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

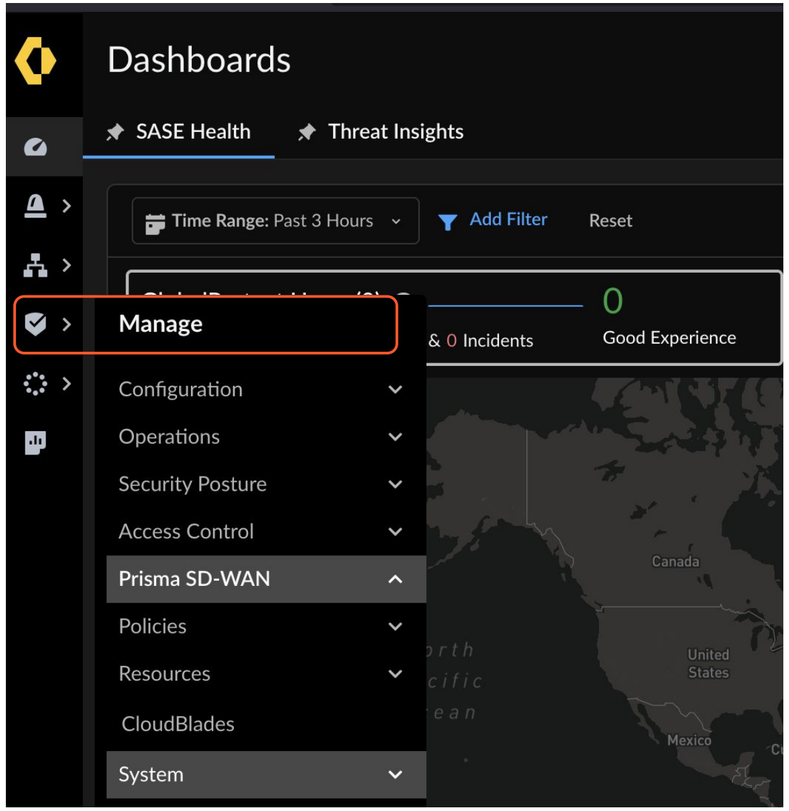
- **Prisma SD-WAN configuration, operation, and troubleshooting of the system is primarily done through the SCM portal.**
- **However there may be times when troubleshooting is required to be done through command line interface.**
- **Prisma SD-WAN offers a Device Toolkit, which is a command line interface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

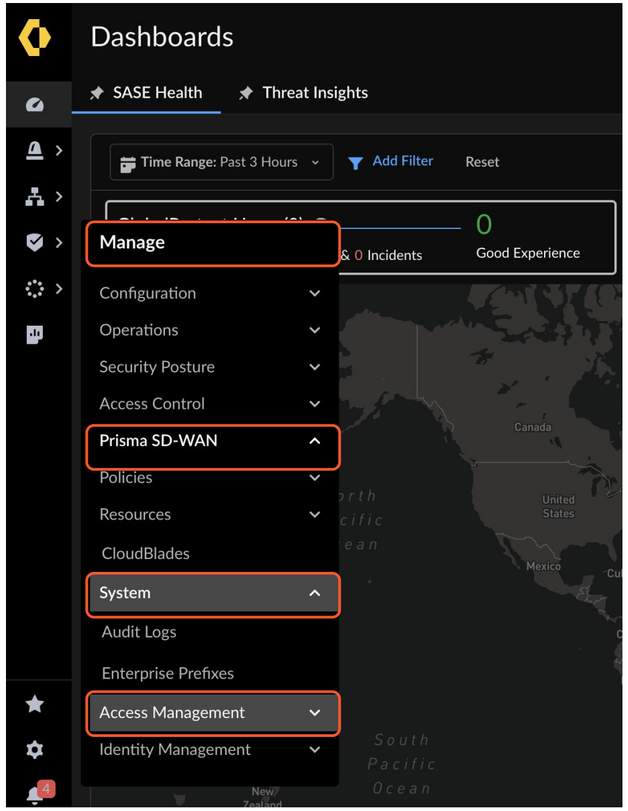
```
ion toolkit# dump overview
Software                : 6.1.10-b1
Hardware Model          : ion 3102v
Time Now                : 2025-02-03 16:25:55
Uptime                  : 45m13.24s
Last Reboot Reason      : declaim requested by root
Device ID               : b2af7b67-c8ba-4bb0-b125-ee48476912ab
Registration 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#
```

