

## Managed Juniper Mist Service Description

### Overview of Service

All Juniper Mist devices which are managed as part of the Service will be supported in accordance with the NTT processes described in the MCN Statement of Work. Technology specific tasks associated with the Juniper Mist technology stack are described in this section. The scope of the Managed Juniper Mist Service is as follows:

- Juniper Mist Wi-Fi Assurance including
  - Mist enabled AP series Access Points
- Juniper Mist Wired Assurance including
  - Mist enabled EX series Switches
- Juniper Mist WAN Assurance including
  - Mist enabled SRX Gateways
- Juniper Mist Cloud Controller

### Client Responsibilities and Prerequisites

- The Client must be in possession of an active hardware service contract for the network device(s) under management with the vendor, or a vendor approved third party such as NTT Uptime Support Services.
- The Client must delegate authority to NTT engineers, via letter of agency (LoA), to contact the vendor (or third party) directly for the purposes of the managed service
- Any license management, if required
- Administrative access to the Juniper Mist cloud based portal is required to manage the described devices
- Any Software or firmware operating on the device must be a version currently supported by the vendor
- Simple Network Management Protocol (SNMP) must be enabled and configured for devices to be managed as part of the Service

### Service Design

The complete Service is defined by the combination of the following items:

- **Managed Campus Network Service Operations**- service delivery operations that are common to all Managed Campus Network Services. See *MCN Statement of Work*, latest version.
- **Common Operations**- service delivery operations that are common to all services within the category of Network Management. See *MCN Common Network Management Service Description*
- **Service-Specific Operations**- service delivery operations that are specific to this Service. These operations are additive to the *MCN Statement of Work* and Common Operations.

### Juniper Mist Cloud Management Portal

All Juniper Mist physical and virtual devices are managed via the Mist Cloud platform, which acts as a centralized control plane. The Juniper Mist Cloud platform controls all endpoints, providing centralized functions like automated template provisioning and updates, de-commissioning, single screen administration, web-scale reporting, and monitoring and alerting.

Alerts can be configured for a variety of failure conditions. These alerts will be sent to NTT's ticketing system.

From a monitoring and management perspective, not all elements of Mist devices can be managed and monitored.


This is a limitation imposed on the solution by the vendor and not as a result of any restrictions enforced by NTT. Elements such as Interface drops, errors and bandwidth are not available for monitoring or reporting from NTT portal.

NTT will manage the Mist Cloud Portal for the devices included in the solution as explained in this section, including the following activities:

- Management of Configuration Templates, where applicable
- Configuration of reports to be sent to the Client
- Configuration of monitoring information as per Client needs and Mist capabilities

### Mist Controller Specific Monitors

The following monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
License	Status of Mist Licenses		N/A	Engineering Teams will notify the client 30 days in advance, if any of the license is going to expire	86400

### Juniper Mist Marvis

Marvis is Virtual Network Assistant by Mist and provides visibility and clarity with real time insights and simplified troubleshooting, allowing for faster incident resolution. NTT recommends this functionality is added for all clients.

### Periodic Maintenance Tasks

As part of the Service, supported periodic maintenance tasks included for Managed Campus Network devices is listed under Common Network Management Service Description.

## Configuration Management - Backup and Restore

An integral part of the Service is the management of the backup policy and execution of configuration restoration requests. The following tasks are included as part of Network Device Management:

Task	Description
<b>Configuration Backup Policy implementation</b>	Juniper Mist by default takes backup of all device configurations twice daily. The frequency or device configuration to be backed up are not configurable.
<b>Restore of System Configuration</b>	Restore of system configuration from the backup policy can be performed by creating a ticket in Mist portal.

The specifics of Mist Cloud Management Portal do not allow execution of the standard and typical backup and restore processes. As this is a cloud-based Service, the configuration is stored in the Cloud provided by Mist. Backup during configuration changes is an automated process in Mist and NTT is not responsible for taking configuration backup. For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

## Firmware Review

Keeping up-to date on firmware allows administrators to utilize the latest features and ensures that the latest security enhancements are running on their hardware. Because Mist is Cloud-based, many aspects of operation and controlled by the vendor and result in specific limitations and or restrictions. These upgrades can be for beta versions of the firmware (only advised under guidance of the vendor) or stable versions.

Upgrades can be scheduled to take place outside of critical business hours from the Dashboard. Firmware upgrades can be manually manipulated in the Mist Dashboard under Organization -> Site Configurations and it is supported only for Access Points from the portal.

The options defined here include:

- Schedule an upgrade for a specific date and time for Access Point to production firmware
- Schedule an upgrade for a specific date and time for Access Point to rc2 firmware
- Auto upgrade to specific firmware for each Access Point within the site
- Disable auto upgrade and upgrade specific firmware for the device manually.

It should be noted that the options will only apply to those devices for which an upgrade is available. The firmware upgrade strategy must be agreed with NTT during the setup of the Mist environment.

