



Juniper U.S. Government Cloud Services

Table of Contents

1. [Executive summary](#)
2. [Eligibility for Juniper Government Cloud](#)
3. [Compliance, data protection, and security](#)
4. [Available cloud services](#)
5. [Data governance and privacy controls](#)
6. [SLA/Performance measures](#)
7. [Support services and access](#)
8. [Product warranty](#)
9. [Legal notices and disclaimers](#)

1. Executive Summary

Juniper's AI-native, cloud-native U.S. Government Cloud Services deliver a secure, compliant platform with full-stack assurance—enabling secure, scalable, assured networks and operational agility in a FedRAMP-authorized cloud environment. This document provides an overview of Juniper's AI-native Government Cloud Service offerings, eligibility, data protection, compliance, data governance, and support services specifically designed for use by only government agencies and authorized system integrators and addressing specific regulatory and compliance requirements at the federal, state, and local level.

Key features:

- **FedRAMP and GovRAMP (formerly StateRAMP) authorization**
Juniper has achieved both FedRAMP and GovRAMP authorization at the "Moderate" Impact level. FedRAMP is sponsored by the U.S Department of Veterans Affairs and our authorization validates compliance with rigorous federal cybersecurity standards and NIST SP 800-53 controls. "Moderate" authorization includes Controlled Unclassified Information (CUI) government data.



- **Marvis AI**
The Marvis® AI engine automates tasks, improves mean time to repair (MTTR), and proactively resolve issues, assuring secure user experiences.
- **Marvis® AI Assistant**
The industry's only AI Assistant delivers intuitive, natural language-based troubleshooting and root cause analysis, leading to a **90%+ reduction** in support tickets.
- **Full stack services**
Wireless Assurance, Wired Assurance, Access Assurance (Network Access Control), WAN Assurance, Premium Analytics, Location Services, Managed Service Providers, and Marvis AI assistant.
- **Zero network downtime**
A modern microservices Government Cloud architecture ensures continuous availability for mission-critical services with zero outages.

2. Eligibility

Juniper's Government Cloud access is restricted to:

- Federal civilian agencies
- State, local, and education (SLED) entities aligned with federal cybersecurity mandates, including federally funded research data centers
- Validated resellers and system integrators operating exclusively within the federal space

To preserve compliance and trust:

- Commercial customers are not eligible
- Authorized resellers may only onboard government clients
- Contractors serving both sectors must use commercial cloud for non-government workloads



Figure 1. Eligible government entities

FedRAMP-authorized security package

Eligible entities can request access to Juniper's FedRAMP-authorized security package via the FedRAMP Package Access Request Portal (MAX.gov), with subject to approval.

Once approved, agencies and partners will receive onboarding credentials and deployment guidance for the Juniper Government Cloud environment.

3. Compliance, Data Protection, and Security

At Juniper, we continuously strive to align the development of our AI systems with both legal and regulatory requirements. Please see our full detailed list here:

<https://www.juniper.net/content/dam/www/assets/faqs/us/en/juniper-mist-ai-faqs.pdf>.

Our Government Cloud is built to enable hardened systems, strict access controls, and validated encryption standards to ensure end-to-end protection of networking data.

Requirement	Status
FedRAMP Moderate	Authorized
NIST 800-53	325+ controls implemented
FIPS 140-2/3 Encryption	Compliant for data in transit and at rest
Data Center Compliance	FedRAMP-authorized U.S. Data Centers
Data Residency	U.S. only
U.S. Cleared Operations	Enforced

Table 1. Compliance and security status

Isolated infrastructure and U.S. data sovereignty

Juniper's Government Cloud operates solely within AWS GovCloud (U.S.) regions, ensuring all data storage and processing remain within U.S. borders. The infrastructure is physically and logically isolated from Juniper's commercial cloud environments, with no cross-border replication or global integration. This guarantees strict data sovereignty aligned with federal mandates for classified and controlled information environments.

Certified hosting and U.S. cleared operations

All cloud operations are managed by U.S. citizens with appropriate security clearances, and hosted in FedRAMP-certified data centers. This provides a robust foundation for compliance, availability, and operational assurance in line with federal risk frameworks. To ensure service continuity and fault tolerance, workloads are distributed across multiple availability zones, maintaining high reliability for agencies with zero network downtime.



FIPS-validated encryption and key management

To protect agency data, Juniper secures all information through the FIPS 140-2/3 validated encryption:

- Data at rest is encrypted with AES-256
- Data in transit is protected using HTTPS/TLS with AES-128 or higher
- Mutual authentication is enforced for device-cloud communication

Juniper maintains centralized key management with role-based restrictions, hardware protections, and auditable processes, ensuring cryptographic material remains secure throughout the life cycle.

Securing end user data with FIPS-compliant edge hardware and operational control

Juniper supports deployment of FIPS 140-2 validated hardware, ensuring compliance down to the device level. All infrastructure at the network edge—including access points, switches, and gateways—is deployed on the end user's premises and fully managed by the customer via Juniper's Government Cloud.

This hybrid model provides government agencies with full control of on-premises assets while benefiting from cloud-scale visibility and automation.