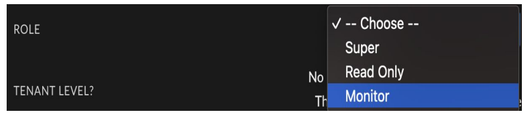
Device Toolkit Workflow

- 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

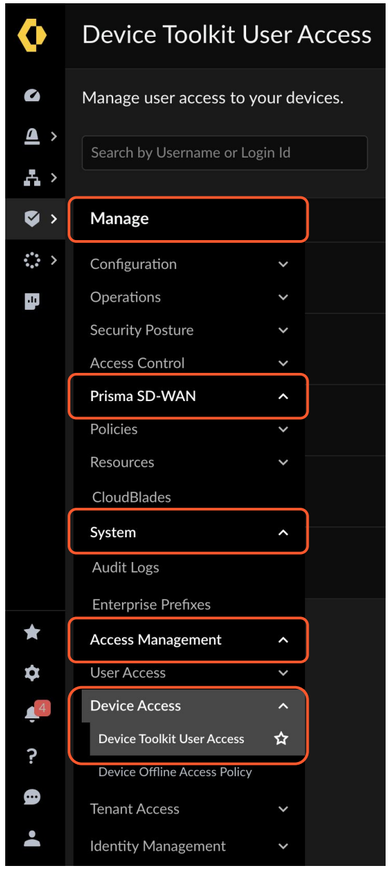


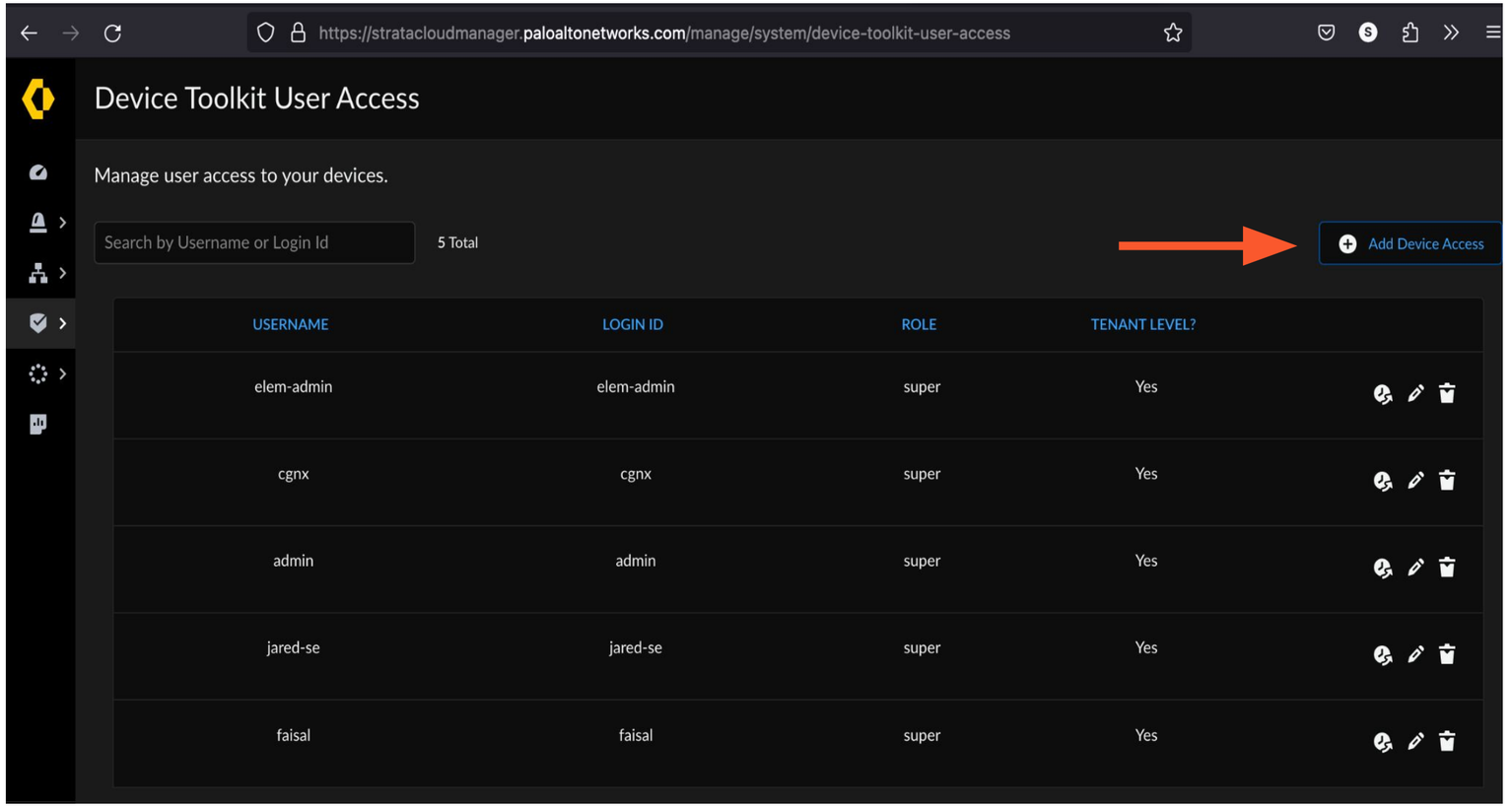




- **Begin the process by entering System Administration**

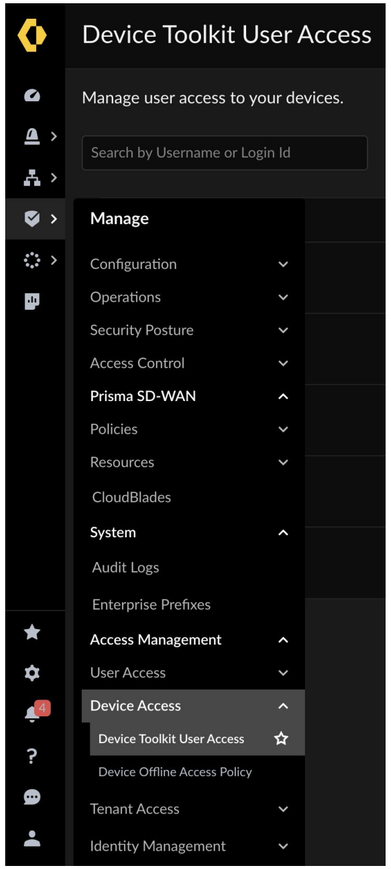
Add Device Toolkit User

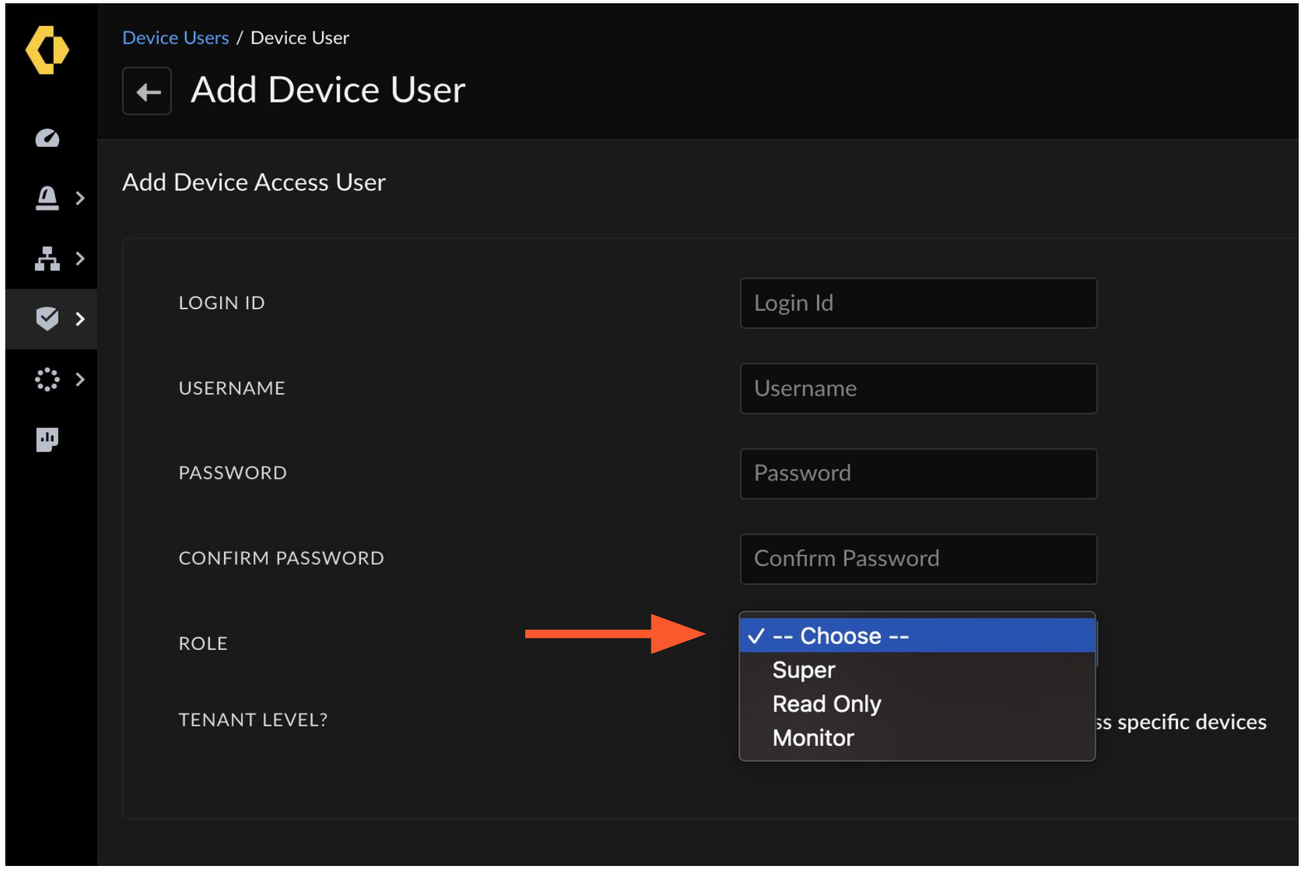




- **Add a user under Device Toolkit User Management**

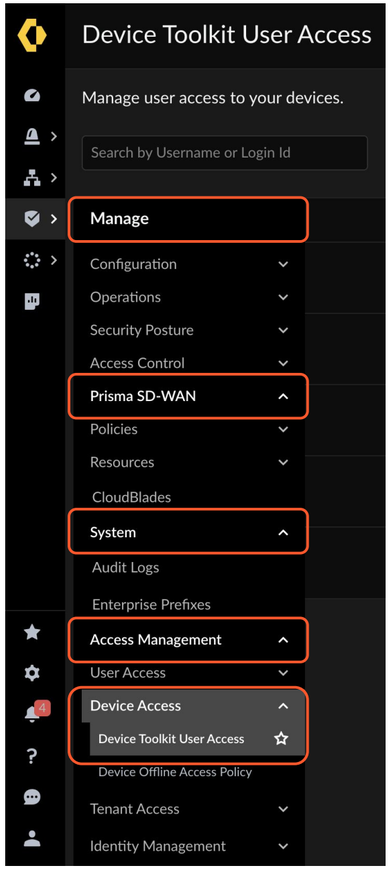
Configure Device Toolkit User Properties

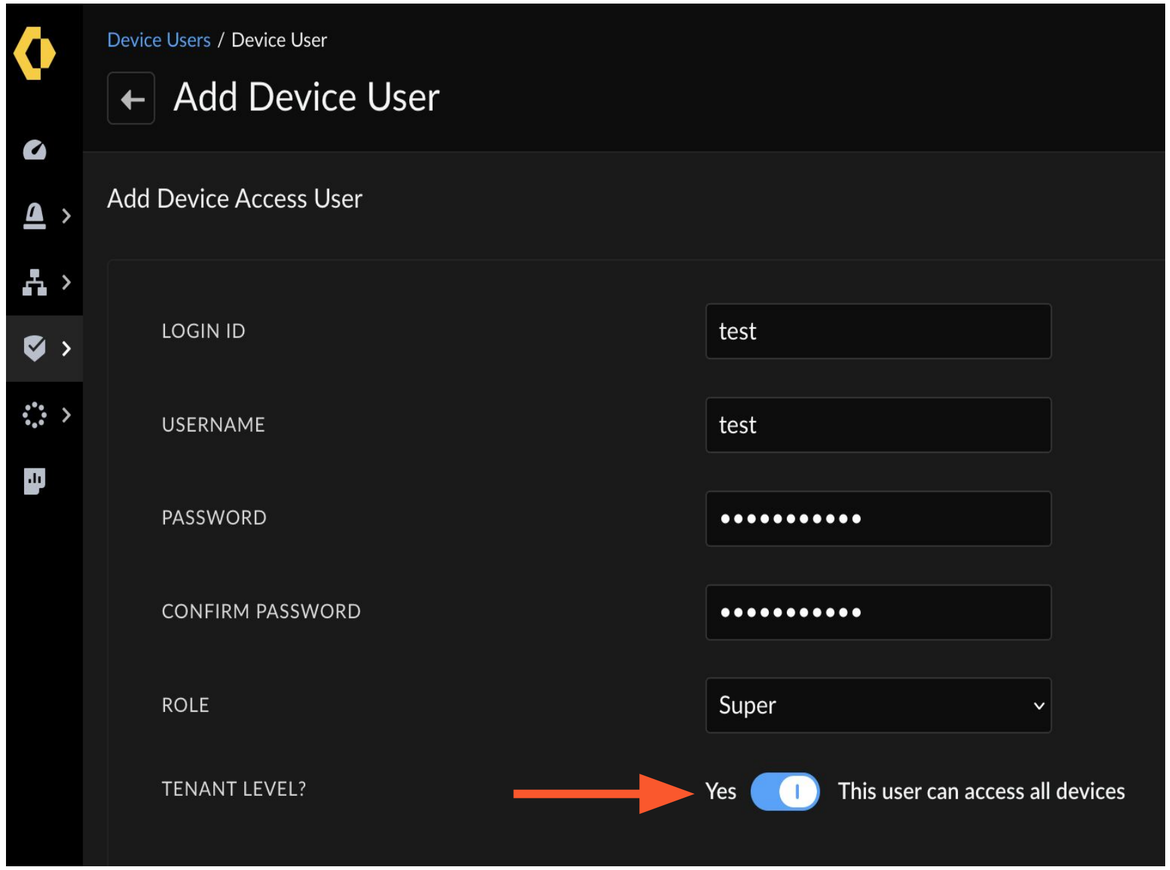




- **Configure login credentials and assign a role to the user**

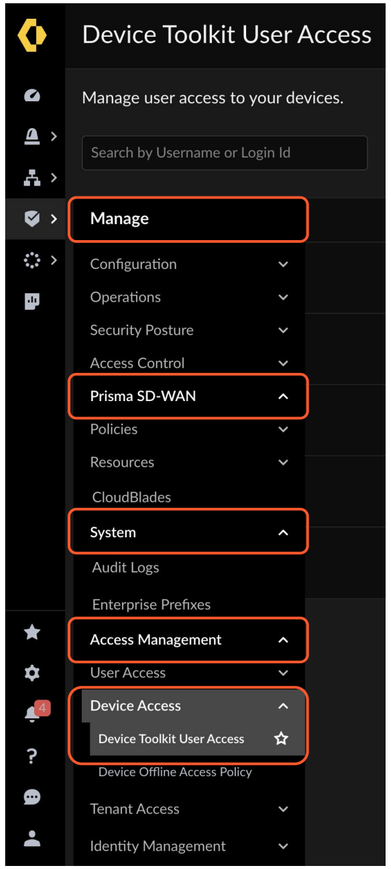
Assign Tenant Level Access

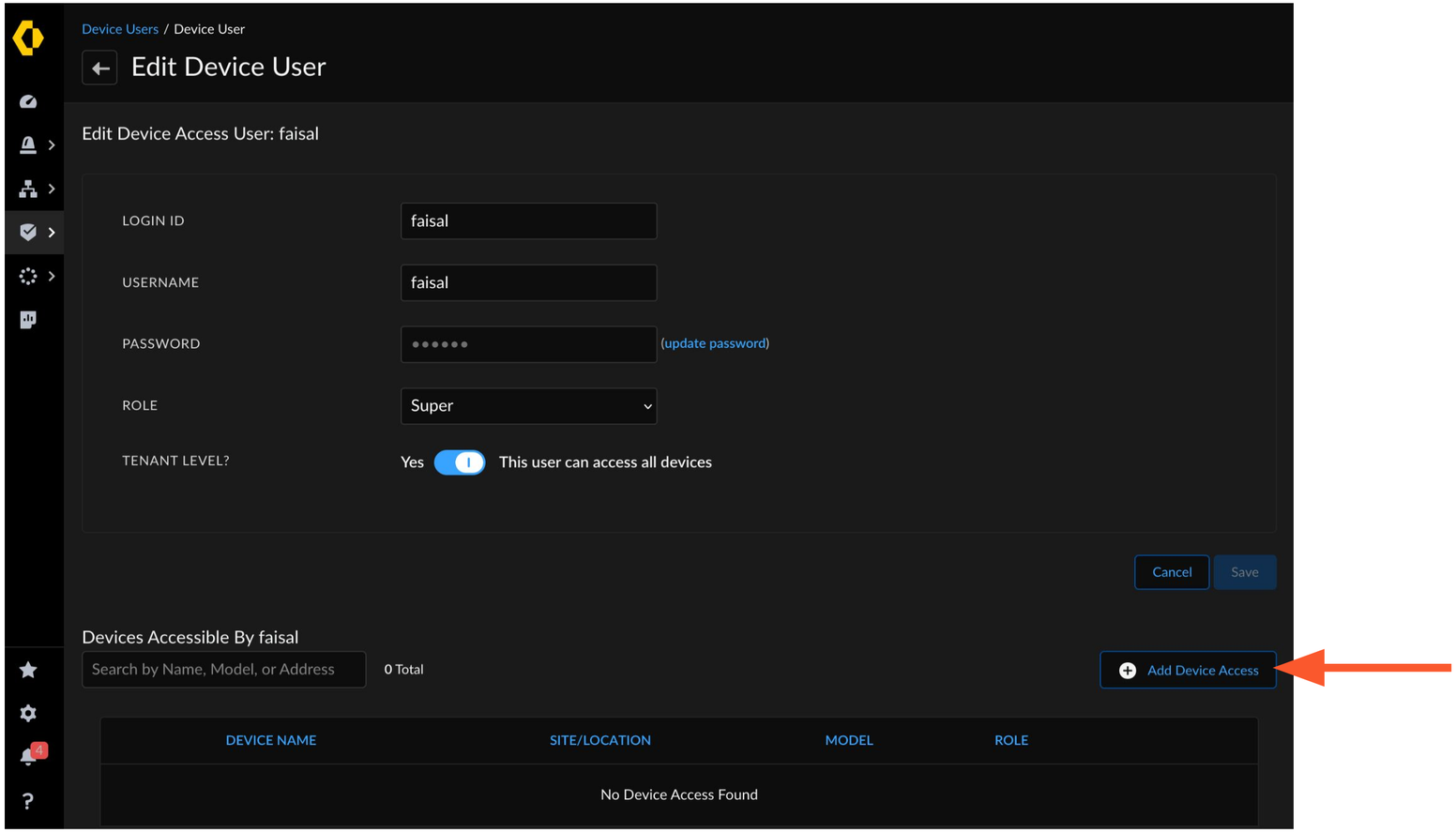




- **Tenant level device access can be enabled for a user**

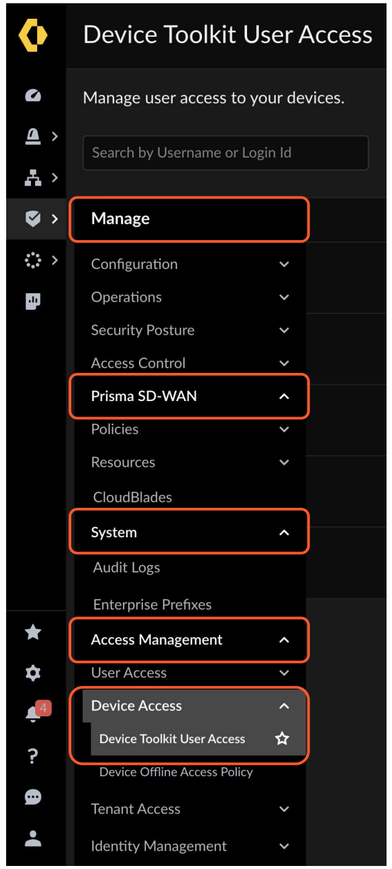
Configure Individual Device (Optional)

