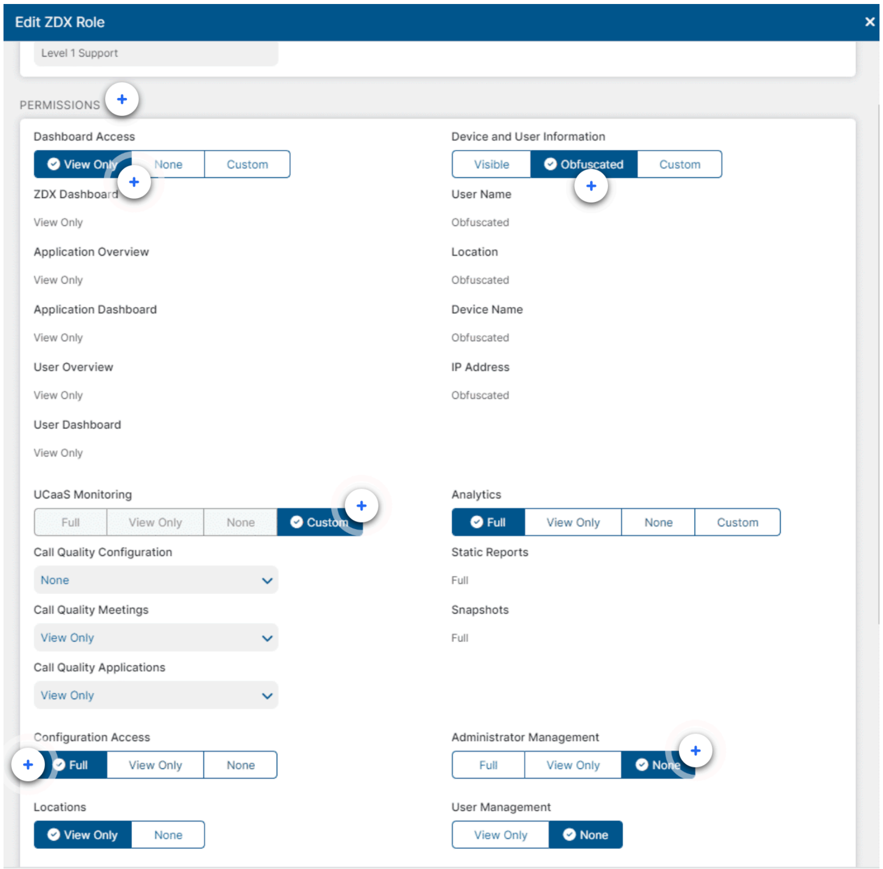
That's all there is to it. The new rule is now listed on the alert rules page and will trigger an email notification whenever one of the criteria threshold holds is exceeded.

To recap, configuring an alert rule involves a few simple steps to define what you want to monitor, When an alert will be triggered and how you wanna be notified.

Configuring Role-Based Administration

ZDX allows for role-based administration. Organizations can easily add administrators and assign them to specific roles with differing levels of access.

The markers below show the access-level options for an administrator role.



Edit ZDX Role ×

Level 1 Support

PERMISSIONS

Dashboard Access: ✓ View Only | None | Custom

ZDX Dashboard: View Only

Application Overview: View Only

Application Dashboard: View Only

User Overview: View Only

User Dashboard: View Only

Device and User Information: Visible | ✓ Obfuscated | Custom

User Name: Obfuscated

Location: Obfuscated

Device Name: Obfuscated

IP Address: Obfuscated

UCaaS Monitoring: Full | View Only | None | ✓ Custom

Call Quality Configuration: None

Call Quality Meetings: View Only

Call Quality Applications: View Only

Analytics: ✓ Full | View Only | None | Custom

Static Reports: Full

Snapshots: Full

Configuration Access: ✓ Full | View Only | None

Administrator Management: Full | View Only | ✓ None

Locations: ✓ View Only | None

User Management: View Only | ✓ None

Permissions

Create levels of permissions for admin users within an organization.

View Only

Allows admins only to view what has been set up.

Obfuscated

Choose if user and device real names should be obfuscated to admins.

Custom

Allows admins to set access rights for specific dashboards or functions.

Full

Admins have full access to configuration options.

None

Admins can view but cannot make changes.

Configuring Role-Based Administration

With role based administration and ZDX you can easily add admins and assign them specific roles, which will define the functions they have access to in their day to day jobs.

For example, for admins in your level one support team, you could create a view only role that allows them access to dashboards and graphs, but removes all configuration functions.

Let's see how this works.

1. Go to the administration menu and select role management. You will then add a new ZDX role and set the permissions to limit access to reporting functions only and, for those who don't need to access personally identifiable information, also obfuscate usernames and device names.
2. Then add the new admin user and assign that user to the role we just created. There is some basic information to fill in here, like the login ID, email address, and display name. For the role, select the level one support role that we created earlier. With the scope option, can allow an admin to manage your entire organization or limit access to a subset of locations.

As always, activate the changes.

There are a couple of additional options that are worth exploring.

- Under administrator management, you have the option to enable passwords to expire after a set period of time. Or you can enable SAML-based authentication so that admins can log in to the ZDX admin portal directly from a single sign-on portal.

- With admins from different teams all accessing the same ZDX tenant, it's sometimes not obvious who created a custom app, set up alerts, and so on. That's where audit logs come in handy. The audit logs page displays recent administrator activity. This page can be filtered so that you can quickly find out who did what and when. For configuration updates, you can even get a side by side view of the changes.

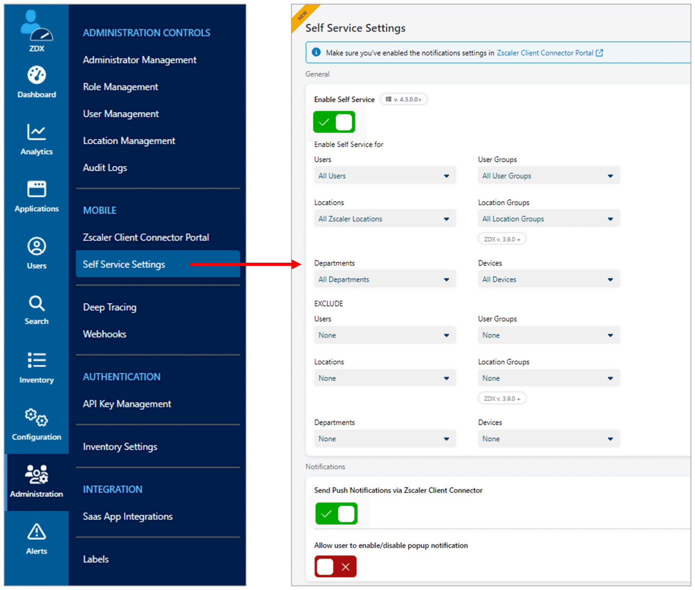
To recap, with role based administration, you can create a hierarchy of admin rules and allow access to all or a subset of ZDX menus and functions.

Configuring Self Service Settings

Self Service notifications are displayed at end users' Client Connector when CPU or WiFi issues are detected and need attention. Each notification contains a brief diagnosis and recommendation that might resolve the issue. Administrators can enable and configure Self Service settings in the Administration menu.

Once Self-Service is enabled, an administrator can:

- select criteria include and exclude specific users, user groups, locations, location groups, departments, and devices.
- configure notification settings to send push notifications via Client Connector or give users the ability to configure notifications.



Self Service Settings

Make sure you've enabled the notifications settings in Zscaler Client Connector Portal

General

Enable Self Service v. 4.3.0.0+

✓

Enable Self Service for

Users: All Users

User Groups: All User Groups

Locations: All Zscaler Locations

Location Groups: All Location Groups (ZDX v. 3.9.0 +)

Departments: All Departments

Devices: All Devices

EXCLUDE

Users: None

User Groups: None

Locations: None

Location Groups: None (ZDX v. 3.9.0 +)

Departments: None

Devices: None

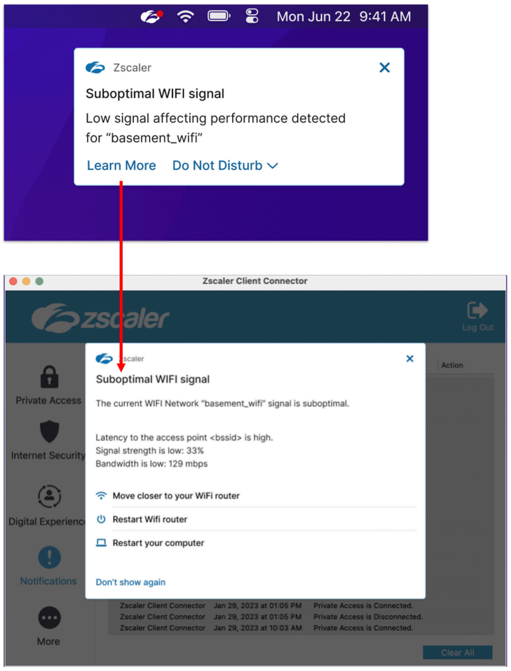
Notifications

Send Push Notifications via Zscaler Client Connector

✓

Allow user to enable/disable popup notification

✗



Suboptimal WIFI signal

Low signal affecting performance detected for "basement_wifi"

Suboptimal WIFI signal

The current WIFI Network "basement_wifi" signal is suboptimal.

Latency to the access point <bssid> is high.
Signal strength is low: 33%
Bandwidth is low: 129 mbps

Move closer to your WiFi router

Restart Wifi router

Restart your computer

```
Zscaler Client Connector   Jan 29, 2023 at 01:05 PM   Private Access is Connected.
Zscaler Client Connector   Jan 29, 2023 at 01:05 PM   Private Access is Disconnected.
Zscaler Client Connector   Jan 29, 2023 at 10:03 AM   Private Access is Connected.
```

When a notification is displayed on an end user's device, the user has the option to see more details about the detected issue and recommended steps to resolve it.

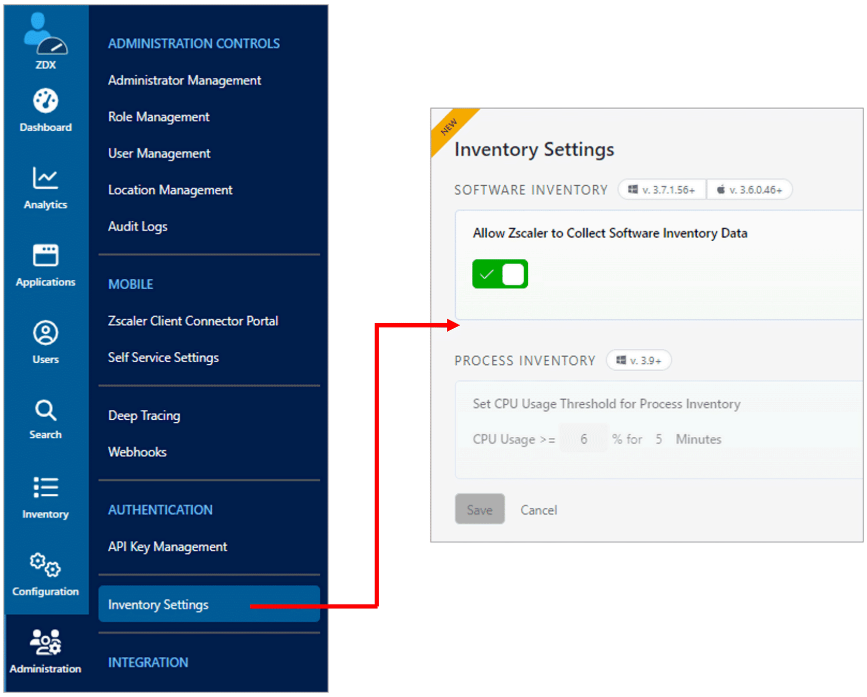
All notifications that were sent to a user can also be reviewed in the user's Client Connector, under the **Notifications** tab.