- **Access points:** Communication between the Juniper Mist™ cloud and access points (APs) uses HTTPS/TLS with AES-128 encryption, and mutual authentication is provided by a combination of digital certificate and per-AP shared key created during manufacturing. Additionally, the 4096-bit key is used for certificate signature.
- **Switches and gateways:** Communication is over SSH to the Juniper Mist cloud. With CloudX enabled on certain switch families, communication is over HTTP/TLS, over port 443, and SSH is not required.
- **UI or API:** API communication (including UI access) uses HTTPS/TLS and is encrypted with AES-256.
- **Internal to cloud:** Data within the cloud is stored using AES-256 encryption.
- **Management/Infrastructure console:** Accessed over HTTPS connection using 2048-bit RSA key. Industry standard encryption is utilized for data communication across network administrators, infrastructure hardware/software, end users, and the Juniper Government Cloud, while stored data is block encrypted.

- **AP/Switch to Access Assurance (NAC):** Accessed over RadSec connection using 2048-bit RSA key. Industry standard encryption (TLS 1.2/1.3) is utilized for authentication of endpoints or end users using AES-256.

System hardening and threat mitigation

All servers in the Juniper Government Cloud platform run hardened Linux OS configurations, continuously patched and monitored to meet federal security benchmarks. A Secure Development Lifecycle (SDL) governs all software development, including:

- Static and dynamic security testing
- Continuous vulnerability scanning
- Threat modeling and attack surface reduction

Juniper's proactive threat mitigation model includes automated patching, real-time intrusion detection, and anomaly monitoring to prevent exploits and maintain compliance readiness.

Granular access controls and network segmentation

Access to Juniper Government Cloud resources is governed by least privilege principles, enforced through segmented security groups and role-based access controls (RBAC). Only essential ports are exposed for cloud services, like AP communications or secure API access, minimizing potential attack surfaces.

AWS Government Cloud model

Juniper's Government Cloud offering is built on top of AWS GovCloud (U.S.), leveraging its security-first infrastructure and compliance tooling. AWS provides the foundational controls for physical security while Juniper layers AI-native automation, encryption, and visibility across the networking stack.

For additional details on the AWS GovCloud environment, visit aws.amazon.com/govcloud-us/security.

Juniper's Government Cloud is built on the AWS GovCloud (U.S.)

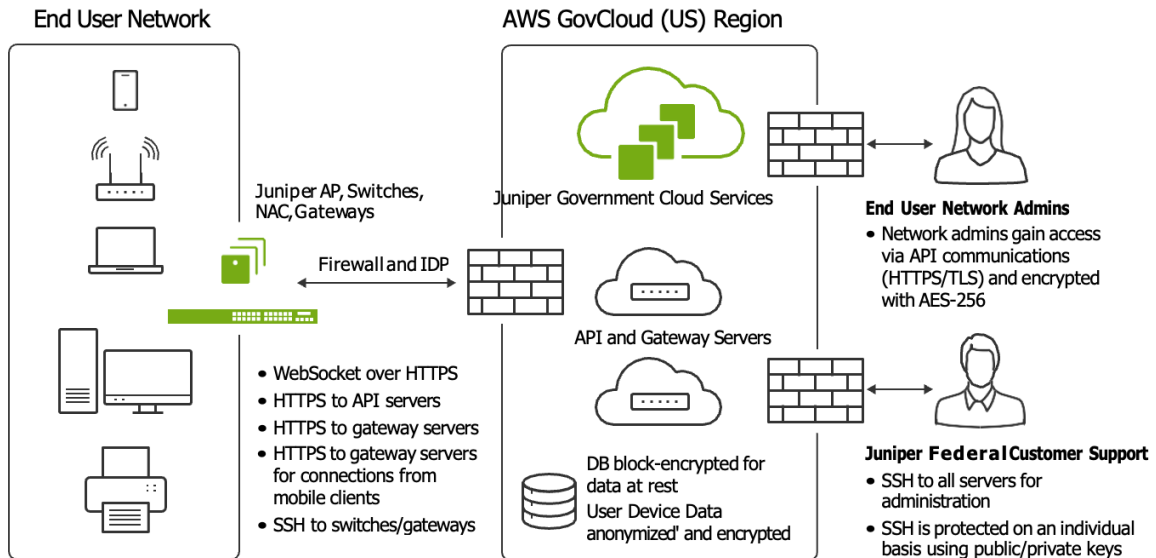


Figure 2. Juniper Wireless, Wired, NAC, WAN, Location, Premium Analytics, and Managed Service Provider dashboard interfaces

