

Prisma Access Autonomous Digital Experience Management - Technical Decision Maker



Satish Kondalam

Principal Technical Marketing Engineer

November 2021

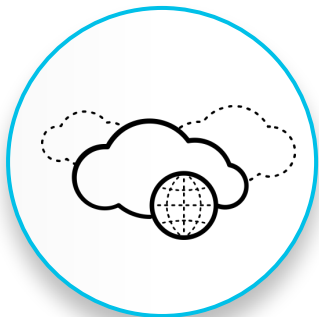
Agenda

- Prisma Access ADEM Overview
 - Problem Statement & Solution Description
 - Prisma Access ADEM Overview
 - How to Log into Prisma Access ADEM App
 - Licensing and Activation

- Prisma Access ADEM High Level Solution Overview
 - ADEM Endpoint agent Installation
 - ADEM Remote network agent installation
 - ADEM Agents Overview
 - ADEM Application Test Creation

- Prisma Access ADEM Product Workflow

Three Trends Reshaping Organizations Today



Cloud Adoption

71% of organizations expect to have their security mostly or completely in the cloud over the next two years*

*The State of Hybrid Workforce Security 2021



Remote User Mobility

62% of organizations are planning a permanent hybrid work posture for employees*



Digital Transformation

By 2024, more than 60% of SD-WAN customers will have implemented a SASE architecture**

** Gartner WAN Edge Infrastructure MQ 2020

IT is losing visibility across the service delivery chain



Apps being Refactored

No visibility into cloud stack

No tools to benchmark Application performance from user's perspective



User Locations Change

No control over the home Wi-Fi and local network

Limited visibility on the endpoint

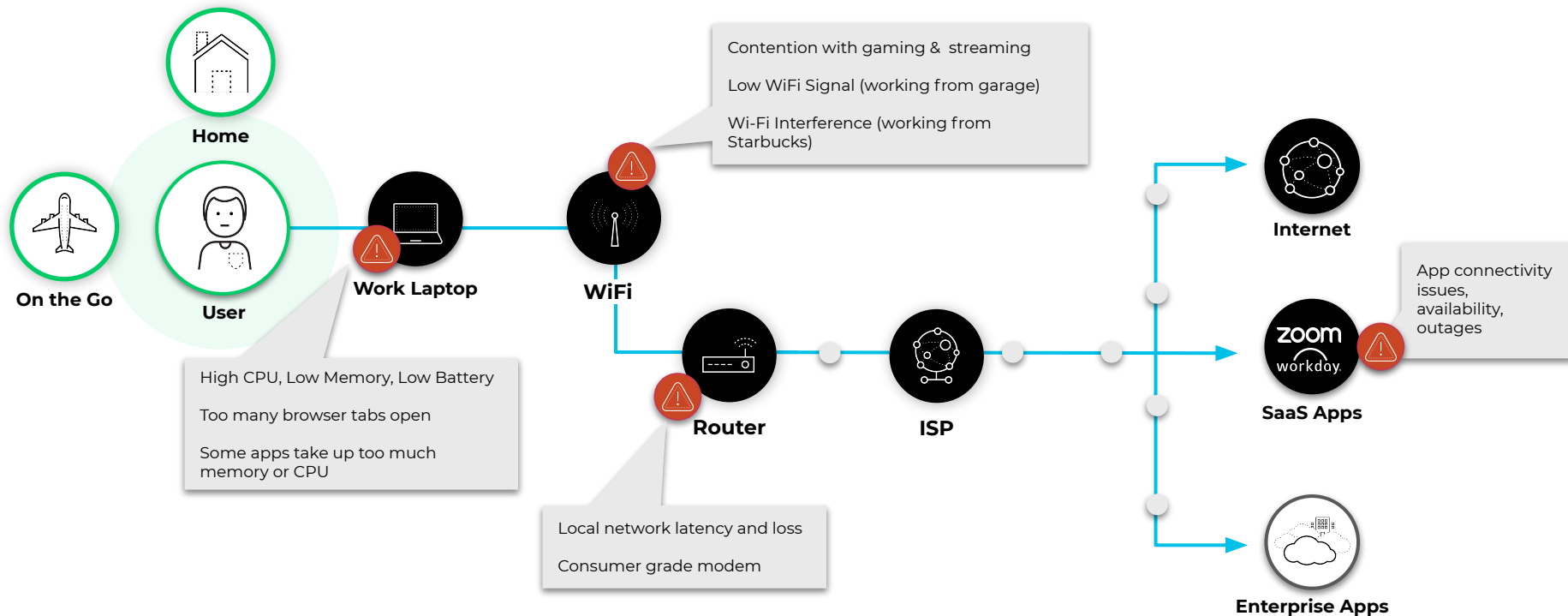


Heterogeneous Transport

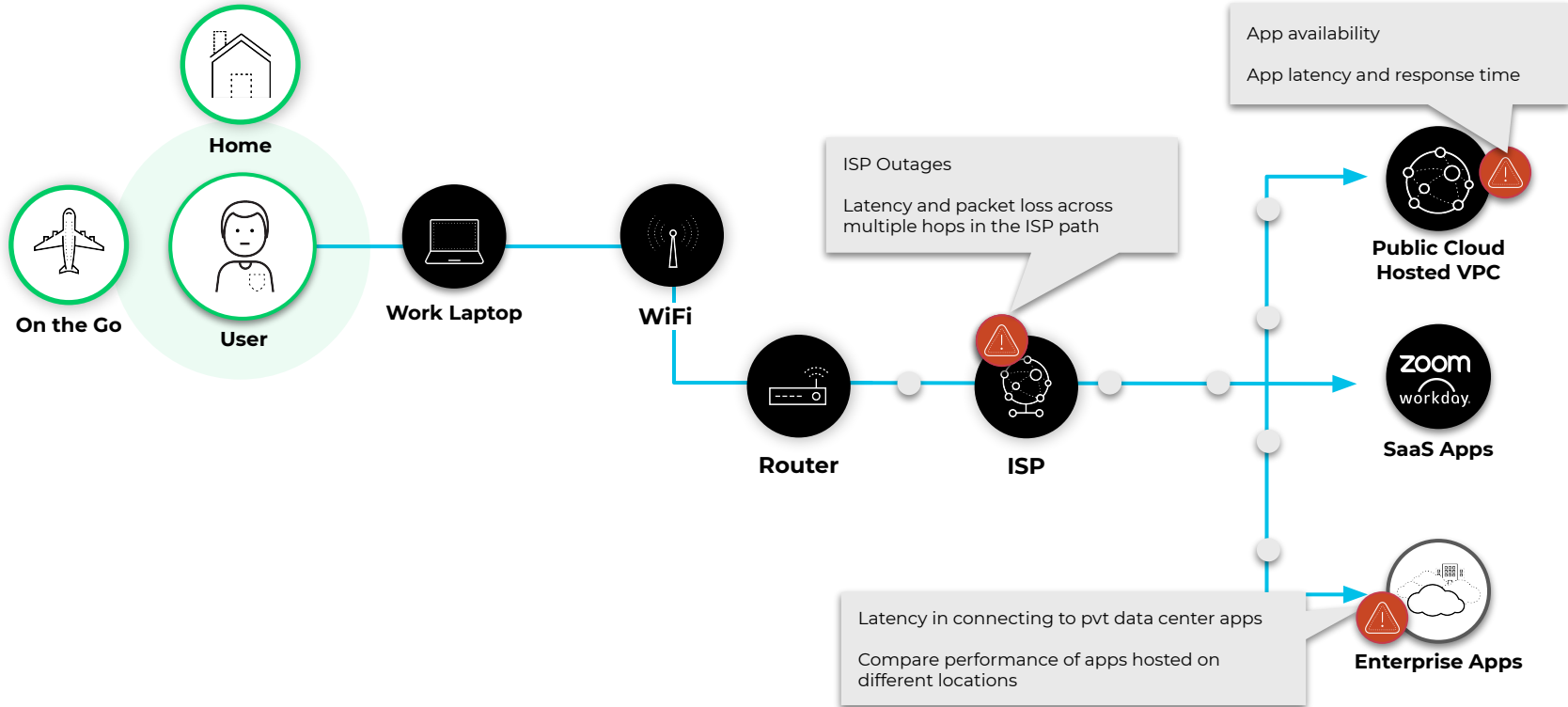
SD-WAN transport with no SLAs from ISP

No visibility into ISP performance

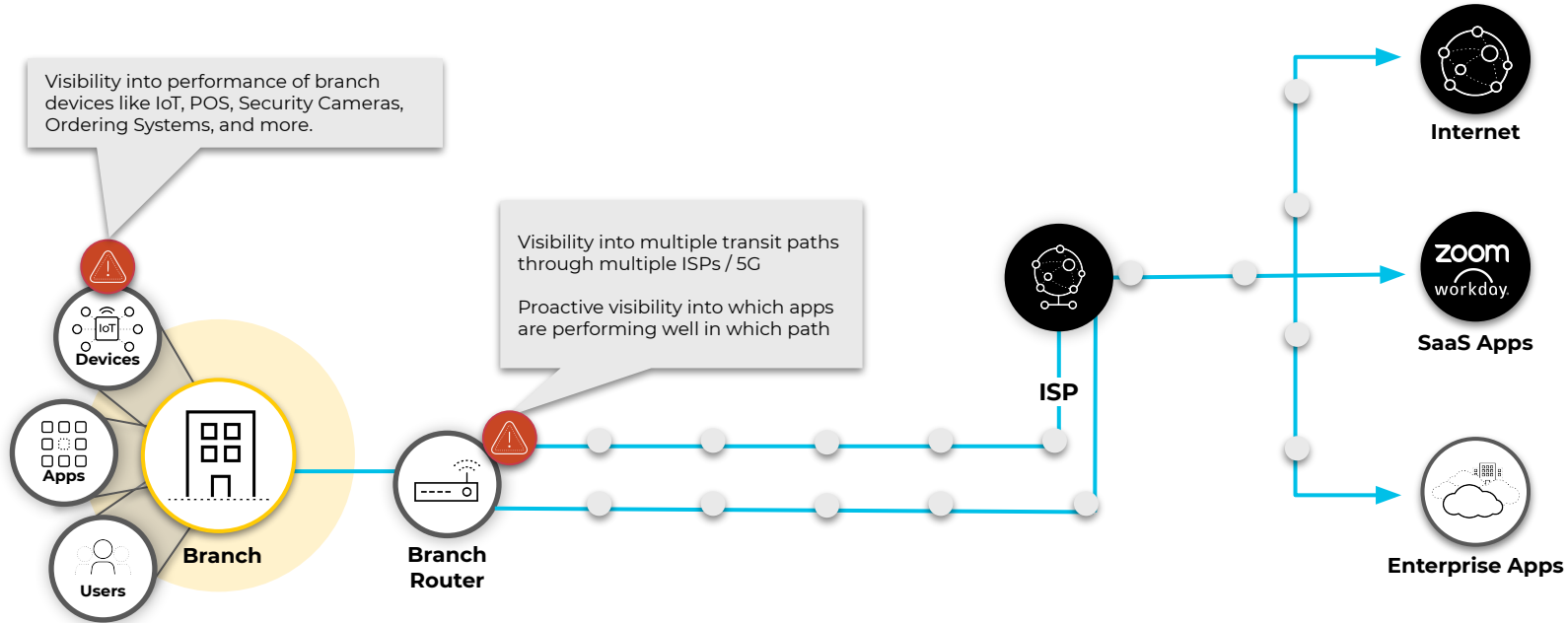
Visibility Challenges With Endpoints and Home Wi-Fi Network



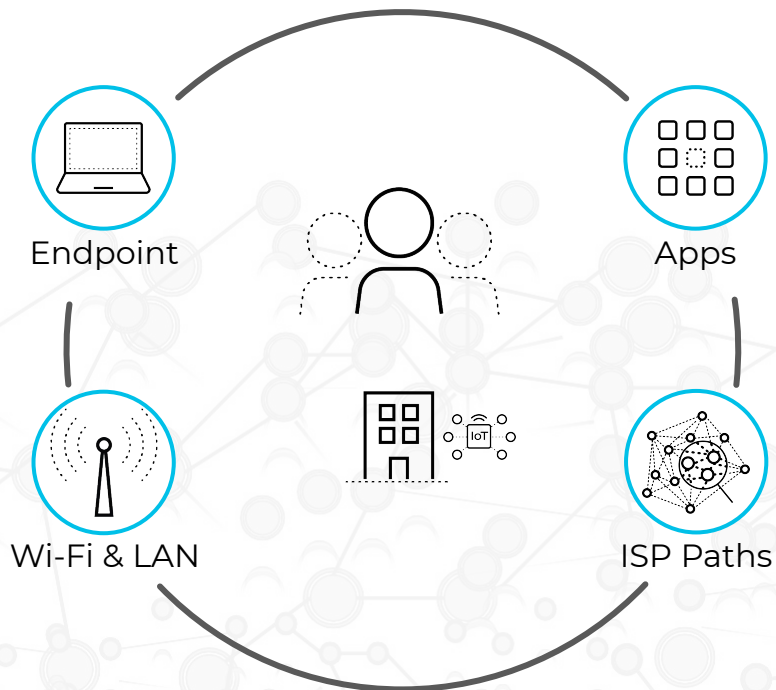
Visibility Challenges With ISP and App Availability



Visibility Challenges With Branch Device Experience

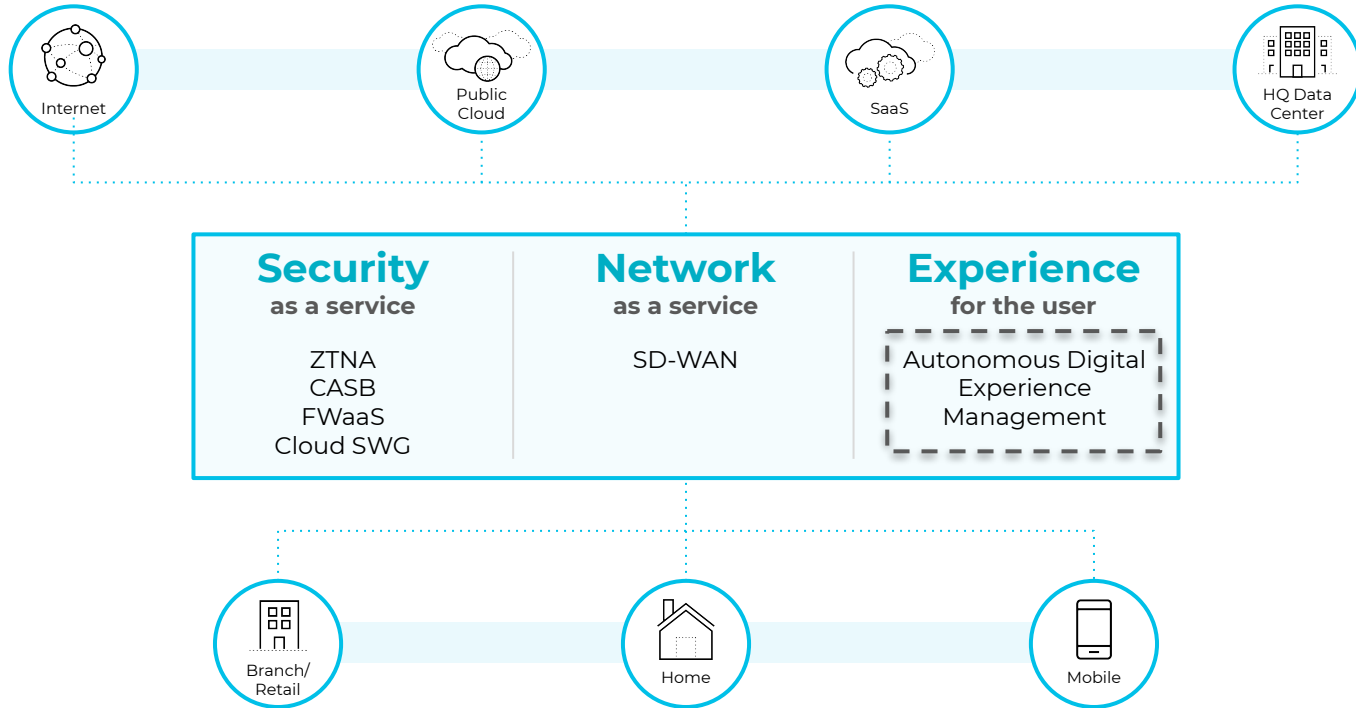


Digital Experience Monitoring (DEM) places user and branch experience at the center of monitoring



Palo Alto Networks Prisma Secure Access Service Edge (SASE)

SASE Native DEM delivers exceptional user experience



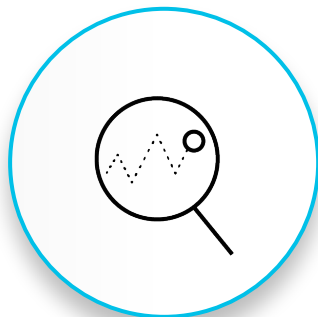
Redefining User Experience Monitoring with Unrivaled ADEM



SASE-Native DEM

Integrated visibility from GlobalProtect clients, Prisma SD-WAN & Prisma Access Cloud

Easy to deploy and operate



Segment-Wise Insights

Gain detailed performance insights across the entire SASE service delivery chain.

