CLOUD SERVICE DESCRIPTION - MIST AI

Contents

Introduction

This Mist AI Cloud Service Description ("CSD") describes Juniper Mist AI hosted in the cloud, ("Mist AI"), as well as the Juniper Care Software Advantage Services offering ("Support Services") that Juniper Networks makes available as part of the Mist AI Subscription for end users of Juniper Networks products ("End User") directly or through its authorized resellers. Your subscription to Mist AI is governed by this Mist AI Description and the Juniper Master Purchase and License Agreement posted at www.juniper.net/documentation/en_US/release-independent/licenses/agreements/eula-generic-en.pdf (or another written master services agreement signed by Juniper Networks and the End User and covering within its scope, the terms and conditions under which Juniper Networks will render support and maintenance services) (the "Master Agreement"). Capitalized terms used in this CSD not otherwise defined herein have the meaning given to them in the Master Agreement.

The Support Services are subject to the terms of this CSD and the Master Agreement.

If applicable to Mist AI, all purchases and license terms for Hardware and Software provided by Juniper Networks as part of the Mist AI solutions are subject to the Master Agreement.

Cloud Service Description

Mist AI uses a combination of artificial intelligence, machine learning, and data science techniques to optimize user experiences and simplify operations across the wireless access, wired access, and SD-WAN domains.

Data is ingested from numerous sources, including Juniper Networks Access Points, switches, and gateways for end-to-end insight into user experiences. These devices work in concert with Mist AI to optimize user experiences from client-to-cloud, including automated event correlation, root cause identification, Self-Driving Network™ operations, network assurance, proactive anomaly detection, and more.

Juniper also leverages Mist AI for next-generation customer support. It is the foundational element behind Marvis, the industry's first AI-driven Virtual Network Assistant, which provides extensive insight and guidance to IT staff via a natural language conversational interface.

The Mist AI overview, including links to its specifications and technical documentation can be found at www.juniper.net/us/en/products/mist-ai.html.

For purposes of clarity, all referenced Juniper Hardware or Software must be purchased and/or licensed separately.

Data Protection and Security

For purposes of this CSD, "End User Data" shall mean all information submitted by End User to Juniper and may include third-party data that the End User submits to Juniper. "Processed Data" shall mean information about End User's devices or systems in connection with End User's usage of Juniper products and services, as well as any network management information or configuration data from the use of End User's Processed Data.

Juniper shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of End User Data.

In accordance with the End User's use of Mist AI, the categories of data that may be processed are as set forth in the Juniper Privacy Notice available at www.juniper.net/us/en/privacy-policy/ together with any Supplemental Privacy Information referenced therein which includes Juniper Networks' collection and use of network device logs configured by the End User such as the metadata from managed devices (IP address of source and destination, accessed applications, or websites).

Protecting our End User's data is mission critical to Juniper. Mist AI offers our End Users the peace of mind that they are always on the latest version of our software. This enhances our ability to innovate and protect our End Users' data with evolving technology. We can respond to security threats rapidly by pushing security updates to our entire End User base and ensuring common data handling standards. Most importantly, Mist AI is co-located in tier-1 data centers with industry standard certifications. These data centers feature state-of-the-art physical and cyber security with highly reliable designs.

Juniper Mist AI Cloud Security Features Overview

- Servers are hosted in an ISO 27001 certified data center, across multiple availability zones, and different cloud providers.
- All servers run Linux OS and are hardened per best practices.
- Servers are hosted at Amazon Web Services (AWS) and Google Cloud Platform (GCP) with security groups. Only the required ports are opened on front end servers or terminators that need to communicate directly with Access Points (APs) or APIs from outside.
- Industry standard encryption is utilized for data in transit and data at rest (Please reference 'Data Security' section for details).
- Web security testing from development to production stages is performed on a continual basis.
- Policies and processes are followed for administering controlled access to the Cloud operations.
- Juniper employs robust key management processes.
- Juniper switches, gateways, and access points are located on End User premises where they are configured and managed by the End User via the Juniper Mist Cloud.
- Further information about security provided by AWS and GCP is available from the AWS and GCP security websites.

