

Day 2: Agenda

Prisma SD-WAN Troubleshooting Tools:

- **Device Toolkit**
- **Dashboard**
- **Activity**
- **Monitor**
- **Incidents and Alerts**
- **Flow Browser**
- **RMA**
- **Demo**

Device Toolkit

Device Toolkit Overview

- **Prisma SD-WAN configuration, operation, and troubleshooting of the system is primarily done through the SCM portal.**
- **However there may be times when troubleshooting is required to be done through command line interface.**
- **Prisma SD-WAN offers a Device Toolkit, which is a command line interface for the ION devices.**

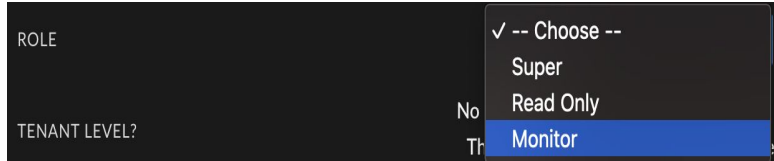
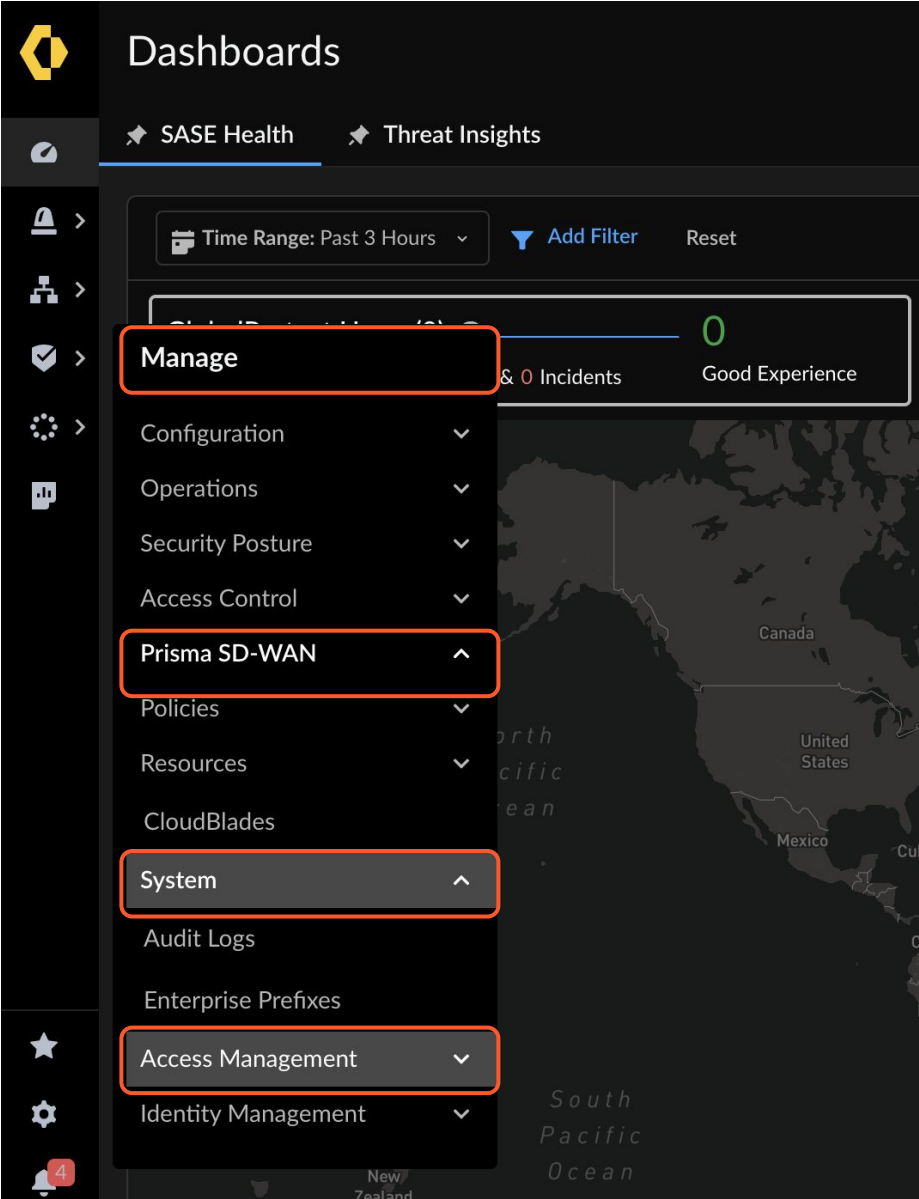
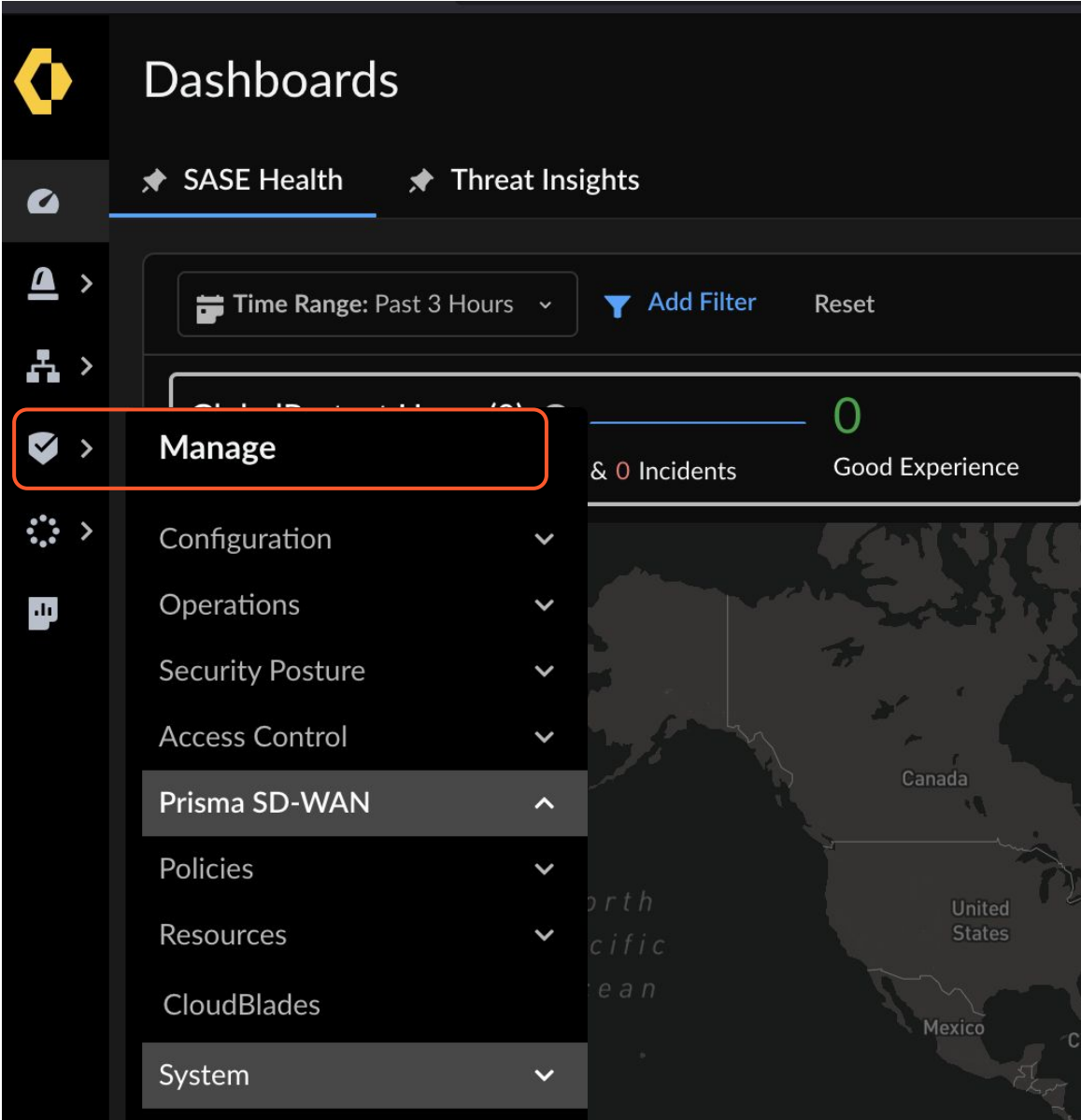
```
ion toolkit# dump overview
Software           : 6.1.10-b1
Hardware Model     : ion 3102v
Time Now           : 2025-02-03 16:25:55
Uptime             : 45m13.24s
Last Reboot Reason : declaim requested by root
Device ID          : b2af7b67-c8ba-4bb0-b125-ee48476912ab
Registration State  : UnClaimed
HA State           : active
Element State      : active
Simple State       : disabled
Controller Connection : Up [MIC]
Controller         : controller.faber.cgnx.net [52.74.47.220 13.251.109.27]
Stats Connection   : Down
Flows Connection   : Down
MIC Certificate    : valid until 2044-11-06 15:48:59 +0000 UTC
Claim Certificate   : not present

operational interfaces
controller 1      : addr 192.168.10.77/24 gw 192.168.10.1
ion toolkit# █
```