Configuring Inventory Settings

The Inventory Settings page provides admins with the ability to configure the settings for data collection for Software Inventory and CPU Incidents information for Process Inventory.

Once *Allow Zscaler to Collect Software Inventory Data* is enabled, Client Connector collects inventory data on end user devices.

Process Inventory monitors the number of CPU Incidents that exceed the CPU Usage threshold (e.g., CPU Usage > 10%) for a duration of 5 minutes.



Inventory Settings

SOFTWARE INVENTORY v. 3.7.1.56+ v. 3.6.0.46+

Allow Zscaler to Collect Software Inventory Data ✓

PROCESS INVENTORY v. 3.9+

Set CPU Usage Threshold for Process Inventory

CPU Usage >= 6 % for 5 Minutes

TROUBLESHOOTING USER EXPERIENCE ISSUES

Workflow Overview

Support teams can use ZDX in two ways:

1. As a **troubleshooting tool** to react to user-reported support tickets, and

2. As a **pre-alerting tool** to proactively alert users of performance issues and reduce the number of generated tickets.

In this chapter, we will look at a suggested ZDX troubleshooting workflow and resources that are meant to:

- Reduce the number of total trouble tickets
- Reduce the number of trouble tickets that require escalation
- Improve the mean time to detection (MTTD), mean time to resolution (MTTR) and mean time to innocence (MTTI) of trouble tickets
- Improve cross-functional collaboration among help desk, desktop, network, application and security teams

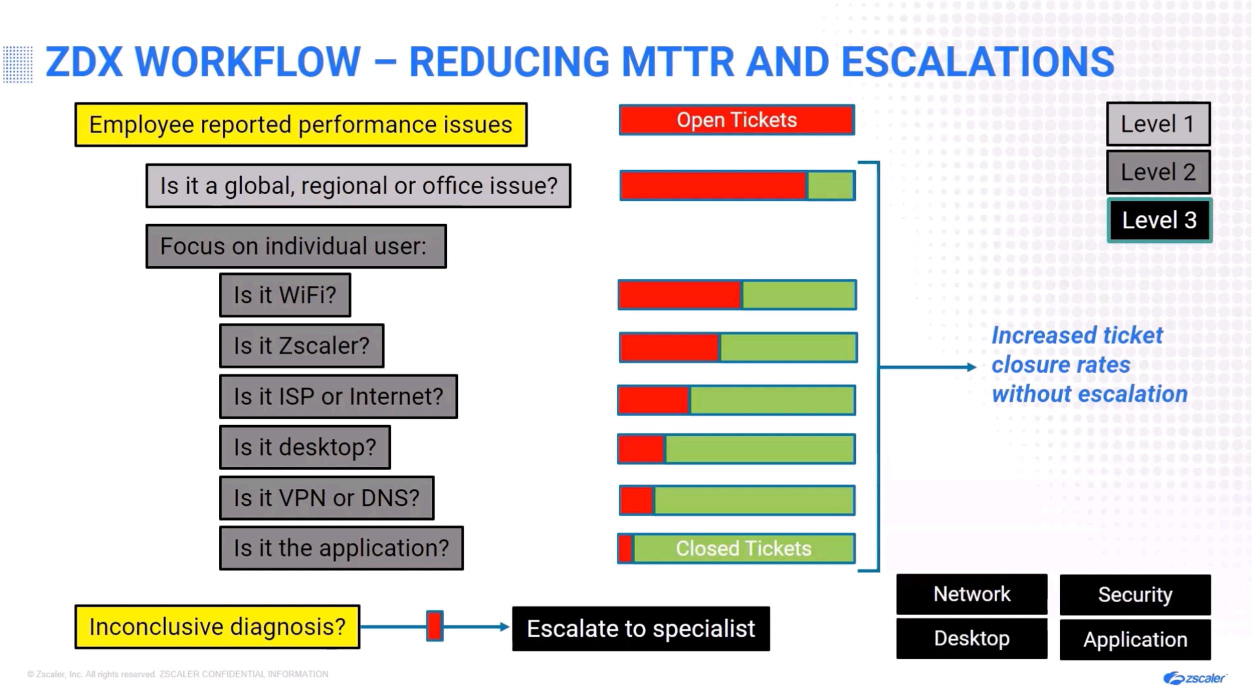
Let’s explore the various levels of a typical support team and their responsibilities when responding to ZDX issues.

ZDX Workflow - Reducing MTTR and Escalations

In their day-to-day operations, support teams need to quickly respond to new trouble tickets, identify the cause of an issue, and either resolve or escalate the issue for further investigation.

So how will support teams use ZDX to do that?

Here is an illustration of a recommended workflow. This process flow is broken down into three levels, and the colors indicate which support team will likely handle which issue. You can adapt this to your organization's operational environment.



ZDX WORKFLOW – REDUCING MTTR AND ESCALATIONS

Employee reported performance issues

Is it a global, regional or office issue?

Focus on individual user:

Is it WiFi?

Is it Zscaler?

Is it ISP or Internet?

Is it desktop?

Is it VPN or DNS?

Is it the application?

Inconclusive diagnosis?

Escalate to specialist

It all starts with an employee reporting an issue. ZDX will help you determine whether only the one user experiences a ZDX score drop for an application, or if there are any broader issues happening at that time. For example, there may be a global application outage, a problem that affects only one geographic region or an office location.

By identifying a global or regional issue, the level one support team can quickly close all open tickets that all relate to that broader issue. If it turns out that the reported issue is specific to that one user, then the ticket is routed to the next level of support. The operator will then work through the questions listed here. ZDX makes it easy to search for that user, review the user details, and either identify the cause of the problem or rule out any of the items listed here.

For example, to identify possible WiFi issues, you can check latency, WiFi signal strength, WiFi type, bandwidth, and any associated device events. So by systematically working through this checklist of potential user specific issues, you can close a large number of open tickets.

While ZDX will help you solve a lot of the reported issues, there will be a certain number of tickets that need to be escalated for further analysis. For example, a level-three desktop specialist can leverage user device metrics, user device events, deep tracing results and other desktop metrics to identify problems with an employee's laptop.

Level 1: Troubleshooting Global, Regional, or Office Issues

Scenario: Several employees in your organization report having problems accessing a critical internal application, and widely used SaaS applications, like SharePoint Online.

As a Level 1 support technician, you now need to determine if this is a global, regional, or office-specific issue. Based on your findings, you can then take action to either resolve the issue or escalate to a Level 2 support engineer.

Troubleshooting Checklist

Here is a list of questions to ask and items to check in order to troubleshoot widespread application issues:

- □ Is the entire organization experiencing an application ZDX Score drop?
  Check in **Applications Tab -> Choose Application**
- □ Is a geographic region experiencing an application ZDX Score drop?
  Check in **Applications Tab -> Choose Application**
- □ Is an entire office experiencing an application degradation?
  Check in **Applications Tab -> Choose Application**

You can also set up alerts to notify your IT team of application issues, based on thresholds for DNS Time, Page Fetch Time, Server Response Time, and Availability.

When troubleshooting an application issue that generated several support tickets, you can start by asking a simple question: Is the entire organization experiencing a ZDX score drop for that application?

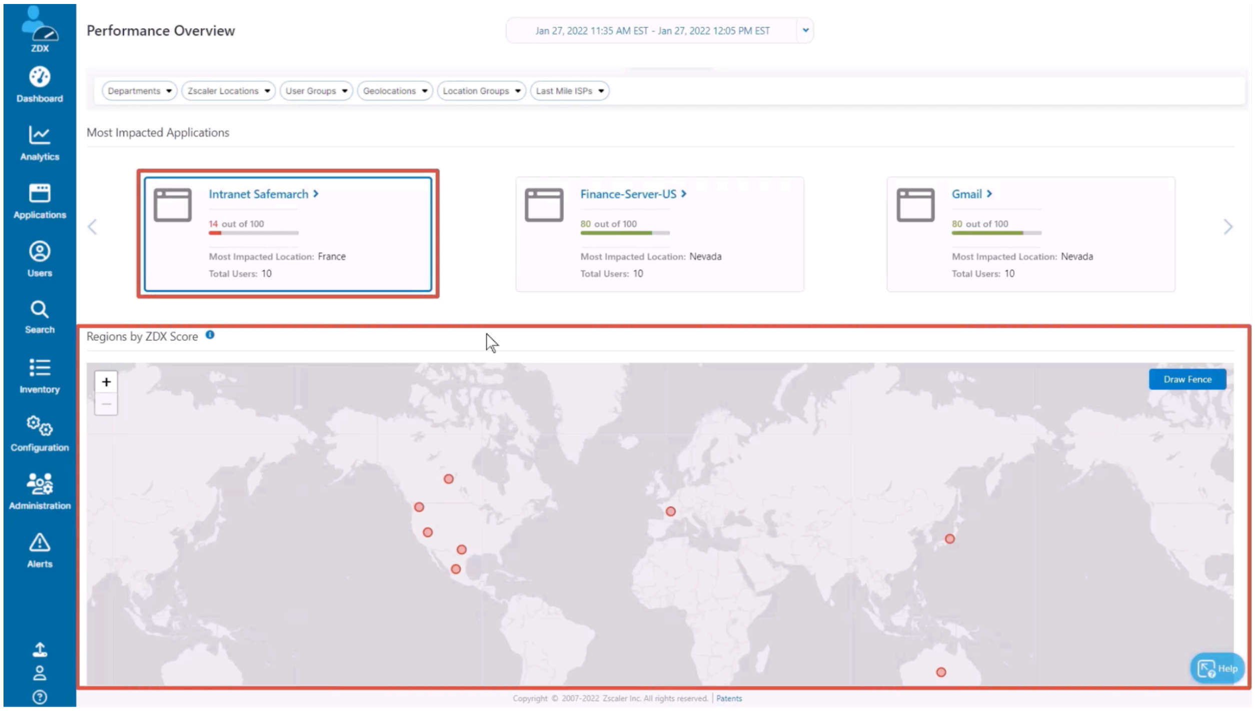
To answer this question, you can start at the ZDX dashboard. A global application outage will be very obvious on the regions by ZDX Score map. with all locations showing a low score. You can then confirm that all other applications perform as expected.

Global Issues

Let's have a closer look at the application that shows low ZDX scores across the board.

You can now go to the applications dashboard and collect more details. For example, you can scroll down the page and check which departments are most impacted by this issue. You can also change the time frame to get a better idea when the service degradation began.