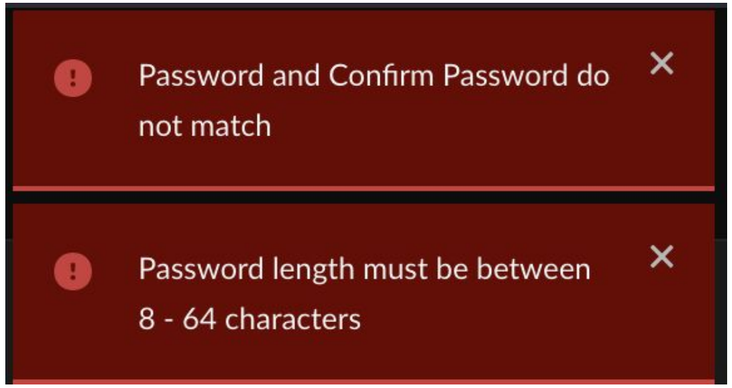




- **Device specific access can be enabled for a user**

Common Errors



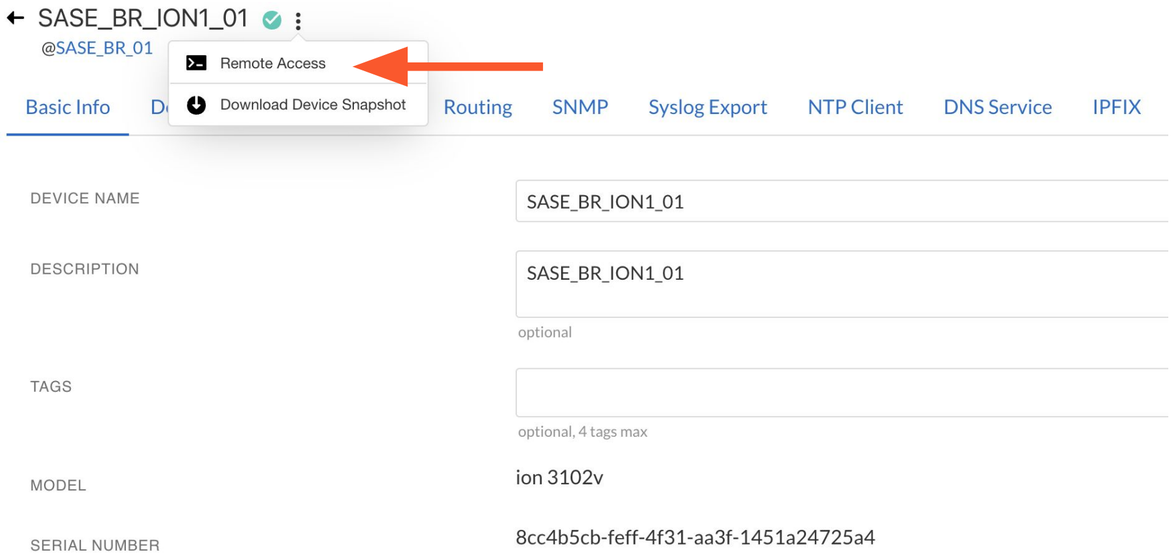


- **Password confirmation need to match and Password length need to be minimum 8 characters.**

Device Access - User Roles

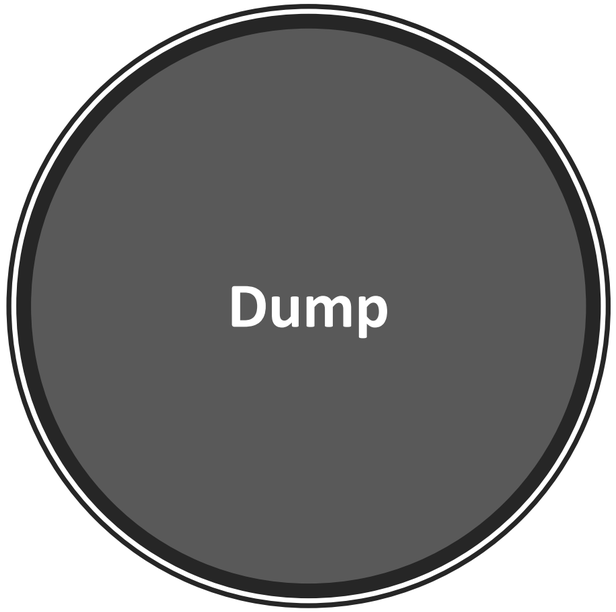
Commands	User Role	Command Description
Dump	**SUPER , READ ONLY, MONITOR**	Displays information Example: Interface config, controller communication status
Inspect	**SUPER , READ ONLY, MONITOR**	Displays dynamic information Example: Routing / ARP tables
File	**SUPER , READ ONLY, MONITOR**	Handles log 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



- **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_elemet    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                     static-arp              extension               overview
hypervisor              qos-bwc                 routing                 security-policy         site                    software                time
troubleshoot            tpm                     vpn                     waninterface            config                  static                  standingalarms
serviceendpoints        ipsecprofiles           reachability-probe      app-l4-prefix           flow                    token                   adem
oss-license             radius                  dpdk                    app-engine
```

- **Provides current system configuration**
- **Access available to all users**

Device Toolkit Commands


```
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
```

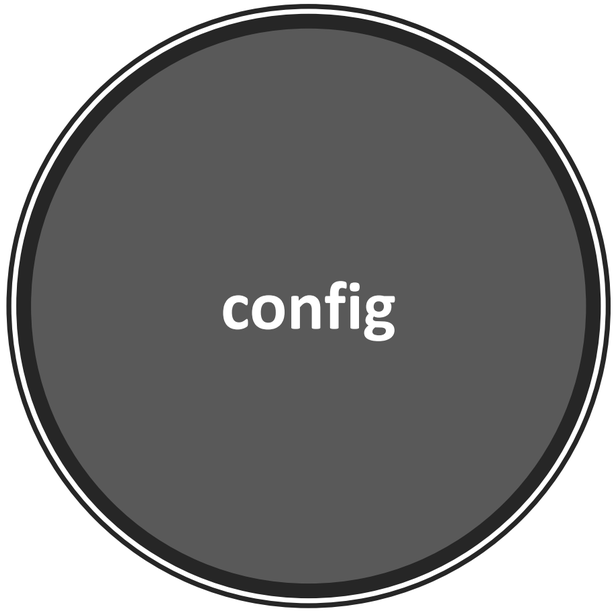
- Shows dynamic information like routing / fib tables, APR tables, etc.
- Access available to all users

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
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#
```

