JUNIPER REMOTE MANAGED SERVICES

JUNE 2020

Contents

Introduction

This Services Description Document ("SDD") describes Juniper Networks® Juniper Remote Managed Service (the "Services") that Juniper makes available for purchase, by End Users of Juniper Networks Products (each, an "End User") directly or through Juniper's authorized resellers.

Juniper's Network Operation Centre (NOC) will actively monitor and manage End User's multi-vendor network 24x7 from a remote location. The End User will have round the clock access to the NOC and a Juniper trained specialist.

The Services are subject to the terms of this SDD and of the Juniper Networks End User Support Agreement, a copy of which is posted at www.juniper.net/support/guidelines.html (or another written master services agreement signed by Juniper Networks and End User and covering within its scope the terms and conditions under which Juniper Networks will render support and maintenance services) (herein, the "End User Support Agreement" or "EUSA"). This SDD, together with EUSA shall form the "Project Contract".

In the event of any conflict between the terms of this SDD and that of the EUSA or Juniper's End User License Agreement ("EULA"), which is located at the following URL (or such other URL that Juniper may designate from time to time): www.juniper.net/support/eula.html; the terms of this SDD shall take precedence. Unless otherwise stated in this SDD, capitalized terms used in this SDD shall be as defined in the EUSA.

In the event the counterparty to the Project Contract is an authorized Juniper reseller (a "Juniper Authorized Reseller"), the Juniper Authorized Reseller must i) communicate this SDD and delegate the obligations under the Project Contract to the End User or its designated systems integrator, and ii) inform Juniper that this has occurred (email is acceptable).

In such event, the Juniper Authorized Reseller i) remains contractually obligated to Juniper for the performance of such obligations, and ii) shall ensure that any third party is qualified to perform such obligations and Juniper is not liable for delays, issues or problems arising out of its reliance on the third party's performance of the Customer's obligations. Juniper Authorized Reseller understands and agrees that it may not delegate any payment obligations arising under the Project Contract. The counterparty to the Project Contract, whether that be a Juniper Authorized Reseller or an End User, is hereby referred to as the 'Customer'.

Eligibility and Purchasing

- The Services are available for purchase only (i) by End Users solely for their own end use or (ii) by Juniper Authorized Resellers solely for resale to the End User identified by name and address in such reseller's PO.
- The Services cover only those Juniper Products as to which all of the following apply:
  - End User is using the Juniper Products to be managed (Managed Assets).
  - End User has purchased or leased Managed Assets from either Juniper Networks or a Juniper Authorized Reseller.
  - Such products are currently covered under a valid Juniper Care Services contract, and, for each such product, only during the term of its associated contract.
  - Managed Assets quantity and type are identified in the PO(s) for the Services placed with Juniper.

  In addition, the Services will also cover third party products requested to be covered by the End User and agreed to in writing by Juniper. The End User will be responsible to make sure such products are covered under a valid third-party maintenance contract.
- The Services for each of the Managed Assets must be purchased for a fixed term lasting at least twelve (12) months unless otherwise specified by Juniper Networks in writing.

  Each Managed Asset is eligible for co-terming Service Terms after the first year of the Services.
- If a Project Contract expires, Juniper will invoice the Customer the current fees on a monthly basis for up to two (2) months provided the Customer submits a letter of intent to renew thirty (30) days before the Project Contract expires. After the 2-month extension, the monthly invoice amount will increase 20%.

Service Features and Deliverables

Fault Monitoring:

- **24/7 Fault Monitoring** - The NOC will monitor the contracted network equipment and devices for fault alarms and conditions. If a critical task or function turns off for some reason (up/down), the NOC monitoring tools send out an alert and the NOC will notify the Customer of the alarm in accordance with the Problem Identification and Triage procedure.
- **Event Log Monitoring** - Most events that happen on a server are recorded in an event log. The NOC monitors all of those logs. If a critical event occurs, the NOC monitoring tools send out an alert and the NOC will notify the Customer of the alarm.
- **Trap Monitoring** - For devices that can support traps, the NOC can configure the traps to send critical event information to the network monitoring tools. These events can create alarms which trigger a trouble ticket.
- **Problem Identification and Triage** - The remote monitoring Service will verify that an alert or alarm is valid and then notify the Customer of a detected problem according to the contact process provided by the Customer and documented in the Customer Service Manual. The Service will document the Customer activities to remediate the issue and report when management systems tools show the issue has been corrected.