The ZDX score over time graph shows a significant score drop, and you can see that this is not just a short term blip. But a sustained drop. Now that you've confirmed that this is in fact a global outage, you can update your employees about the issue and get in touch with whoever manages the application.



Performance Overview

Jan 27, 2022 11:35 AM EST - Jan 27, 2022 12:05 PM EST

Most Impacted Applications

Intranet Safemarch
14 out of 100
Most Impacted Location: France
Total Users: 10

Finance-Server-US
80 out of 100
Most Impacted Location: Nevada
Total Users: 10

Gmail
80 out of 100
Most Impacted Location: Nevada
Total Users: 10

Regions by ZDX Score

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

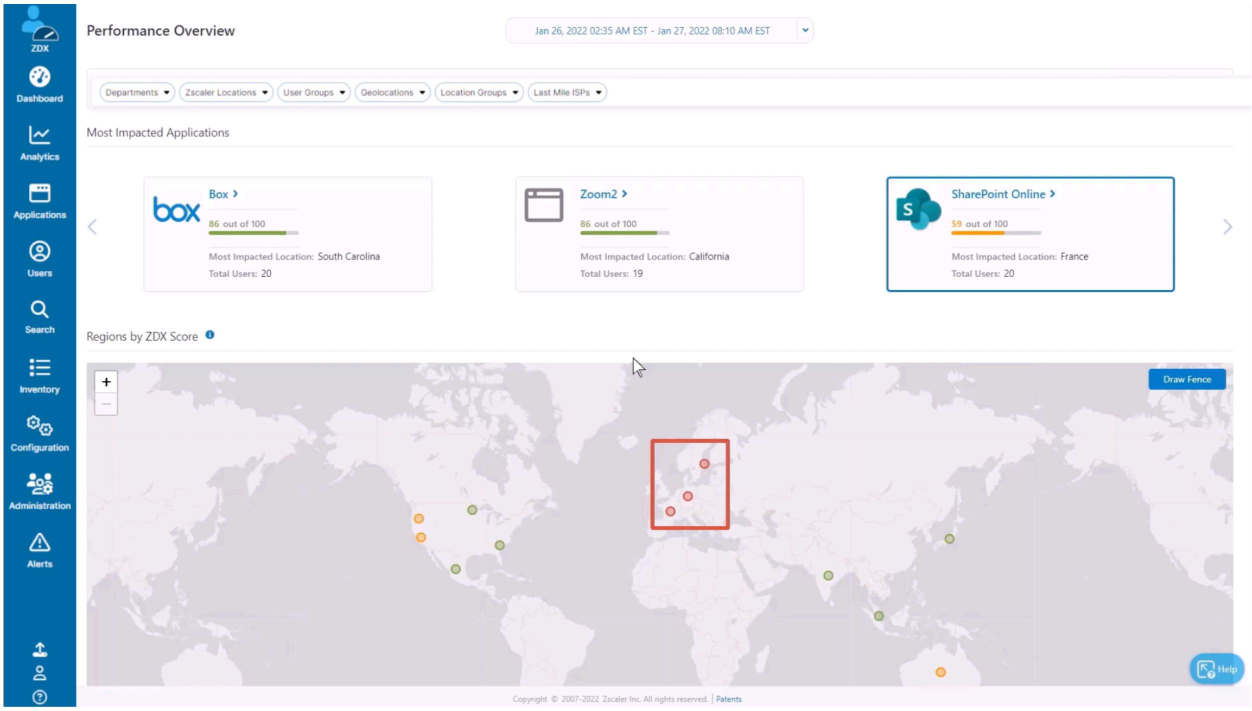
Regional Issues

For an internal app that would be your application team or tech support for a SaaS application., there may be situations where an application issue is limited to a geographic region and the ZDX dashboard is, again, a great starting point to confirm that.

On the regions by ZDX Score map, you'll see that only locations in the affected region show low scores. As before, you can then go to the applications dashboard and collect more details. Depending on the number of users in the affected region, the ZDX score over time graph will show a slight or more significant score drop.

To get a clearer picture, you could now apply a geolocations filter and check the ZDX score for that region, which, as expected, is a lot lower than the overall score.

Now that you've confirmed that this is a regional issue, you can update the employees in that region and get in touch with the application owner.



Performance Overview

Jan 26, 2022 02:35 AM EST - Jan 27, 2022 08:10 AM EST

Most Impacted Applications

Box
86 out of 100
Most Impacted Location: South Carolina
Total Users: 20

Zoom2
86 out of 100
Most Impacted Location: California
Total Users: 19

SharePoint Online
59 out of 100
Most Impacted Location: France
Total Users: 20

Regions by ZDX Score

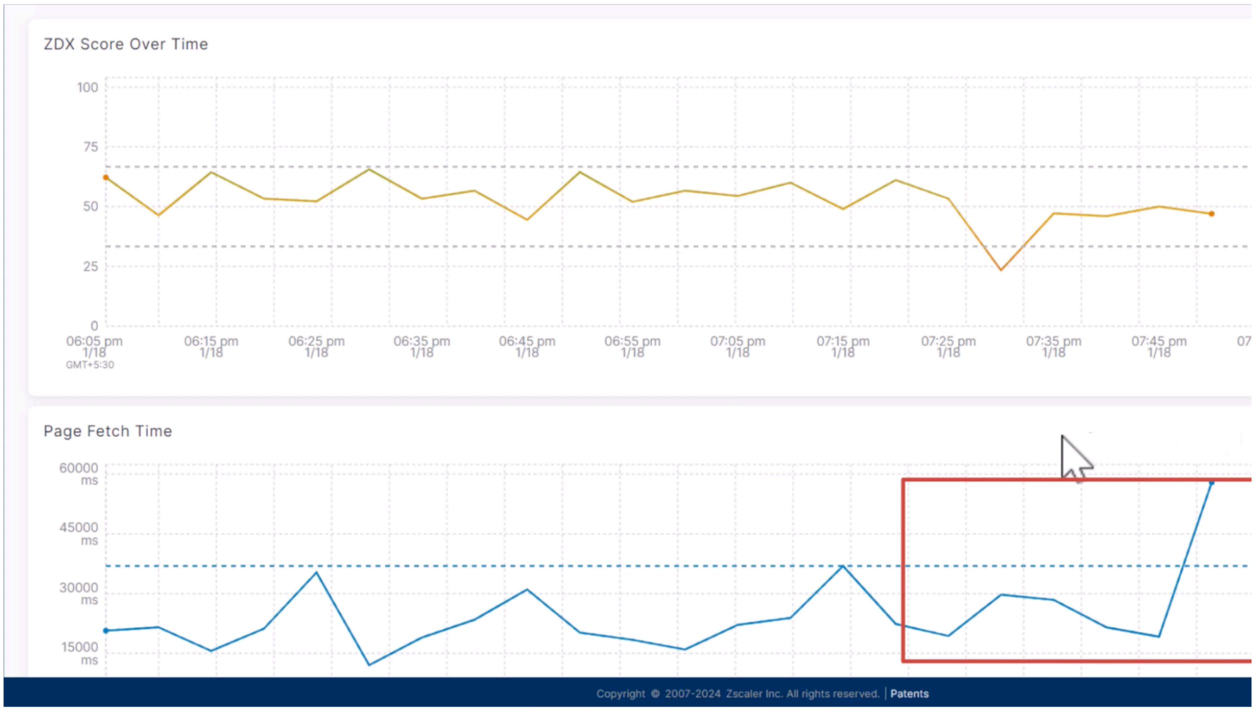
Copyright © 2007-2022 Zscaler Inc. All rights reserved. | Patents

Office Issues

In addition to more widespread issues, you may also have to deal with application degradation that only affects one of your office locations.

Again, a quick glance at the ZDX dashboard lets you confirm that. Except for the one location, the application is performing as expected.

Apply a Zscaler location filter and check the application ZDX score for that location. As before, you can then go to the applications dashboard and collect more details. As you can see, there is a significant ZDX score drop and a corresponding spike in page fetch time.



You can now update employees at that location, alert the application owner, and also escalate this ticket further. The level two support team will then investigate further to identify the root cause of the problem.

Level 2: Troubleshooting WiFi Issues

Scenario: A home-office user in the Marketing department reports problems with slow connectivity to applications that he uses on a daily basis, SharePoint Online being the most important one.

The Level 1 support team has completed their initial checks and verified that this is not a global, or regional issue.
As a Level 2 support engineer, you now need to troubleshoot this issue further.

Troubleshooting Checklist

Here is a list of questions to ask and items to check in order to identify WiFi problems during a ZDX Score drop (*Thresholds are estimates and may vary by customer):

□ Is WiFi Signal Strength < 65%* ?
Check in **Device Health -> WiFi Signal**

□ Is WiFi Type not an 802.11ac or 802.11ax, assuming the wireless interface type is 'AC' or 'AX' (Windows only)?
Check in **User Devices -> More Device Details -> Network**

□ Is WiFi Channel < 15, which indicates a 2.4 GHz channel?
Check in **More Device Details -> Network**

□ Is Network Bandwidth expected for the wireless interface (en0 for Mac)?
Check in **Device Health -> Network Bandwidth (interface name)**

- For 802.11ax, dropping well below 1 Gbps?
- For 802.11ac, dropping well below 300 Mbps?
- For 802.11n, dropping well below 100 Mbps?

□ Is Latency between the desktop and the gateway excessive or fluctuating over 50ms* ?
Check in **Cloud Path -> Hop to Gateway**

□ Is there Packet Loss on the Gateway and Egress node?
Check in **Cloud Path ->** Mouseover **Gateway** and **Egress -> Packet Loss**

□ Do any User Device Events show any of these attributes changing during the performance degradation?

Troubleshooting WiFi Issues

Since this issue is limited to a specific user, you can start your analysis on the user details page. It's a good idea to have a quick look at the device details and make a note of the user's WiFi adapter type and channel.

You can later check if the bandwidth for the wireless network is in line with the expectation for, let's say, an 802.11 AC network. Click on the ZDX score drop.

Remember, with a ZDX advanced or ZDX advanced plus plan, you can also use the analyze score function and display potential factors that may have contributed to the score. Then scroll down to the cloud path section.

- Is the latency between the device and the gateway excessive or fluctuating?
- Or is there a packet loss on the gateway or egress node?
- What was the wifi signal strength and wifi type at the time of the score drop?

Compare that to a point on the cloud path graph with no performance degradation.

Scroll down to the device health section, check the WiFi signal strength. Is WiFi signal strength lower than expected?

Next, verify that the network bandwidth is as expected for the wireless interface type you noted earlier.

And finally, check the user device events section. Do user device events show any of these attributes changing during the performance degradation? For example, look for change in wifi type, channel, or SSID, or a change in the gateway MAC address.

To try to resolve these issues, you could start a deep tracing session and then ask the user to debug their wifi. For example, have them reset the gateway, or suggest they move closer to their access point. That way, the deep tracing results give you a detailed before and after picture. And if the problems are still unresolved, escalate to a level three network specialist.

Level 2: Troubleshooting Zscaler Issues

Scenario: Several users in one geographic region report problems with slow connectivity to several applications. The Level 1 support team was not able to pinpoint the exact cause of what looks to be a regional issue.

