



Deliver Exceptional
End User Experiences
with **ZDX Copilot**

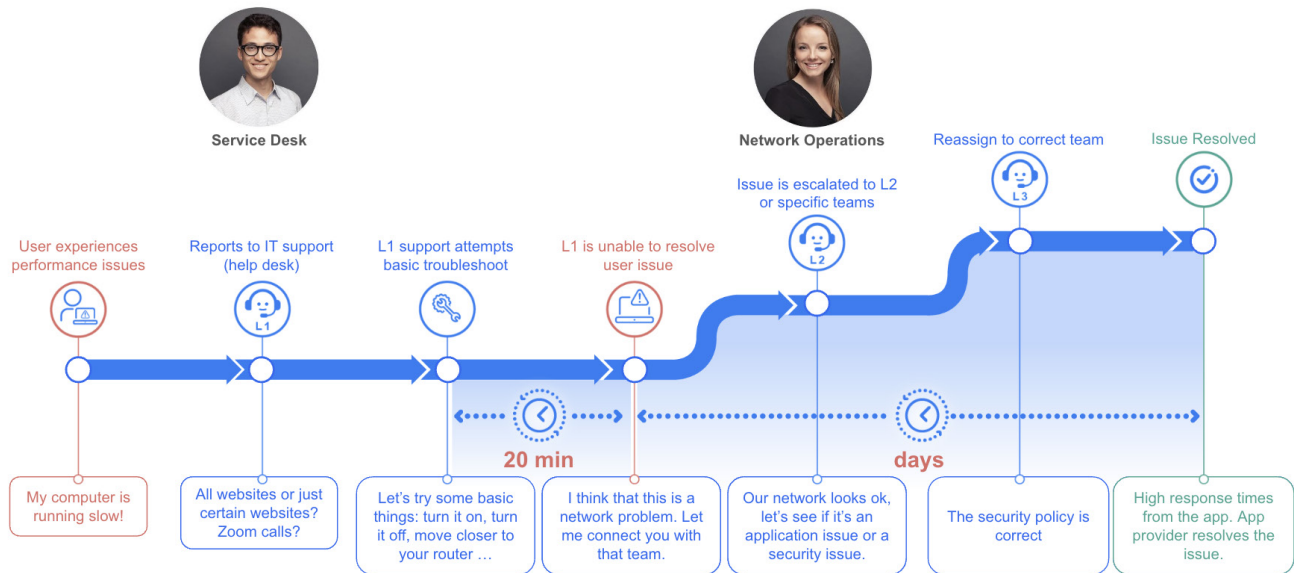
Table of Contents

Introduction	3
Getting Access to ZDX Copilot	8
Using ZDX Copilot	8
Prompts	8
Clickable prompts	8
Supervised learning feedback	8
Prompt Examples	9
Foundational questions	9
Product knowledge questions	11
Configuration questions	12
Best practice questions	13
Analytics questions	14
Copilot Example Scenarios	15
Wi-Fi Connectivity Issues	15
End User Device Issues (high CPU)	15
Product Usage disclaimer	17

Introduction

Our businesses rely on technology to keep employees productive, and customers today expect flawless digital experiences when interacting with customer support, placing orders, or using online services.

IT teams provide a critical function here—they keep the bedrock of the business, its technology, running smoothly. They have the essential task to ensure that all networks, applications, and services—even those that they don't control, perform reliably 24/7. Below is the daily challenge IT teams face, which is often tedious, expensive, and leaves end users frustrated.



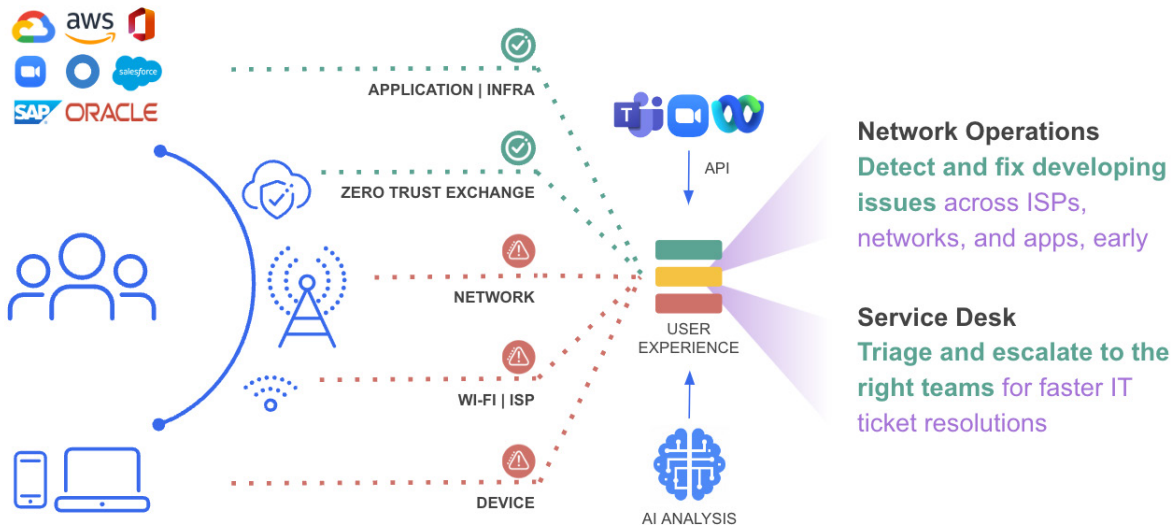
We built Zscaler Digital Experience (ZDX) to provide IT teams with end-to-end visibility, and performance metrics across user devices, Wi-Fi, ISPs, SSE services like Zscaler, and applications, so that they can ensure optimal digital experiences.