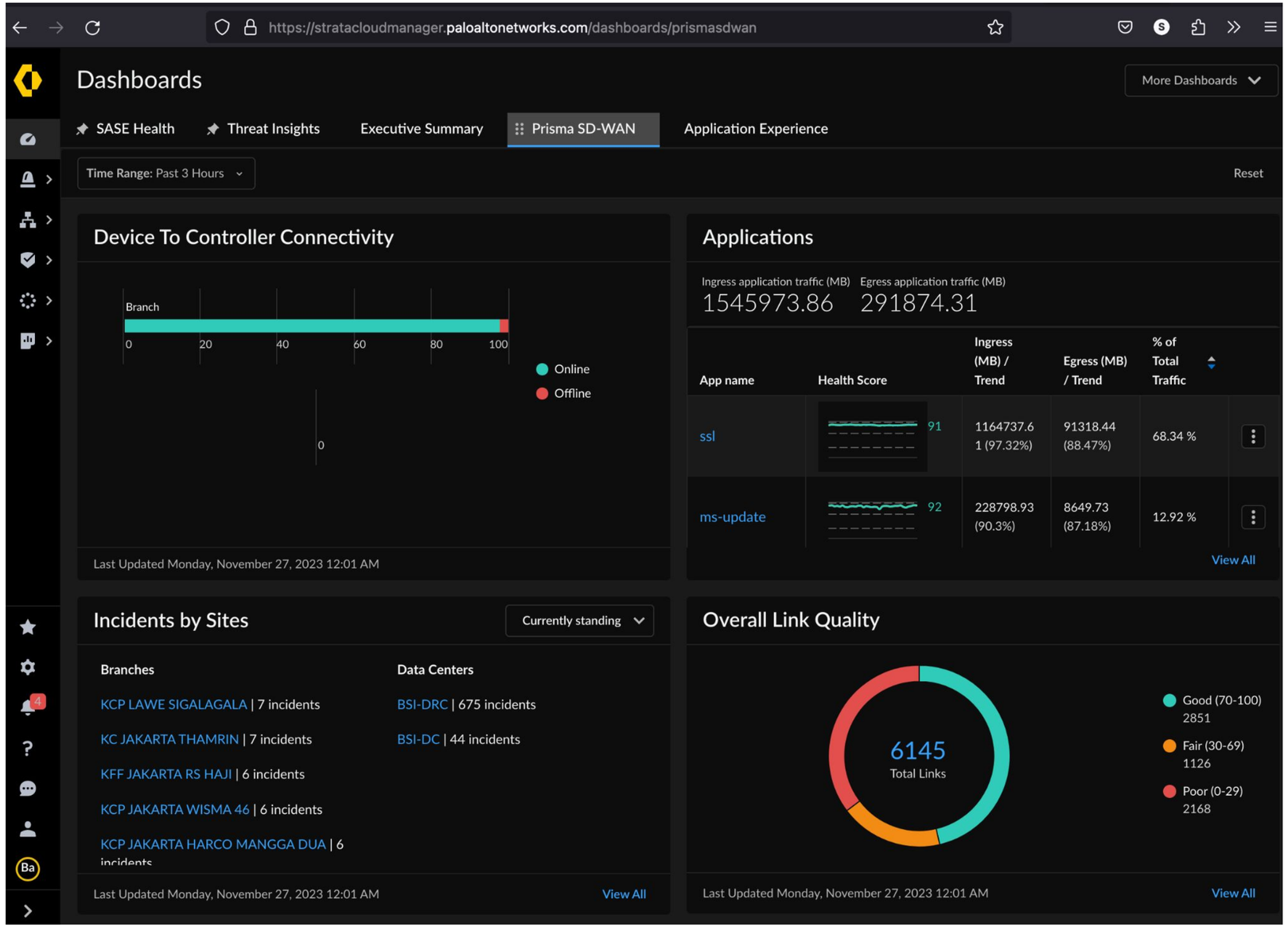
Viewing / Exporting a .pcap file

```
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

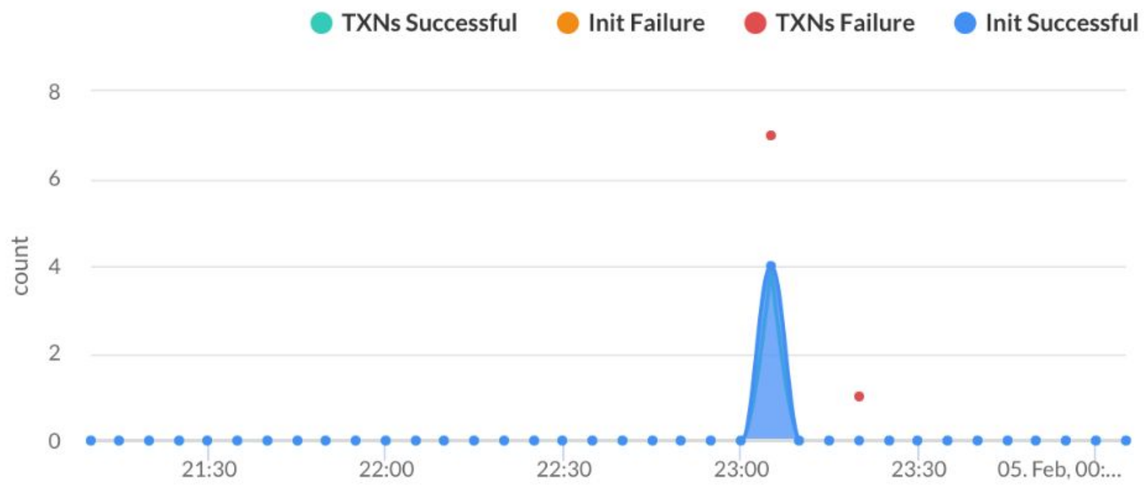
Bandwidth Utilization

Summary

Updated a few seconds ago

View All

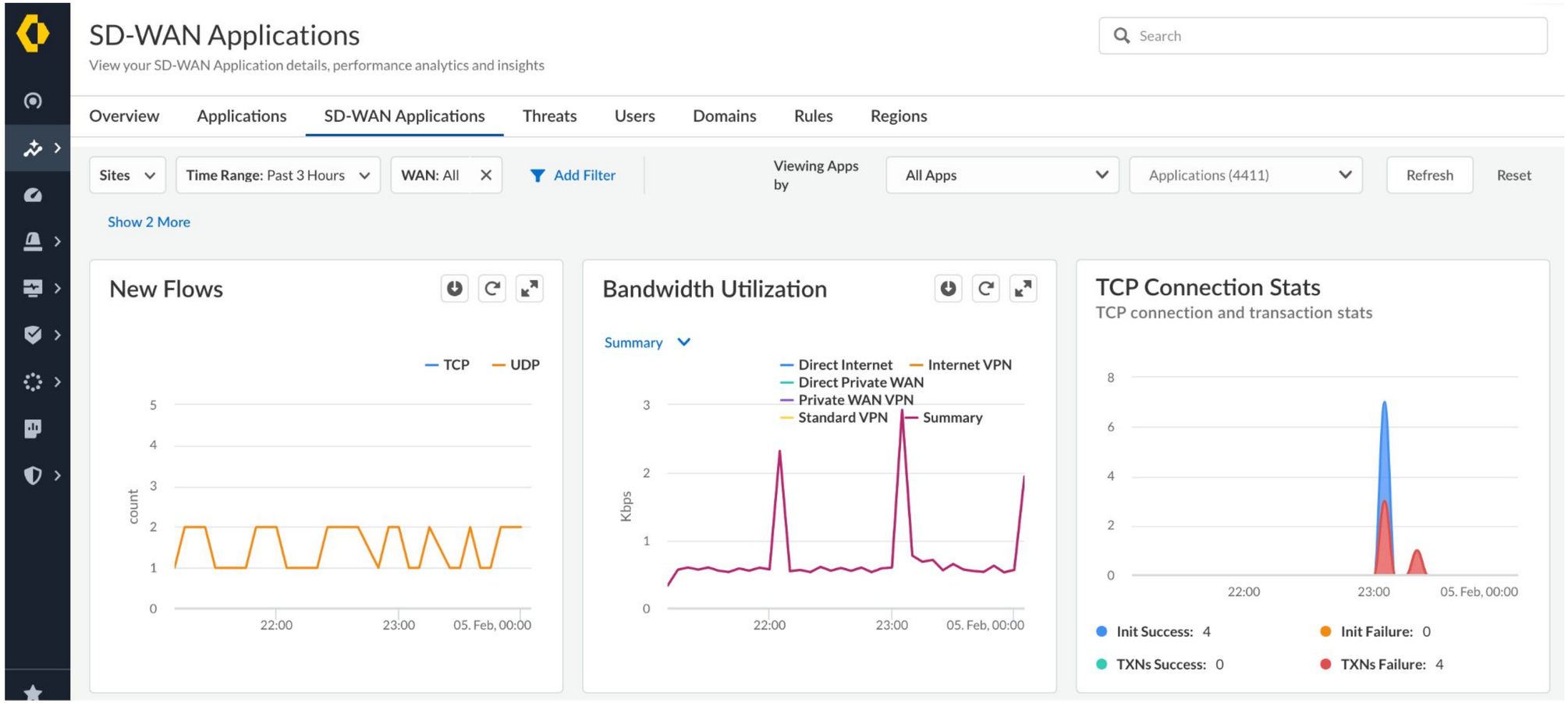
Transaction Stats



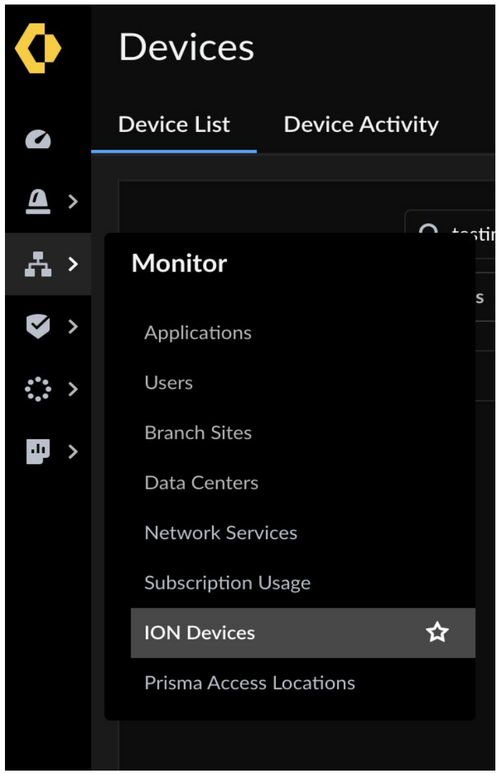
Updated a few seconds ago

View All

Network - Activity Insights > SD-WAN Applications



Monitor > Devices > ION Devices



SASE_LAB_1200S_C

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