Fault Management:

- **Fault** - A fault is defined as a failed device poll indicating the target device is not visible to the NOC's network management systems and tools.
- **24/7 Fault Management** - The remote management service will manage the contracted network devices for fault alarms and conditions. If a critical task or function turns off for some reason (up/down), the monitoring tools send out an alert and the NOC will notify the Customer of the alarm. The NOC will open a ticket and troubleshoot the alarm and resolve the issue. If the NOC cannot fix the issue directly, the NOC will open a ticket with the vendor (under a vendor maintenance support contract, i.e. Juniper maintenance) and work with the vendor support team to resolve the issue. When a fault is identified, the remote management Service will take ownership of the issue until it is resolved.
- **Problem Identification and Triage** - The remote management Service will verify that an alert or alarm is valid and then notify the Customer of a detected problem according to the contact process provided by the Customer and documented in the Customer Service Manual. The Service will open a trouble ticket and start the remediation actions.
- **Event Management** - Most events that happen on a server are recorded in an event log. The NOC monitors all of those logs. If a critical event occurs the NOC monitoring tools send out an alert and the NOC will notify the Customer of the alarm. The NOC engineers will open a ticket and troubleshoot the cause of the alarm. When the cause of the alarm is confirmed, the NOC engineers will [use their commercially reasonable efforts to] resolve the issue. If the NOC cannot fix the issue directly, they will open a ticket with the vendor (under a vendor maintenance support contract, i.e. Juniper Care Services) and work with the End User and the vendor support team in an effort to resolve the issue.

- **Trap Monitoring** - For devices that can support traps, the NOC can configure the traps to send critical event information to the network monitoring tools. These events can create alarms, which trigger a trouble ticket. Corrective action will be taken by the NOC staff depending on the nature of the alarm.

Configuration Management:

- **Access Control and Monitoring** - For security and compliance reasons, this Services provides access control giving the NOC secure and quick remote access to the managed equipment and keeps an audit trail of who has logged into the system and when.
- **Equipment Configuration Management** - The Service scans the managed network equipment daily and stores all configuration changes. This feature allows the NOC to quickly restore the last known good configuration of a critical device in case of hardware failure or an inadvertent command being placed in the device that would cause the device to not function as designed. Highlights of the configuration management Service include:
  - Maintaining a log of network device configuration changes
  - Daily polling of each contracted network device to determine if configuration changes have occurred
  - Automatic notification of configuration changes
  - Capturing and archiving the most recent thirty (30) device configuration changes
  - Ability to quickly provide the last good archived configuration to assist with rapid recovery in the event of configuration loss (including during any outage or disaster) or changes, or performance issues

Performance and Patch Management:

- **Performance Analysis** - The NOC monitoring tools measure performance benchmarks of managed network devices. Information such as CPU processor utilization, CPU memory utilization, bandwidth utilization over a specific timeframe, dropped packets, jitter and a host of other data points are captured and analysed. The NOC engineers use this information to see a clear picture of the overall network performance. This is a major benefit because it illustrates how managed devices are handling the workload of the environment. In addition, it helps to identify and resolve performance bottlenecks in the system, and with capacity planning and budgeting.
- The Service monitors the data gathered from the contracted devices (i.e. CPU, memory, etc.) and compares it against the established performance thresholds. It notifies the Customer when normal device performance thresholds have been exceeded. Juniper working collaboratively with the Customer mutually agree the settings for performance thresholds of all devices. Thresholds will initially be evaluated after ninety (90) days of recorded remote monitoring.
- **Patch Management** - Patches are enhanced features or bug fixes released by Juniper. As part of the Service, the NOC will provide remote critical patch updates for all managed LAN/WAN systems. When critical software, firmware or OS patch/updates become available, the NOC will alert the Customer of the availability. The NOC will discuss with the Customer the critical updates available, the current configuration and operational status of the Customers devices affected, any associated problems or concerns about the updates, and any additional hardware requirements that may be required to implement the upgrades. If it is determined that the patch update is appropriate for the Customer's current environment, the NOC will perform the remote patch update installation via remote access in accordance with the Customer's change management processes. The remote management Service can deploy and apply the recommended patches to contracted network equipment according to the End User maintenance and patch policies and procedures.
- **Best Practice Monitoring** - For specific devices and system designs there are recommended or best practice system configurations. The remote management Service will review periodically the network environment that the NOC is managing and monitoring and compare it to best practice recommendations. If there are any best practice recommendations that are found by the NOC, the Customer will be notified in the periodic business review.

