Managed Aruba Technical Service Description

Overview of Service

All Aruba 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 Aruba technology stack are described in this section. The scope of the Managed Aruba service is as follows:

- Aruba Access Points
- Aruba Mobility Controller
- Aruba Switches
- Aruba Gateways (Security Appliances / Routers)
- Aruba Central (cloud management platform)
- Aruba Airwave (On premise management platform)
- Aruba ClearPass secure network access control software

Further detail on these service offers can be found in their specific sub-sections.

Client Responsibilities and Prerequisites

- The Client must be in possession of an active hardware service contract for the devices(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 to contact the device vendor (or third party) directly for the purposes of the managed service
- Any licenses management, if required
- 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
- Administrative access to the Aruba Central SaaS based portal, or the on-premise instance of Aruba Central, Aruba Airwave, or the individual Mobility Controller instances is required to manage the described devices.

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.

Configurations Not Supported

The managed Aruba Service does not include management of location services applications running on top of the Aruba technology stack.

Tasks Included in the Standard Transition

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

- Inventory of the device
- Creation of templates for the different Aruba devices
- Setup of initial access - configuration of network interfaces
- Application of firmware upgrades to the latest recommended level
- Creation of administrative and supervisor users required for management by NTT and the Client
- Configuration of syslog parameters (if an external syslog or SIEM service exists)
- Configuration of high availability (if 2 devices exist)
- Monitoring setup
- Configuration backup setup
- Configuration management set up and implementation of security standards
- Device documentation

Tasks Included in the Takeover of a Client System

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 Aruba templates
- Review of the configuration of network interfaces
- Review of firmware upgrades and their installation if agreed with the Client as detailed in the *MCN Statement of Work*
- Change of the credentials required by the administrative and supervisor users required for management by NTT and the Client
- 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 highly available environments*: Review and documentation of the high availability, clustering or stack configuration of the Service
- Creation and review of monitoring
- Configuration backup setup
- Implementation of security standards
- Documentation of the device

Tasks Excluded from the Standard Transition

- Rack mounting of the device(s)
- Physical setup (cabling of Ethernet and power chords) and labelling of the device(s), or
- Configuration of other connected device(s) not managed by NTT

These tasks can be completed by the relevant NTT country or regional team as required.

Tasks excluded from taking over of an existing installation, and 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
- 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

Aruba Device Management via Centralized Management Portal

The Managed Aruba Service offer has 3 options for management of Aruba technology:

1. Aruba Central – this is a cloud based (SaaS) network management solution that encompasses full service AI insights, security and unified infrastructure management of branch, remote and data center networks. This platform is the preferred choice for Aruba device management.
2. Aruba Central On Premise – this is an on-premise version of the cloud based SaaS offering.
3. Aruba Airwave – this is an on-premise software solution, that runs on dedicated hardware, or as a virtual appliance. Airwave is a versatile network management system for enterprise campus wired, wireless and remote connectivity. Airwave consolidates information from Mobility Master instances into a central place.

The NTT Managed Aruba Service offer will manage all aspects of the Client's network leveraging one of these 3 tools. Where one of these 3 tools is not available, management of access points via the local Mobility Master instance will be utilized for device management.

Aruba Central SaaS portal Management & Aruba Airwave

The Aruba Central portal provides:

- multi-tenant centralized management
- management options like automation of provisioning, licensing, de-commissioning with single screen administration, and web scale reporting
- GUI based configuration capability across all Aruba devices in a network, as well as auto-deployment services using predefined or customized templates, Software upgrades, monitoring, and alerting

NTT will manage the Aruba Central portal for the devices included in the solution as explained in this section, including the following activities:

- Management of *Configuration Templates*
- *Configuration of reports to be sent to the Client*
- *Configuration of monitoring information as per Client needs and Aruba Central capabilities*

The following information can be captured in alerts from the Aruba Central Management portal:

- Device MAC address
- Device Serial Number
- Device Name
- Device Status (Online or Offline)
- Device Last Contacted - Date and Time
- Mesh Status (Gateway or Repeater)
- Public IP Address (if applicable)
- Product Code
- Product Description (e.g. Aruba AP xxxx)
- Name of the Network that the device resides in (Dashboard Network)
- Packets/Bytes In/Out on each physical interface

Supported Configurations

- Single Airwave instance: A standalone on-prem Aruba Airwave instance.
- Set of Airwave instances in high availability configuration: Two or more on-prem Airwave instances that have been configured as an HA pair.