Unlike endpoint and network monitoring tools, ZDX gathers performance metrics from 500T daily signals, and 390B daily transactions, across end user devices, networks, and applications. This simplifies your monitoring stack with a consolidated view and makes it easier to detect and fix performance issues.



ZDX Consolidates Monitoring Silos Reducing Overall Complexity and Costs

IT teams have to grapple with vast amounts of performance data across devices, networks, and applications. So, in May 2022, we introduced AI-powered problem detection and root cause analysis to help them accurately detect performance anomalies that can impact digital experience and make it significantly easier to isolate root cause of issues, fix them quickly, and put employees back to work faster.

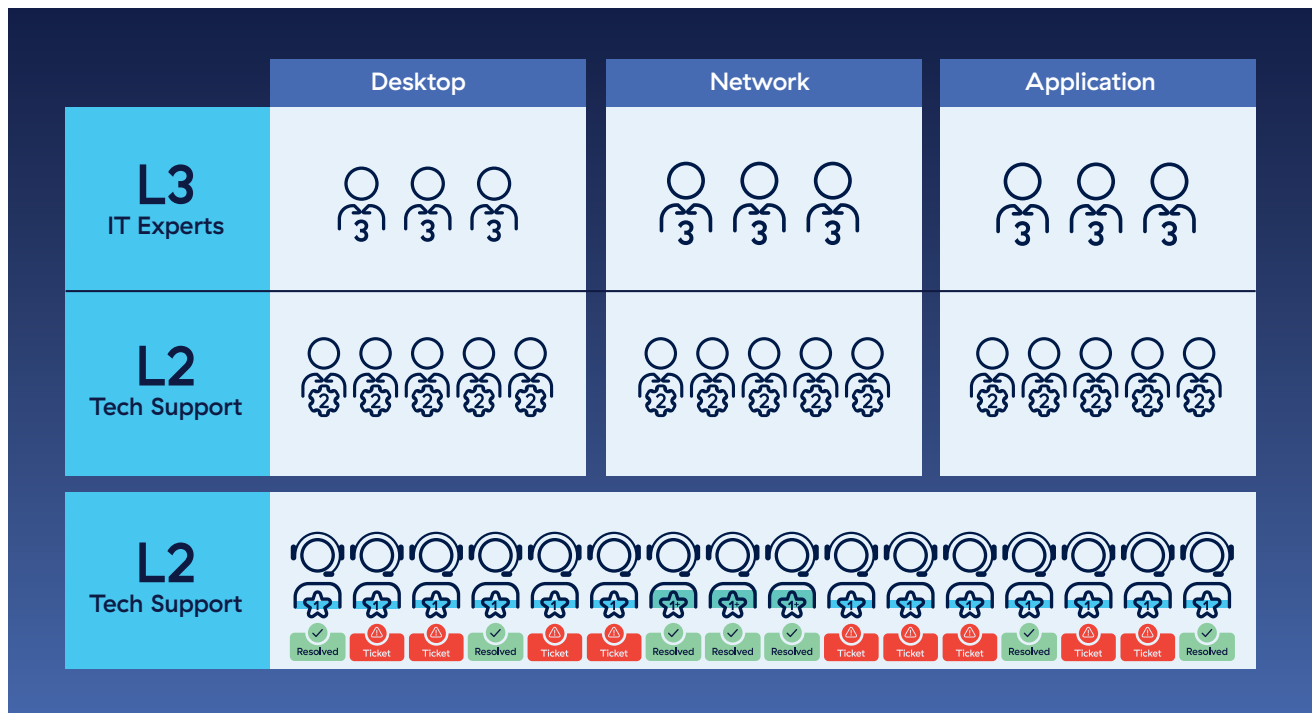


ZDX Copilot takes us a step farther.

ZDX Copilot, your AI assistant, unlocks productivity for IT teams by empowering them to get the information they need using a simple sequence of questions.

