Monitor & Notify (M&N) user guide

Author: Product Management

verizon business



Table of contents

1. Introduction: Monitor & Notify (M&N) Managed Network Service 3

2. Getting started: Device provisioning 4

   2a. Status types 5

   2b. Support resources 5

   2c. Device workflow status tab 6

3. Insights 6

   3a. Device health calculation metrics 6

   3b. Strategic health dashboards 7

   3c. Performance diagnostics and operational pillars 7

   3d. Automated remediation and response framework 8

4. Network monitoring 9

   4a. Sites overview 9

   4b. Devices overview 9

5. Security and compliance 12

6. REST APIs 13

7. FAQs 13

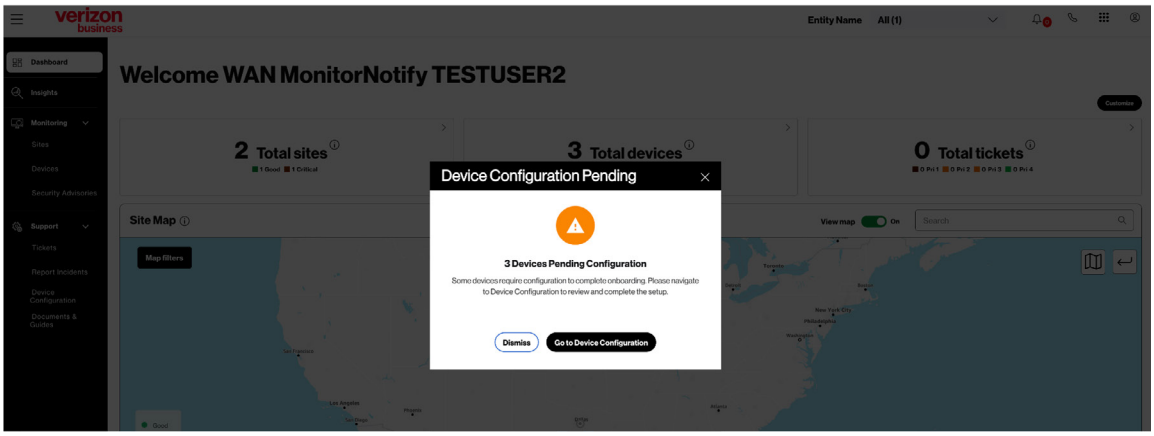
8. Glossary of terms 15



1. Introduction: Monitor & Notify (M&N) Managed Network Service

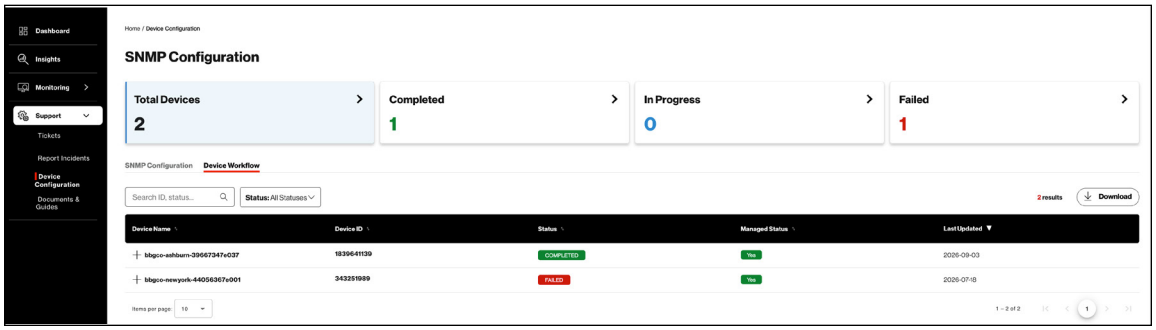
The Monitor & Notify (M&N) management level provides critical intelligence and real-time visibility for WAN devices. This service enables businesses to protect operations through enhanced performance reporting, actionable analytics and automated security advisories. By centralizing traffic visibility and self-service capabilities, M&N supports data-driven connectivity decisions and proactive infrastructure management.

2. Getting started: Device provisioning



To begin monitoring, navigate to the Support page to access the device configuration workflow. This process is essential for establishing analytics on your hardware:

1. A Verizon Engineer will be assigned to verify Customer Premise Equipment (CPE) details, including Make, Model, OS Version and WAN Interface IP.
2. Verizon generates a configuration snippet containing unique SNMP V3 configurations and Access Control Lists (ACLs) for management traffic. Verizon utilizes SNMP V3 protocols exclusively, eliminating the use of legacy SNMP V2 communities. Each hardware asset is secured with unique, Verizon generated credentials consisting of a 15-character alphanumeric string. Management traffic is further protected via SNMP V3 with AUTH (SHA) and PRIV (AES128) encryption standards. Configuration parameters are dictated by the specific management domain designated to each client. Within these domains, distinct PIP and INET management subnets are utilized, alongside additional subnets reserved for network platform management operations. Users are required to notify the Verizon Implementation Engineer should they necessitate the use of legacy SNMP V2 community strings.