The endpoint, WiFi, router, ISP, Prisma Access, and application



Comprehensive Visibility

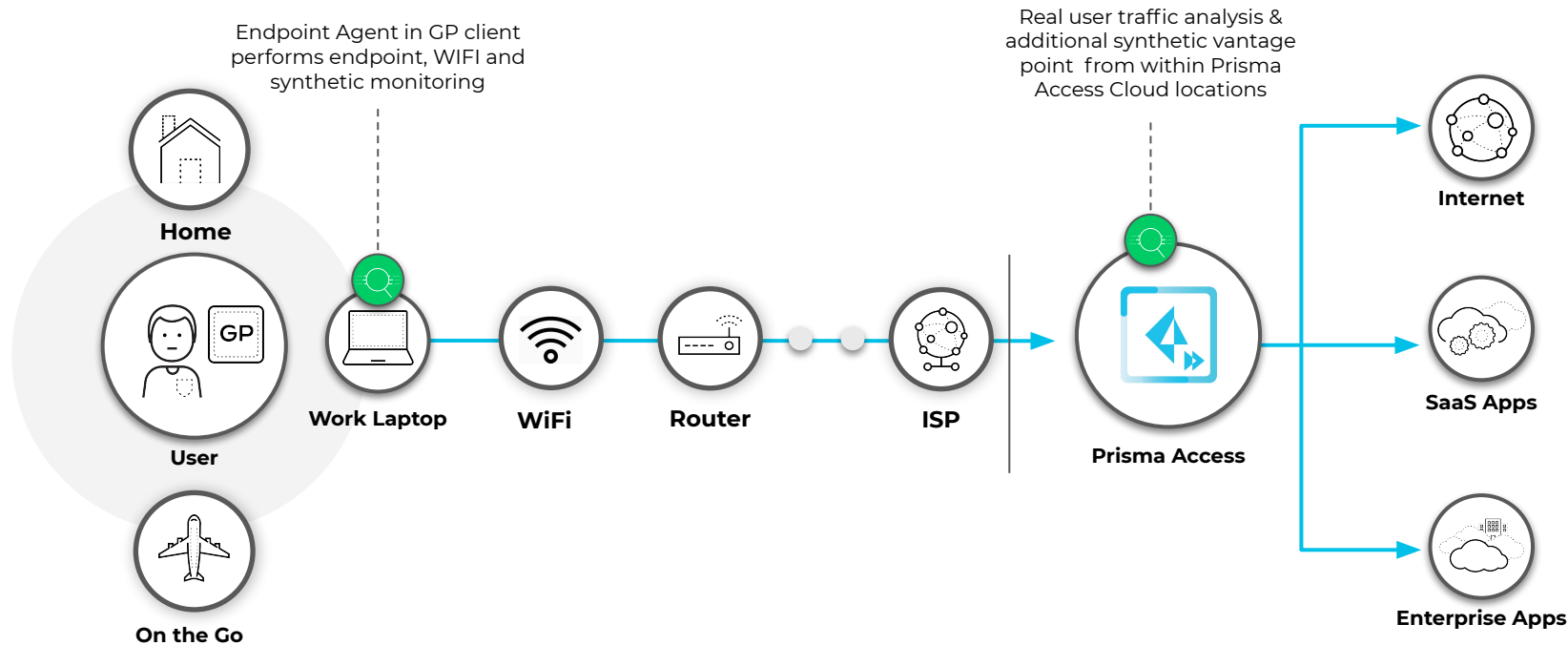
Single dashboard for cloud-delivered security, network and user experience monitoring

Rapid problem isolation and root cause analysis

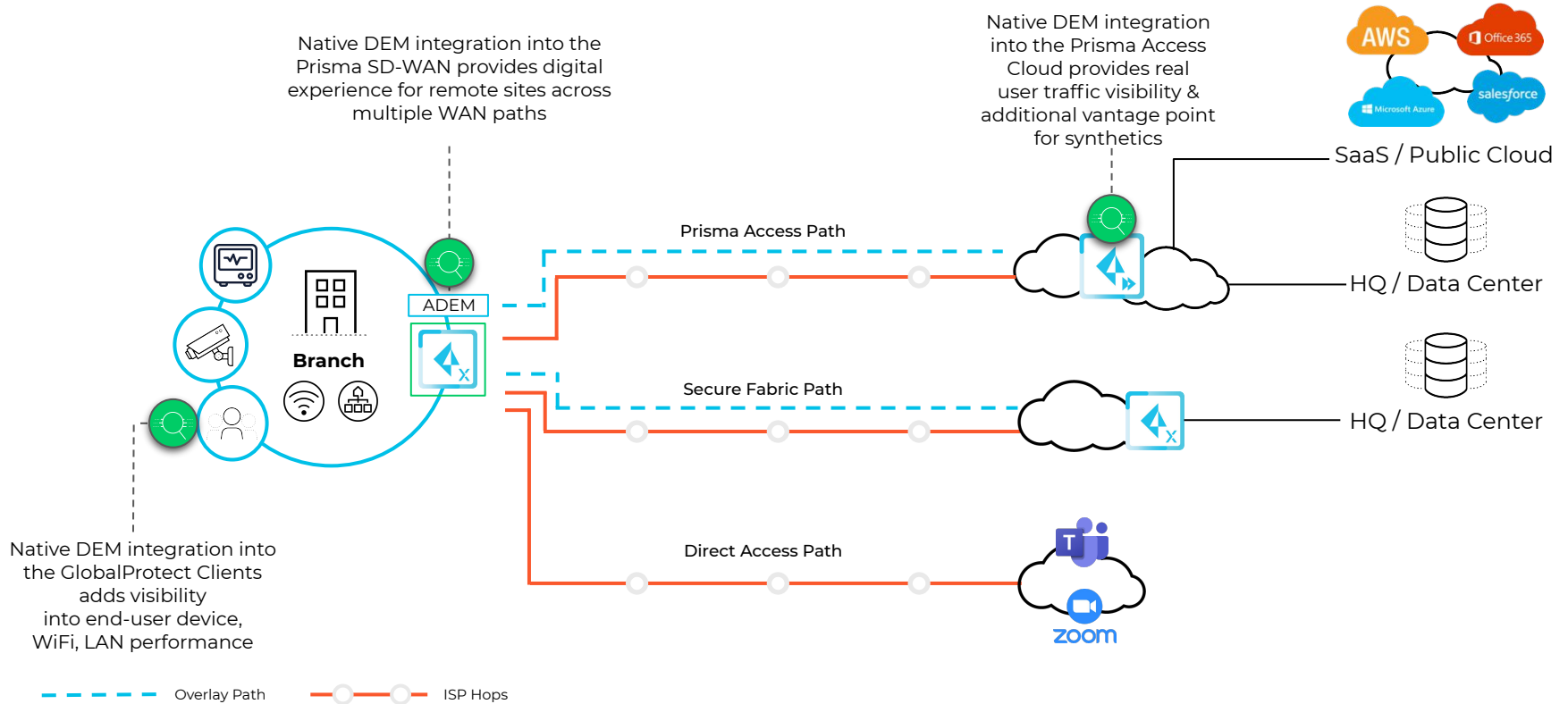
ADEM for Users

A Comprehensive Monitoring Approach

Endpoint | Synthetics | Real User Traffic



ADEM for Remote Networks



Autonomous DEM Overview - Log into Prisma Access for ADEM

Get to Prisma Access Autonomous DEM

Prisma Access Autonomous Digital Experience Management (ADEM) is integrated the Prisma Access App itself.

We can get to Prisma Access App from:

The Hub:

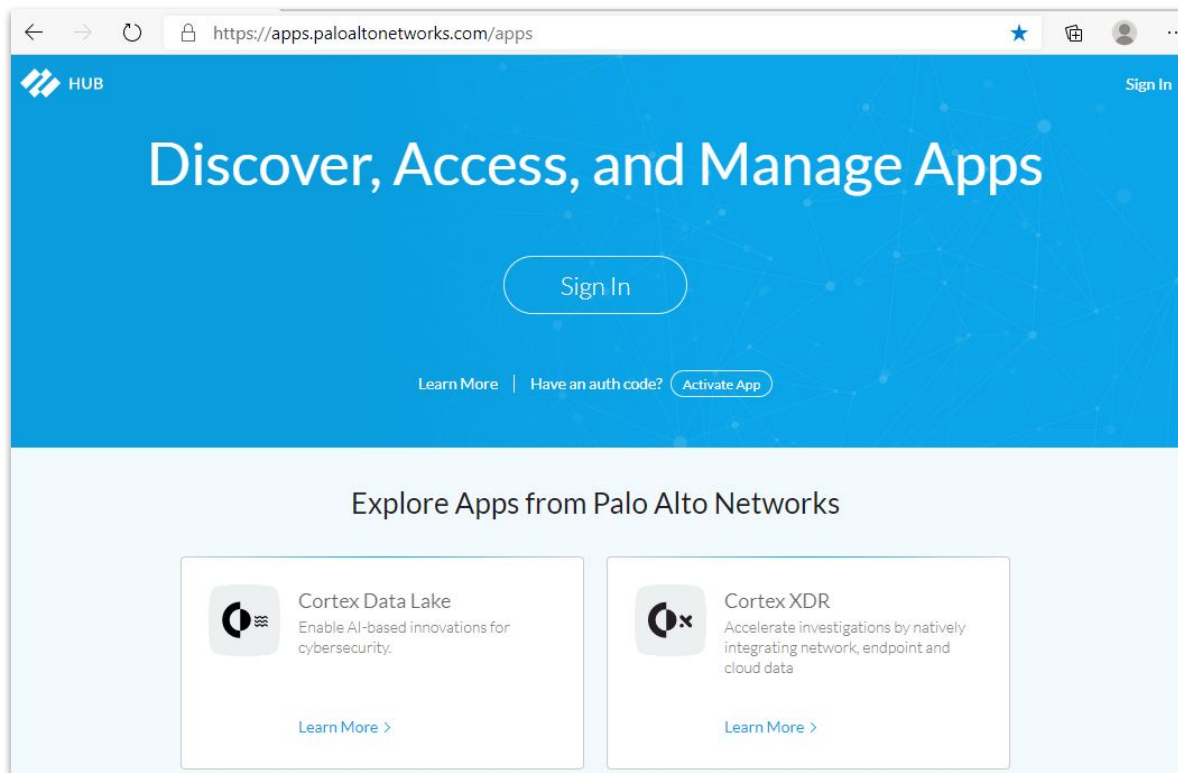
The Hub is a single place where you can access all of the Palo Alto Networks Cloud Services and Apps for your Organization.

Prisma Access App: The Hub

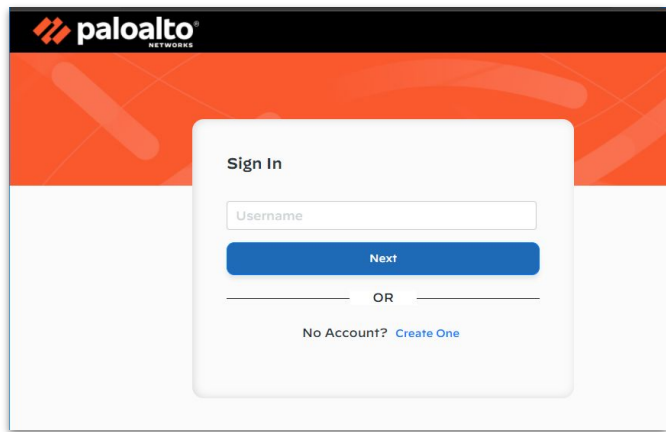
Open The Hub

URL:

<https://apps.paloaltonetworks.com/>



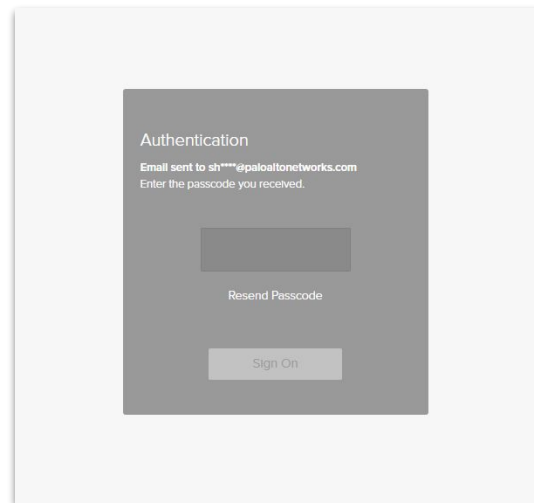
Prisma Access App: The Hub



The screenshot shows the Palo Alto Networks logo at the top left. Below it is a white sign-in form with a blue header bar. The form contains a "Sign In" title, a "Username" input field, a blue "Next" button, and an "OR" separator. At the bottom of the form, there is a link that says "No Account? [Create One](#)".

Login to The Hub:

Use the credentials associated with your Palo Alto Networks Customer Support Account to log in to the Hub.



The screenshot shows an authentication screen with a dark grey background. It features the title "Authentication", a message "Email sent to sh****@paloaltonetworks.com", and the instruction "Enter the passcode you received." Below this is a dark grey input field for the passcode, a "Resend Passcode" link, and a "Sign On" button.

Prisma Access App: The Hub

The Hub: Dashboard

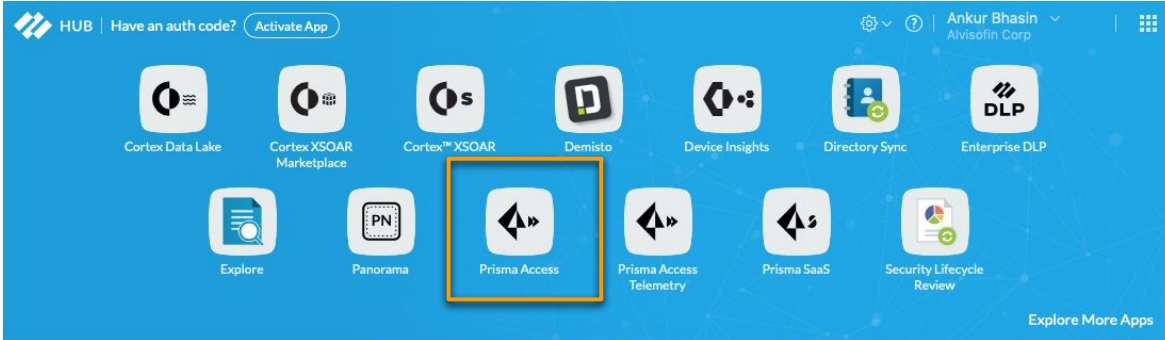
If the The Hub user is part of multiple CSP accounts, use the drop down on the top right corner to select the appropriate Account Name.

Click on the Prisma Access Icon to access the Autonomous DEM.

If you are not able to see the Prisma Access App, it might be because you are not assigned the required Hub role.



Account administrators can access any of your organization's apps (including Prisma Access), and can assign roles to other users by selecting Settings > Access Management

The Account Administrator role on the hub is automatically assigned to the first user from your organization to register on the Palo Alto Networks customer support portal.



The screenshot displays the Palo Alto Networks Hub dashboard. At the top left, it shows the 'HUB' logo, a 'Have an auth code?' prompt, and an 'Activate App' button. On the top right, there is a user profile for 'Ankur Bhasin' from 'Alvisofin Corp' and a settings icon. The main area features a grid of application icons: Cortex Data Lake, Cortex XSOAR Marketplace, Cortex™ XSOAR, Demisto, Device Insights, Directory Sync, Enterprise DLP, Explore, Panorama, Prisma Access (highlighted with an orange border), Prisma Access Telemetry, Prisma SaaS, and Security Lifecycle Review. A 'Explore More Apps' link is located at the bottom right of the dashboard.

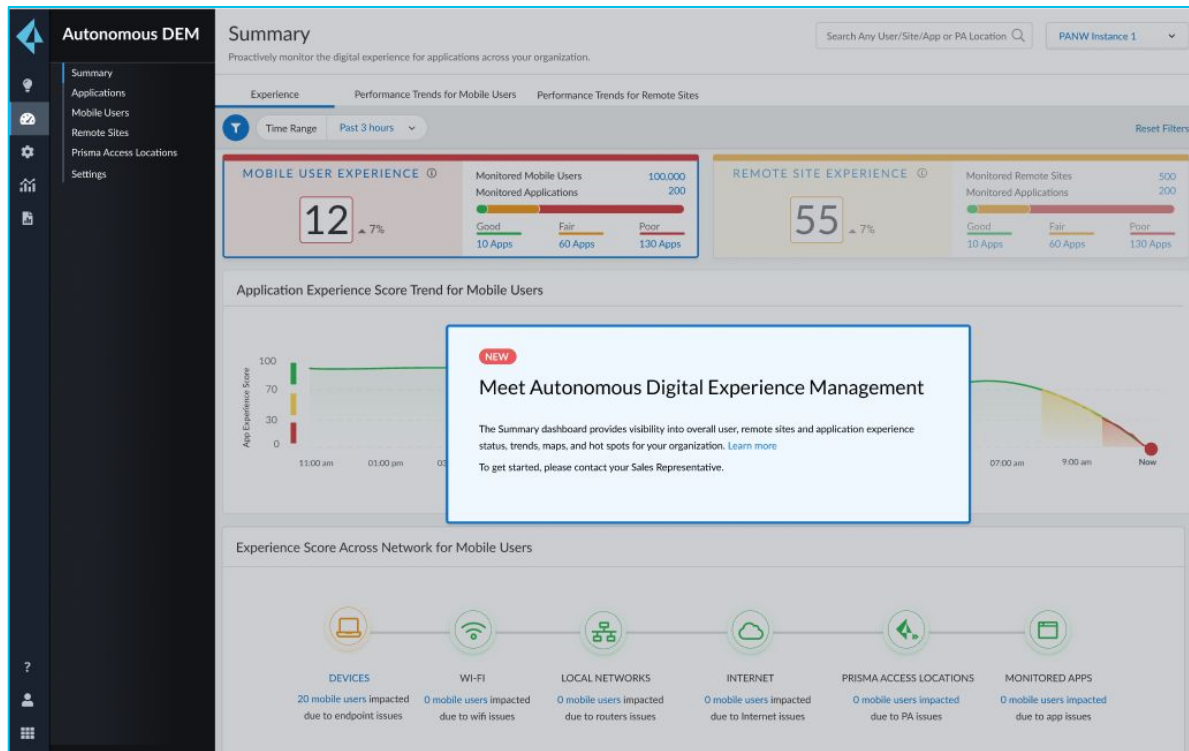
Explore Apps from Palo Alto Networks

App Icon	App Name	Description	Action
	Cortex Data Lake	Enable AI-based innovations for cybersecurity.	Learn More >
	Cortex XDR	Accelerate investigations by natively integrating network, endpoint and cloud data	Learn More >

Prisma Access ADEM App: The Hub

The Hub: Open ADEM App

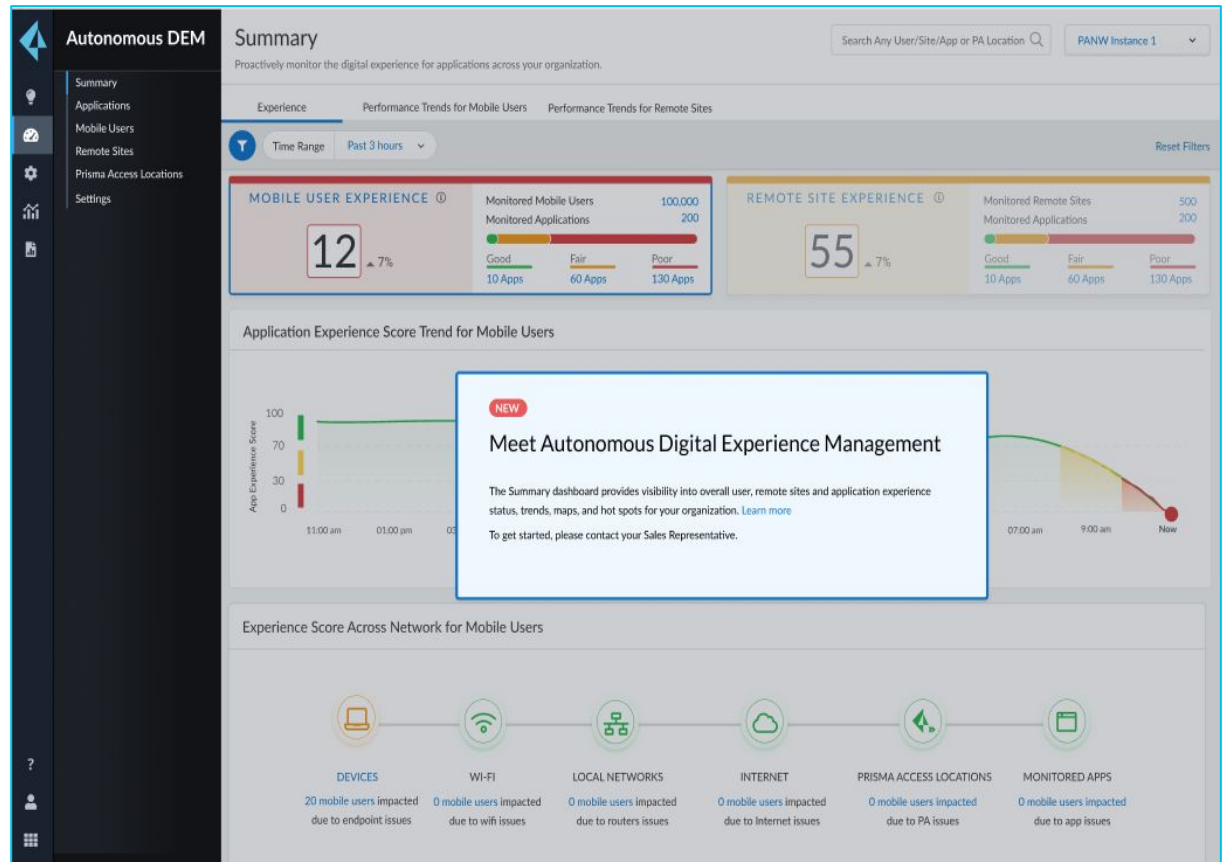
The users who have the correct roles should be able to see the Autonomous DEM in the Prisma Access navigation bar. Click on the summary tab to access ADEM