Monitors

Monitoring will be performed in accordance with the process described in Event Management (see *MCN Statement of Work*). The following monitors are configured by default for all Managed Aruba Device types:

Sensitivity Label: General

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Ping / Network	Time taken for responding to a Ping from a poller and packet loss	✓	N/A	Engineering Teams will resolve the issue	60
Device Availability	Up / Down status of the device	✓	N/A	Engineering Teams will resolve the issue	180
CPU	CPU usage of the device	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	180
Memory	Memory usage of the device	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	240

NTT can follow the procedures below for escalating the following Events to the Client:

Escalation Task	Description
Email message	Generation of an email message with the following information: • System that generated the alert • Configured Thresholds • Threshold that caused the error • Additional diagnostic information
Phone call	Phone call to a defined number, notifying the Client about the error condition and all the background information around the alert

Periodic Maintenance Tasks

As part of the Service, the following periodic maintenance tasks are included for Managed Aruba Devices:

Task	Frequency	Description
Firmware review	Continuous process	Notify the Client of outstanding critical firmware upgrades which address vulnerabilities that may affect the Service, such as security exploits or bugs. If the Client chooses to proceed with the upgrade, follow the process defined for firmware patching in *the MCN Statement of Work*. Upgrade of firmware is not considered the same as patching, but as an installation of a new operating system version for the device.
Configuration Management		Review of the correct execution of the associated configuration backup; in case of an error with the execution of a backup configuration, resolution will follow the process for Incident Management.

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. Admins can upgrade to the latest stable or latest beta firmware. NTT will communicate with the Client to proceed with the firmware update:

- For all the networks in scope
- For a series of networks of the total scope
- For all the devices of a certain type
- For all devices in a certain version, or
- For an individual device

The firmware upgrade will not be executed unless:

- It was previously agreed as part of the Patching Design sessions with the Client (as an example, all the critical security patches must be applied within 24 hours of a firmware release), or
- It was approved by the Client specifically

The firmware upgrade will be executed at an agreed time by NTT engineers. The firmware upgrade process can happen out of business hours if required.

Sensitivity Label: General

Configuration Management - Backup and Restore

Aruba Central SaaS portal Managed Devices

The specifics of the Aruba Central Service does 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 Aruba. All the changes to the configuration can be checked using the configuration audit menu from within the Aruba Central portal. The Change Log allows checking of all the changes executed in a Aruba deployment. This is helpful for basic troubleshooting and manual changes on individual Client requests.
As per the current Aruba Central configuration, only devices managed using the template-based configuration method can be backed up centrally. Any manually configured settings such as local overrides may not be backed up nor restored. Because of this behavior of the Aruba Central portal, the backup and restore process will include a mix of automatic and manual processes. NTT will have documented in the CMDB, in addition to the backup details extracted from the Aruba Central portal using automatic tooling, all the parameters that would require additional manual actions.

Aruba Central On-Premise, Aruba Airwave, or Mobility Controller Managed Devices

The Aruba Central On Premise version, the Aruba Airwave software stack, and individual Aruba Mobility Masters support backup of all data (device templates and configs, as well as the management system database) and shipping of that backup file to an SFTP or SCP server.
Unless specified in the Statement of Work, the Client is responsible for providing suitable SFTP or SCP infrastructure to facilitate backup and restore activity.
Recommended minimum disk space for Aruba Central On-Premise data backup is 5 TB. For Airwave, recommended minimum disk space for backup is 120GB. This needs to be evaluated based on the complexity of the device configuration and the number of devices managed.
For details of backup and restore, consult MCN Managed Configuration Backup Service Description