## Service Transition

### Tasks Included in the Standard Transition

As part of the Service, the following tasks are included in the setup fee to validate NTT's ability to manage the devices:

- Inventory of the device
- Review of the existing Juniper Mist templates
- Review of the configuration of network interfaces
- Review high availability and redundancy configuration
- Review of firmware upgrades and recommendation if upgrade is required. If the Client chooses to proceed with the upgrade, the process defined for firmware patching in the MCN Service Schedule will be followed.
- Change of the credentials required by the administrative and supervisor users required for management by NTT
- Review and change the configuration of syslog or SIEM parameters (if a syslog or SIEM exists)
- Review and documentation of the device configuration
- Deliver recommendations after the initial review by NTT network engineers
- In *high availability* environments, review and documentation of the Service high availability, clustering or stack configuration
- Creation and review of monitoring
- Documentation of the device

### Tasks excluded from the Standard Transition

The following tasks are excluded from the standard transition require further services:

- Physical activities at the premises where the device is installed
- Audit and review of the physical premises where the device is installed
- Review of the configuration or actions of other connected devices not under management
- Upgrading and or patching the device firmware
- Analysis and redesign of the network topology is an activity that can be conducted as a chargeable engagement, if not included as part of the Statement of Work, or
- Remediation Activities to be conducted after the audit may be chargeable, if not included as part of the Statement of Work.

Juniper Mist SRX Gateway Devices

Juniper Mist SRX gateway devices provide security and routing functionality.

## Supported Configurations

- Physical devices

- HA security appliance configurations - two compatible physical or virtual security appliances in an active / passive configuration, both connected at the same time.
- Create, delete, modification of security zones and associated interface configurations etc.
- Create, delete, modifications of layer3 physical interfaces.
- Create, delete, modification of layer3/4 port-based access list without security profiles.
- Create, delete, modification of "one to one" / "many to one" Source static & Source dynamic NAT policies.
- Create, delete, modification of basic S2S IPsec with pre-shared key & Static routes.
- Create, delete, modification of basic Remote access VPN configuration with local accounts.
- Create, delete, modification of Default & Static routes.

### Supported Technologies

For a listing of supported Routing and Security Appliance models and their respective sizing, consult the MCN Supported Technology documentation.

### Security Appliance Specific Monitors

The following monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Interfaces	Status of device interfaces (virtual or physical), sent / received packets and bytes	✓	Graphs of the parameter measured over time	Engineering Teams will solve the issue	600
Device Status and Operational State	Operational status of the device	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
HA Status (if any)	Check the status of High Availability	✓	N/A	Engineering Teams will solve the issue	180

### Service Requests

As part of the Service, the fulfilment of the tasks listed in the table below are included.

### Juniper Mist Security Appliance Service Requests

Task	Description	Included
<b>Management of Security Zones</b>	Create, delete, modification of security zones and associated interface configurations etc.	✓
<b>Creation and management of VPNs</b>	Creation, change and deletion of VPNs configured in the device, including the users in the VPNs; this does not include connection to the external peer to configure the remote end point, or the installation of any customer on any end user computer.	✓
<b>Management of access rules</b>	Creation, change and deletion of access rules configured in the device that allow and deny traffic to/from the servers in the DMZs and other internal networks without security profiles.	✓
<b>Creation and management of NATs</b>	Create, delete, modification of "one to one" / "many to one" Source static & Source dynamic NAT policies.	✓
<b>Routing management</b>	Create, delete, modification of Default & Static routes.	✓
<b>Management of failover</b>	Only in HA or clustering configurations: management of failover policy to allow the service to continue working if a device error occurs	✓
<b>Management of disk space</b>	Evaluation and study of actions for freeing and optimising disk space (if disk is present in the device)	✓
<b>Bandwidth Management and connectivity features</b>	Basic creation, addition or deletion of Bandwidth Management, Quality of Service or shaping rules. Additionally, changes to the most specific routing features, including changes and reconfiguration of: <ul style="list-style-type: none"> <li>• Branch Routing (route redistribution) administration</li> <li>• Traffic shaping management</li> <li>• Dual uplink port management</li> </ul>	✓

Task	Description	Included
<b>Management of SSL certificates and settings</b>	Addition, removal and modification of SSL certificates associated to the device and services	✓
<b>Relaying of network generic services</b>	Configuration of NTP, DHCP and DNS settings for these to be resolved by external services	✓
<b>Creation and management of Geo-based security</b>	Configuration and management of: <ul style="list-style-type: none"> <li>• Reputation</li> <li>• Geo-IP and Botnet filter</li> <li>• Other Geo-related policies</li> </ul>	✓
<b>Forward logs to an external SIEM service</b>	Changes in the settings to forward logs to an external SIEM and SOC solution, destination, port, and/or information being sent	✓

## SRX Requests Excluded from the Service

### IDS / IPS

IDS and other advanced security features' correct operation is heavily dependent on the application(s) being protected, which means that the ones applying the intelligence on the security policy must be the Client's relevant contacts. The scope of the managed IDS and advanced security features will be limited to applying changes based on what the Client requests. NTT expects the Client will identify the changes to perform based on the SIEM (or whatever the log management tool the Client uses). On the SIEM, the reason why applications are blocked generating false positives, or not blocked when these should, would be identified by the Client. As part of the ongoing management of an Advanced Security device, it is not included in the review of all the logs for an unidentified error or false positive. This is an activity for the Client to perform. While NTT will make all attempts to reduce the number of false positives, it will not be responsible for authentic users being denied access to the Client application.