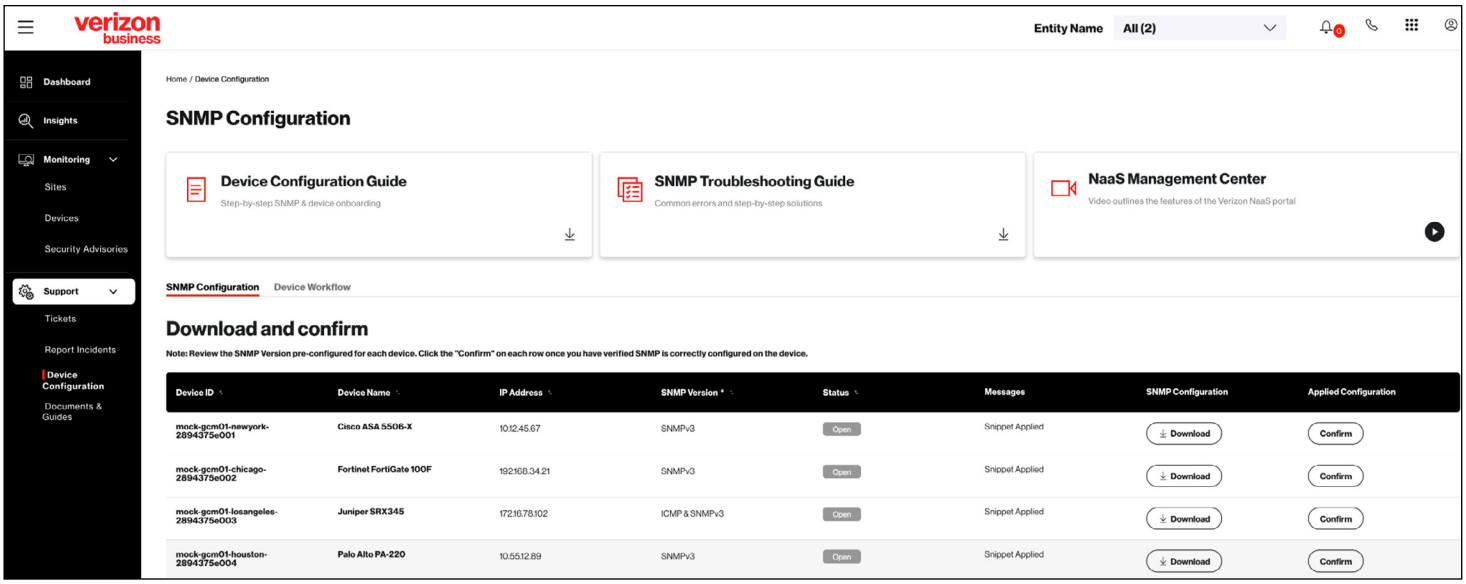


3. Users must apply this configuration patch to their devices and confirm deployment through the onboarding workflow.
4. Final testing and verification are performed before the product is moved to full deployment.
5. The Support documents at the top of the page provide information on how to configure your device, a NaaS portal user guide that explains all the elements in the portal and a short video tutorial.

Please note the “Confirm” button will be displayed until the user takes action to apply the community string and notifies Verizon once the configuration is applied.

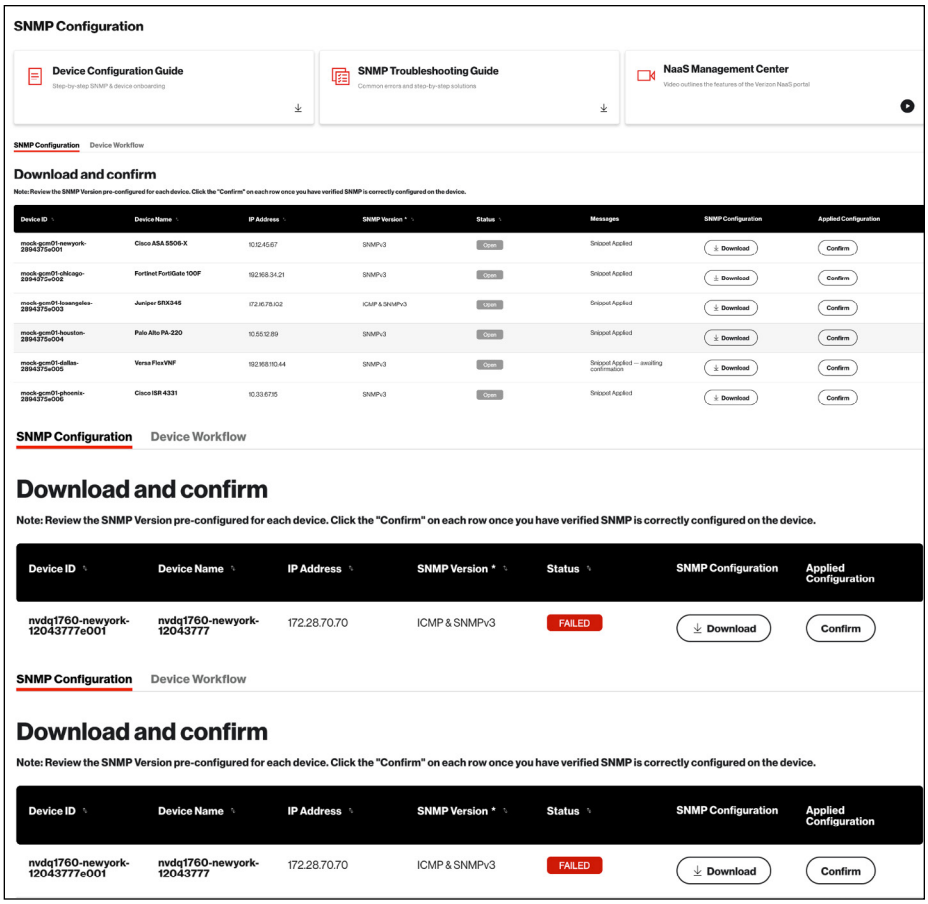
2a. Status types:

- **Open/Empty:** Indicates the configuration is ready to be applied by you on your device and after applying, you can inform Verizon by clicking the Confirm button for the device.
- **Progress:** Indicates the customer has clicked on Confirm button earlier but not all devices under this Order have been acted upon by the customer. The Confirm button will be greyed out during this status for that particular device.
- **Failed:** Indicates that Verizon is facing issues with internal systems after the you has already confirmed that he has applied the configuration. A Confirm button will be available for the customer to signal completion again after discussion with Verizon contact.



2b. Support resources

The Support page provides access to comprehensive documentation, user guides and a centralized hub for repository of all guidelines and documents.