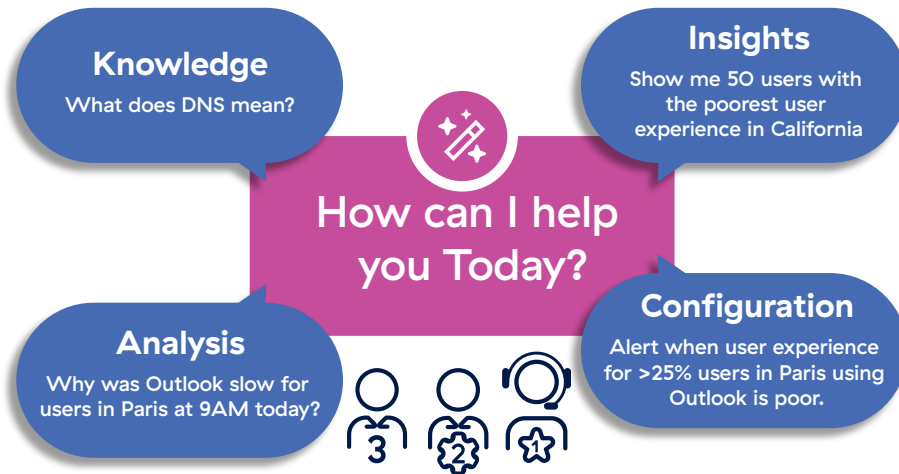
Organizations often struggle to hire the perfect IT team, as it requires significant effort to onboard and train IT professionals to be effective in their roles. Gaining the necessary knowledge to effectively handle end user issues typically takes years of experience. Consequently, many organizations have only a few IT experts who specialize in different domains such as devices, networks, and applications. These experts are constantly under pressure to assist other IT teams in identifying the root causes of issues, which diverts their attention from larger business-focused objectives.

Hiring the perfect team is challenging

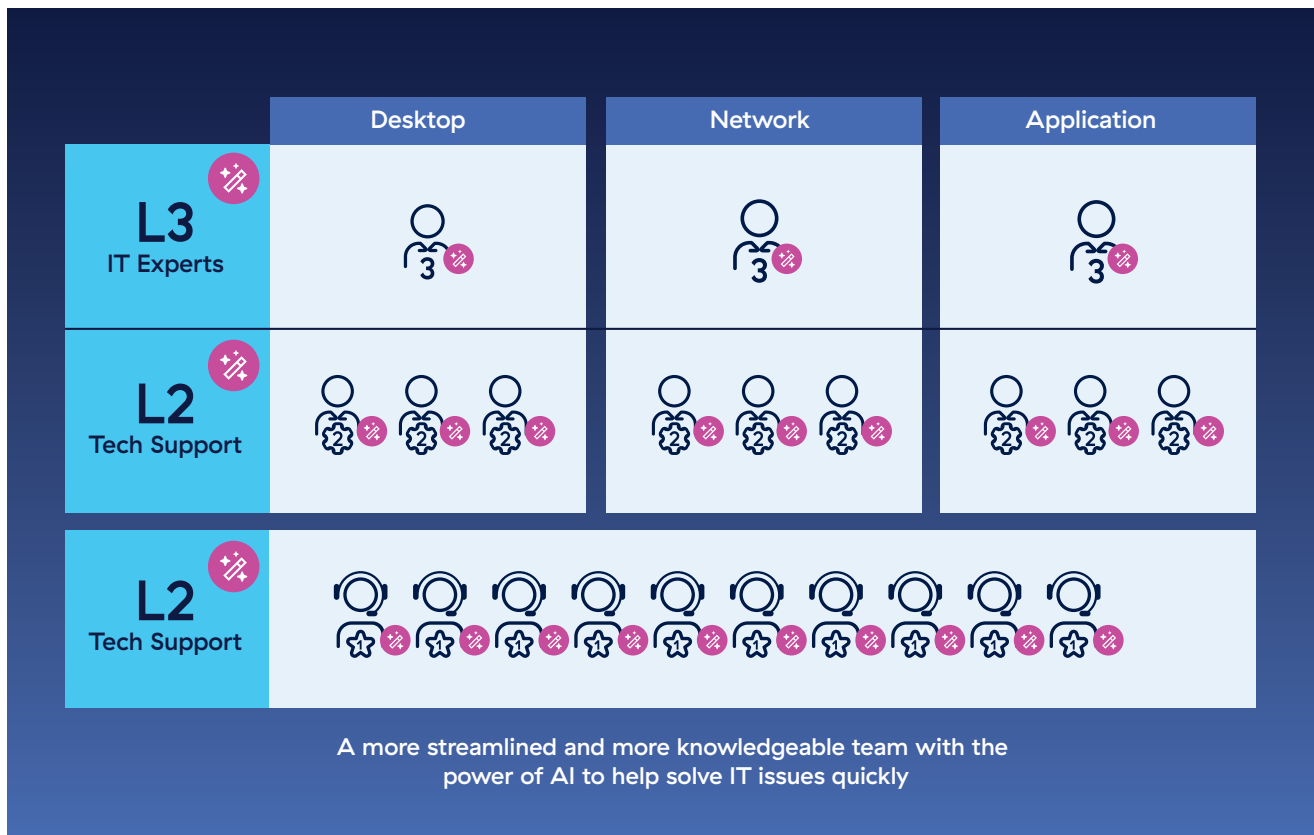


However, with ZDX Copilot, every member of the IT team will have access to an AI assistant that empowers them to become IT experts almost instantly. Copilot enables IT teams to identify the root causes of issues, assist in triaging end user problems, reduce escalations, enhance their knowledge through interactive questionnaires, and drive cost savings by freeing up resources in compute, network, security, and application teams that support end users