Service Requests & Trouble Tickets

A trouble ticket is usually generated automatically by the NOC's monitoring tools. The Customer can open a trouble ticket by sending an email to the NOC, making a phone call into the NOC or using the Web portal. If a problem is critical (S1 or S2), the Customer is urged to call into the NOC via phone call. MACD (as defined in Section 3.5.3) requests can also be requested through the NOC. The following information is needed in order to open a NOC trouble ticket:

- Contact name and telephone number of the user making request.
- Model number and serial number of the equipment to be serviced.
- Site location address of equipment to be serviced.
- Description of the problem or MACD request.

Vendor Management:

The NOC will manage vendors (through letters of agency) for:

- Replacement parts dispatch thru vendor maintenance contracts
- Vendor on-site technician dispatch thru vendor maintenance contracts
- Incident management with telco's (PSTN or WAN)
- Vendor tickets

Web Portal Access:

The remote management service can provide access into the ticketing system and monitoring tools via a secure Web portal. The Web portal is configured to provide 7x24x365 read only access into the Customer's devices and tickets. The portal can provide the following to the Customer:

- View open and closed tickets
- Open a new S3 or S4 ticket
- Change Customer contact information
- View Customer devices in real time using the NOC monitoring tools

Some of the information available through the portal includes:

- Network performance information
- Bandwidth utilization
- Network latency
- Mean Opinion Score (MOS)
- Jitter
- Packet loss
- Circuit status

Device Performance Information

- Device CPU utilization
- Device memory utilization
- Device buffer performance
- Gateway utilization
- Power supplies
- Fans
- Temperature

A list of authorized Customer users will need to be provided to the NOC for access into the Web portal. The list can be identified in the Customer Service Manual provided at the Customer kick off meeting. The Web portal training (usually one (1) hour) for the Customer portal users will be scheduled through the NOC.

Extended Professional Services:

Separate Professional Services are available if required to address Customer requests beyond normal device problem management included in the scope of this SDD. The professional services hours will be provided on a T&M basis for onsite or remote support and will be used for non-break fix support or small project-based activities. This additional scope will be either contracted separately via the Juniper Fixed T&M contract or, if NOC's Professional Services team can perform these activities, they will be budgeted, scoped, delivered and charged against MACD program for time tracking and budget. The NOC will perform the requested support, track the hours utilized and report on the usage and hours remaining in the monthly report. There will be no credit carried over to the following year for any unused hours.

Larger projects requiring additional services are contracted in a fixed price SOW and will be delivered as a project outside of this SOW.

Remote Technical Support:

The remote management service will work with the hardware vendor (through letter of agency) on the Customer's behalf to expedite replacement of defective parts. The service does not include on-site engineers for break/fix support. All managed devices are required to have a vendor maintenance contract to provide replacement parts.

Remote Technical Support is intended for resolution of identified problems with contracted devices, not Customer's end user help desk support. The NOC will receive calls from the Customers internal IT group or designated contacts after a problem has been identified. The Customer's end users should not call the NOC directly to ask questions regarding use of the servers, applications, features or capabilities.

The NOC will answer technical questions and perform remote diagnostic and troubleshooting activities pertaining to contracted devices. Once a problem has been identified, the NOC will attempt to resolve the issue remotely (i.e. working with Customer's site contact as needed). If the issue is hardware related, the NOC will open a trouble ticket with the appropriate hardware vendor (under an executed letter of agency) and work the problem through resolution.