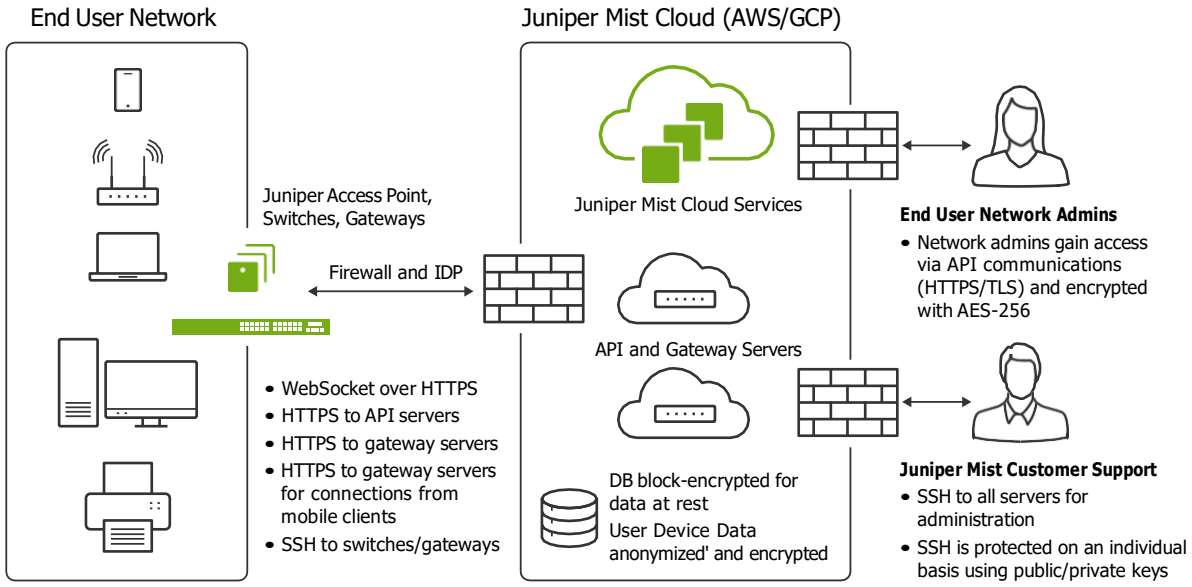

Fig. 1. Juniper Mist Wi-Fi/Wired/WAN Assurance Secured Interfaces

Data Security

Industry standard encryption is utilized for data communications across network administrators, infrastructure hardware/ software, end users, and the Juniper Mist Cloud, while stored data is block-encrypted. Juniper secures End User data by implementing various controls, such as encryption and obfuscation, including:

- AP: Communication between the Juniper Mist Cloud and 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. 4096-bit key is used for certificate signature.
- Switches and Gateways: Communication is over SSH to the Juniper Mist Cloud.
- 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.

AI-Driven Enterprise Privacy Regime

Supporting our privacy-driven architecture and internal administrative and procedural safeguards, 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 to its End Users 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 its 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 which, when combined with Marvis, can deliver proactive anomaly detection.

Device Data

Here is a description of the data elements processed in the Juniper Mist Cloud which may also be considered personal data under applicable data protection laws.

Juniper Mist 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, IP address of sender and recipient

Juniper Mist Wired Assurance

- IP address
- MAC address
- Hostname
- Username
- Interface Statistics (Tx/Rx, errors)
- Group
- LLDP information

Juniper Mist WAN Assurance

- IP address
- Interface Statistics (Tx/Rx, errors)
- Application Information
- Summary of Session Records

With Juniper Mist Premium Analytics, End Users may authorize Juniper to retain End User's 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 Mist 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 Mist 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 organization 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 its 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 a 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 its Customer's Data. In connection with 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 the Cloud Services and support to End User and to improve Juniper Cloud Services in general, including but not limited to, integrating such Processed Data on an anonymized basis into our Cloud Services. By using the Cloud Service, End User agrees to allow Juniper to use suggestions and collect End User Data to generate Processed Data as defined in this CSD.

Data Location

The Cloud Service's public cloud instance is hosted in multiple cloud environments in Top Tier One data centers from AWS and GCP (Refer to www.mist.com/documentation/cloud-instances/ for more information). End users may elect US, UK, EU, Canada, and Australia hosting based on their regulatory requirements. Juniper personnel who are granted access to network management data or a Cloud Service instance may be located in regions outside of the EU where data privacy and data protections laws may differ. Nonetheless, Juniper has established standard information security policies and practices that apply globally to all Juniper locations.

