Client service description

Proactive Support Services

25 November 2019 | Document Version 9.11

Rich Schofield
+1 508 424 3325 | +1 508 958 2958
rich.schofield@global.ntt

NTT contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Rich Schofield - VP, Service Offer Management Technical and Support Services, Mobile Phone: +1 508 958 2958

NTT Limited
4F Verde Building, 10 Bressenden Place,

Victoria, London, SW1E 5DH
☏ +1 508 424 3325
✉ rich.schofield@global.ntt

Please quote reference {Document Reference Number} in any correspondence or order.

Confidentiality

This document contains confidential and proprietary information of NTT Limited ('NTT'). {ClientFull} ('{Client}') may not disclose the confidential information contained herein to any third party without the written consent of NTT, save that {Client} may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of {Client}'s evaluation of the document. {Client} agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as {Client}. As a condition of receiving this document, {Client} agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

This document is valid until 06 June 2020 and, in the absence of any other written agreement between the parties, NTT and {Client} acknowledge and agree is subject to NTT's standard terms and conditions which are available on request. NTT reserves the right to vary the terms of this document in response to changes to the specifications or information made available by {Client}. Submission of this document by NTT in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

NTT does not assume liability for any errors or omissions in the content of this document or any referenced or associated third-party document, including, but not limited to, typographical errors, inaccuracies, or outdated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with NTT will be governed by {Law} Law and be subject to the exclusive jurisdiction of the {Law} courts.

Table of Contents

List of Figures

List of Tables

1. Service description

1.1. Overview

Uptime and Proactive Support Services are a portfolio of worldwide support services for information technology (IT), networking, security, collaboration, and telephony infrastructure that improves uptime and enables your organization to better balance the cost of supporting your infrastructure with minimum downtime.

Our Uptime Service Plans are designed to allow you to choose the best-fit service level on a per asset basis from each of the four service plans ranging from remote to mission critical and a set of additional proactive support service options to help you manage your IT estate and operational processes more efficiently.

The scope of this service description is the add-on Proactive Support Services. For a detailed description of the Uptime Service Plans, please reference the companion Uptime Service Plans client service description.

1.2. Key benefits

We are a trusted IT support and maintenance partner for over 8,000 clients located across five continents. Many other support service providers depend on us as a subcontractor.

We've got 2,000 experts in our service centers and another 15,000 certified engineers on the ground in 178 countries.

We keep spares nearby, have engineers on call, and we speak 19 different languages. We give you one point of contact where you can get IT problems fixed any hour of the day, every day of the year.

We can service and maintain your assets even if we have not provided them to you. We can consolidate all your existing service contracts under a single contract managed by NTT.

We can offer you unified service level commitments across your whole IT infrastructure – globally. No other support or maintenance offering can provide this like Uptime can.

With our Uptime Service Plans, NTT is able to deliver:

- higher availability through real-time lightweight monitoring, allowing for early detection of incidents in combination with service level commitments
- on-demand access to up-to-date asset inventory to help you stay in control of your IT asset inventory
- access to technology and service experts to support you in making the most effective use of your IT assets and help you plan for the future
- enhanced (automated) service management tools making it easier for your in-house support teams to engage with NTT and ensure continuous visibility of support status
- multivendor and multi technology service aggregation to help your organization navigate through the complexities of dealing with multiple support providers by reducing the number of support contracts

1.3. Uptime Service Plans

We offer Uptime Service Plans with progressive levels of coverage from remote to mission critical. Proactive support service options can be added as needed to complement any of the four plans. Please refer to appendices G-K for region specific deliverables.

With our plans, you can select the desired support coverage by asset rather than having one plan for your entire estate. This gives you the flexibility to tailor support by asset and location to minimize cost while achieving the IT availability levels required to meet your unique business needs. These plans include:

- Remote – designed primarily for the support of software products for which incidents are handled remotely. It is a cost-effective plan offering 24x7 remote support with incident response within 30 minutes.
- Parts only – A cost-effective hardware plan that delivers 24x7 remote support and parts only on-site delivery. When needed, we deliver parts based on your choice of coverage: 24x7 response with parts delivery in four hours or business hours with parts delivered in 4 hours; or business hours with parts delivered the next business day.

  This plan is ideal for organizations who have the skilled staff to perform an on-site repair when needed, but don't have the scale to stock their own spares or the logistics capabilities to get parts to the right location a t the right time.
- On-site – For hardware and software infrastructure, this plan provides incident response within 15 minutes. Options for on-site include: 24x7 with the engineer and parts on-site within 4 hours; business hours with support within 4 hours; or business hours with support the next business day.

This is suited to organizations who do not have local teams, parts, and/or engineering expertise to perform on-site repairs.

- Mission critical – for mission critical hardware and software, this plan includes fast track access (warm transfer) to our engineers, Availability and Capacity Monitoring and reporting, configuration archiving, and on-site engineer and part support within two hours for incidents that can't be resolved remotely. This service plan provides an elevated level of support to save critical time on mission critical IT assets when incidents occur.

1.4. Service features

Each plan includes a set of service features as shown in the Figure 1 below.

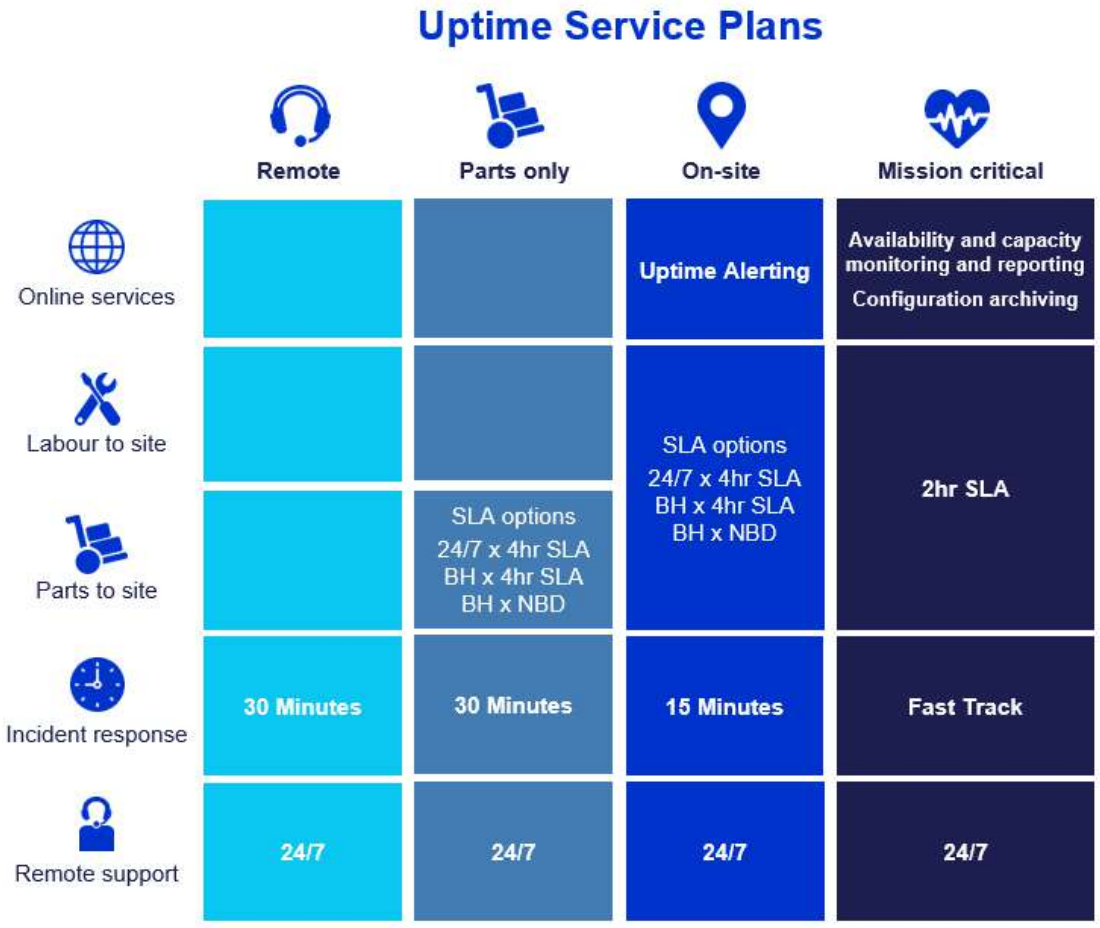

Figure 1 Uptime Service Plans

Mission Critical and on-site Plans can be applied to hardware and software

On-site parts and labour SLAs apply only when required to restore service

Where 2-hour response times are not available in remote geographies, response time will be 4 hours

BH=Business Hours NBD = Next Business Day SLA = Service Level Agreement

Each service feature is as follows:

1.4.1 Remote support

When your IT team places a call to our service center, we provide your team with remote support on a 24x7 basis, regardless of the on-site parts and/or labour service level commitment you have purchased with us. We aim to resolve the vast majority of all incidents remotely. Resolving incidents remotely allows NTT to restore service more quickly, avoiding the need for unnecessary dispatch.

1.4.2 Incident response

We ensure that we respond to incidents, either reported to us by your team or detected by our monitoring systems, within predefined timeframes and, wherever possible, remotely resolve them. If the incident can't be resolved remotely, we dispatch replacement parts, and/or an engineer to your site for resolution within the committed timeframe. NTT engineers carry 30,000 certificates (many carry more than one) across 36 technologies to get your business operational again quickly.

1.4.3 Parts to site

We hold spares for your equipment near where you are in 178 countries, either ourselves or through Preferred Partners. Our ability to get parts anywhere around the world quickly is one of our core strengths. In addition, we start the SLA clock when you place the call with us to get you up and running again fast. Most providers only start the SLA clock after the diagnostic process is complete making it difficult to predict when on-site resources arrive.

1.4.4 Labour to site

If we cannot fix an incident remotely, we'll send an engineer, who would get you up and running again quickly. We begin our service level timer at the time you place the call with us and not when we have completed diagnosis allowing you to rest assured knowing when we arrive on-site when required.

1.4.5 Online services

Our online services enable faster response and repair. These services provide warnings of a failure or imminent failure of hardware components enabling us to proactively initiate fault resolution. On average, this accelerates incident response by 69% and repair time by 32%. It saves you time by eliminating the tasks normally required to identify the failure and submit a ticket.

Depending upon the service plan you purchase, one or more of the online service options in the following sections will apply:

1.4.6 Uptime alerting

Uptime alerting is a lightweight 'phone home' style monitoring feature included in the on-site service plan. Through Uptime alerting, NTT receives hardware failure alerts from Cisco assets in your IT environment.

1.4.7 Availability monitoring and reporting

In our mission critical service plan, we include availability monitoring which improves on hardware alerting by providing active polling of your covered assets to determine their status and predict incidents. We diagnose the event information to resolve incidents faster. If availability is affected, we notify your team within 15 minutes of incident detection. We also make available, on our Manage Centre portal, a set of availability reports to aid your availability planning initiatives.

1.4.8 Capacity monitoring and reporting

We will remotely monitor for abnormal events that could affect your capacity or performance targets or even future uptime. Based on agreed thresholds, we notify you in advance of any service impacts. We also make available, on our Manage Centre portal, a set of capacity reports to aid your capacity planning initiatives.

1.4.9 Configuration archive

On an ongoing basis, in our mission critical plan, we will archive the configurations of your covered assets saving both the current configuration and current minus one. Most supported devices have the capability to alert NTT monitoring systems that the configuration has been changed, initiating a fresh configuration download. In addition, configurations are archived on a monthly basis and compared to the last stored configuration to ensure the latest version is saved.

1.5. Proactive Support Services

Our Uptime Service Plans are complemented by a set of advanced Proactive Support Services that provide performance management, service management support and service aggregation. You can add any of these Proactive Support Services to any of our Uptime Service Plans based on your needs.

These include:

Performance management support

1. Asset Tracking and Analytics
2. Availability and Capacity Monitoring
3. Configuration Archive
4. Moves, Adds, Changes, and Deletes (MACDs)

Service management support

1. Service Delivery Assurance
2. Technical Account Management
3. Proactive Problem Support
4. Annual Version Updates

Service aggregation

1. IT Service Integration
2. Third-Party Support

The details of these options are provided in Proactive Support Services Client Service Description (PSS CSD).

1.5.1 Asset Tracking and Analytics

Keeping track of ICT assets can be difficult in today's fast pace world of business. For Cisco assets, we have the capability to track your installed technology assets to better enable your asset management practices[1].