Device Toolkit Workflow

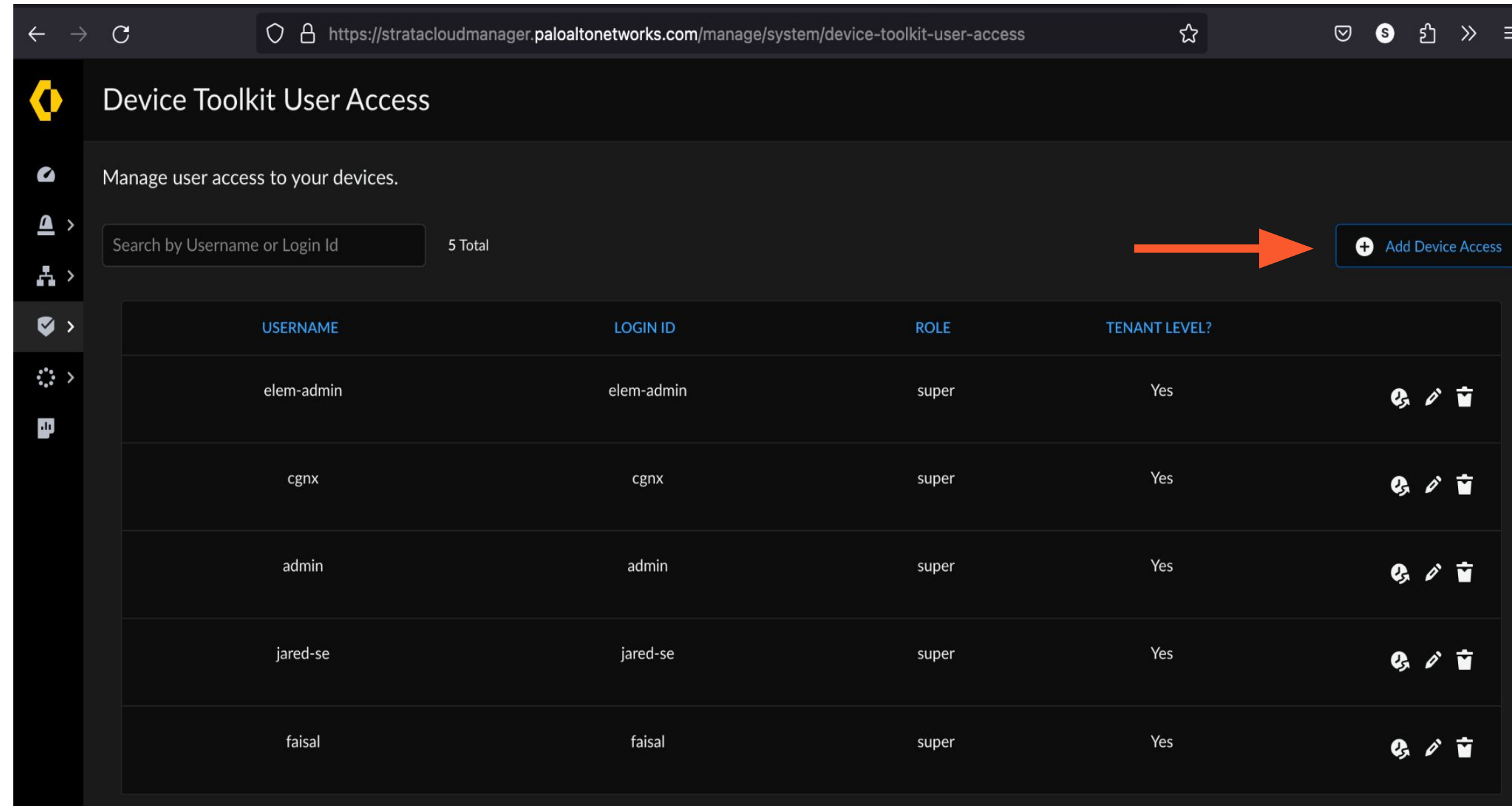
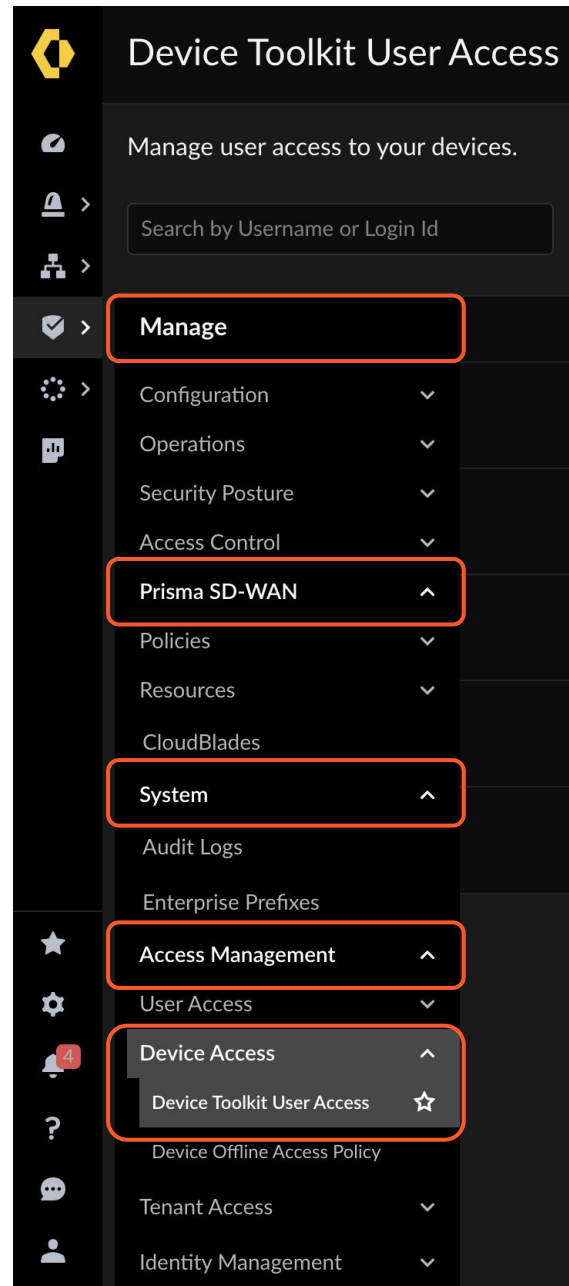
- **Prisma SD-WAN offers the ability to provide selective role-based access to the Device Toolkit.**
- **Workflow to enable the Device Toolkit User:**
 - **Add a user under the System Administration**
 - **Device Toolkit User Management**
 - **Assign User Rules**
 - **Assign Tenant or Device Level Permissions**
 - **Optionally assign permissions to specific devices within Tenant**

Configure Device Toolkit User Access



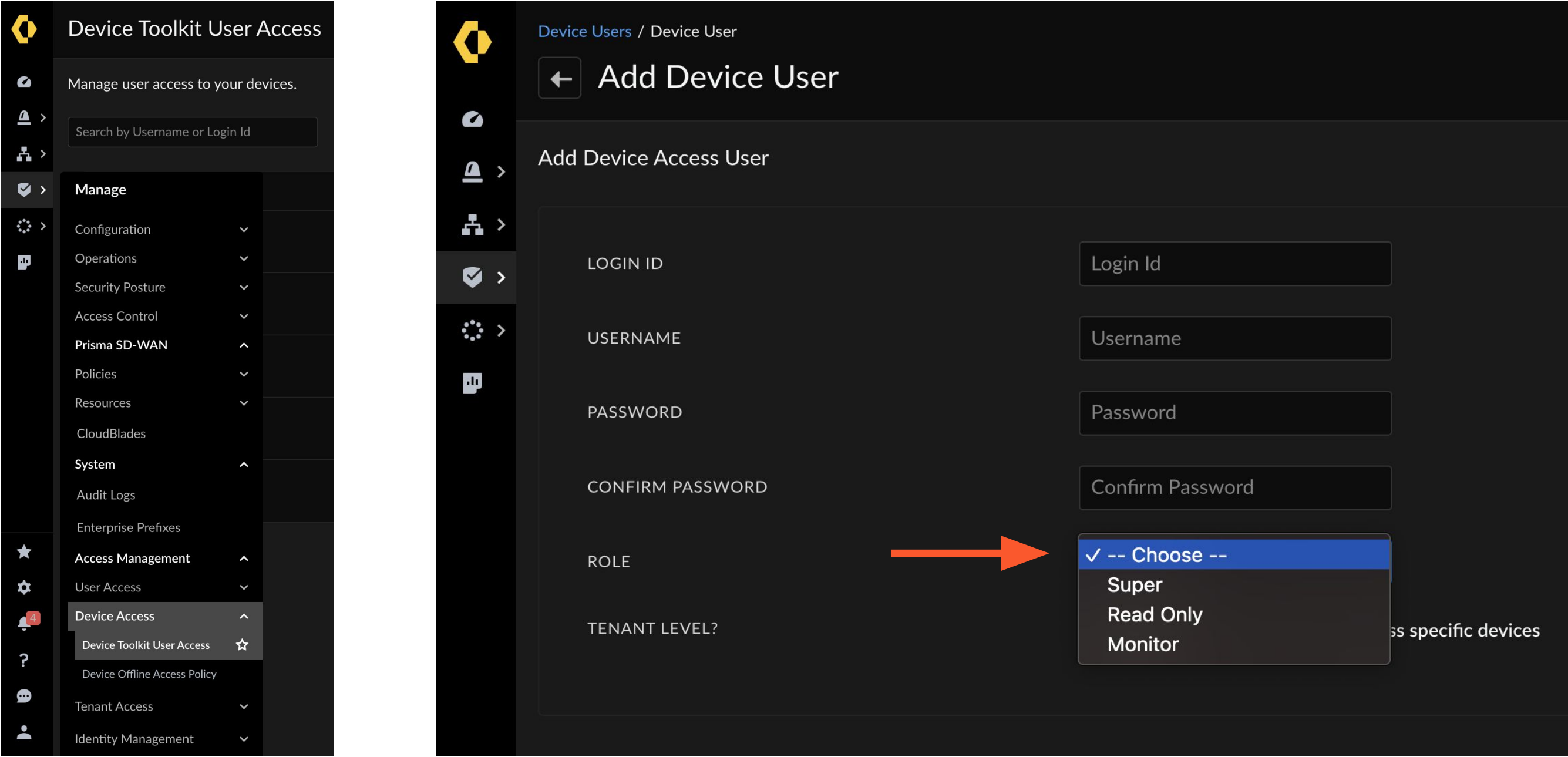
- **Begin the process by entering System Administration**

Add Device Toolkit User



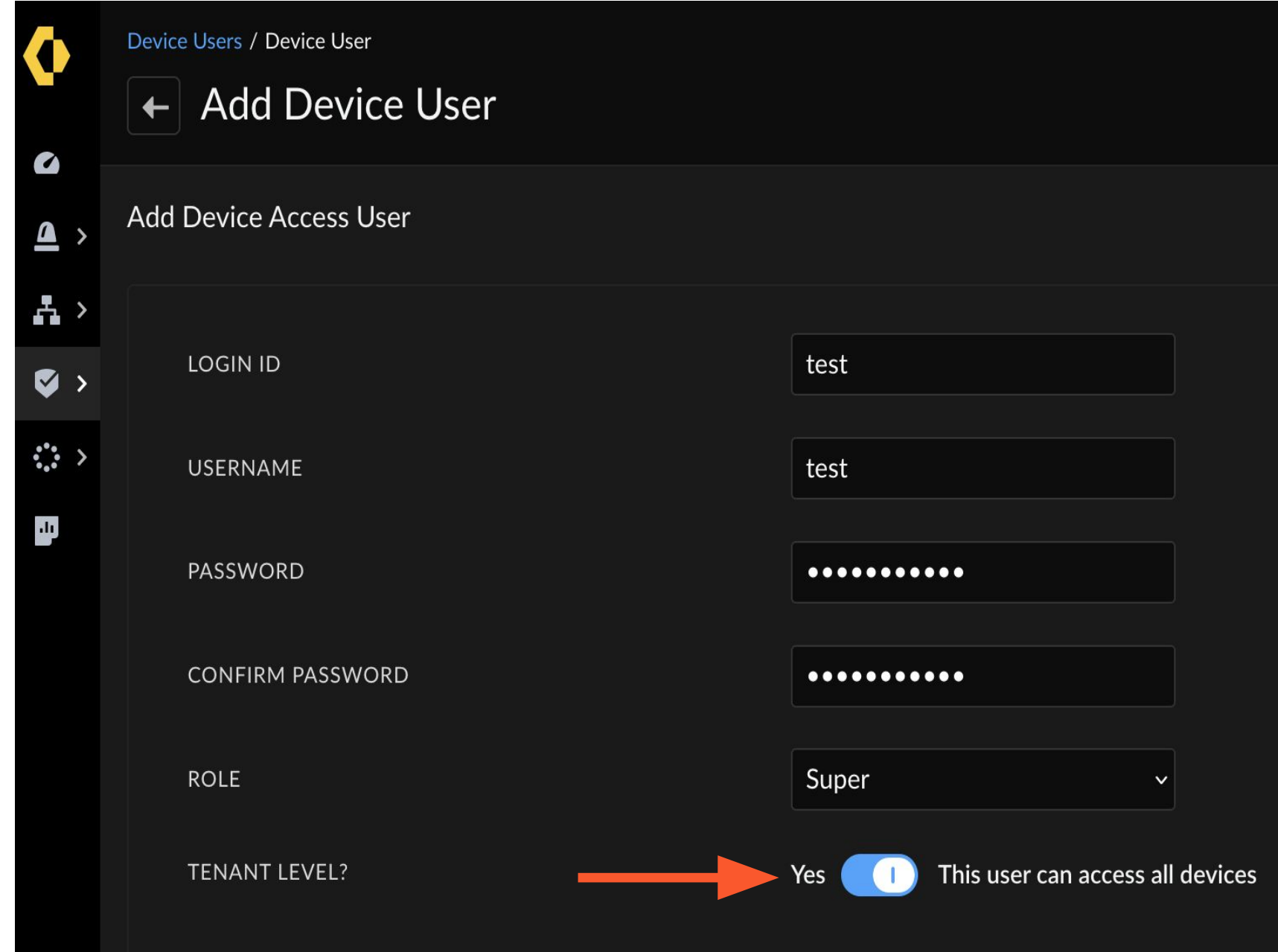
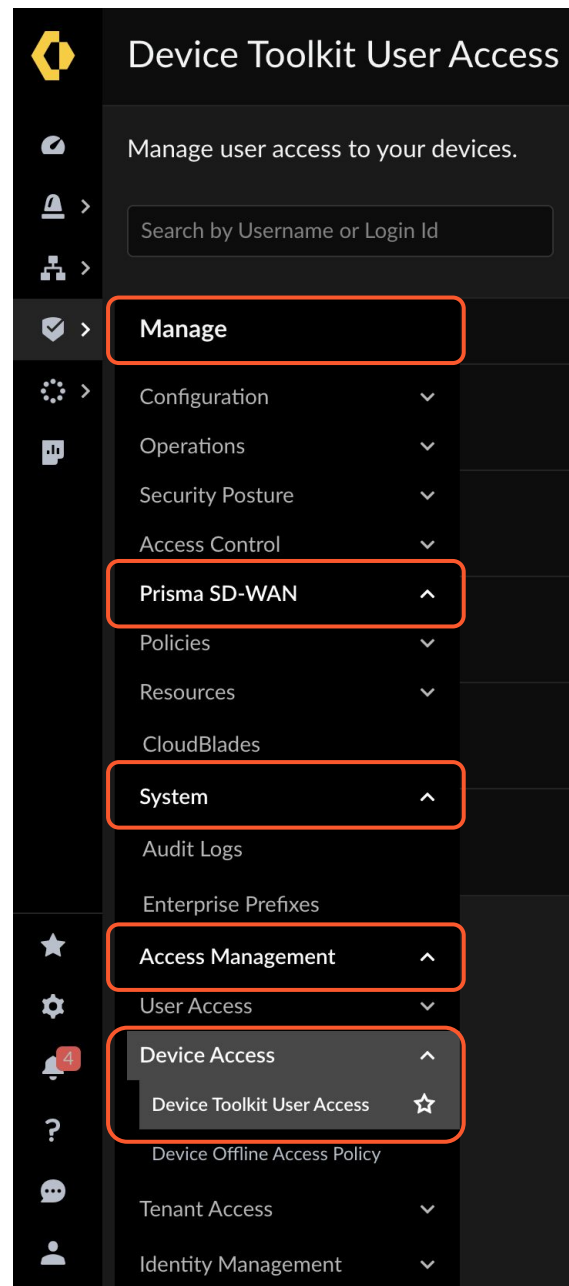
- Add a user under Device Toolkit User Management

