Device Management Standard

Name	NTT Service Description – Device Management Standard
Owner	NTT
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V1.2
Date	29 March 2019

Contents

1 Service Matrix **3**

2 Service Prerequisites **3**
2.1 General Requirements 3
2.2 Communication Requirements 4

3 Core Service Elements **5**
3.1 Hours Of Operation 5
3.2 Security Operation Centers (SOCs) 5
3.3 NTT Portal 5
3.4 Language Support 5
3.5 Management Of Devices 5
3.6 Communications 5
3.7 Escalation Management 6

4 Service Transition **6**
4.1 Engagement Phase 6
4.2 Planning Phase 7
4.3 Staging Phase 7
4.4 Integration Phase 7
4.5 Go-Live Phase 7
4.6 Service Transition Deliverable Acceptance 7

5 Device Management Features **8**
5.1 Health And Availability Monitoring 8
5.2 Incident Management 8
5.3 Capacity Management 9
5.4 Asset Tracking And Reporting 9
5.5 Service Request Fulfilment 9
5.6 Problem Management 10

6 Terminology And Definitions **10**

7 Operational Level Agreements **10**

8 Changes In Service **10**
8.1 Regulatory Change Requirements 10
8.2 Method Of Service Delivery 10
8.3 Supported Devices 10

9 Service Exclusions **10**

10 Controlling Terms **11**

1 Service Matrix

The Device Management Standard service consists of a core set of Service Modules and associated Service Elements.

Section	Service Modules and Elements	Device Management Standard
0	Core Service Elements	
3.1	24/7 Hours of Operation	✔
3.2	Security Operation Centers	✔
3.3	NTT Portal	✔
3.4	Language Support	✔
3.5	Management of Devices	✖
3.6	Communications	✔
3.7	Escalation Management	✔
4	Service Transition	
4.1	Engagement	✔
4.2	Planning	✔
4.3	Staging	✔
4.4	Integration	✔
Error! Reference source not found.	Go-Live	✔
5	Device Management Features	
5.1	Health and Availability Monitoring	
5.1.1	Health and Availability Monitoring	✔
5.1.2	Health and Availability Improvement and Recommendation	✔
5.1.3	Health and Availability Change Implementation	✖
5.2	Incident Management	
5.2.1	Incident Generation	✔
5.2.2	Incident Diagnosis	✔
5.2.3	Incident Resolution	✖
5.2.4	Incident Reporting	✔
0	Capacity Management	
5.3.1	Capacity monitoring and reporting	✔
5.3.2	Capacity improvement recommendation	✔
5.3.3	Capacity Planning	✔
5.3.4	Capacity Change Implementation	✖
5.4	Asset Tracking and Reporting	
5.4.1	Configuration Item Recording	✔
5.4.2	Configuration Item Control and Updates	✖
5.4.3	Configuration Item Backup	✖
5.4.4	Configuration Item Restore + OOB	✖
5.4.5	Configuration Item Status Reporting	✔
5.4.6	Co-Management	✖
5.5	Service Request Fulfilment	
5.5.1	Service Request Management	✔
5.5.2	Move, Add, Change, Delete (MACD) Fulfillment	✖
5.5.3	Change Management	✖
5.6	Problem Management	
5.6.1	Problem Identification and Recording	✔
5.6.2	Problem Reporting	✔
5.6.3	Solution Identification and Recording	✔
5.6.4	Solution Implementation	✖

2 Service Prerequisites

2.1 General Requirements

2.1.1 In all cases

The standard delivery model shall be 24 hours a day, 7 days a week leveraging NTT Ltd. SOCs. Deviation from this standard shall only be considered on a case by case basis and must be supported by a completed application for non-standard services. NTT Ltd. shall consider the request, any cost implications and wherever possible shall strive to meet the requested requirements. However, NTT Ltd. reserves the right to refuse any request for deviation from the standard delivery model.

2.1.2 Configuration Item

An NTT Ltd. supported configuration item to be managed by the service.

2.1.3 Software/appliance license

Client is responsible for a valid manufacturer product license(s) which is required for all components (including security application and operating system) of the configuration item under management for the duration of the NTT Ltd. Service contract period. The Client must ensure that licenses are valid at the start of the NTT Ltd. service contract through to the end of the NTT Ltd. service contract.