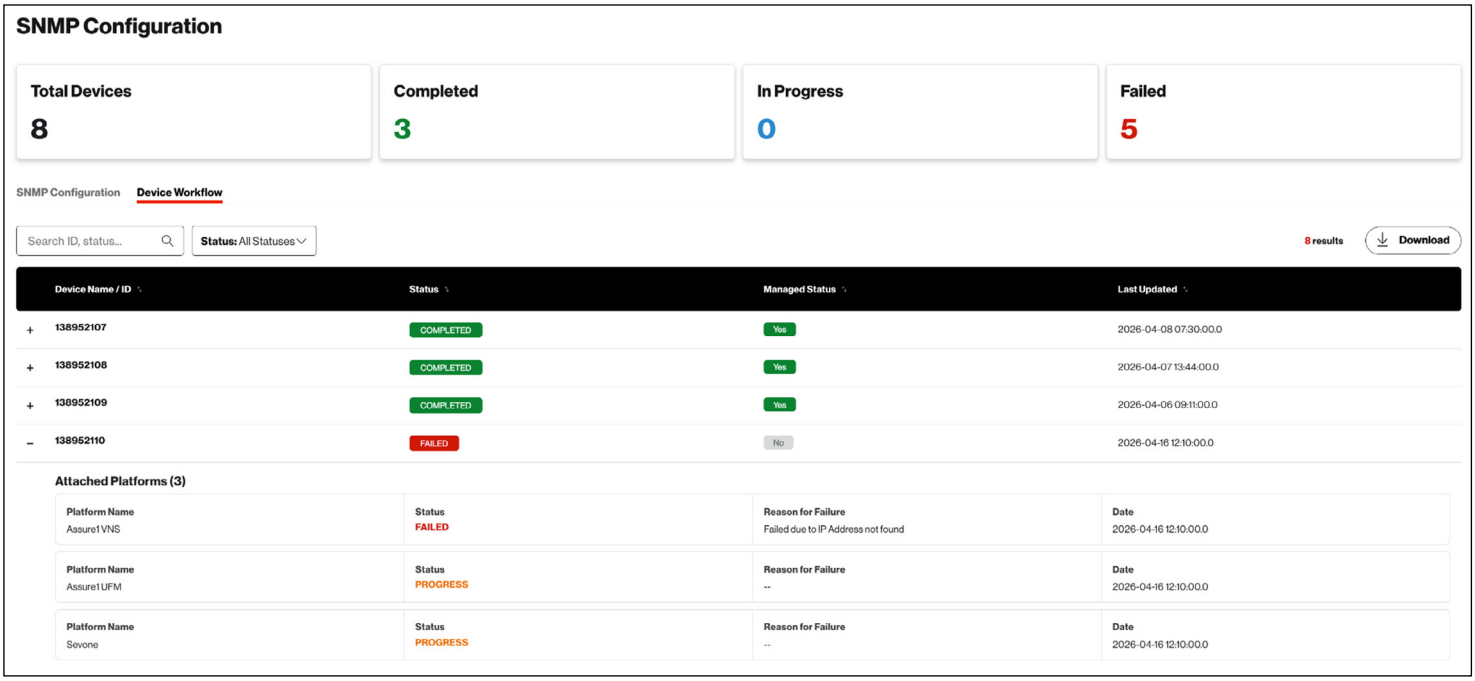
2c. Device workflow status tab

Status types:

- **Completed:** Indicates the configuration is successfully recorded in the Verizon inventory system.
- **Progress:** Indicates the configuration application is currently underway.
- **Failed:** Indicates that Verizon identified issues after the user applied the configuration. Verizon will work with the customer to fix identified issues.

Managed status:

- Yes – The device has passed all validation and is now considered as Managed device with Monitor & Notify service level.
- No – The device has not passed all validations and is not yet considered Managed.



3. Insights

The Insights section provides a clear, data-driven view of your network's performance. You can use these tools to proactively manage your infrastructure:

- Router Health Dashboard: Quickly identify which devices are performing optimally and which need attention. The dashboard features a WAN Health Status widget at the top for an immediate summary.

3a. Device health calculation metrics

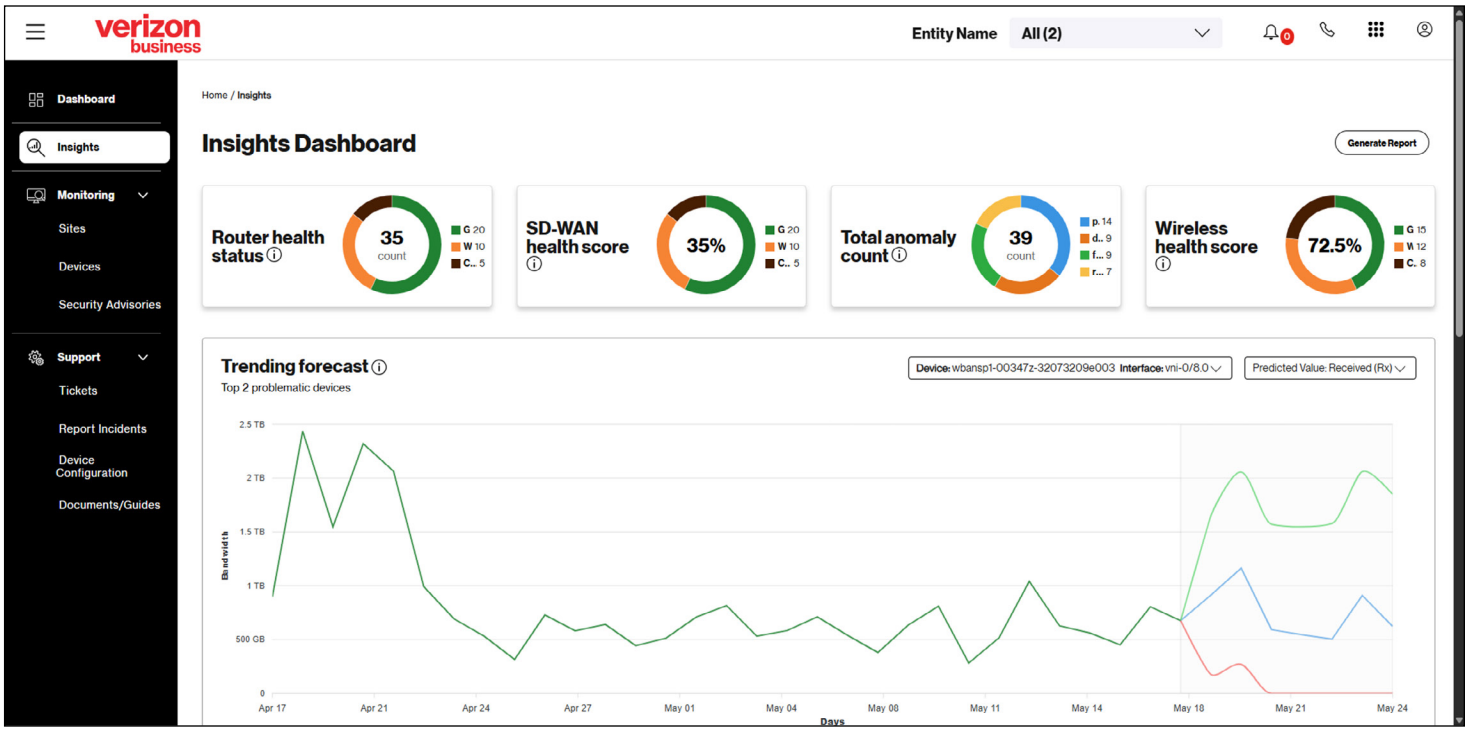
To determine the router's overall health, the system evaluates the following metrics from each poll:

Metric	Measurement method	Good (green)	Warning (yellow)	Critical (red)
Tx Bandwidth	Max (In %, Out %)	< 70%	71–85%	> 85%
Rx Bandwidth	Max (In %, Out %)	< 70%	71–85%	> 85%
Errors	Errors per sec	0	> 0	> 5
Discards	Discards per sec	0	> 0	> 10
Reachability	SNMP status – poll every 5 minutes	Yes	Unreachable on last poll	Unreachable for 2+ polls

Health status logic:

The Status is calculated for the router health. The dashboard uses a “rollup” methodology to aggregate these metrics into a single device status:

- **Critical:** Any single metric reaches the Critical threshold.
- **Warning:** No critical failures, but one or more metrics indicate a Warning state.
- **Good:** All metrics are within standard operating ranges.
- **Trending and forecasting:** View 30 days of historical data and see 7-day performance predictions to help you stay ahead of capacity needs. You can use the Predictive Value dropdown to toggle between Received (RX) and Transmitted (TX) data. Predictions include an Upper Bound (UB) and Lower Bound (LB) for bandwidth utilization, helping identify the 20 interfaces expected to grow the fastest.



- **NOC reports:** Generate detailed, historical reports to support capacity planning and technology investment decisions.