Configure Device Toolkit User Properties



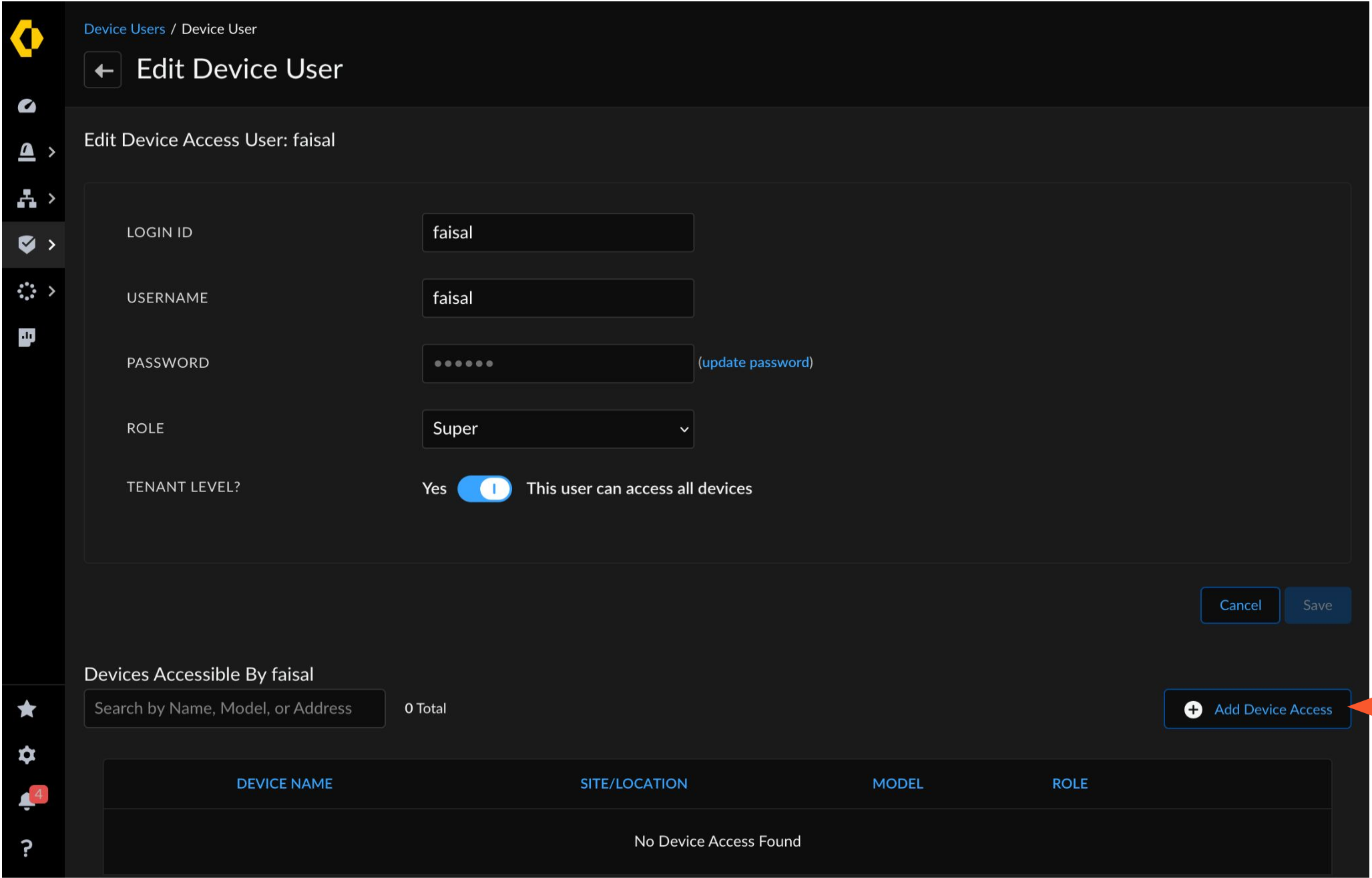
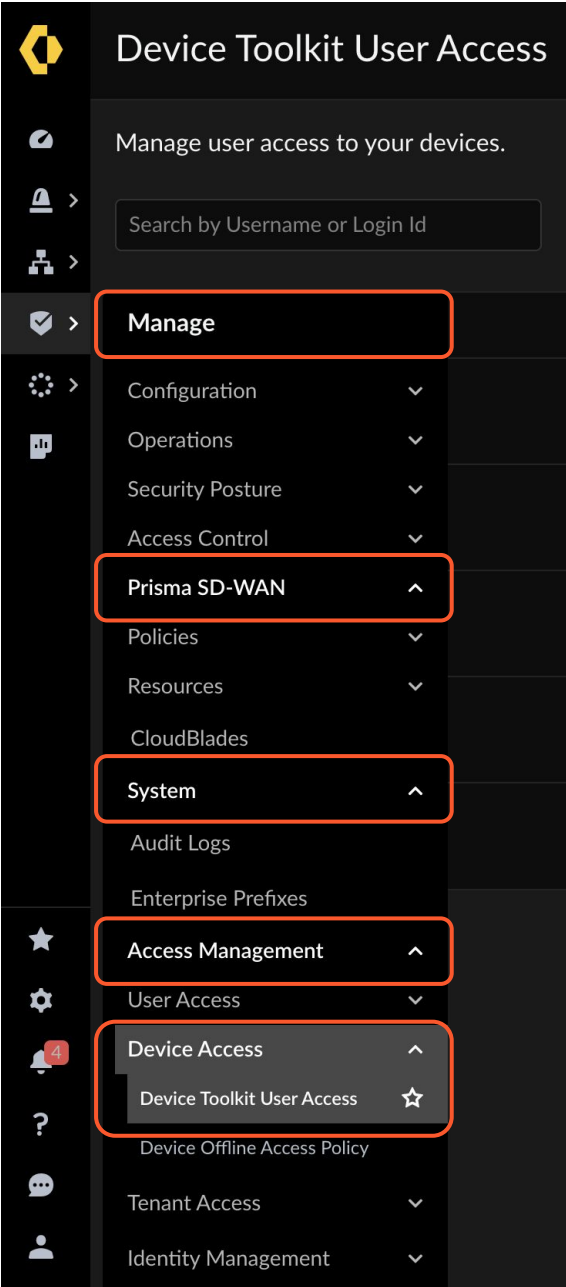
- **Configure login credentials and assign a role to the user**

Assign Tenant Level Access



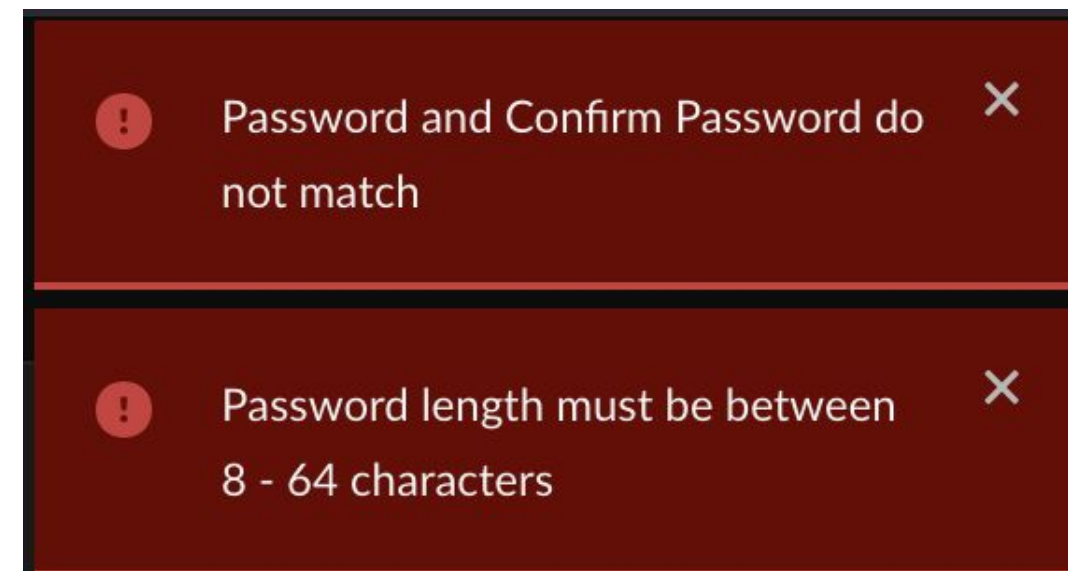
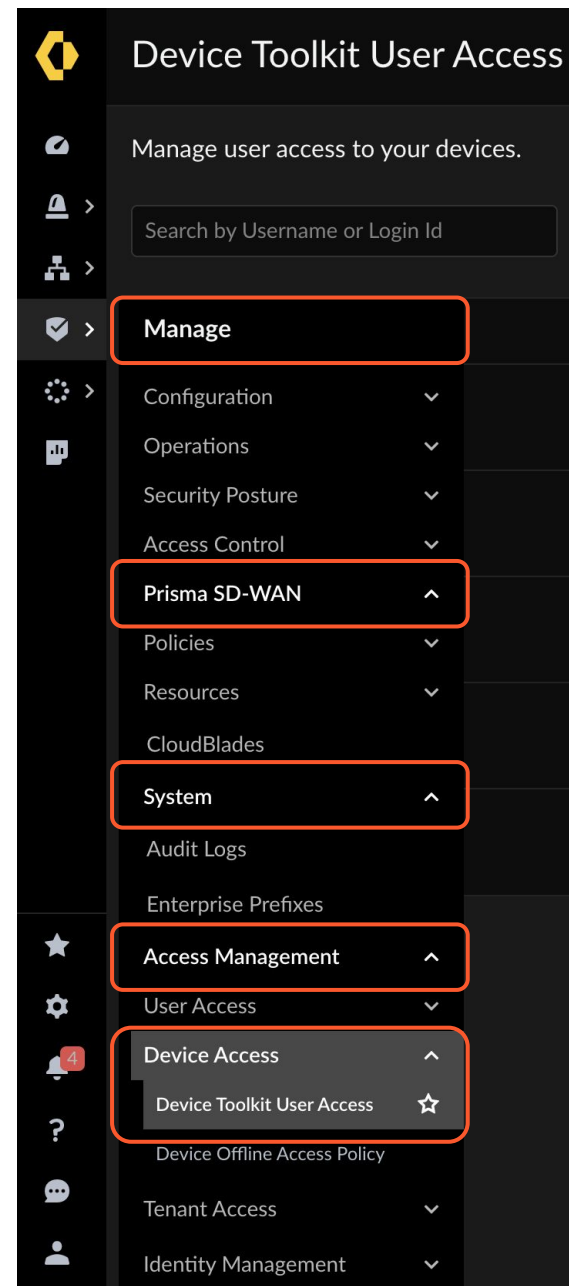
- **Tenant level device access can be enabled for a user**