Juniper's Government Cloud Services

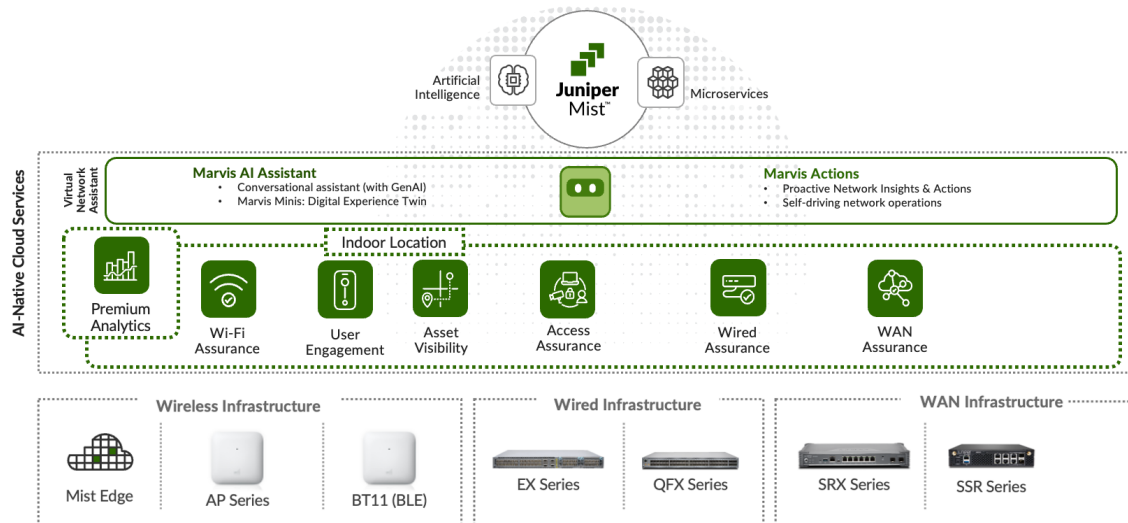


Figure 3. AI-native portfolio of services covered in Juniper's Government Cloud

4. Available Cloud Services

Marvis AI Assistant	Marvis AI Assistant enriches natural language processing (NLP) capabilities by integrating natural language understanding (NLU), allowing it to function as a conversational assistant that not only comprehends user language, but also understands intent. The power of Marvis AI Assistant is that it can contextualize requests to accelerate troubleshooting workflows, converse with the network, provide information about the network, answer product- or feature-specific questions, and help find any type of network device/client.	<u>Marvis AI Assistant</u> <u>Marvis AI Assistant Datasheet</u>
Wireless Assurance	Juniper® Wi-Fi Assurance leverages industry-leading AIOps to simplify and accelerate troubleshooting while significantly lowering OpEx. It replaces manual troubleshooting tasks with automated wireless operations to make Wi-Fi predictable, reliable, and measurable while providing unique visibility into user service levels.	<u>Juniper Access Points</u> <u>Wi-Fi Assurance Datasheet</u>
Wired Assurance	Juniper® Wired Assurance brings cloud management and the Marvis AI engine to campus fabrics, from access to core. This service improves the experiences of devices connected through Juniper EX Series Switches and simplifies EVPN-VXLAN campus deployments and operations, delivering new levels of consistency and scale.	<u>Juniper EX Series Switches</u> <u>Wired Assurance Datasheet</u>
Access Assurance (NAC)	Juniper® Access Assurance provides secure network access control based on user and device identities. The service enforces Zero Trust network access policies for guest, IoT, BYOD, and corporate devices. With integrations for a range of endpoint management solutions, Access Assurance can assess user and device posture, verify eduroam credentials, and validate other identity provider (IdP) credentials to control network access.	<u>Access Assurance Datasheet</u>
WAN Assurance	The Juniper® WAN Assurance cloud service is transforming network management by streamlining deployment and operations, enhancing end user experience visibility, and significantly reducing SD-WAN mean time to repair (MTTR).	<u>WAN Assurance Datasheet</u>
Indoor Location Services	Juniper Indoor Location Services provide real-time cloud-native and AI-native-services that combine personalization, data analytics, and operational simplicity to deliver turn-by-turn navigation and comprehensive visibility—all while reducing operational costs through intelligent automation.	<u>Indoor Location Services Datasheet</u>
Premium Analytics	Juniper® Premium Analytics is a cloud-based subscription service that provides end-to-end network observability and business intelligence to IT networking, security, and line-of-business users. It is the only service of its kind to offer long-term data storage for full stack network, security, and location insights.	<u>Premium Analytics Datasheet</u>
Managed Service Providers	Juniper's MSP dashboard delivers unparalleled visibility and streamlined management for managed service providers in government cloud environments. This modern infrastructure accelerates connectivity to mission-critical cloud applications while reducing operating complexity and enhancing service agility.	<u>Managed Service Providers White Paper</u>

5. Data Governance and Privacy Controls

Juniper is committed to ensuring transparency, data control, and privacy protection across all Juniper Mist cloud services. This section outlines the AI-native privacy framework, end user controls, data handling practices, and security safeguards specific to Government Cloud deployments.

AI-native government privacy regime

Supporting our advanced, privacy-driven architecture and internal administrative and procedural safeguards for government agencies, Juniper by default only collects certain device data (reference “Device data” section below for details) and does not collect the payload data of applications, network devices, Internet of Things (IoT) devices, or individual device end users by default. The collection and analysis of device data allows Juniper to provide insights into a specific network, IoT, or user device’s behavior (and location information if enabled), along with analytics across device types. This is key for baselining and monitoring trends and, later, identifying macro issues early so that Juniper and our end users can proactively address any possible networking issues. For example, user device roaming time, hardware radio performance, and device throughput can all be analyzed to identify system issues such as a performance degradation when a new mobile device operating system version is released. For wired network and IoT devices, end users can set, monitor, and enforce service-level expectations (SLEs) for key wired experience metrics such as throughput, network, and switch health that, when combined with Marvis AI Assistant, can deliver proactive anomaly detection.