Service Requests

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

Aruba Central Service Requests

Task	Description	Included
Creation of users / groups	Creation of users and groups in the portal, including password maintenance	✓
Management of network interfaces (ports)	Creation and changes in the network interface parameters (IP addresses, gateways, ...)	✓
Log subsystem configuration	Management of log information, resending to a syslog server (if any)	✓
Management of vendor support	Management of hardware or firmware errors with Aruba. The Client must authorize NTT to open support cases with the vendor, during the onboarding and transition in project	✓
Configuration Management: data restoration	Restore device configuration from backup, either as an automatic process from the Aruba Central SaaS portal, or as a mix of automatic and manual processes from configuration backups stored external to the Aruba Central portal, or for the Aruba Central on-premise or Aruba Airwave Software	✓

Managed Aruba Switching

Supported Technologies

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

Supported Configurations

- Single switch: A standalone switch or a set of standalone switches (managed independently from each other)
- Set of switches in high availability configuration: Two or more switches of compatible models in an HA configuration

Specific Tasks Associated with the Installation of a Switch

As part of the Service, the following tasks are included in the setup fee:

- Creation of VLANs
- Creation and configuration of spanning tree
- *In stack environments*: Service clustering

Switch Specific Monitors

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

Sensitivity Label: General

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Port Usage	Check port's bandwidth usage	✗	Graphs for the parameter measured over time	N/A	120
Port Status	Check port's status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	60
Hardware Status	Check switch hardware failure status	✓	N/A	Engineering Teams will diagnose , try to resolve the issue, and escalate to the vendor if needed	180
Switch PoE Utilization (if applicable)	Check Power over Ethernet utilization for the specific switch	✓	N/A	If power utilized exceeds threshold, Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	300

By default, 4 uplink ports are monitored per Edge switch. Additional ports can be monitored on request, at additional cost.

Configuration Management - Backup and Restore

Configuration backup of Aruba switches not managed by Aruba Central or Aruba Airwave will be stored in NTT Managed cloud.
For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

Backup and Restore Testing

NTT includes the following backup and restore schedule:

- Daily review of the correct execution of the associated configuration backup; in case of an error with the execution of a backup configuration, resolution will follow the process for Incident Management
- As part of onboarding and transition, NTT can, on the Client's request, perform a restore of a device's configuration, to validate successful backup completion

By default NTT does not provide routine backup restore testing. Quarterly or annual backup restore testing can be provided at additional cost, unless this has been specified in the Statement of Work.

Service Requests

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

Aruba Switch Service Requests

Task	Description	Included
Creation and management of VLANs	Creation, change and deletion of VLANs configured in the device and its nodes	✓
Management of spanning tree	Management of the spanning tree protocol to handle link redundancy	✓
Management of port channel / ether channel	Creation, change and removal of port channel interfaces	✓
Addition or removal of switches	Addition of new switches (either independently or to existing switch stacks) or removal of switches	✓

All of the above tasks will be performed according to the Change Management process defined for the Client.

Managed Aruba Gateways (Security Appliances)

General Statement relating to Management of Security Appliances

Please note that NTT will make changes to security devices under management, based on Client instruction. The Client is fully and solely responsible for the security of their environment. Where a designated Client security contact requests a change to the security policy of a device under management, NTT will make this change on the Client's behalf, under appropriate change control. Any security specific Incidents or alerts generated by this device will be directed to the Client for confirmation of the approach to take.

Prerequisites

- Access to the Aruba Central SaaS portal, on-premise installation or instance of Aruba Airwave to manage the described devices
- An appropriate license that enables advanced routing and/or Security functionality (if required)

Sensitivity Label: General

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

Supported Security Appliance Configurations
- Single security appliance / gateway: a standalone security appliance / gateway
- HA security appliance / gateway configurations (only physical devices): two security appliances / gateways of compatible models in an active/passive configuration, both connected at the same time (fail recovery can be manual)

Security Appliance Configurations Not Supported
- Virtual security appliances / gateways with HA configuration in public clouds, or
- Virtual security appliances / gateways functioning as perimeter security appliance in a private cloud solution

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:
- Registration of the device to Aruba Central portal (either SaaS or on-premise) or Airwave 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.
- Initial licenses and contracted subscriptions configuration
- Configuration of error pages and error page groups
- Configuration of log relaying and other log management mechanisms if contracted
- Routing configuration in the Aruba portal or Airwave appliance
- Dual uplink port configuration (if applicable)
- LTE failover configuration (if applicable)
- Configuration of Intelligent Path Control policies
- Create, delete, modification of Default & Static routes.