NOC reports: Generate detailed, historical reports to support capacity planning and technology investment decisions. Here is the executive-level breakdown of the report's structure and contents:

3b. Strategic health dashboards

- The report commences with high-level summaries providing executive leadership with an immediate pulse on infrastructure integrity:
- **Overall circuit health:** Delivers a macroscopic evaluation of the network by categorizing circuits into intuitive Good, Warning or Critical operational states.
- **Consolidated action table:** Functions as a live operational dashboard, quantifying sites triggering alerts across four essential domains: Reachability, bandwidth, anomalies and physical integrity.

3c. Performance diagnostics and operational pillars

- To facilitate granular troubleshooting, the report utilizes specialized time-series analytics across designated historical periods:
- **Node reachability:** Benchmarks uptime against a rigorous 95.0% baseline, leveraging line charts to isolate availability dips and performance degradation.
- **Link capacity and utilization:** Correlates throughput with active user density, enabling engineers to differentiate between legitimate traffic spikes and background management tasks.
- **Physical integrity and interface health:** Employs stacked area charts to monitor error and discard rates, distinguishing between internal Customer Edge (CE) hardware issues and Verizon Provider Edge (PE) drops.

3d. Automated remediation and response framework

- The core of the reporting suite is an automated recommendation ledger, mapping breached thresholds directly to actionable technical protocols:
- Bandwidth utilization (TX/RX)
  - Elevated Utilization peaks that correlate with standard business hours, suggesting the current provisioned capacity is no longer sufficient for peak loads.
    - **Warning (71-85%):** Initiate temporary traffic shaping and flag for immediate capacity assessment.
    - **Critical (>85%):** Implement permanent traffic controls and proceed with urgent circuit upgrades.
- Customer Edge (CE) quality
  - A low volume of errors on the CE interface was observed. This could indicate minor physical layer imperfections or transient interface issues.
    - **Warning (>0 minor errors):** Maintain surveillance for transient congestion or intermittent drops.
    - **Critical (>5 errors/10 discards):** Mandate physical layer audits, verify MTU consistency and replace SFP components.
- Verizon Edge (PE) quality
  - This information is provided to offer visibility into the Verizon network edge, which is proactively monitored and maintained by Verizon to ensure service integrity.
    - **Warning (>0 errors):** Monitor provider boundary performance and escalate to Verizon NOC if persistent.
    - **Critical:** Execute carrier escalation protocols to ensure strict SLA compliance.
- Node reachability
  - A brief interruption in availability from the Verizon performance monitoring servers. This could be a result of network path changes or a brief interruption in power.
    - **Warning (Single failed poll):** Verify local power status and recent routing updates.
    - **Critical (2+ failed polls):** Initiate high-priority circuit diagnostics and audit SNMP/firewall configurations.

Essentially, the report is designed to remove the guesswork, providing a scannable operational review for leadership while handing engineers an explicit checklist to remedy network degradation before it impacts the broader business.

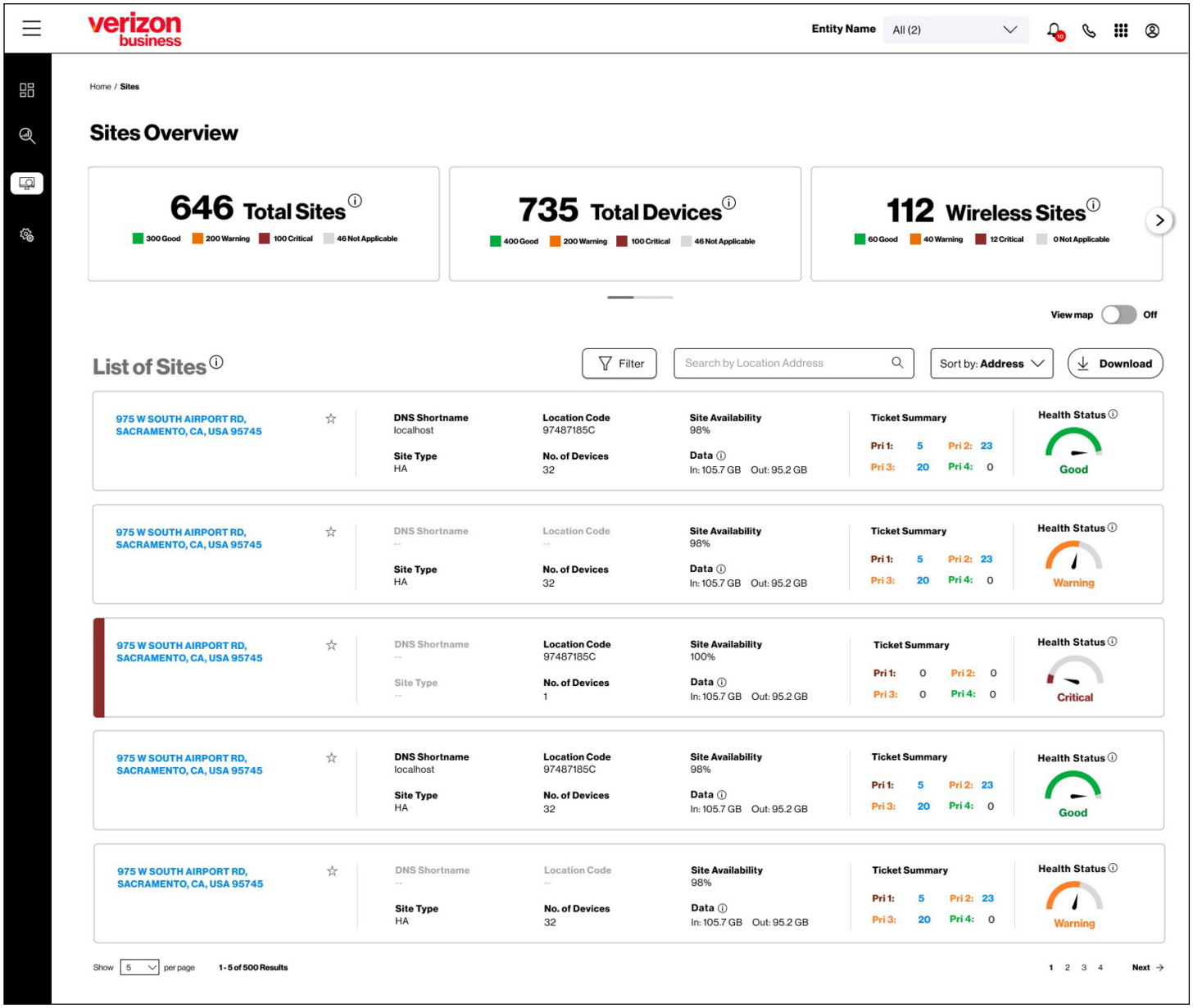


4. Network monitoring

4a. Sites overview

The Sites page provides a consolidated view of physical network locations. Key features include:

- **Health Summary widget:** Uses “weakest link” logic to aggregate SD-WAN performance, reachability and active tickets into a status of Good, Warning, Critical or Not Available.
- **Ticket Summary widget:** Provides a real-time snapshot of pending issues segmented by priority (P1–P4).