As a Level 2 support engineer, you now need to troubleshoot this issue further.

Troubleshooting Checklist

Here is a list of questions to ask and items to check in order to identify Zscaler problems during a ZDX Score drop:

- □ Is Latency of Zscaler Cloud > 25 ms*?
  Check in **Cloud Path ->** Mouseover **Zscaler** icon

- □ Is the user going to an unexpected Zscaler ZIA Service Edge?
  Check in **Cloud Path ->** Mouseover **Zscaler** icon

- □ Are there excessive Zscaler Events showing ZIA or tunnel ‘Off’ or in ‘Unknown’ state?
  Check in **User Device Events**
  (Note: this may be a symptom of network issues and not a cause)

- □ Are there excessive Zscaler Events showing DTLS to TLS downgrades or Tunnel 2.0 to 1.0 downgrades?
  Check in **User Device Events**
  (Note: this may be a symptom of network issues and not a cause)

*Thresholds are estimates and may vary by customer

Troubleshooting Zscaler Issues

In the user details page, identify the ZDX score drop and then scroll down to review the cloud path details.

Is latency in the Zscaler cloud higher than expected? While latency in the Zscaler cloud is minimal, typically less than 1 millisecond, you may occasionally see slightly higher values. Anything higher than 25 milliseconds requires further investigation.

You should also check if, based on their location, the user is going to an unexpected Zscaler service. Scroll down further and have a closer look at the Zscaler category in the user device events section.

Are there excessive Zscaler events showing ZIA tunnel state changes or the tunnel is shown in the off or unknown state? Or are there excessive events showing DTLS to TLS downgrades or tunnel 2.0 to 1.0 downgrades? Keep in mind that these tunnel change events may be a symptom of network issues and not the cause.

For example, ZIA will downscale a tunnel from version 2.0 DTLS, to version 2.0/TLS, to version 1.0 when a network connection is unstable.

For Zscaler related issues, it is recommended to run a deep tracing session and attach the exported PDF to a Zscaler support ticket. You should also escalate the issue to a level three security specialist.

Level 2: Troubleshooting ISP or Internet Issues

Scenario: A user working from his home office reports problems with slow connectivity with applications he uses for his job, including Office 365 and a few custom applications. The Level 1 support team has already verified that this issue is limited to the one user.

As a Level 2 support engineer, you now need to troubleshoot this issue further.

Troubleshooting Checklist

Here is a list of questions to ask and items to check in order to identify ISP or Internet problems during a ZDX Score drop:

- ☐ Is Latency between Gateway and Egress excessive – bursting higher than normal (typically < 50ms*?)
  Check in **Cloud Path** -> Mouseover **Gateway to Egress** link

- ☐ Is Packet Loss between Gateway and Egress sustained > 0?
  Check in **Cloud Path** -> Toggle to **Command Line View**

- ☐ Is Latency between Egress and Zscaler Service Edge higher than normal (typically < 100ms*)?
  Check in **Cloud Path**
  Expand leg between **Egress** and **Zscaler** -> Identify high-latency hop

- ☐ Is Latency between Zscaler Service Edge and the application higher than normal?
  Check in **Cloud Path**
  Expand leg between **Zscaler** and **Application** -> Identify high-latency hop

*Thresholds are estimates and may vary by customer

Troubleshooting ISP or Internet Issues

You can start by searching for the user that reported the issue and select an application to display the user details page.

To check for potential issues with the user's internet service provider, scroll down to the cloud path section and focus on latency between the user's gateway and egress point, which is **typically less than 50 milliseconds**.

In the cloud path graph, you can check how much latency is added by the client to egress leg. Then expand that segment in hop view and check the latency and packet loss details for each of the hops. If you prefer, you can also check the command line view for latency details and sustained packet loss between gateway and egress.

Here are some suggestions to help troubleshooting the issue:

- If the users are working from home, you can ask them to examine their ISP connection.
- You can also quickly check the ZDX ISP insights dashboard or any ongoing incidents in the user's region.
- Provided this feature is available with your ZDX subscription, you can also run a deep tracing session for a few minutes and check if the client to egress leg shows high latency and or packet loss during that time. And if your investigation doesn't identify the root cause, you can always escalate the issue to a level three network specialist.
- Besides ISP issues, there is always a chance excessive latency or packet loss is caused by a hop either between the egress point and Zscaler or between Zscaler and the application. Have a look at the cloud path graph. Is the latency between the egress point and the Zscaler service edge higher than normal? **Typically, this should be less than one hundred milliseconds.** Or is latency between the Zscaler service edge and the application higher than normal? In the hop view, you can quickly expand a way that shows the highest latency and then check the details for the individual hops.

If you have identified high latency or packet loss on either leg, it is a good idea to run a deep tracing session and attach the exported PDF to a Zscaler support ticket. And you should escalate the issue to a level three network specialist.

Level 2: Troubleshooting Desktop Issues

Scenario: A user reports problems with sluggish, unresponsive applications. The Level 1 support team has already verified that this is not a global or regional issue.

As a Level 2 support engineer, you now need to troubleshoot this issue further.

Troubleshooting Checklist

Here is a list of questions to ask and items to check in order to identify issues with a user's desktop during a ZDX Score drop:

- □ Is CPU bursting high (> 85%*)?
  Check in **User Device** Metrics -> **CPU Usage**

- □ Is Memory bursting high (> 85%*)?
  Check in **User Device** Metrics -> **Memory**

- □ Is Disk Usage bursting high (> 98%*)?
  Check in **User Device** Metrics -> **Disk Usage**

- □ Is Disk I/O bursting high?
  Check **User Device** Metrics -> **Disk Inbound/Outbound**

- □ Is Network Interface I/O bursting high?
  Check in **User Device** Metrics -> **Network Inbound/Outbound**

- □ Is the user on battery during the score drop?
  Check in **User Device** Metrics -> **Battery Level**

- □ Are unexpected User Device Events being generated?
  Check in **User Device Events** (Note: CPU speed change events can be ignored, as they are typically not impactful)

*Thresholds are estimates and may vary by customer

Troubleshooting Desktop Issues

To identify issues with the end user device during a ZDX score drop, You can start by searching for the user that reported the issue and select one application to display the user details page.

Click on a graph point with a poor ZDX score.

Remember, with a ZDX advanced or ZDX advanced plus plan, you can use the analyze score function and display potential factors that may have contributed to the score drop. In this example, the automated root cause analysis suggests high CPU utilization as a possible factor.

Scroll down to the device health section to confirm what you are seeing.

Try to identify a device parameter that shows a significant change during the score drop, looking for any burst in CPU, memory, disk, or network usage. As suggested by the automated root cause analysis, you might see that CPU usage burst up to one hundred percent during the score drop. If the device is a laptop, check to see if it's running on battery during the score drop.

You can also check for unexpected user device events such as changing interface status, tunnel changes, etc. Events that indicate changes in CPU speed typically don't impact application performance and can be ignored.

After reviewing the graphs in the device health section, here are some suggested actions you can take to resolve the issue:

1. Ask the user to close and restart applications. Stop processes, or reboot the device.
2. Provided this feature is available with your ZDX subscription, you can run a deep tracing session for a few minutes and then review the list of top processes.

If your investigation doesn't identify the root cause, you can always escalate the issue to a level three desktop specialist.

Level 2: Troubleshooting DNS or VPN Issues

Scenario: The Level 1 support team had a number of complaints from users in the Finance department not being able to access a cloud-based custom application. This problem seems to affect users in one geographic region, but initial checks were inconclusive.

As a Level 2 support engineer, you now need to troubleshoot this issue further.

Troubleshooting Checklist

Here is a list of questions to ask and items to check in order to identify DNS or VPN problems during a ZDX Score drop:

- □ Is DNS Resolution Time abnormally high (> 200ms*) or spiking during the ZDX Score drop?
  Check in **Web Probe** Metrics -> **DNS Resolve Time**

- □ Is there a VPN Client running that coincides with ZDX Score drop or high DNS?
  Check in **Device Health** -> **Network Bandwidth (VPN Client Name)** (Windows only)

- □ Is there a VPN client running and a DNS suffix change showing a domain change that coincides with a ZDX Score drop?
  Check in **User Device Events**

*Thresholds are estimates and may vary by customer

Troubleshooting DNS or VPN Issues

With a DNS issue, you'll likely see a lot of users having a poor experience with multiple applications.

Let's look at the details for one such user.

DNS Related

With server response time, page fetch time and availability being pretty flat, pay close attention to the DNS Resolve time graph. Is DNS resolution time that normally high or spiking during the ZDX score drop?

Based on your findings, you should contact your network infrastructure team and suggest switching to another DNS server. And if that doesn't fix the issue, you can always escalate to a level three network specialist.

VPN Related

You can also check if there is a VPN client running that coincides with a ZDX score drop or a high DNS resolution time.

For Windows devices, scroll down to the device health section where one of the network bandwidth graphs will identify the VPN client name.

Make sure you scroll down to the user device events section and look for a DNS suffix change event that coincided with the ZDX score drop.

As a quick test, ask one of the affected users to turn off their VPN client, then try to access the application again and confirm whether or not that resolved the issue. And if your investigation doesn't identify the root cause, you can always escalate the issue to a level three security specialist.

Level 2: Troubleshooting Application Issues

Scenario: The Level 1 support team had a number of complaints from users not being able to access a cloud-based Finance application. This problem seems to affect users in different locations and regions, but initial checks were inconclusive.

As a Level 2 support engineer, you now need to troubleshoot this issue further.

Troubleshooting Checklist

Here is a list of questions to ask and items to check in order to identify application-related issues during a ZDX Score drop:

- □ Is Server Response Time highly correlated with ZDX Score Drop and a large percentage of Page Fetch Time, while Latency is flat during the same time?
  Check in **Web Probe Metrics -> Server Response Time**

Troubleshooting Application Issues

A good starting point for analyzing an application issue is the user overview page for that application. What would you expect to see here? Well, you'll likely see several users having a poor experience.

Start by selecting one of those affected users and see what's going on. In the user's detail page, pay close attention to the web probe metrics.

- Is the ZDX score drop closely correlated with a spike in either server response time or page fetch time?
- Is there a change in availability?

It's good practice to send out an update to let the affected employees know that this is likely an issue with the application itself. You can also use a site like Down Detector to quickly check for service degradations of popular SaaS applications like OneDrive, AWS, Gmail, and others. And you should escalate the issue to a level three application specialist.

Level 3: Troubleshooting Escalated Tickets

As described in the previous sections, whenever the Level 2 analysis of application, network or end user issues is inconclusive, unresolved tickets can be escalated further to Level 3 support specialists.

These are the recommended steps for each level 3 specialist to close escalated tickets:

Network Specialist

Detailed investigation of issue identified by ZDX, leveraging Cloud Path, DNS times and other network metrics

Security Specialist

Leveraging Cloud Path latency metrics to check if the Zscaler Cloud is exhibiting excessive Latency or generating User Device Events

Working with Zscaler Support to identify root cause

Desktop Specialist

Detailed investigation of issue identified by ZDX, leveraging User Device Metrics, Device Inventory, User Device Events and other desktop metrics

Application Specialist

Detailed investigation of issue identified by ZDX, leveraging Page Fetch Time, Server Response Time, Software Inventory and other end user metrics

Proactively Reducing New Tickets

In addition to responding to user-reported issues, support teams, for example an organization's Global Operations team, can leverage ZDX for proactive, 24 x 7 monitoring.