Asset Tracking and Analytics discovers your Cisco asset data and transforms it into actionable information to help you make informed infrastructure decisions. Asset tracking provides predefined reports and offers information on: device configuration, service records, vulnerability alerting and lifecycle status.

With this service you get a view of all your assets. You can make sure that you have support coverage on all needed assets and review coverage on each, so you aren't overpaying for coverage you don't need or risking downtime on mission critical infrastructure. You can avoid productivity loss by making certain the right patches have been implemented and service incidents are prevented.

1.5.2 Availability and Capacity Monitoring

Poorly performing or unavailable ICT assets can have a huge impact on the continuity of business. We have the ability to remotely monitor your infrastructure and application environments for conditions that detect and help prevent issues and outages that impact business continuity.[2]

Our capability spans a broad technology stack and includes growing list of automations and reports being made available via our Manage Centre client service portal.

---

[1] Asset Tracking and Analytics requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

[2] Availability and Capacity Monitoring requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

This service provides our clients with insights to help them make better decisions, tightly manage capacity, and plan upgrades more carefully.

1.5.3 Third-Party Support

We offer two Third-Party Support Services that can be purchased separately or combined based on your needs and requirements.

- Third-Party Incident Coordination off loads the coordination of third-party maintenance providers during incidents. We determine the correct resolver and ensure that the appropriate third-party provider resolves the incident to your satisfaction.
- Technical Incident Management - With Technical Incident Management, we resolve the incident remotely and utilise your maintenance contract with the third party for on-site support and/or parts replacement only when it is required.

1.5.4 Configuration Archive

One of the most effective mechanisms to ensure the shortest possible repair times when failures occur is a backup of the last known good configuration file. Significant time may be wasted attempting to regenerate the previous configuration during a crisis. Often there are small configuration tweaks that have been implemented that won't be discovered for weeks or months. We provide automatic configuration backups to eliminate the risks associated with configuration errors. We save configurations in order to speed time to resolution by rapidly retrieving stored configurations to configure the replacement part[3].

1.5.5 Proactive Problem Support

Although the identification and remediation of recurring problems is provided in the base Uptime service, to provide proactive future downtime avoidance we offer Proactive Problem Support. This service provides identification and root-cause analysis our clients need to stay ahead of these chronic incidents[4]. We provide

them with Proactive Problem Support by regularly reviewing service incidents and identifying the source of potential future downtime.

[3] Configuration Archive requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

[4] Proactive Problem Support requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

Proactive Problem Support must be sold in conjunction with Availability and Capacity Monitoring or the client must have previously contracted with us for Availability and Capacity Monitoring.

1.5.6 Technical Account Management

NTT provides an assigned senior engineer who understands the client's operational environment and technology being supported. The Technical Account Manager (TAM) tracks the client's technology support needs, monitors their service requests, troubleshoots issues and identifies opportunities to improve infrastructure availability.

Technical Account Management must be sold in conjunction with the following services or the client should already have each of these other services under contract with us – Availability and Capacity Monitoring, and Proactive Problem Support.

1.5.7 IT Service Integration

Clients and service providers need to leverage automation and integration of their value chains to deliver the expected end user satisfaction. IT Service Integration automates workflows between the client's service desk application and our IT Service Management system. The service also provides the ability to create a complete integrated ecosystem between our client's vendors and service providers. Our IT Service Integration offering provides automatic transmission of new incidents, problems, changes and service requests from our client's service desk application to our IT Service Management System. The service also allows our clients to view real-time updates on task status directly from within your service desk application.

1.5.8 Service Delivery Assurance

NTT will assign a Service Delivery Manager (SDM) to provide continuity in service levels and act as an advocate for your organization within NTT. They are the primary interface managing the services relationship between you and NTT. The Service Delivery Manager will own establishing the service governance structure, scheduling, running all service management review meetings, and ensure all processes and documentation are in place[5].

1.5.9 Moves, Adds, Changes, and Deletes (MACDs)

We provide our expertise and remote system administration services to assist you in the coordination and management of changes within your ICT estate, to minimize business disruption and impact due to change. When combined with IT Service Integration it provides processes to help accelerate your change process and reduce human error.

[5] Service Delivery Assurance requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

1.5.10 Annual Version Updates

Software upgrades, patching, security fixes, and configuration changes can be a significant operational overhead just to maintain and stay on top of. Not doing so can lead to business risk, exposure, and non-compliance. We provide our clients with an annual project to plan, schedule and control updating of their IT operating systems and asset configurations proactively. We follow their change management policies for every covered asset, ensuring each one is up-to-date and amended once a year[6].

1.6. Supported products

NTT provides Uptime and Proactive Support Services across a broad range of vendors and product families enabling you to simplify your support processes by engaging a single support partner, saving you time and money.

Supported products fall into two broad categories:

- Tier one – tier one vendors are those where we are able to provide worldwide coverage
- Tier two – tier two vendors may be limited to specific geographic regions. Geographical coverage maps of supported tier two technologies are available upon request.

For information on currently supported products please check with your NTT Account Manager.
Please note that service level commitments drop to service level targets on products which are past the manufacturer's documented end-of-support date.

1.7. NTT's delivery model

We offer a globally integrated service delivery model with services delivered when and how you need them.

We use a two-tier delivery model allowing us to apply specialized resources centrally, providing the quickest response and deploy local resources to give you the best possible service experience.

The two-tier delivery model is comprised of the following components:

[6] Annual Version Updates requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

- Global Delivery Centers (GDCs): are centrally run support services centers that consolidate and standardize services across all clients. GDCs deliver 24/7 proactive and support services quickly with the deepest level of expertise. The GDCs are also responsible for service activation.
- Local (Country): is the primary interface managing the Support Services relationship between you and NTT and is responsible for the on-site aspects of the service including Client Service Delivery Management, On-site Engineering and Field Engineering.

Standardizing our services and centralizing our delivery at two Global Delivery Centers, optimizes our assets and resources, delivers worldwide consistency in our delivery, and provides a rich global engineering talent pool capable of supporting over 28 technologies in multiple languages.

- Global Delivery Center Bangalore (Bengaluru) supports 5 regions – Asia Pacific, Australia, Americas, Middle East and Africa, and Europe in English
- Global Delivery Center Prague supports 16 countries in Europe and seven European languages including: Czech, Dutch, English, French, German, Italian and Spanish

Figure 2 Delivery model

2. Proactive Support Services

2.1. Asset Tracking and Analytics

Tracking assets properly is difficult, and it requires people, systems, and processes to ensure accurate asset base and asset health (e.g. lifecycle status, security vulnerabilities, up-to-date software versions). Naturally, it is important for you to be aware of the health of your IT estate which includes various models in diverse locations and configurations. In today's dynamic IT environments assets are constantly changing, being taken out of commission or new product deployed. Asset sprawl is a significant problem that all organizations face from the smallest 'mom and pop shop' to the largest multi-billion dollar worldwide corporation.

2.1.1 Asset Tracking and Analytics key client benefits

With the Asset Tracking and Analytics service, you can expect to:

- reduce risk and costs of downtime caused by unknown and/or unsupported assets
- reduce risk and costs associated with unknown and unpatched security vulnerabilities
- reduce costs leading to improved return on assets
- support contract rationalization and reduce renewal efforts
- leverage the data collected and better plan technology refresh and standardization
- receive customizable and interactive reporting dashboards making information retrieval easier

2.1.2 Asset Tracking and Analytics deliverables[7]

NTT's Asset Tracking and Analytics service has the following service deliverables:

- regularly scheduled and automated asset discovery
- interactive asset data reporting and analytics on our award winning Manage Centre Portal

[7] Asset Tracking and Analytics requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

2.1.2.1 Automated asset discovery

NTT will provide automated discovery of the hardware and embedded software products in your network via NTT's Global Service Operating Architecture (GSOA) at a frequency mutually agreed between your team and NTT.

Asset discovery is not a once-off process that provides a snapshot in time of your IT assets. It needs to be an ongoing and regular discovery that keeps track of the changes in your dynamic environment. Discoveries are run once a month. Through the asset discovery the following asset information will be captured and additional attributes of the discovered assets will be subsequently enriched:

- asset model
- serial number
- manufacturer
- IP address and host name
- location details (if available)

Connectivity and security requirements and set-up

To enable the automated discovery of the assets in your network, connectivity must be established via secure Virtual Private Network (VPN) from NTT's GSOA environment to your network. SNMP, SSH/Telnet and/or HTTP/HTTPS access is necessary to collect sufficient data from your assets. SNMP (v1, v2c or v3) is the minimum requirement and must be enabled on all the assets that need to be discovered.

Collections are performed relatively infrequently, and during low network traffic times in order to minimize the impact to peak-time network usage. Collection intervals are configurable and will be scheduled by NTT. Collection duration and collected data size will depend on the size and complexity of your network being polled.

Impact on bandwidth utilization in your environment will vary due to a number of factors including:

- total device count
- device type and mix
- collection rules applied
- number of devices simultaneously polled

Results from performance testing for a typical collection conducted in a controlled Cisco laboratory environment of 5,000 devices where the polling was the only traffic and the default collection rules used produced the following results:

Metric	Result
Discovery time (hours)	5.5
Packets transmitted	4,540,241
Bytes transmitted	2,152,900,782
Average packet size (bytes)	474.18
Average packets per second	66.73
Average bytes per second	31,643.50
Average MB per second	.25

Table 1 Example performance testing results

2.1.2.2 Vendor update notification

NTT will process and evaluate vendor notifications and advise you of only those relevant to your infrastructure for the following types of vendor notifications on a monthly basis:

- end-of-support / end-of-life
- software updates
- field notices
- known bugs
- security

If a configuration item requires an update to address issues of concern by your organization, required changes can be addressed as a MACD, or during an Annual Version Updates, or a separately quoted project.

2.1.2.3 Configuration item reporting and analytics

Following the asset discovery, and currently available for Cisco products only, the asset data is enriched through NTT's and Cisco’s enrichment applications. The enrichment applications provide additional asset data such as vendor lifecycle (EoX) data, field notifications, security alerts and NTT service coverage. The enriched asset data is presented in flexible reporting formats on NTT's Manage Centre Portal at the same frequency as agreed for discoveries. This includes comparison reporting to allow you to identify changes that have occurred between discoveries.

The following Asset Tracking and Analytics service reports and analysis options are available in the Manage Centre Portal:

- summary dashboard
- vulnerable items report (assets with a known or potential security vulnerability)
- outdated items report (assets that have a known EoX status and assets that are not covered by a valid support contract)
- items becoming outdated soon
- comparison report
- advanced analysis that provides your team with the ability to run some custom reporting to suit your requirements

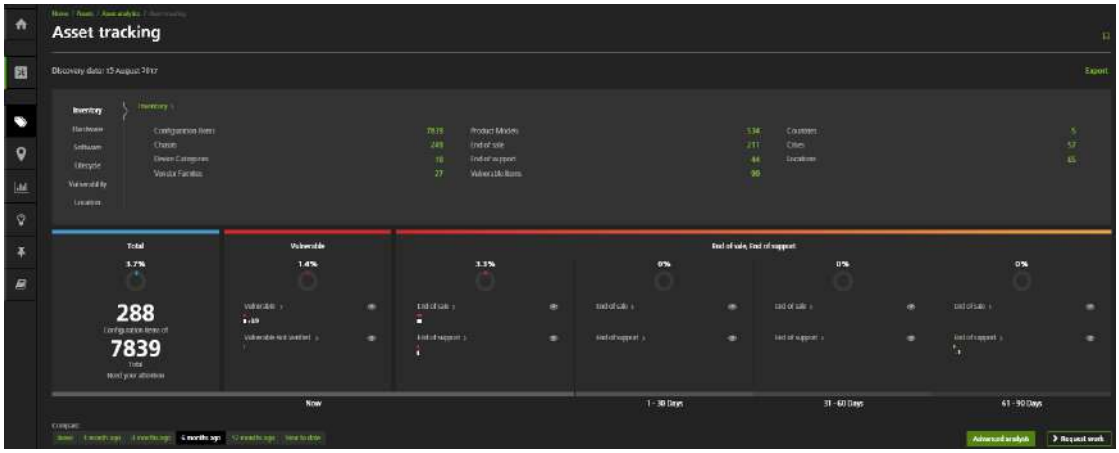

Figure 3 Asset Tracking and Analytics service homepage

You can select any of the above-mentioned sections to open up the advanced analytics page and drill down into more detailed information.