Optional Tasks (additional charges will apply)
- Security policy definition: this is a consultancy task which must be contracted in addition to the Service
- Analysis of the Client's applications, consultancy, audits and advisory services are not included in the setup fee
- SIEM and SOC services
- Hardware, Software and/or support around it

Required from the Client: Aruba Security Appliance / Gateway Management
As a general approach, the following will happen when a IDS/IPS device is activated as part of a managed service:
- The installation process will configure all the policies as desired by the Client
- This will generate a large number of false positives, so on the first days of the Service the security policy should be loosened
- Additional rules are added little by little to strengthen the security policy
- This will eliminate false positives and provide a more secure environment for the Client's applications
- Once stabilised, no more changes would be required until new versions of the Client's applications are released and deployed. At that moment, the process can start again

Because of the above expected results, it is important that the starting point of the security appliance policy operation counts with the relevant Client contacts to adapt the security appliance policy to the Client's applications. This activity is not something the engineers managing the devices will do. In the case of issues once the policy has been activated, the only expected outcome from the engineers will be complete deactivation of the policy or (if possible) change the policy from "Block" to "Alert", "Log" or whatever non-blocking option is available. 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's application.

Security Appliance / Gateway Specific Monitors
The following monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Disk(if any)	Disk usage in %	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	180
Interfaces	Check of the device interfaces (virtual or physical)	✓		Engineering Teams will diagnose and try to resolve the issue	300

Sensitivity Label: General

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Sessions	Check the number of current/active sessions in the device	✓	Graphs for the parameter measured over time	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	✓		Engineering Teams will diagnose and try to resolve the issue	60
Routing Protocols	BGP or OSPF session errors, route table limits	✓		Engineering Teams will diagnose and try to resolve the issue	180
Licensing	Check whether license capacity limits have been exceeded	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Cellular Data Usage (if any)	Alerts when Cellular data usage exceeds the defined threshold	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	900
WAN Uplinks	Alerts related to WAN uplink ports	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300
IPSEC	Alerts for IPSEC tunnel related issues	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	60
WAN Health Alerts	If configured, alerts related to WAN uplink health (throughput, loss, latency, jitter)	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	60

Configuration Management - Backup and Restore

Configuration backup of Aruba security appliance and gateway not managed by Aruba Central or Aruba Airwave will be stored in NTT Managed cloud.
For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

Not Included Client Requests or Troubleshooting Activities: Advanced Aruba Gateway Service

- 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, are identified by the Client.
- As part of the ongoing management of an Advanced Aruba Gateway device, the review of all the logs for an unidentified error or false positive is not included. 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.

Not Included Client Requests or Troubleshooting Activities: Advanced Routing

- Advanced routing features and configuration depend on the applications being routed. Not having access to the applications, NTT support can only apply on the monitoring capabilities of the contracted Aruba Software features.

Not Included Ongoing Maintenance Activities

A SIEM independent log management system or SOC threat analyst team is not included as part of the Advanced Aruba Gateway 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 for it. As such, the following is not part of the Service unless additionally contracted:

- Log management service
- Log correlation service

Sensitivity Label: General

- Threat Correlation, Collaborative Intelligence, Monitoring and analysis of logs with SOC analysts to detect and/or investigate alerts

Disclaimer

While NTT will help the Client in resolving security issues, NTT does not take responsibility for any loss as a result of a Security Incident. NTT will use reasonable efforts to resolve Problems as quickly as possible.