Recommended best practice is to leverage Webhooks and Alerts to notify support teams of performance issues.

Remember: Alerts enable you to monitor device, application, network performance, and ZDX Score. Alert rules can be configured, so that alerts are triggered when a preset threshold is exceeded for different types of events.

Level 1: Being Proactive about Application Issues

Rather than wait for users to open support tickets, you can monitor the ZDX Dashboard for widespread score drops and set up alerts that notify your IT team of application issues.

Here is a list of questions to ask and items to check in order to recognize widespread ZDX Score drops:

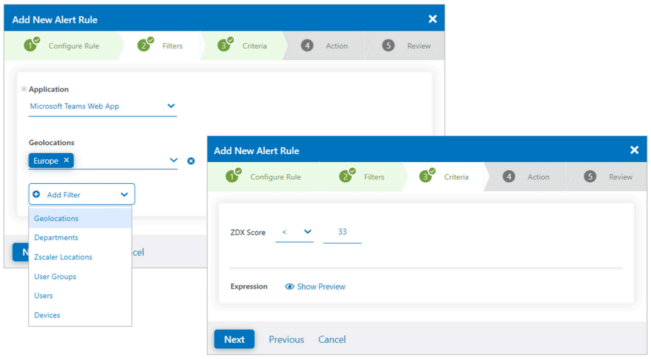
- □ Is the entire organization experiencing an application ZDX Score drop?
  Check in **Application** Tab -> Choose **Application**, or check for **ZDX Score** alert

- □ Is a geographic region experiencing an application ZDX Score drop?
  Check in **Application** Tab -> Choose **Application**, or check for **ZDX Score** alert

- □ Is an entire office experiencing an application degradation?
  Check in **Application** Tab -> Choose **Application**, or check for **ZDX Score** alert

Remember, you can configure alerts based on ZDX Score and apply filters as needed.

Based on ZDX Score indications and alerts, you can take action before tickets are opened. In addition to updating your employees, you should inform the application owner about the service degradation. For an internal application, that would be your Application team, or tech support for a SaaS application.



Add New Alert Rule

Application: Microsoft Teams Web App

Geolocations: Europe

Add New Alert Rule

ZDX Score < 33

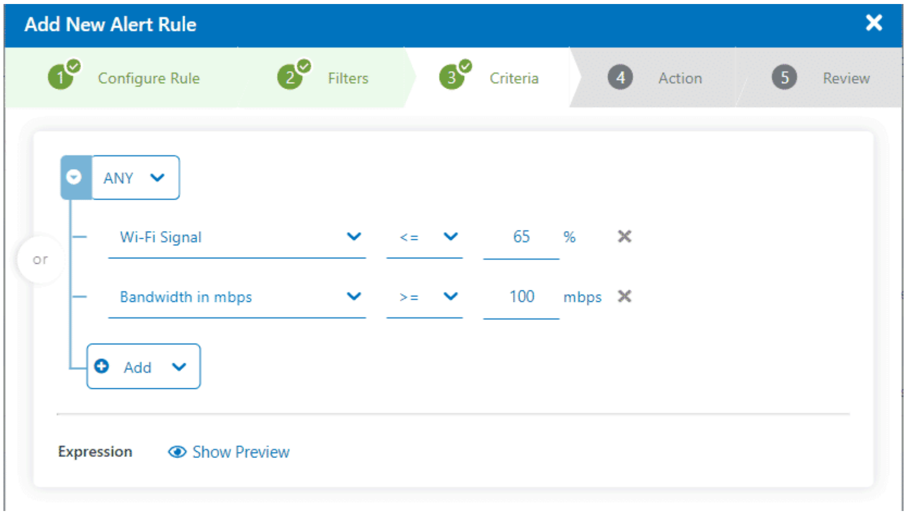
Expression

Level 2: Being Proactive about Application Issues

The Level 2 Support team can use alerts to be proactive about common network, Zscaler or desktop-related issues.

WIFI ISSUES

Alert Example: **Who has weak WiFi?**



ANY

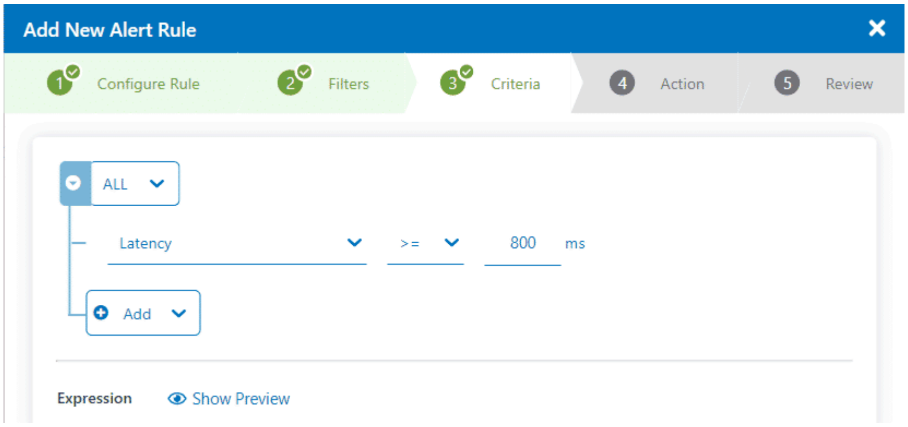
or

Wi-Fi Signal <= 65 %

Bandwidth in mbps >= 100 mbps

LATENCY ISSUES

Alert Example: **Who has high latency occurring on a Zscaler data center, ISP or Internet hop?**

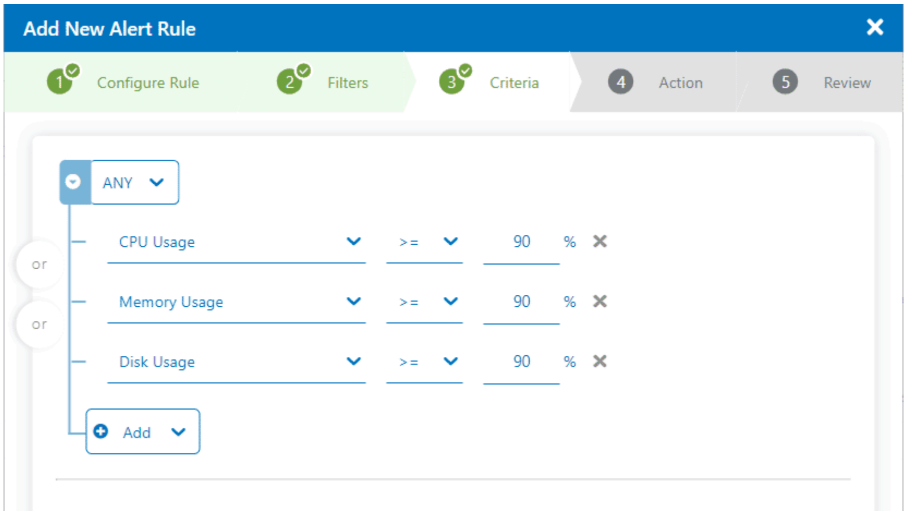


ALL

Latency >= 800 ms

DESKTOP ISSUES

Alert Example: **Who has a poorly performing desktop?**



Add New Alert Rule

1 Configure Rule 2 Filters 3 Criteria 4 Action 5 Review

ANY

CPU Usage >= 90 %

or

Memory Usage >= 90 %

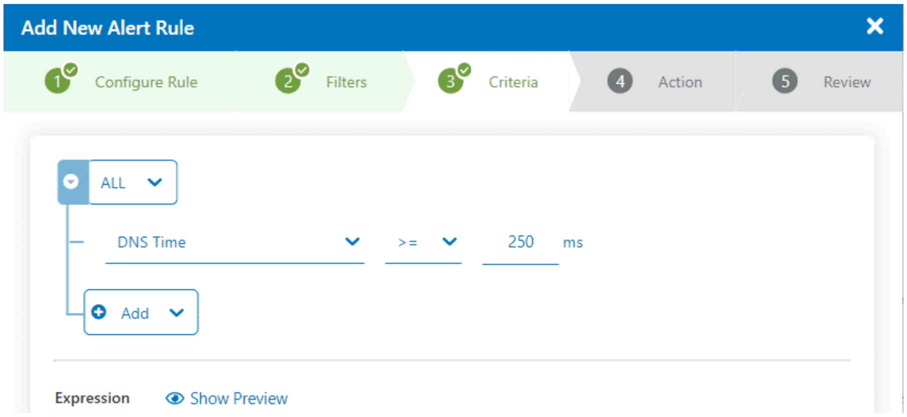
or

Disk Usage >= 90 %

Add

DNS ISSUES

Alert Example: **Who has a DNS-related issue?**



Add New Alert Rule

1 Configure Rule 2 Filters 3 Criteria 4 Action 5 Review

ALL

DNS Time >= 250 ms

Add

Expression Show Preview

The alert criteria and thresholds in the examples above will vary based on your conditions and reporting needs.

Level 3: Being Proactive about Network Analysis & Planning

Beyond the day-to-day operations, Level 3 Support specialists are often involved in broader analysis of an organization's network infrastructure and application analysis.

Here’s a list of questions that ZDX can help answer in the analysis of general performance issues:

Network Specialist

- How do various ISPs differ in terms of performance and latency?
- How do various ISPs peer with different backbone providers?

Application Specialist

- Why do particular applications underperform other applications, based on global benchmark comparisons?
- Is application performance impacted by their hosting location?

Security Specialist

- How do specific Zscaler data centers/tunnel settings play a role in performance?

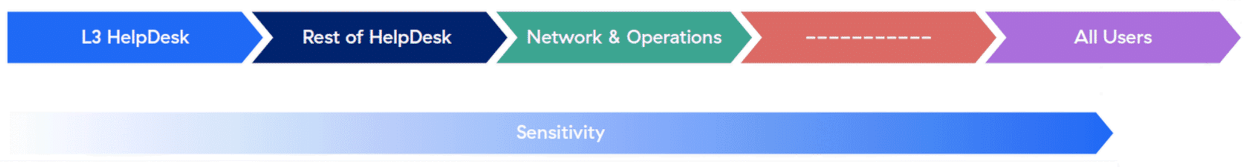
Desktop Specialist

- Why do particular desktops underperform other desktops?
- Are employee desktops up to specification (type, CPU, memory, etc.)
- Are there more widespread issues affecting more than one desktop?

BEST PRACTICES FOR OPERATIONALIZING ZDX

Rollout Strategy

Although the ZDX service does not make any forwarding decisions or change configurations on end user devices, it is recommended to roll out the ZDX service in a staggered fashion, so that any adverse impact on the end user experience is prevented or identified at an early stage of deployment and tackled.