Summary dashboard

The summary dashboard provides you with a view of the high-level details on your IT estate scope and health. It contains the following information:

- number of assets
- number of product models
- number of vendor families
- number of asset categories
- number of active contracts with NTT
- number of service levels
- number of expired contracts
- number of assets which are end-of-sale (including bundled IOS software)
- number of assets which are end-of-support (including bundled IOS software)
- number of vulnerable assets (including vulnerable and vulnerable not verified)
- number of countries, cities, and locations where the assets are placed

Vulnerable Asset report

The Vulnerable Asset report provides an overview of assets that have a known or potential security vulnerability alert associated to it by Cisco and require immediate attention and are split into two categories:

- vulnerable, where based on your specific configuration the security vulnerability is relevant
- vulnerable not verified, where not enough detail on your specific configuration is known but where CI model-specific security vulnerability is known

You can view and export the following detailed summary information about assets with selected vulnerability status:

- number of IP addresses
- number of assets
- number of product models
- number of vendor families
- number of locations

Outdated Assets report

The Outdated Assets report provides an overview of outdated assets or out-of-contract items. The Asset Tracking and Analytics homepage in Manage Centre contains the following summary information about outdated configuration items:

- percentage of outdated assets out of the total asset count. An asset is treated as outdated in one of the following cases:
  - expired contract
  - no contract
  - end-of-sale
  - end-of-support
- breakdown percentage of the out-of-contract (expired or no contract), end-of-sale, end-of-support assets out of the total outdated assets

You can view and export the following detailed summary information about assets with selected outdate reason:

- number of IP addresses
- number of assets
- number of product models
- number of vendor families
- number of locations
- number of contract types
- number of items with expired contract
- number of items with no contract

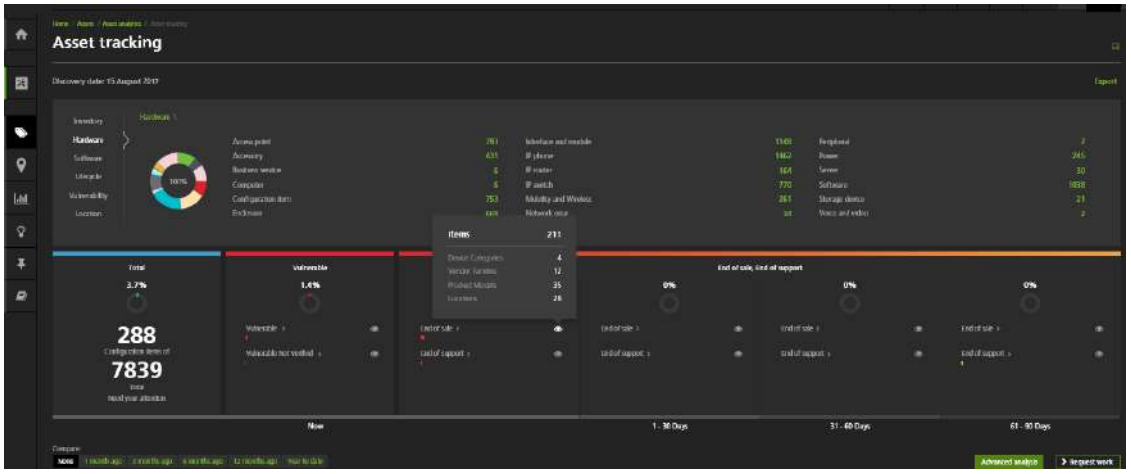

Figure 4 Outdated Assets report

Assets Becoming Outdated Soon report

The Assets Becoming Outdated Soon report provides an overview of assets which will require your attention in the near future. The Asset Tracking and Analytics homepage contains the following summary information about assets which will soon become outdated (end-of-sale, end-of-support, expired contract):

- summary of assets which will be outdated in the next 30 days
- summary of assets which will be outdated in 31 - 60 days
- summary of assets which will be outdated in 61 - 90 days

Comparison report

The comparison report compares the asset summary view with a point in time in the past to allow you to view changes between two points in time and to provide trend information.

The following metrics are included in the comparison:

- vulnerable asset charts
- outdated asset charts
- soon to become outdated assets charts

The percentage delta between past and present is shown for each metric and it is possible to select the comparison point in the past from the following options (dependent on the number and frequency of the discoveries that have taken place):

- one month ago
- three months ago
- six months ago
- one year ago
- year to date (YTD)

You will only see available data for a particular option (e.g. if the data discovery has started one month ago, then you will see the ‘three months’ option and further options are not available).

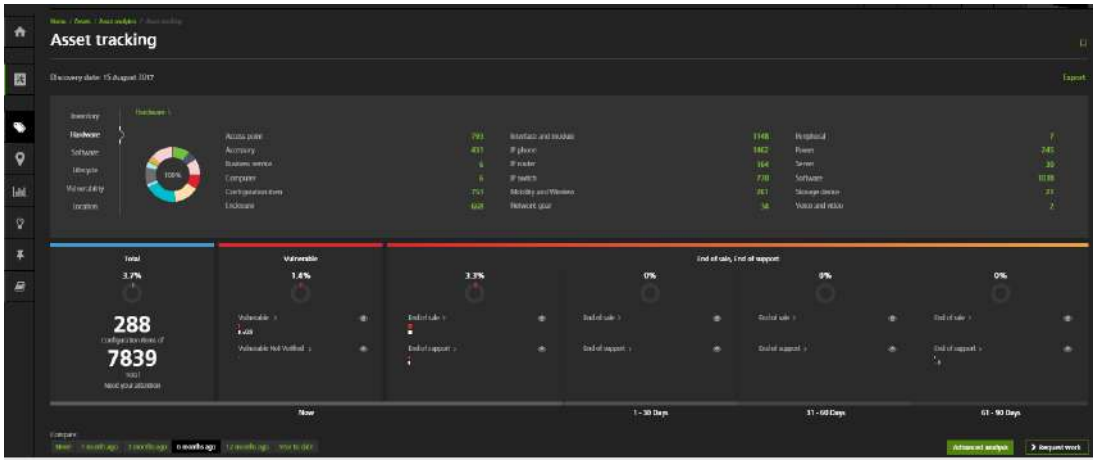

Figure 5 Comparison report

Advanced analysis

The advanced analysis functionality within Manage Centre provides you with the capability to run an advanced asset query and select a metric by which to view and export the data. You can apply multiple selection criteria and also view and export the data by:

- product (hardware)
- asset category
- vendor family
- product model
- product (software)
- operating system (OS)
- OS version
- contract
  - contract status (active/expired/no contract/third party)
  - contract expiry date period (not available if the contract status is ’no contract ‘or ’third party’)
- service level agreement (SLA)
  - SLA type
- SLA namelifecycle
  - lifecycle status (current, aged, obsolete)
  - lifecycle expiry date period
- location
  - region

- country
- state
- city
- address

- vulnerability status

It is also possible to select assets by IP address range.

The advanced analysis section of the Manage Centre Asset Tracking and Analytics portal allows you to apply multiple filters and selection criteria depending on your specific needs and provides an export function into csv format.

2.1.3 Asset Tracking and Analytics service level commitments

Description	Service level
Discovery will be scheduled as per the requirements in the transition questionnaire.	The schedule will be setup during business hours. However, once set-up, subsequent discoveries may happen 24/7.
Asset record data will be discovered and updated, and reports will be available on Manage Centre.	Reports will be available by the 5th working day after the scheduled discovery but may vary dependant on successful discovery and size of your IT estate.

Table 2 Asset Tracking and Analytics service level commitments

2.1.4 Asset Tracking and Analytics summary of responsibilities

Activity	NTT	Client
Completing the Asset Tracking and Analytics Service pre-sales questionnaire and workbook	A	R
Enable SNMP, SSH/Telnet and/or HTTP/HTTPS to collect data	C	R
Add security rules to firewall(s) allowing collector access to client assets	C	R
Disable the alerts or notifications on intrusion detection when the discovery is scheduled to run	C	R
Contract set-up in NTT systems	RA	C
Establish VPN connectivity between your infrastructure and NTT toolset	RA	R
Deploy and configure the collector in NTT's Global Service Operating Architecture (GSOA)	RA	I

Activity	NTT	Client
Set-up and provide Manage Centre login credentials	RA	C
Conduct a training session on Manage Centre portal usage	RA	C

Table 3 Asset Tracking and Analytics summary of responsibilities

2.2. Availability and Capacity Monitoring

Availability and Capacity Monitoring helps to ensure that the configuration items supported are available and operating at acceptable levels. Availability and Capacity Monitoring will help enable your organization to sustain the service availability required to support your organization's needs and predict your future needs.

NTT will proactively monitor the availability and performance of your covered infrastructure on a real-time basis by configuring a set of asset-applicable thresholds. This will include such key performance indicators as central processing unit (CPU) utilization, memory, key processes, physical and virtual network interfaces, and the performance of carrier services, to name just a few. Such key performance indicators will be measured when supported by the vendor.

NTT will implement an initial set of thresholds and conduct an analysis of the first three months of performance data. The results will be compared against best practice standards to assist in determining what, if any, future actions should be taken to ensure an appropriate performance level is maintained and what, if any, adjustments in threshold settings should be implemented. All data related to availability and capacity is available to you and can be downloaded via the Manage Centre portal.

2.2.1 Availability and Capacity Monitoring key client benefits

Availability and Capacity Monitoring helps to ensure that your IT infrastructure availability and performance matches the evolving needs of your organization. It directly influences your users' satisfaction and the reputation of your organization by helping to provide your users with a consistent experience that will increase productivity and a reduction in user complaints.

The key client benefits of Availability and Capacity Monitoring are:

- proactively identifies areas of attention so that remediation actions can be taken prior to an impact on performance
- increased IT service availability to your users and your customers through accelerated resolution times
- reduced cost of support by leveraging NTT's rich set of monitoring, management, and reporting tools, saving you the related operational expenses as well as software development and integration costs

- improved resource utilization through proactive event management that filters out false positives to highlight key events that may result in incidents and service downtime
- improved future downtime avoidance by ensuring intermittent events that can result in incidents are not ignored
- improve identification of assets requiring upgrade (i.e. more memory, faster storage devices, faster processors, greater bandwidth)
- better balance the risk of sweating assets with the cost of upgrades or renovation

2.2.2 Availability and Capacity Monitoring deliverables

2.2.2.1 Availability and capacity event monitoring and management

NTT will monitor the availability of configuration items to include identified capacity thresholds. We have a carefully developed monitoring plan for each asset type that allows us to ensure that we are notified by events that matter and we don't distract you with ones that don't. Availability and capacity related events (whether informational or exceptions such as a component failure) are recorded and managed, and, if required, logged and addressed as an incident. We will:

- receive events from the supported assets
- validate the accuracy of the information in the event
- analyse and filter the events
- correlate events
- classify events
- perform initial remedial actions where required
- log incidents into our IT Service Management system
- route logged incidents to the appropriate resolver group where required (these may also be third parties)
- notify on events to your organization

It is critical however, for any event that affects IT service availability and for which we create a service incident (provided Uptime contract is in place), that you be notified within 15 minutes of the actual detection of the event by our monitoring systems – referred as proactive notification. This notification can be via email or SMS as determined by you at service transition.