MACD (Moves, Adds, Changes & Deletions):

MACDs are used for items such as User Administration (i.e., NOC remotely adds and removes users from the system, resets passwords, or assigns new passwords as needed), patch application or managing code upgrades, and other ad-hoc services such as on-boarding new devices during in contract true-ups.

A MACD is tracked and delivered in 15-minute increments typically sold based on the size of the environment starting with a 120 MACD bundle equating to a 30-hour bundle defined as when the NOC remotely adds and removes users from the system, resets passwords, or assigns new passwords as needed. The initial allotment of the remote support MACD requests over the Service Term, are managed, tracked and reported on a monthly basis.

All MACDs will expire if not used prior to the end of the Service Term. If the number of MACD requests in any month exceed the monthly MACD allotment, additional MACDs shall be purchased by, and will be invoiced to, the Customer, to the extent no unused and unexpired pooled MACDs exist from other sites under contract.

The Juniper quote specifies the quantity of MACDs purchased for the Service Term. To the extent there are multiple sites with devices under management, the parties can specify additional MACDs to cover multiple sites, which will be pooled MACDs with usage also tracked monthly.

If a MACD requires onsite support, the Customer may contract with Juniper Networks on a Time and Materials (T&M) fee-basis therefor.

The MACDs will be performed remotely by the NOC using a secure VPN connection. The timeframe in which the NOC will complete the remote MACDs varies based upon the quantities of activities requested. However, the NOC will make all reasonable efforts to complete requested MACDs within 48 hours of receipt of the remote MACD request.

Unless otherwise specified, remote MACDs will generally be handled Monday-Friday 8 a.m. to 8 p.m. EST. The Customer will submit a MACD request to the NOC via email, WEB portal or phone call. Upon receipt of the request, the NOC technician will verify submission, open a trouble ticket and provide the Customer with e-mail confirmation of receipt of the remote MACD and the trouble ticket information. The NOC will follow all Customer change procedures when performing a remote MACD on behalf of the Customer. Upon completion of the remote MACD, the NOC's technical staff will verify the change was successful, update the documentation to reflect the change, notify the Customer and update and close the trouble ticket.

Reports

The NOC will provide reports to help the Customer understand the state of the managed service environment. The type of reports and the information available is dependent on the packaged remote management service purchased. A list of available reports is provided in the table at the end of this sub-section 3.6.

Weekly Reports:

Weekly Reports summarize the weekly ticket activity showing all tickets opened, closed and still active.

Monthly Performance Reporting:

Monthly Reports look at the contracted infrastructure devices. The NOC will send out detailed reports each month to the Customer's designated contact person. The reports include statistics on:

- Network and device uptime and availability
- Fault history
- Trouble tickets
- MACDs used
- Professional Services hours used
- Configuration changes during the month

Strategic Reporting:

- Periodic Business Review - Provides business intelligence information based on the data that the NOC gathers during the period under review. This information has potential business impacting information that reflects network trends observed, capacity planning, resource utilization trends, ticketing trends, compliance issues, best practice standards, security concerns and business continuity planning. The goal of this report is to:
  - Characterize the existing managed environment
  - Make specific recommendations for improvement
  - Provide budgetary information to implement the recommendations
- The first category of recommendations is referred to as Immediate Impact recommendations. These recommendations are intended to provide an immediate impact on performance across the managed network. The second category of recommendations is referred to as High Impact recommendations. These recommendations are intended to provide additional improvements in performance as well as increasing network management efficiency. The third category of recommendations is referred to as Strategic recommendations. These recommendations are intended to ensure that the network will scale to meet future business requirements and that the Customer will be able to proactively monitor and manage network performance through the use of the NOC.
- Performance Analysis provides detailed information that reflects the overall performance of the managed network showing bottlenecks, areas of high utilization, areas of under-utilization, dropped packets, unusually high error rates and lower than normal device uptime.