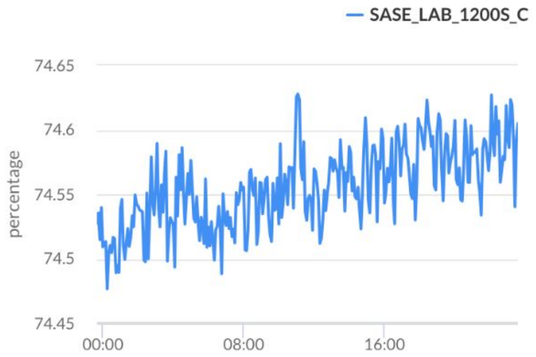
Device Overview

Device Name	SASE_LAB_1200S_C
Site	Cellular_5G_Site 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

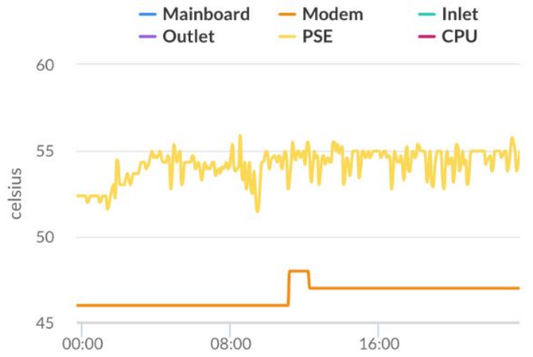
Updated a few seconds ago

Memory Utilization



Updated a few seconds ago

Device Temperature



Disk Utilization

Interface Bandwidth Utilization

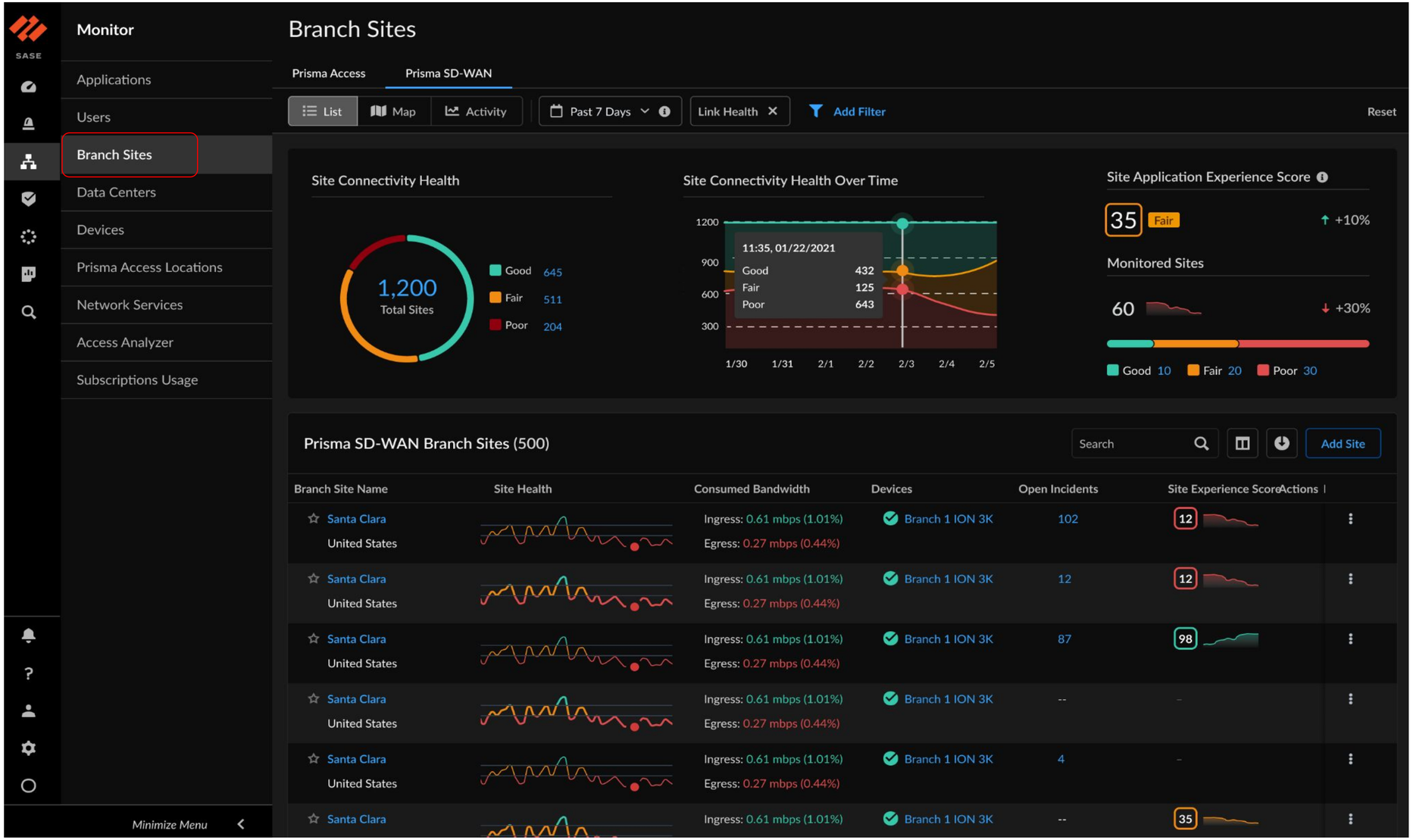
Summary

No Results

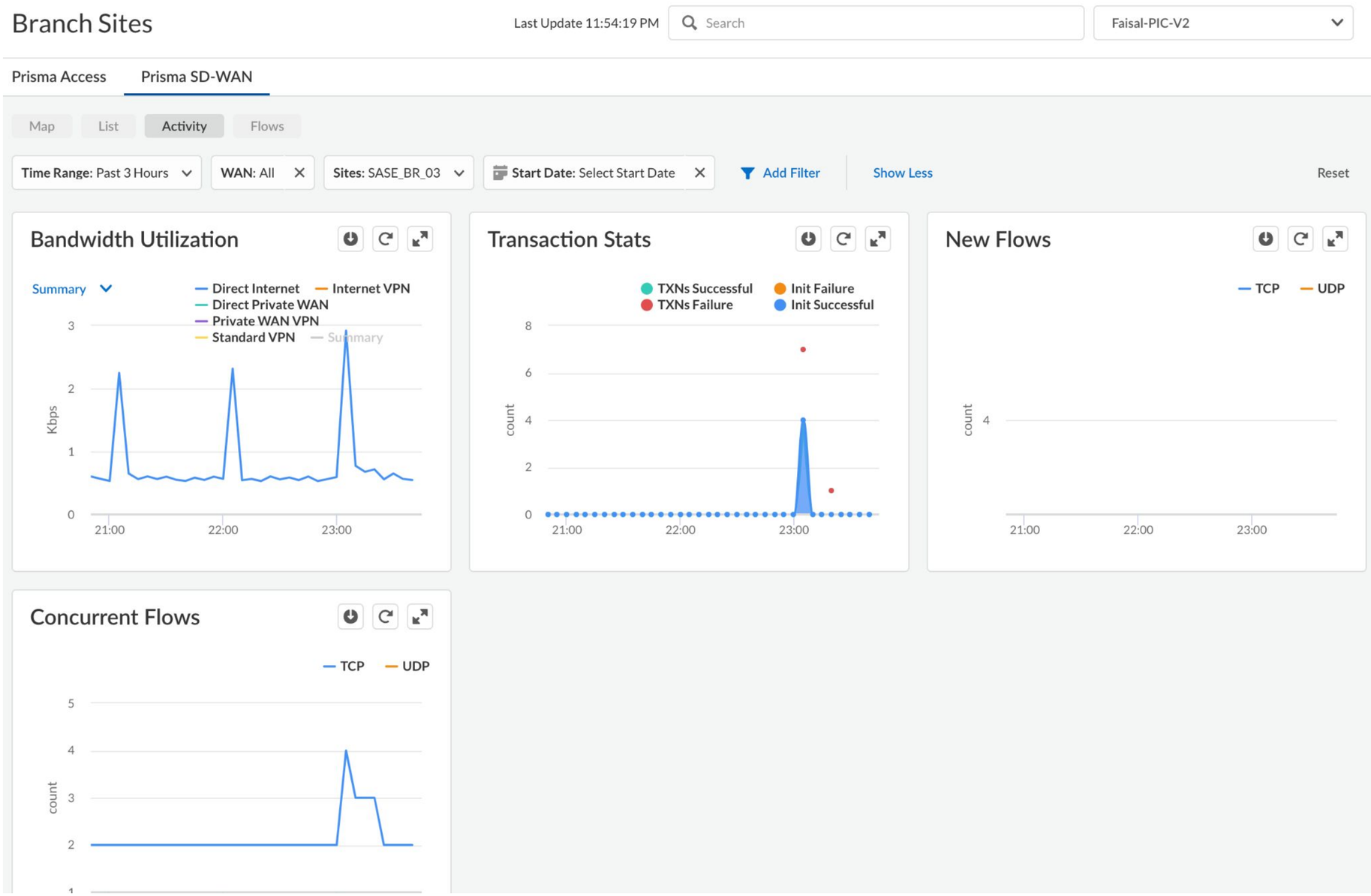
This chart requires the following filters: interface

Monitor

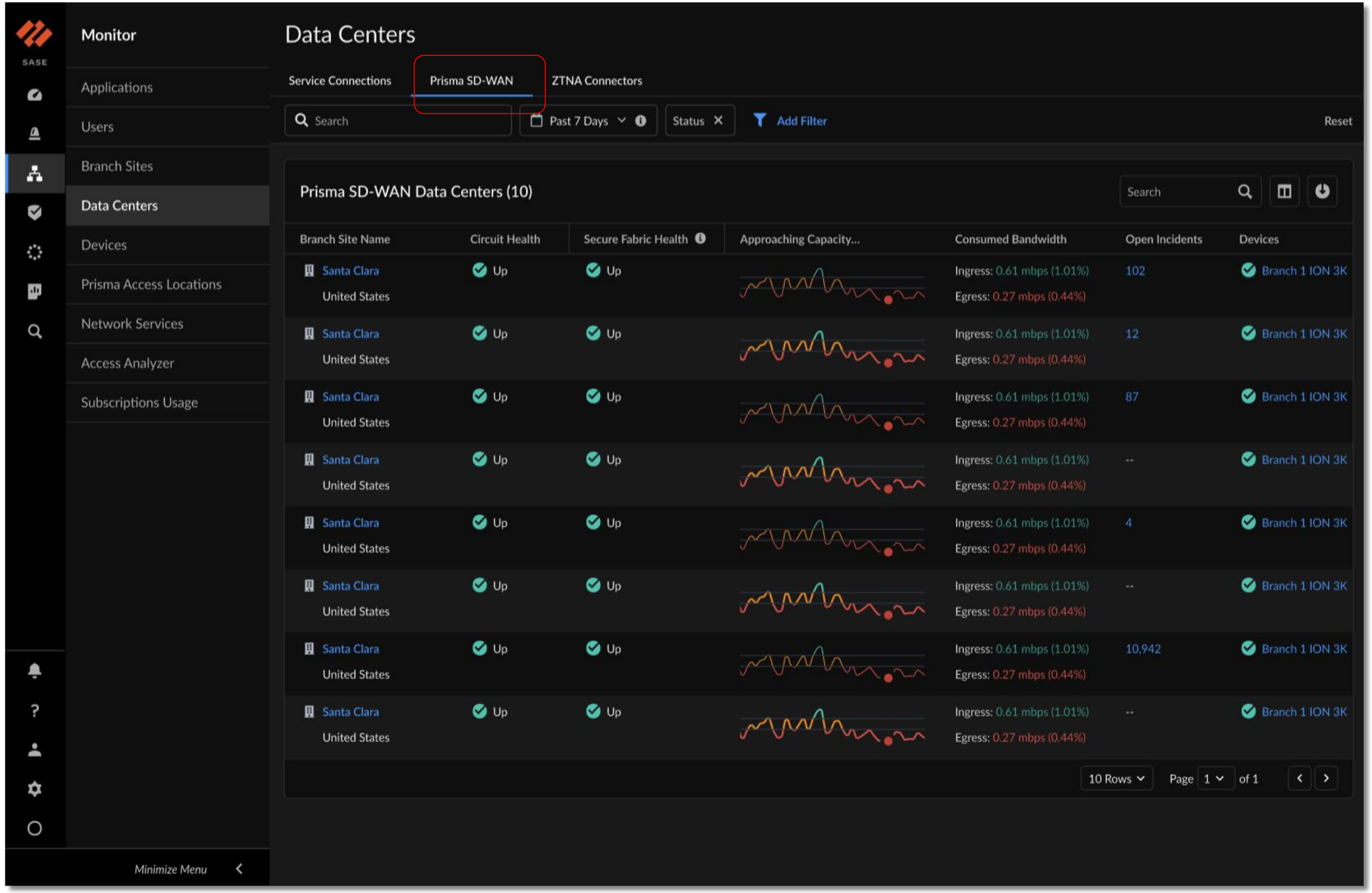