2.2.2.2 Availability reporting

On a monthly basis, the following availability reports can be generated via the Manage Centre portal:

- **Infrastructure availability summary** is a monthly tabular report that displays the availability of each asset along with the downtime experienced by the asset for a selected time frame. It is sub-divided by asset type when applicable and includes the following information:
  - **device**: configured name given to the asset
  - **model**: manufacturer name and product family of the asset
  - **availability %**: percentage of time the asset was available during the selected reporting period (last calendar month)

- **downtime duration**: total downtime of the asset during the selected reporting period (last calendar month)
- **up since**: date and time since the asset last went from unavailable to available

- **Top availability problems** is a monthly tabular report that can be generated via the Manage Centre Portal for the top ten assets with the greatest number of availability problems. It shows:
  - **type**: asset category such as router, load balancer, firewall, etc.
  - **configuration item name**: configured name given to the asset
  - **average availability**: the average monthly availability of the asset
  - **unreachable period**: the amount of time the asset was unreachable (last calendar month)
- **Availability exceptions** is a monthly tabular report that can be generated via the Manage Centre Portal and provides details on the top ten availability exceptions for the previous calendar month. If there has been 100% uptime, then the report is empty as shown in the screenshot below. The report is organized by asset type and includes:
  - **device**: configured name given to the asset
  - **model**: manufacturer name and product family of the asset
  - **availability %**: percentage of time the asset was available during the selected reporting period (last calendar month)
  - **downtime duration**: total downtime of the asset during the selected reporting period (last calendar month)
  - **up since**: date and time since the asset last went from unavailable to available

Figure 6 Availability exceptions report

In addition to the monthly availability reports, it is also possible to get a near real - time view of the availability of any managed device by accessing the Manage Centre Portal. The Manage Centre availability performance chart shows both the availability of the device (green graph area) as well as the number of incidents logged against the device (red circles) over the period of time selected. An example of this report is shown below:

Figure 7 Availability performance chart

2.2.2.3 Capacity reporting

In addition to the threshold alerting discussed in the previous section and o n a monthly basis, a set of capacity reports can be viewed via the Manage Centre Portal that help you in planning changes to your environment to meet the evolving needs of your business. These reports include:

- **Interface bandwidth utilization** is a report that provides utilization information on a per interface basis allowing you to analyse things such as your telecommunications circuit bandwidth needs.
  - **configuration item**: configured name given to the asset
  - **type**: asset category such as router, load balancer, firewall, etc.
  - **interfaces**: number of interfaces the asset has
  - **peak utilization**: a snapshot of the utilization of the highest utilized interface at its peak over the reporting period (last calendar month)
  - **average utilization**: the calculated average of the asset's interface utilization over the reporting period (last calendar month)
- **Processor utilization** is a tabular report designed to identify the level of CPU utilization to ensure appropriate hardware is deployed in your environment. The report provides the following asset details:
  - **configuration item**: configured name given to the asset
  - **processor ID**: the name of the processor as assigned by the associated asset's operating system
  - **peak utilization**: a snapshot of the processor's utilization at its peak over the reporting period (last calendar month)
  - **average utilization**: the calculated average of the processor's utilization over the reporting period (last calendar month)

- **Memory utilization** is a report designed to identify the level of CPU utilization to ensure appropriate hardware is deployed in your environment. The report provides the following asset details:
  - **configuration item:** configured name given to the asset
  - **memory type:** physical memory types such as read-only memory (ROM), programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), random access memory (RAM), static random access memory (SRAM), etc.
  - **peak utilization:** a snapshot of the processor's utilization at its peak over the reporting period (last calendar month)
  - **average utilization:** the calculated average of the processor's utilization over the reporting period (last calendar month)

Interface bandwidth utilization, memory utilization and CPU utilization can also be viewed in near real-time by accessing the Manage Centre portal. By having the ability to view these metrics in real-time NTT support staff and you are able to quickly eliminate or confirm performance issues being experienced. These charts are also easily exportable for reference purposes. The report can be interactively adjusted for the reporting period (e.g. one day, one week etc.).

The figure below is an example of the CPU utilization report from Manage Centre. Notice the slide bar below the graph which allows the user to interactively change the reporting period.

Figure 7 Real-time CPU utilization

Similarly, the following two charts represent the memory and interface bandwidth utilization reports available on Manage Centre. These charts also allow for quick diagnosis capability.

As with the CPU utilization report, the memory utilization report can be interactively adjusted for the reporting period. The ability to monitor memory performance is also of significant value when trying to identify ‘memory leaks’ since the memory utilization is graphically displayed which would otherwise have to be manually captured at various intervals and recorded for later analysis.

The interface bandwidth utilization report in addition to average and peak utilization statistics, also provides statistics of error packets as well as traffic volumes in both inbound and outbound directions as can be seen in the chart below.

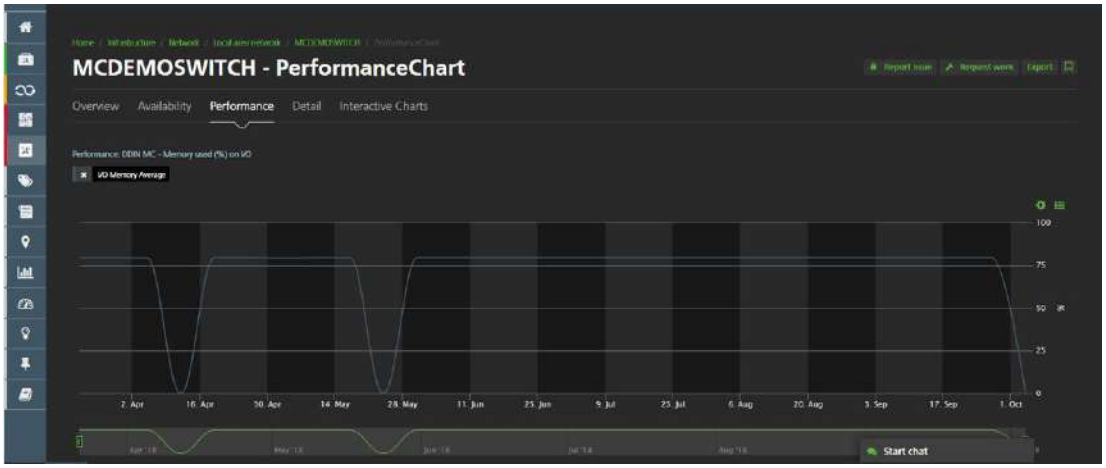

Figure 8 Real-time memory utilization

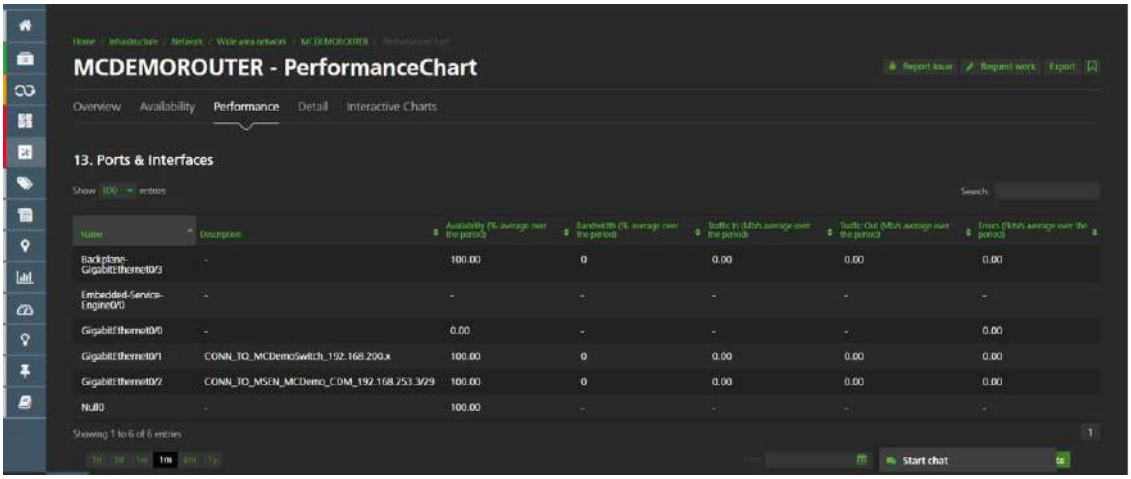

Figure 9 Real-time interface bandwidth utilization

2.2.3 Availability and capacity service level commitments

Description	Service level
Initial notification	Notification to your organization within 15 minutes

Table 4 Availability and capacity service level commitments

2.2.4 Summary of responsibilities

Activity	NTT	Client
Establish a connectivity between your infrastructure and NTT RIM toolset.	AR	R
Enable SNMP on assets to send alerts.	C	RA
Configure GSOA systems to collect events from your covered assets.	RA	I
Tuning of events to trigger the event management process.	RA	C
Firewall and access control list configuration modifications to enable monitoring.	C	RA
Advise of scheduled outages.	I	RA
Advise of MACDs that will impact monitoring.	CI	RA
Notify client of actionable events and track progress (with underpinning Uptime contract).	RA	C
Tuning of thresholds after the three-month baseline period to trigger the incident management process (with underpinning Uptime contract).	RA	C

Table 5 Availability and Capacity Monitoring summary of responsibilities

2.3. Third-Party Support

When faults occur in your IT environment where there are multiple support providers involved, it typically falls on your organization, by default, to identify the fault domain to such an extent that they can reasonably assign the fixing task to the correct support provider. Anything else will simply delay incidents diagnosis and extend mean-time-to-repair while the issue gets bounced from supplier to supplier. Similarly, at the other end of the incident management process, once a support provider claims a successful fix has been provided or implemented, your organization must perform some level of check (testing, acceptance and subsequence deployment) to ensure that the issue is resolved. All of this takes time and some level of technical expertise which distracts your IT team from other priorities.

We offer two Third-Party Support Services: Third-Party Incident Coordination (TPIC) and Technical Incident Management (TIM).

2.3.1 Third-Party Support key client benefits

Third-Party Support reduces the number of service providers your organization must work with during service-affecting incidents. Thus, it simplifies management and relieves your IT staff from time consuming processes.

Depending on the option you choose, our Third-Party Support Services can provide you with a single point of contact for your support contracts across a wide range of technologies and vendors. And, when incidents involve multiple vendors we can also coordinate incident-related activities for you, relieving your IT operations staff of the need to manage the conflicts and requirements of different parties, throughout the process through resolution.

2.3.2 Third-Party Support deliverables

Third-Party Support includes taking a letter of authorization (LoA) from you to manage incidents relating to configuration items with third-party suppliers on your behalf.

Examples include:

- third-party network hardware maintenance providers
- WAN carrier services

The business outcomes are:

- improved availability
- simplified fault assessment and diagnosis
- efficient incident management across multiple vendors
- avoid managing vendor conflict

2.3.3 Third-Party Incident Coordination (TPIC)

When a fault occurs in your environment and there are multiple support providers involved, we coordinate incident-related activities, determining the right resolver and manage the incident through closure.

2.3.4 Third Party Incident Coordination service level commitments

Description	Service level
Incident updates	NTT will update your organization via email on the status of third-party incidents according to the following schedule, or at the next mutually agreed time ● P1 = 30 minutes ● P2 = 2 hours ● All others = 4 hours

Table 6 Third-Party Incident Coordination service level commitments

2.3.5 Third Party Incident Coordination summary of responsibilities

Activity	NTT	Client	Vendor
Provide the ability to log incidents and requests 24x7 with the specified vendors	RA	I	I
Log a new incident and perform component level fault isolation, as well as responding to further requests for information (from NTT)	I	RA	
Determine the right resolver party and log incident with vendor	RA	I	I
Provide letter of authorization for each third party	C	RA	I
Drive third party to resolution (within its agreed commitment)	RA	C	I
Provide periodic status updates (see commitments section)	RA	I	C
Incident diagnosis and resolve issue	I	I	RA
Accept and deploy resolution	I	RA	I

Table 7 Third-Party Incident Coordination summary of responsibilities

2.3.6 Technical Incident Management (TIM)

For devices and/or licenses that you have under maintenance or subscription contract with a third-party vendor (including maintenance contract that NTT holds on your behalf), we will perform incident management including accepting notification of a service incident, diagnosis of the problem, remote resolution when feasible (either by NTT or by a vendor), and incident coordination and management through the third party when on-site support is required. We also deliver visibility of the service status of your assets through our Manage Centre portal.

To be eligible to receive our Technical Incident Management Service, you must have an active on-site support contract with a third-party vendor.

This service supports clients that:

- need one technical point of contact to address incident management across multiple technologies and vendors
- require a transition strategy when they wish to migrate their maintenance support to NTT, but their support contracts are not coterminous
- appreciate the quality of our remote support capabilities but have an existing on-site maintenance contract with another supplier

2.3.7 Technical Incident Management summary of responsibilities

Activity	NTT	Client	Vendor
Provide letter of authorisation for each third party where applicable	C	RA	I
Provide the necessary information for our Delivery Centers and engineers when logging an incident or request, as well as in response to further requests for information during the lifecycle of the incident or request	C	RA	RA
Provide remote diagnostic connectivity	C	RA	
Provide the ability to log incidents and requests 24/7.	RA	I	I
Collect physical indicators (lights, etc.)	AI	CR	
Log a new incident and provide the necessary information for our Delivery Centers and engineers when logging an incident or request, as well as in response to further requests for information during the lifecycle of the incident or request.	C	RA	
Update incident and status	RA	I	C
Incident Diagnostics	RA	CI	
Drive third party to resolution	RA	C	I
Resolve incident or request	RA	I	C
On-site visit when applicable	A	C	R

Activity	NTT	Client	Vendor
Despatch new hardware when applicable	A	C	R
Provide periodic status updates	RA	I	C

Table 8 Technical Incident Management summary of responsibilities

2.4. Configuration Archive

One of the most effective mechanisms to ensure the shortest possible repair times when failures occur is a backup of the last known good configuration file. Loads of time can be wasted attempting to regenerate the most recent configuration before the failure 'in the haze of battle'. Often there are small configuration tweaks that have been implemented that won't be discovered for weeks or even months. Automated configuration backups that include most recent configurations is key to gaining this benefit[8].