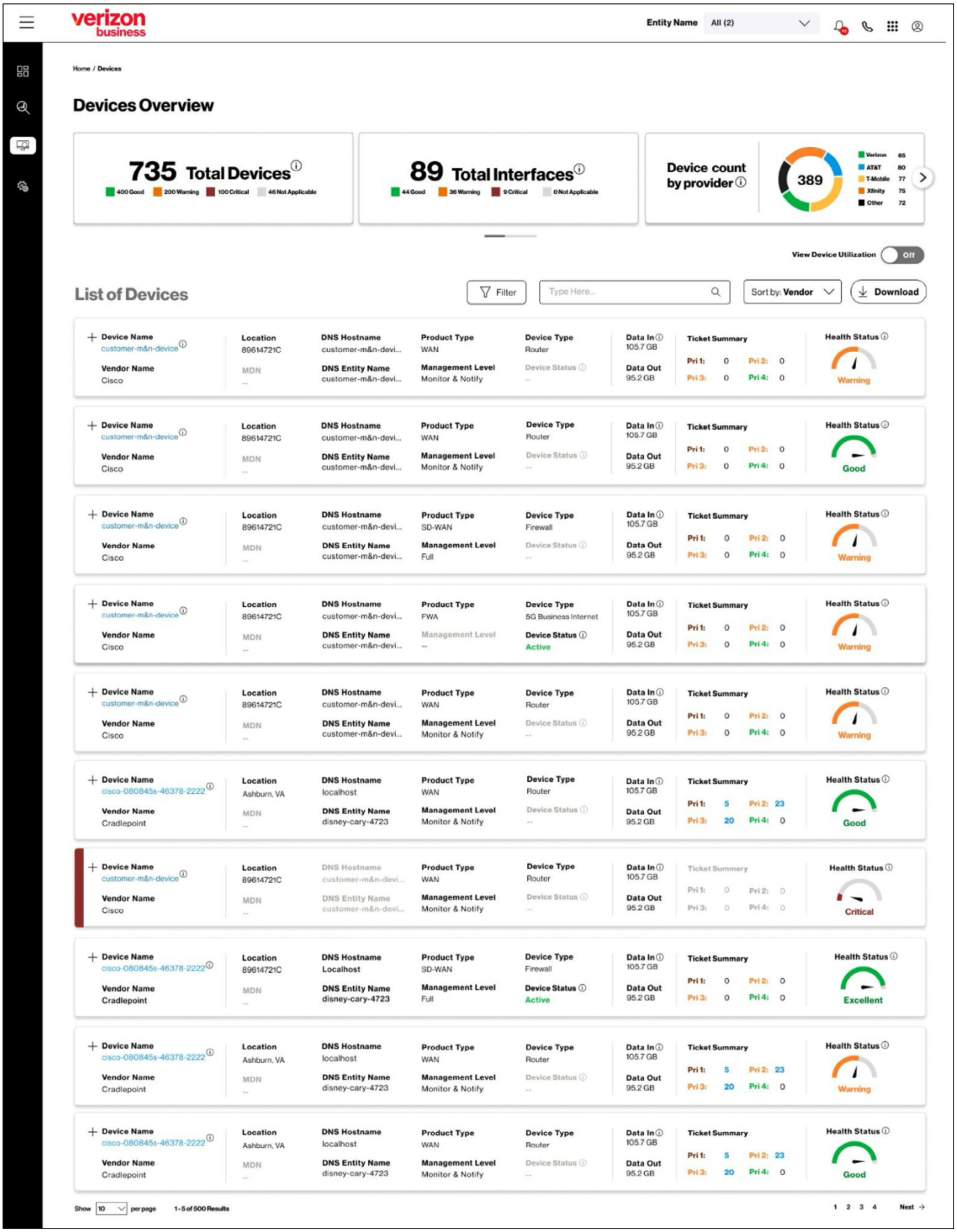


4b. Devices overview

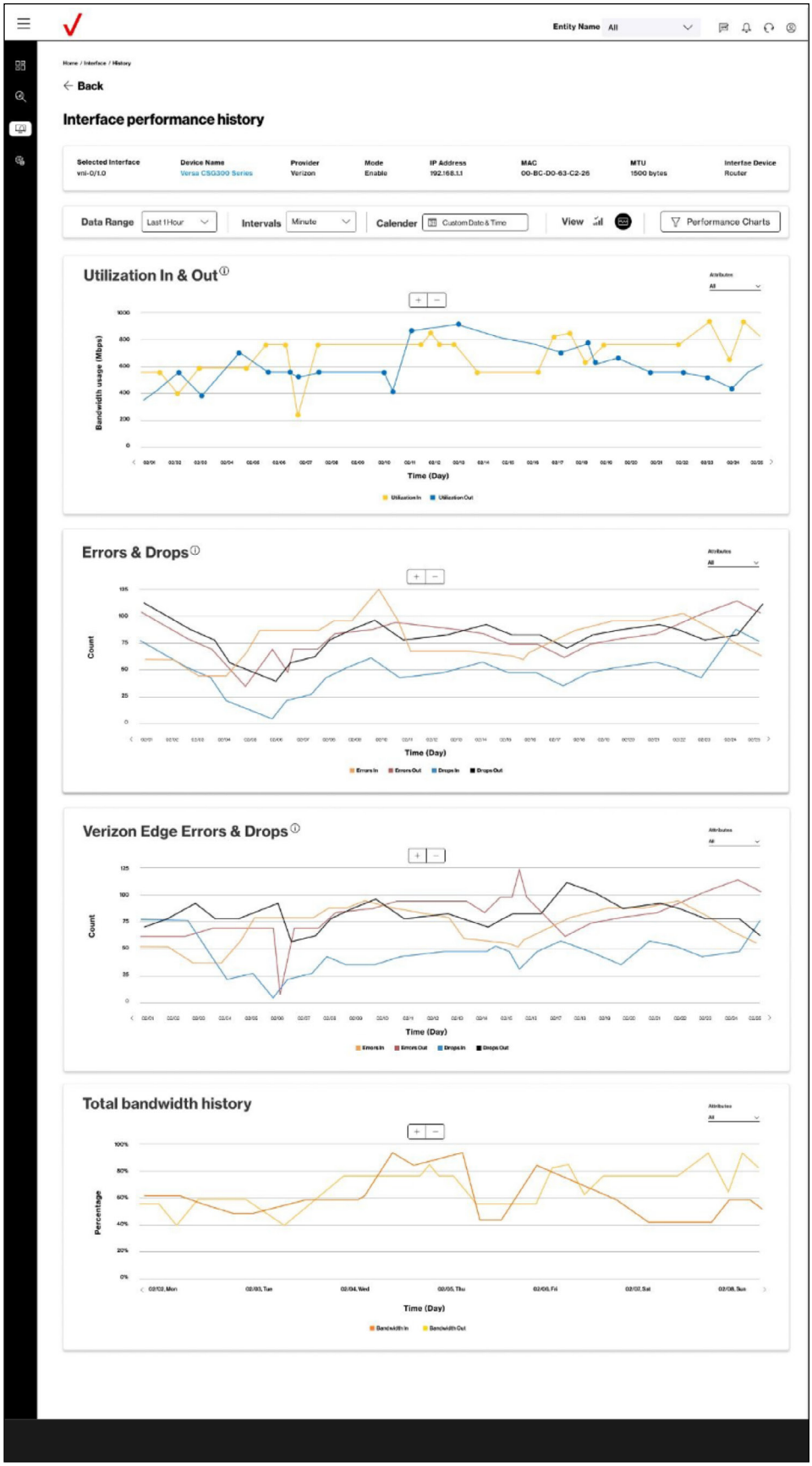
The Devices Overview acts as a centralized dashboard for network inventory. Users can filter assets by Device Type, Management Level, Status or Account ID. Selecting an asset unlocks granular performance charts, including:

- **Utilization:** This metric leverages time-series line charts tracking inbound and outbound data rates over time to instantly isolate traffic spikes from standard off-peak patterns, automatically flagging ports that breach predefined warning (71–85%) or critical (>85%) capacity thresholds.
- **Health metrics:** This visualization utilizes color-coded stacked area charts to differentiate inbound and outbound packets per second, allowing operators to immediately isolate internal Customer Edge (CE) hardware buffer issues from Verizon Provider Edge (PE) network drops.

- **Availability and reachability:** This timeline tracks operational uptime against a strict 95.0% baseline – dynamic color-coding instantly highlights dips into the red – to generate a real-time site health score categorized as Good, Warning or Critical based on consecutive polling failures.



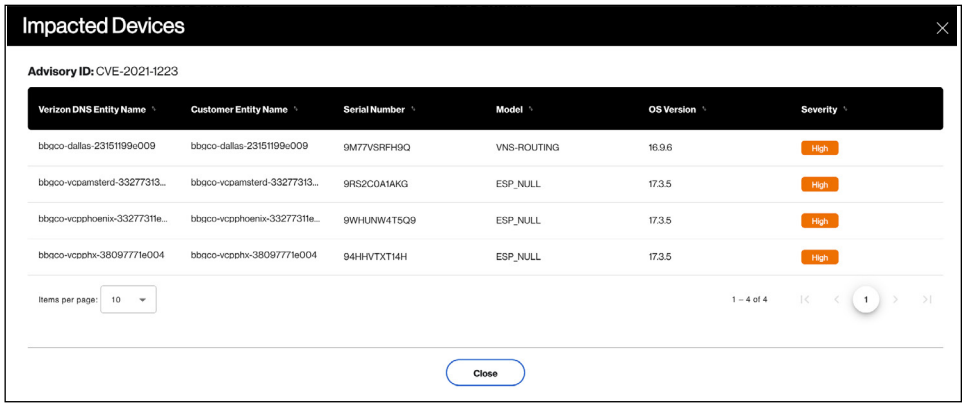
Click of the + sign on Device Name to expand the Interface statistics:

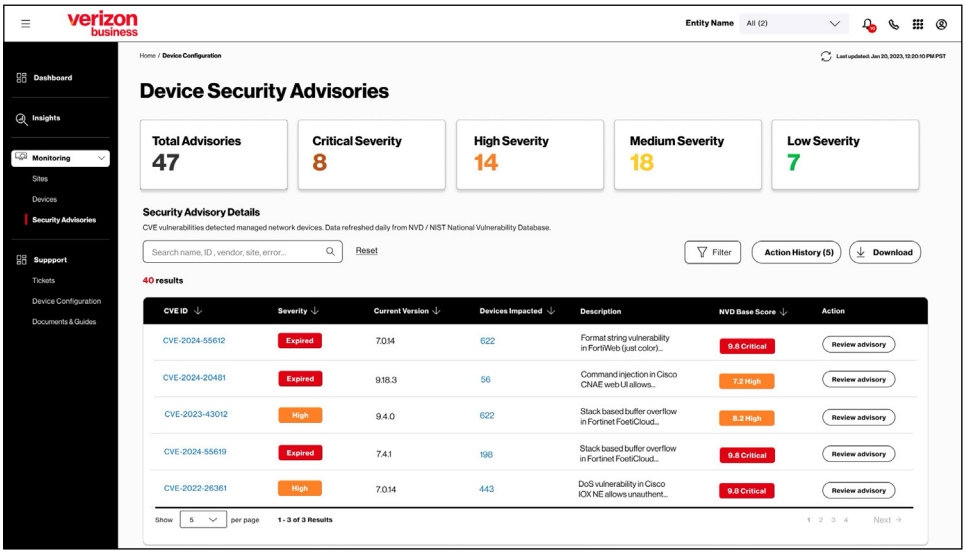


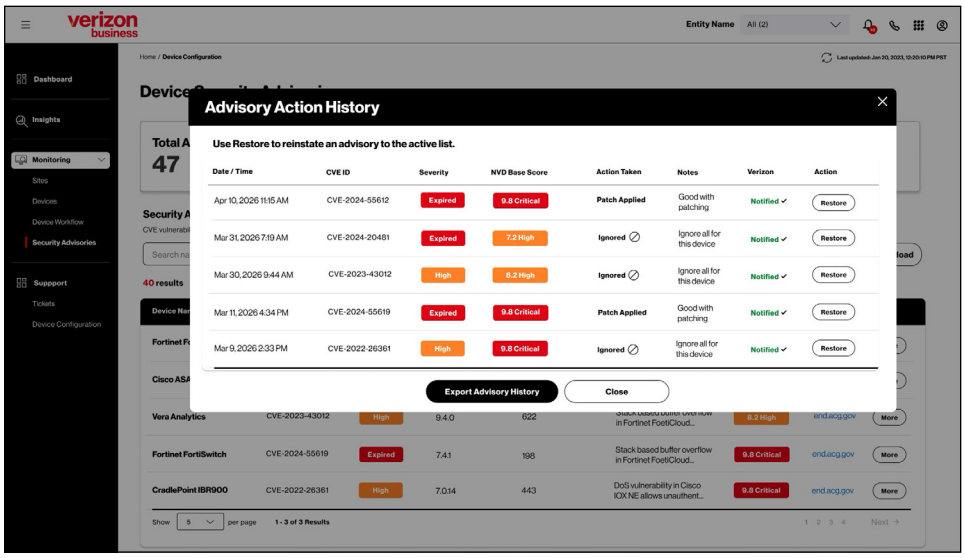
5. Security and compliance

The Security Advisories page automates threat tracking by linking WAN router vulnerabilities directly to the NIST National Vulnerability Database (CVE/CVSS). Verizon's feed is hourly and available in the NaaS Management Center at this interval. This establishes a proactive defense strategy through:

- **Prioritization:** Severity alerts allow users to instantly identify high-risk threats.
- **Acknowledge and update:** Users click "Review Advisory" to acknowledge vulnerabilities and update the state once patches or firmware updates are applied.
- **Audit trail:** The "Action History" provides a historical record of all remediation steps taken.