L3 HelpDesk

Rest of HelpDesk

Network & Operations

All Users

Sensitivity

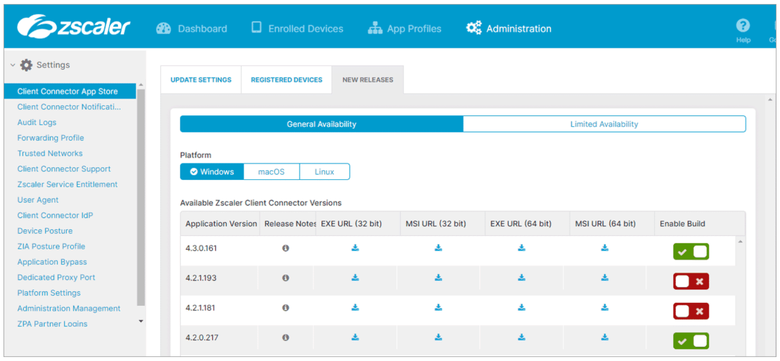
Step 1: Meet prerequisites

Several destination **domains** need to be placed on the a**llowlist on your firewall** or non-Zscaler proxy, including probes that are initiated by Zscaler Client Connector, as well as the monitored information sent by Zscaler Client Connector to the Zscaler cloud.

Also, make sure that your users' devices have inbound rules that **allow** the Zscaler Client Connector binaries and **processes**. For details on the required domains and process, check the Zscaler Help documentation.

Step 2: Zscaler Client Connector Version

Since ZDX runs as a module within ZCC, we have a one-to-many compatibility relationship. Ensuring support for the latest ZDX version is key to take advantage of new features and bug fixes.



Platform

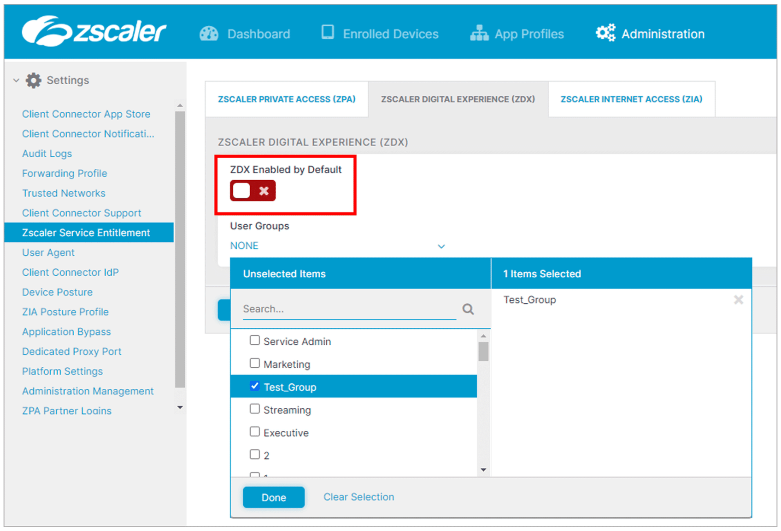
● Windows ○ macOS ○ Linux

Available Zscaler Client Connector Versions

Application Version	Release Notes	EXE URL (32 bit)	MSI URL (32 bit)	EXE URL (64 bit)	MSI URL (64 bit)	Enable Build
4.3.0.161	ⓘ	⤓	⤓	⤓	⤓	✓
4.2.1.193	ⓘ	⤓	⤓	⤓	⤓	✗
4.2.1.181	ⓘ	⤓	⤓	⤓	⤓	✗
4.2.0.217	ⓘ	⤓	⤓	⤓	⤓	✓

Step 3: Pilot Rollout

The rollout should begin with the users that are least resistant to change and self-sufficient in debugging basic device issues such as Tier 3 help desk.



ZSCALER DIGITAL EXPERIENCE (ZDX)

ZDX Enabled by Default ☒

User Groups
NONE

Unselected Items
- ☐ Service Admin
- ☐ Marketing
- ☑ Test_Group
- ☐ Streaming
- ☐ Executive
- ☐ 2

1 Items Selected
Test_Group

Step 4: Successful Staggered Rollout

After a week of a pilot group of users running the service without disruptions, creating a staggered rollout plan is next in deploying the entitlement across the entire user base.

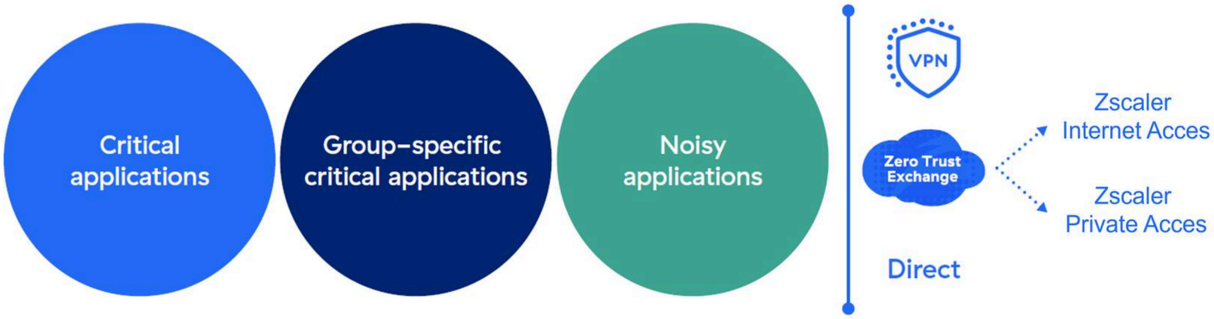
It is recommended to start by rolling out across an entire team, such as the helpdesk, before continuing with other teams. The number of rollout phases depends on the organization’s size and appetite for change. The recommendation is to onboard up to 5,000 users at a time.

Application Strategy

To ensure ZDX does not impact the end user experience that we are monitoring in the first place, the number of probes a user can run is limited to 30. Therefore it is important to consider which applications to monitor, how these applications are delivered and how to best organize them for accurate reporting.

Application Categories

It is recommended best practice to have applications selected based on three usage-based categories.



- **Critical Applications:** These applications are critical from an employee/user productivity perspective and need to be monitored across the board regularly. Common examples include Microsoft 365, Zoom, etc.

- **Group-Specific Applications:** This category is creating groups of applications segmented based on a team's priority. For example, the PagerDuty application would be critical for the Operations team, but the Salesforce application wouldn't. Rather, the Sales team would prioritize the Salesforce application.

- **Noisy Applications:** To derive maximum value from ZDX, monitoring unstable applications and generating the top ticket volumes is essential.

  The noisy application category is the only dynamic category, as the application state varies from stable to unstable at a given time. This means it's important to revisit this list periodically.

  During quarterly reviews, previously noisy applications can be disabled, and others onboarded. This also leaves the opportunity to run a Deep Trace on disabled noisy applications should a user complain about performance.

At any given point in time, an organization relies on a multitude of applications. However, within the context of End User Experience Monitoring, it is not possible to measure performance of them all.

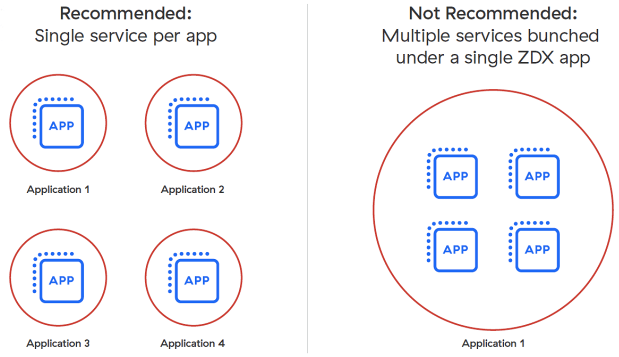
It is recommended to focus on a few select delivery paths. With this in mind, if a good balance between the delivery paths and usage-based app categories is achieved, existing data can be leveraged to baseline performance based on forwarding used. For example, if your organization routes Outlook Online through Zscaler Internet Access (ZIA), that can be used to baseline performance for all apps funneled through ZIA.

- **Zscaler Internet Access (ZIA):** Data-driven SaaS applications are generally funneled through the ZIA Cloud Infrastructure.
- **Zscaler Private Access (ZPA):** Private applications that an organization manages and are not publicly accessible are primary drivers for ZPA. Source IP compliance requirements can also drive apps to be routed through ZPA.
- **VPNs:** Organizations yet to adopt full zero trust will have private applications riding the legacy VPN tunnels.
- **Direct/Zscaler Bypassed:** Real-time applications, such as UCaaS, are usually bypassed from ZIA. Users on the production network will usually route DIRECT to private applications.

Application Layout

A suitable application layout is essential in ensuring ZDX dashboards report the accurate status for a particular service.

Example: SAP is critical for my organization and there are two instances, Europe and Americas, that are independent of each other and either can go down without the other. It's then recommended to set up two applications: SAP Americas and SAP Europe.



Having both services combined under a single SAP application poses the risk of diluting trends for each application and prevents the ability to understand how each instance is performing.

UCaaS Applications

In order to get the most accurate Cloud path information for UCaaS applications, Zscaler recommends configuring Autosense probes.

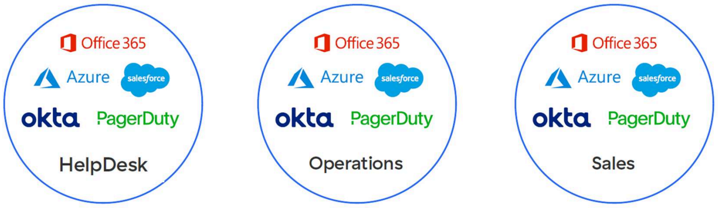
Probes

Configuring probes correctly is at the core of ZDX user experience monitoring. This section provides best practice recommendations for each factor of the probe configuration.

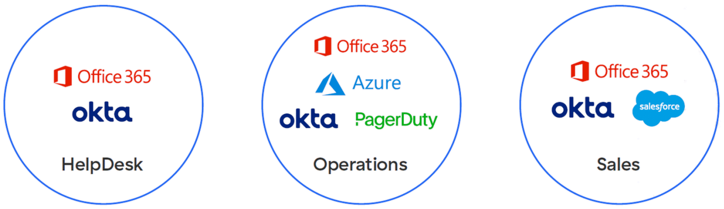
Criteria: Run for select users/all

The 30 probe per user limit means utilization of active probes is critical to a platform's health. These approaches depend on the actual probe entitlement of an organization.

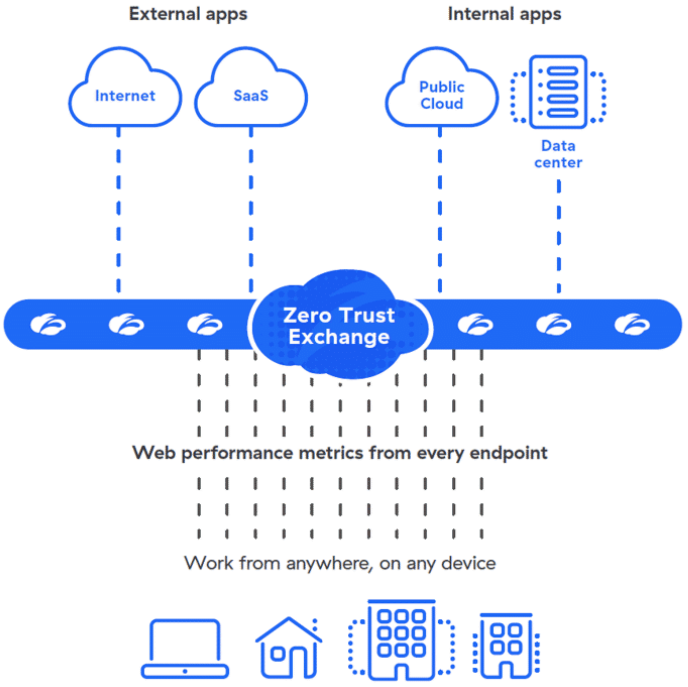
- **Organizations with 30 probes:** Since you can only enable 30 probes on the platform at a time, running each probe from everyone with ZDX enabled provides a more granular understanding of an application's performance. However, if the application is not accessible to everyone, only users with access should be assigned to the probe.