Data Minimization

The Mist AI platform by default collects the information required to provide and maintain the 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 and upon an End User's written request. Packet data is retained and available for seven (7) 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 End User, if they are consuming that subscription.

Data Subject Requests–including access and erasure/ deletion

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 Mist 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 would not 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 does not store the location history of devices and by default provides only real-time non-specific location information, or as 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.

Cyber Incident Response Team (CIRT)

Juniper's Cyber Incident Response Team (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 CIRT Teams 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.

SLA/Performance Measures

Mist AI Resiliency

By leveraging the public cloud, the infrastructure components and services of Mist AI are deployed redundantly (across cloud providers clusters and zones) in an effort to provide 24 x 7 availability. In addition, Mist AI is based on microservices so issues with one microservice does not directly affect other microservices. The Juniper Mist 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 Mist AI when performing either. This reduces the need for planned downtime.

In the rare event of a cloud outage impacting the Juniper Mist Cloud Service, Juniper Wi-Fi access points, 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 Mist AI fully available and operable over the internet in full conformity with Mist AI specifications for access and use by End User, as measured over the course of each calendar month, an average of 99.99% of the time, calculated as follows:

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

Where:

"total" means the total number of minutes in the calendar month;

"nonexcluded" means downtime that is not excluded; and

"excluded" means any planned downtime of which Juniper gives three business days or more written notice via email or banner on Mist AI dashboard. All scheduled maintenance work and planned downtime will be during the hours from 7:00 p.m. PST to 7:00 a.m. PST 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 Mist AI suffers an incident causing unscheduled unavailability, Juniper will publish a status message on status.mist.com or other URL that Juniper may designate from time to time) and Mist AI landing page. Upon request, Juniper will provide End User with an incident report indicating the total period of unavailability and the End User locations effected.

Support Services Eligibility

The Support Services are provided only to End Users who purchase Mist AI directly from Juniper or through Juniper's Authorized Resellers. For the avoidance of doubt, this CSD does not apply to End Users who have purchased Juniper Mist Cloud Services as part of a managed service offering from an Authorized Reseller. The Support Services, subject to certain exceptions described below, are available during the Subscription Term (as defined in the Master Agreement). Support Services will end when the End User's Subscription Term expires.

End User will be required to renew and pay for its Mist AI subscription from the date of expiration of the previous Subscription Term in order for these Support Services to be available. If the Mist AI subscription has expired for more than twelve months, End User will not be permitted to renew End User's subscription without the prior written consent of Juniper Networks (Juniper's Support Services Inspection and Reinstatement Policy (www.juniper.net/support/guidelines.html).

Support Service Overview

The Support Services include access to Juniper's technical support engineers (TSE) for Juniper Mist Cloud Services, Embedded Software updates for hardware products, training materials, online technical support, and, for specified periods of time, hardware product replacement.

The Support Services are in addition to any other Juniper Care Service that the End User may be required to purchase in order to receive similar services for other Juniper Products. Juniper offers support Services for other Juniper Products, including Advanced Care and Premium Care. These other support Service plans are not available for purchase with Juniper Products (Access Points and Juniper Mist Edge) currently.

Support Services shall be delivered remotely from an authorized Juniper location unless specified otherwise. All service deliverables in this offering are available in English only unless otherwise specified by Juniper.

Support Services Features and Deliverables

Juniper Networks will use commercially reasonable efforts to provide End User with the Support Services. The Support Services may include access to TSE team members, software releases, and online tools.

Support Access

With Juniper support, the End User will have unlimited access online 24/7/365. Juniper engineers will help diagnose system problems, configure, troubleshoot, and provide workaround solutions where necessary.

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 (if Wi-Fi Product is eligible for replacement pursuant to Section 6). 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 Cloud 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 which 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.