Introducing ZDX Copilot



ZDX Copilot for All IT Teams



ZDX Copilot Details

- ZDX Copilot is built as an AI-agent that includes LLM as part of its architecture
- No customer data is used to train the system, rather a frozen model is used
- Prompts history is kept according to the ZDX logs and data retention (up to 14 days) policy

Note: Each customer tenant has an instance of ZDX Copilot which can access only your data to answer questions but does not share or store additional data and is not trained on any customer data.

The ZDX Copilot architecture includes an accuracy loop to avoid competitive, unethical, and other hallucinations.

Competitive	Unethical	Others
Questions related to competitive positioning against vendors.	Questions related to unethical usage of products and processes.	Questions related to politics, racism and content outside the scope of digital experience monitoring context.

Copilot is trained with ZDX domain knowledge. It includes knowledge of other products to be able to answer queries in the context of user experience. ZDX Copilot is designed to assist multiple IT teams:

- **Security operations** can ensure their services are always performing as well as instantly expose the root cause of issues and affected parties when performance lags.
- **Network operations** can conversationally perform deep analysis across networks, applications, and regions to identify trends or find opportunities for optimization.
- **Service and Help Desk** can isolate root cause of user complaints to efficiently triage tickets and collaborate with other teams; they can also easily look up technical information.
- **IT executives** can conveniently extract and present digital experience trends and performance insights to show progress or identify new opportunities

The screenshot shows the ZDX Copilot interface. On the left, there is a sidebar with the Copilot logo, the text "Digital Assistant Powered by AI", a "+ New Session" button, and a "Current" section with the text "what are you". The main chat area contains the following text:

what are you

I'm the ZDX Copilot, here to assist with questions about Zscaler and ZDX, help you resolve network issues, support data visualization and exploration, and offer insights into Zscaler products like Zscaler Digital Experience. How can I assist you today?

ok, how to configure an alert to detect isp issues

To configure an alert in Zscaler Digital Experience (ZDX) for detecting ISP issues, follow these steps:

1. Go to **Alerts > Rules** in the ZDX Admin Portal.
2. Click **Add New Alert Rule**.
3. **Name** your rule and set its **Status** to Enabled.
4. Choose the **Severity** based on the impact level (High, Medium, Low).
5. Select **Network** as the **Type** of alert.
6. Use the **Add Filter** option to specify **ISP** as a criterion.
7. In the **Criteria** tab, select metrics such as **Latency**, **Packet Loss**, or **ZDX Score Drops** that are relevant to ISP performance.
8. Set thresholds for these metrics using the < or > symbols and specify values in ms or %.
9. Configure the **Action** tab with **Throttling options** and **Alert Delivery Method**.
10. Review your configurations on the **Review** tab, then click **Submit**.

Enter your question here...

Copilot may generate inaccurate info. [View policy](#)

Getting Access to ZDX Copilot

- Copilot is included in ZDX Advanced Plus
- No configuration is needed
- A “**Magic Wand**” icon allows administrators to enter the full immersive Copilot exploration mode
- Currently, only an administrator with full, or read access to all pages will have access to Copilot

ZDX

Dashboard

Copilot

Analytics

Using ZDX Copilot

The screenshot shows the ZDX Copilot interface. On the left is a sidebar with a 'Copilot' header and a '+ New Session' button. Below are sections for 'Today', 'Yesterday', and 'Last Week' with various event titles. The main area displays a 'Response' to the query 'How is the user's experience for Sharepoint in the last 2 days?'. The response includes a world map titled 'Regions by ZDX Score' with colored markers. Below the map are 'Admin feedback' icons and 'Clickable prompts' such as 'Show me the ZDX score trend', 'Zoom into Asia', and 'Show it for users in North America'. At the bottom is a 'Prompt area' with an input field and a 'View policy' link.

Prompts

Copilot understands users, timeframes and maintains context for related questions. Avoid using acronyms, for example, use Page Fetch Time instead of PFT.

Clickable prompts

Suggested prompts to initiate session or follow up questions.

Supervised learning feedback

Admin can rate the responses as good or bad in the answer directly.

Prompt Examples

Foundational questions

Copilot Prompt: How is network latency created?