Configure Individual Device (Optional)



- **Device specific access can be enabled for a user**

Common Errors



- **Password confirmation need to match and Password length need to be minimum 8 characters.**

Device Access - User Roles

Commands	User Role	Command Description
Dump	SUPER , READ ONLY , MONITOR	Displays information Example: Interface config, controller communication status
Inspect	SUPER , READ ONLY , MONITOR	Displays dynamic information Example: Routing / ARP tables
File	SUPER , READ ONLY , MONITOR	Handles log files and packet captures
Debug	SUPER , READ ONLY	Debug commands and tools Example: TCPdump, reboot
Set	SUPER , READ ONLY	Configures session parameters Example: Login timeout , prompt
Config	SUPER	Perform limited config on the device Example: Interface IP, Controller cipher

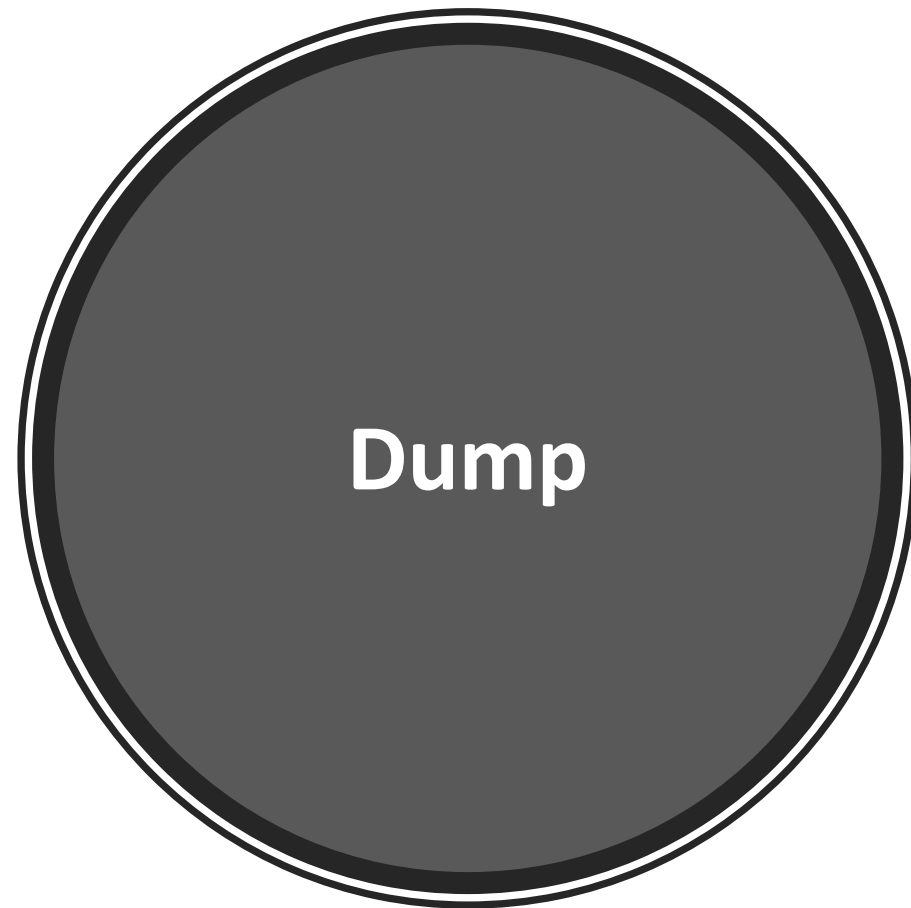
Device Toolkit Access

The screenshot shows the Device Toolkit interface for a device named SASE_BR_ION1_01. A dropdown menu is open, showing two options: 'Remote Access' (highlighted with a red arrow) and 'Download Device Snapshot'. The main interface displays the following fields:

DEVICE NAME	SASE_BR_ION1_01
DESCRIPTION	SASE_BR_ION1_01 <small>optional</small>
TAGS	 <small>optional, 4 tags max</small>
MODEL	ion 3102v
SERIAL NUMBER	8cc4b5cb-feff-4f31-aa3f-1451a24725a4

- **Launched by clicking to the right of the device name and selecting “Remote Access”**

Device Toolkit Commands



```
ION_KCP_TESTING# dump
appdef          nat          cpu          disk          sfp          vlan          spoke-ha
link-aggregation  cgnxinfra   device-management  element_to_controller  controller_to_element  app-probe      ipfix
network-policy   priority-policy  sensor       auth          banner       bfd            bypass-pair
controller       device       servicelink  smartctl-data  syslog       dnsservice    snmpagent
syslog-rtr       snmptrap     cert-operation-state  dhcpstat     dhcp-server  dhcp-relay    lqm
lldp             interface    sase         poe           security-policy  static-arp     extension    overview
hypervisor       qos-bwc      routing      waninterface  waninterface  site          software      time
troubleshoot     tpm         vpn          reachability-probe  app-l4-prefix  config        static        standingalarms
serviceendpoints ipsecprofiles  radius       dpdk          app-engine   flow          token         adem
oss-license
```

- Provides current system configuration
- Access available to all users

Device Toolkit Commands

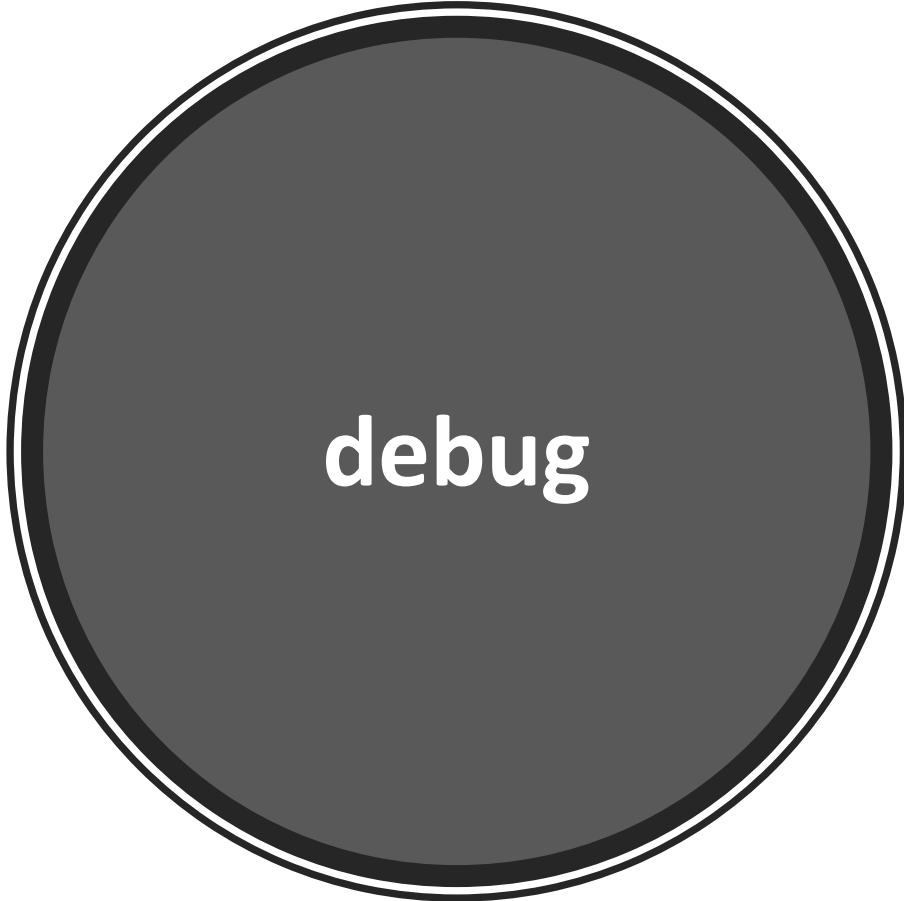


Inspect

```
ION_KCP_TESTING# inspect
cgnxinfra      system      interface   ipv6         lqm          lqm-server  certificate  flow-arp
dhcplease     wanpaths    fib         flow         connection  ipfix       network-policy policy-manager
policy-mix     priority-policy security-policy app-flow-table ip-rules     ipv6-rules  vrf         lan-network
router-connectivity dump-rtmstate memory       app-map      process      qos-bwc     app-l4-prefix user-app-session
slab-allocator routing      dpdk
```

- Shows dynamic information like routing / fib tables, APR tables, etc.
- Access available to all users

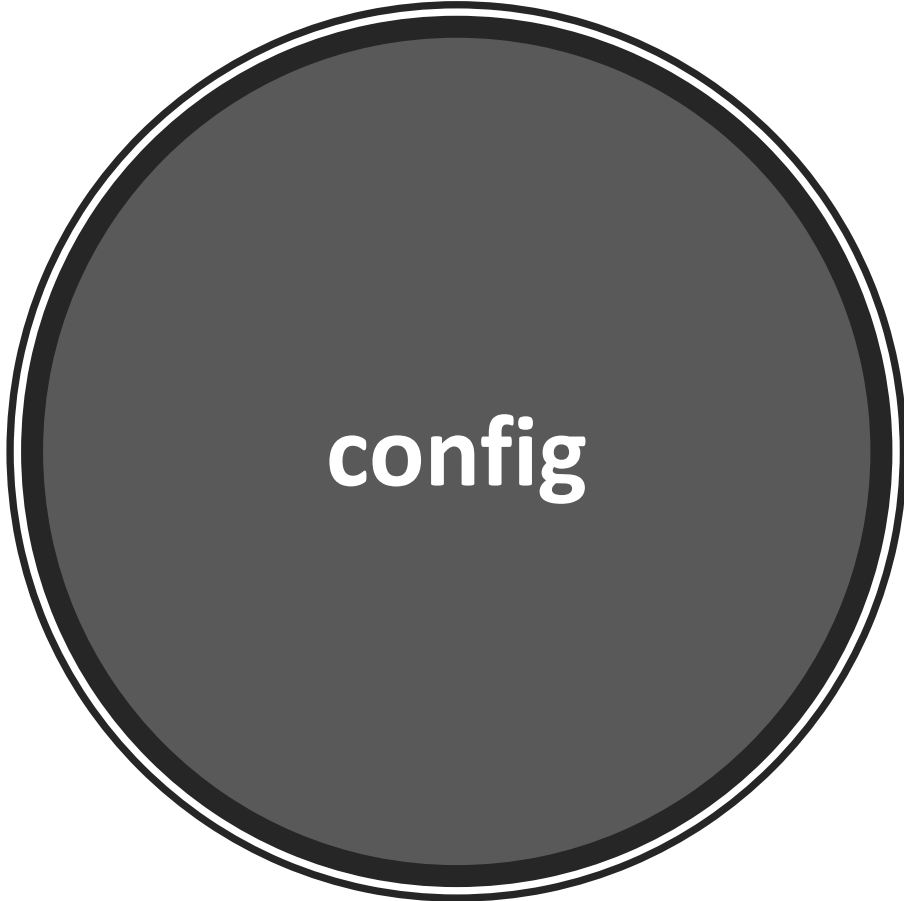
Device Toolkit Commands



```
ION_KCP_TESTING# debug |
controller time bounce reboot shutdown adem lqm ave process dnsservice bw-test flow ipfix
routing logs logging servicelink probe at-command poe
```