The reports that are included with the monitoring and management package are reflected in the table below:

Report	Select Service Management
Weekly Report (fault/ticket summary)	X
Monthly Report	X
Fault History	X
Trouble Tickets	X
Device Uptime	X
Periodic Business Review	X
Fault History	X
Trouble Tickets	X
Device Uptime	X
MACD's Performed	X
Average PRI/T-1 Utilization	X
Professional Service Hours	X
Performance Analysis	X
Configuration Management Changes	X

Support Levels and Definitions

Support Severity Level Summary:

Fault ID	Objective Description	Service Level Response
S1	Detection of Severity 1 (P1) events on the Customer network	Within 15 Minutes
S2	Detection of Severity 2 (P2) events on the Customer network	Within 15 Minutes
S3	Detection of Severity 3 (P3) events on the Customer network	Within 1 hour
S4	Detection of Severity 4 (P4) events on the Customer network	Within 2 Business Days

Support Level Definition:

(S1) - Critical Priority:

Produces an emergency situation in which the network is inoperable, produces incorrect results, or fails catastrophically, or a mainline function of the network is inoperative (i.e. a critical application server), causing significant impact on the Customer's business operations (i.e., the Customer's production network is down causing critical impact to business operations if service is not restored quickly).

(S2) - High Priority:

Produces a serious situation in which the network is inoperable, produces incorrect results, or a mainline function of the network is inoperative (i.e. a critical application server), causing a major impact on the Customer's business operations (i.e., the Customer's production network is severely degraded, impacting significant aspects of business operations).

(S3) - Medium Priority:

Produces a non-critical situation in which the network produces incorrect results, or a feature of the network is inoperative, causing a minor impact on the Customer's business operations (i.e., the Customer's network performance is degraded; network functionality is noticeably impaired, but most business operations continue).

(S4) - Low Priority:

Incidents that cause little or no impact on the Customer's business operations

Device Count Reconciliation True Ups:

The NOC will conduct a quarterly audit of total device counts. This review will produce a current device inventory. The current device inventory and quantities will be compared to the devices and quantities under contract for the managed devices per site (or the prior quarter's true up of revised device and quantities if after the initial quarter), to determine if any additions or deletions to the device count has occurred. If the number of devices (firewall, router, server, etc.) exceeded contracted device quantities, a true up fee will be charged and invoiced to cover the added devices for the remainder of the Service Term.

The true up fees typically include a setup or onboarding fee for each new device to cover administrative costs of adding device to systems and testing connectivity and annual price of the device(s) added based on the Service level.

True up fees can be paid with MACD reductions (three [3] per newly added device), or a separate invoice.

All new devices that are on-boarded will be monitored for two (2) full weeks to ensure continuous availability prior to starting Day 2 Support. If during the 2-week period, issues are discovered, the NOC will report to the Customer/installer to ensure the issues are addressed prior to Day 2 Support beginning. If a device is not able to be successfully on-boarded due to issues, the Customer will not be charged the on-boarding fee and the device will be removed from the NOC's monitoring systems.

Onsite Maintenance:

RMS Services provides the Customer with remote maintenance service coverage for contracted network devices. If on-site device replacement is required, a Change Order will be required. The Services do not include on-site engineering support as part of this SDD.

End User Responsibilities

Minimum Services Requirement:

The provision of Services is based on the standards and minimums outlined below. In the event that these standards and minimums are not maintained, Services pricing and/or SLA's will be impacted.

- All devices and applications supported by Juniper must be no more than two (2) revisions from the latest major release from the vendor. These versions must also still be supported by the vendor and the Customer must have an active maintenance service contract in place for each contracted device.
- Devices under support services contract must be configured to adhere to industry best practices to ensure stability and security. These best practices include but are not limited to:
  - Passwords encrypted and complex
  - Using SSH vs. Telnet
  - Not openly accessible via internet
  - NTP configured and pointing towards reliable server
  - Ensure failover is configured and working properly, when redundancy is in place
  - Perform regularly scheduled user audits to ensure only active administrators have privilege level access
  - Backups are configured and working properly and periodically tested and validated at least once a year
- Redundancy is configured and working. Failover should be tested at least once a year. Customer is required to provide evidence of last test and results/actions.
- Devices under support services contract must be properly implemented and functioning as designed in the production environment prior to Juniper beginning remote monitoring and management Services