6. REST APIs

REST APIs are provided for customers that wish to integrate the data associated with their service directly into their own applications. The corresponding documentation is available through the Verizon API First Hub. The documentation for the AI Ops specific APIs can be found here. Security protocols: Connectivity via the API First Hub mandates OAuth2-based authentication. Users must utilize their designated credentials. The API First ecosystem utilizes OAuth2-based authentication protocols. Following the submission of valid credentials (username and secret), the system generates a Bearer token required for all subsequent API Endpoint queries. During this transaction, the Apigee management layer transparently swaps the OAuth2 token for a JWT variant that embeds the user's unique Team ID to secure the session. To maintain service integrity, standard rate limits are currently capped at 300 transactions per hour. The API catalog supports a diverse range of endpoint categories, including Site, Device, Interface and Tunnel configurations, alongside advanced analytics such as TSF, NHS and WHS metrics. Typical operational use cases include retrieving detailed, device-specific performance telemetry via the "Get Device Performance" endpoint.

Note: Beyond registering to access API First, a support ticket will also need to be raised to obtain access to access the AIOps APIs specifically.

7. FAQs

Q: How do I apply the configuration snippet to my device during onboarding?

A: During the Device Provisioning phase, you will download a configuration snippet containing unique SNMP configurations and Access Control Lists (ACLs). To apply this you must log into your specific device's Command Line Interface (CLI) or management portal and paste the configuration. For detailed, step-by-step instructions tailored to your device type, please refer to the Device Configuration Guide located in the Support documents section of the portal.

Q: What does "weakest link" logic mean in the Sites Overview Health Summary?

A: The "weakest link" logic means that a site's overall health status is determined by its most severe active issue. For example, if a site has 32 devices and 31 are in "Good" health, but one device triggers a "Critical" alert, the entire site's status will reflect as "Critical" until that specific device's issue is resolved.

Q: My device shows a "Critical" status for reachability. What does this mean?

A: Reachability is determined by SNMP polling at five minute intervals. If a device is unreachable for a single poll, it goes into a "Warning" state. If the device remains unreachable for 2 or more consecutive polls, it transitions to a "Critical" state.

Q: How should I respond if my device shows high Errors or Discards in the Insights dashboard?

A: This depends on where the errors are occurring:

- **Customer Edge (CE) errors/discards:** High errors or discards on your equipment often indicate internal switch-buffer exhaustion or mismatched interface speeds. You should schedule a physical layer audit of your cables and transceivers, and verify your MTU settings.
- **Verizon Edge (PE) errors/discards:** The portal provides visibility into the Verizon Provider Edge (PE) as a courtesy. Verizon proactively monitors these interfaces to ensure optimal traffic flow. If you notice a consistent increase in errors on the Verizon Edge, please raise a ticket with the Verizon NOC for further troubleshooting.

Q: Does Verizon automatically apply patches for the vulnerabilities shown in the Security Advisories tab?

A: No, Verizon does not automatically patch your devices. The Security Advisories page automatically links your device inventory to the NIST National Vulnerability Database to proactively alert you of threats. It is your responsibility to review the advisory, apply the necessary firmware update or patch and then click "Review Advisory" in the portal to log the action you took (e.g., "Patch Applied" or "Ignored").

Q: I want to integrate this data into my own applications. How do I get API access?

A: You can use our REST APIs to integrate AIOps data. First, you must register for access through the Verizon API First Hub. Once registered, you must raise a support ticket to request specific access to the AIOps APIs.

Q: I don't see all our sites or devices listed in the portal. How do I resolve this?

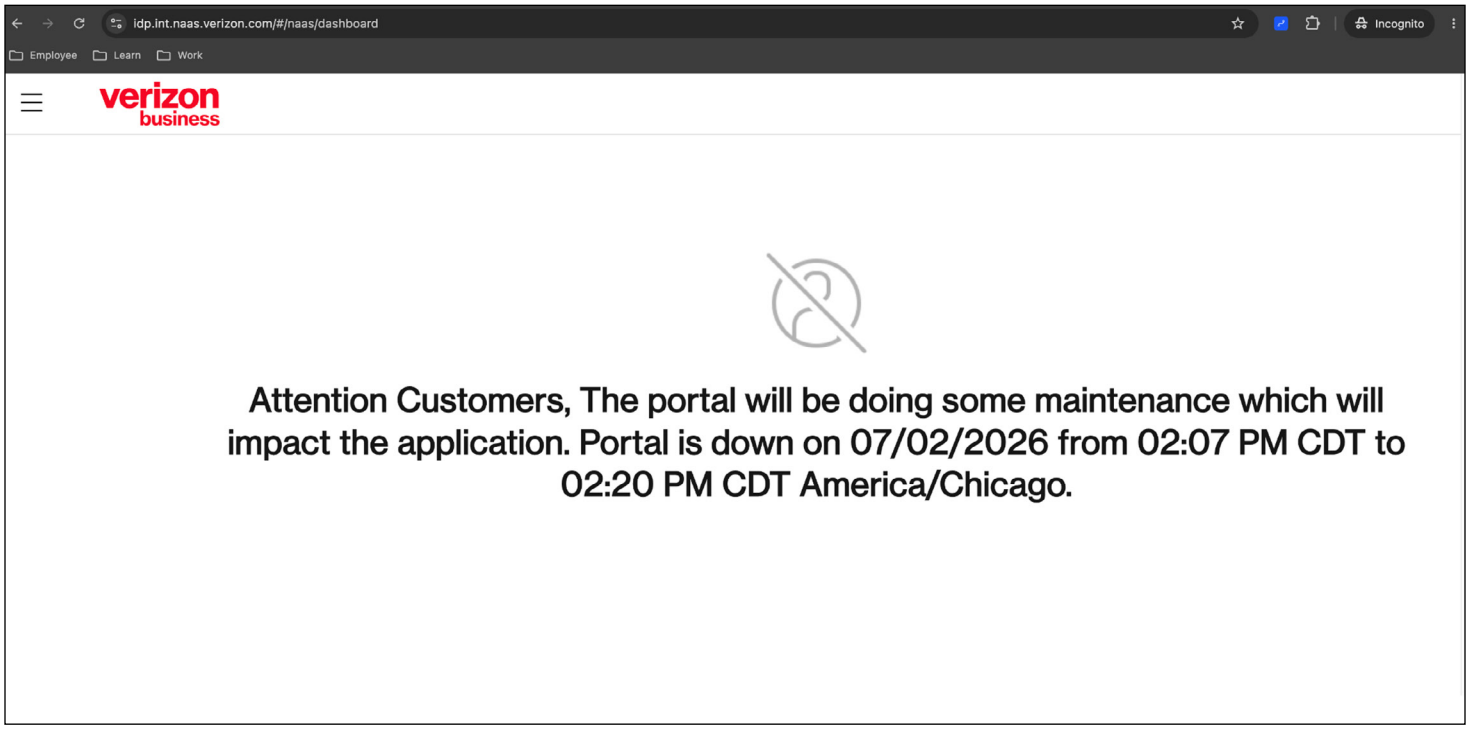
A: This discrepancy typically happens if your traditional WAN assets are registered under a different Billing Account Number (BAN) or Customer Legal Entity than what is linked to your current portal view.