- Provides tools to troubleshoot a problem
- Access available to SUPER USER and READ ONLY

Device Toolkit Commands



```
ION_KCP_TESTING# config  
cellular poe interface controller extension dns static banner token
```

- To perform limited configuration on the device
- Access available to SUPER USER

Packet Capture

`tcpdump interface args="" show | save filename`

- Used to capture packets sent or received over a network interface
- Packet capture can be printed on console or saved to a file
- “args” - To filter captures, example, source or destination port

```
MAN-3K-1# tcpdump 4 args="src port 443" show
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth4, link-type EN10MB (Ethernet), capture size 262144 bytes
19:00:26.692033 IP 100.64.0.129.443 > 100.64.0.130.58594: UDP, length 64
19:00:26.709453 IP 100.64.0.72.443 > 100.64.0.71.46837: UDP, length 64
19:00:26.749066 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 577473472, win 6501, options [nop,nop,TS val 2538170576 ecr 452252], length 0
19:00:26.778220 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 112, win 6501, options [nop,nop,TS val 2538170583 ecr 452282], length 0
19:00:26.780164 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 222, win 6501, options [nop,nop,TS val 2538170583 ecr 452283], length 0
19:00:26.780218 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 331, win 6501, options [nop,nop,TS val 2538170583 ecr 452285], length 0
19:00:26.791648 IP 100.64.0.129.443 > 100.64.0.130.58594: UDP, length 64
19:00:26.795290 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 438, win 6501, options [nop,nop,TS val 2538170587 ecr 452301], length 0
19:00:26.809078 IP 100.64.0.72.443 > 100.64.0.71.46837: UDP, length 64
```

Packet Capture

```
MAN-3K-1# tcpdump 4 args="src port 443" save file=sample.pcap

Saving...
Press CTR+C to stop.
tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 262144 bytes
^C44 packets captured
55 packets received by filter
0 packets dropped by kernel
MAN-3K-1#
```

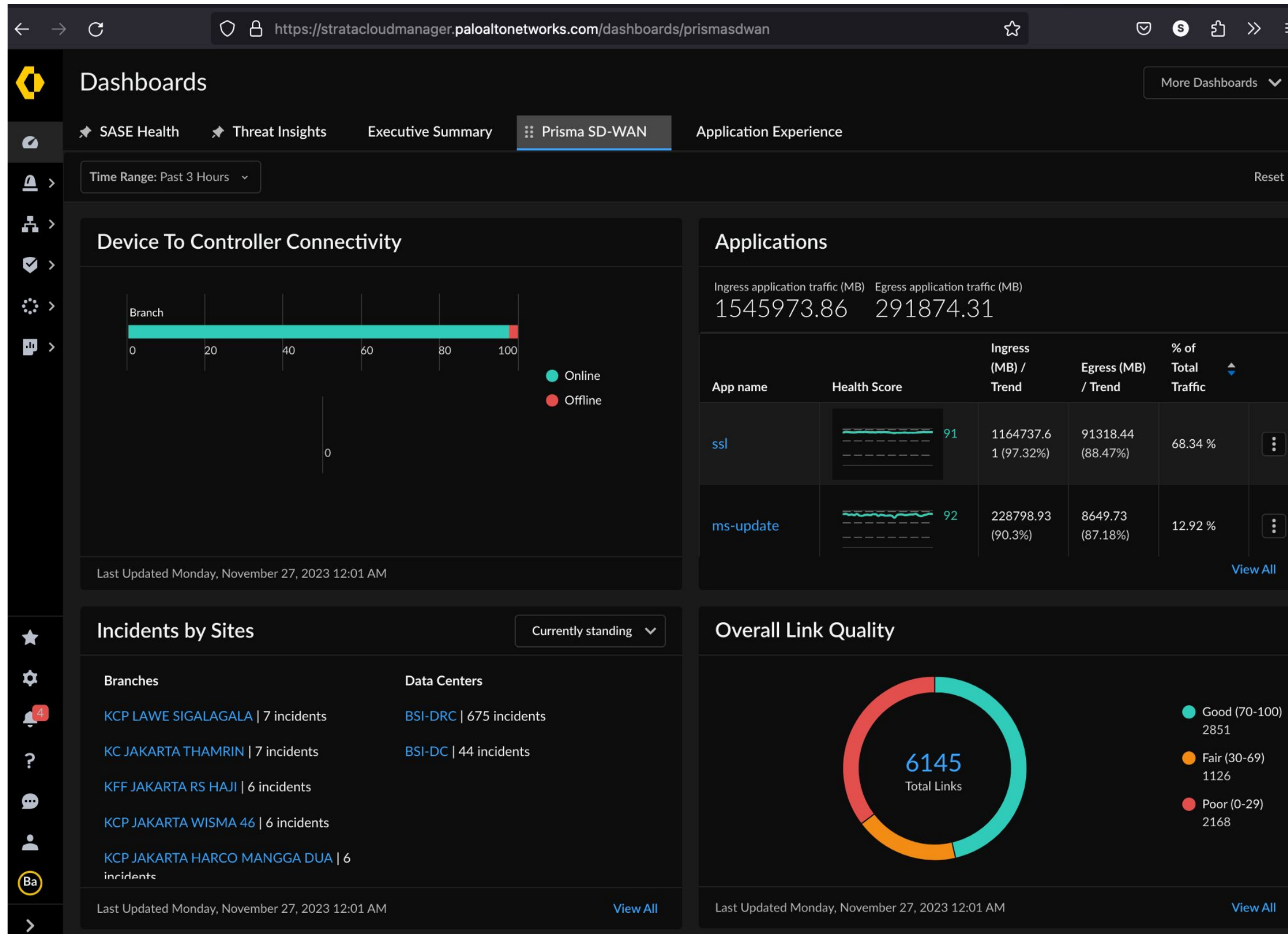
Viewing / Exporting a .pcap file

```
MAN-3K-1# file view sample.pcap
19:04:45.509087 IP 100.64.0.129.443 > 100.64.0.130.46546: UDP, length 64
19:04:45.525771 IP 100.64.0.72.443 > 100.64.0.71.51780: UDP, length 64
19:04:45.530368 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 577544303, win 6614, options [nop,nop,TS val 2538235272 ecr 711029], length 0
19:04:45.530400 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 72, win 6614, options [nop,nop,TS val 2538235272 ecr 711034], length 0
19:04:45.558762 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 116, win 6614, options [nop,nop,TS val 2538235279 ecr 711064], length 0
19:04:45.558793 IP 52.8.91.10.443 > 200.41.0.1.44715: Flags [.], ack 226, win 6614, options [nop,nop,TS val 2538235279 ecr 711064], length 0
19:04:45.608487 IP 100.64.0.129.443 > 100.64.0.130.46546: UDP, length 64
19:04:45.625558 IP 100.64.0.72.443 > 100.64.0.71.51780: UDP, length 64
19:04:45.708077 IP 100.64.0.129.443 > 100.64.0.130.46546: UDP, length 64
19:04:45.725492 IP 100.64.0.72.443 > 100.64.0.71.51780: UDP, length 64
```

```
MAN-3K-1#
MAN-3K-1# file export 4 sample.pcap scp://user@host[:port]:location
```

Dashboard

Dashboards - Prisma SD-WAN



Know the health and performance of

- Users
- branch sites
- Applications
- IT infrastructure, from a single dashboard

Dashboards - Prisma SD-WAN



Know the health and performance of

- Users
- branch sites
- Applications
- IT infrastructure, from a single dashboard

Activity

Activity

	Location
Network	Monitor > Sites Dashboard > Prisma SD-WAN Monitor > Applications
Link Quality	Monitor > Site N > Site Summary
Flows	Monitor > Branch Sites > Prisma SD-WAN Site N > Action > View Flows Monitor > Branch Sites > Prisma SD-WAN > Flows Site Summary > Apps Widget > View All Flows
Routing	Monitor > Site N > Devices > Routing
System	Monitor > ION Devices > Device Activity
Cellular	Monitor > ION Devices Monitor > Site N > Devices Monitor > Site N > Circuit

Note: Replace “N” with the site name

Network - Dashboards > Prisma SD-WAN

Bandwidth Utilization



Summary ▼



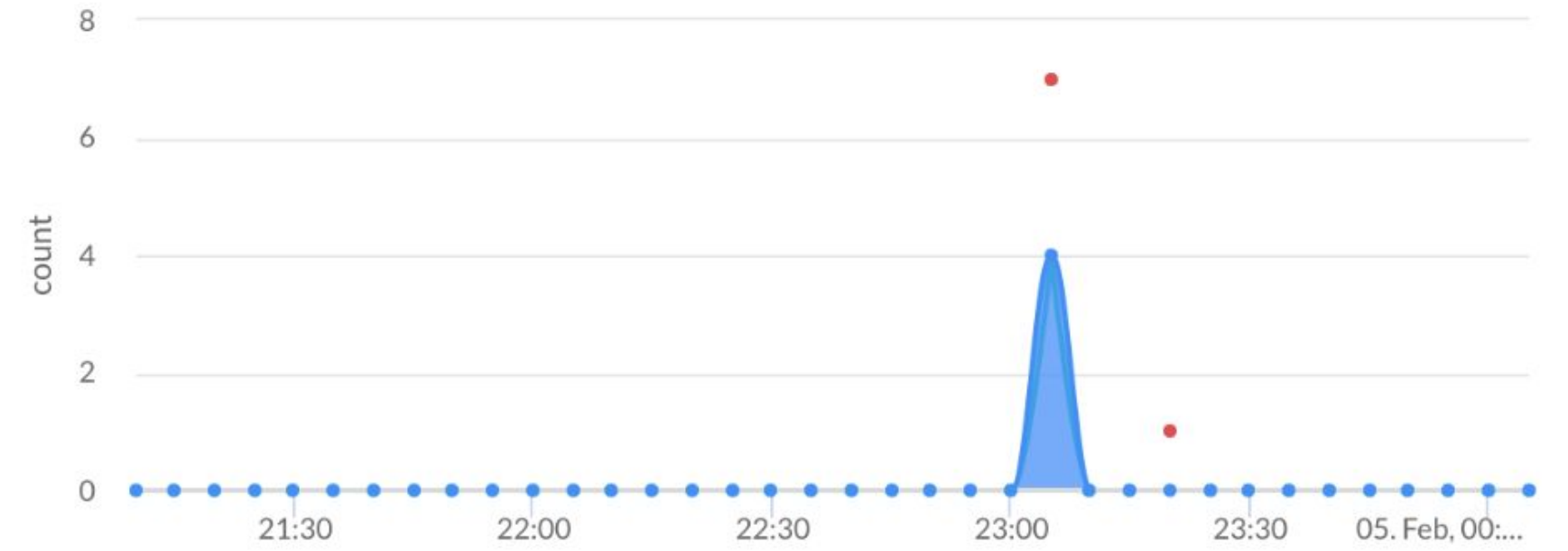
Updated a few seconds ago

[View All](#)

Transaction Stats



● TXNs Successful ● Init Failure ● TXNs Failure ● Init Successful



Updated a few seconds ago

[View All](#)

Network - Activity Insights > SD-WAN Applications

SD-WAN Applications

View your SD-WAN Application details, performance analytics and insights

Overview Applications **SD-WAN Applications** Threats Users Domains Rules Regions

Sites Time Range: Past 3 Hours WAN: All Add Filter Viewing Apps by All Apps Applications (4411) Refresh Reset

Show 2 More

New Flows

Time	TCP	UDP
22:00	0	1
22:10	0	2
22:20	0	1
22:30	0	2
22:40	0	1
22:50	0	2
23:00	0	1
23:10	0	2
23:20	0	1
23:30	0	2
23:40	0	1
23:50	0	2
00:00	0	1

Bandwidth Utilization

Time	Summary
22:00	0.5
22:10	2.5
22:20	0.5
22:30	0.5
22:40	0.5
22:50	0.5
23:00	0.5
23:10	2.5
23:20	0.5
23:30	0.5
23:40	0.5
23:50	0.5
00:00	0.5

TCP Connection Stats

TCP connection and transaction stats

Time	Init Success	Init Failure	TXNs Success	TXNs Failure
22:00	0	0	0	0
23:00	4	0	0	4
00:00	0	0	0	0

Monitor > Devices > ION Devices

Devices

Device List | Device Activity

Monitor

- Applications
- Users
- Branch Sites
- Data Centers
- Network Services
- Subscription Usage
- ION Devices** ☆
- Prisma Access Locations

← SASE_LAB_1200S_C ...