Monitor > Branch Sites



Monitor > Branch Sites > Activity

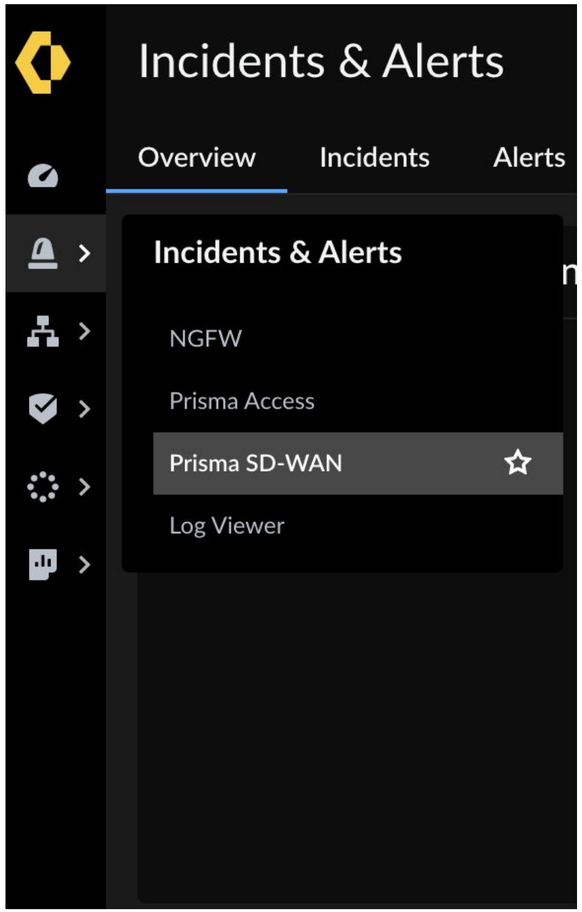


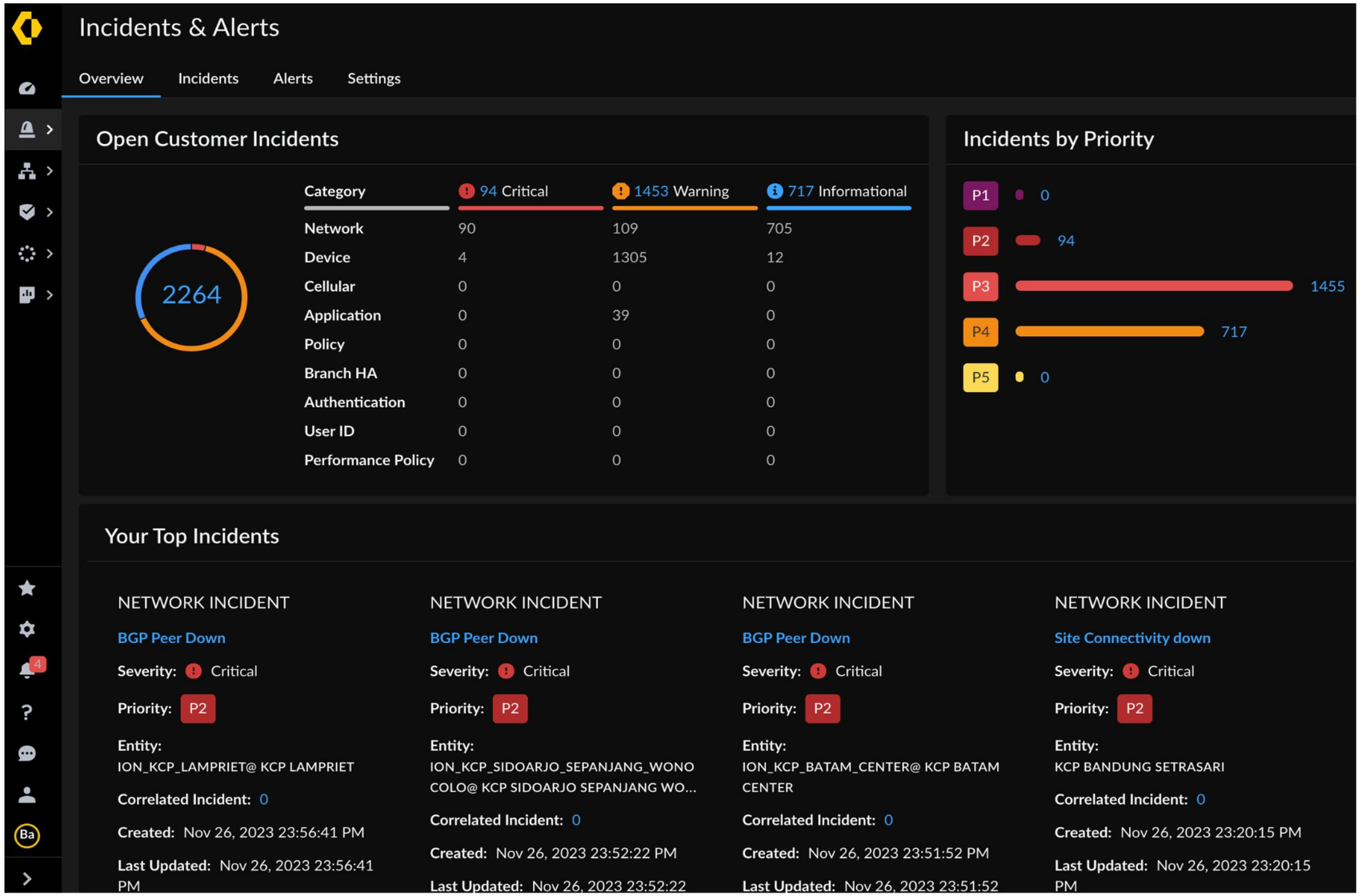
Monitor > Data Centers



Incident and Alerts

Events - Incidents and Alerts





Events - Incidents

Severity Matrix

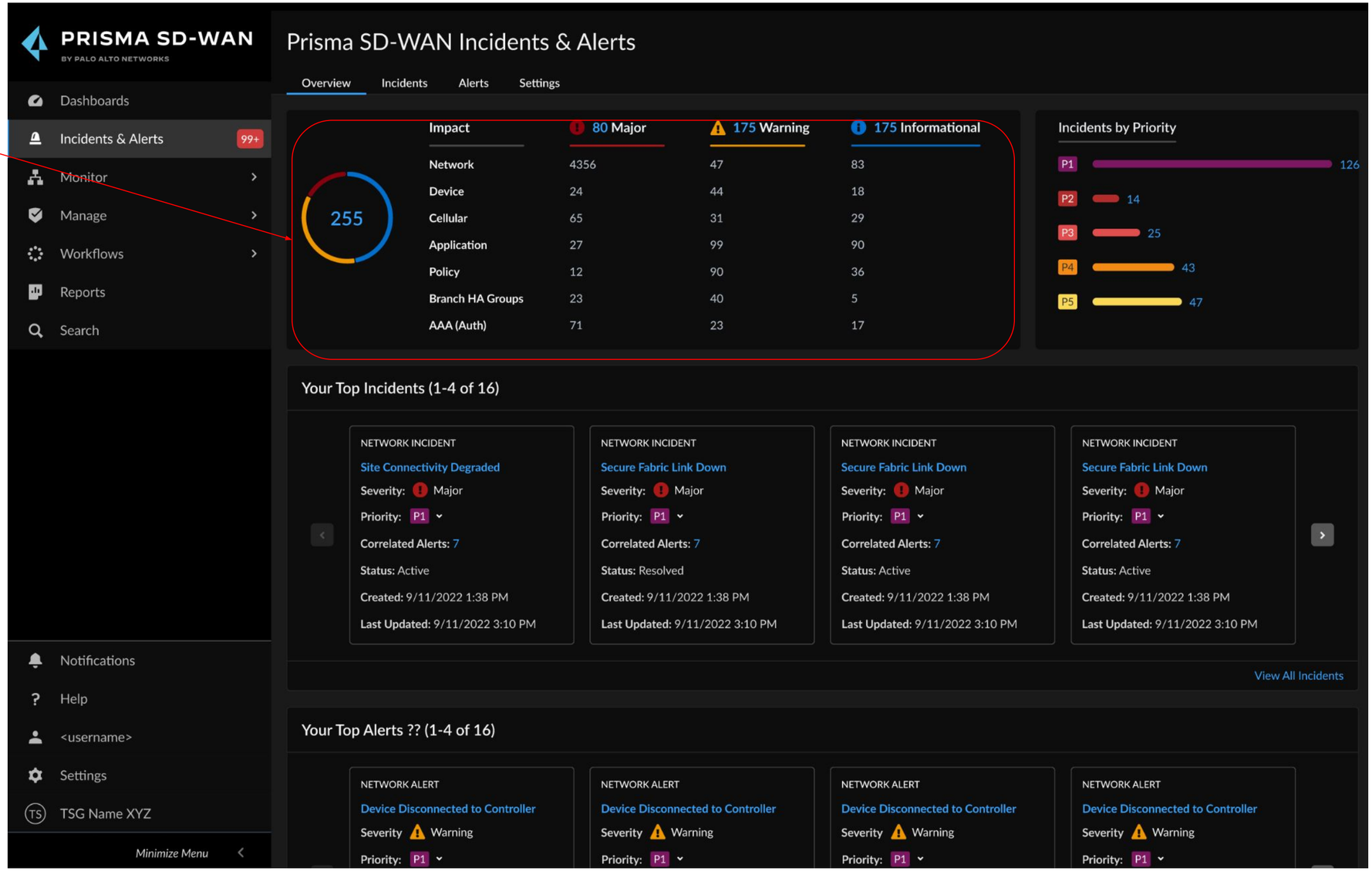
Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details



Events - Incidents

Severity Matrix

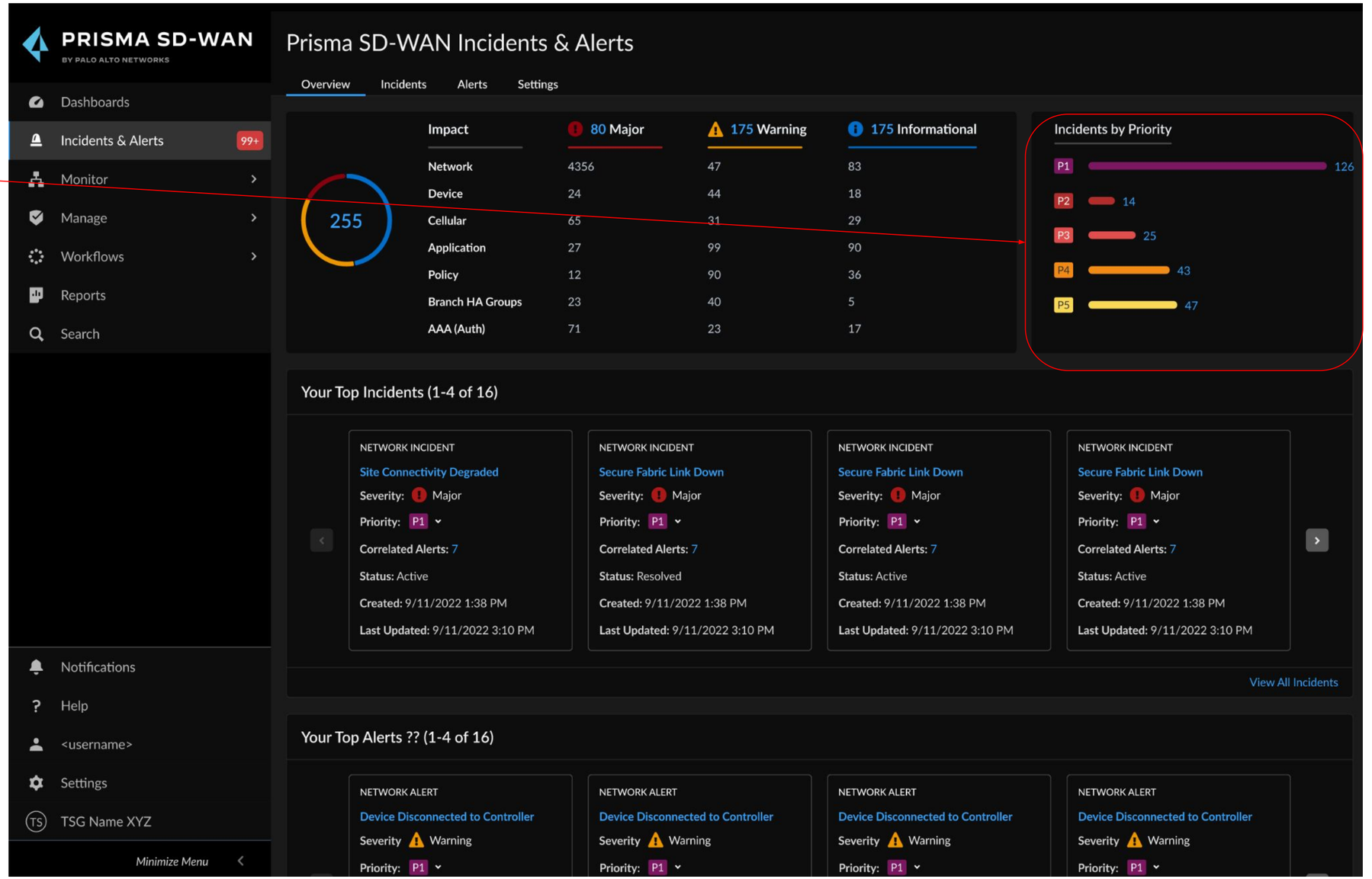
Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details



Events - NOW Incidents