ADEM License Lock Dashboard - No ADEM License

ADEM License activation

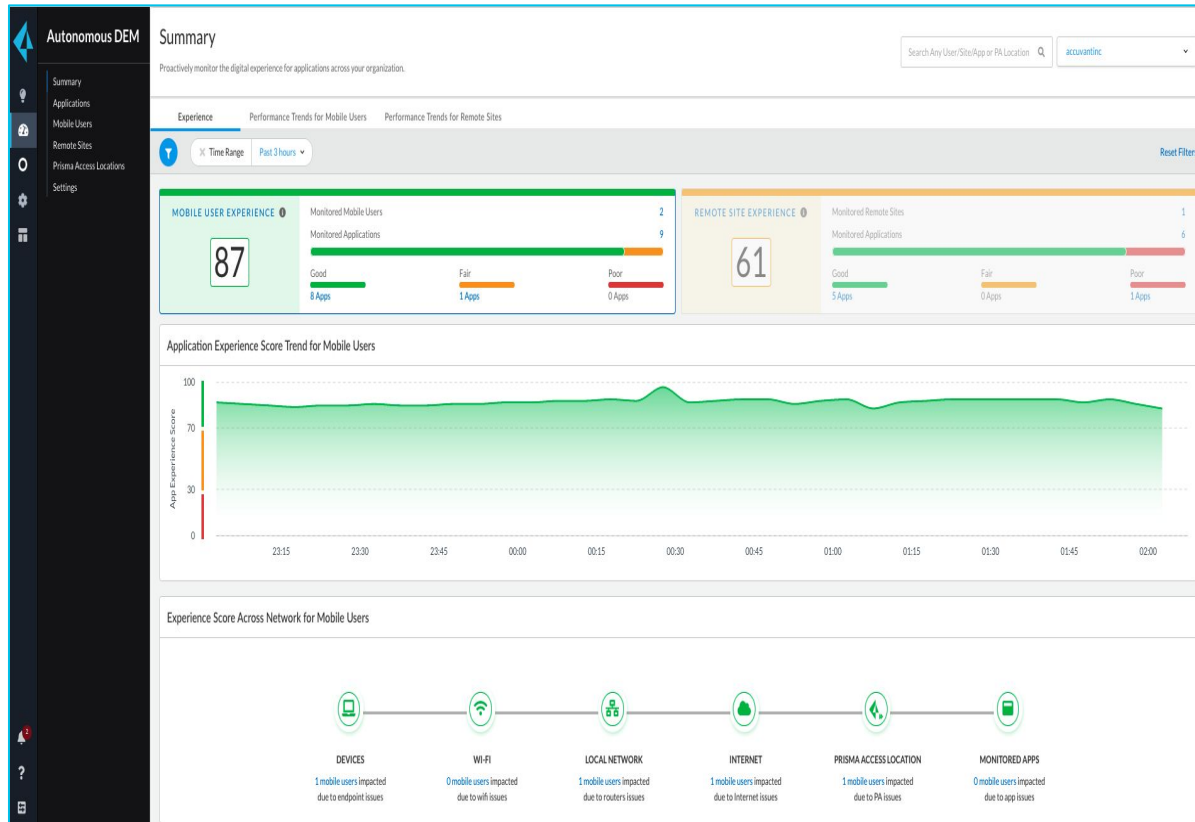
ADEM is an add-on purchase/license to prisma access. If the right license is not purchased and activated then the ADEM application is not accessible



ADEM Licensed for Mobile Users and Remote Networks

ADEM License activation

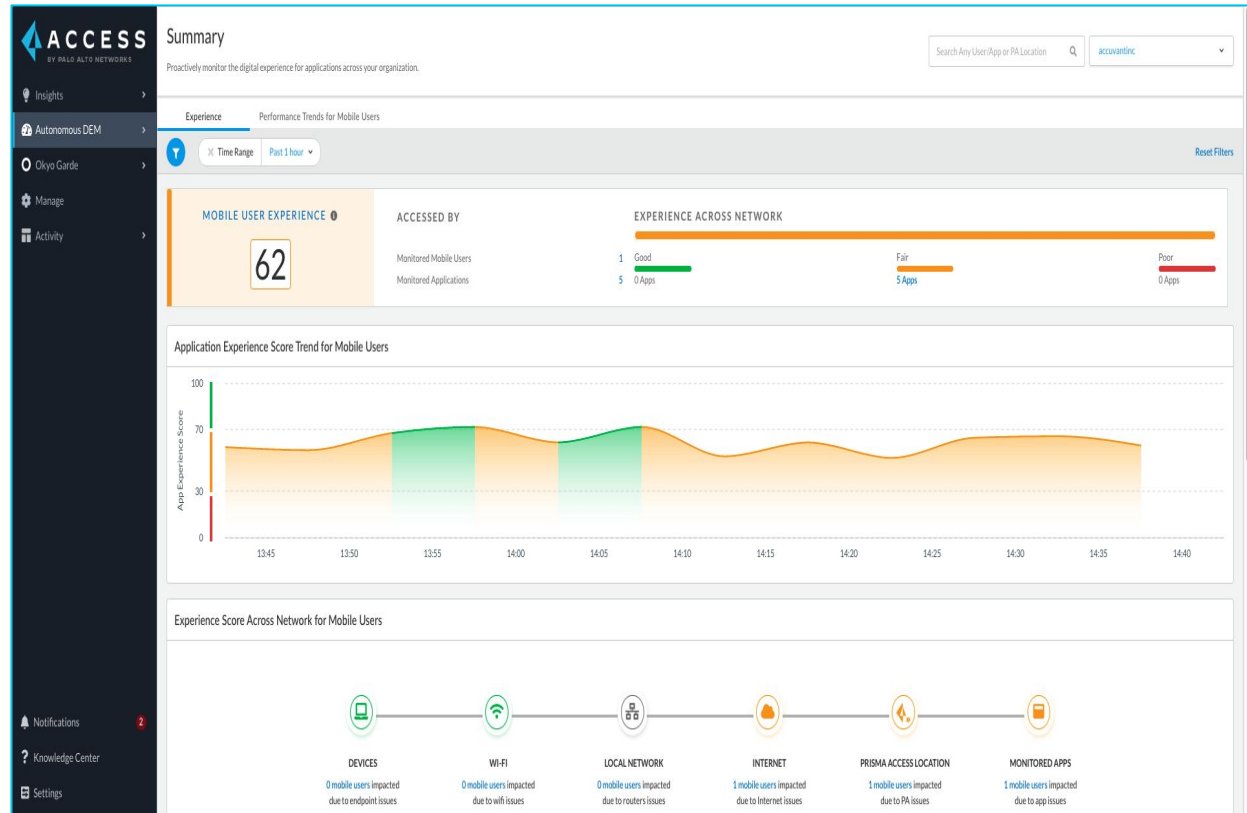
Upon the activation to the license the ADEM application becomes accessible to the users



ADEM Licensed for Mobile Users Only

ADEM License activation

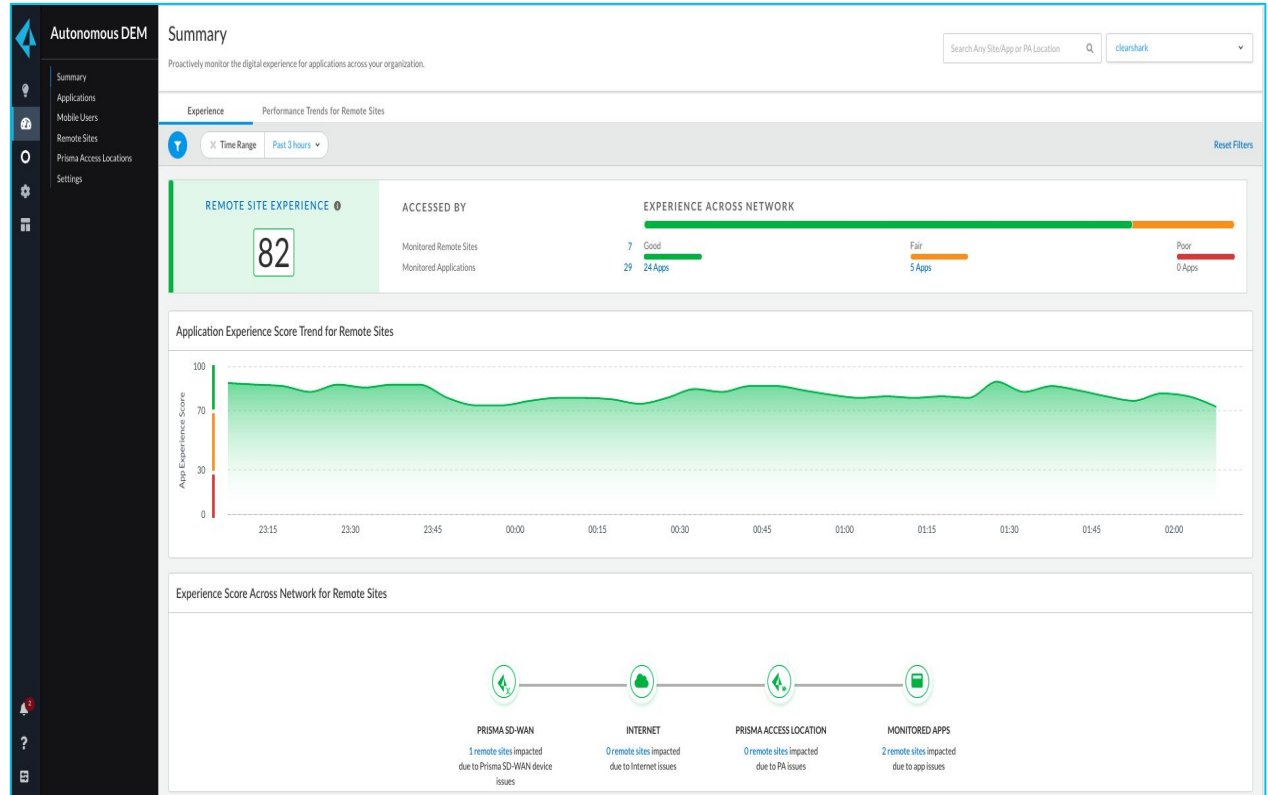
If only the ADEM Mobile users license is purchased only the Mobile users screens are activated



ADEM Licensed for Remote Network Only

ADEM License activation

If only the ADEM Remote Networks license is purchased only the Remote Network screens are activated



ADEM Solution Overview - High Level Overview

Autonomous DEM High Level Solution Overview

Cloud Managed
ADEM Portal

Synthetic Test Configs
Synthetic Test Metrics

Synthetic Test Configs
Synthetic Test Metrics

Synthetic Test Configs
Synthetic Test Metrics

ADEM Agent

GP Client

Endpoint
(Windows /
macOS)

GP



Mobile
Users

GP

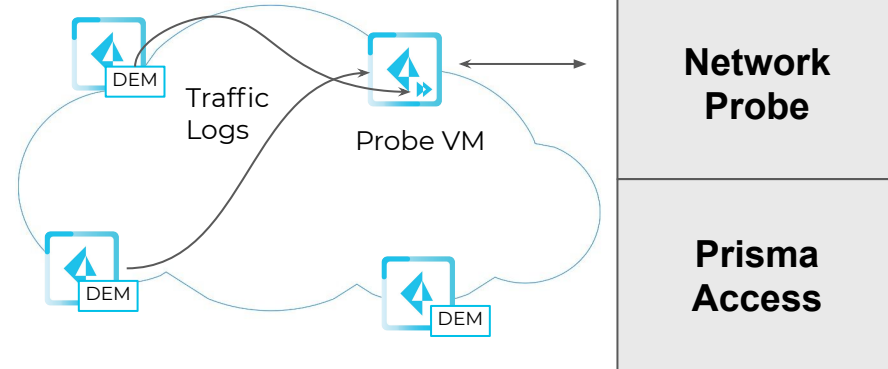


Mobile
Users

ADEM Agent

Prisma
SD-WAN ION

Branch



Autonomous DEM Telemetry Data Storage

- All ADEM data is stored in one of 8 DEM regions for a given tenant
- These map to existing CDL regions
- All DEM data is contained in a single region (DEM data for a single tenant never leaves its region)

DEM Country (AWS)	DEM Region
US	Ohio (us-east-2)
Europe	Frankfurt (eu-central-1)
UK	London (eu-west-2)
Singapore	Singapore (ap-southeast-1)
Canada	Canada Central (ca-central-1)
Japan	Tokyo (ap-northeast-1)
Australia	Sydney (ap-southeast-2)
India	Mumbai (ap-south-1)

Prisma Access Configuration To Enable ADEM for Mobile Users and Remote Networks

Prisma Access Configuration to Enable ADEM for Mobile users

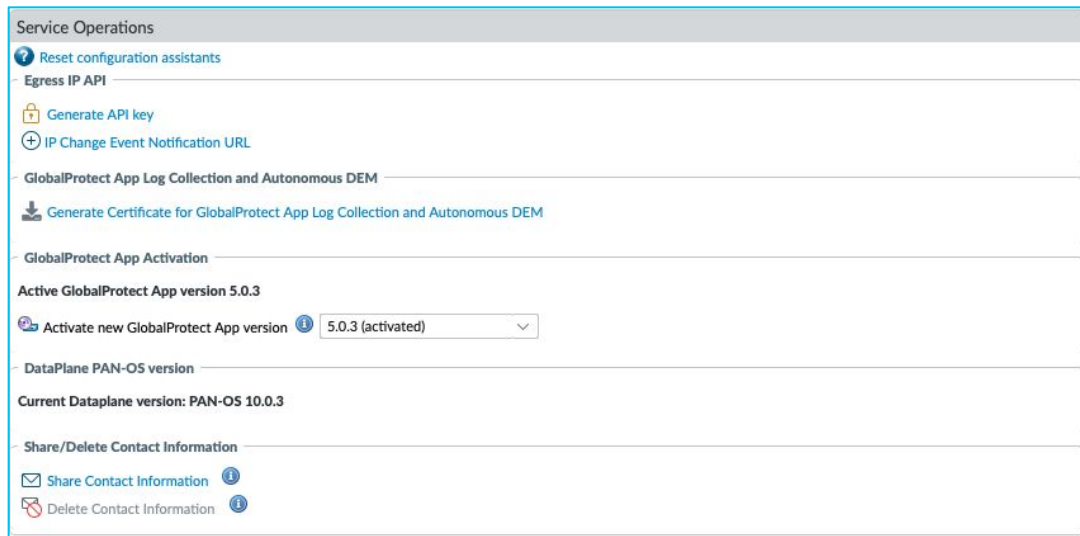
Four simple steps to enable ADEM on Prisma Access

- 1 Generate Client Certificate and select the certificate in Portal Agent Configuration
- 2 Enable “Log Collection for Troubleshooting”
- 3 Enable DEM in App Portal Settings
- 4 Enable DEM for Remote Networks
- 5 Optional-Add Security policies to make sure agent registration to DEM portal is allowed - if no other allow policies match this https traffic
- 6 Optional- Add Decryption policies to make sure traffic to DEM portal is allowed if Decryption is enabled

Note: If Prisma Access is already deployed, there is a possibility Step 1, 2 is already configured

Panorama Configuration to enable ADEM

- Generate Client Certificate for the endpoint agent to authenticate with DEM Portal. DEM uses the same endpoint certificate used for the GP App log collection feature.



Panorama Configuration to enable ADEM

- Set “Enable Log Collection for Troubleshooting” to Yes
- Enable DEM. Default value is “Do Not Install”

The screenshot shows the 'App' configuration page in the Panorama GUI. The 'App Configurations' table is visible on the left, and the 'App' tab is selected in the top navigation. The 'Digital Experience Monitoring Endpoint Agent for Prisma Access (Windows & Mac Only)' is highlighted, with the dropdown menu open showing 'Install and user can enable/disable a...'. The right side of the page contains various settings for the GlobalProtect app, including 'Welcome Page' (None), 'Disable GlobalProtect App' (Passcode, Confirm Passcode, Max Times User Can Disable: 0, Disable Timeout (min): 0), 'Uninstall GlobalProtect App' (Uninstall Password, Confirm Uninstall Password), and 'Mobile Security Manager Settings' (Mobile Security Manager, Enrollment Port: 443). The 'OK' and 'Cancel' buttons are at the bottom right.