Before Services Commencement

- The End User must complete a Service Initiation Form
- The End User must provide network diagrams, as built documentation, configuration files, security profiles or other applicable documentation regarding supported devices.
- The End User must provide the NOC remote VPN connectivity to all devices under the Juniper Care Service contract.
- The End User must provide the NOC with necessary security information to include, but not be limited to, dial-in numbers, access ID's, passwords, and SNMP community names necessary for the NOC to perform the contracted support services. Any device under the support services contract should be SNMP capable.
- The End User must provide the NOC access to maintenance vendor contracts.

Obligations:

- End User is responsible for alerting the NOC of changes to its network that could affect its devices under the Juniper Care Service contract.
- End User is responsible for alerting Juniper of any security requirements for monitoring of infrastructure.
- Juniper and its delegates will not take responsibility for remote monitoring of any existing devices or systems until the existing system is validated to be functioning properly.
- The NOC is not responsible for system problems caused by the End User or other vendors accessing the network and the servers. Problems created by the End User or other vendors will be addressed by the NOC under T&M billing.
- Remote Monitoring and Managed Services assumes no liability for security breaches, security policies, denial of service incidents or other related security incidents.
- The End User has legal copies and licenses for all software and applications that are under Remote Monitoring Service.
- Pricing for Remote Monitoring Services is based on the number of devices being monitored. A quarterly audit will be conducted by the NOC to determine if any devices or equipment have been added to or deleted from the original contracted amount. An increase (if more devices are being monitored) or a decrease (if less devices are being monitored) of the contracted amount will be invoiced (using the same monthly, annual or contract term invoicing schedule) reflecting the change. The End User is required to pay for any additional invoiced amounts.
- All devices must be set up in a professional business grade environment, meaning power/circuits/devices are always powered on. If reoccurring issues are identified that are not resolved by the End User due to the environment, equipment or grade of Service purchased, Juniper will discontinue proactive monitoring and notify the End User.
- In the event that any portion of Payment Card Industry Data Security Standard (PCI DSS) compliance is required for this Service, Juniper will work in good faith with the End User to become compliant in a reasonable, agreed to timeframe. Should compliance efforts require specific hardware, software, and/or custom services, then additional costs outside of the scope of this Project Contract will be negotiated with the End User.

- In the event that any portion of e-bonding is required for this Service, Juniper will work in good faith with the End User to establish e-bonding in a reasonable, agreed to timeframe. Should e-bonding efforts require specific hardware, software, and/or custom services, then additional costs outside of the scope of this Project Contract will be funded by Extended Professional Service (section 3.5.3 above) hours or otherwise negotiated with the End User.
  - End User will provide a point of contact for the duration of the Service Term who will act as End User's central point of contact in connection with the provision of the Services.
  - End User will manage, coordinate and provide the timely participation of any third parties (including, but not limited to, other vendors and systems integrators) required for successful provision of the Services. Unless agreed otherwise in writing, Juniper Networks shall have no responsibility for any third party engaged, or related costs incurred to facilitate performance of the Services.
  - As requested, and on a timely basis, End User shall provide access to all required and requested data, subject matter and technical experts without charge.
  - All information required for the provision of Services and provided by parties other than Juniper must be accurate, complete and up to date. Juniper Networks will not be liable for any shortcomings, errors or deficiencies from inaccurate or incomplete non-Juniper information.
  - End User shall provide written notice to Juniper Networks as soon as it becomes aware or has reason to believe that (i) it will not meet one of its obligations under this Project Contract and/or (ii) any of assumptions referenced in this Project Contract will not occur, will not occur in a timely manner, are misleading or are inaccurate.