Network latency is created by several factors as data packets travel across a network from a source to a destination. Here are the primary causes:

- **Propagation Delay:** The time it takes for a signal to travel from the source to the destination. This delay is influenced by the distance between the two points and the speed of light in the medium (fiber, copper, etc.).
- **Transmission Delay:** The time required to push all the packet's bits into the wire at the packet's departure point. This delay depends on the size of the packet and the bandwidth of the network.
- **Processing Delay:** The time routers or switches take to process the packet header, check for bit-level errors in the packet, and determine the packet's next destination.
- **Queueing Delay:** The time a packet waits in a queue until it can be processed or transmitted. Queueing delay varies as it depends on the number of packets waiting to be transmitted.
- **Serialization Delay:** Related to transmission delay, it's the time needed to convert the packet from a queue into electrical or optical signals.
- **Medium Access Control (MAC) Delay:** In networks that share access to the medium (e.g., Wi-Fi networks), this delay is encountered due to protocols that manage how devices take turns to transmit data to avoid collisions. Each of these factors contributes to the overall network latency, impacting the speed and efficiency of data transmission. High latency can degrade the performance of applications, especially those requiring real-time interaction, such as VoIP calls or online gaming.



Copilot Prompt: How can I reduce latency?

To effectively reduce network latency, consider these measures:

- **Optimize Wi-Fi and Connectivity:** Use 5 GHz Wi-Fi for less interference and faster speeds. Stay close to routers or switch to wired connections for lower latency.
- **Manage Device Load:** Close unnecessary high-bandwidth or high-CPU applications to reduce load and improve performance.
- **Upgrade Network Equipment:** Modern routers and switches handle data more efficiently, which can decrease latency.
- **Implement Quality of Service (QoS):** Prioritize traffic for real-time applications like VoIP or video calls to ensure they have sufficient bandwidth.
- **Minimize Interference:** Identify and remove sources of Wi-Fi interference such as microwaves or cordless phones.
- **ISP and Routing Optimization:** Contact your ISP for potential service improvements or optimizations.
- **Use CDNs for Business Applications:** CDNs reduce latency by caching content closer to users.
- **Continuous Monitoring:** Use tools like Zscaler Digital Experience (ZDX) for ongoing performance monitoring and to identify specific latency issues for targeted troubleshooting. These strategies can help lower latency, enhancing network performance and user experience.



Copilot Prompt: What affects quality in voice over ip calls? (summarize in 800 chars)

The quality of Voice Over IP (VoIP) calls can be significantly impacted by latency, jitter, packet loss, and bandwidth. Latency, or delay, affects how quickly speech is transmitted, with lower values (under 100ms) being ideal. Jitter, the variability in packet arrival times, can cause audio distortion; managing it is crucial, especially for real-time communications like Microsoft Teams Calls. Packet loss leads to gaps in audio or video streams, degrading call quality even at low rates, particularly for real-time applications. Insufficient bandwidth can exacerbate these issues by causing network congestion. Zscaler Digital Experience (ZDX) provides insights and recommendations to optimize network performance, including monitoring device and application performance, improving Wi-Fi connectivity, and managing CPU usage. ZDX also calculates the ZDX Score for Call Quality using metrics such as the Mean Opinion Score (MOS), which considers latency, jitter, and packet loss, to evaluate call quality on a scale from 1 (worst) to 5 (best). Configuration of monitoring tools for specific platforms, such as Microsoft Teams or Webex, involves verifying prerequisites, authenticating, and setting up probes or tenants to collect detailed call quality metrics, aiding in targeted troubleshooting and improvement efforts.



Product knowledge questions

Copilot Prompt: How is the ISP detected in the Cloud Path?

In Zscaler Digital Experience (ZDX), ISPs are detected as part of the Cloud Path analysis process. This detection is primarily accomplished through the use of Cloud Path Probes, which are designed to measure various metrics such as hop count, packet loss, and latency across the network path from the user's device to the destination application or service. The process involves the following steps:

- 1. Cloud Path Probes:** These probes are configured to target specific applications or services, and they collect data on the network path between the client device and the application. The probes can be set to run at regular intervals, providing ongoing monitoring of network performance.
- 2. Hop-by-Hop Visualization:** The Cloud Path provides a detailed visualization of the network hops from the client device to the destination. This includes identifying each hop along the path and measuring latency and packet loss at each point.
- 3. ISP Identification:** The ISP is identified as part of the network path analysis. ZDX utilizes integration with MaxMind to determine the ISP name based on the public IP address associated with the egress point of the client device's network connection. This is achieved using a Location API call to the Zscaler Public Service Edge, similar to how "what's my IP address" services work. The public IP address used by the client device is key to identifying the egress point and, by extension, the ISP.
- 4. Forward and Reverse Traceroute:** ZDX supports both forward and reverse traceroute to map the network path. Forward traceroute is used to identify the path from the client device to the destination, while reverse traceroute can be enabled to map the path back from the Zscaler Cloud to the customer's network when the forward path is blocked or to provide additional visibility.
- 5. Analyzing ISP Performance:** Once the ISP is identified, ZDX can monitor and analyze the performance of the ISP's network. This includes measuring latency to the ISP, packet loss, and other relevant metrics that impact user experience. Through these methods, ZDX provides comprehensive visibility into the network path, including ISP performance, which is crucial for identifying and troubleshooting network issues that could impact the digital experience of users.