Time Range: Past 24 Hours | Interfaces | Add Filter | Show Less | Cellular Activity | Refresh | Reset

Device Overview

Device Name	SASE_LAB_1200S_C
Site	Cellular_5G_Site
Description	Santa Clara, CA, United States
Description	SASE_LAB_1200S_C
Tags	--
Model	ion 1200-s-c5g-ww
Cellular Status	T-Mobile
Role	Spoke
FIPs Mode	non-fips

CPU Utilization

Updated a few seconds ago

Memory Utilization

Updated a few seconds ago

Device Temperature

Updated a few seconds ago

Disk Utilization

Updated a few seconds ago

Interface Bandwidth Utilization

Summary ▾

No Results
This chart requires the following filters: interface

Monitor

Monitor > Branch Sites

Monitor

- Applications
- Users
- Branch Sites**
- Data Centers
- Devices
- Prisma Access Locations
- Network Services
- Access Analyzer
- Subscriptions Usage

Branch Sites

Prisma Access | Prisma SD-WAN

List | Map | Activity | Past 7 Days | Link Health | Add Filter | Reset

Site Connectivity Health

Site Connectivity Health Over Time

Site Application Experience Score

35 Fair ↑ +10%

60 ↓ +30%

Legend: Good 10, Fair 20, Poor 30

Prisma SD-WAN Branch Sites (500) Search [] [] [] Add Site

Branch Site Name	Site Health	Consumed Bandwidth	Devices	Open Incidents	Site Experience Score	Actions
★ Santa Clara United States		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	✓ Branch 1 ION 3K	102	12	⋮
★ Santa Clara United States		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	✓ Branch 1 ION 3K	12	12	⋮
★ Santa Clara United States		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	✓ Branch 1 ION 3K	87	98	⋮
★ Santa Clara United States		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	✓ Branch 1 ION 3K	--	-	⋮
★ Santa Clara United States		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	✓ Branch 1 ION 3K	4	-	⋮
★ Santa Clara United States		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	✓ Branch 1 ION 3K	--	35	⋮

© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Monitor > Branch Sites > Activity

Branch Sites

Last Update 11:54:19 PM

Search

Faisal-PIC-V2

Prisma Access Prisma SD-WAN

Map List Activity Flows

Time Range: Past 3 Hours

WAN: All

Sites: SASE_BR_03

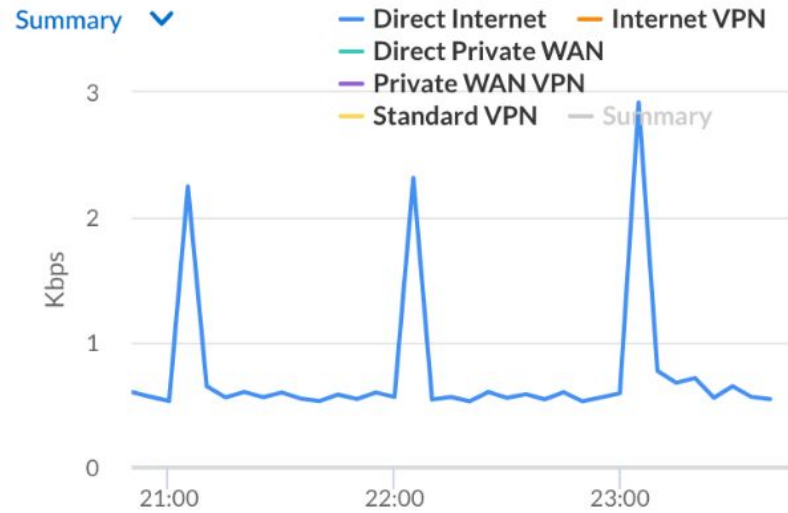
Start Date: Select Start Date

Add Filter

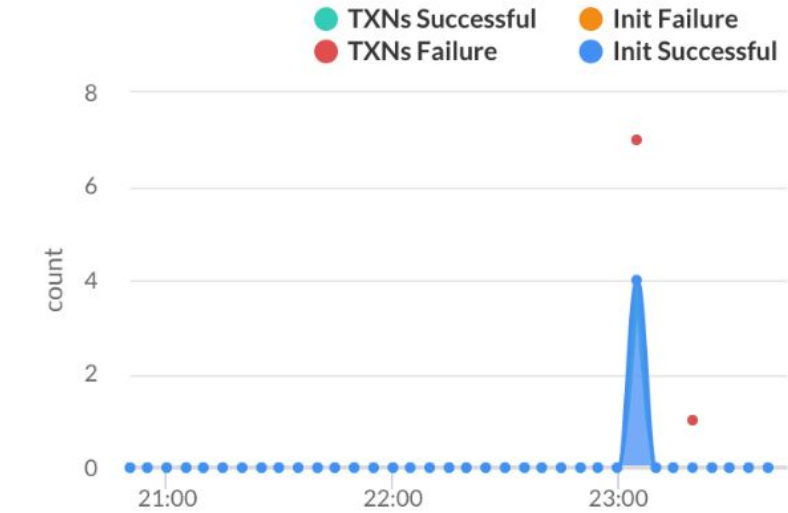
Show Less

Reset

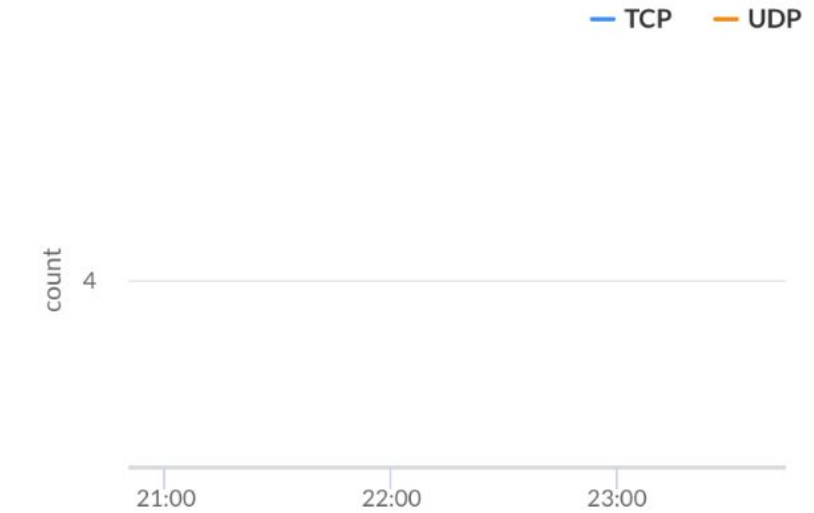
Bandwidth Utilization



Transaction Stats



New Flows



Concurrent Flows



Monitor > Data Centers

The screenshot shows the Palo Alto Networks SASE Monitor interface. The left sidebar contains navigation options: Monitor, Applications, Users, Branch Sites, Data Centers (highlighted), Devices, Prisma Access Locations, Network Services, Access Analyzer, and Subscriptions Usage. The main content area is titled 'Data Centers' and has tabs for 'Service Connections', 'Prisma SD-WAN' (selected), and 'ZTNA Connectors'. Below the tabs is a search bar and filters for 'Past 7 Days', 'Status', and 'Add Filter'. The main data table is titled 'Prisma SD-WAN Data Centers (10)' and displays the following information for each entry:

Branch Site Name	Circuit Health	Secure Fabric Health	Approaching Capacity...	Consumed Bandwidth	Open Incidents	Devices
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	102	Branch 1 ION 3K
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	12	Branch 1 ION 3K
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	87	Branch 1 ION 3K
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	--	Branch 1 ION 3K
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	4	Branch 1 ION 3K
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	--	Branch 1 ION 3K
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	10,942	Branch 1 ION 3K
Santa Clara United States	Up	Up		Ingress: 0.61 mbps (1.01%) Egress: 0.27 mbps (0.44%)	--	Branch 1 ION 3K

At the bottom right of the table, there are pagination controls: '10 Rows', 'Page 1 of 1', and navigation arrows.

Incident and Alerts

Events - Incidents and Alerts

Incidents & Alerts

Overview Incidents Alerts

Incidents & Alerts

- NGFW
- Prisma Access
- Prisma SD-WAN** ☆
- Log Viewer

Incidents & Alerts

Overview Incidents Alerts Settings

Open Customer Incidents

2264

Category	94 Critical	1453 Warning	717 Informational
Network	90	109	705
Device	4	1305	12
Cellular	0	0	0
Application	0	39	0
Policy	0	0	0
Branch HA	0	0	0
Authentication	0	0	0
User ID	0	0	0
Performance Policy	0	0	0

Incidents by Priority

- P1: 0
- P2: 94
- P3: 1455
- P4: 717
- P5: 0

Your Top Incidents

NETWORK INCIDENT	NETWORK INCIDENT	NETWORK INCIDENT	NETWORK INCIDENT
BGP Peer Down	BGP Peer Down	BGP Peer Down	Site Connectivity down
Severity: Critical	Severity: Critical	Severity: Critical	Severity: Critical
Priority: P2	Priority: P2	Priority: P2	Priority: P2
Entity: ION_KCP_LAMPRIET@ KCP LAMPRIET	Entity: ION_KCP_SIDOARJO_SEPANJANG_WONO COLO@ KCP SIDOARJO SEPANJANG WO...	Entity: ION_KCP_BATAM_CENTER@ KCP BATAM CENTER	Entity: KCP BANDUNG SETRASARI
Correlated Incident: 0	Correlated Incident: 0	Correlated Incident: 0	Correlated Incident: 0
Created: Nov 26, 2023 23:56:41 PM	Created: Nov 26, 2023 23:52:22 PM	Created: Nov 26, 2023 23:51:52 PM	Created: Nov 26, 2023 23:20:15 PM
Last Updated: Nov 26, 2023 23:56:41 PM	Last Updated: Nov 26, 2023 23:52:22 PM	Last Updated: Nov 26, 2023 23:51:52 PM	Last Updated: Nov 26, 2023 23:20:15 PM

Events - Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Prisma SD-WAN Incidents & Alerts

Overview Incidents Alerts Settings

Dashboards

Incidents & Alerts **99+**

Monitor >

Manage >

Workflows >

Reports

Search

Notifications

Help

<username>

Settings

TS TSG Name XYZ

Minimize Menu <

255

Impact	80 Major	175 Warning	175 Informational
Network	4356	47	83
Device	24	44	18
Cellular	65	31	29
Application	27	99	90
Policy	12	90	36
Branch HA Groups	23	40	5
AAA (Auth)	71	23	17