Severity Matrix

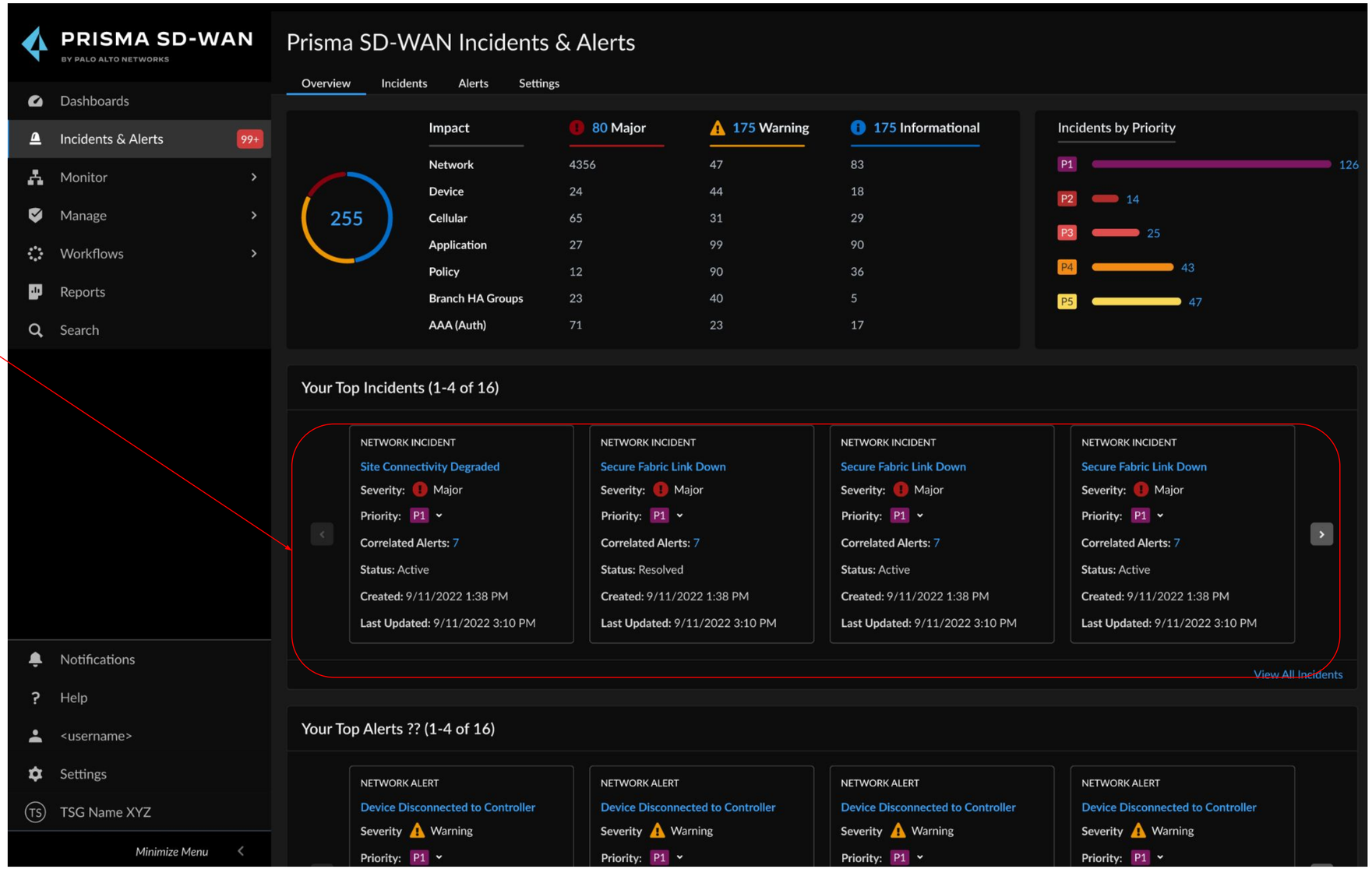
Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details



Events - Incidents

Severity Matrix

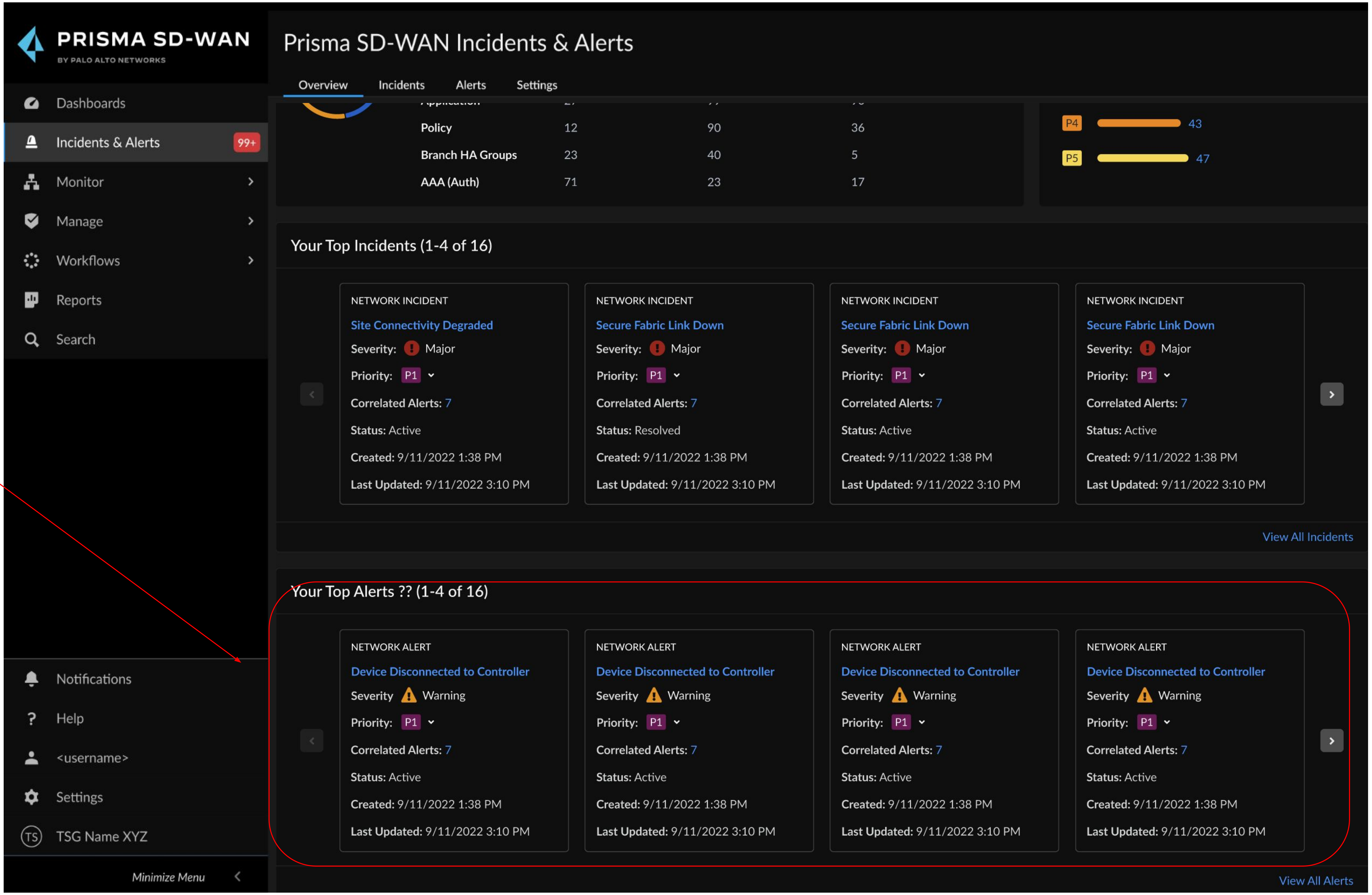
Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details



Events - Incidents

Severity Matrix

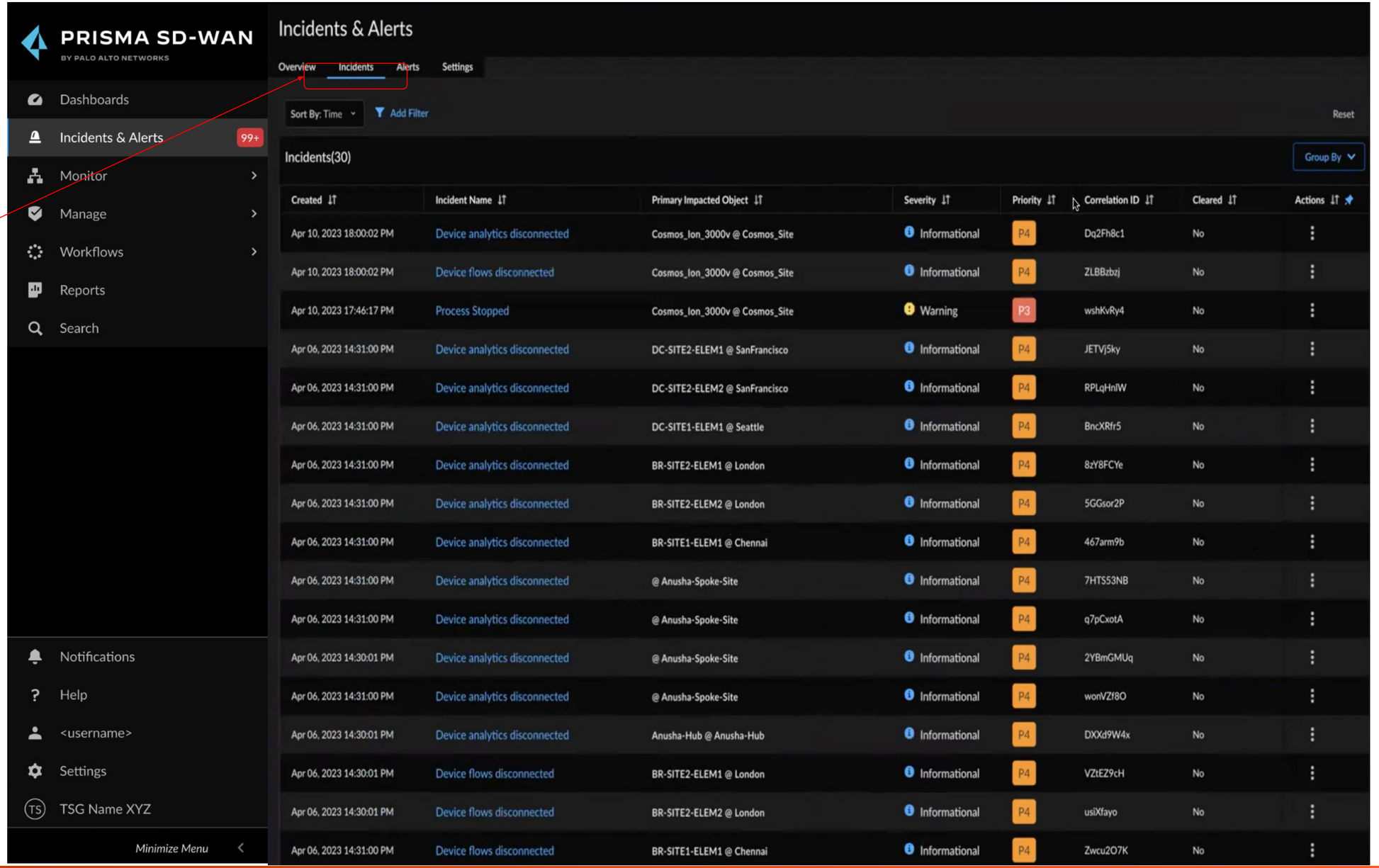
Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details



Events - Incidents

Severity Matrix

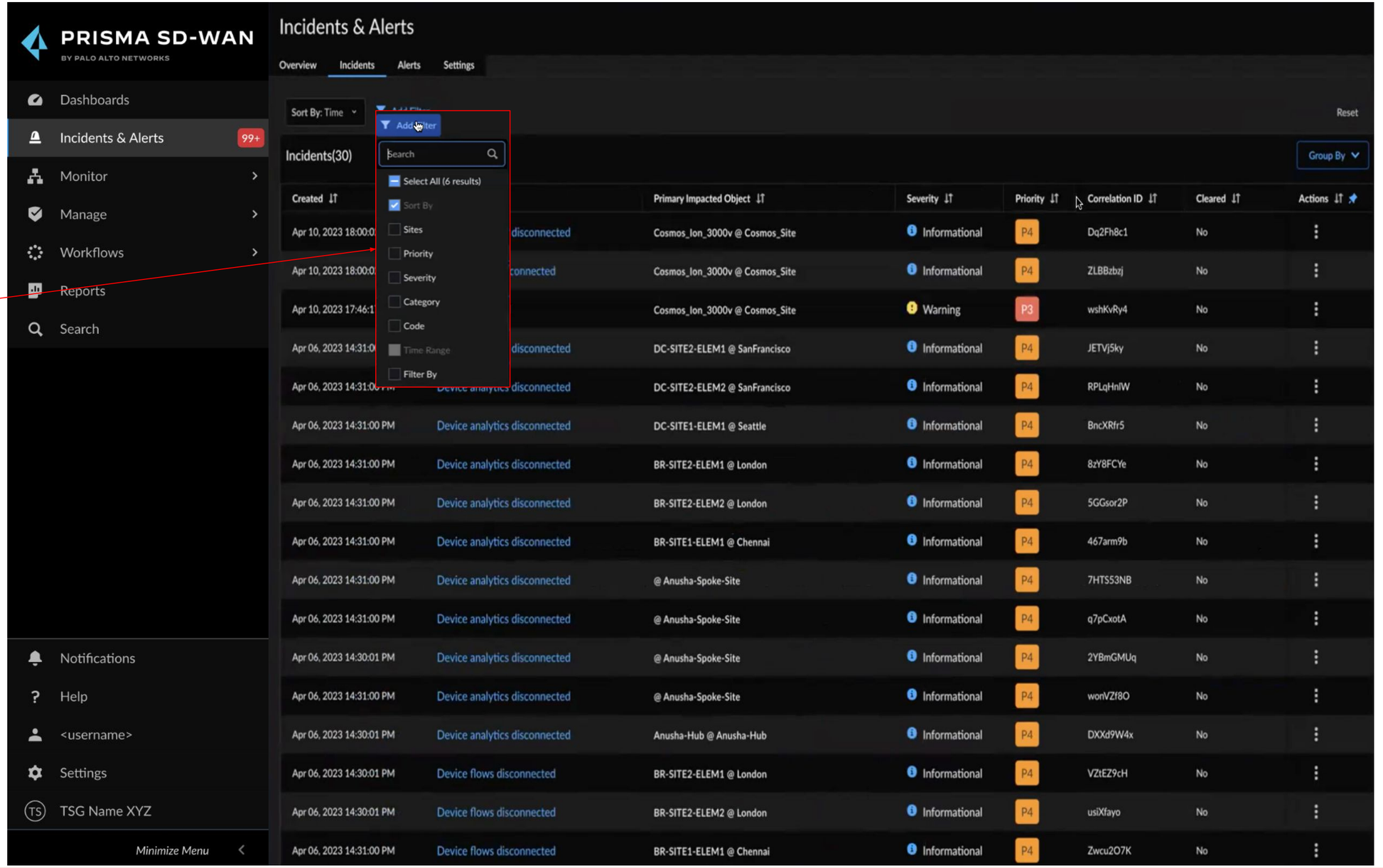
Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details