Copilot Prompt: Summarize in 300 Chars

ZDX utilizes Cloud Path Probes to map network paths, identifying ISPs through MaxMind integration based on the client's IP. This enables detailed hop-by-hop visualization and analysis of ISP performance.



Copilot Prompt: What version of ZCC do I need to configure adaptive mode?

To utilize the Adaptive Mode feature in Zscaler Digital Experience (ZDX), your organization needs to deploy Zscaler Client Connector (ZCC) version 3.4.2.3 for Windows. This version is required to ensure compatibility and enable the full functionality of the Adaptive Mode, which selects the best protocol for each leg of the cloud path probe to reach its destination. Please ensure your ZCC is updated to this version or later to use Adaptive Mode effectively.



Configuration questions

Copilot Prompt: How do you configure a network alert to monitor an ISP?

To configure a network alert in Zscaler Digital Experience (ZDX) to monitor ISP performance, follow these steps:

1. **Go to Alerts > Rules** in the ZDX Admin Portal and click **Add New Alert Rule**. This will open the Add New Alert Rule window.
2. **Configure Rule:**
 - **Name:** Enter a name for the rule.
 - **Status:** Choose "Enabled" to activate the rule.
 - **Severity:** Select the severity level (High, Medium, or Low) based on the impact.
 - **Type:** Select "Network".
 - **Labels:** Optionally, specify labels for better organization.
3. **Filters:**
 - If you selected "Network" as the Rule Type, you can add filters such as Geolocations, Locations, Location Groups, Departments, User Groups, Users, and Devices to specify which network alerts you want to monitor.
 - **Add Filter:** Choose filters to narrow down the monitoring scope. For ISP monitoring, select the appropriate filters that align with the ISPs you want to monitor.
4. **Criteria:**
 - Define the specific conditions that will trigger the alert. For ISP monitoring, you can use parameters such as Latency, Packet Loss, and others relevant to ISP performance.
 - You can choose to trigger the alert if all conditions are met (ALL) or if any condition is met (ANY).
5. **Action:**
 - **Throttling options:** Define how often you want to receive alerts. You can specify the number of times an event must occur before an alert is sent and the minimum number of devices impacted.
 - **Alert Delivery Method:** Choose how you want to be notified (e.g., Email, Webhook).
6. **Review and Submit:** Review your configurations and click "Submit" to finalize the alert rule.
7. **Save and Activate:** Don't forget to save your changes to activate the alert rule. Keep in mind that alerts have a display delay of 30 minutes. This general guideline provides a framework for setting up a network alert to monitor ISP performance within ZDX. Remember to adjust the specific criteria and filters according to the ISPs you intend to monitor and the performance metrics most relevant to your organization's needs. For detailed steps or additional configurations like Cloud Path Probe, refer to the ZDX documentation or contact Zscaler support for further assistance.



Best practice questions

Copilot Prompt: What is the recommended protocol for Cloud Path?

For configuring Cloud Path probes within Zscaler Digital Experience (ZDX), the recommended protocol to use is **Adaptive**. This mode is designed to optimize the delivery path visibility by automatically selecting the best protocol (TCP, UDP, or ICMP) for each leg of the cloud path probe, based on factors such as latency and packet loss. This auto-discovery process ensures that the cloud path employs the most efficient protocol combination to reach its destination, providing accurate and comprehensive network path analysis. However, it's important to note that for applications requiring special treatment, it is recommended to use the port/protocol that the application relies on. This ensures that the cloud path probe is accurately reflecting the application's network behavior and requirements. In summary:

- **Adaptive Mode** is the general best practice for most applications, as it dynamically selects the optimal protocol for each part of the network path.
- For **specific applications** with unique network characteristics, choose the protocol (TCP, UDP, ICMP) that best matches the application's needs. This approach allows for a detailed and adaptable analysis of the network path, ensuring visibility into performance issues and optimization opportunities.



Copilot Prompt: What is the recommended latency from Client to Public Service Edge?

The recommended latency from a client to a Zscaler Public Service Edge (PSE) for optimal user experience is less than 50 milliseconds (ms). This threshold ensures smooth and efficient data transfer, minimizing any perceptible delay in network communication. Zscaler's global infrastructure, which includes over 150 data centers, is strategically located to ensure users are in proximity to a PSE, thereby achieving low latency and high connectivity with premium bandwidth services. This setup is designed to optimize speed and performance for users accessing the internet and cloud services through Zscaler. It's important to note that while less than 50 ms is the recommended latency for the best user experience, actual latency can vary based on several factors, including the physical distance between the client and the PSE, the quality of the network connection, and the current load on the network. Zscaler continuously works on optimizing the routing and performance to ensure the lowest possible latency for its users.