Device data

Data elements processed in the Juniper Government Cloud, that may also be considered personal data under applicable data protection laws, include:

Juniper Access Assurance

- Device name, type, model, family, and OS
- MAC address
- IP address
- Username
- User agent
- Hostname
- Location data
- Captive portal data
- Email address
- Login

- Password
- Certificate information
- User group

Note: Username and/or email addresses are used by Access Assurance for authenticating when customers rely on user certificates or EAP-TTLS based authentication

Juniper Wi-Fi Assurance

- Device name
- Device type, model, family, and operating system
- MAC address
- IP address
- User agent
- Username
- Generic or specific location
- Dynamic PCAP (packet capture): limited data such as header information and IP address of sender and recipient

Juniper Wired Assurance

- IP address
- MAC address
- Hostname
- Username
- Interface statistics (Tx/Rx, errors)
- Group
- LLDP information
- Dynamic PCAP (packet capture): limited data such as header information and IP address of sender and recipient

Juniper WAN Assurance

- IP address
- Interface statistics (Tx/Rx, errors)
- Application information
- Summary of session records
- MAC address
- LLDP information
- Device model
- Dynamic PCAP (packet capture): limited data such as header information and IP address of sender and recipient

With Juniper Premium Analytics, end users may authorize Juniper to retain end users’ Wi-Fi, wired, and WAN user session metadata for longer periods to display trends, analysis, and a more comprehensive view of network operations using device data and other data collected through Marvis AI.

End user choices and control

End users may configure their Juniper APs to collect additional device data, depending on the desired implementation and level of support. To provide support to our end users when needed, our customer success team is able to access an end user's device data. However, end users have options for how much device data Juniper may access. For example, end users have the option within the Juniper Government Cloud to temporarily authorize Juniper personnel to access and view an organization's device data processed by Juniper in order for Juniper to provide support services. Using this access authorization feature, end users have more control over when Juniper personnel have access to the end user's device data. Upon granting permission to Juniper, Juniper Mist ingests existing customer service data from Microsoft Teams, Zoom, and Cradlepoint in order to provide application and network service insights. Zoom and Teams integration is an "opt-in" service. The additional data collected are email IDs of the Teams/Zoom sessions' participants and details on their devices, such as CPU and battery, which is then used for measuring and explaining the user experience. If your agency is subject to the Health Insurance Portability and Accountability Act (HIPAA), please check with your legal team before opting in to this service.

Privacy compliance

When an end user decides to deploy Wi-Fi Assurance in their offices, retail business, or other environment, the end user deploys a wireless LAN using Juniper access points that collect and process device data in order to better manage that wireless network and offer additional services (wayfinding and other location-based services) at the end user's election. When end users deploy Wired Assurance and/or WAN Assurance, they implement an AIOps framework to provide insights and management capability for their Juniper switches and gateways. Juniper has developed and adopted information security policies designed to protect the confidentiality, integrity, and availability of device data.

Data ownership

The licensed entity or end user retains ownership of their customer's data. In connection with the end user's use of the cloud service, Juniper collects and uses processed data in accordance with the Juniper Privacy Policy. Juniper uses processed data to enable, optimize, and provide our cloud services and support to end user and to improve Juniper cloud

services in general, including but not limited to, integrating processed data on an anonymized basis into our cloud services. By using the cloud service, the end user agrees to allow Juniper to use suggestions and collect end user data to generate processed data as defined in this Government Cloud Services Description document.

Data minimization

The Marvis AI engine by default collects the information required to provide and maintain services, anticipate and address network performance and connectivity issues, and troubleshoot support requests. Using the captive portal in the Juniper Mist cloud, end users are generally able to configure the type and quantity of data collected from data subjects for select Juniper Mist services when their end customers connect to a Juniper AP.

Data retention

Juniper deletes end user data (including device data) from the Juniper Mist cloud on a 60-day rolling basis or upon an end user's written request. Packet data is retained and available for seven days. Juniper retains certain other data for longer periods, as determined by end user if end user orders Premium Analytics. See applicable product documentation for further details on retention of information on Juniper devices.

Data portability

End users may download a copy of selected data through the dashboard or by using Juniper's API or other tools dependent on the applicable service. Reports produced from the Premium Analytics services can be downloaded by the end user if they are consuming that subscription.

Data subject requests

Juniper is committed to assisting end users who need to respond to certain data subject requests regarding device data processed by Juniper on the end user's behalf (for example, to receive a copy of, delete, or correct certain data). In addition, end users can directly manage any data downloaded by end users from the cloud service dashboard. By minimizing our collection and retention of personal data, we help simplify the data subject response process.

Notice and consent

Juniper provides functionality as part of its captive portal offering, enabling end users to present a notice to data subjects and consent to accept or decline terms. End users are responsible for managing and implementing any consents provided.

Tracking technologies

If an end user elects to subscribe to Juniper location services, Juniper will process a device's precise location information. Less precise location information may be collected by default for devices connecting to a Juniper AP using Wi-Fi, even if such location services are not enabled. Depending on the device and the protocol used to connect to the Juniper AP, the individual connecting to the AP ("data subject") may be prompted to opt-in to location sharing.