Events - Incidents

Severity Matrix

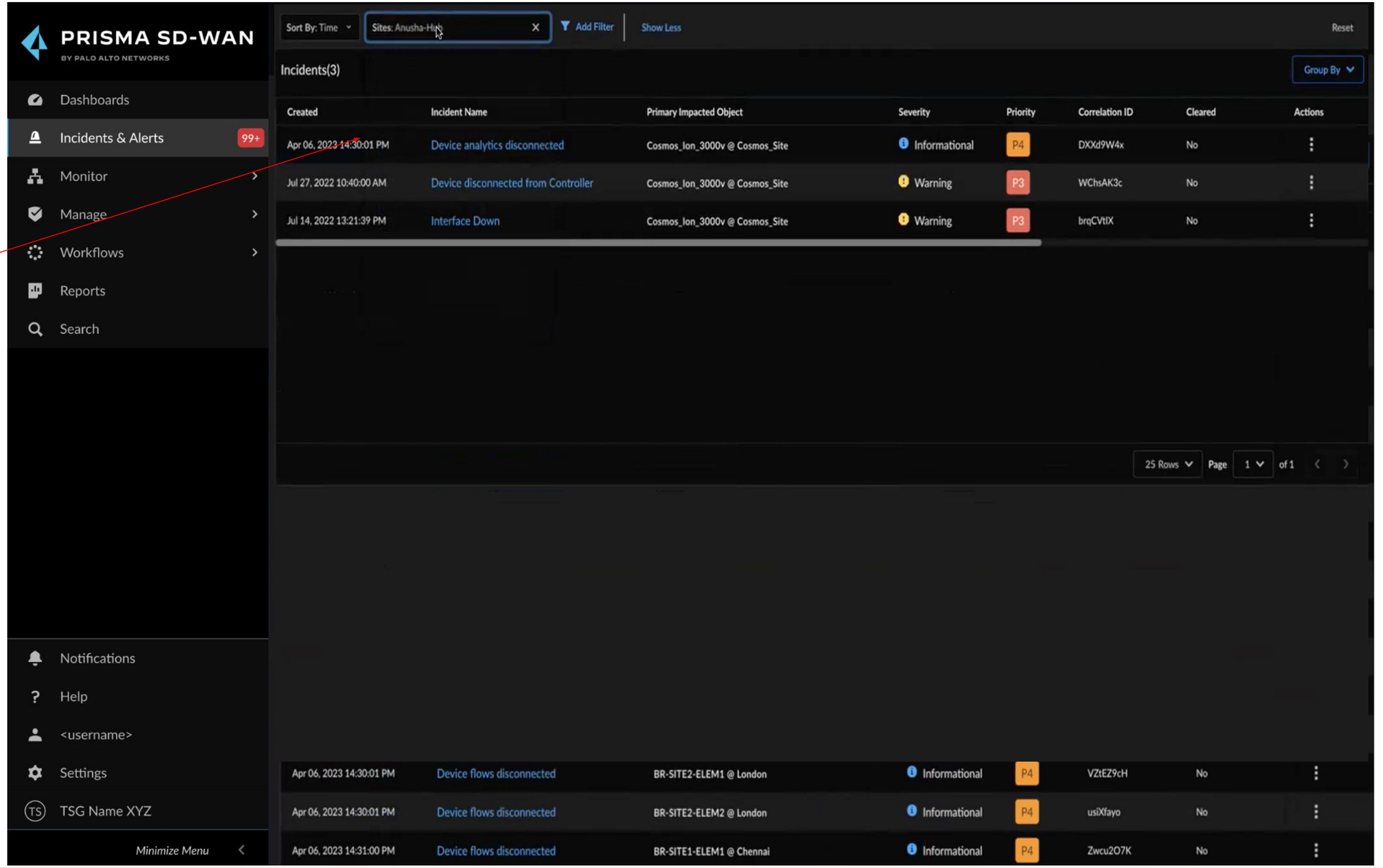
Priority Summary

Top Incidents

Top Alerts

Incident List

Incident Details



Events - Incidents

Severity Matrix

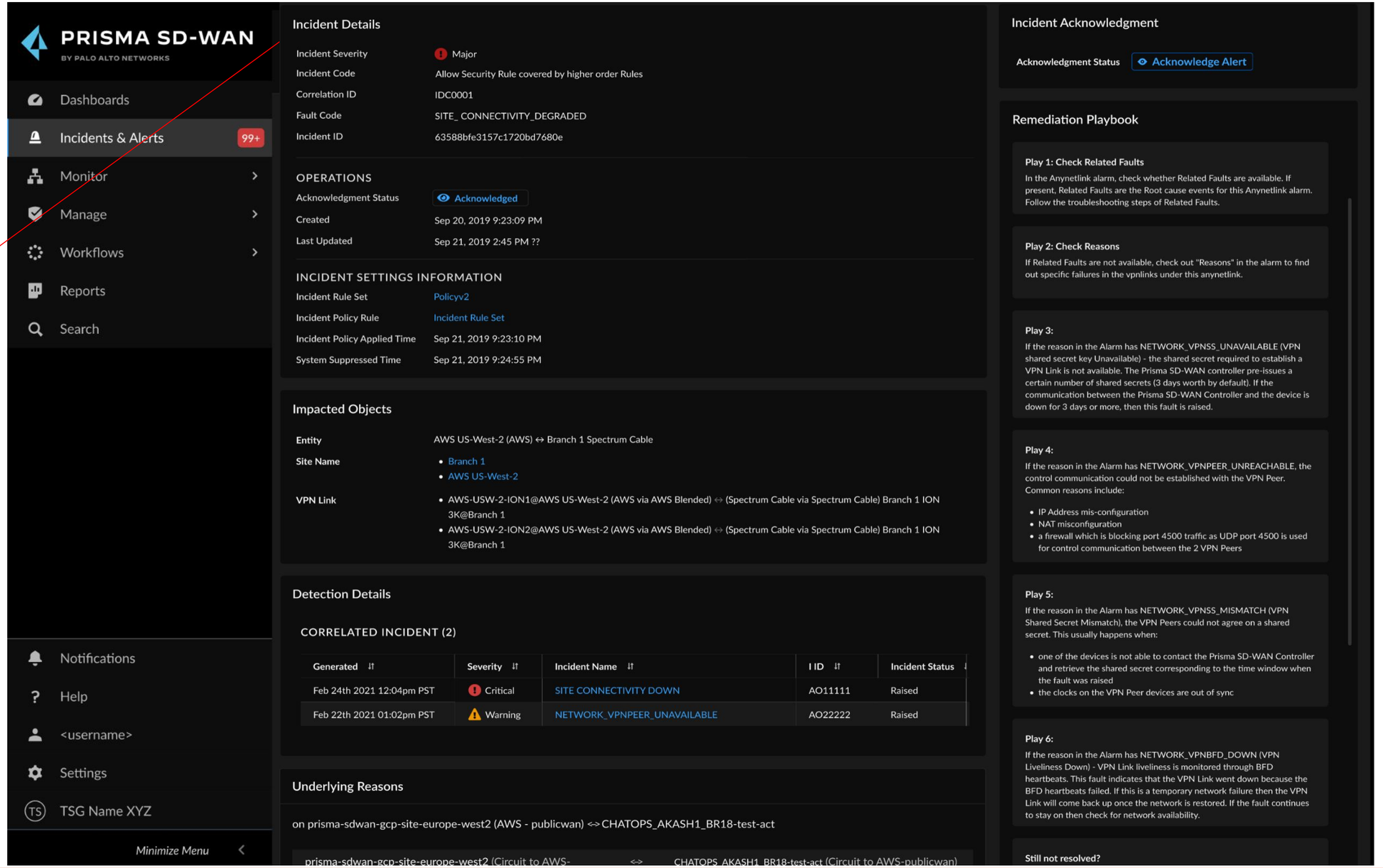
Priority Summary

Top Incidents

Top Alerts

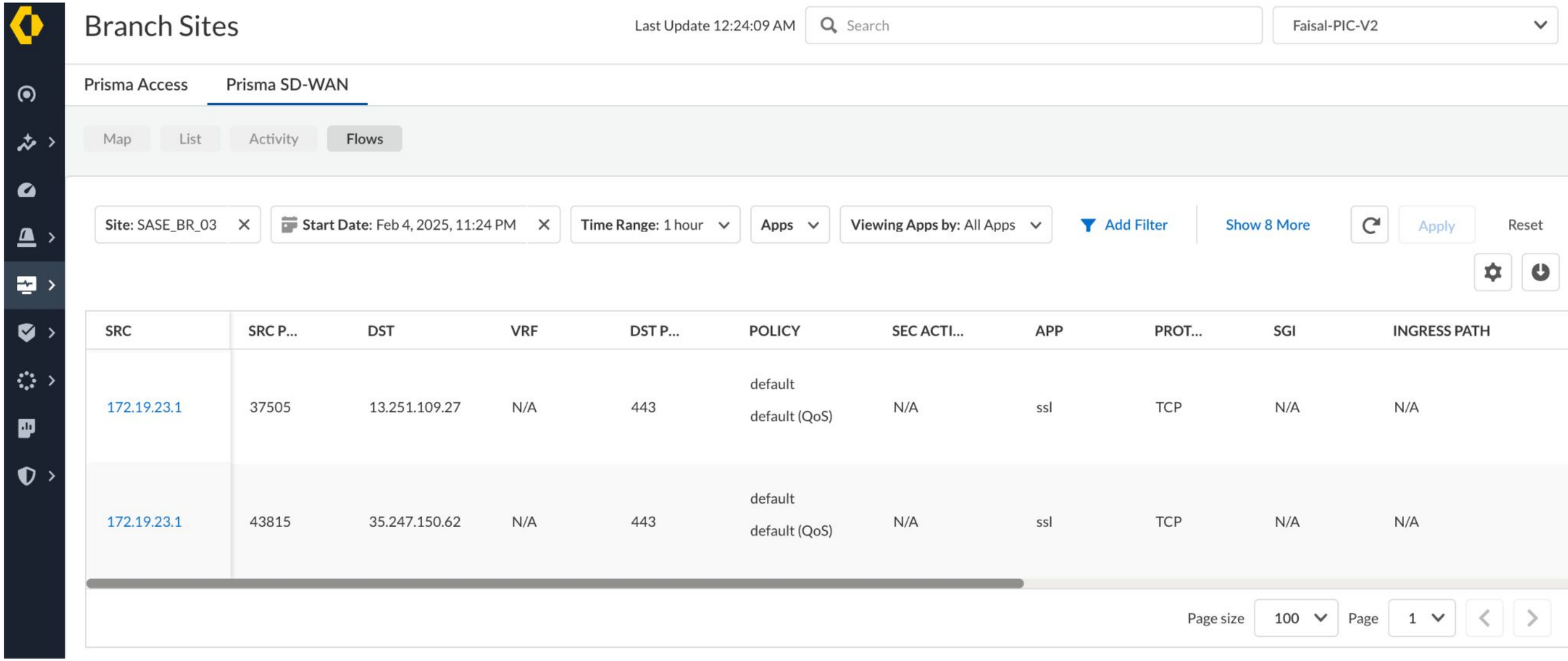
Incident List

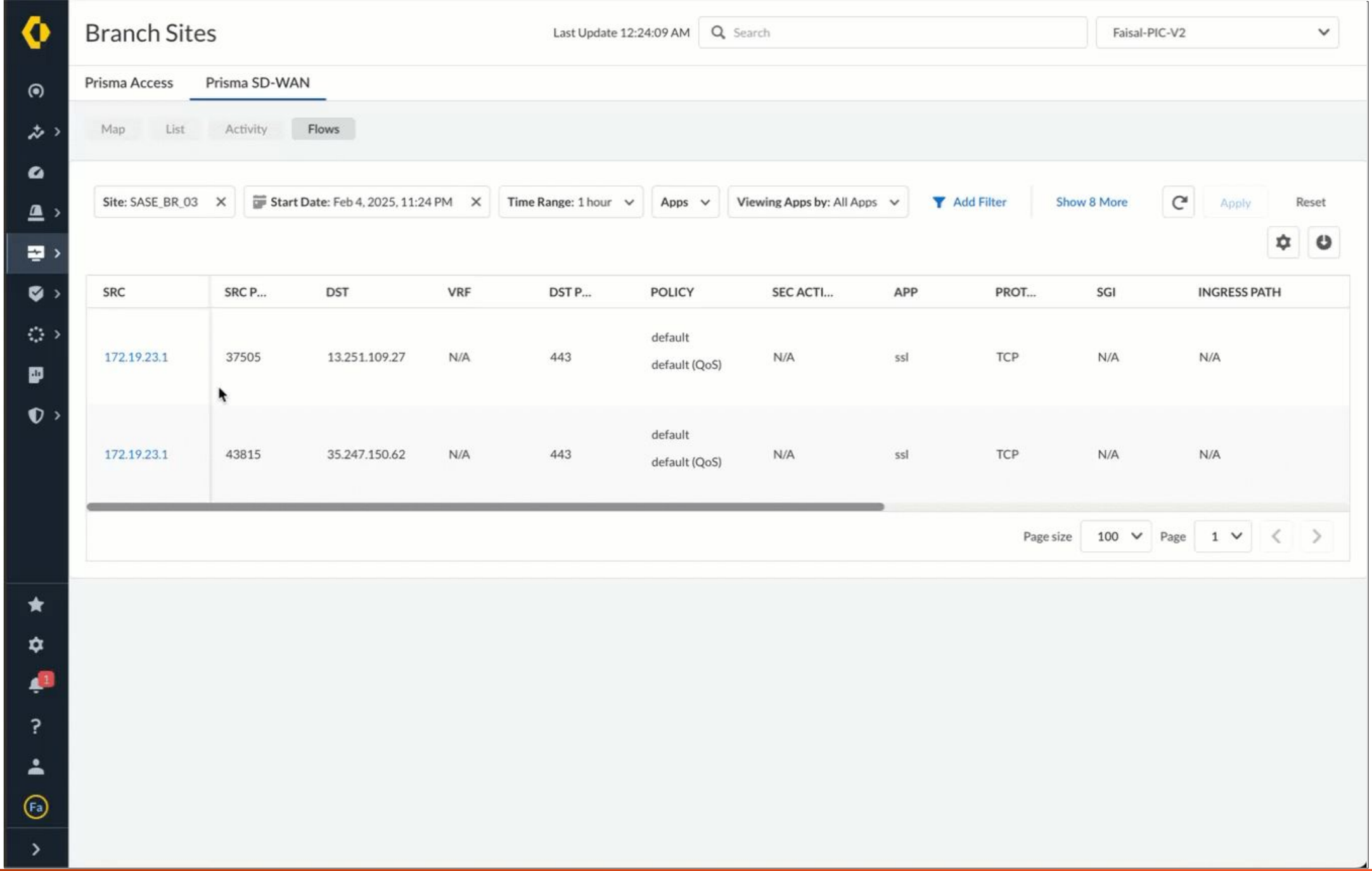
Incident Details



Flow Browser

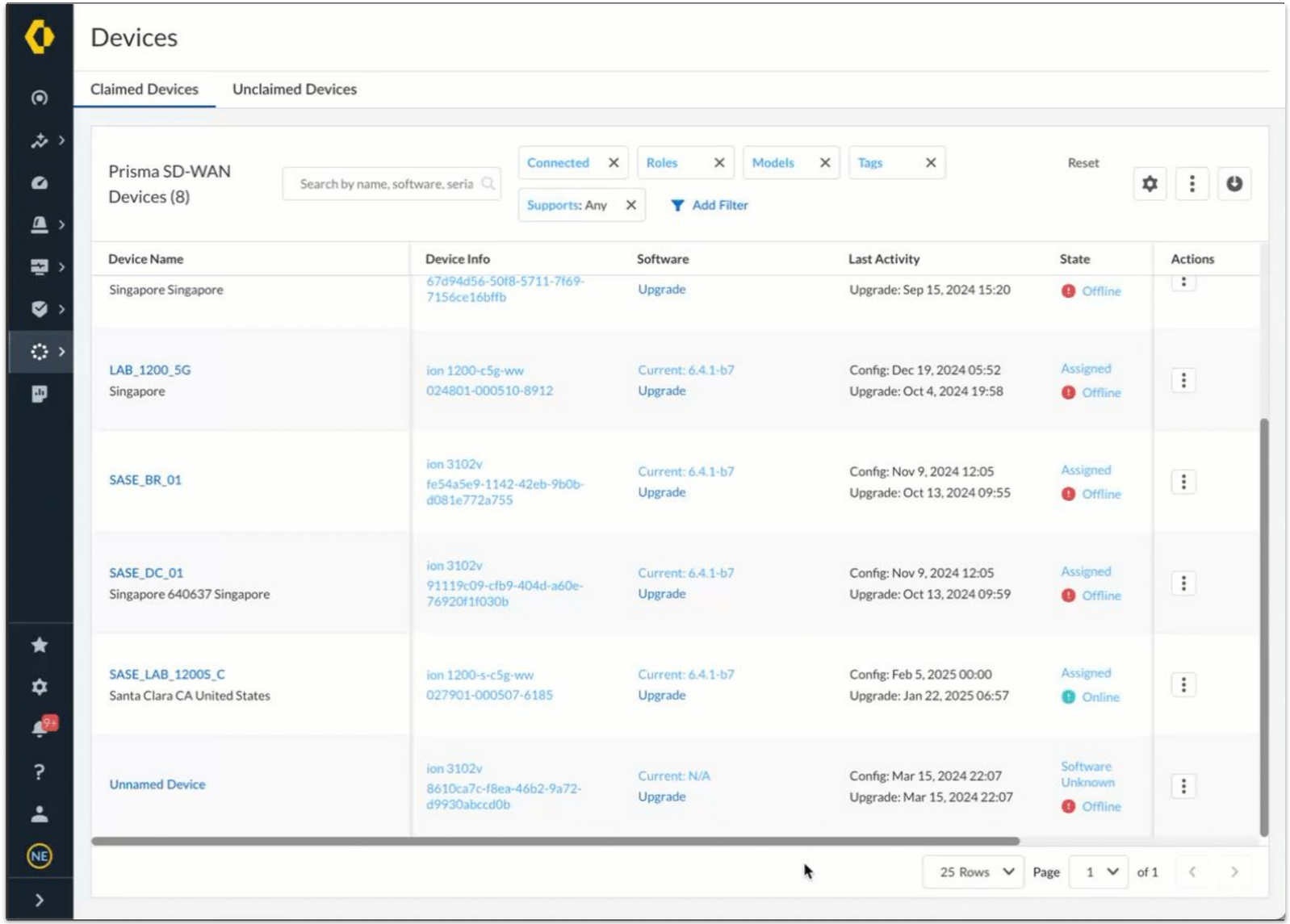
Flow Browser





RMA

RMA



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