### SIEM Services

A SIEM independent log management system or SOC threat analyst team is not included as part of the Mist SRX Management Service. This means that the detection of vulnerabilities, threats and similar security activities are limited to the features included in the devices under management and that NTT will not include additional tooling. As such, the following is not part of the Service unless additionally contracted:

- Log Management Service
- Log Correlation Service
- Threat Correlation, Collaborative Intelligence, Monitoring and Analysis of Logs with SOC analysts to detect and/or investigate alerts

## Service Transition

### Tasks Included in the Standard Transition

As part of the Service, the following tasks, when defined by the design authority are included in the setup fee to validate NTT's ability to manage the devices:

- Registration of the device to the Juniper Mist portal
- Create, delete, modification of security zones and associated interface configurations etc.
- Create, delete, modifications of layer3 physical interfaces.
- Create, delete, modification of layer3/4 port-based access list without security profiles.
- Create, delete, modification of "one to one" / "many to one" Source static & Source dynamic NAT policies.
- Create, delete, modification of basic S2S IPsec with pre-shared key & Static routes.
- Create, delete, modification of basic Remote access VPN configuration with local accounts.
- Initial licenses and contracted subscriptions configuration
- Configuration of Geo-based security
- Configuration of log relaying and other log management mechanisms if contracted.
- Routing configuration in the Mist Portal, if supported
- Dual uplink port configuration
- Configuration of Branch Routing (route redistribution) policies
- Configuration of Traffic shaping, Bandwidth Management and Quality of Service

### Optional Tasks

The following tasks may be provided at additional charge, unless specified in the Statement of Work:

- Security policy definition: this is a consultancy task which must be contracted in addition to the Service
- Analysis of the Clients applications, consultancy, audits and advisory services are not included in the setup fee
- SIEM and SOC services
- Hardware, Software and/or support around it

## Juniper Mist EX Switches

Juniper Mist EX switches provide wired switching functionality in Juniper Mist networks.

### Supported Configurations

- Single switch (standalone switch) or a set of standalone switches (managed independently from each other)
- Stacked switch
- Set of switches in high availability configuration i.e. two or more switches of compatible models in an HA configuration

### Supported Technologies

For a listing of supported Switching models and their respective sizing, consult the MCN Supported Technology documentation.

### Switch Specific Monitors

The additional monitors which can be configured for switch management are:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
<b>Availability</b>	Device is available	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
<b>Interfaces</b>	Status of device interfaces (virtual or physical), sent / received packets and bytes	✓	Graphs of the parameter measured over time	Engineering Teams will solve the issue	600

### Service Requests

As part of the Service, the fulfilment of the tasks listed in the table below are included.

### Juniper Mist EX Switch Service Requests

Task	Description	Included
<b>Creation and management of VLANs</b>	Creation, change and deletion of VLANs configured in the device and its nodes	✓
<b>Management of spanning tree</b>	Management of the spanning tree protocol to handle link redundancy	✓
<b>Routing management</b>	Management of the routing elements available in the firewall	✓

All of the above tasks will be performed according to the Change Management process defined in the *MCN Statement of Work*.

## Service Transition

### Tasks Included in the Standard Transition

As part of the Service, the following tasks are included in the setup fee to validate NTT's ability to manage the devices:

- Creation of VLANs
- Configuration of spanning tree
- Service clustering (in stack environments)

### Juniper Mist Access Points (AP)

Juniper Mist AP Wireless infrastructure provides the cloud-based control plane, as well as wireless Access Points (AP's) that form part of a Juniper Mist network.

### Supported Configurations

- Juniper Mist APs will only be managed from the Mist Cloud platform

### Supported Technologies

For a listing of supported Switching models and their respective sizing, consult the MCN Supported Technology documentation.

## Service Transition

### Tasks Included in Standard Transition

As part of the Service, the following site-specific tasks are included in the setup fee to validate NTT's ability to manage the devices:

- Creation of SSID's and WLANs


- Creation and configuration of security policies
- Addition of AP's to networks
- Connection to external user directory or database

**Tasks Excluded from Standard Transition**

- End User support, or
- Management of AP's that are not in-scope

**Wireless Controller Specific Monitors**

The additional monitors which can be configured for Wireless Controller management are:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Availability	Device is available.		N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed.	180