Incidents by Priority

P1	126
P2	14
P3	25
P4	43
P5	47

Your Top Incidents (1-4 of 16)

NETWORK INCIDENT

Site Connectivity Degraded

Severity: **Major**

Priority: **P1**

Correlated Alerts: 7

Status: Active

Created: 9/11/2022 1:38 PM

Last Updated: 9/11/2022 3:10 PM

NETWORK INCIDENT

Secure Fabric Link Down

Severity: **Major**

Priority: **P1**

Correlated Alerts: 7

Status: Resolved

Created: 9/11/2022 1:38 PM

Last Updated: 9/11/2022 3:10 PM

NETWORK INCIDENT

Secure Fabric Link Down

Severity: **Major**

Priority: **P1**

Correlated Alerts: 7

Status: Active

Created: 9/11/2022 1:38 PM

Last Updated: 9/11/2022 3:10 PM

NETWORK INCIDENT

Secure Fabric Link Down

Severity: **Major**

Priority: **P1**

Correlated Alerts: 7

Status: Active

Created: 9/11/2022 1:38 PM

Last Updated: 9/11/2022 3:10 PM

[View All Incidents](#)

Your Top Alerts ?? (1-4 of 16)

NETWORK ALERT

Device Disconnected to Controller

Severity: **Warning**

Priority: **P1**

NETWORK ALERT

Device Disconnected to Controller

Severity: **Warning**

Priority: **P1**

NETWORK ALERT

Device Disconnected to Controller

Severity: **Warning**

Priority: **P1**

NETWORK ALERT

Device Disconnected to Controller

Severity: **Warning**

Priority: **P1**

Events - Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Prisma SD-WAN Incidents & Alerts

Overview Incidents Alerts Settings

Dashboards

Incidents & Alerts **99+**

Monitor >

Manage >

Workflows >

Reports

Search

Notifications

Help

<username>

Settings

TSG Name XYZ

Minimize Menu <

Impact	80 Major	175 Warning	175 Informational
Network	4356	47	83
Device	24	44	18
Cellular	65	31	29
Application	27	99	90
Policy	12	90	36
Branch HA Groups	23	40	5
AAA (Auth)	71	23	17

255

Incidents by Priority

P1	126
P2	14
P3	25
P4	43
P5	47

Your Top Incidents (1-4 of 16)

NETWORK INCIDENT Site Connectivity Degraded Severity: Major Priority: P1 Correlated Alerts: 7 Status: Active Created: 9/11/2022 1:38 PM Last Updated: 9/11/2022 3:10 PM	NETWORK INCIDENT Secure Fabric Link Down Severity: Major Priority: P1 Correlated Alerts: 7 Status: Resolved Created: 9/11/2022 1:38 PM Last Updated: 9/11/2022 3:10 PM	NETWORK INCIDENT Secure Fabric Link Down Severity: Major Priority: P1 Correlated Alerts: 7 Status: Active Created: 9/11/2022 1:38 PM Last Updated: 9/11/2022 3:10 PM	NETWORK INCIDENT Secure Fabric Link Down Severity: Major Priority: P1 Correlated Alerts: 7 Status: Active Created: 9/11/2022 1:38 PM Last Updated: 9/11/2022 3:10 PM
--	---	---	---

[View All Incidents](#)

Your Top Alerts ?? (1-4 of 16)

NETWORK ALERT Device Disconnected to Controller Severity: Warning Priority: P1	NETWORK ALERT Device Disconnected to Controller Severity: Warning Priority: P1	NETWORK ALERT Device Disconnected to Controller Severity: Warning Priority: P1	NETWORK ALERT Device Disconnected to Controller Severity: Warning Priority: P1
---	---	---	---

Events - NOW Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Prisma SD-WAN Incidents & Alerts

Overview Incidents Alerts Settings

Dashboards

Incidents & Alerts **99+**

Monitor >

Manage >

Workflows >

Reports

Search

Notifications

Help

<username>

Settings

TS TSG Name XYZ

Minimize Menu <

Impact	80 Major	175 Warning	175 Informational
Network	4356	47	83
Device	24	44	18
Cellular	65	31	29
Application	27	99	90
Policy	12	90	36
Branch HA Groups	23	40	5
AAA (Auth)	71	23	17

Incidents by Priority

Priority	Count
P1	126
P2	14
P3	25
P4	43
P5	47

255

Your Top Incidents (1-4 of 16)

Incident Title	Severity	Priority	Status	Created	Last Updated
Site Connectivity Degraded	Major	P1	Active	9/11/2022 1:38 PM	9/11/2022 3:10 PM
Secure Fabric Link Down	Major	P1	Resolved	9/11/2022 1:38 PM	9/11/2022 3:10 PM
Secure Fabric Link Down	Major	P1	Active	9/11/2022 1:38 PM	9/11/2022 3:10 PM
Secure Fabric Link Down	Major	P1	Active	9/11/2022 1:38 PM	9/11/2022 3:10 PM

[View All Incidents](#)

Your Top Alerts ?? (1-4 of 16)

Alert Title	Severity	Priority
Device Disconnected to Controller	Warning	P1
Device Disconnected to Controller	Warning	P1
Device Disconnected to Controller	Warning	P1
Device Disconnected to Controller	Warning	P1

Events - Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Prisma SD-WAN Incidents & Alerts

Overview Incidents Alerts Settings

Application	Incidents	Alerts	Settings
Policy	12	90	36
Branch HA Groups	23	40	5
AAA (Auth)	71	23	17

Your Top Incidents (1-4 of 16)

- NETWORK INCIDENT**
Site Connectivity Degraded
Severity: ! Major
Priority: P1
Correlated Alerts: 7
Status: Active
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM
- NETWORK INCIDENT**
Secure Fabric Link Down
Severity: ! Major
Priority: P1
Correlated Alerts: 7
Status: Resolved
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM
- NETWORK INCIDENT**
Secure Fabric Link Down
Severity: ! Major
Priority: P1
Correlated Alerts: 7
Status: Active
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM
- NETWORK INCIDENT**
Secure Fabric Link Down
Severity: ! Major
Priority: P1
Correlated Alerts: 7
Status: Active
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM

[View All Incidents](#)

Your Top Alerts ?? (1-4 of 16)

- NETWORK ALERT**
Device Disconnected to Controller
Severity: ! Warning
Priority: P1
Correlated Alerts: 7
Status: Active
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM
- NETWORK ALERT**
Device Disconnected to Controller
Severity: ! Warning
Priority: P1
Correlated Alerts: 7
Status: Active
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM
- NETWORK ALERT**
Device Disconnected to Controller
Severity: ! Warning
Priority: P1
Correlated Alerts: 7
Status: Active
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM
- NETWORK ALERT**
Device Disconnected to Controller
Severity: ! Warning
Priority: P1
Correlated Alerts: 7
Status: Active
Created: 9/11/2022 1:38 PM
Last Updated: 9/11/2022 3:10 PM

[View All Alerts](#)

Notifications Help <username> Settings TSG Name XYZ Minimize Menu

Events - Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Incidents & Alerts

Overview **Incidents** Alerts Settings

Sort By: Time ▼ + Add Filter Reset

Incidents(30) Group By ▼

Created ↑↓	Incident Name ↑↓	Primary Impacted Object ↑↓	Severity ↑↓	Priority ↑↓	Correlation ID ↑↓	Cleared ↑↓	Actions ↑↓ ⚡
Apr 10, 2023 18:00:02 PM	Device analytics disconnected	Cosmos_Ion_3000v @ Cosmos_Site	Informational	P4	Dq2Fh8c1	No	⋮
Apr 10, 2023 18:00:02 PM	Device flows disconnected	Cosmos_Ion_3000v @ Cosmos_Site	Informational	P4	ZLBBzbzj	No	⋮
Apr 10, 2023 17:46:17 PM	Process Stopped	Cosmos_Ion_3000v @ Cosmos_Site	Warning	P3	wshKvRy4	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	DC-SITE2-ELEM1 @ SanFrancisco	Informational	P4	JETVj5ky	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	DC-SITE2-ELEM2 @ SanFrancisco	Informational	P4	RPLqHnlW	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	DC-SITE1-ELEM1 @ Seattle	Informational	P4	BncXRfr5	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	BR-SITE2-ELEM1 @ London	Informational	P4	8zY8FCYe	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	BR-SITE2-ELEM2 @ London	Informational	P4	5GGsor2P	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	BR-SITE1-ELEM1 @ Chennai	Informational	P4	467arm9b	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	@ Anusha-Spoke-Site	Informational	P4	7HTS53NB	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	@ Anusha-Spoke-Site	Informational	P4	q7pCxotA	No	⋮
Apr 06, 2023 14:30:01 PM	Device analytics disconnected	@ Anusha-Spoke-Site	Informational	P4	2YBmGMUq	No	⋮
Apr 06, 2023 14:31:00 PM	Device analytics disconnected	@ Anusha-Spoke-Site	Informational	P4	wonVZf8O	No	⋮
Apr 06, 2023 14:30:01 PM	Device analytics disconnected	Anusha-Hub @ Anusha-Hub	Informational	P4	DXXd9W4x	No	⋮
Apr 06, 2023 14:30:01 PM	Device flows disconnected	BR-SITE2-ELEM1 @ London	Informational	P4	VZtEZ9cH	No	⋮
Apr 06, 2023 14:30:01 PM	Device flows disconnected	BR-SITE2-ELEM2 @ London	Informational	P4	usiXfayo	No	⋮
Apr 06, 2023 14:31:00 PM	Device flows disconnected	BR-SITE1-ELEM1 @ Chennai	Informational	P4	Zwcu2O7K	No	⋮

Notifications
Help
<username>
Settings
TSG Name XYZ

Minimize Menu ◀

Events - Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Incidents & Alerts

Overview Incidents Alerts Settings

Sort By: Time

Incidents(30)

Created

Created	Primary Impacted Object	Severity	Priority	Correlation ID	Cleared	Actions
Apr 10, 2023 18:00:00	Cosmos_Ion_3000v @ Cosmos_Site	Informational	P4	Dq2Fh8c1	No	⋮
Apr 10, 2023 18:00:00	Cosmos_Ion_3000v @ Cosmos_Site	Informational	P4	ZLBBzbzj	No	⋮
Apr 10, 2023 17:46:10	Cosmos_Ion_3000v @ Cosmos_Site	Warning	P3	wshKvRy4	No	⋮
Apr 06, 2023 14:31:00	DC-SITE2-ELEM1 @ SanFrancisco	Informational	P4	JETVj5ky	No	⋮
Apr 06, 2023 14:31:00	DC-SITE2-ELEM2 @ SanFrancisco	Informational	P4	RPLqHnlW	No	⋮
Apr 06, 2023 14:31:00 PM	DC-SITE1-ELEM1 @ Seattle	Informational	P4	BncXRfr5	No	⋮
Apr 06, 2023 14:31:00 PM	BR-SITE2-ELEM1 @ London	Informational	P4	8zY8FCYe	No	⋮
Apr 06, 2023 14:31:00 PM	BR-SITE2-ELEM2 @ London	Informational	P4	5GGsor2P	No	⋮
Apr 06, 2023 14:31:00 PM	BR-SITE1-ELEM1 @ Chennai	Informational	P4	467arm9b	No	⋮
Apr 06, 2023 14:31:00 PM	@ Anusha-Spoke-Site	Informational	P4	7HTS53NB	No	⋮
Apr 06, 2023 14:31:00 PM	@ Anusha-Spoke-Site	Informational	P4	q7pCxotA	No	⋮
Apr 06, 2023 14:30:01 PM	@ Anusha-Spoke-Site	Informational	P4	2YBmGMUq	No	⋮
Apr 06, 2023 14:31:00 PM	@ Anusha-Spoke-Site	Informational	P4	wonVZf8O	No	⋮
Apr 06, 2023 14:30:01 PM	Anusha-Hub @ Anusha-Hub	Informational	P4	DXXd9W4x	No	⋮
Apr 06, 2023 14:30:01 PM	BR-SITE2-ELEM1 @ London	Informational	P4	VZtEZ9cH	No	⋮
Apr 06, 2023 14:30:01 PM	BR-SITE2-ELEM2 @ London	Informational	P4	usiXfayo	No	⋮
Apr 06, 2023 14:31:00 PM	BR-SITE1-ELEM1 @ Chennai	Informational	P4	Zwcu2O7K	No	⋮