For example, device users generally wouldn't be prompted to opt in to location sharing for passive Wi-Fi (when the device is not connected to the Wi-Fi network). Bluetooth devices, like activity trackers, could be prompted to opt in to location sharing of their mobile phone through Bluetooth Low Energy via an app developed and configured by the end user.

Once the end user enables device location services, the end user will have access to the location of all devices within range of its Juniper AP network—whether the device is communicating through connected or unconnected Wi-Fi, Bluetooth Low Energy, assets such as Bluetooth Low Energy badges, and passive Bluetooth, among others. Juniper generally doesn't store the location history of devices and, by default, provides only real-time, nonspecific location information or aggregated statistics for delivering zone visitation/dwell time analytics to end users. If an end user requests to turn on visibility for unconnected devices, Juniper generally would process the MAC address and approximate location for the device (typically within 10 meters of accuracy). If an end user subscribes to location services, the following settings are configured by default:

- **Devices communicating via Wi-Fi:** Location information is made more accurate (within 5-10 meters, dependent on network design). Specific location tracking is not enabled by default if the device is not connected.
- **Mobile phones communicating via BLE application:** Location tracking is not enabled by default. The user must opt in for location sharing in the mobile application.
- **Assets (named) communicating via BLE:** Specific location tracking is not enabled by default.
- **Assets (passive) communicating via BLE:** Specific location tracking is not enabled by default.

Juniper enables end users to determine which tracking technologies to use and when and how to configure them (for example, whether to enable location services for more precise location tracking of users).

Government Cloud Cyber Incident Response Team (CIRT)

Juniper's CIRT manages vulnerability reports and provides support for security incidents. CIRT works with the Operational Security Community, other CIRT teams, and end users to maintain situational awareness of threats. This information is processed and communicated to the larger CIRTs and our end users. To report a potential security vulnerability, refer to www.juniper.net/us/en/security/report-vulnerability/.

Security testing

Juniper performs web security testing from development through development to production. Juniper periodically scans for SQL injections, cross-site-scripting (XSS), and more than 700 other vulnerabilities, including the OWASP Top 10.

6. SLA/Performance Measures: Marvis AI Resiliency

By leveraging a microservices cloud, the Government Cloud infrastructure components and services of Marvis AI are deployed redundantly in an effort to provide 24x7 availability. In addition, Marvis AI is based on multiple microservices, so issues with one microservice do not directly affect other microservices. The Juniper Government Cloud Service buffers data in the event of a component disaster, such as the loss of backend microservice. Once the disaster has been addressed, the data is replayed to fill in the lost analytics. System upgrades and feature introductions also benefit from microservices to avoid impact to Marvis AI when performing either. This reduces the need for planned downtime. In the rare event of a cloud outage impacting Juniper Government Cloud services, Juniper Wi-Fi APs, switches, and gateways are expected to continue to function. Any existing client device already authorized are expected to continue to access applications through Wi-Fi without undergoing any disruption of services.

Availability

Juniper will use commercially reasonable efforts to make Marvis AI fully available and operable over the internet in full conformity with Marvis AI specifications for access and use by the end user, as measured over the course of each calendar month, an average of 99.99% of the time, calculated as follows:

$$\left[\left(\frac{\text{total} - \text{nonexcluded} - \text{excluded}}{\text{total} - \text{excluded}} \right) * 100 \right] \geq \text{Available \%}$$

Where

"Total" means the total number of minutes in the calendar month. "Nonexcluded" means downtime that is not excluded. "Excluded" means any planned downtime of which Juniper gives three business days or more written notice via email or banner on the Marvis AI dashboard. All scheduled maintenance work and planned downtime will be during the hours of 7:00 p.m. PT to 7:00 a.m. PT on any day. Planned downtime is not expected to occur more than once or twice per year and is not expected to exceed 120 minutes in any given month. If Marvis AI suffers an incident causing unscheduled unavailability, Juniper will publish a status message on status.mist.com or another URL that Juniper may designate and the Marvis AI landing page. Upon request, Juniper will provide the end user with an incident report indicating the total period of unavailability and the end user locations effected.

7. Support

Juniper provides support services for U.S. public sector agencies through two different tiers: Government Advanced Care and Government Advanced Care Plus Services.

Government Advanced Care	Government Advanced Care Plus
N/A	Named Service Manager
24x7 Government customer care	24x7 Government customer care
24x7 Government Network Technical Support-Clearance eligible	24x7 Government Network Technical Support-Clearance eligible
Secure Case Management (FedRAMP certified)	Secure Case Management (FedRAMP certified)
Onboarding Assistance	Onboarding Assistance
Customized Reports	Customized Reports
Best Practices Knowledge Transfer	Best Practices Knowledge Transfer
Initial Response Time: P1/P2: 30 mins; P3/P4: 4 hours	Initial Response Time: P1/P2: 30 mins; P3/P4: 4 hours

Table 2: Support tiers

Support services include:

- Access to U.S.-based Juniper Technical Support Engineers (TSEs)
- Embedded software updates for supported hardware
- Online case management and technical resources
- Hardware replacement services during the coverage period, where applicable

For a detailed description of Government Cloud support tiers, please refer to the Juniper Service Description Document:

[Juniper Government Advanced Care](#)

[Juniper Government Advanced Care Plus Services Description \(PDF\)](#).

Support eligibility:

Support services are available to U.S. public sector agencies and authorized system integrators with an active subscription to Juniper Government Cloud Services.