- **Organizations with more than 30 probes:** In this case, ensuring the entitled probes can be utilized is vital since the 30 probes per user limit is still enforced, so proper planning is required. The specific group applications in this scenario should only be run for the concerned group, as this helps ensure other users can run probes for maximum applications that are of interest to them.



Criteria: DDOS concerns



With ZDX, whenever a probe flows through Zscaler Clouds, the service edges perform smart caching to ensure the end service does not get overwhelmed and, at the same time, gives users accurate results back.

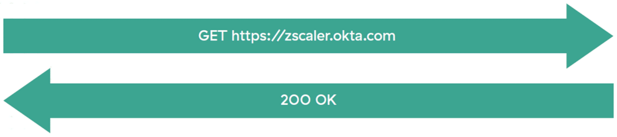
When the application is accessed directly by the client, all requests will reach the end service; hence, it's essential to scale testing accordingly. Given that a privately-hosted application might not have the same resources as a SaaS application, starting small with a group/department of geographically dispersed users is recommended. The idea is to keep the total number of users small enough for the service to sustain requests. A Deep Trace can be run on demand if an issue arises for a user who is not running the application probing.

Best Practices for Web Probes

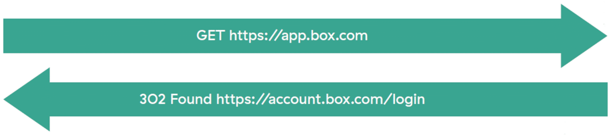
Setting the redirect and expected response codes is critical to ensure the metrics represent the desired performance. The configuration should be based on how the application responds to an unauthenticated HTTP request.

Here are two examples:

1. For an application that responds with a **200 OK** response code, the success must be measured against the 200 and redirects followed.



2. For an application that redirects to another service such as login with a **302 Found**, measuring availability based on a 200 OK coming from a different service than the original renders the metrics skewed. Hence, availability should be measured based on the ability of the original application to redirect.



Best Practices for Cloud Path Probes

- Since the internet is “best-effort,” and devices on the internet do not consistently respond to a specific protocol for network measurements, it’s recommended to use the **Adaptive** protocol for the Cloud Path probe.

  In custom routing situations, such as a particular port/protocol being bypassed, it’s vital to use the specific protocol and port to ensure correct Cloud Path probe metrics.

- **Packet Count** is the number of traces each cloud path attempts, this plays a pivotal role on the number of connection requests a destination, perimeter firewalls, and intermediate devices receive. Setting this up to an optimum level is critical for efficient probing.

  Recommendation is to use a forwarding-based approach here, use 5 for SaaS ZIA//Direct destinations and 3 for Private/ZPA destinations.

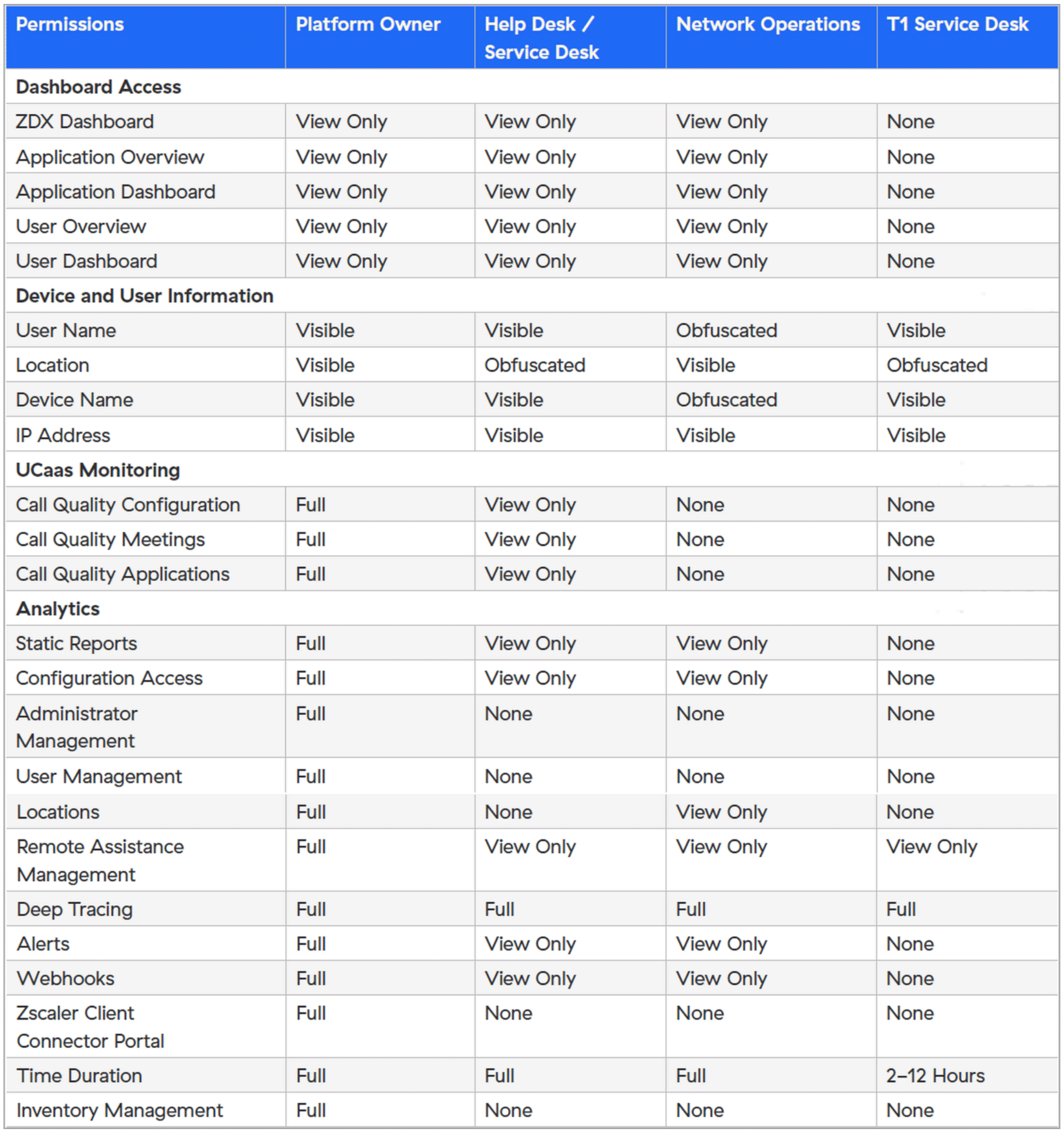
Administrator Access

Provisioning sufficient and “just needed” levels of ZDX access to personnel is critical to maintaining platform hygiene. Along with authentication, authorization is a major aspect of Administrator access.

ZDX provides the ability to granularly control the level of access an administrator has in the form of permission-based roles.

These roles can then be assigned to administrators within a predefined scope.

It is recommended best practice to customize access for various different personas as shown in the example below.



Permissions	Platform Owner	Help Desk / Service Desk	Network Operations	T1 Service Desk
Dashboard Access				
ZDX Dashboard	View Only	View Only	View Only	None
Application Overview	View Only	View Only	View Only	None
Application Dashboard	View Only	View Only	View Only	None
User Overview	View Only	View Only	View Only	None
User Dashboard	View Only	View Only	View Only	None
Device and User Information				
User Name	Visible	Visible	Obfuscated	Visible
Location	Visible	Obfuscated	Visible	Obfuscated
Device Name	Visible	Visible	Obfuscated	Visible
IP Address	Visible	Visible	Visible	Visible
UCaas Monitoring				
Call Quality Configuration	Full	View Only	None	None
Call Quality Meetings	Full	View Only	None	None
Call Quality Applications	Full	View Only	None	None
Analytics				
Static Reports	Full	View Only	View Only	None
Configuration Access	Full	View Only	View Only	None
Administrator Management	Full	None	None	None
User Management	Full	None	None	None
Locations	Full	None	View Only	None
Remote Assistance Management	Full	View Only	View Only	View Only
Deep Tracing	Full	Full	Full	Full
Alerts	Full	View Only	View Only	None
Webhooks	Full	View Only	View Only	None
Zscaler Client Connector Portal	Full	None	None	None
Time Duration	Full	Full	Full	2–12 Hours
Inventory Management	Full	None	None	None

Alerting

ZDX collects many data points, but it’s not possible to manually sift through them. To address this challenge, you should configure Alerts within ZDX. Alerts drive proactiveness with notifications that act as early alarms before the wider population feels the impact.

This section provides best practice recommendations for different alert configurations.

Condition values

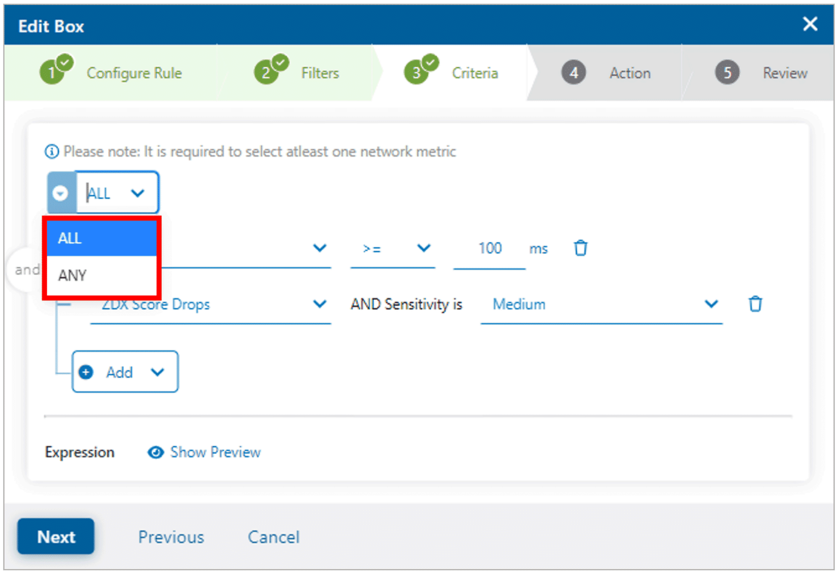
Setting up alerts with the right conditions is critical to identifying issues before they take shape. From an end user perspective, performance can be slow, or requests can fail at various stages. Here are the most important metrics to be considered:

	Slowness	Failure	Comprehensive
Web Probe	Page Fetch, DNS Time	Availability	ZDX Score, Score Drops
Cloud Path Probe	Latency	Loss	

CPU Utilization, Memory Utilization and **Wi-Fi Signal Strength** can similarly be configured from the device health perspective.