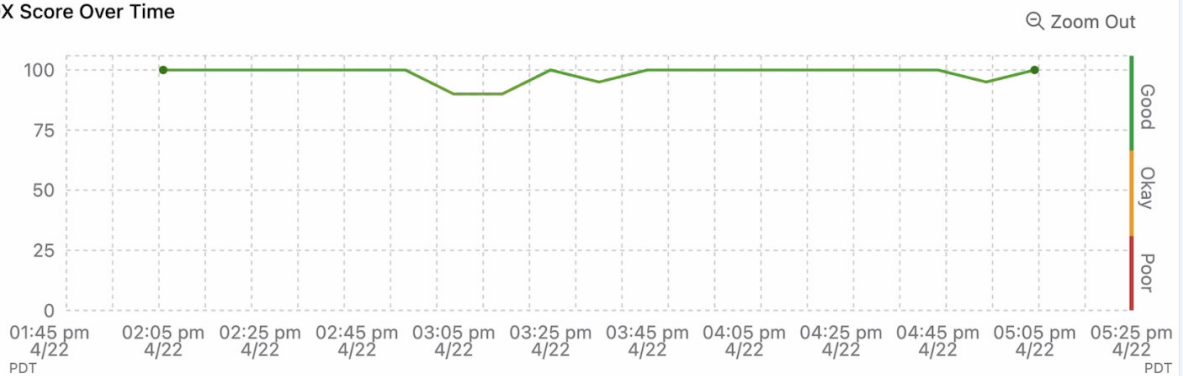
Analytics questions

Copilot Prompt: What is Javier's ZDX Score for SharePoint in the last 4 hours?

User ZDX Score for Javier Rodriguez Gonzalez - SharePoint Online

- **Initial Score:** 90.0
- **Data Gaps:** 4 instances of 'Not Available' data
- **Score Range:** 90.0 to 100.0
- **Final Score:** 100.0
- **Trend:** Improvement over time, stabilizing at 100.0
- **Observations:**
 - Majority scores at 100.0
 - Minor fluctuations to 90.0 and 95.0
 - Consistent high performance towards the end

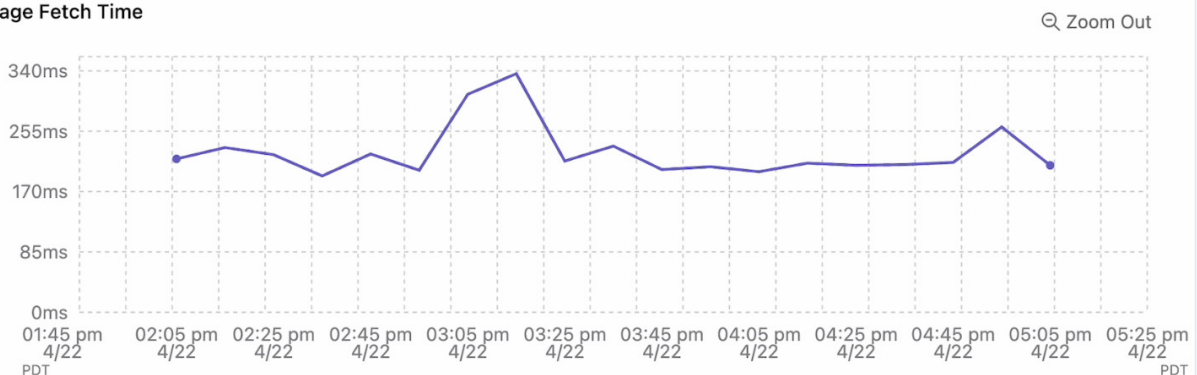
ZDX Score Over Time



Copilot Prompt: How about Page Fetch Time?

**Page Fetch Time Insights for Shar

Page Fetch Time



Copilot Example Scenarios

Here are some common troubleshooting scenarios that involve poor end user experiences, and how you may use Copilot to analyze and resolve them.

Wi-Fi Connectivity Issues

A user has reported poor Wi-Fi connectivity to the service desk, experiencing frequent disconnections, slow internet speeds, and challenges in completing work tasks. This issue is affecting the user's productivity and causing frustration.

Copilot Prompt: Analyze Curtis Hardwick's Wi-Fi issue?