2.1.4 Manufacturer Hardware/Software Support

Managed configuration items must have full manufacturer support at all times during the NTT Ltd. service contract period. NTT Ltd. will not provide any services for any configuration item not covered by a valid maintenance contract. Neither shall NTT Ltd. manage any configuration item where the software or hardware has been declared 'end of life' or 'end of support' by the manufacturer, prior to the start of any NTT Ltd. contract or subsequent 12-month renewal period. Replacement of obsolete hardware/software is not included in the service.

2.1.5 Software Updates (Subscriptions)

The Client is responsible for all Manufacturer's Software Subscriptions (i.e. software updates) for any configuration items to be managed. Such subscriptions are required for the duration of the NTT Ltd. service contract period. The Client must ensure that any software subscriptions are valid at the start of the NTT Ltd. service contract through to the end of the NTT Ltd. service contract. NTT Ltd. will not provide any services for expired subscriptions.

2.1.6 Limitations of use

Only the manufacturers' security application/operating system software, relevant and/or necessary software/applications and software provided by NTT Ltd. (where applicable) to support the NTT Ltd. service are to be run on the configuration item.

2.1.7 Secure System Management

NTT Ltd. highly recommend that any in-scope configuration item(s) have a secure configuration/policy implemented prior to the start of any NTT Ltd. service contract (including renewals). This must be maintained for the full-service period.

2.1.8 Secure facility

It is the Client's responsibility to provide and maintain a physically secured and environmentally suitable facility for any manufacturer hardware/software and associated NTT Ltd. supplied hardware/software including appropriate rack space and power.

2.1.9 Virtual environment

All virtual environments provided by the Client for the NTT Appliance must adhere to specifications outlined within the latest 'NTT Appliance Installation and Configuration Guide' which can be found on the NTT Portal. In addition, proactive monitoring of any shared resources (CPU, memory, network and storage) is the responsibility of the Client to ensure a stable virtual environment. Any hardware or software issues relating directly to the virtual environment are the Client's responsibility, however NTT Ltd. will work with the Client to resume normal operations in the event of appliance related failures.

2.1.10 Designated Security Contacts

The Client must provide at minimum two staff members to be the security contacts and if applicable a Service Desk contact that NTT Ltd. will liaise with to deliver the Device Management Service. Full contact and authentication details for each of the security contacts must be provided by the Client and included within the Client Security Service Detail (CSSD).

2.2 Communication Requirements

2.2.1 NTT Appliance

Managed Security Services require an NTT Appliance.

The NTT Appliance is available in multiple form factors which includes both virtual and physical hardware, all of which must be installed, initially configured and enrolled by the Client. NTT Ltd. will only be responsible for management and maintenance of the appliance software (in both physical and virtual form factors) and the physical appliance form factor if supplied by NTT Ltd.

NTT Appliances gather Logs, events, reports, and evidence data from in-scope Client devices and systems, then prepare the data for secure transmission and processing. The NTT Appliance also provides a secure communication path for Device Management service delivery. Ongoing configuration and maintenance of the NTT Appliance is conducted by NTT Ltd. and therefore the appliance must be installed by the Client in a suitable location on the Client network infrastructure to facilitate both NTT Ltd. access and log collection.

The NTT Appliance requires:

- At least one static (non-dynamic) IP address
- Permanent LAN Connectivity
- Permanent internet connectivity on TCP port 443

For the virtual form factor the appliance also requires:

- Configuration to power on automatically if the hypervisor is restarted
- Minimum resources from the hypervisor in the virtual environment as specified by NTT Ltd.

2.2.2 Configuration Item Requirements

All in-scope configuration items require:

- For internet facing configuration items a static (non-dynamic) public IP address
- For non-internet facing configuration items – a static (non-dynamic) RFC 1918 IP address
- Necessary network connectivity to NTT Appliance as specified by NTT Ltd.

2.2.3 Connection to Client Network

The Client must supply all the necessary network hardware and cabling to connect the configuration item to the Client's own, third party and ISP networks. All network interfaces connecting to the configuration items must be a minimum of 1 Gigabit Ethernet interfaces. The standard for Gigabit stipulates auto mode as mandatory. However, some manufacturers have deviated from this and do facilitate the hard coding of interface speed and duplex. Where this is enabled, it is imperative that both ends of the network cable are set to fixed speeds and duplex modes (in other words both Switch and Configuration Item). In this instance it is important that the Client discusses any potential infrastructure changes that may affect this setting during the Service Transition process or directly with the SOC during service operation.