2.4.1 Configuration Archive key client benefits

The benefits of archived configurations include:

- improved security posture
- better adherence to regulatory compliance standards and enhances auditing of same
- reduced risk associated with configuration errors by enabling the return to known good versions
- greatly enhanced speed of on-site device replacements by avoiding the need to reconfigure from scratch and the associated errors

2.4.2 Configuration Archive deliverables

The following deliverables will be performed as part of configuration archive:

2.4.2.1 Configuration backup

NTT will back up the configuration item's configuration file and compare that file to the most recently stored version. If they are the same, the most recent backup is discarded. If they are different, the new file becomes the most recent backup and the previous version becomes current minus one. The previous current minus one is discarded.

[8] Configuration Archive requires a connection to the client be available via a Virtual Private Network (VPN). The method of connection is agreed upon with the client.

2.4.2.2 Configuration access

Easy and quick access to stored configuration files are critical not only during incidents, but also for any configuration analysis or regulatory compliance requirements your organization might have.

Configuration Archive report will be published as Knowledge Article in ITSM every month and will be available on Manage Centre.

2.4.3 Configuration Archive summary of responsibilities

Activity	NTT	Client
Modify firewall rules as required to allow archiving[9]	C	RA
Provide necessary device credentials to allow configuration download[10]	C	AR
Configure NTT systems to collect archives per schedule	RA	I

Table 9 Configuration Archive summary of responsibilities

[9] For Cisco equipment, for example, this requires port 22 or 23 to be allowed through the VPN.

[10] For Cisco equipment, for example, this requires level 15 login access.

2.5. Proactive Problem Support

An integral part of NTT's Proactive Problem Support is the identification and root-cause analysis of chronic incidents. A chronic incident is any repeated incident or pattern of incidents with a configuration item. A chronic condition may be the result of an intermittent hardware fault, WAN circuit, software, power issue, or periodic congestion on the network that affects your end users' ability to access and use applications. These conditions initiate the problem support process in which NTT determines whether there is an underlying problem which may otherwise go unnoticed until actual failure.

Once the chronic condition has been identified and validated by NTT, a root-cause analysis of the problem will be performed, reviewed with your team, and appropriate actions taken by the NTT technical and operations teams to prevent or minimize the impact of these problems, when within the scope of services purchased.

All problems will have a root-cause analysis done. This review will consider at least the following:

- review of support processes to determine the tasks that were executed correctly and those that were not
- what service or process improvements are recommended
- what may be done to prevent a recurrence
- whether there was any third-party responsibility and whether follow up actions are needed as part of NTT's vendor management support or you with the third party or vendor

The outcome of the review may be recommended changes to your covered infrastructure to prevent incidents from occurring or reoccurring.

Please note that Proactive Problem Support will require, as one of its primary sources of information, Availability and Capacity Monitoring and, therefore, requires the purchase of that service also[11].

2.5.1 Proactive Problem Support key client benefits

Proactive Problem Support key client benefits include:

[11] Proactive Problem Support requires a connection to the client be available. The method of connection is agreed upon with the client.

- reduction of downtime to business services supported by the infrastructure that can directly affect the bottom line
- less demand on your internal teams resulting in a potential cost reduction
- increased focus on core business activities for your internal IT teams

2.5.2 Proactive Problem Support deliverables

2.5.2.1 Problem identification and recording

NTT will identify and record problems on the configuration items and IT services supported by the services. NTT will perform frequent and regular analyses of incident and problem data to identify any trends as they become discernible. Once detected, we will record, categorise, and prioritise the problem.

2.5.2.2 Solution identification and recording

NTT investigates and determines the root cause of a problem. Based on the root cause, a permanent resolution to the problem is then identified (or further investigation suggested) using one or more applicable techniques and all available information. NTT notifies you when the problem record is updated with the identified permanent resolution according to the notification matrix and provides all relevant information. A known error record is created in NTT's known error database.

2.5.2.3 Solution implementation

Upon receipt of a notification from NTT, your organization reviews the permanent resolution and determines the course of action to take (if any).

If requested by you, NTT implements the permanent resolution remotely where it is within the scope of the Services through the MACD or Annual Version Updates services as contracted with NTT.

Based on scope, size, and complexity of the solution, NTT may propose a fixed price project or perform the work on a time and materials basis for a permanent resolution not within the scope of the Services.

2.5.2.4 Root-cause analysis review

NTT will conduct a root-cause analysis review of problems. Proactive Problem Support root cause analysis will be published as Knowledge Article whenever there is a Problem Ticket and will be available on Manage Centre.

2.5.3 Proactive Problem Support summary of responsibilities

Activity	NTT	Client
Modify firewall rules as required to allow archiving[10]	C	RA
Provide necessary device credentials to allow configuration download[11]	C	AR
Configure NTT systems to collect archives per schedule	RA	I

Table 10 Proactive Problem Support summary of responsibilities

2.6. Technical Account Management

Maintaining expertise in all the technologies that organizations employ can be difficult. Many organizations focus their teams on how the technology is implemented to support business outcomes. In contrast, Support organizations like NTT, typically have more technical skills than many organizations, but lack the understanding of their client's specific implementation of said technologies. The Technical Account Manager bridges the gap between deep technical support and your specific implementation.

Please note that many of the activities of Technical Account Management rely on Proactive Problem Management and, therefore, that service feature is required to be purchased as well as Availability and Capacity Monitoring.

2.6.1 Technical Account Management key client benefits

The primary goal of Technical Account Management is to provide your organization a direct relationship with a senior technical resource who has an in-depth knowledge of your environment

Specifically, your organization will see the following business benefits:

- maximum return on future IT investments
- reduced total cost of ownership
- improved service performance
- reduction in number of incidents
- reduction in incident resolution time

2.6.2 Technical Account Management deliverables

2.6.2.1 Assigned Technical Account Manager

A Technical Account Manager will be assigned to you who will provide the vast majority of their deliverables on a remote basis but will be responsible for establishing a good technical relationship with your engineering team to facilitate the quick completion of in-scope activities providing you with the maximum technical value.

He/she will have advanced skills in the technologies associated with the assets covered by our service.

2.6.2.2 Priority one and priority two incident and problem escalation management and support

During business hours, the TAM will act as the primary technical contact for priority one (P1) and priority two (P2) incidents or be available for technical escalation of same. The TAM will work with your team to identify required documentation, and help collect same, and provide that documentation to our operations center team in order to properly scale their client-specific knowledge.

The TAM will also participate in regularly scheduled service incident reviews as scheduled by your organization.

2.6.2.3 Root-cause analysis

When problems are identified, proper problem tickets will be created in our IT Service Management system. It will be the responsibility of the Problem Manager to ensure a root-cause analysis of all opened problem tickets is performed and documented in the problem ticket.

2.6.2.4 Monthly technical reviews

On a monthly and remote basis, the TAM will be responsible to schedule and hold technical reviews and include relevant technical issues in the agenda of which should include, at a minimum:

- incident review
- problem/root-cause review
- recommendations
  - configuration
  - software patches
  - architecture

2.6.2.5 Change impact analysis

The assigned TAM will evaluate normal, urgent, and emergency changes for their impact on the covered assets and make a recommendation regarding the impact of the change. The TAM will prepare a recommendation that will include a description of the planned change and impacts on the existing infrastructure. Where possible, the following information/considerations will be included in the recommendation:

- the impact the change will have on business operations
- the impact on IT services that run on the network
- the effect of not implementing the change

2.6.3 Technical Account Management service level commitments

Description	Service level
Technical review meetings	Will be held within 12 business days after the start of the following month

Table 11 Technical Account Management service level commitments

2.6.4 Technical Account Management summary of responsibilities

Activity	NTT	Client
Provide information on proposed changes	C	RA
Evaluate change impact	R	A
Provide documentation and as built information	C	RA
Technical review meetings	RA	C
Create and update GDC run books	RA	C

Table 12 Technical Account Management summary of responsibilities

2.7. IT Service Integration

IT Service Integration offers you real-time visibility, within your own systems, into the status and resolution of tasks affecting your covered infrastructure. By integrating your internal service desk application with the NTT IT Service Management system (ITSM), you can:

- open new incidents, change service requests, and problem tasks
- exchange files and information
- see the status of tasks in near real-time through a secure, predefined interface and protocol to exchange information.

IT Service Integration allows you and NTT to efficiently collaborate on the resolution of incidents, problems, and requests by sharing information in a

consistent manner. This improves the responsiveness of call center agents and engineers when contacting you and updating tasks.

Through IT Service Integration you can achieve the following business benefits:

- reduced time, effort, and expense through automated workflow collaboration
- reduction of mean-time-to-repair
- transparent visibility in service performance.

2.7.1 IT Service Integration key client benefits

Benefits of service desk integration:

- inter-partner/vendor operational efficiency
- real-time and end-to-end visibility of the resolution process in your own systems
- minimized downtime due to transcription and data entry errors
- reduced costs through integrate once, connect to multiple, cloud-based service approach.

2.7.2 IT Service Integration deliverables

IT Service Integration provides the following two key deliverables:

- workflow automation and
- advanced message tracking.

2.7.2.1 Workflow automation

Many of our clients implement an internal IT Service Management (ITSM) system in order to track and manage the resolution of incidents affecting their infrastructure. When an incident is logged, much of the information we need is already contained in the client's internal ITSM system.

IT Service Integration provides a structured format to share specific information about incidents, problems, change and service requests, which enables more efficient collaboration.

This format includes, but is not limited to:

- task name
- task description
- priority
- contract item
- classification

Through this integration, you will be able to:

- open new incident, problem, change and service requests from within your own ITSM system and have them transmitted to NTT automatically,
- see real-time updates on task status from within your own ITSM system,
- provide real-time information and updates to a task through your own ITSM system, and
- exchange relevant files with NTT.

You will be able to open four types of tasks through IT Service Integration:

1. incidents
2. service requests
3. change requests
4. problems

For each of the task types a specific workflow will be implemented from your service desk application, through our cloud-based integration platform (IT Service Integration Platform) to NTT's IT Service Management system (ITSM). Workflow mapping is used to define the possible status and transactions on both sides (your system(s) and NTT).

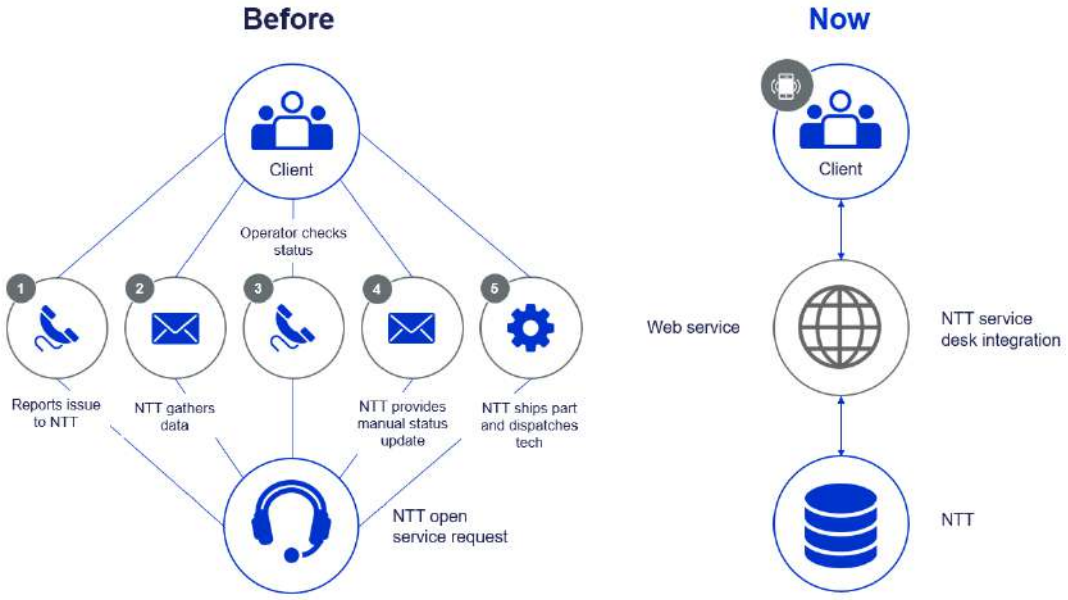

Figure 10 Workflow automation

Workflows are mapped through status code mapping tables within the IT Service Integration Platform (ITSI platform). Using these tables, each incoming transaction can be automatically transformed into the transaction type that the other side expects. Mapping tables define the correct mapping between the status codes and the core transaction types on both sides (your systems and NTT).