App Configurations	
Log Gateway Selection Criteria	No
Enable Log Collection for Troubleshooting	Yes
Digital Experience Monitoring Endpoint Agent for Prisma Access (Windows & Mac Only)	Install and user can enable/disable a... Install and user can enable/disable a...
Run Diagnostics Tests for These Destination Web Servers	Do not install
Device Added to Quarantine Message	Install and user cannot enable/disable... to the network from this device. If the issue persists, contact your administrator.
Device Removed from Quarantine Message	Your security policy has restored access to the network from this device. If you still cannot access the network, contact your administrator.
Display Status Panel at Startup (Windows Only)	No

Panorama Configuration to enable ADEM

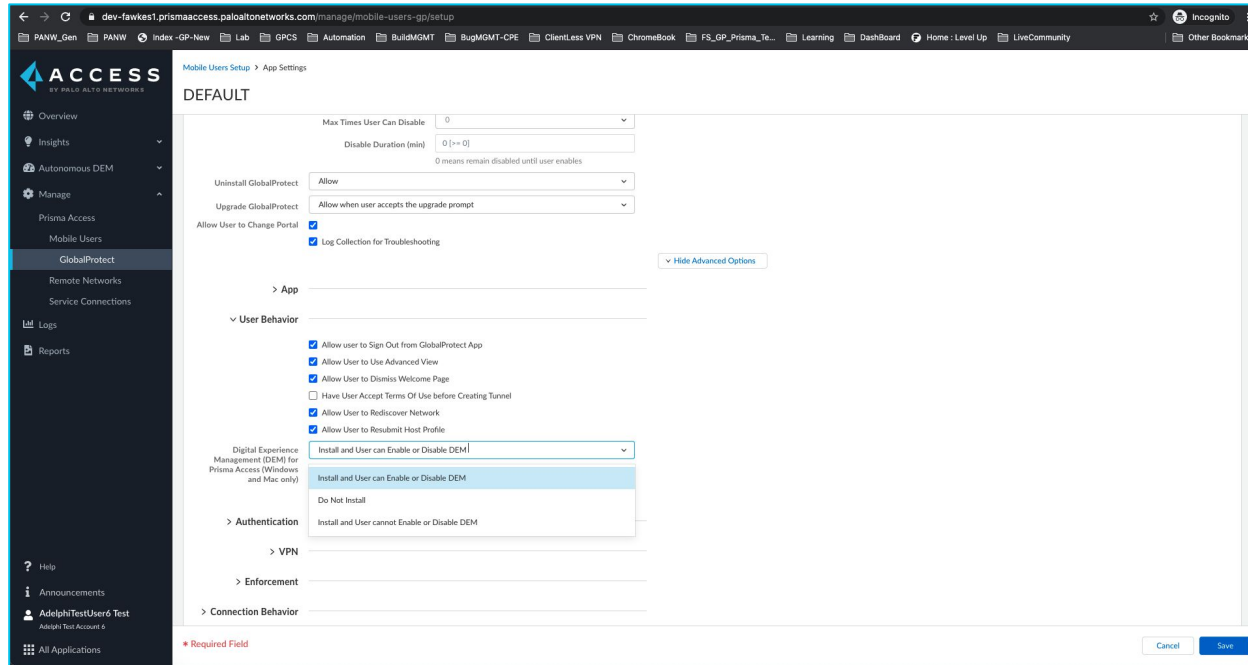
- Select the Client Certificate in Portal Agent Configuration

The screenshot shows the 'Configs' window in the Palo Alto Networks Panorama management console. The 'Authentication' tab is selected, and the 'Config Selection Criteria' is set to 'Internal'. The configuration is for a 'DEFAULT' client certificate. The 'Client Certificate' dropdown is set to 'Local', and the selected certificate is 'globalprotect_app_log_cert-old'. The 'Save User Credentials' option is set to 'Yes'. Under the 'Authentication Override' section, the 'Generate cookie for authentication override' and 'Accept cookie for authentication override' options are unchecked. The 'Cookie Lifetime' is set to 24 hours. The 'Certificate to Encrypt/Decrypt Cookie' is set to 'Authentication Cookie Cert'. In the 'Components that Require Dynamic Passwords (Two-Factor Authentication)' section, the 'Portal' option is checked, while 'Internal gateways-all', 'External gateways-manual only', and 'External gateways-auto discovery' are unchecked. At the bottom, there are 'OK' and 'Cancel' buttons.

- Add Security policies to make sure traffic to DEM portal is allowed. DEM endpoint registers to agent.dem.prismaaccess.com (prod). The policy should allow SSL traffic to the DEM portal

Fawkes Configuration to enable ADEM

- Fawkes also support DEM configuration. Log collection and DEM should be enabled as shown below:

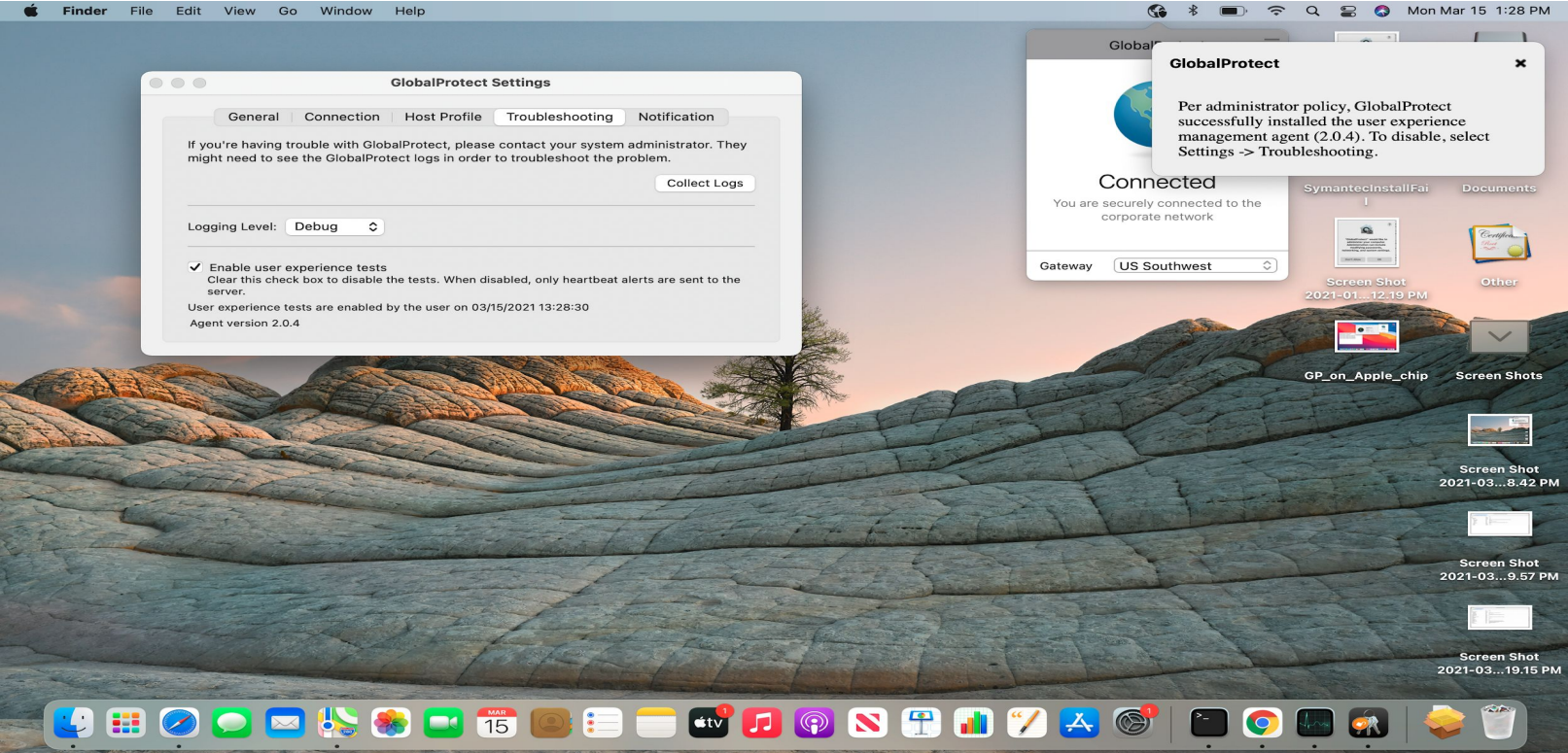


DEM EndPoint Agent: Windows

- DEM install package is part of the GlobalProtect 5.2.6
- DEM gets installed once GP connects to Prisma Access Portal if enabled on Portal



DEM EndPoint Agent: Mac



EndPoint Registered in DEM Portal

ACCESS
BY PALO ALTO NETWORKS

Settings

Review and adjust the settings for managing the lifecycle of the Endpoint Monitoring agent and customizing the health score metrics.

933908038

Time Range: Past 3 hours

Endpoint Agent Management | Audit Logs | License Details

1 Total Endpoint Agents

User	Device	Hostname	Last Seen	First Seen	User Status	Monitoring State	Endpoint Agent Version	Action
<input type="checkbox"/> gpcptest	Windows	DFWWIN014F5DF	9 mins ago	14 hours ago	Online	Enabled	2.0.3	

Rows: 12 | Page: 1 of 1

933908038

Help | User Name | Logout | App Switcher

Starting GlobalProtect 5.2.8, admin will have the flexibility to suppress receiving all ADEM endpoint update notifications (Install, Uninstall, Upgrade)

Configs ?

Authentication | Config Selection Criteria | Internal | External | **App** | HIP Data Collection

App Configurations

Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting	Yes
Display Autonomous DEM Updates Notification	No
Run Diagnostics Tests for These Destination Web Servers	Yes
Autonomous DEM endpoint agent for Prisma Access (Windows & MAC only)	No
Device Added to Quarantine Message	Install and user can enable/disable agent from GlobalProtect
Device Removed from Quarantine Message	Access to the network from this device has been restricted as per your organization's security policy. Please contact your IT Administrator.

Welcome Page: **None**

Disable GlobalProtect App

Passcode:

Confirm Passcode:

Max Times User Can Disable:

Disable Timeout (min):

Uninstall GlobalProtect App

Uninstall Password:

Confirm Uninstall Password:

Mobile Security Manager Settings

Mobile Security Manager:

Enrollment Port:

OK Cancel

App Configuration

Connect:

Disable GlobalProtect:

Max Times User Can Disable:

Disable Duration (min):
0 means remain disabled until user enables

Uninstall GlobalProtect:

Upgrade GlobalProtect:

Allow User to Change Portal:

Enable Log Collection for Troubleshooting:

App

GlobalProtect App Config Refresh Interval (hours):

Show GlobalProtect Icon in System Tray

Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)

Show Status Panel at Startup (Windows Only)

Display ADEM Updates Notification Message

Autonomous DEM for Remote Networks

- ADEM for Remote Network is only supported with Prisma Access and Prisma SD-WAN integrated deployments. No support for 3rd party Remote Network deployments.
- CloudBlade is required for Prisma Access and Prisma SD-WAN integration to enable ADEM
- Remote Network for Prisma Access should be configured with Aggregate Bandwidth.
- ADEM for RN can be enabled on Prisma Access on one or more compute locations.
- Software Version Matrix

	Minimum Release
Prisma Access	2.2 Preferred
Prisma SD-WAN	5.6.1-b12
CloudBlade Panorama	2.1.2
CloudBlade Fawkes	3.1.1

- Supported for all Prisma SD-WAN Hardware and Virtual appliances

Deployment Facts for ADEM Remote Networks

- To enable ADEM for Remote Networks, ADEM bandwidth should be allocated on Prisma Access compute locations following existing remote network aggregate bandwidth workflow
 - Supported from Panorama and Cloud Management App
 - ADEM bandwidth allocation should match allocated remote network bandwidth on each compute location

Bandwidth Allocation			
Remote Network Allocated Total : 250 / 2000 Mbps Click each bandwidth allocation to edit bandwidth allocated to compute location		Autonomous DEM Allocated Total : 100 / 2000 Mbps To allocate, enable Autonomous DEM for each compute location. It will use the same bandwidth as the remote network	
Bandwidth Allocation (Mbps)	Autonomous DEM Allocation	Compute Location	Prisma Access Locations
0	<input type="checkbox"/> Enable	Canada Central New	Canada Central
0	<input type="checkbox"/> Enable	Canada Central	Canada East
0	<input type="checkbox"/> Enable	US Northwest	Canada West, US Northwest
50	<input type="checkbox"/> Enable	US Southeast	Costa Rica, Mexico Central, Panama, US Southeast, Colombia
50	<input checked="" type="checkbox"/> Enable	US Southwest	Mexico West, US Southwest, US West
0	<input type="checkbox"/> Enable	US Central	US Central, US South
50	<input checked="" type="checkbox"/> Enable	US East	US East, US Northeast
0	<input type="checkbox"/> Enable	South America East	Argentina, Bolivia, Brazil Central, Brazil East, Brazil South, Chile, Ecuador, Paraguay, Peru, Venezuela
0	<input type="checkbox"/> Enable	Europe Central	Andorra, Austria, Bulgaria, Croatia, Czech

Manage

Service Setup

- Overview
- Shared
- Mobile Users
- GlobalProtect
- Explicit Proxy
- Remote Networks
- Service Connections

Configuration

Manage > Remote Networks Setup Push Config

Remote Networks Setup

Onboard geographically-distributed sites—branch offices, retail stores, and SD-WAN deployments—to Prisma Access.

Remote Networks Inbound Access Remote Networks **Bandwidth Management** Advanced Settings

Bandwidth Allocation for Remote Networks

Configure the bandwidth and allocation at computing locations and sites level.
For QoS at compute location, the max bandwidth is allocated bandwidth or max bandwidth per node.

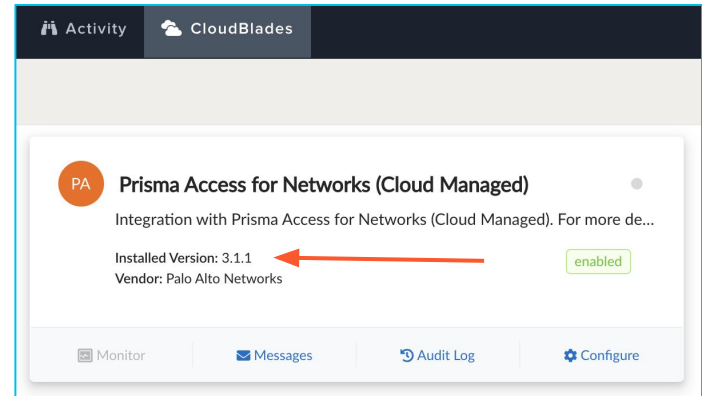
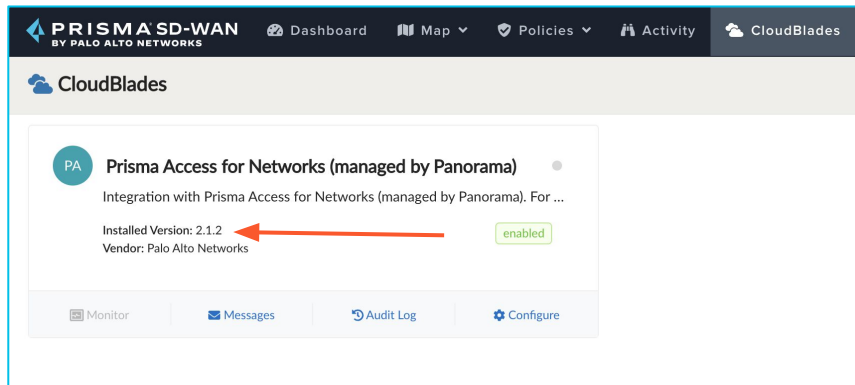
Remote Networks 1,600/3,000 Mbps is allocated Autonomous DEM 1,600/3,000 Mbps is allocated

Show Compute Locations that are in use

Compute Location	Assigned Bandwidth (Mbps)	Prisma Access Locations	Autonomous DEM	QoS	Guaranteed Bandwidth (Mbps)
Asia South	200	Bangladesh, India North, India South, India West, Pakistan South, Pakistan West	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Asia Southeast	400	Cambodia, Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Australia Southeast	0	Papua New Guinea, Australia East, Australia South, Australia Southeast, New Zealand	<input type="checkbox"/>	<input type="checkbox"/>	
Bahrain	0	Bahrain	<input type="checkbox"/>	<input type="checkbox"/>	
Belgium	0	Belgium	<input type="checkbox"/>	<input type="checkbox"/>	
Canada Central	0	Canada Central, Canada East	<input type="checkbox"/>	<input type="checkbox"/>	
Europe Central	1000	Andorra, Austria, Bulgaria, Croatia, Czech Republic, Germany Central, Germany North, Germany South, +26 more	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Europe North	0	Belarus, Finland, Lithuania, Norway, Russia Central, Russia Northwest, Sweden	<input type="checkbox"/>	<input type="checkbox"/>	
Europe Northwest	0	France South, UK	<input type="checkbox"/>	<input type="checkbox"/>	
Europe West	0	Denmark, Netherlands Central, Netherlands South	<input type="checkbox"/>	<input type="checkbox"/>	
France North	0	France North	<input type="checkbox"/>	<input type="checkbox"/>	
Hong Kong	0	Hong Kong	<input type="checkbox"/>	<input type="checkbox"/>	
Ireland	0	Ireland	<input type="checkbox"/>	<input type="checkbox"/>	

Prisma SD-WAN Site Registration on ADEM

- Following are the criterias for a successful ADEM agent registration with ADEM portal:
 - SD-WAN ION - 5.6.1
 - SD-WAN IONs deployed in Branches will have a new process “adem” after upgrading to 5.6.1 software
 - SD-WAN IONs deployed in DataCenter will not have this “adem” process
 - CloudBlade (CB) - 2.1.2 and 3.1.1:
 - CB-2.1.2 provides the following information to the SD-WAN controller
 - Prisma Tenant-ID
 - All SPN and RN information where tunnels are established
 - SD-WAN controller provides these information to the SD-WAN ION
 - ADEM agent in the SD-WAN ION will use the following information to register with the ADEM portal:
 - SD-WAN ION CIC certificate
 - Prisma Tenant-ID
 - SPN/RN information (SPN should have the ADEM enabled)
 - ADEM Portal will validate these information and successfully registers the ADEM agent



Prisma SD-WAN Site Registration on ADEM Portal

The screenshot shows the 'Settings' page for 'Autonomous DEM' in the Prisma SD-WAN ADEM Portal. The page is titled 'Settings' and has a subtitle 'Review and adjust the settings for managing the lifecycle of the agents'. A search bar with the text 'clearshark' is visible in the top right. The left sidebar contains navigation options: Summary, Applications, Mobile Users, Remote Sites, Prisma Access Locations, and Settings. The main content area is divided into tabs: Endpoint Agent Management, Remote Site Agent Management (selected), Health Score Profiles, Audit Logs, and License Details. Below the tabs, it shows '7 Total Remote Site Agents' with a 'More Actions' dropdown and an 'Upgrade Options' button. A table lists the agents with columns for Remote Site Name, Device Model, Hostname, HA Peer Hostname, Last Seen, First Seen, Site Status, Monitoring State, and Remote Site Agent Version. Two rows for 'Lille' are highlighted with red boxes: one with 'Online' status and one with 'Offline' status.

	Remote Site N...	Device Model	Hostname	HA Peer Hostn...	Last Seen	First Seen	Site Status	Monitoring State	Remote Site Agent Version	Ac...
<input type="checkbox"/>	Switzerland	ion 3108v	fei_b3-3108v1	Not Applicable	2 mins ago	1 months ago	Online	Enabled	10.9.0	
<input type="checkbox"/>	Vancouver	ion 2000	fei_b5-2k2		1 days ago	1 months ago	Offline	Enabled	10.9.0	
<input type="checkbox"/>	Vancouver	ion 2000	fei_b5-2k1		1 days ago	1 months ago	Offline	Enabled	10.9.0	
<input type="checkbox"/>	Chennai	ion 1200-c5g-ww	fei_b4-cellular	Not Applicable	2 mins ago	1 months ago	Online	Enabled	10.9.0	
<input checked="" type="checkbox"/>	Seoul	ion 9000	fei_b7-9k	Not Applicable	1 days ago	25 days ago	Offline	Enabled	10.9.0	
<input type="checkbox"/>	Lille	ion 1000	fei_b6-1k02	fei_b6-1k01	2 mins ago	25 days ago	Online	Enabled	10.9.0	
<input type="checkbox"/>	Lille	ion 1000	fei_b6-1k01	fei_b6-1k02	7 mins ago	25 days ago	Online	Enabled	10.9.0	

Rows: 20 | Page: 1 of 1

Prisma Access Security Policy for Agent Registration

Manage > Security Policy > Security Policy Rule for Entire Service

Allow All Traffic for ADEM clients

Enforce traffic based on its origin.