3 Core Service Elements

3.1 Hours of Operation

Managed Security Services are delivered through the Security Operations Centers (SOCs) of NTT Ltd. Unless otherwise stated, MSS hours of operation are 24 hours a day, 7 days a week.

3.2 Security Operation Centers (SOCs)

NTT Ltd. will deliver services through its SOCs. NTT Ltd. may at its sole discretion deliver services through any of its SOCs, and Client data may be held in any SOC and/or NTT Ltd. Infrastructures unless there is prior agreement and approval between NTT Ltd. and the Client for data to be held in any reduced subset of the above. The Client will be provided with the contact details of relevant SOCs through the Service Transition process.

3.3 NTT Portal

The NTT Portal is a globally available web-based application, which allows Clients to interact with, manage, and monitor Managed Security Services.

3.4 Language support

Services are provided in English language only, unless there is prior agreement and approval between NTT Ltd. and the Client.

3.5 Management of Devices

Device Management Standard is a monitoring only service and therefore does not include management of configuration items.

3.6 Communications

3.6.1 MSS Infrastructure

NTT Ltd. utilize a regional-based infrastructure with security by design principles built in, it is highly resilient and secured using best practice methodologies tools and techniques. It is fully managed by Global Services staff and monitored using our DM, ESM and TD security services.

3.6.2 Notifications

3.6.2.1 Email

For security and data privacy reasons, email notifications will only contain minimal information to notify Clients about creation of, or updates to, Cases. Such emails shall not contain any sensitive information apart from the appropriate ticket reference number (and where possible not to disclose any private information a short description of the ticket).

Clients may send emails relating to new or existing Cases to NTT Ltd. In the case where no reference number is provided as formatted by NTT Ltd., NTT Ltd. shall create a Case with a short description based on the subject line provided.

When a Client is replying to an email with an existing reference number (as provided by NTT Ltd. and unchanged by the Client), the message body text shall be copied (upon receipt) to the journal of the relevant Case and shall be marked as updated by the customer and waiting on NTT Ltd.'s further input.
For security reasons, if Clients wish to send sensitive information to NTT Ltd. or provide approval workflow pertaining to an existing or new incident or request, they are urged to do so using the NTT Portal.

3.6.2.2 File attachments

Diagrams, images, PDFs, executables and any other attachments must not be attached to any Case via email. Where file attachments are necessary, the Client must log in to the NTT Portal and attach the file securely through their web browser connected to the NTT Portal.

3.6.2.3 Telephone

SOC staff may contact Clients and Clients may contact SOCs by telephone. In both cases an authentication shall be completed to verify Client identity.

3.6.2.4 NTT Portal

Unless otherwise stated and agreed, all other communications originating from NTT Ltd. SOCs shall be secure and follow security best practices and shall be via the NTT Portal.

3.6.3 ITSM (Service Management) Tool

NTT Ltd.'s ITSM module manages Cases aligned with ITIL wherever appropriate. Access is provided to appropriate NTT Ltd. staff only.

3.6.4 Monitoring

3.6.4.1 Protocols

Client configuration items are monitored utilising multiple protocols including SNMP v2, v3, SSH v2, HTTP, HTTPS and ICMP.

3.6.4.2 Health and Availability Monitoring Events

The event feeds from in-scope configuration items are sent to the NTT Appliance and securely sent via a VPN to the monitoring server in the MSS infrastructure.

3.7 Escalation Management

NTT Ltd. utilizes escalation processes and defined responsibilities for addressing escalated matters. To escalate a Case, the Client may telephone or email the service desk (quoting the reference number).

Only configuration item Incident and Service Request Cases are applicable to Device Management Standard.

Dependent on the escalation, NTT Ltd. may assign an Escalation Manager who is responsible for:

- Monitoring escalated matters through to resolution
- Creating and maintaining an action plan for each escalation
- Making any decision appropriate to the resolution of the escalation
- Arranging escalation meetings and/or phone conferences (as appropriate) between the Client, NTT Ltd. and relevant third parties
- Regularly communicating escalation status to:
  - The Client
  - The NTT Ltd. Client Services Manager (if assigned)
  - Any other parties relevant to the escalation
- Regularly updating and seeking the advice and support of NTT Ltd. management
- For the duration of an escalation, ensuring all appropriate personnel are available to support the agreed action plan

NTT Ltd. may downgrade an escalated Case if it is being managed to a scheduled timeframe, or resolution has been provided to the Client and is in the process of being tested. If the Client initiated the escalation, NTT Ltd. will obtain the Client's approval prior to downgrading an escalated Security Incident, Incident, Change Request or Service Request.