Service desk agents from both NTT and your organizations will manage tasks as per the standard processes within their respective organizations. Updates are automatically sent when modifications are made against a task. Any updates received from you will automatically update or create a ticket in ITSM.

2.7.2.2 Advanced message tracking

NTT will track the delivery and processing of transactions exchanged between our IT Service Management systems.

For each task update submitted, a delivery status can be available in the middleware (ITSI platform) and indicate:

- if the update has been sent,
- if you have received the update,
- if your service desk application has processed the update, and
- if there have been partial delivery issues.

2.7.2.3 Multiparty integration

The same IT Service Integration solution can be used if you want to integrate to other service providers and vendors with whom you may have a support agreement. As your connection, processes and workflows will already have been established into the IT Service Integration solution, the service provider or vendor needs to be connected into the IT Service Integration solution and their processes and workflows established into the IT Service Integration solution (and mapped to your processes and workflows). If the service provider or vendor already has an established workflow into the IT Service Integration solution, connecting to them can be performed by mapping their workflow to yours.

You can build, with IT Service Integration, an ecosystem of integrated vendors, service providers and other partners. Each additional vendor/service provider and workflow will be quoted separately.

2.7.3 IT Service Integration service level commitments

Description	Service level
Provide information on proposed changes	System availability greater than or equal to 99.85%
Evaluate change impact	Priority 1: 15 minutes with an 24/7 service calendar Priority 2: 1 hour with an 8/5 service calendar Priority 3 and 4: 1 day with an 8/5 service calendar
Update to client	Priority 1: every 2 hours with an 24/7 service calendar Priority 2: every 8 hours with an 8/5 service calendar Priority 3: every 4 days with an 8/5 service calendar Priority 4: every 7 days with an 8/5 service calendar

Table 13 IT Service Integration service level commitments

2.7.4 IT Service Integration summary of responsibilities

Activity	NTT	Client
Notification of any changes to the integration or systems that will impact the ongoing delivery of the service	RA	RA
Provide documentation of existing and future processes	I	RA
Ensure connectivity to your ITSM system	C	RA
Run test cases as part of service deployment	RA	R
Provide technical expertise on your organization's ITSM system	I	RA

Table 14 IT Service Integration summary of responsibilities

You will be required to make the following resources available to form part of the transition team:

- a business owner to be responsible for the Project Deliverables
- a project manager to manage and coordinate transition effort, as the primary point of contact
- a business analyst and/or process manager to understand requirements, help define operational process and provide direction to developers, should have an understanding of the client system and operational process
- developer(s) to develop the integration interface between NTT's Management System and the client system, ensuring that data is aligned between systems for integrated elements and defines the value mapping

2.8. Service Delivery Assurance

Service Delivery Assurance provides governance and control across the various service entitlements, processes, and systems necessary to manage the full lifecycle of Services that are offered to your organization. It covers transition, operation, account governance, and continuous improvement of services[12].

NTT will assign a Service Delivery Manager (SDM) to provide continuity in service and act as an advocate for you within NTT. The Service Delivery Manager is the primary interface who will manage the Services relationship between your organization and NTT. The Service Delivery Manager will own establishing the service governance structure, scheduling, running service management review meetings, and ensure processes and documentation are in place to manage your covered infrastructure.

The Service Delivery Manager will also oversee:

- operations performance - including:
  - status of ongoing initiatives and actions
  - review of the most recent service management reports
  - agreement on new service improvement initiatives
- operations run book - The Service Delivery Manager will work with the transition team and/or the assigned Technical Account Manager to develop a run book that will include processes, escalation lists, and documentation.

  Once operations support is initiated, the run book will be updated on a continuous basis to reflect changes to your covered infrastructure. Specifically, the run book will include such items as:
  - network map(s)
  - site-level engineering diagrams
  - client and site contacts
  - configuration item and IT service mappings (relationships)
- contract and financials management – The Service Delivery Manager will:
  - provide assurance regarding the compliance of, and lifecycle management for, all contracted Services
  - receive and manage change requests relating to the statement of work (SOW) and agreement, e.g. additional engagements or projects, adding configuration items and IT services support to the Services (service coverage), migrating configuration items and IT services to new or different locations etc.
  - interface with NTT internal contract management teams to normalise and execute change orders

[12] Service Delivery Assurance requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

- support billing/invoicing inquiries and/or disputes

- client satisfaction – NTT will monitor your satisfaction and, as required, identify service improvement plans to address your satisfaction with the Service.

Overall, the Service Delivery Manager is responsible for ensuring that both your organization and ours have a clear and unambiguous expectation of the level of service to be delivered to you.

2.8.1 Service Delivery Assurance key client benefits

The key client benefits of service delivery assurance are:

- a single trusted communication channel for the Services provided
- service level targets are agreed, monitored, and reported on
- alignment and visibility of the Services being delivered by NTT
- strong relationships within your organization's management and executive team, that establish NTT as a trusted advisor
- a structured alignment between your organization and NTT to maximise the quality of the Services by providing a feedback mechanism
- a means for you to raise and resolve issues and concerns with NTT Services

2.8.2 Service Delivery Assurance deliverables

NTT will provide a robust set of deliverables to increase the effectiveness of the business relationship throughout your organization and manage the service level targets.

2.8.2.1 Assigned Service Delivery Manager

NTT's Service Delivery Assurance Service offers an assigned account advocate who is responsible for delivering control across service entitlements, processes, and systems under contract with us, as well as providing continuous service improvements.

The Service Delivery Manager will:

- be both an ambassador of NTT and representative of your organization and needs back into NTT,
- preserve and maintain the quality, integrity, and availability of the Services,
- be the primary interface that manages the service relationship with service delivery teams,
- be responsible for the execution phase of the agreement/contract post sales,
- maintain overall contractual governance to ensure compliance, and drive consistency of Services, and
- where required, manage across multiple NTT Services towers.

Specifically, his/her responsibilities will include:

Capturing and managing minutes, agenda items, actions, and decisions

NTT will ensure that all meeting-related tasks are actioned. This includes scheduling of meetings, management of attendees, capturing of inputs/outputs, and management of minutes, agendas, actions, and decisions taken from meetings. The key outcome of this deliverable is to provide a traceable history of meetings and their outcomes and to enable improved governance.

Single point of reporting access

NTT will ensure that all reporting and additional service collateral is maintained and delivered via the Manage Centre portal. This includes all reports for service availability, performance and capacity management, service level management etc.

Establish, monitor, and report

NTT will create and publish a report that will provide an 'as is' view of your satisfaction levels within the Services. Publishing of reports to the Manage Centre portal will create an auditable history.

Issue management and reporting

Issue management involves key stakeholders such as your organization, NTT, vendors, or third-party suppliers capturing and tracking issues in a central repository via the Manage Centre portal. Issues may be logged because of risks being identified, although risks are not necessarily a requisite predecessor. Issues can be identified as situations that may affect the Services being delivered.

2.8.2.2 Service level requirements discovery

The Service Delivery Manager will assemble and compile the committed service levels relative to all services for which we have engaged with your organization and develop report against which we will measure the success of the Services. There is a standard report template that is used.

2.8.2.3 Service level monitoring and reporting

NTT will continuously monitor the service level targets agreed with you, and compile and make available a monthly service level management report. This report will also include NTT recommendations for service level target improvements.

2.8.2.4 Service management review meetings

The Service Delivery Manager will establish the business and technical relationships that are focused on reviewing service delivery results and activities.

In addition, the Service Delivery Manager will facilitate quarterly service management review meetings with you to review operations performance and adherence to service level targets.

2.8.3 Service Delivery Assurance service level commitments

Description	Service level
Monthly business review meetings	Will be held within 12 business days after start of the following month after the end of the month
Monthly service level management reports	Reports will be available 10 business days after start of the following month

Table 15 Service Delivery Assurance service level commitments

2.8.4 Service Delivery Assurance summary of responsibilities

Activity	NTT	Client
Develop reporting with service level targets	RA	C
Identify service improvement opportunities	RA	C
Participate in monthly review meetings	RA	R

Table 16 Service Delivery Assurance summary of responsibilities

2.9. Moves, Adds, Changes, and Deletes (MACDs)

MACDs is a service option that offers a flexible model for managing and executing the moving, adding, changing, and removing of hardware and software configuration in your environment.

2.9.1 MACDs key client benefits

MACDs provide a mechanism, in the form of a time block composed of a number of 'service units', for your organization to get standard changes fulfilled without the need for a purchase order process. Specifically, benefits include:

- an easy pay system for standard changes,
- more cost predictability through prepaid time blocks,
- volume discounting for prepaid blocks, and
- less demand on internal teams leading to lower costs.

2.9.2 MACDs deliverables

2.9.2.1 MACD request management

NTT will manage the execution of requests for MACDs on your behalf. This includes the following:

- providing a method to log request
- validation of the request as an agreed MACD
- execution of the MACD

MACDs are administered through a service unit system, where service units are purchased in advance and then deducted in the execution of the MACDs.

A list of common MACDs and the number of service units required to perform each is available in the appendix C.[15]

Should a client require performance of a MACD onsite, the number of service units deducted per MACD is based on:

- the time it takes to perform the task
- the urgency
- the requested hours of execution
- the engineering skill required for the task
- the time it takes to travel to and from the client site

2.9.2.2 MACDs fulfilment

NTT will implement the MACDs in accordance with your implementation plan. After execution, MACDs will be reviewed with your team to confirm that they produced the expected result.

The following tasks are indicative examples of those that can be delivered under the configuration MACDs service feature:

- configuration of, and configuration changes to, covered assets
- software provisioning of IP phones
- adding or deleting access credentials
- routing changes

For tasks to qualify as configuration MACDs, they must have all of the following attributes:

- relate directly to assets supported under the Services
- can be performed remotely
- no scoping or project management is required for the execution of the tasks
- performance of a single instance of the task should not take more than four hours
- performance of the complete set of requested tasks (that is, repeating the same single instance or similar tasks in multiple locations or configuration items) shouldn't take one of our appropriately skilled engineers more than 4 hours

[15] Emergency MACDs, and out-of-business-hours MACDs will be charged at a higher rate

All MACDs are considered to be client pre-approved, standard changes for which the client has already mitigated potential risk. However, NTT may, at our discretion, consider and inform the client of the potential impact of a MACD[13].

Executing tasks outside of Business Hours will be based on availability of engineers and will be planned in consultation.

For out-of-business-hours changes, an uplift factor is added vs standard changes according to the table below:

Service window	Uplift factor
Workweek business hours[14]	Standard charges apply
Workweek non-business hours[15]	1.5xStandard charges per 15min MACD
Weekend and public holidays	2xStandard charges per 15min MACD

For emergency changes during business hours, service units will be deducted at twice the rate of standard changes.

Emergency changes during out-of-business-hours will be deducted at twice the rate of out-of-business hours changes.

2.9.2.3 MACDs reporting

Our management system will manage the service unit balances in real-time as configuration MACDs are completed. Should the service unit balance drop below a certain threshold, a notification will be sent to a designated representative in your organization as well as to our client manager or another designated resource.

We will also provide you with a service unit report on the service portal. The report will include:

[13] Engagements that take longer than 4 hours will be pursued as separately billable Professional Services engagements.

[14] Workweek may differ in different countries (e.g. Mon-Fri in Europe/Americas/APAC; Sun-Thurs in Middle East/Israel)

[15] Workweek may differ in different countries (e.g. Mon-Fri in Europe/Americas/APAC; Sun-Thurs in Middle East/Israel)

- the opening balance
- the number of service units purchased during the period
- the number of service units used during the period
- the closing balance

2.9.3 MACDs service level commitments

Service window	Uplift factor
MACDs completion time	MACDs will be completed within the time frame agreed between your organization and NTT The default lead times to commence execution are as follows: Standard: 3 business days (2 business days assessment and preparation) Emergency: 4 business hours

Table 17MACDs service level commitments

2.9.4 MACDs summary of responsibilities

Activity	NTT	Client
Approve a set of standard changes	C	RA
Open MACDs request on the Manage Centre portal	I	RA
Record MACDs and manage change to conclusion	RA	I
Approve emergency changes as generated	I	RA

Table 18 MACD summary of responsibilities

2.10. Annual Version Updates

The goal of Annual Version Updates is to provide a once annual project to plan, schedule, and control the insertion of updated device operating systems and/or asset configurations in bulk and in a proactive manner. Individual operating system patches or configuration changes that are a result of service-affecting incidents are handled under incident management and availability management[16].