Note: Support does not extend to customers consuming Juniper services through third-party managed offerings. Subscriptions must remain active to retain access, and renewals are required annually. Reinstatement is subject to [Juniper's Reinstatement Policy](#).

Online support access for Juniper Government Cloud

During the term of an active Juniper Government Cloud subscription, end users receive access to the Juniper Government Support Portal through the Mist Government online portal. These platforms provide tools, documentation, and support options for managing Marvis AI deployments.

Available online support capabilities include:

- **Case management:** Create, track, and update support cases; search by case number, RMA number, or internal reference ID
- **Access to technical documentation:** View release notes, known issues, configuration guidance, and troubleshooting resources
- **Product defect reporting:** Submit suspected product defects directly to Juniper's TSE team for validation and escalation
- **Knowledge base access:** Search technical articles, compatibility guides, and interoperability documentation
- **Feature enhancement requests:** Eligible users may suggest product improvements via the Mist portal

How to submit a support request:

- **Web (preferred):** <https://manage.mist.com/> (top-right "?" icon)
- **Email:** support@mist.com. For information on case handling and the technical support resolution process, please refer to the [JTAC User Guide](#).

Responsibilities

Once an end user initiates a service request with the TSE team, a TSE will take the following actions:

- Begin troubleshooting, diagnostics, and problem replication as appropriate
- Provide the end user with periodic updates on problem status and escalate the problem as required according to escalation management guidelines, or at the end user's request
- Generate a Return Merchandise Authorization (RMA) when the TSE determines that the end user's hardware product is defective or otherwise needs replacement. In these service requests, RMA information such as the number and the type of replacement is provided to the end user
- Close the service request when the end user agrees that the problem has been resolved.

The end user can monitor the service request progress through the Mist GovCloud service dashboard. When the TSE team updates a service request, the end user will receive an email with the update.

Resolution process

The assigned TSE will make use of all available resources to provide a resolution to the reported problem. Where a resolution is not readily available, the TSE will use commercially reasonable efforts to identify workarounds, resolutions, or ways to mitigate the impact of the problem. As part of the resolution process, the TSE may take any of the following steps:

- Review configuration/debug information to identify resolution of issue
- Replicate the scenario/issue in the Juniper lab (where possible)
- Troubleshoot live on the affected equipment
- With the end user's consent, create and review packet captures to isolate the problem
- Create an RMA where the cause of a problem is related to failed hardware product that is eligible for replacement
- Create an engineering defect ticket (problem report or bug) where the cause appears to be a hardware product defect

Escalation

Automatic escalation alerts to senior management are triggered on all P1 issues. In addition, TSE team members can escalate any support request to senior management.

Replacing defective hardware products

If the TSE determines that an end user's hardware product is defective and is eligible for replacement as set forth in the table below, the TSE will initiate the process for creating an RMA. The RMA is dispatched directly to the end user who will receive instructions and status on the RMA via email.

Definitions of key terms

- **Business day:** In connection with the particular Juniper Networks resource supporting Mist Wi-Fi Care Services, means Monday through Friday, 8:00 a.m. to 5:00 p.m., in the time zone where such resource is located, excluding local holidays
- **Ship-to address:** A warehouse or other manned operating facility within the applicable service availability area that is either (i) the installation site of the affected Juniper Wi-Fi product or the facility the end user (or the end user's agent or contractor) designated in their request for RMA (but only if the end user also designates therein in writing the name and office address (including country name) of that end user or of such end user agent or contractor as applicable) or (ii) the end user's facility
- **Service availability area:** With respect to the Juniper Mist Edge Wi-Fi product, the city and zip/postal code associated with the support availability verification number (as generated by Juniper's online support availability tool) designated in the PO for the Juniper Mist Edge hardware product replacement plan

8. Product Warranty/Business Summary

The following section summarizes the warranty terms and post-warranty replacement benefits for eligible Juniper hardware products. The warranty information in Table 3 is meant as a summary only. The formal warranty statements will always supersede any information provided in this Government Cloud Services document. All Juniper warranty statements can be found at <https://support.juniper.net/support/warranty/> (or such other URL that Juniper may designate from time to time).

Juniper Mist Hardware Products	Warranty Period ¹	Update Frequency*	Post Warranty Support
Indoor rated Wi-Fi and BLE access points (ex: AP21, AP41, AP43)	Longer of 1 year or last order date ²	Replace	Access to Juniper helpdesk; embedded software bug fixes and updates, hardware product replacement for 5 years from last order date as defined in the EOL Policy (subscription required) ³
Outdoor rated Wi-Fi access points (ex: AP61, AP63, AP64)	1 year	Replace	Access to Juniper helpdesk; bug fixes and updates (subscription required)
Juniper Mist Edge server	1 year	Replace	Access to Juniper helpdesk, Juniper Mist Edge software updates and bug fixes (Juniper Mist Edge service subscription required); support contract must be purchased for hardware product replacement

Table 3 Product warranty

1. Warranty begins upon delivery of the hardware product in accordance with the shipping terms
2. See EOL/EOS Policies for more information about end-of-sale notification and end-of-life support (<https://www.juniper.net/support/eol/#> or such other URL that Juniper may designate from time to time)
3. Post-warranty hardware replacement is provided for all indoor rates Wi-Fi products for as long as the end user has paid for a subscription to a Juniper Mist cloud service, subject to the hardware product reaching its end of life

Wi-Fi AP hardware replacement—RMA process

The following is a summary of the return process for eligible Wi-Fi products and is provided for information purposes only to assist the end user in understanding the benefits of support for Juniper Mist Wi-Fi products. A complete description of the RMA process is set forth in the Juniper Networks RMA Repair and Return Policy and Procedure: <https://support.juniper.net/support/rma-procedure/>.