Clients may request their Case be escalated to a higher priority at any time if sufficient justification is provided. Upon review, the SOC manager shall be responsible for agreeing actions.

4 Service Transition

Service Transition is executed in five phases, these are:

1. Engagement
2. Planning
3. Staging
4. Integration
5. Go-Live

The five phases and activities and procedures within them, ensure a consistent approach to management and completion of the transition and a framework for governance and communication. During the first four phases of the Service Transition period there will be no alerts, incidents, or cases generated for customer review and triage.

4.1 Engagement Phase

To initiate the Service Transition, the Client will submit a Purchase Order (PO) along with the Pricing Information from the approved quotation, a High Level Design document, and the Client Security Services Detail to NTT Ltd.

- Purchase Order (PO) and
- Pricing Information
- Client Security Service Detail (CSSD)
- High Level Solution Design

NTT Ltd. reviews the provided documentation and confirms that all the requirements for commencement of the transition have been met.

A Kick-off meeting is held to communicate the Transition Process, the project tasks, roles and responsibilities and introduce the key stakeholders.

The Engagement Phase is expected to take 12 business days and can be accelerated if the Client provides completed and accurate documentation when submitting the Transition Service Request.

4.1.1 Engagement Phase Activities

The key activities during the Engagement Phase are as follows:

- Receive the Service Transition Request and PO and respond within three business days
- Review provided documentation within six business days
- Provide feedback and confirm content is complete and aligned to the Service Order
- Assign a Service Transition team including allocation of an NTT Ltd. Client Service Manager (CSM)
- Create the Draft Service Transition Project Plan, including timeline and constraints within 10 business days
- Arrange a Kick-off meeting within 12 business days (if documentation is complete and confirmed)

4.1.2 Engagement Phase Deliverables

The deliverables provided during the Engagement Phase are as follows:

- Purchase Order Approval
- Kick-off meeting (face to face or call)
- Draft Service Transition Project Plan, including timeline, standard risks and issues

4.2 Planning Phase

The Service Transition Planning Phase validates the provided documentation and locks down the transition plan, scope, and timeline. The Planning Phase is expected to take six business days.

4.2.1 Planning Phase Activities

The key activities during the Planning Phase are as follows:

- Agree on final architecture, including devices and logs collection
- Assess Log Source Scope and Prioritization, including completing Log Source Inventory where applicable
- Client Approval of Final Service Transition Plan
- Confirm Services Delivery Model, including Incident Management and Steady State Governance

4.2.2 Planning Phase Deliverables

The Final Service Transition Plan (including timeline, risks, and issues) is provided as a deliverable during the Planning Phase.

4.3 Staging Phase

The Service Transition Staging Phase establishes the primary service elements for NTT Ltd. to provide the service. It includes connectivity, appliances for log collection and device management access, and Portal and IT Service Management (ITSM) setup. The Staging Phase is expected to take 12 working days.

4.3.1 Staging Activities

The key activities during the Staging Phase are as follows:

- Install appliances (shipping, if required)
- Appliance initial configuration and hardening
- Setup and validation of remote access
- Log(s) events/ monitoring setup (Client device)
- OOB configuration (if applicable)
- MSS SOC Portal account(s) configuration
- MSS SOC infrastructure preparation

4.3.2 Staging Deliverables

The deliverables provided during the Staging Phase are as follows:

- Appliance required to support Client services
- Client credentials for MSS Portal
- Client Entitlement in NTT Ltd. ITSM
- Test results

4.4 Integration Phase

The Service Transition Integration Phase completes the required technical service elements for NTT Ltd. to provide the service. It includes configuration of all purchased services, advanced features for log collection (if applicable) and device management, and final Portal and ITSM integration. Additionally, during the Integration Phase, the NTT Ltd. CSM conducts the Welcome meeting and Portal training with the Client. The Integrwation Phase is expected to take 21 business days.

Following the Welcome meeting, the CSM becomes the interface into the NTT Ltd. services.