To resolve this, please verify your ESP information and confirm that Monitor & Notify is active. If you still cannot see your sites or devices, please select the "Chat with Us" button at the bottom of the page, or contact the VEC Help Desk at 1-800-569-8799 to open a support ticket for Tier 2 triage.

- **Phone support:** Monday – Friday, 9 AM – 6 PM ET
- **Live chat support:** Saturday – Sunday, starting at 8 PM ET

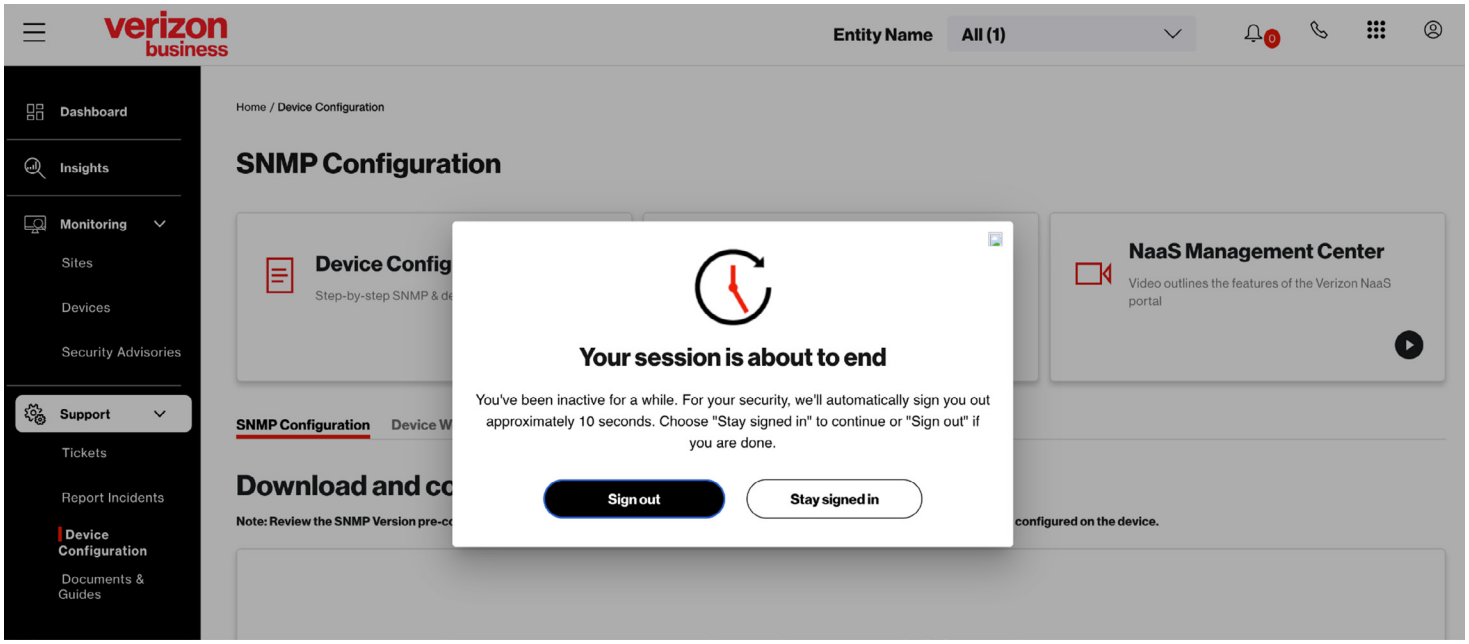
Q: How can I track scheduled maintenance for the NaaS portal?

A: Formal notifications for planned maintenance windows are published within the NaaS Management Center. For operational analytics, the system processes real-time availability metrics through our backend Datalake infrastructure, presenting live dashboard views based on the current persisted data state.



Q: Is there a session time-out for the NaaS Management Center?

A: Following 28 minutes of inactivity, the system triggers an automated prompt requesting the user to maintain the active state or terminate the session. Failure to select the “Stay Signed In” option will result in an immediate session closure to maintain portal security.



Glossary of terms

ACL (Access Control List): A set of rules applied to network interfaces that dictates what traffic is allowed to pass through or be blocked, based on factors like IP addresses, protocols or port numbers.

CE (Customer Edge): A router or switch located on the customer's premises that acts as the gateway to the service provider's network. It connects directly to the Provider Edge (PE) device.

CPE (Customer Premises Equipment): Any telecommunications or network hardware located physically at the subscriber's location rather than in the provider's central office. This includes items like modems, routers and VoIP gateways.

CVE (Common Vulnerabilities and Exposures): A standardized, publicly available list of known security flaws in software and hardware. Each flaw is given a unique identifier so security professionals can track patches.

CVSS (Common Vulnerability Scoring System): A framework used to rate the severity of a security vulnerability (CVE). It generates a score from 0.0 to 10.0, helping providers prioritize which security patches to deploy first.

NaaS (Network as a Service): A solution that helps customers simplify network management and transformation by providing a single contract and consolidated Service Level Agreement (SLA) for selected core networking products and services from Verizon and from other vendors.

NOC (Network Operations Center): A centralized location where network engineers and technicians monitor, manage and maintain the ISP's network infrastructure 24/7 to ensure maximum uptime and performance.

PE (Provider Edge): A router located at the boundary of the ISPs core network. It communicates directly with the Customer Edge (CE) device to route traffic from the customer into the provider's backbone.

RX/TX (Receive/Transmit): Standard abbreviations used to measure data flow. RX refers to incoming data (received), and TX refers to outgoing data (transmitted). Technicians monitor these rates to troubleshoot line quality and bandwidth congestion.

SD-WAN (Software-Defined Wide Area Network): A modern approach to WAN management that uses software to dynamically and intelligently route traffic across multiple connection types (like broadband, MPLS or LTE) based on real-time network conditions.

SLA (Service Level Agreement): A formal contract between the ISP and the customer that guarantees a specific level of performance. It usually outlines strict metrics for network uptime (e.g., 99.99%), maximum latency and how quickly the provider must respond to resolve outages.

SNMP (Simple Network Management Protocol): A standard protocol used for exchanging management information between network devices. ISPs use it to monitor device health, track bandwidth utilization and receive automated alerts when something goes wrong.

WAN (Wide Area Network): A telecommunications network that extends over a large geographical distance (e.g., connecting branch offices across different cities or countries).



© 2026 Verizon. This content was created with the assistance of artificial intelligence and validated by humans. VZUG4701026