Online Support

During the term of the Juniper Networks Service Contract, Juniper Networks provides the End User with self-service access to the Juniper Networks Customer Service Center (CSC) and Mist online portal, which provides information, answers, tools, and service options for the End User's use in supporting Mist AI. Offerings include, but are not limited to:

Online case management: create new cases, check the status of existing cases, update cases with new information, and search by case numbers, RMA numbers, and the End User's own internal case reference numbers.

End Users can open a Service Request with the TSE team as follows:

- (Preferred) Web: manage.mist.com (top right corner under "?" icon)
- Email: support@mist.com

- Product Defect (Bug) Reporting Process – End Users may check the product Release Notes on the Mist Cloud Service dashboard for the latest information on known issues or existing bugs with the Wi-Fi Products. Any new and suspected product defects (bugs) found in the field should be reported to the Juniper TSE team using the problem reporting procedure described above. The TSE team verifies all issues before they are escalated to development engineering, and all known Juniper Wi-Fi Product defects are documented.
- Feature Enhancement Requests – The End User can submit Product feature improvement requests through the Mist Cloud Services dashboard at https://ideas.mist.com/forums/912934-product-features.

Juniper and Mist Knowledge Center: ability to search thousands of articles, including configuration assistance, known issues, interoperability, and compatibility information.

Priority Levels Guidelines

Table 1: Priority Ranking Guidelines for Service Requests

Priority	Juniper Responsibilities	End User Responsibilities	Examples
P1: Critical	Resources dedicated 24x7x365 until a resolution of workaround is in place	Designated resources that are available 24x7x365* Ability to provide necessary diagnostic information. *If the assigned TSE cannot reach the End User within one hour, the priority is temporarily lowered.	Business critical function is down across one or more sites, due to performance failure of multiple Wi-Fi hardware products Major impact to End User's business at one or more sites, across multiple Hardware Products The Mist Cloud Service or Mist Edge Service are down, inoperable, inaccessible or unavailable, such that the performance or nonperformance of the Mist Cloud Service or Edge Services prevents critical work from being done
P2: High	Resources are available 24x7x365. On-going case work will generally be worked Monday-Friday during local business hours or as otherwise agreed to with End User.	Resources available Monday through Friday during local business hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information	Business critical function is impaired or degraded at an entire site (or multiple sites). Performance of multiple Wi-Fi access points is degraded or experiencing random interruptions in performance. The Mist Cloud Service or Mist Edge Service are severely limited or degraded, major functions are not performing properly, the situation is causing a significant impact to certain portions of End User's operations or productivity; or the Mist Cloud Service or Edge Services have been interrupted but recovered, and in End User's reasonable opinion there is high risk of reoccurrence.
P3: Medium	Resources are available 24x7x365. On-going case work will generally be worked Monday-Friday during local business hours or as otherwise agreed to with End User.	Resources available Monday through Friday during local business hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information	Non-critical function is down or impaired and does not have significant current performance impact to the Wi-Fi access points. Performance is slightly degraded across multiple Wi-Fi access points. A minor or cosmetic problem with the Mist Cloud Service or Edge Services in which any of the following occur: the problem is an irritant, affects non-essential functions, has minimal impact to business operations; the problem is localized or has isolated impact; the problem is an operational nuisance; the problem results in documentation errors; or the problem is any other problem that is not a P1 or P2, but is otherwise a failure of the Mist Cloud Service or Edge Services to conform to its User Guide
P4: Low	Resources are available 24x7x365. On-going case work will generally be worked Monday-Friday during local business hours or as otherwise agreed to with End User.	Resources available Monday through Friday during local business hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information	Information requests. Standard questions on configuration or functionality of Hardware Products or Mist Cloud Service. Non-urgent RMA requests. Cosmetic defects.

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 Wi-Fi 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 which is eligible for replacement pursuant to Section 6.
- Create an Engineering Defect ticket (problem report or bug) where the cause appears to be a Hardware Product defect.

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 e-mail.

Definitions of Key Terms:

- "Business Day" in connection with the particular Juniper Networks resource supporting Mist WiFi 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" means a warehouse or other manned operating facility within the applicable Service Availability Area and which is either (i) the installation site of affected Juniper Mist Wi-Fi Product or other facility of End User (or of the End User's agent or contractor) designated by the End User in its 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 and of such End User agent or contractor, as applicable; or (ii) otherwise, the End User's facility.
- "Service Availability Area" means 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.