4.4.1 Integration Activities

The key activities during the Integration Phase are as follows:

- Final validation of connectivity to the SOC
- Device(s), log(s), and service testing and final verification
- Normalization and tuning (logs, not devices)
- Quality assurance review and activation of the service(s)
- Risk and Issue documentation
- MSS SOC Welcome meeting or call with Partners and Client (NTT Ltd. decision)
- MSS SOC Portal training meeting or call with Partners and Client (NTT Ltd. decision)
- Confirm Service Activation Date (in phases, if required), Billing Date, and SLA start date

4.4.2 Integration Deliverables

The deliverables provided during the Integration Phase are as follows:

- Client Welcome meeting and Portal training
- Service Activation Date
- Confirmation of Device Management Readiness
- Client review and acceptance of the Risk and Issue Register

4.5 Go-Live Phase

The Service Transition Go-Live confirms that the service is live and closes the Service Transition Project. The Go-Live Phase is expected to take six working days.

4.5.1 Go-Live Activities

The key activities during the Go-Live Phase are as follows:

- Operational Check List review by SOC
- Conduct Service Transition Plan closure review meeting or call with Partners and Client (NTT Ltd. decision)
- Review all remaining open action items including lessons and risks/issues to be considered for Steady State (going forward)
- Receive Client Service Transition Plan closeout final approval

4.5.2 Go-Live Deliverables

The deliverables provided during the Go-Live Phase are as follows:

- Risks/Issues Register (if any)
- Commencement of service and Billing
- Lessons learnt (if any)

4.6 Service Transition Deliverable Acceptance

The Service Transition is considered complete on the Service AcwService Transition by agreeing to the closure of the parent ticket in ServiceNow.

5 Device Management Features

Security Device Management Standard service utilizes the Global Managed Security Services Platform to provide 24/7 health and availability monitoring of devices and notifies Clients of any incidents which may cause disruption to their business. In this service offering, the Client maintains complete control of their security infrastructure but leverage our 24/7 Security Operations capabilities.

This section presents the features of the Device Management Standard service.

5.1 Health and Availability Monitoring

5.1.1 Health and Availability Monitoring

Device Management (Standard) Service monitors key performance indicators of in-scope configuration item's service state and resource utilization to determine overall health, performance and availability. The service automatically generates Incidents in the ITSM system based on events which exceed thresholds against specific poll cycles of key metrics. Events are investigated and analysed by a SOC engineer who determines a potential corrective or control action to resolve the related Incident as defined within Section 5.2. The Client will be notified and kept up to date of issues with overall health and availability via the Incident ticket available on the NTT Portal.

5.1.2 Health and Availability Improvement and Recommendation

NTT Ltd. utilize standard poll cycles and thresholds when monitoring in-scope configuration items. NTT Ltd. may adjust thresholds based on historical data collected to eliminate unnecessary events occurring. With this data, NTT Ltd. may identify potential methods of improving configuration item performance and overall health and availability.

For applicable service levels and where NTT Ltd. does not have access to make changes, if NTT Ltd. make recommendations to the Client which have not been implemented and configuration item(s) in scope create unacceptable levels of events and/or incidents (assessed by NTT Ltd.), NTT Ltd. reserve the right to disable health and availability monitoring until recommendations have been actioned.

5.1.3 Health and Availability Change Implementation

The Client is responsible for any corrective or control action to resolve an incident through their own Change Management process.

5.2 Incident Management

Incident Management focuses on responding to any unplanned interruption to service and configuration item operation to minimize any impact to business operations and ensure service quality and availability.

5.2.1 Incident Generation

Incidents may be generated through Health and Availability Monitoring by the SOC or Client raising an Incident Case via the NTT Portal or telephone call to the SOC.

An Incident Case raised via the NTT Portal, with a provided Impact and Urgency, the SOC team will validate the ticket and reserves the right to modify the Impact and Urgency as deemed necessary.

For an Incident Case raised via a telephone call to the SOC, the SOC shall create an Incident Case on behalf of the Client with the relevant Impact and Urgency.

5.2.2 Incident Diagnosis

Incident Cases are managed based on the priority of the Incident ticket raised on the NTT Portal. Priorities are calculated based on Impact and Urgency of an Incident Case, leading to a specific priority. Priorities are defined as Major, High, Moderate and Low as outlined in the table below.