The objectives of Annual Version Updates are to:

- reduce the number of deployed versions in the environment
- ease the burden of patch management
- keep more current to the latest operating system version

[16] Annual Version Update requires that a persistent connection to the client environment be available; such connection method to be agreed with the client.

- reduce the risk of deploying patches and upgrades

The following may be included in version updates:

- technology updates (patches, service packs …)
- minor OS releases (software updates, dot releases …) that are necessary for future problem or incident avoidance
- major releases (generally current minus one) of the latest generally deployable software currently supported by the vendor

There may be cases where a technology update or a minor OS release requires a system hardware upgrade to comply with current manufacturer's specifications. Such hardware upgrades are not provided as part of Annual Version Updates. NTT will provide you with an estimate and statement of work (SOW) prior to deploying any hardware or software upgrades for configuration items or IT services under support.

2.10.1 Annual Version Updates key client benefits

The key client benefits of Annual Version Updates are:

- keeping configuration items current with all OS releases and patches
- meeting compliance requirements and maintaining internal security policies
- fewer roll backs due to failed or poorly planned updates
- better control over your covered assets
- lower demand on internal IT teams and a potential cost reduction

2.10.2 Annual Version Updates deliverables

2.10.2.1 Version update planning

NTT will complete planning and preparation activities for version updates approved by your CAB. These activities include:

- identification of the scope, model, and content of the version update,
- a risk assessment for the version update,
- identification of stakeholders affected by the version update,
- identification of the stakeholders that approved the version update,
- identification of the team responsible for the version update,
- development of a deployment plan
  - delivery and deployment strategy
  - resources for the deployment

- pass/fail criteria
- roll back plan

- building and testing prior to production.

2.10.2.2 Version update building and testing

NTT will, prior to building the actual version update, work with your organization to construct the test environment for the release in your lab or safe or low-impact segment of your environment and document the build and test procedures. Once the version update has been built, it will be tested, and the results provided to your requestor/approver.

2.10.2.3 Version update deployment

NTT will deploy the version update in accordance with the deployment plan, build, and test procedures. A deployment review document will be completed and provided to you.

The review document will contain, at a minimum, the following information:

- version update deployed with or without issues
- information on issues experienced, if any
- a list of configuration items on which the version update was deployed

2.10.2.4 Early life support

Early life support is provided to ensure stability and verify performance. NTT will resolve initial incidents and problems associated with the version update. The deployment team will ensure that the documentation and knowledge management system are updated with additional diagnostics, known errors, and workarounds.

2.10.3 Annual Version Updates service level commitments

Service window	Uplift factor
Timely execution of updates	Updates will be completed within the maintenance window agreed between your organization and NTT

Table 19 Annual Version Updates service level commitments

2.10.4 Annual Version Updates summary of responsibilities

Activity	NTT	Client
Identification of recommended updates to apply	RA	C
Creation of test plan	R	A
Supply of assets on which to test the release	C	RA
Contractual mechanism to obtain required updates	I	RA

Table 20 Annual Version Updates summary of responsibilities

3. Manage Centre Portal

NTT enables its clients to visualize vast volumes of data and to easily access information about their assets through the **Manage Centre** portal.

The Manage Centre portal, a web-based portal that enables clients to log incidents and service requests, query the status of incidents and service requests, and view contract information and other service reports.

Note that as part of the service transition activities, NTT train s designated representatives in your organization on the use of Manage Centre portal. The training includes a demonstration to up to five designated contacts.

3.1. View infrastructure health

If we monitor your environment, you'll be able to:

- easily see the health status of your infrastructure
- drill down to view impacted devices
- drill down into each device and see
  - impacting incidents
  - historical and real-time availability metrics
  - historical and real-time capacity and performance metrics

Figure 11 View infrastructure health

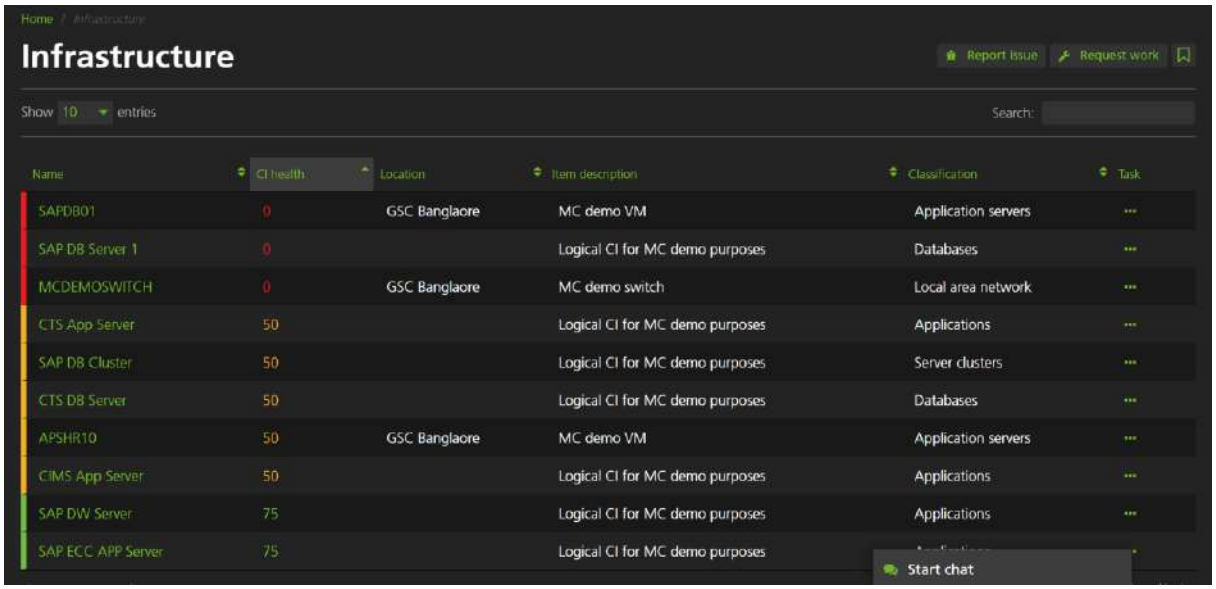

Figure 12 View infrastructure health

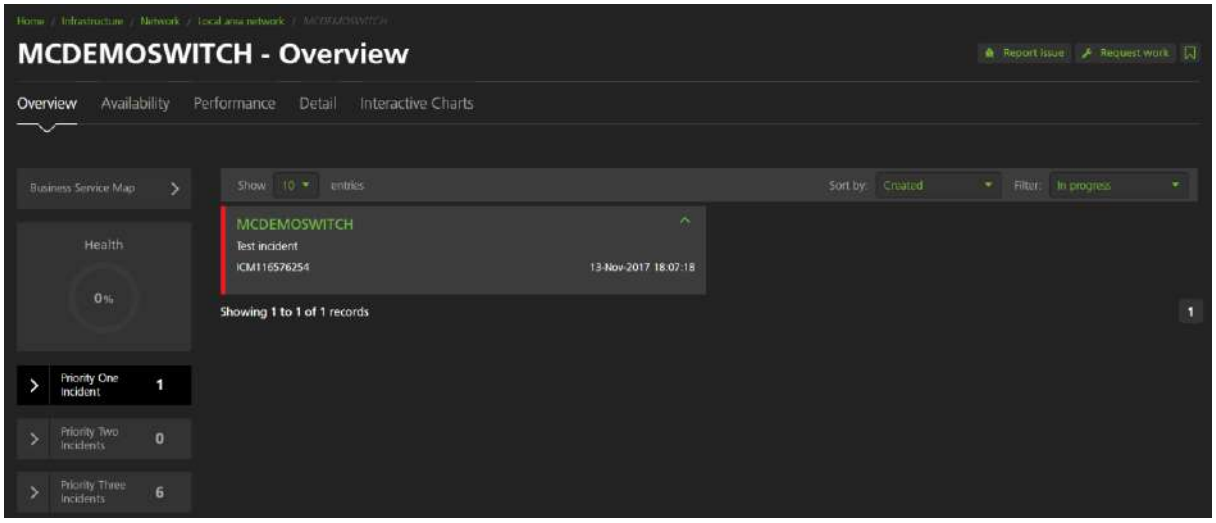

Figure 13 View infrastructure health - overview

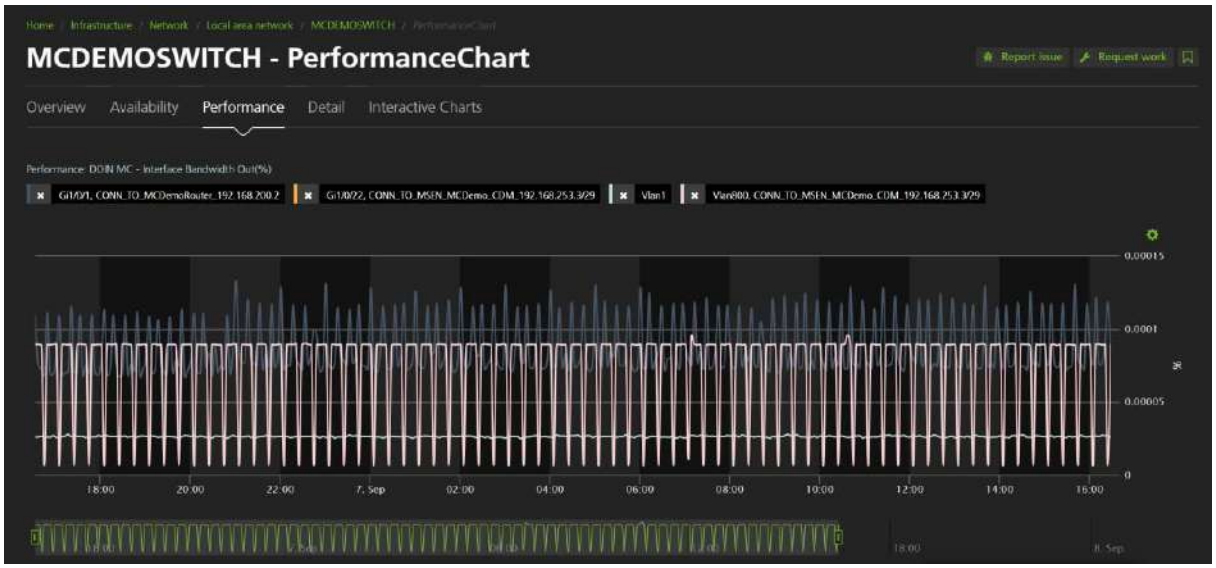

Figure 14 View infrastructure health – performance chart

Figure 15 View infrastructure health – availability chart

3.2. Online incident and request logging

Manage Centre provides your team with the 24/7 online capability to:

- log incidents and service requests [17]
  - search by site or asset
  - include attachments or comments
- requests for one-time reports
- requests for Manage Centre support
- requests for Manage Centre feature enhancements
- view all open incidents and service requests and the real-time status of service level targets
- view incident and service request history (up to 18 months)
- query incidents and service requests by NTT reference number, date, status or client's internal reference number (if provided to Global Delivery Centers)

[17] Priority one and two incidents should be logged by phoning the Global Delivery Centers.