Equipment & Facilities

- End User is responsible for ensuring timely access to all facilities, equipment and tools and for ensuring that such facilities, equipment and tools are fully available, properly functioning and supported during the execution of Services.
- In the event work is performed onsite: End User will provide an adequate and reasonable office environment and equipment, including external access to the Internet, internal access to its Intranet and secure network connectivity to any required network equipment, applications and databases that are essential for successful completion of Services without additional charge.
- The End User is responsible for providing the NOC with full, complete, and timely access to any and all sites where Services will be performed, as well as all information, access to personnel and resources, etc. that the NOC will need to perform the Services.
- Where connectivity cannot be provided to Juniper Networks' own laptops, End User will provide alternative PCs with appropriate capabilities and connectivity or other functionally equivalent connectivity.
- Any additional equipment required for successful completion of the Services, such as network analysers, test equipment and/or laboratory equipment, will not be provided by Juniper Networks and must be provided by End User at End User's expense.
- Juniper Networks Products shall be procured, installed and powered, put into production and operational by End User outside of this Project Contract.

Availability

- Services, which are delivered remotely, are available to the End User location excluding countries listed in Group E under the U.S. Export Administration Regulations (currently, Cuba, Iran, North Korea, Sudan, and Syria) and any other countries as to which the furnishing of such Services may be prohibited by law or regulation.
- In the event that there is a site-related issue (loss of power to site, damage to premise cabling, accidental disconnection of cabling or equipment, or carrier issues) that causes on outage of devices or systems under NOC management, the NOC will document the issue within the NOC ticketing system, notify the End User, and track and manage the issue until resolution. The NOC will close the ticket once the site-related issue clears up. When the ticket is closed, the End User contact will receive an email indicating that the site-issue is resolved.
- In the event that a contracted device has a component hardware failure, the NOC will diagnose and attempt to resolve the issue remotely. If the hardware failure cannot be resolved remotely, the NOC will begin dispatch of a replacement part (via the End Users vendor support contract and letter of authorization) when needed.

Scope

- Services shall be delivered remotely (excludes Professional Services on Time and Materials (T&M) fee-basis) from an authorized Juniper location unless otherwise specified.
- End User understands and agrees that Juniper Networks may, in its sole discretion, subcontract the performance of the Services.

- Unless otherwise specified in writing by Juniper, all Service deliverables in this offering are available in English only unless otherwise specified in writing by Juniper and all information provided to Juniper Networks from End User (or a 3rd party at End User's direction) must be in English.
- End User acknowledges that the results it obtains from the Services are dependent on the accuracy of the information it provides Juniper Networks and will not be deemed deficient due to errors or deficiencies in End User-provided information.
- Juniper Networks is not responsible for providing any services or performing any tasks not expressly set forth in the Project Contract.
- Juniper Networks is not responsible for any obligations by and between End User and any other party.
- The parties will use best efforts to resolve any disputes or issues no later than five (5) working days after such disputes or issues arise.
- Where an unforeseen change is required and the parties cannot reach agreement in relation to such change, Juniper Networks shall, where it is unable to continue Services, stop Services without liability and End User will be invoiced and pay the full fee.
- The Project Contract start date, including staffing, onboarding and resource allocation required for the Services, will not commence until execution of the Project Contract and issuance by End User of a purchase order [and full payment] for the Services.
- Juniper's obligation to provide the Services is conditioned on the End User performing its obligations under the Project Contract
- 24x7x365 device and circuit monitoring to include real-time polling of devices to confirm their visibility to the NOC's network management systems, up/down status and archiving the events in the current and historical event log.
- Commercially reasonable efforts to detect, isolate, and diagnose each fault and restoration to normal operating conditions, testing and documenting each fault within the NOC's ticketing system.
- Ownership of resolution of the problem on behalf of the End User and act as an agent for the End User under executed letters of agency.
- End User notification of the progress of all faults per the End User provided contact and escalation process.
- Safeguard End User's proprietary information and take all necessary precautions to ensure a secure connection from the NOC into the End User's network.
- Secure End User web portal access to view the fault management alarms and event logs, open tickets and contact information; and
- Weekly and monthly reports.