Impact
1. Organization wide
2. Multiple Departments
3. Single Department
4. Individual

Urgency
1. Work blocked
2. Work degraded
3. Work not affected

Impact \ Urgency	1	2	3
1	Major=P1	Major=P1	High=P2
2	Major=P1	High=P2	Moderate=P3
3	High=P2	Moderate=P3	Low=P4
4	Moderate=P3	Low=P4	Low=P4

For Device Management Standard, incident diagnosis is limited due to NTT Ltd. providing health and availability monitoring only. NTT Ltd. will help to resolve an Incident Case through providing additional health and/or availability data available.

5.2.3 Incident Resolution

Within the Device Management Standard offering NTT Ltd. does not have the ability to resolve incidents due to having no administrative privileges to configuration item(s). Therefore, NTT Ltd. will work to advise the Client on potential actions to resolve the incident. The Client is responsible for the resolution of incidents and must update any Incident Cases within the NTT Portal to a 'resolved' state to allow Clients to confirm resolution. Incidents will then remain in a resolved state until:

- Client confirms resolution and the incident will be moved to a 'closed' state
- Client confirms incident is not resolved, the ticket will be moved back to a 'In Progress' state (to be actioned by the Client)
- Client does not respond, and the incident will be auto closed after 10 days

5.2.4 Incident Reporting

Clients are notified of all Incidents via a notification email which contains very minimal information for security purposes, with the full Incident details only available via the NTT Portal.

5.3 Capacity Management

5.3.1 Capacity monitoring and reporting

The monitoring systems utilized within the Device Management service regularly check a number of telemetry points. Through continuous monitoring, NTT Ltd. is able to highlight potentially impacting trends. This can be useful for determining if there is a problem that needs to be addressed or if configuration items are becoming oversubscribed, eg. a disk filling with log data. Using this as a starting point for Incident or Problem Management, NTT Ltd. will work with Clients to advise on potential resolution or mitigate the risk.

NTT Ltd. utilize standard thresholds when gathering monitoring data, acknowledging that these thresholds may not be applicable to some Client environments, NTT Ltd. can work with the Client to adjust thresholds during the Service Transition process or after service go-live where a baseline can be identified. If thresholds are changed, the Client must accept that this may result in unnecessary events or even false positives and NTT Ltd. reserves the right to adjust thresholds accordingly.

5.3.2 Capacity improvement recommendation

Where NTT Ltd. monitoring determines a device is oversubscribed, NTT Ltd. shall liaise with the Client to determine the best plan and path forwards. Examples include but are not limited to the following: Request the Client change logging levels or to network architecture; Request Client change monitoring levels within the configuration item (for example turning off debug logging); Request Client update hardware or licenses to facilitate greater capacity.

5.3.3 Capacity Planning

With the aforementioned trend data available, NTT Ltd., Partners and/or Clients may make decisions about future requirements and expected growth. This provides invaluable forward planning to those responsible for budgeting or capacity planning. For example, trend analysis reports will show disk consumption over time which could be an indicator of a need to procure new hardware or additional storage in the next budgeting cycle.

5.3.4 Capacity Change Implementation

Through the consistent and uniform measurement of telemetry from managed security configuration items, NTT Ltd. can make recommendations to be actioned by the Client to enhance or avoid future capacity issues that might arise.

5.4 Asset Tracking and Reporting

5.4.1 Configuration Item Recording

NTT Ltd. record and track in-scope Client configuration items with information available within the NTT Portal.

5.4.2 Configuration Item Control and Updates

NTT Ltd. do not provide any configuration item updates under the Device Management Standard offering. The Client is responsible for patching and updates of in-scope configuration items.

5.4.3 Configuration Item Backup

NTT Ltd. do not provide backup of configuration items under the Device Management Standard offering. The Client is responsible for configuration item backup.

5.4.4 Configuration Item Restore + OOB

NTT Ltd. do not provide configuration item restore within the Device Management Standard offering. The Client is responsible for restoration of configuration items.

5.4.5 Configuration Item Status Reporting

Configuration item status reporting is available via the NTT Portal. Status reports include version details and traffic light status.

5.4.6 Co-Management

The Client has full responsibility for configuration item management therefore Co-Management is not an option within the Device Management Standard offering.

5.5 Service Request Fulfilment

Service Request Fulfilment focuses on request for information, advice or access.

5.5.1 Service Request Management

Service requests are managed through ITIL process and raised via a Case in the NTT Portal. Attainment of various key performance metrics are tracked, monitored and reported within NTT Ltd. on a monthly basis.

5.5.1.1 Request for Information

Clients may request information through the NTT Portal about the performance, configuration or other aspects of in-scope configuration items. NTT Ltd. shall provide the information in the Service Request.