Any Juniper hardware product that needs to be returned to Juniper requires an RMA. If a hardware product defect is determined to be the cause of the problem and the hardware product is eligible for replacement, or if a hardware product

replacement is required for any other reason, the TSE will create an RMA. The RMA number is communicated via email to the end user and linked to their service request. For eligible Wi-Fi hardware products, Juniper will, within three business days of issuing an RMA to the end user, ship a replacement unit to the ship-to address in advance of receiving returned defective hardware product.

The end user can use the same packaging to return the defective unit. The end user must label the outside of the box with the RMA number to ensure proper tracking and handling. Provided that the end user follows the instructions for return shipment provided with the RMA, Juniper will pay the costs for return shipment of the defective hardware product.

If any equipment arrives at a Juniper Networks shipping and receiving dock with an unnumbered RMA and the equipment serial number cannot be verified against an existing RMA, the equipment will not be accepted and will be returned to sender at the sender's cost.

Juniper Mist Edge hardware advanced replacement plan

The end user may purchase a support plan for a Juniper Mist Edge hardware product that includes next day shipment of advance replacement units. Juniper Networks will ship a Juniper Mist Edge replacement unit to the ship-to address in advance of receiving the returned defective hardware product on the next business day, if the RMA is issued by 3:00 p.m. local time (based on the regional distribution center or in-country depot, if available). If the RMA is issued after 3:00 p.m., Juniper Networks will ship on the business day following the next business day.

In order to receive next-day shipment support service, the end user must have a service availability verification number to indicate that next-day shipment support service is available where the end user has installed the Juniper Mist Edge hardware product. Either the end user or the authorized reseller can request a support availability verification number.

Returns not received

The end user has 30 days from receipt of the replacement unit to return the defective hardware product under an RMA. After 30 days, Juniper Networks has the discretion to charge the end user

at the price paid for the nonreturn of a defective unit. This notice is included in the confirmation of the RMA that is sent to the end user on the date of issuance.

RMAs that are “not received” can occur in one of the following ways:

- The return is received after 30 days from receipt of the replacement unit and processed in the normal manner by the Juniper Networks RMA repair and return department
- The end user decides not to return the equipment and the RMA is canceled when the end user issues a purchase order for the specified equipment

NAC, Wired, and WAN Assurance support process

Juniper Wired Assurance and WAN Assurance services bring AI-native operations and automation to NAC, switching, and routing. They set a new network management standard, securing and improving the experiences of devices connected to resources through Juniper switches and gateways. To provide the best end user experiences for government agencies, Juniper also extends Juniper Networks Technical Assistance Center (JTAC) support to NAC, WAN Assurance, and Wired Assurance end users.

The support process has been aligned so that end users can access support through the Mist Government portal, and Juniper will internally manage the communication and escalation process. The customer/end user managing the Marvis AI cloud offering can raise a ticket on the Mist Government portal to get support, as the portal can be leveraged for issue identification and resolution plan.

Access

For details on the JTAC support center structure, how to access JTAC support, JTAC response time guidelines, problem reporting and escalation procedures, case workflow, and end user communication guidelines, please refer to the JTAC User Guide at www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.

Problem Report (PR) Search

Access the most complete and up-to-date information about known Juniper Networks operating system defects with PR Search. This tool allows you to search for defects by PR number, Junos OS release version, and keyword, providing upgrade analysis and impact information. The end user can also subscribe to PRs of interest in order to receive automated updates as specific PRs change.

Online tools

Various tools are available to help analyze hardware and software information such as configuration tool, translator, migration tool, and so on.

Technical bulletins

Bulletins offer timely notifications on new feature releases, end of life, known product issues, and more.

Use of online tools is subject to the following:

End users shall have personal, nontransferrable, non-sublicensable, nonexclusive access during the term of the support services to Juniper Networks’ Government Support Portal through Mist Government online portal, subject to limited use terms posted at such site, all solely for the end user’s internal use in support of the Juniper Networks product covered under the Juniper Networks Service Contract. The end user shall maintain an active subscription contract to access resources.

Juniper Networks reserves the right in our discretion to limit or prohibit access by any end user if we believe that such access may give rise to violation of export control laws or regulations, or any other violation of Juniper Networks’ rules or the limited use terms identified above.

Replacing defective hardware products

If the TSE determines that an end user’s hardware product is defective and is eligible for replacement, the TSE will initiate the process for creating an RMA. The RMA is dispatched directly to the end user who will receive instructions and status updates on the RMA.