ZONES * Custom ▾
Zones
trust × +

ADDRESSES * Any Address
Add Addresses
Add Address Groups
Add External Dynamic Lists
Add Regions

USERS * Any User ▾
Add Users

HIP PROFILES ENTITIES ▾
Add HIP Profiles

Destination

Enforce traffic based on where it terminates.

ZONES * Custom ▾
Zones
untrust × +

ADDRESSES * Custom ▾ Match Exclude (Negat
Address Groups
ADEM-URL × +

Add Addresses
Add External Dynamic Lists
Add Regions
Add SaaS Application Endpoints

Address Groups

Name *
ADEM-URL

Description

Type
Static ▾

Address Entities *
▾
Address
ADEM-1 ... ADEM-4 ... ADEM-5 ... ADEM-6 ... ADEM-7 ... ADEM-8 ... +

Tag
+

* Required Field

Cancel Save

Prisma Access Decryption Policy for Agent Registration (When SSL Decryption is Enabled)

The screenshot displays the Palo Alto Networks Prisma Access configuration interface. The left sidebar shows the navigation menu with 'Manage' selected. The main content area is titled 'ADEM-POLICY' and shows the configuration for a decryption policy. The 'ADDRESSES' section is expanded, showing a list of addresses: 'ADEM-1' and 'ADEM-2'. A red arrow points from the 'ADEM-2' address in the list to the 'Addresses' configuration form on the right.

The 'Addresses' configuration form includes the following fields:

- Name ***: AEM-3
- Description**: (Empty)
- Type**: FQDN
- FQDN ***: agents.dem.prismaaccess.com
- Tags**: (+)

At the bottom of the form, there is a legend for the asterisk: *** Required Field**. There are 'Cancel' and 'Save' buttons at the bottom right of the form.

Prisma Access URL Filtering Policy to Suppress Agent Registration Logs

- When URL filtering capability is enabled, the URL filtering logs within Prisma Access will log all of the call-home entries by the ADEM Agents.
- If we need to suppress them - Create an allow rule for *.dem.prismaaccess.com that doesn't log those entries.

ADEM License Usage Visibility on ADEM Portal

Autonomous DEM Settings clearshark

Review and adjust the settings for managing the lifecycle of the agents

Endpoint Agent Management Remote Site Agent Management Health Score Profiles Audit Logs **License Details**

License Details for Autonomous Digital Experience Management

License Type: **PAID**

License Count and Dates: **MOBILE USERS**

User Count: 5000 TOTAL | 34 USED | 4966 AVAILABLE

Application Tests: 50000 TOTAL | 102 USED | 49898 AVAILABLE

Expiration Date: 23.06.2024 974 DAYS REMAINING

REMOTE SITES

Bandwidth: 5000 TOTAL | 2500 USED | 2500 AVAILABLE

Expiration Date: 23.06.2024 974 DAYS REMAINING

Autonomous DEM Agents Overview

Autonomous DEM Endpoint Agents - Overview

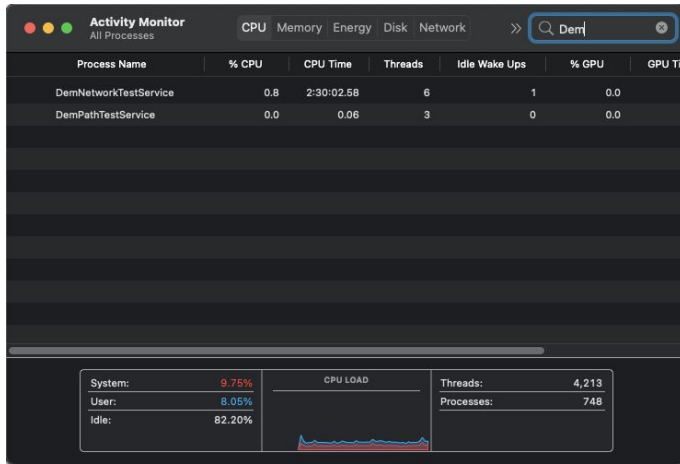
- Available for Windows and macOS
- Auto-installed by GP client
- Runs in the background, as a service (no UI)
- Connects to ADEM portal via HTTPS
- All connectivity via *.dem.prismaaccess.com domains
- Sends up telemetry every 5 minutes

Autonomous DEM Endpoint Agents - Windows

- Currently Intel-based Windows
- Supports Windows 10 (and newer)
- Low footprint (<1%CPU, < 50MB RAM, <50MB disk)

Autonomous DEM Endpoint Agents - macOS

- Currently Intel-based Macs
- Supports OS X / macOS El Capitan (10.11) and newer
- Low footprint (<1%CPU, < 50MB RAM, <50MB disk)
- Search for “Dem” in Activity monitor



Autonomous DEM Prisma SD-WAN Agent - Overview

- Bundled with SD-WAN ION software
- Auto-enabled by ADEM license
- Runs in the background, as a service (no UI)
- Connects to ADEM portal via HTTPS
- All connectivity via `*.dem.prismaaccess.com` domains
- Sends up telemetry every 5 minutes
- Auto-update independent of SD-WAN ION software

Autonomous DEM Prisma SD-WAN Agent - Metrics

- Collect element/device metrics
 - CPU, RAM
 - Device, Site Name and details

- Runs synthetic tests *
 - VPN Overlay - Delay, Jitter, Loss
 - VPN Underlay - Delay, Jitter, Loss AND Hop-by-hop
 - User-defined tests
 - End-to-end delay, jitter and loss
 - End-to-end hop-by-hop
 - End-to-end web

* All tests are run over all possible paths.

Autonomous DEM Application Test Creation

ADEM Application Test configuration on ADEM Portal

Autonomous DEM

- Summary
- Applications
- Mobile Users
- Remote Sites
- Prisma Access Locations
- Settings

Applications

View enterprise-wide application performance and usage details. Drill-down to access details for a specific application.

Applications
Application Tests

<input type="checkbox"/>	Priority	Application Test Name	Date Created	Application Name	Assigned Mobile Users	Assigned Remote Sites	Excluded Remote Sites	Status
<input type="text" value="Search Priority"/>	<input type="text" value="Search Test Name"/>	<input type="text" value="Search Date Created"/>	<input type="text" value="Search Application Name"/>	<input type="text" value="Search Assigned Mobile Users"/>	<input type="text" value="Search Assigned Sites"/>	<input type="text" value="Search Excluded Remote Sites"/>	<input type="text" value="Search Status"/>	
☰	<input type="checkbox"/> 1	facebook	20 Sep 2021 09:43:45 PM	facebook	0	5	4	Enabled
☰	<input type="checkbox"/> 2	DC1 Server	22 Sep 2021 12:17:39 AM	icmp	0	5	4	Enabled
☰	<input type="checkbox"/> 3	Google	06 Sep 2021 01:28:05 PM	google-base	0	5	4	Enabled
☰	<input type="checkbox"/> 4	DC2 Server	22 Sep 2021 12:18:59 AM	http	0	5	4	Enabled
☰	<input type="checkbox"/> 5	yahoo	11 Oct 2021 11:42:14 PM	yahoo	0	5	4	Enabled
☰	<input type="checkbox"/> 6	Youtube	16 Oct 2021 01:30:19 PM	youtube	0	5	4	Enabled
☰	<input type="checkbox"/> 7	Limit-1-twitter	11 Oct 2021 11:40:32 PM	twitter-base	0	1	8	Enabled
☰	<input type="checkbox"/> 8	Limit-2-akamai	13 Sep 2021 07:25:00 PM	akamai-client	0	1	8	Enabled
☰	<input type="checkbox"/> 9	Limit-3-Salesforce	13 Sep 2021 06:25:38 PM	salesforce-base	0	1	8	Enabled
☰	<input type="checkbox"/> 10	Limit-4-office	13 Sep 2021 07:26:05 PM	ms-office365	0	2	7	Enabled
☰	<input type="checkbox"/> 11	Limit-5-maps	13 Sep 2021 07:27:31 PM	apple-maps	0	2	7	Enabled
☰	<input type="checkbox"/> 12	Limit-6-bingmaps	13 Sep 2021 07:30:05 PM	bing-maps	0	2	7	Enabled
☰	<input type="checkbox"/> 13	Limit-7-gmaps	13 Sep 2021 07:28:46 PM	google-maps	0	2	7	Enabled
☰	<input type="checkbox"/> 14	Limit-8-instagram	13 Oct 2021 12:46:43 AM	instagram-base	0	1	8	Enabled
☰	<input type="checkbox"/> 15	Limit-9-reddit	13 Oct 2021 12:48:05 AM	reddit	0	1	8	Enabled
☰	<input type="checkbox"/> 16	Limit-10-Zoom	13 Oct 2021 12:49:09 AM	zoom-base	0	1	8	Enabled
☰	<input type="checkbox"/> 17	Limit-11-teams	13 Oct 2021 12:51:30 AM	ms-teams-audio-video	0	1	8	Enabled
☰	<input type="checkbox"/> 18	Limit-12-slack	13 Oct 2021 12:55:18 AM	slack	0	1	8	Enabled
☰	<input type="checkbox"/> 19	Limit-13-jira	13 Oct 2021 12:57:52 AM	jira	0	1	8	Enabled
☰	<input type="checkbox"/> 20	Limit-14-confluence	13 Oct 2021 12:59:23 AM	confluence	0	1	8	Enabled

ADEM Application Test configuration - Select Remote Sites

Autonomous DEM

Application List > Add New App Test

New App Test

Add tests to monitor user experience and application performance on your network.

Name *

Description

1. Select Mobile Users and/or Remote Sites
Select mobile users and remote sites you want to start the test on.

2. Choose Apps
Confirm the apps you want to test.

3. Save
Click on save to start the test and monitoring.

Source

Select mobile users and remote sites that you want to monitor.

MOBILE USERS None ▾

REMOTE SITES Custom ▾

Remote Sites

Lille × Seoul × Switzerland × Chennai × Vancouver ×

- Naples
- Singapore
- Switzerland
- Chennai
- Vancouver

Target

Select target applications that you want to monitor.

APPLICATION ENTITIES

* Required Field

By default, all licensed Autonomous DEM mobile users and remote sites are assigned to the test. You can modify the default and select specific users and sites for which you want to enable a test.

Select an application for which you want to monitor the performance and user experience. For a custom application, define an application target by specifying the domain or an IP address to identify the

ADEM Application Test configuration - Select Mobile Users

The screenshot shows the 'New App Test' configuration page in the Palo Alto Networks ADEM console. The left sidebar contains navigation options: Summary, Applications, Mobile Users (selected), Remote Sites, Prisma Access Locations, and Settings. The main content area is titled 'New App Test' and includes a breadcrumb 'Application List > Add New App Test'. Below the title is a description: 'Add tests to monitor user experience and application performance on your network.' The configuration form has two main sections: 'Source' and 'Target'. In the 'Source' section, 'MOBILE USERS' is set to 'None' (indicated by a red arrow) and 'REMOTE SITES' is set to 'Custom'. Below this, a list of remote sites is shown: Lille, Seoul, Switzerland, Chennai, and Vancouver. A search dropdown is open for 'Search Remote Sites', showing a list of sites with checkboxes: Naples, Singapore, Switzerland (checked), Chennai (checked), and Vancouver (checked). The 'Target' section is partially visible, with 'APPLICATION ENTITIES' set to a dropdown menu. At the bottom right, there are 'Cancel' and 'Save' buttons. A lightbulb icon with text provides a tip: 'By default, all licensed Autonomous DEM mobile users and remote sites are assigned to the test. You can modify the default and select specific users and sites for which you want to enable a test.'

Autonomous DEM

Application List > Add New App Test

New App Test

Add tests to monitor user experience and application performance on your network.

Name *

Description

1. Select Mobile Users and/or Remote Sites
Select mobile users and remote sites you want to start the test on.

2. Choose Apps
Confirm the apps you want to test.

3. Save
Click on save to start the test and monitoring.

Source

Select mobile users and remote sites that you want to monitor.

MOBILE USERS **None** ▼

REMOTE SITES **Custom** ▼

Remote Sites

Lille x Seoul x Switzerland x Chennai x Vancouver x

Search Remote Sites

- Naples
- Singapore
- Switzerland
- Chennai
- Vancouver

Target

Select target applications that you want to monitor.

APPLICATION ENTITIES

* Required Field

Cancel Save

By default, all licensed Autonomous DEM mobile users and remote sites are assigned to the test. You can modify the default and select specific users and sites for which you want to enable a test.

Select an application for which you want to monitor the performance and user experience. For a custom application, define an application target by specifying the domain or an IP address to identify the

ADEM Application Test configuration - Select Application

The screenshot displays the 'Autonomous DEM' configuration interface. The left sidebar contains navigation options: Summary, Applications, Mobile Users, Remote Sites, Prisma Access Locations, and Settings. The main content area is divided into two steps: '1. Select Mobile Users and/or Remote Sites' and '2. Choose Apps'. Step 1 includes sections for 'Source' (with 'MOBILE USERS' set to 'None' and 'REMOTE SITES' set to 'Custom') and 'Target' (with 'APPLICATION ENTITIES' set to 'amazon-aws-console' and 'Domains' set to 'www.aws.amazon.com'). A red arrow points to the 'amazon-aws-console' dropdown. Step 2 includes an 'Edit Target' dialog box with 'Ip Addresses' and 'Domain' fields. The 'Ip Addresses' field contains 'e.g. 1.2.102.219' and the 'Domain' field contains 'www.aws.amazon.com' and 'e.g. www.google.com'. The 'Edit Target' dialog box has 'Cancel' and 'Save' buttons.

ADEM Application Test configuration - Advanced Config Options

The screenshot displays the 'Advanced Options' configuration page for an application test in the Autonomous DEM console. The interface is divided into several sections:

- MOBILE USERS:** All Mobile Users Selected
- REMOTE SITES:** All Remote Sites Selected
- Target:** Select target applications that you want to monitor. The 'APPLICATION ENTITIES' dropdown is set to 'salesforce'. Domains are listed as 'www.salesforce.com'.
- Advanced Options:**
 - ADVANCED NETWORK TEST OPTIONS:** Protocol: TCP, Port: 443. Checked options include 'Measure end-to-end availability, latency, jitter and loss' and 'Measure per-hop network paths'. 'Split Tunnel' is unchecked.
 - ADVANCED WEB TEST OPTIONS:** 'Enable HTTP/HTTPS testing' is checked. 'Ignore SSL warnings and errors' and 'Override the default HTTP/HTTPS port' are unchecked.
 - Protocol: https, Path: (empty), Target URL: https://www.salesforce.com/
 - Headers: e.g. Accept: application/json
 - ADVANCED MOBILE USERS TEST OPTIONS:** 'End-to-end Application Experience monitoring from Untrusted Networks when VPN is disabled' is checked. 'End-to-end Application Experience monitoring from Trusted Networks (In Office)' is unchecked.
 - ADVANCED REMOTE SITES TEST OPTIONS:** 'Enable Application Experience monitoring on active and backup paths' is checked. 'Enable Application Experience monitoring on active paths only' is unchecked.

Two red arrows point to the checked options in the 'ADVANCED MOBILE USERS TEST OPTIONS' and 'ADVANCED REMOTE SITES TEST OPTIONS' sections. A 'Required Field' asterisk is visible at the bottom left. 'Cancel' and 'Save' buttons are at the bottom right.

ADEM RN Application Test Summary - Assigned/Excluded Sites

Autonomous DEM Applications

View enterprise-wide application performance and usage details. Drill-down to access details for a specific application.

Search Any Site/App or PA Location clearshark

Reset Filters

Applications Application Tests

50 Application Tests Delete Enable Disable Add New App Test

Priority	Application Test Name	Date Created	Application Name	Assigned Remote Sites	Excluded Remote Sites	Status
1	Google	02 Nov 2021 12:58:57 PM	google-base	5	0	Enabled
2	Yahoo	02 Nov 2021 12:59:53 PM	yahoo	5	0	Enabled
3	Youtube	02 Nov 2021 01:35:18 PM	youtube	5	0	Enabled
4	Facebook	02 Nov 2021 01:40:15 PM	facebook	5	0	Enabled
5	Twitter	02 Nov 2021 01:41:52 PM	twitter-base	5	0	Enabled
6	DC1_Server1_ICMP	02 Nov 2021 02:14:56 PM	icmp	5	0	Enabled
7	DC2_Server2_ICMP	02 Nov 2021 02:16:28 PM	00-7812	5	0	Enabled
8	Scale-Redfin	02 Nov 2021 02:18:27 PM	http	2	0	Enabled
9	Scale-Zillow	02 Nov 2021 02:28:48 PM	http2	2	0	Enabled
10	Scale-Microsoft	02 Nov 2021 02:30:38 PM	ssl	2	0	Enabled
11	Scale-Google_Drive	02 Nov 2021 02:33:59 PM	google-drive-web	2	1	Enabled
12	Scale-Google_Maps	02 Nov 2021 02:35:23 PM	google-maps	2	1	Enabled
13	Scale-Google_Docs	02 Nov 2021 02:36:51 PM	google-docs-base	2	1	Enabled
14	Scale-Google_Cloud	02 Nov 2021 02:38:23 PM	google-cloud-console	2	1	Enabled
15	Scale-Bing_Maps	02 Nov 2021 02:39:47 PM	bing-maps	2	1	Enabled
16	Scale-Slack	02 Nov 2021 02:44:39 PM	slack-base	2	1	Enabled
17	Scale-Zoom	02 Nov 2021 02:45:36 PM	zoom	2	1	Enabled
18	Scale-Etrade	02 Nov 2021 02:48:45 PM	finance-and-investment	2	1	Enabled
19	Scale-Lucidchart	02 Nov 2021 02:51:16 PM	web-browsing	2	1	Enabled
20	Scale-Amazon_AWS	02 Nov 2021 02:59:04 PM	amazon-aws-console	2	1	Enabled

Drag Application Tests in the order you prefer OR use ↑ and ↓ to change the order and click Save to confirm test priority order

Rows 20 Page 1 of 3

Assigned Remote Sites:

- When an App test is configured and the SD-WAN site is able to run the test, it is counted towards the Assigned Remote site count.

Excluded Remote Sites:

- When an App test is configured and the Sd-WAN site is unable to run the test because it has reached its max supported capacity it is counted towards the Excluded Remote Site count.