Service Requests

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

Aruba Security Appliance / Gateway Service Requests

Task	Description	Included
Creation and management of security zones	Creation, change and deletion of Security Zones configured in the device	✓
Creation and management of VPNs	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 client on any end user computer	✓
Management of access rules	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	✓
Creation and management of NATs	Create, delete, modification of “one to one” / “many to one” Source static & Source dynamic NAT policies.	✓
Routing management	Create, delete, modification of Default & Static routes.	✓
Management of failover	Only in HA or clustering configurations: management of failover policy to allow the service to continue working if a device error occurs	✓
Management of disk space (if applicable)	Evaluation and study of actions for freeing and optimizing disk space (if disk is present in the device)	✓
Bandwidth management and connectivity features	Basic creation, addition or deletion of Bandwidth Management, Quality of Service or shaping rules. Additionally, changes to the most specific routing and connectivity features, including changes and reconfiguration of: • Intelligent Path Control administration • Branch Routing (route redistribution) administration • Traffic shaping management • Dual uplink port management • LTE failover management • LTE data usage alerting and management	✓
Management of SSL certificates and settings	Addition, removal and modification of SSL certificates associated to the device and services	✓
Relaying of network generic services	Configuration of NTP, DHCP and DNS settings for these to be resolved by external services	✓
Forward logs to an external SIEM service	Changes in the settings to forward logs to an external SIEM and SOC solution, destination, ports and or information being sent	✓
Forward logs to a managed log management service	Changes in the settings to forward logs to an associated (and managed) log management system	✓

Managed Aruba Wireless Controllers

Aruba wireless controllers are Aruba’s legacy method of managing fleets to AP’s. This Service is only required when taking over an existing Aruba deployment. New environments would likely contain gateways, switches and Instant Access Points (IAP’s), and not individual wireless controllers (as Aruba Central provides this functionality).

Sensitivity Label: General

Supported Technologies
For a listing of supported Aruba Wireless Controller models and their respective sizing, consult the MCN Supported Technology documentation.

Supported Components
- Management of Aruba Mobility Masters (which in turn manage fleets of Mobility Controllers)
- Management of 7000 series, and 7200 series appliances acting as Mobility Controllers

Specific Tasks Associated with Installation
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 SSID's, VLANs and WLANs
- Creation and configuration of new wireless networks
- Creation and configuration of security policies
- Connection to external user directory or database
- *In HA environments*: Service clustering

Specific Tasks Not Included with Installation
- End user support; or
- Management of the AP's if these AP's are not in-scope

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

Monitor	Description	Alerts	Resolution	Poll Intervl (sec)
Availability	Device is available	✓	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Authentication Service	If authentication service is used, check availability and response time	✓	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300
Interfaces	Check interface response time, as well as a range of statistics for interfaces (throughput, utilization, packets in / out), port errors, TCP / UDP errors and re-transmits	✗	N/A	300
IAP Clients	Number and type of client devices connected to IAP's (Instant Access points)	✗		180
Temperature	Check whether WLC device temperature is within normal range	✓	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180

Configuration Management - Backup and Restore
Configuration backup of Aruba Wireless Controller not managed by Aruba Central or Aruba Airwave will be stored in NTT Managed cloud.
For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

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

Aruba Wireless Service Requests

Task	Description	Included
Creation and management of VLANs	Creation, change and deletion of VLANs configured in the device and its nodes	✓
Creation and management of WLANs	Creation, change and deletion of WLANs configured in the device	✓
Creation and management of MACs	Creation, change and deletion of MAC addresses configured in the device, including auto-discovery; this does not include connection to the external device to configure the remote NIC	✓

Sensitivity Label: General

Task	Description	Included
Creation and management of security policies	Creation, change and deletion of security policies in the controller	✓

All of the above tasks will be performed according to the Change Management process defined for the Client.

Managed Aruba Access Points

Supported Technologies
For a listing of supported Aruba Wireless Access Point models and their respective sizing, consult the MCN Supported Technology documentation.

Supported Configurations
- By default IAP / UAP Aruba Access Points will only by managed by NTT from an Aruba Central SaaS, on-premise or Airwave instance
- CAP Aruba Access Points, the optional Aruba Wireless Controller Management Service is required, as these Access Points need to connect to a Aruba Mobility Controller
- In both solution scenarios, AP's are monitored indirectly via the controller. Direct AP monitoring via SNMP can be provided for IAP's at additional charge

Access Point Specific Monitors
The additional monitors which can be configured for Access Point management are:

Monitor	Description	Alerts	Resolution	Poll Interval (sec)
Availability	Device is available	✓	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Radio	Radio channel utilization, noise floor	✗	N/A	180
Connected Clients	Connected Clients per AP or Controller	✗	N/A	180

Specific Tasks Associated with Installation
As part of the Service, the following tasks are included in the setup fee to validate NTT's ability to manage the devices:
- Add the device to Aruba Central portal or Airwave instance
- Add the device to the Aruba Mobility Controller or Mobility Master

Specific Tasks Not Included with Installation
- End-user support

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

Aruba Wireless Access Point Service Requests

Task	Description	Included
Creation and management of security policies	Creation, change and deletion of security policies in the AP	✓

All the above tasks will be performed according to the Change Management process defined for the Client.