5.5.1.2 Service Request Reporting

All Incidents, Service Requests or Problems are recorded in the ITSM system and reported back through the NTT Portal.

5.5.2 Move, Add, Change, Delete (MACD) Fulfilment

As Change Management is not a component of the Device Management Standard offering, MACD is not applicable.

5.5.3 Change Management

Change Management is not a component of the Device Management Standard offering.

5.6 Problem Management

5.6.1 Problem Identification and Recording

NTT Ltd. follow ITIL best practices for Problem identification and recording. Problem identification is performed in a number of ways and will typically result in a Problem Case in the NTT Ltd. ITSM tool and NTT Portal. Typically, Problems are derived from a number of factors such as:

- Repeated Incidents of same or similar nature within single Client or across multiple Clients
- Compound problems caused by multiple Incidents of different nature within single Client
- Notification of problem from Manufacturer
- Lack of timely patch from Manufacturer to address security vulnerability
- Trend analysis

5.6.2 Problem Reporting

All Problems are recorded in the ITSM system and reported back through the NTT Portal.

5.6.3 Solution Identification and recording

Once a problem is identified and recorded, a suggested plan or where appropriate a number of suggested options for resolution will be recorded in the problem ticket.

5.6.4 Solution Implementation

The Client and NTT Ltd. shall discuss and agree on the best or most appropriate solution with the Client being responsible to implement as a controlled change or series of changes in line with their standard change process.

6 Terminology and Definitions

Terminologies and Definitions for Security Device Management services are presented in the 'NTT Ltd. - Terminology and Shared Services Reference' document that accompanies this Service Description.

The unique definitions used within this Service Description are:

Case	A Case is a record used to identify and resolve various types of issues or requests – they are related to record types such as change requests, incidents and service requests.
Out of Band (OOB)	Access to a configuration item through a stream that is independent from the main in-band data stream
Problem	A cause of one or more Incidents

7 Operational Level Agreements

Operating Level Agreements for Security Device Management services are presented in the 'Operating Level Agreements – Managed Security Services' document that accompanies this Service Description.

8 Changes in Service

8.1 Regulatory Change Requirements

If regulatory changes (e.g., changes by a regulatory agency, legislative body, or court of competent jurisdiction) require NTT Ltd. to modify the Services described herein, NTT Ltd. will modify the Services and this Service Description accordingly without diminishing the features, functionality or performance. In the event a modification in response to regulatory changes results in a diminishment of features, functionality or performance, Client agrees in good faith to work with NTT Ltd. to amend this Service Description accordingly and execute any additional agreement which may be reasonable requested by NTT Ltd. to document such amendment.

8.2 Method of Service Delivery

NTT Ltd. reserves the right to make changes to the service, provided these changes do not have a material adverse impact on functionality or performance.

8.3 Supported Devices

NTT Ltd. reserves the right to change Supported Device's over time as new manufacturer hardware models and software versions are released or announced by the manufacturer as End of Support and/or End of Life.

9 Service Exclusions

Unless otherwise expressly agreed by NTT Ltd. in writing, the services described in this document do not include the following:

- Configuration of in-scope security systems and devices to allow for Log, Events, and evidence collection.
- Support and Remedial Work which is not expressly stated in this Service Description. This includes any troubleshooting and problem solving related to issues arising from Client actions or Client's network.
- Project Orientated Requests (PORs) are not included in the Services described herein and are subject to additional fees. NTT Ltd. and the Client will develop a scope for the POR and NTT Ltd. will provide a separate quote to Client, which must be executed prior to performance 1of any such work.
- Client requests for advice or consultation regarding network or configuration item configuration not specifically outlined in this Service Description is not included are subject to additional fees.
- Client staff training unrelated to NTT Ltd. services (NTT Ltd. provides written and video training on the NTT Portal and the different functions that Client may use within the portal.).
- Software or hardware maintenance (unless otherwise stated).
- Software licensing (unless otherwise stated).
- Software or hardware upgrades.

- Network connectivity troubleshooting.
- On-site forensic services.
- Security policy or procedure establishment.
- Firewall rule set design, validation and troubleshooting.
- Remediation of a Security Incident or attack on a Client's network, server or application.

10 Controlling Terms

In the event of any conflict between the terms of this Service Description and the terms of the Client agreements, then terms of this Service Description shall control.

Together we do great things