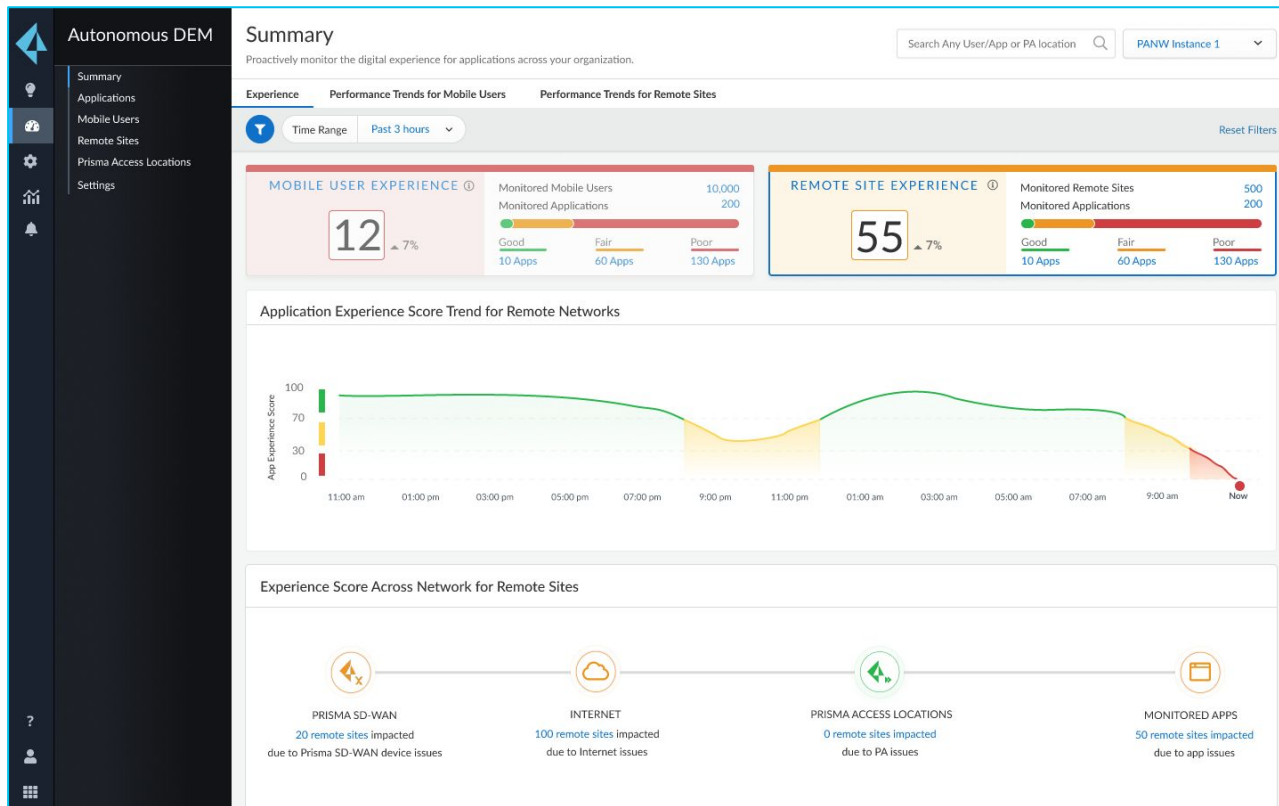
Autonomous DEM Synthetic Tests - Device Capacity

Prisma SD-WAN ION Platform	Application Test*
ION-1000	Upto 20
ION-1200	Upto 20
ION-2k	Upto 30
ION-3k	Upto 40
ION-7k	Upto 50
ION-9k	Upto 75
ION-3102V	Upto 30
ION-3104V	Upto 40
ION-3108V	Upto 50

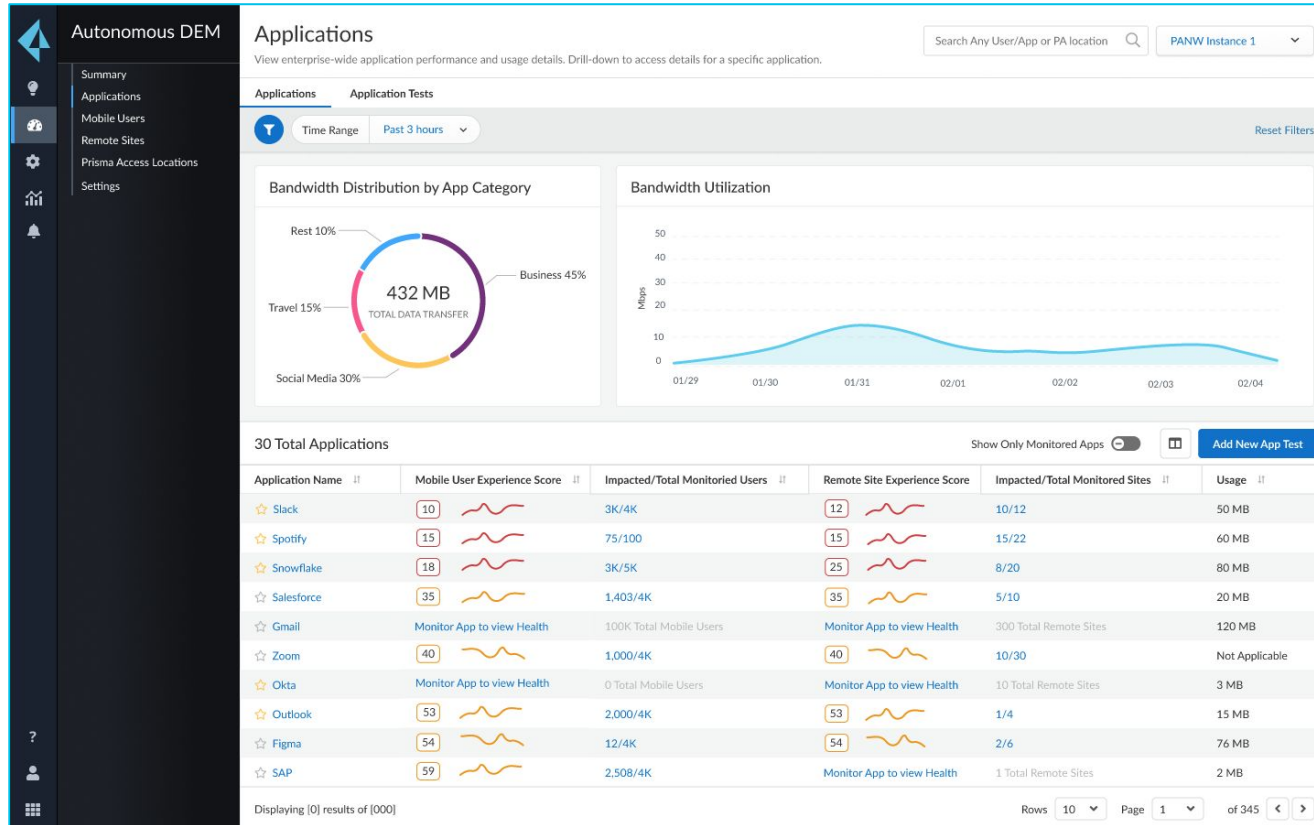
***Note:** Each platform can run upto defined number of application test presuming each application is configured to use max 4 paths. If number of paths configured per application increases, it will reduce the overall application test per platform. Admin has flexibility to enable app performance monitoring on active paths only while creating app test on ADEM portal

Autonomous DEM Product Workflow

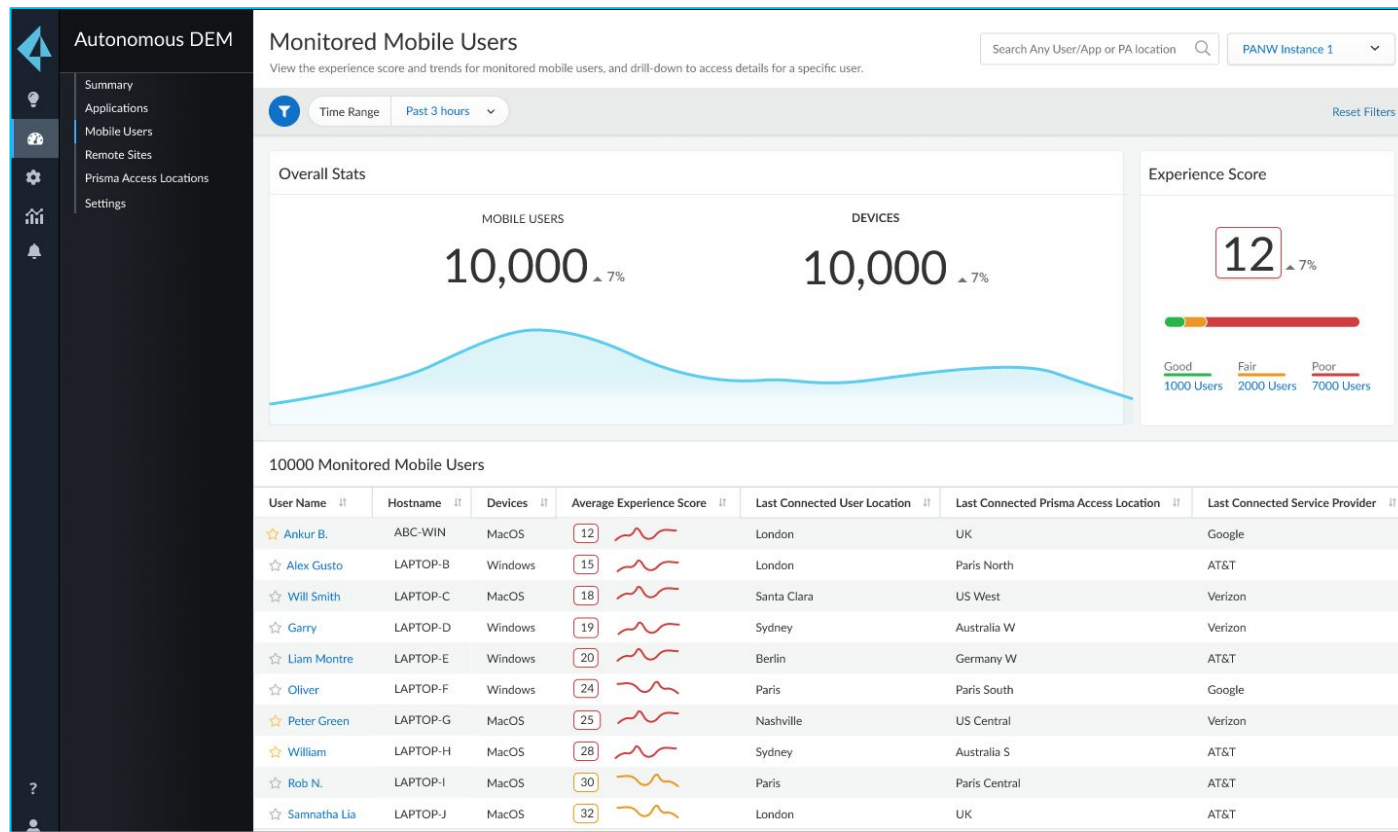
Organization Experience Dashboard for Mobile Users and Remote Sites



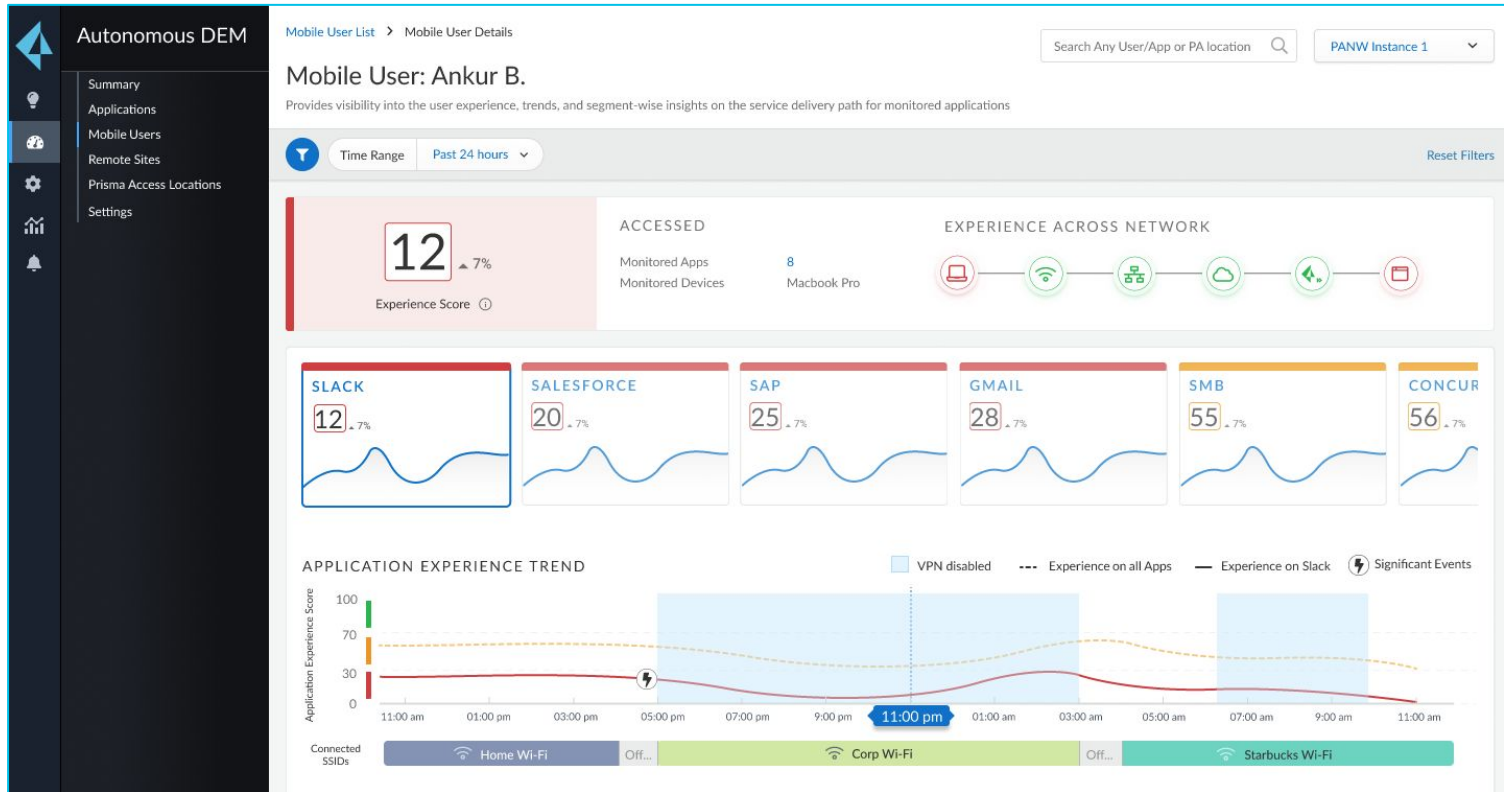
Unified Application Experience Dashboard for Mobile User and Remote Sites



Experience Dashboard for all Monitored Mobile Users



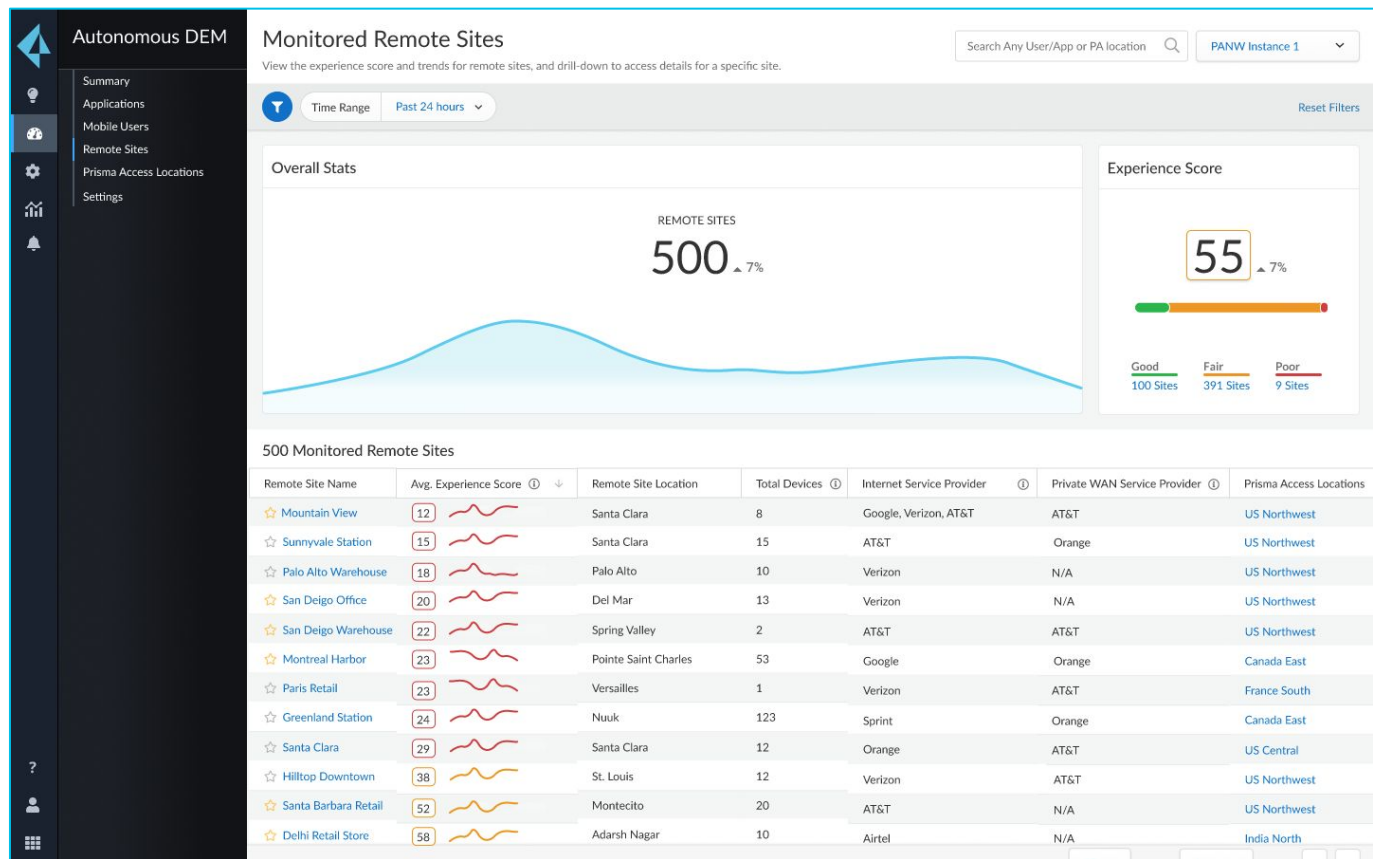
Mobile User Experience Dashboard with Per Application Experience Visibility