Managed Aruba ClearPass
Aruba ClearPass is a network access control software solution from Aruba, that provides device visibility, control and attack response. This is achieved through 3 core functions:
- Identify - what devices are being used, how many, where they are connecting from, and which OS's are supported
- Enforce – accurate policies that provide proper user and device access, regardless of user, device type or location
- Protect – resources via dynamic policy controls and real-time threat remediation

Aruba ClearPass integrates with a number of identity stores and third party security solutions.

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

Supported Configurations
- Single appliance: A single Aruba ClearPass physical or virtual appliance

Sensitivity Label: General

- Multiple Aruba ClearPass devices in high availability configuration: Two or more Aruba ClearPass devices in an HA configuration

Unsupported Configuration

- Unless specified in the relevant Statement of Work, management of external IAM sources, or third party security integrations is not included

Aruba ClearPass Specific Monitors

The additional monitors which can be configured for Aruba ClearPass management are:

Monitor	Description	Alerts	Resolution	Poll Interval (sec)
Availability	Device is available	✓	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
HTTP / HTTPS	Status and response time for HTTP / HTTPS page loads	✓	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	60
System	System health (disk, memory, etc)	✓	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Network	Check interface response time, as well as a range of statistics for interfaces (throughput, utilization, packets in / out), port errors, TCP / UDP errors and re-transmits	✗	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	120
Authorization Sources	Authorization source counters (total, success, failure)	✗		

Configuration Management - Backup and Restore

The Aruba ClearPass supports backup of complete configuration to an SFTP or SCP server. Unless specified in the Statement of Work, the Client is responsible for providing suitable SFTP or SCP infrastructure to facilitate backup and restore activity.
Recommended minimum disk space for backup is 12GB. This needs to be evaluated based on the complexity of the device configuration and the number of devices managed.
For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

Specific Tasks Associated with Installation

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

- Creation and configuration of security policies
- Connection to external user directory or database
- Connection to an external security source
- *In HA environments*: Service clustering

Specific Tasks Not Included with Installation

- Roles Based Access Control (RBAC) policy definition for dynamic segmentation: This is a consultancy task which must be contracted in addition to the Service
- End user support

Specific Tasks Excluded from the Service

- End user support, including OS and PKI related issues
- Movement of individual users between dynamic segmentation groups within ClearPass. It is expected that the Client will perform these functions in the IAM source (and not in ClearPass)

Optional Tasks (additional charges may apply)

- Definition of ClearPass policies: This is a consultancy task that must be contracted in addition to the Service
- Roles Based Access Control (RBAC) policy definition for dynamic segmentation: This is a consultancy task which must be contracted in addition to the Service
- Analysis of customer's applications, consultancy, audits and advisory services are not included in the setup fee
- SIEM and SOC services
- Hardware, Software and/or support around it
- Migration from, or replacement of an existing Identity and Access Management source with a new one. This is a complex change that will require design consultancy

Sensitivity Label: General

Not Included Ongoing Maintenance Activities

A SIEM independent log management system or SOC threat analyst team is not included as part of the Aruba ClearPass 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 for it. 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 Requests

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

Aruba ClearPass Service Requests

Task	Description	Included
Creation and management of ClearPass policies	Creation, change and deletion of policies in the ClearPass platform (eg; staff, guest or BYOD access policies)	✔
Changes to device health check policies	Changes to what a device health check policy probes for on connected devices	✔

All the above tasks will be performed according to the Change Management process defined for the Client.

Disclaimer

While NTT will help the Client in resolving security issues, NTT does not take responsibility for any loss as a result of a Security Incident. NTT will use reasonable efforts to resolve Problems as quickly as possible.