Product Warranty—Business Summary

The warranty information in Table 3 is meant as a summary only. The formal warranty statements will always supersede any information provided in this CSD. 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).

Table 3: Warranty Summary

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 and AP63)	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

Notes:

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 Access Point 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 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/.

In the event of a conflict between the RMA Repair and Return Policy and the summary in this Section 6.3, the RMA Repair and Return Policy will prevail.

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 its Service Request.

For eligible Wi-Fi Hardware Products, Juniper will within three (3) business days of issuing an RMA to the End Use 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 Advance Replacement Plan

End User may purchase a support plan for 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 p.m. local time (based on the regional distribution center or in-country depot if available). If the RMA is issued after 3 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 thirty (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 non-return 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.

Wired and WAN Assurance Support Process

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

When Juniper support such as Core, CorePlus, Same Day, or Next Day is purchased as part of the WAN Assurance and/or Wired Assurance offerings, the support process has been aligned such that end users can access support through the Mist portal, and Juniper will internally manage the communication and escalation process. The Customer/End user managing the Mist AI cloud offering can enter a ticket on either the Mist portal or the JTAC portal to get support, as either 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: 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, non-transferrable, non-sublicensable, nonexclusive access during the term of the Support Services to Juniper Networks' online Customer Support Center (CSC), 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. End User shall maintain an active subscription contract to access resources.

Juniper Networks reserves the right in its discretion to limit or prohibit access by any End User if Juniper Networks believes 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, End User will provide Juniper Networks or its authorized service representative access to the affected network environment, and will assign a technical contact for Juniper Networks. Furthermore, if Juniper Networks determines that its 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. End User shall have the right to observe such access.

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.

End User shall maintain the role changes or resignation of its support engineers so that their individual accounts are modified/deactivated as needed.

End User shall provide access to servers, equipment, information, logs, infrastructure, and resources that are necessary for the delivery of the Service.

End User shall advise Juniper Networks of any information Juniper Networks 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 the End User responsibilities, End User shall be responsible for getting such participation and cooperation.

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.

Compliance with Laws; Export Requirements

End User shall comply with all applicable laws and regulations and with all terms of the Export Note incorporated in the Shipping Terms Exhibit posted at www.juniper.net/Shipping-Terms-Exhibit. End User warrants that it has no knowledge or reason to believe that it has received any Juniper product through any export or re-export in violation of U.S. or other applicable laws or regulations, that it is not a Sanctioned Party (as that term is defined in the Export Note), that no Juniper product or Mist AI is located in or controlled from a site in a Group E country (Cuba, Iran, North Korea, Syria, or in the region of Crimea), and that it is not using any product or Mist AI to support activities in support of development, manufacture, or use of nuclear fuel or weapons, missiles, or chemical or biological weapons or other Prohibited Uses as that term is defined in the Export Note. End User further covenants that it will immediately notify Juniper Networks if at any time such warranties and representation become no longer accurate at such time. Regardless of any disclosure made by the End User to Juniper Networks of an ultimate destination of the Products. End User will not export, either directly or indirectly, any Juniper products or Mist AI without first obtaining any and all necessary approvals from the competent government authorities administering U.S. and other applicable country export controls. End User understands and agrees that certain restrictions on services described herein may be imposed by Juniper Networks to avoid violations of export control laws.

Availability

These Support Services are available where they can lawfully be sold and subject to applicable limitations posted by Juniper Global 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.

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 Mist AI Products that are exposed to normal weather conditions);
- Problems relating to incompatibility of Mist AI with third-party devices;
- Problems caused by the use of Mist AI other than in accordance with applicable documentation;
- Problems with Mist AI where End User did not provide the required information;
- Problems caused by the misuse of Mist AI generally;
- Problems with Software used in connection with Mist AI that is not a Supported Release;
- Problems with a cloud managed hardware device that is not compatible, nor under a supported release of Mist AI.

Disclaimer

The service levels (for example, Mist AI availability or response times) described in this CSD 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.

About Juniper Networks

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Juniper's AI-Native Networking Platform is built from the ground up to leverage AI to deliver the best and most secure user experiences from the edge to the data center and cloud. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on X (Twitter), 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