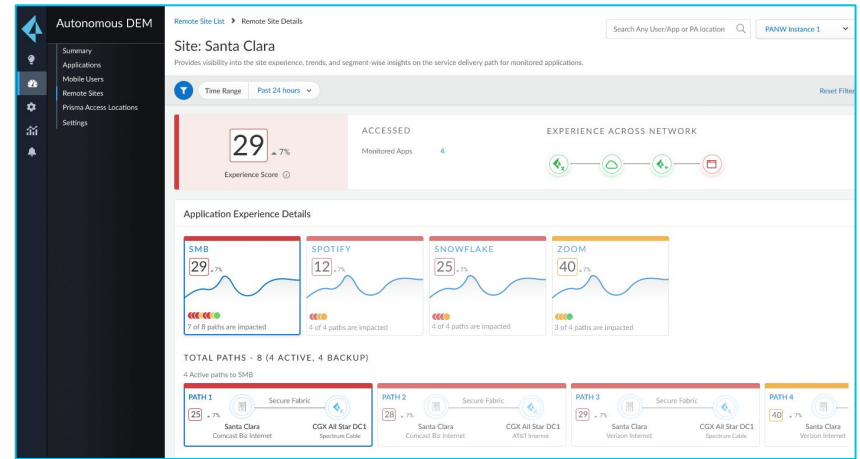
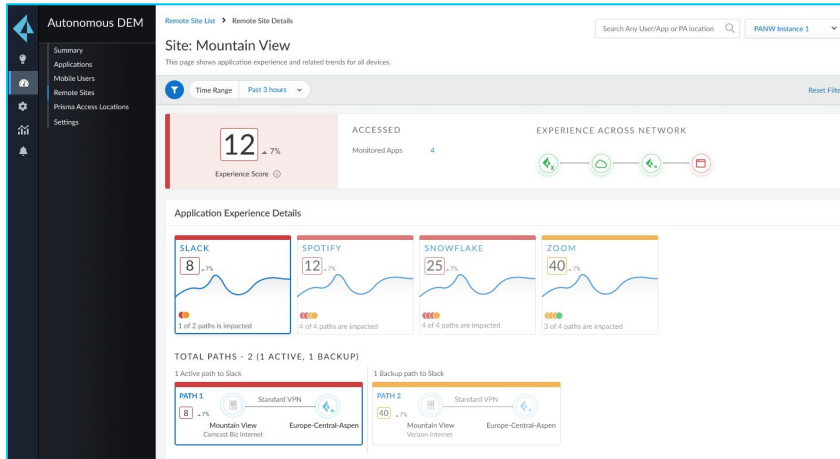
Mobile User to Application Path Visualization (Hop-By-Hop Node Experience Visibility)

The screenshot displays the Palo Alto Networks Autonomous DEM interface. On the left is a dark sidebar with navigation icons and the text "Autonomous DEM". The main content area is titled "Mobile User: Ankur B." and includes a search bar and a dropdown for "PANW Instance 1". Below the title, there's a "Time Range" selector set to "Past 24 hours" and a "Reset Filters" button. The main visualization is titled "PATH TO SLACK AT 11:00 AM 16 APR 2021" with a sub-note "Slack traffic is sent over Internet". It features a horizontal flow diagram with five nodes: "DEVICE" (laptop icon), "WIFI" (Wi-Fi icon), "LOCAL NETWORK" (server rack icon), "INTERNET" (cloud icon), and "SLACK" (document icon). Below this diagram are controls for "Show ISP Hops" (8 hops First mile, 27 total hops, 0 hops Last mile), "Group By" (IP Address), "Filter" (IP, Country, Network Name), and "Show Hop Performance" (Highlight None). A "Reset Path Topology" button is also present. At the bottom, a detailed path visualization shows a sequence of nodes from the device to Slack, with a "3 more" button indicating intermediate hops. A legend identifies node types: Discovered Node (green), Unknown Node (grey), and Destination Network Node (blue).

Experience Dashboard for all Monitored Remote Sites



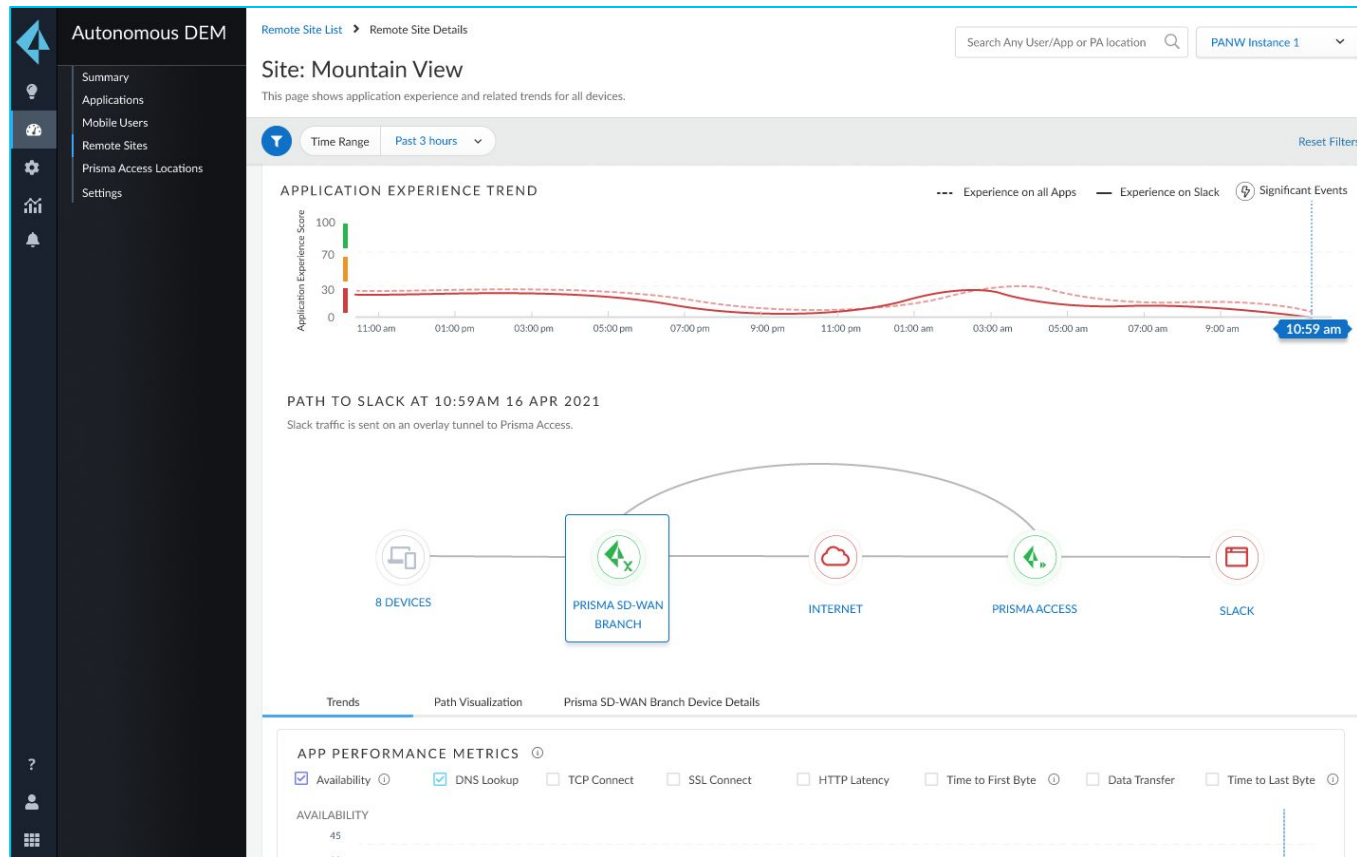
Remote Site Experience Dashboard with Per Application Per Path Experience Visibility



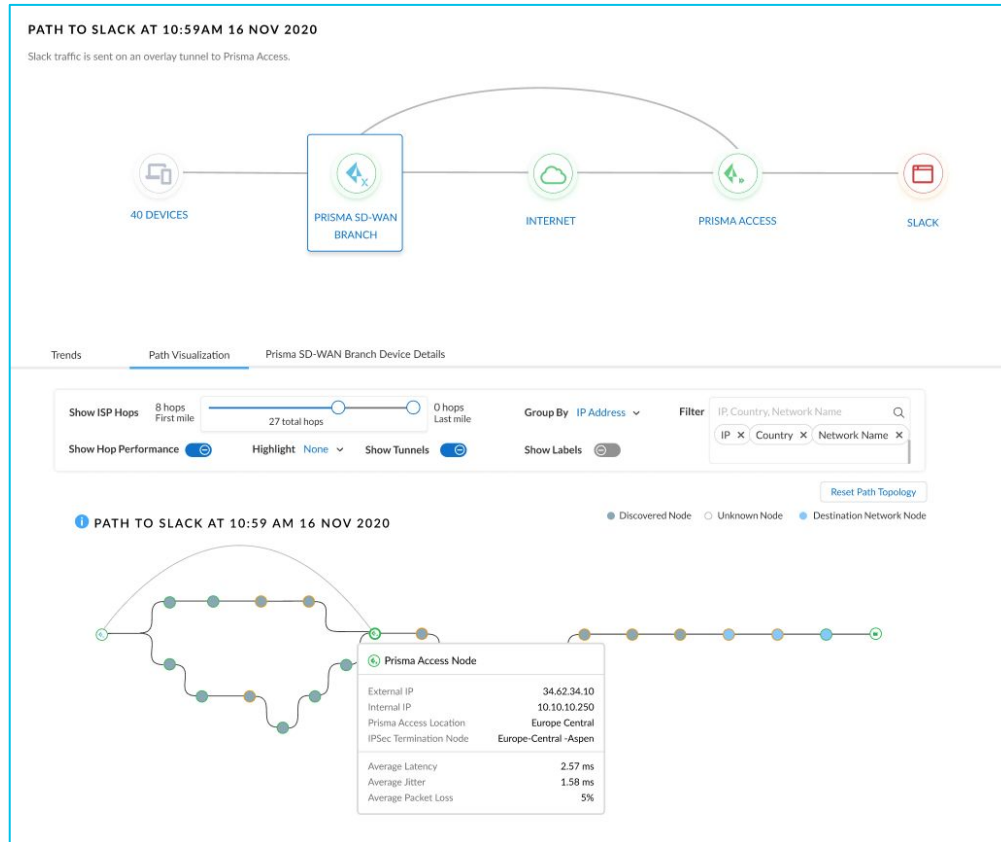
Provide performance experience for all WAN paths (Active and Backup)

Per application Per Path Connectivity and Experience visibility

Remote Site Experience Dashboard - Per App Path Topology



Remote Site to Application Path Visualization (Hop-By-Hop Node Experience Visibility)

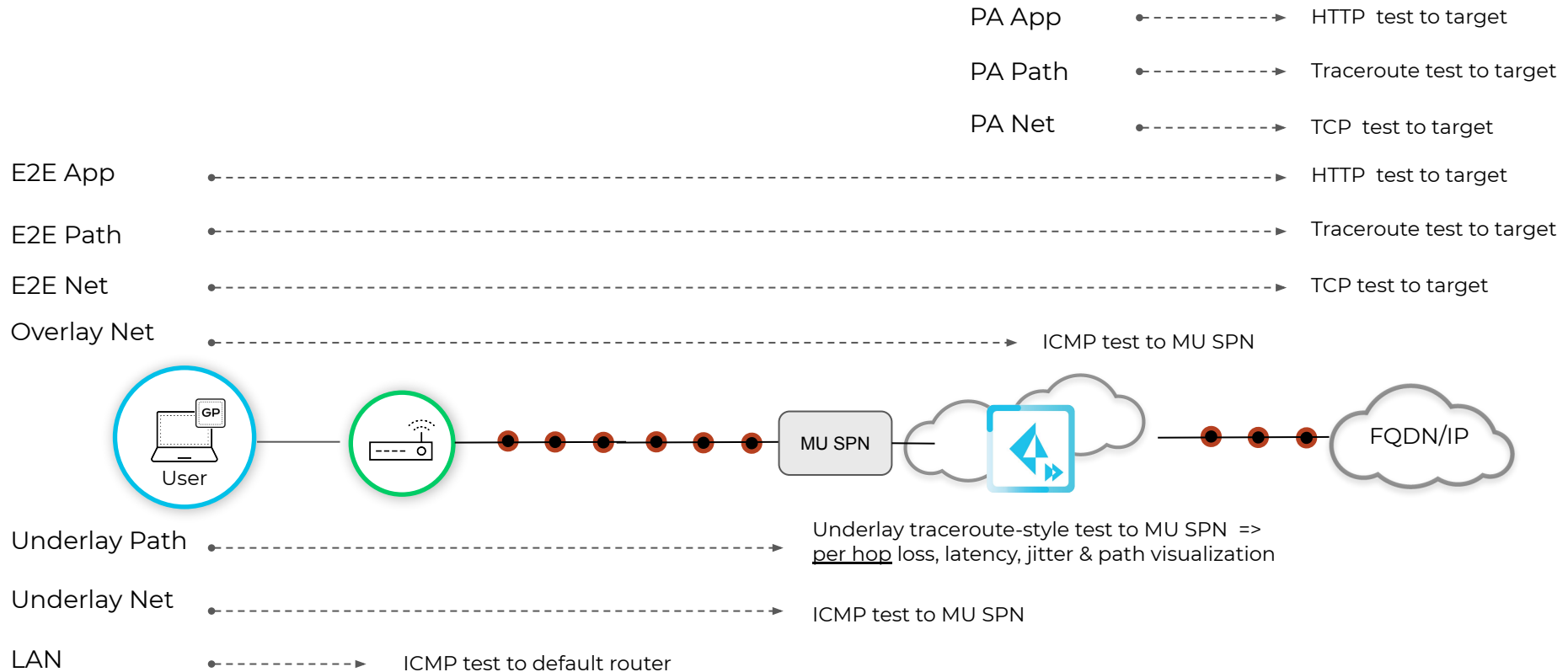


Thank you

BackUP Slides

Autonomous DEM for Mobile Users - Segment Wise Test Details

Segment-Wise: Synthetics Cover Multiple Segments & Layers



Autonomous DEM Synthetic Tests

Endpoint Agents

- Local Network/Router - Delay, Jitter, Packet Loss
- VPN Overlay - Delay, Jitter, Packet Loss
- VPN Underlay - Delay, Jitter, Packet Loss and Hop-by-hop
- User-defined tests
 - End-to-end Delay, Jitter and Packet Loss
 - End-to-end hop-by-hop
 - End-to-end web

Network Probes

- User-defined tests
 - PA-to-service Delay, Jitter and Packet Loss
 - PA-to-service hop-by-hop
 - PA-to-service web

Network Metrics

- **Availability** is calculated by measuring the duration each sample period had 3 or more of consecutive loss events.
- **Delay** is the time taken, in msec, to complete a round trip request/response circuit.
- **Jitter** is the variation in delay, in msec, and is calculated by taking the median absolute deviation (MAD) of the delays for each sample period.
- **Loss** is the number of packets lost, per sample period represented as a percentage.

Web HTTP/S Metrics

- **Availability** is the number of successful transactions expressed as a percentage. A transaction is considered successful if no connection errors were encountered and the HTTP return code started with a 2 or a 3 (e.g. 200, 302, etc).
- **DNS Lookup** is the time taken, in msec, to complete the DNS resolution of the target URL's domain.
- **TCP Connect** is the time taken, in msec, to complete the TCP 3-way handshake/connection establishment.
- **SSL Connect** is the time taken, in msec, to complete the SSL handshake and establish a secure connection between the client and the server.

Web HTTP/S Metrics (cont'd)

- **Time To First Byte** is the time taken, in msec, from the start of the DNS lookup to receive the 1st byte of data from the server. It is effectively the same as DNS Lookup + TCP Handshake + SSL Handshake + Waiting.
- **Data Transfer** is the time taken, in msec, to receive all of the data from the server.
- **Time To Last Byte** is the total time, in msec, of the entire transaction. It is effectively the same as DNS Lookup + TCP Connect + SSL Connect + HTTP Latency + Data Transfer.
- **HTTP Latency** is the time taken, in msec, for the server to process the HTTP request and send the first part of the response back.

Autonomous DEM Synthetic Tests

Endpoint Agents

Local Network/Router - Delay, jitter, loss

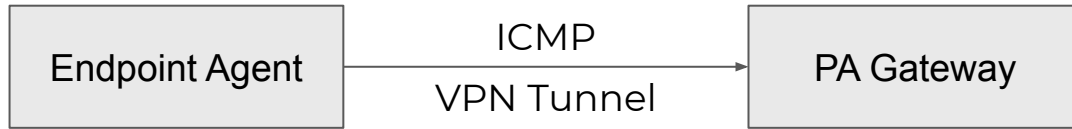


- Uses ICMP to “ping” the local network router/firewall once every 10 secs.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.

Autonomous DEM Synthetic Tests

Endpoint Agents

VPN Overlay - Delay, jitter, loss

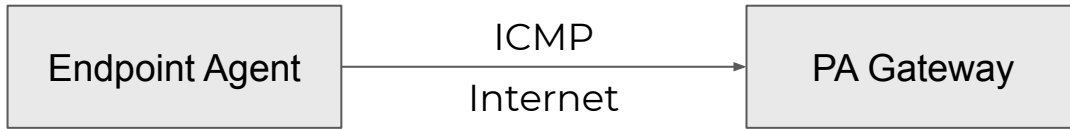


- Uses ICMP to “ping” the remote end of the VPN tunnel (**the private tunnel IP**) once every 10 secs.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.

Autonomous DEM Synthetic Tests

Endpoint Agents

VPN Underlay - Delay, jitter, loss

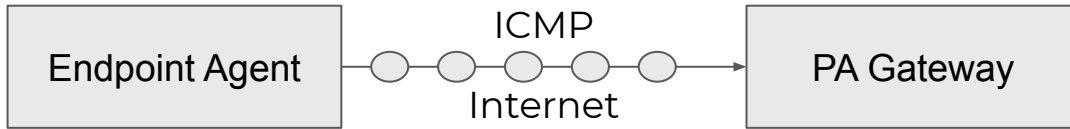


- Uses ICMP to “ping” the PA **gateway public IP** once every 10 secs.
- Traffic to the gateway’s public IP is always routed outside the tunnel.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.

Autonomous DEM Synthetic Tests

Endpoint Agents

VPN Underlay - Hop-by-hop

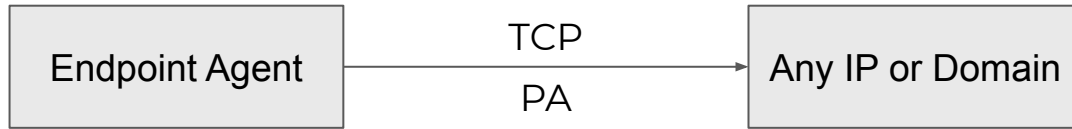


- Uses ICMP to “ping” the PA **gateway public IP** with incrementing TTLs to discover the hops along the path.
- The path trace is run once every 5 minutes.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss for each discovered hop in the path.