Hardware warranty:

<https://support.juniper.net/support/warranty/>

EOL/EOS: <https://www.juniper.net/support/eol/>

Procedure: <https://support.juniper.net/support/rma-procedure/>

End user responsibilities

For any problem identified as a Priority 1 Problem, the end user will provide Juniper Networks or our authorized service representative access to the affected network environment and will assign a technical contact for Juniper Networks. Furthermore, if Juniper Networks determines that our technical personnel need access to the end user’s network to remotely diagnose a problem, the end user will ensure that Juniper Networks’ personnel have the necessary level of authorized access to such network. The end user shall have the right to observe such access. The end user shall maintain a reasonable number of support engineers who are trained on Juniper products. All communication to Juniper Networks’ engineers of end user issues and responses will be conducted in English. The end user shall maintain the role changes or resignation of its support engineers so that their individual accounts are modified/deactivated as needed.

The end user shall provide access to servers, equipment, information, logs, infrastructure, and resources that are necessary for the delivery of the service.

The end user shall advise Juniper Networks of any information we may reasonably request about the execution of the services throughout the delivery of services. If third-party participation and cooperation is required for the end user to perform their responsibilities, the end user shall be responsible for getting such participation and cooperation.

The end user shall provide written notice to Juniper Networks as soon as it becomes clear or there is reason to believe that the end user will not meet any of the end user responsibilities.

API deprecation policy

It is our endeavor to continue supporting each API in its native form as long as possible. However, to improve the capability and performance of the API, some may be deprecated.

Whenever a Mist API is to be deprecated, advance notice will be given at least three months before the deprecation date. Post deprecation, the backward compatibility will be maintained for at least nine months to give a sufficient time window for partners and end users to migrate their API-dependent applications. The notifications will be sent out as part of the regular feature updates.

Availability

These support services are available where they can lawfully be sold and subject to applicable limitations posted by Juniper Support Operations on the Juniper website or the Juniper price list. Support services are available with a subscription for a minimum fixed duration of 12 months.

Scope

Support services shall be delivered remotely from an authorized Juniper Networks location unless specified otherwise.

All service deliverables in this offering are available in English only unless otherwise specified by Juniper Networks.

Juniper Networks' obligation to perform any particular support services hereunder is contingent upon Juniper Networks receiving from the end user such cooperation, network access, consents, information, and materials that Juniper Networks may reasonably request to enable Juniper Networks' proper and efficient performance of such support services and to enable Juniper Networks to do so in compliance with all applicable laws and regulations.

9. Exclusions, Legal, and Disclaimer

Exclusions

Juniper Networks is not obligated to provide support services for any of the following:

- Third-party devices (hardware, software cabling, etc.) not provided by Juniper Networks or problems associated with or arising directly or indirectly from such components
- Problems with a Juniper Mist cloud service that have been modified without Juniper Networks' written consent by any person (including unauthorized modifications by Support Services Specialist)
- Juniper product that is physically damaged by the end user or damaged from any exposure to water (except for outdoor rated Marvis AI products that are exposed to normal weather conditions)
- Problems relating to incompatibility of Marvis AI with third-party devices
- Problems caused by the use of Marvis AI other than in accordance with applicable documentation
- Problems with Marvis AI where the end user did not provide the required information
- Problems caused by the misuse of Marvis AI generally
- Problems with software used in connection with Marvis AI that is not a supported release
- Problems with a cloud-managed hardware device that is not compatible, nor under a supported release of Marvis AI

Disclaimer

The service levels (for example, Marvis AI availability or response times) described in this Government Cloud Services document are targets or objectives that Juniper strives to achieve consistently in providing support services to end users. A failure to meet any one or more of the service levels will not create any liability on the part of Juniper, nor a right to any credits or to withhold payment for Juniper AI products on the part of end users.

Legal notice

This Government Cloud Service ("Government Cloud CSD") outlines the scope of Juniper Marvis AI cloud services ("Marvis AI") and the support services available to end users ("end users") through authorized U.S. government procurement channels. Support for Marvis AI in the Government Cloud is provided exclusively through Advanced Care or Advanced Care Plus, as described in the applicable Juniper support documentation

All Marvis AI subscriptions and associated services described in this Government Cloud Service document are governed by the Juniper Purchase and License Agreement ("JPLA"), which is available at <https://www.juniper.net/us/en/legal-notices/juniper-networks-contractsresource.html> or such other location designated by Juniper Networks. In some cases, an alternative signed agreement between Juniper Networks and the end user may apply. In the event of any conflict between this Government Cloud Service document and the JPLA (or other applicable signed agreement), the terms of the JPLA or signed agreement shall prevail.

Unless otherwise defined in this Government Cloud Service document, capitalized terms have the meanings set forth in the JPLA.

For any hardware or software components delivered as part of the Marvis AI Government Cloud solution, including physical appliances or on-premises elements, purchase and license terms are subject to the JPLA or an applicable public sector-specific master agreement, including any required federal- or state-specific terms and flow-down provisions.

Juniper Networks is now part of HPE

Juniper Networks is now part of [HPE](#). Together, we're building industry-leading, secure, self-driving networks – purpose-built with and for AI. As AI and networking converge, we're driving a bold transformation across enterprises, service providers, and cloud operators.

Juniper's Mist™ AI-native networking platform is purpose-built to run AI workloads and simplify IT operations assuring exceptional secure user and application experiences. Additional information can be found at www.juniper.net, [X](#), [LinkedIn](#), and [Facebook](#).

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700