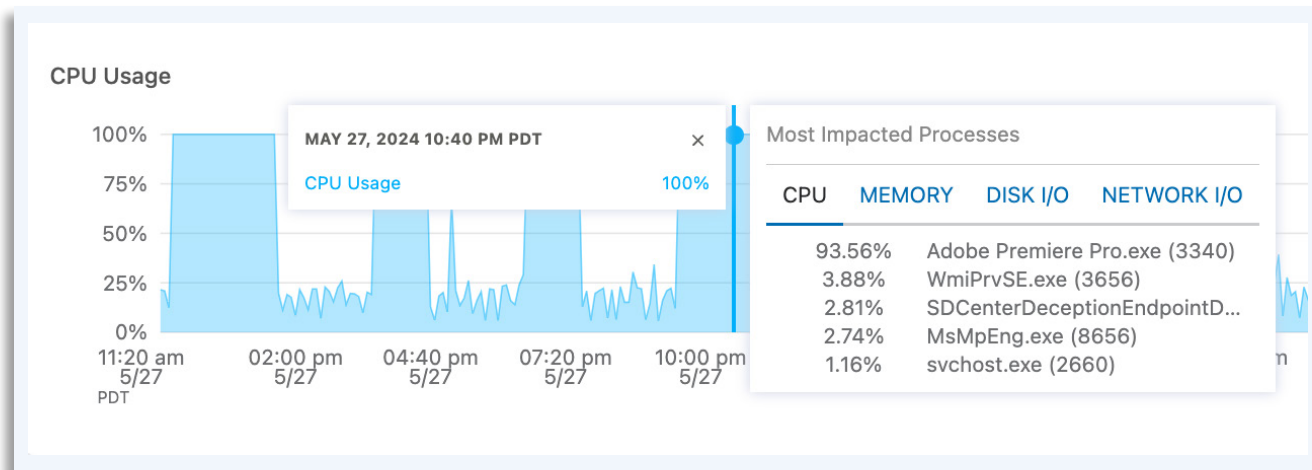


End User Device Issues (high CPU)

The user is experiencing slow device performance and delayed application access. They have reported these issues to the service desk, requesting immediate assistance to enhance their system's efficiency. From the service desk's perspective, it is challenging to determine the cause of the degradation and identify if it is related to a software process or which process might be affecting performance.

Copilot Prompt: Analyze Barry Bogdown's Wi-Fi issue?





Poor Microsoft Teams Call Quality

The user has reported experiencing intermittent issues with poor call quality and unsatisfactory overall experiences during Microsoft Teams meetings. These sporadic occurrences have made it difficult for the service desk to identify and troubleshoot the underlying problems effectively.

Copilot Prompt: Analyze Grady Archie's Microsoft Teams call quality issue?

Meeting Details

Meeting ID: TEAMS-ceb62a54-0a6d-445a-9553-2d3d55a059de Host: Grady Archie (grady.archie@thezerotrustexchange.com)

Start Time: May 29, 2024 10:01 AM PDT End Time: May 29, 2024 11:02 AM PDT

ZDX Score: 22

Meeting ID: TEAMS-0c24e067-f205-4de0-8894-ef762d7945ee

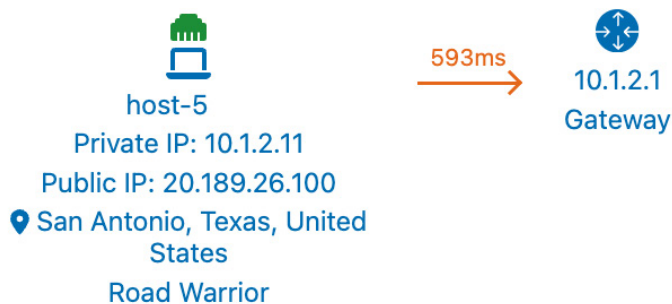
Audio mos score In 2

Audio mos score Out 2.1

Meeting ID: TEAMS-0c24e067-f205-4de0-8894-ef762d7945ee

Audio latency In 648ms

Audio latency Out 626ms



Usage disclaimer

The acceptable user policy includes a new section for the AI chatbot usage. <https://help.zscaler.com/acceptable-use-policy>

Please remember that ZDX Copilot uses generative AI technology. We include engines to measure accuracy, provide safeguards and protect privacy data. Please remember that there is some small probability that answers may not be correct.

Product Usage disclaimer

For avoidance of doubt, Zscaler expressly disclaims warranty or representation of any kind with respect to any qualitative or quantitative information, including but not limited to risk scores, vulnerability assessments, mitigation measures, policy recommendations, etc., presented by Zscaler products which may be powered by generative AI, machine learning, and other emerging technologies (collectively "Product Outputs"). Customer acknowledges and agrees that Product Outputs are for general informational purposes only. Product Outputs may be incomplete, inaccurate, and/or inappropriate and may not represent all the information required for a comprehensive security vulnerability assessment, breach response planning, root cause analysis, and the like. Product Outputs do not, and are not intended to, constitute legal or professional advice by Zscaler or any of its personnel. By accessing and using Zscaler products, customers acknowledge and agree to assume the risks disclosed in this disclaimer. All liability with respect to actions taken or not taken based on the Product Outputs are hereby disclaimed. The Product Outputs are provided on an "as is" basis only.



Experience your world, secured.™

About Zscaler

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

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.