Change control Requests

Juniper Networks will initiate these change control procedures if one or more of the following occur:

- End User requests a modification to the Services described in this SDD (including, but not limited to, the Juniper Networks Products being supported, additional services requests or other issues causing a modification to the scope, schedule or location or a delay in Juniper's ability to properly perform the Services); and
- Unforeseen factors change the scope of this SDD and/or impact the term and cost of Juniper Networks-provided Services that are outside the direct control of Juniper Networks. Unforeseen factors may include, but are not limited to, changes caused by new critical End User requirements, new information about the current network, requests for non-standard working hours, additional services, access and delays to the start of the Service Term.

When change control is initiated, End User and Juniper Networks may agree to revise the Project Contract and Juniper Networks will provide End User with an estimate of the impact of such revisions on the fees, payment terms, delivery schedule and other applicable provisions of this SDD. If the parties mutually agree to such changes, a written description of the agreed change ("Change Request") will be prepared and must be signed by both parties. The terms of a Change Request amend and prevail over any conflicting terms of the then-current Project Contract.

Exclusions

The following are examples of activities that fall outside of the standard Monitoring and Managed Service agreement. In the event these services are requested and can be delivered, they will fall into the Extended Professional Services (3.2.3) for remote work and T&M SOW's for any onsite activities or if other specialized skills are required. These activities will be scoped, agreed to and assigned to appropriate resources. This includes, but is not limited to, the following out of scope tasks for all contracted devices.

- Any physical staging, configuring and installing of equipment
- Software upgrades outside of security patches and/or minor revisions
- Major re-configuration activities to support non-break fix activities. (Not including MACD)
- Custom Reports (standard weekly, monthly reports will be provided)
- Help desk support for End Users. Only authorized Customer personnel will be approved to contact the NOC for support.
- On-site support. For exception, please see section 3.5.3.
- Firewall configuration and security policies
- Security operations including log and data analysis
- Security application monitoring, management and patching including SIEM, IPS, or IDS
- Security reporting including alerts for DDOS, Malware, Intrusion Attempts or Unauthorized Access Attempts.

In addition to the above, Juniper Networks is not obligated to provide services for any of the following:

- Problems with Products or software or parts thereof that are past their End of Support (as provided for in Juniper's EOL/EOS Policies) date.
- Unauthorized third-party products
- Third-party products with no active maintenance contract with the third-party vendor
- Gray market products.
- End User or third party modified software code.
- Lab testing

Glossary

Item	Definition
Services Delivery Location	REMOTE SERVICES – USA BASED DELIVERY
Service Term	The time between the contract start date and the end date.
Fault	Fault - A fault is defined as a failed device poll indicating the target device is not visible to the NOC's network management systems and tools.
Third-Party	Any organization other than Juniper Networks, Juniper Subcontractor or the End User.
On-boarding	Initial setup of active monitoring of devices as part of the Service. A one-time charge is included in the year one (1) pricing on a per device basis to initiate the Service. On-boarding services includes the initial setup of the connectivity to the Customer environment executing procedures for device information gathering, importing devices into the platform, and baselining the performance and fault data to be monitored.
MACDs	Move, Adds, Changes and Deletions (See Section 3.2.5) quantities will be specified on a per site basis.
Extended Professional Services	Extended Professional Services (See Section 3.2.3) may be contracted separately on a T&M basis to be consumed hourly or otherwise as specified in a separate SOW for work not covered by this SDD.
e-bonding	For the purposes of this SDD, e-bonding is defined as the interface between the JRMS ticketing system and Customer's system
Customer Service Manual	The document that contains details that define the service relationship and interaction between the NOC and the End User, and the processes that the NOC will follow during the service delivery phase.
Service Initiation Form	The document which provides all contracted infrastructure device information to enable the NOC to discover the contracted devices and load site information into the NOC's systems. The information includes, but is not limited to, device information, system access, network diagrams, site information, client contact information, circuit information, and current software levels and patch levels.
Change Order	A mutually executed contractual document between Juniper and the Customer to capture requested changes which are outside the scope of the then-current Project Contract.
Day 2 Support	The NOC starts to actively monitor and manage a device after the device being fully on-boarded (continuous availability for 2 weeks) in the NOC's system

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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: +31.0.207.125.700