Nesting

Nesting conditions in an alert rule is an important configuration.



Please note: It is required to select atleast one network metric

ALL

>= 100 ms

ZDX Score Drops AND Sensitivity is Medium

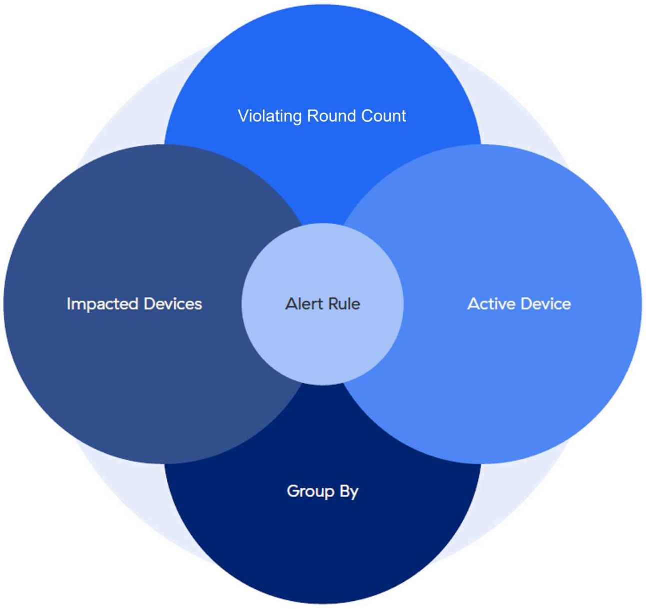
Conditions nested with a logical ‘OR’ will cover all the user experience issues.

Nesting them with an ‘AND’ won’t trigger the alert unless all the conditions are violated. This can cause alerts to stay silent during an actual service degradation and is not recommended.

Throttling: Violating Count, Devices, and Group By

Setting additional throttles on top of violating conditions helps to get alert rules production ready. Click each marker below to see recommended settings.

Violating Rounds Count: Setting this to a number >1 is important to prevent “spike” or a “one off” issue alerting. Alerts should trigger on sustained violations only, setting this at 2 violating counts is a right balance.

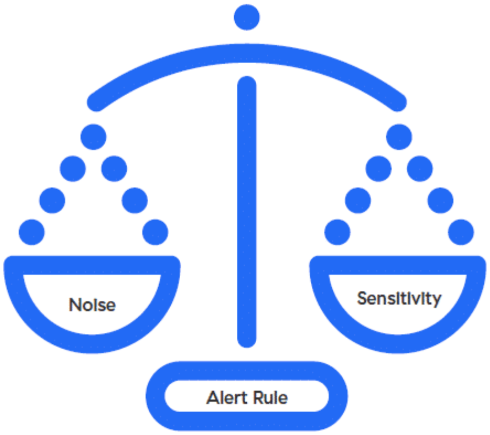


Impacted Devices: This number should be set at the value which translates to a significant number of users seeing poor performance. In order to better scale the alert, it’s recommended to set this to a percentage for violating devices and set a Minimum Device count to the smallest population of the group by entity of interest.

Active Devices: This is very important to set a scalable global alert. This should be set to the total population of the smallest group by entity the organization needs to be alerted upon.

Group By: This value determines the scope for Devices and Violating Count. The preferred value here varies by organization. An organization with known Zscaler locations available for the majority of users can use them vs. others can utilize Cities or Regions.

Tweaking/Soak Period

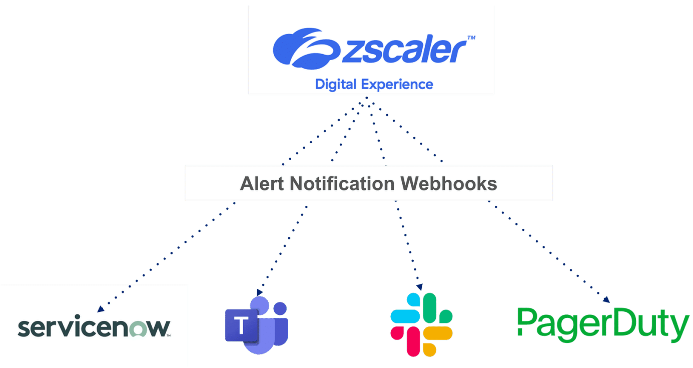


Alerts need constant tuning and tweaking over a soak period to be operationalized. At least a two week soak period is recommended after ZDX is rolled out to all users.

Getting the right balance between alert noisiness and sensitivity is key to optimal alerting.

ITSM/IM integrations with webhook

To reap the full benefits of alerting, it's recommended to configure webhook notifications for generating automatic tickets and have a process to mitigate tickets. This ensures a process is built around alerts and incidents do not go unnoticed for long.



Setting up webhooks to IM tools such as Slack and Microsoft Teams also helps to get more eyes on emerging issues before they become critical.

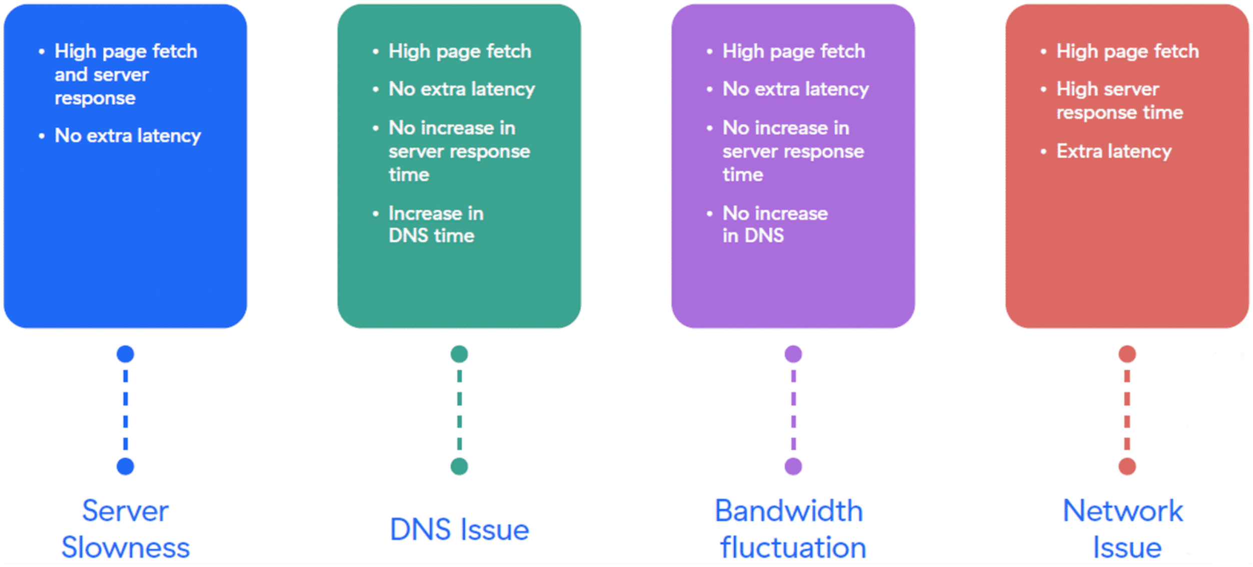
ITSM Routing

Once the tickets are created, the next step is routing them to the relevant team. Here, an approach needs to be taken depending on the delivery path of the alerted application and the layer of alert rule.

Data Analysis

With all the performance data available in ZDX, it’s important to look at metrics within the context of other available metrics (same timestamp) such as comparisons of application performance to network and device performance.

Here’s a recommended way of looking at Page Fetch Time, Server Response Time, DNS Time and Latency to derive actionable insights:



- High page fetch and server response
- No extra latency

Server Slowness

- High page fetch
- No extra latency
- No increase in server response time
- Increase in DNS time

DNS Issue

- High page fetch
- No extra latency
- No increase in server response time
- No increase in DNS

Bandwidth fluctuation

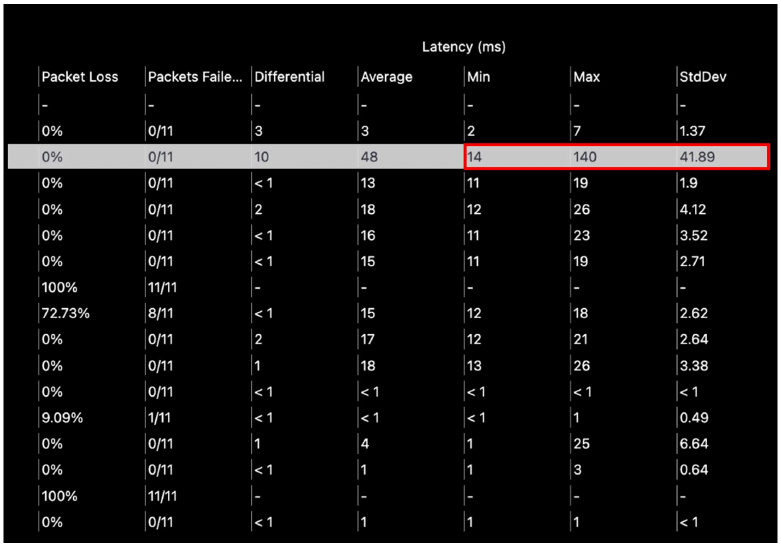
- High page fetch
- High server response time
- Extra latency

Network Issue

UCaaS Monitoring

When it comes to Call Quality applications, ZDX Score is the most important metric on a user’s overall meeting experience. Looking at network performance, Jitter is also an important factor that impacts real-time applications in particular.

In the CLI View of Cloud Path, the StdDev column highlights the impact of jitter, the highlighted hop in the example screenshot is adding between 14 to 140 ms of latency driving down performance.



			Latency (ms)			
Packet Loss	Packets Faile...	Differential	Average	Min	Max	StdDev
-	-	-	-	-	-	-
0%	0/11	3	3	2	7	1.37
0%	0/11	10	48	14	140	41.89
0%	0/11	< 1	13	11	19	1.9
0%	0/11	2	18	12	26	4.12
0%	0/11	< 1	16	11	23	3.52
0%	0/11	< 1	15	11	19	2.71
100%	11/11	-	-	-	-	-
72.73%	8/11	< 1	15	12	18	2.62
0%	0/11	2	17	12	21	2.64
0%	0/11	1	18	13	26	3.38
0%	0/11	< 1	< 1	< 1	< 1	< 1
9.09%	1/11	< 1	< 1	< 1	1	0.49
0%	0/11	1	4	1	25	6.64
0%	0/11	< 1	1	1	3	0.64
100%	11/11	-	-	-	-	-
0%	0/11	< 1	1	1	1	< 1

RECAP

From this study guide, you should now be able to:

1. **Describe** what Zscaler Digital Experience (ZDX) is and why it was created

2. **Describe** the core components that make up ZDX and the important aspects of each component

3. **Describe** the various dashboards, graphs and widgets within the ZDX Administrator Portal

4. **Understand** and interpret the presented data

5. **Configure** ZDX components and functions

6. **Analyze** ZDX dashboards and metrics to troubleshoot user experience issues