Autonomous DEM Synthetic Tests

Endpoint Agents

User defined test - End-to-end delay, jitter, loss

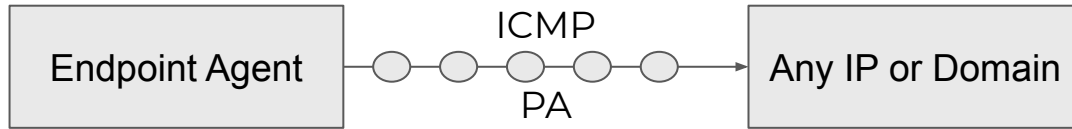


- Uses TCP to “ping” any user-defined IP/domain as part of a configured “test” once every 10 secs.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.

Autonomous DEM Synthetic Tests

Endpoint Agents

User defined test - End-to-end hop-by-hop

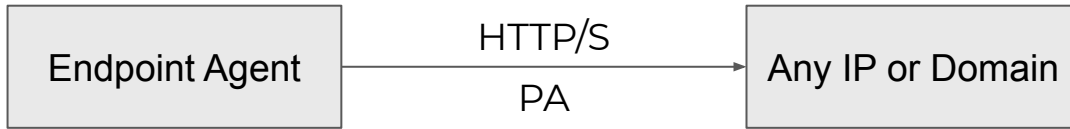


- Uses ICMP to “ping” any user-defined IP/domain IP with incrementing TTLs to discover the hops along the path.
- The path trace is run once every 5 minutes.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss for each discovered hop in the path.

Autonomous DEM Synthetic Tests

Endpoint Agents

User defined test - End-to-end web

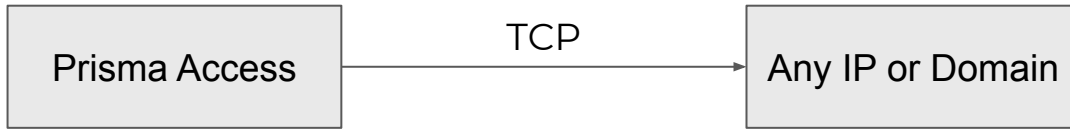


- Uses HTTP/S to “GET” any user-defined IP/domain as part of a configured “test” once every 5 mins.
- Results sent to DEM portal every 5 mins, and contains HTTP/S timing metrics.

Autonomous DEM Synthetic Tests

Network Probes

User defined test - PA-to-service delay, jitter, loss

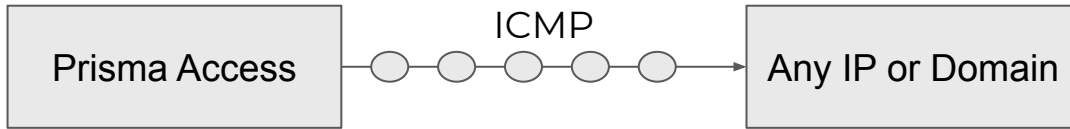


- Uses ICMP to “ping” any user-defined IP/domain as part of a configured “test” once every 10 secs.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.

Autonomous DEM Synthetic Tests

Network Probes

User defined test - PA-to-service hop-by-hop



- Uses ICMP to “ping” any user-defined IP/domain IP with incrementing TTLs to discover the hops along the path.
- The path trace is run once every 5 minutes.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss for each discovered hop in the path.

Autonomous DEM Synthetic Tests

Network Probes

User defined test - PA-to-service web



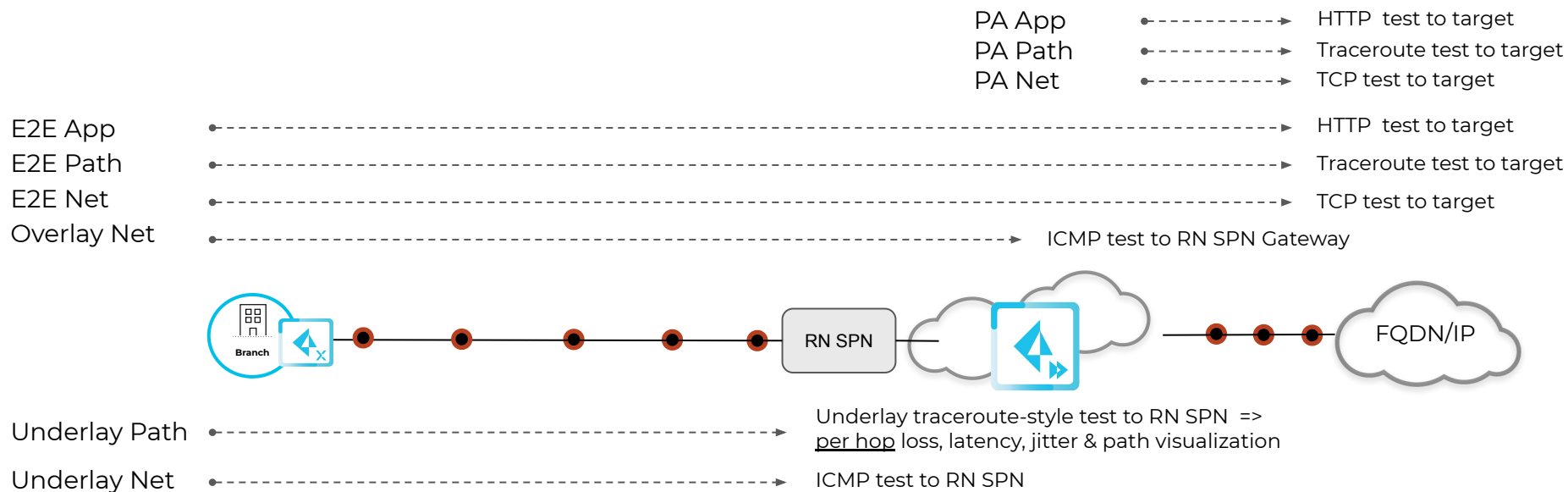
- Uses HTTP/S to “GET” any user-defined IP/domain as part of a configured “test” once every 5 mins.
- Results sent to DEM portal every 5 mins, and contains HTTP/S timing metrics.

Autonomous DEM Split Tunneling for Mobile Users

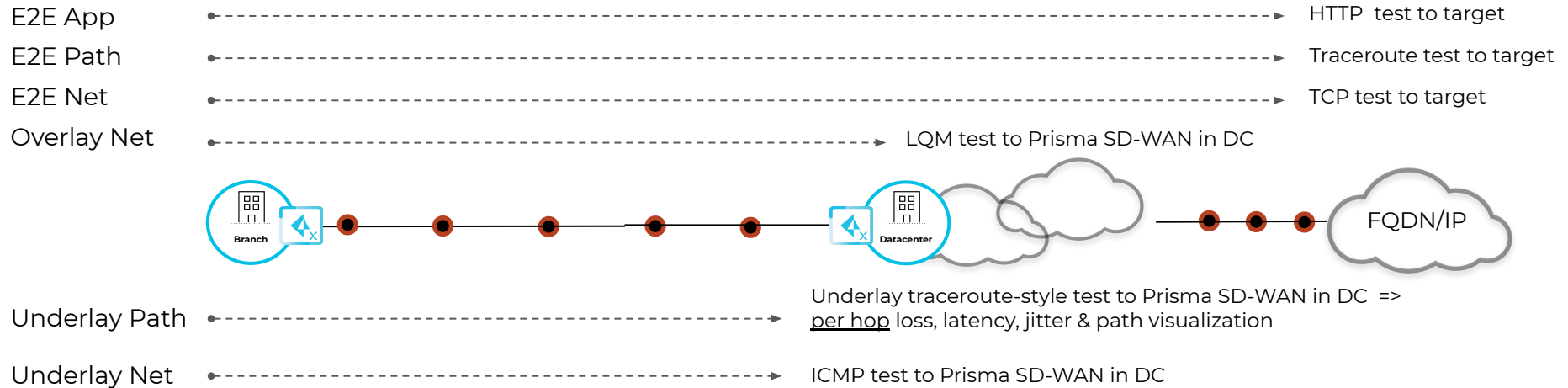
	Network Performance	Application Performance	Network Path Visibility
Traffic Destined to Prisma Access	TCP	HTTP/HTTPs	ICMP
Split Tunnel DIA traffic	TCP	HTTP/HTTPs	Not Supported

Autonomous DEM for Remote Networks - Segment wise Test Details

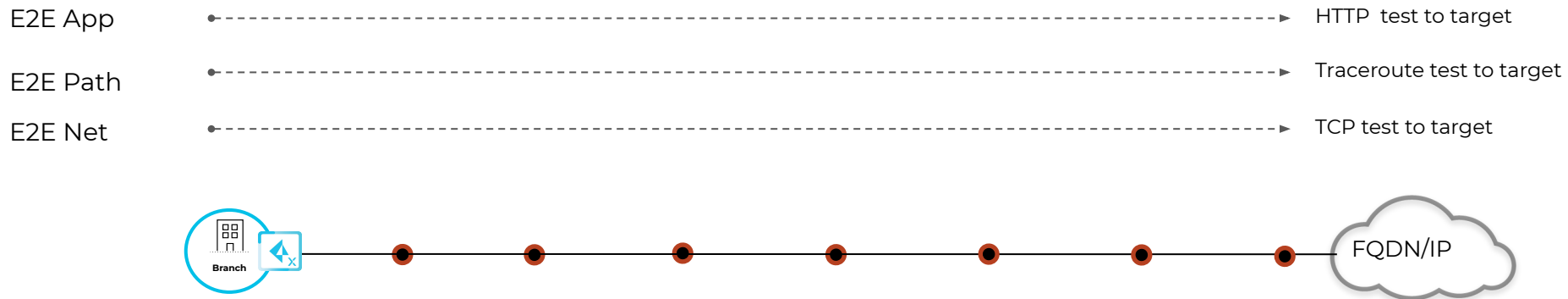
Synthetics to Cover Multiple Segments and Layers - Prisma Access Path



Synthetics to Cover Multiple Segments and Layers - Secure Fabric Path



Synthetics to Cover Multiple Segments and Layers - Direct Access Path



Autonomous DEM Synthetic Tests

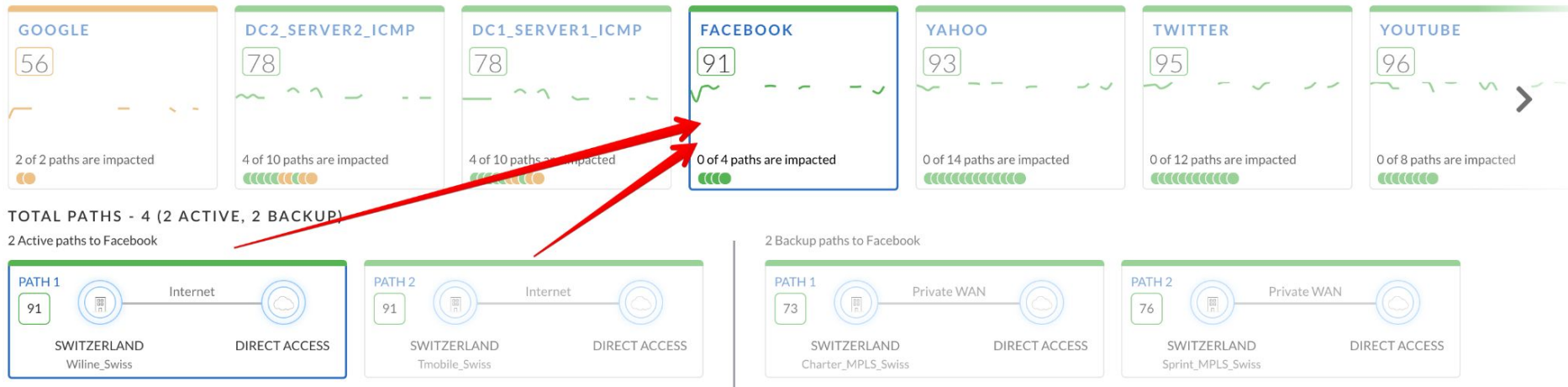
Prisma SD-WAN ADEM Agents

- VPN Overlay - Delay, Jitter, Packet Loss
 - (except Secure Fabric overlay, that uses LQM)
- VPN Underlay - Delay, Jitter, Packet Loss and Hop-by-hop
- User-defined tests
 - End-to-end Delay, Jitter and Packet Loss
 - End-to-end hop-by-hop
 - End-to-end web

* All tests are run over all possible paths.

Autonomous DEM - Prisma SD-WAN Paths - Active / Backup

- Only “**Active**” paths are used when calculated rollup/aggregate experience scores.
- The same path could be active or backup for different applications, based on policy.



Network Metrics

- **Availability** is calculated by measuring the duration each sample period had 3 or more of consecutive loss events.
- **Delay** is the time taken, in msec, to complete a round trip request/response circuit.
- **Jitter** is the variation in delay, in msec, and is calculated by taking the median absolute deviation (MAD) of the delays for each sample period.
- **Loss** is the number of packets lost, per sample period represented as a percentage.

Web HTTP/S Metrics

- **Availability** is the number of successful transactions expressed as a percentage. A transaction is considered successful if no connection errors were encountered and the HTTP return code started with a 2 or a 3 (e.g. 200, 302, etc).
- **DNS Lookup** is the time taken, in msec, to complete the DNS resolution of the target URL's domain.
- **TCP Connect** is the time taken, in msec, to complete the TCP 3-way handshake/connection establishment.
- **SSL Connect** is the time taken, in msec, to complete the SSL handshake and establish a secure connection between the client and the server.

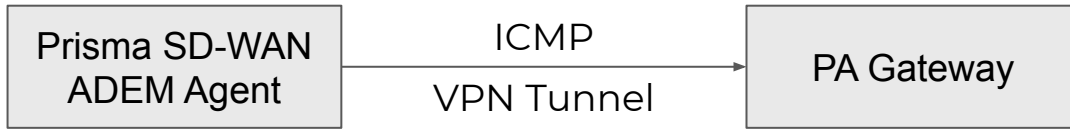
Web HTTP/S Metrics (cont'd)

- **Time To First Byte** is the time taken, in msec, from the start of the DNS lookup to receive the 1st byte of data from the server. It is effectively the same as DNS Lookup + TCP Handshake + SSL Handshake + Waiting.
- **Data Transfer** is the time taken, in msec, to receive all of the data from the server.
- **Time To Last Byte** is the total time, in msec, of the entire transaction. It is effectively the same as DNS Lookup + TCP Connect + SSL Connect + HTTP Latency + Data Transfer.
- **HTTP Latency** is the time taken, in msec, for the server to process the HTTP request and send the first part of the response back.

Autonomous DEM Synthetic Tests

Prisma SD-WAN ADEM Agent

VPN Overlay - Delay, jitter, loss



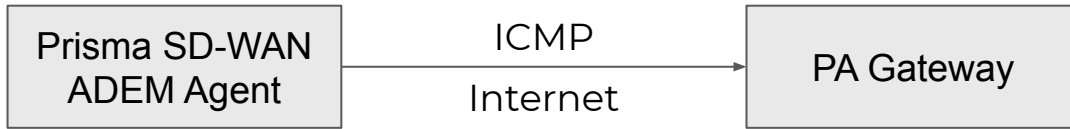
- Uses ICMP to “ping” the remote end of the VPN tunnel (**the private tunnel IP**) once every 10 secs.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.

Note: Secure Fabric VPN connections use CGX LQM in place of ADEM synthetic tests.

Autonomous DEM Synthetic Tests

Prisma SD-WAN ADEM Agent

VPN Underlay - Delay, jitter, loss

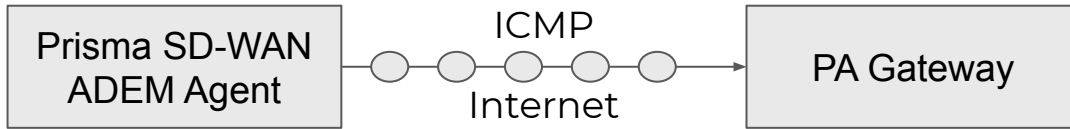


- Uses ICMP to “ping” the PA **gateway public IP** once every 10 secs.
- Traffic to the gateway’s public IP is always routed outside the tunnel.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.

Autonomous DEM Synthetic Tests

Prisma SD-WAN ADEM Agent

VPN Underlay - Hop-by-hop

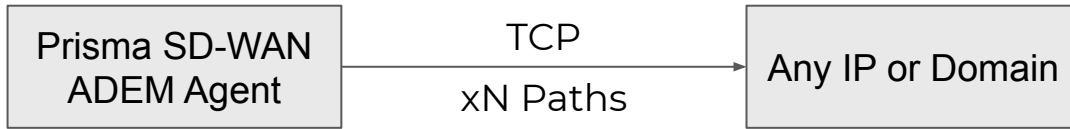


- Uses ICMP to “ping” the PA **gateway public IP** with incrementing TTLs to discover the hops along the path.
- The path trace is run once every 5 minutes.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss for each discovered hop in the path.

Autonomous DEM Synthetic Tests

Prisma SD-WAN ADEM Agent

User defined test - End-to-end delay, jitter, loss

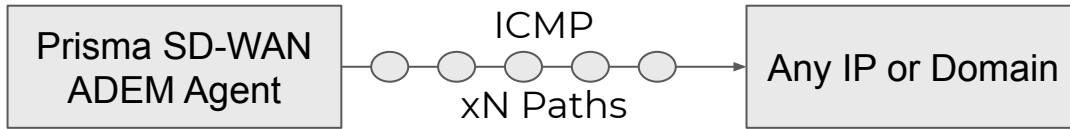


- Uses TCP to “ping” any user-defined IP/domain as part of a configured “test” once every 10 secs.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss comprising of up to 30 measurements.
- Each test is run over each path.

Autonomous DEM Synthetic Tests

Prisma SD-WAN ADEM Agent

User defined test - End-to-end hop-by-hop path trace

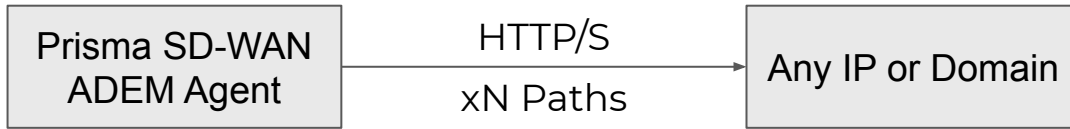


- Uses ICMP to “ping” any user-defined IP/domain IP with incrementing TTLs to discover the hops along the path.
- Results sent to DEM portal every 5 mins, contains average delay, jitter and loss for each discovered hop in the path.
- One test is run per 5 mins, for each path.

Autonomous DEM Synthetic Tests

Prisma SD-WAN ADEM Agent

User defined test - End-to-end web



- Uses HTTP/S to “GET” any user-defined IP/domain as part of a configured “test” once every 5 mins.
- Results sent to DEM portal every 5 mins, and contains HTTP/S timing metrics.
- One test is run per 5 mins, for each path.

Thank You