Notifications

Help

<username>

Settings

TSG Name XYZ

Minimize Menu

Events - Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Sort By: Time | Sites: Anusha-Hip | Add Filter | Show Less | Reset

Incidents(3) | Group By

Created	Incident Name	Primary Impacted Object	Severity	Priority	Correlation ID	Cleared	Actions
Apr 06, 2023 14:30:01 PM	Device analytics disconnected	Cosmos_Ion_3000v @ Cosmos_Site	Informational	P4	DXXd9W4x	No	
Jul 27, 2022 10:40:00 AM	Device disconnected from Controller	Cosmos_Ion_3000v @ Cosmos_Site	Warning	P3	WChsAK3c	No	
Jul 14, 2022 13:21:39 PM	Interface Down	Cosmos_Ion_3000v @ Cosmos_Site	Warning	P3	brqCVtIX	No	

25 Rows | Page 1 of 1

Notifications | Help | <username> | Settings | TSG Name XYZ | Minimize Menu

Events - Incidents

Severity Matrix

Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details

PRISMA SD-WAN
BY PALO ALTO NETWORKS

Incident Details

Incident Severity: ! Major
 Incident Code: Allow Security Rule covered by higher order Rules
 Correlation ID: IDC0001
 Fault Code: SITE_CONNECTIVITY_DEGRADED
 Incident ID: 63588bfe3157c1720bd7680e

OPERATIONS

Acknowledgment Status: 👁 Acknowledged
 Created: Sep 20, 2019 9:23:09 PM
 Last Updated: Sep 21, 2019 2:45 PM ??

INCIDENT SETTINGS INFORMATION

Incident Rule Set: [Policyv2](#)
 Incident Policy Rule: [Incident Rule Set](#)
 Incident Policy Applied Time: Sep 21, 2019 9:23:10 PM
 System Suppressed Time: Sep 21, 2019 9:24:55 PM

Impacted Objects

Entity: AWS US-West-2 (AWS) ↔ Branch 1 Spectrum Cable

Site Name:

- Branch 1
- AWS US-West-2

VPN Link:

- AWS-USW-2-ION1@AWS US-West-2 (AWS via AWS Blended) ↔ (Spectrum Cable via Spectrum Cable) Branch 1 ION 3K@Branch 1
- AWS-USW-2-ION2@AWS US-West-2 (AWS via AWS Blended) ↔ (Spectrum Cable via Spectrum Cable) Branch 1 ION 3K@Branch 1

Detection Details

CORRELATED INCIDENT (2)

Generated	Severity	Incident Name	ID	Incident Status
Feb 24th 2021 12:04pm PST	! Critical	SITE CONNECTIVITY DOWN	AO11111	Raised
Feb 22th 2021 01:02pm PST	! Warning	NETWORK_VPNPEER_UNAVAILABLE	AO22222	Raised

Underlying Reasons

on prisma-sdwan-gcp-site-europe-west2 (AWS - publicwan) ↔ CHATOPS_AKASH1_BR18-test-act

prisma-sdwan-gcp-site-europe-west2 (Circuit to AWS-... ↔ CHATOPS_AKASH1_BR18-test-act (Circuit to AWS-publicwan)

Incident Acknowledgment

Acknowledgment Status: 👁 Acknowledge Alert

Remediation Playbook

Play 1: Check Related Faults
 In the Anynetlink alarm, check whether Related Faults are available. If present, Related Faults are the Root cause events for this Anynetlink alarm. Follow the troubleshooting steps of Related Faults.

Play 2: Check Reasons
 If Related Faults are not available, check out "Reasons" in the alarm to find out specific failures in the vpnlincs under this anynetlink.

Play 3:
 If the reason in the Alarm has NETWORK_VPNSS_UNAVAILABLE (VPN shared secret key Unavailable) - the shared secret required to establish a VPN Link is not available. The Prisma SD-WAN controller pre-issues a certain number of shared secrets (3 days worth by default). If the communication between the Prisma SD-WAN Controller and the device is down for 3 days or more, then this fault is raised.

Play 4:
 If the reason in the Alarm has NETWORK_VPNPEER_UNREACHABLE, the control communication could not be established with the VPN Peer. Common reasons include:

- IP Address mis-configuration
- NAT misconfiguration
- a firewall which is blocking port 4500 traffic as UDP port 4500 is used for control communication between the 2 VPN Peers

Play 5:
 If the reason in the Alarm has NETWORK_VPNSS_MISMATCH (VPN Shared Secret Mismatch), the VPN Peers could not agree on a shared secret. This usually happens when:

- one of the devices is not able to contact the Prisma SD-WAN Controller and retrieve the shared secret corresponding to the time window when the fault was raised
- the clocks on the VPN Peer devices are out of sync

Play 6:
 If the reason in the Alarm has NETWORK_VPNBFD_DOWN (VPN Liveliness Down) - VPN Link liveliness is monitored through BFD heartbeats. This fault indicates that the VPN Link went down because the BFD heartbeats failed. If this is a temporary network failure then the VPN Link will come back up once the network is restored. If the fault continues to stay on then check for network availability.

Still not resolved?

Flow Browser

Flow Browser

Branch Sites

Last Update 12:24:09 AM

Search

Faisal-PIC-V2

Prisma Access Prisma SD-WAN

Map List Activity **Flows**

Site: SASE_BR_03

Start Date: Feb 4, 2025, 11:24 PM

Time Range: 1 hour

Apps

Viewing Apps by: All Apps

Add Filter

Show 8 More

Apply

Reset

SRC	SRC P...	DST	VRF	DST P...	POLICY	SEC ACTI...	APP	PROT...	SGI	INGRESS PATH
172.19.23.1	37505	13.251.109.27	N/A	443	default default (QoS)	N/A	ssl	TCP	N/A	N/A
172.19.23.1	43815	35.247.150.62	N/A	443	default default (QoS)	N/A	ssl	TCP	N/A	N/A

Page size

100

Page

1



Branch Sites

Last Update 12:24:09 AM

Search

Faisal-PIC-V2

Prisma Access Prisma SD-WAN

Map List Activity Flows

Site: SASE_BR_03

Start Date: Feb 4, 2025, 11:24 PM

Time Range: 1 hour

Apps

Viewing Apps by: All Apps

Add Filter

Show 8 More

Apply

Reset

SRC	SRC P...	DST	VRF	DST P...	POLICY	SEC ACTI...	APP	PROT...	SGI	INGRESS PATH
172.19.23.1	37505	13.251.109.27	N/A	443	default default (QoS)	N/A	ssl	TCP	N/A	N/A
172.19.23.1	43815	35.247.150.62	N/A	443	default default (QoS)	N/A	ssl	TCP	N/A	N/A

Page size 100 Page 1

RMA

RMA

Devices

Claimed Devices Unclaimed Devices

Prisma SD-WAN
Devices (8)

Search by name, software, serial

Connected Roles Models Tags Supports: Any Add Filter Reset

Device Name	Device Info	Software	Last Activity	State	Actions
Singapore Singapore	67d94d56-50f8-5711-7f69-7156ce16bffb	Upgrade	Upgrade: Sep 15, 2024 15:20	Offline	
LAB_1200_5G Singapore	ion 1200-c5g-ww 024801-000510-8912	Current: 6.4.1-b7 Upgrade	Config: Dec 19, 2024 05:52 Upgrade: Oct 4, 2024 19:58	Assigned Offline	
SASE_BR_01	ion 3102v fe54a5e9-1142-42eb-9b0b-d081e772a755	Current: 6.4.1-b7 Upgrade	Config: Nov 9, 2024 12:05 Upgrade: Oct 13, 2024 09:55	Assigned Offline	
SASE_DC_01 Singapore 640637 Singapore	ion 3102v 91119c09-cfb9-404d-a60e-76920f1f030b	Current: 6.4.1-b7 Upgrade	Config: Nov 9, 2024 12:05 Upgrade: Oct 13, 2024 09:59	Assigned Offline	
SASE_LAB_1200S_C Santa Clara CA United States	ion 1200-s-c5g-ww 027901-000507-6185	Current: 6.4.1-b7 Upgrade	Config: Feb 5, 2025 00:00 Upgrade: Jan 22, 2025 06:57	Assigned Online	
Unnamed Device	ion 3102v 8610ca7c-f8ea-46b2-9a72-d9930abccd0b	Current: N/A Upgrade	Config: Mar 15, 2024 22:07 Upgrade: Mar 15, 2024 22:07	Software Unknown Offline	

25 Rows Page 1 of 1

RMA

Prisma SDWAN TSG ID:

Faulty ION S/N:

RMA Shipping Company Name:

RMA Shipping Address:

RMA City:

RMA State/Province:

RMA Country:

RMA Zip/Postal code:

Site contact:

Site phone:

Site email:

Site access hours (in local timezone GMT+8):

DEMO

Prisma SDWAN Useful Reference

PRISMA SDWAN Useful Reference:

- **Prisma SDWAN Release Guidelines:**
<https://live.paloaltonetworks.com/t5/customer-resources/prisma-sd-wan-ion-software-release-guidelines/ta-p/578685>
- **Prisma SASE (SD-WAN And Prisma Access) Status Page:**
<https://sase.status.paloaltonetworks.com/>
- **Prisma SD-WAN Upgrade / Downgrade Considerations:**
<https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/6-3/prisma-sd-wan-ion-release-notes/prisma-sd-wan-ion-device-release-6-3/upgrade-downgrade-considerations-in-prisma-sd-wan-ion-release-6-3>
- **Prisma SD-WAN Software End of life Announcement:**
<https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-summary#cloudgenix>
- **Prisma SD-WAN Admin Guide:**
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-admin.pdf
- **Prisma CLI Reference Guide:**
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/prisma/prisma-sd-wan/prisma-sd-wan-ion-cli-reference/prisma-sd-wan-ion-cli-reference.pdf
- **Alerts and Alarms Codes:**
<https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/alert-and-alarm-event-codes>

PRISMA SDWAN Useful Reference (contd.):

- **Prisma SD-WAN CloudBlade for Prisma Access Integration Requirements:**
<https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/deployment-and-integrations/3-1-6/prisma-access-cloudblade-integration-guide-panorama-managed/prisma-sd-wan-and-prisma-access-integration/prisma-sd-wan-cloudblade-for-prisma-access-integration-requirements>
- **Generate Panorama Authorization Key for Prisma SD-WAN Integration:**
<https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/deployment-and-integrations/3-1-6/prisma-access-cloudblade-integration-guide-panorama-managed/prisma-sd-wan-and-prisma-access-integration/generate-panorama-authorization-key-for-prisma-sd-wan-integration>
- **Use the Prisma SD-WAN ION device toolkit commands to troubleshoot cloudblade VPNs:**
<https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/deployment-and-integrations/3-1-6/prisma-access-cloudblade-integration-guide-panorama-managed/troubleshoot-the-integration-process-and-standard-vpns/use-the-device-toolkit>
- **Replace or Change existing Panorama Serial Number Post CloudBlade Integration:**
<https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/deployment-and-integrations/3-1-6/prisma-access-cloudblade-integration-guide-panorama-managed/troubleshoot-the-integration-process-and-standard-vpns/change-existing-panorama-serial-number-post-cloudblade-integration>

End of Session