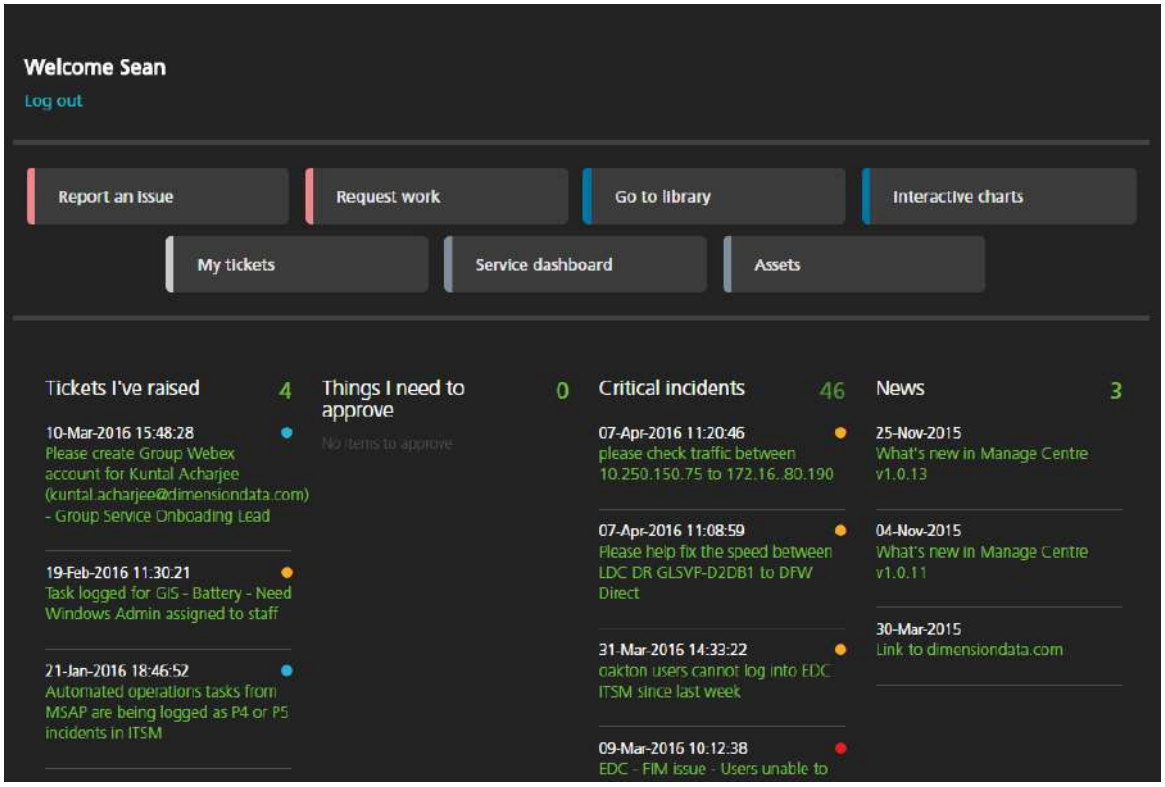

Figure 16 Incident and service request logging

3.3. Online access to incident and request reports

Manage Centre provides easy and convenient access to a variety of prebuilt incident and service request reports. These reports include:

- Incidents
  - Closed incident summary
  - Incident summary
  - Historical incident trend
  - Escalated incidents
  - Mean time to respond
  - Mean time to restore
  - Incidents by age
  - Closed in the last 30 days
  - Historical major incident trend
- Requests
  - Requests
  - Closed request summary
  - Request summary

Uptime Proactive Support Services

- Historical request trend
- Closed in the last 30 days
- Requests by age
- Average time to close

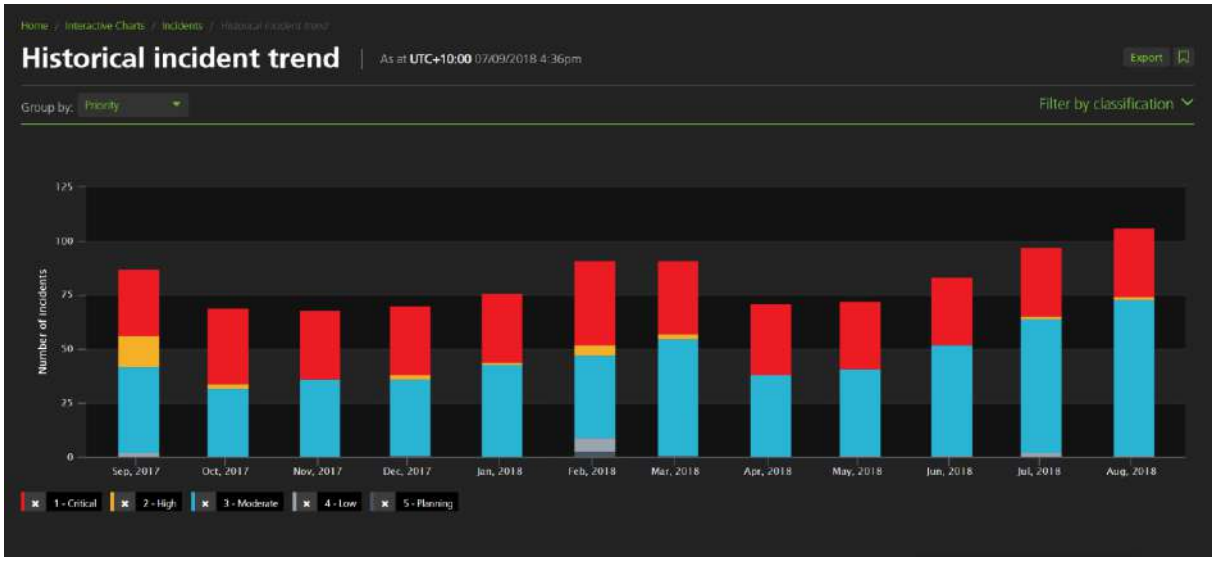

Figure 17 Historical incident trend report chart

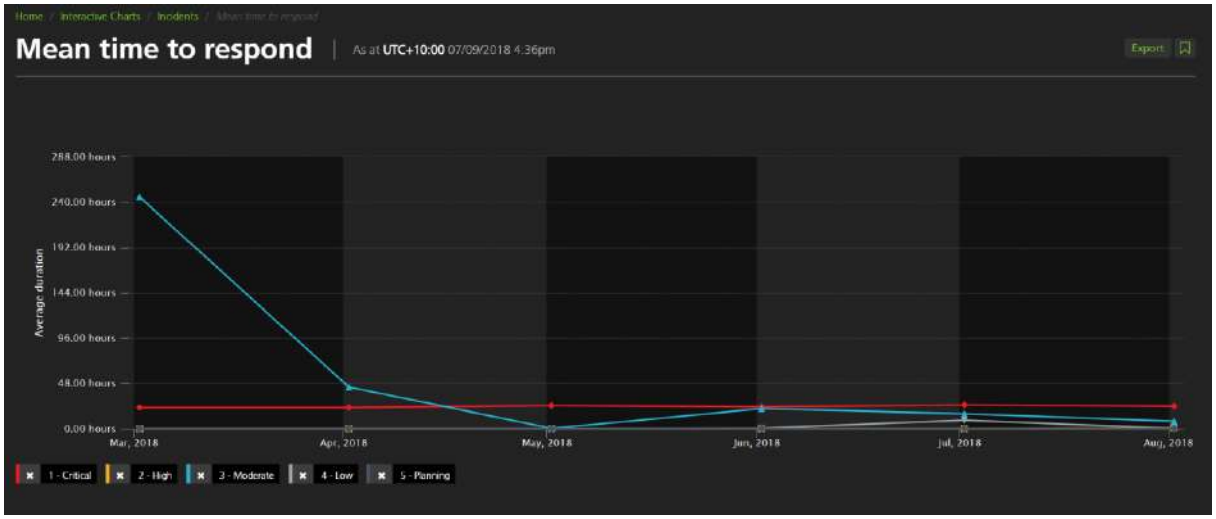

Figure 18 Mean time to respond report chart

3.4. Online access to asset reports

Manage Centre provides easy and convenient access to asset reports.

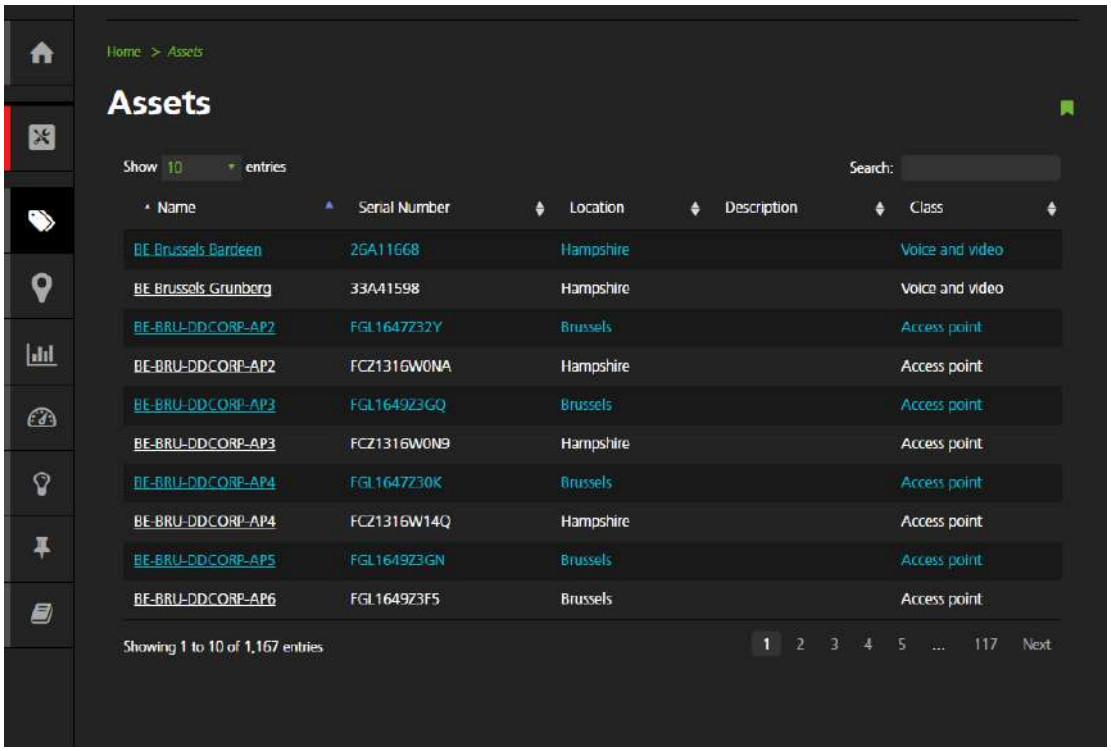

Figure 19 Asset reports

3.5. Service level dashboard

With all Uptime Service Plans we provide some mix of service level commitments which include incident response, parts to site, and labour to site. To enable you to track our achievement on our commitments we provide you the ability to see our current compliance status on a service level dashboard.

This dashboard allows you to view SLA achievement for each service level and each task type for the last 12 months.

You can also drill down into any figure that is less than 100% to view the list of breaches, the tickets and the ticket comment history.

Your view from our Manage Centre portal will look similar to the below.

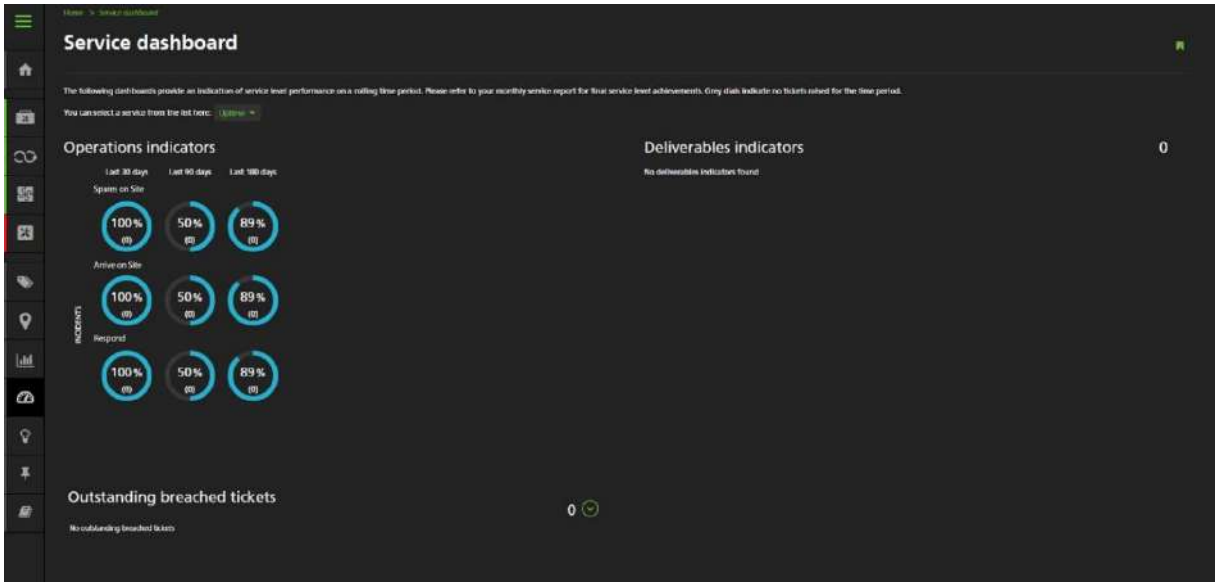

Figure 20 Service level dashboard

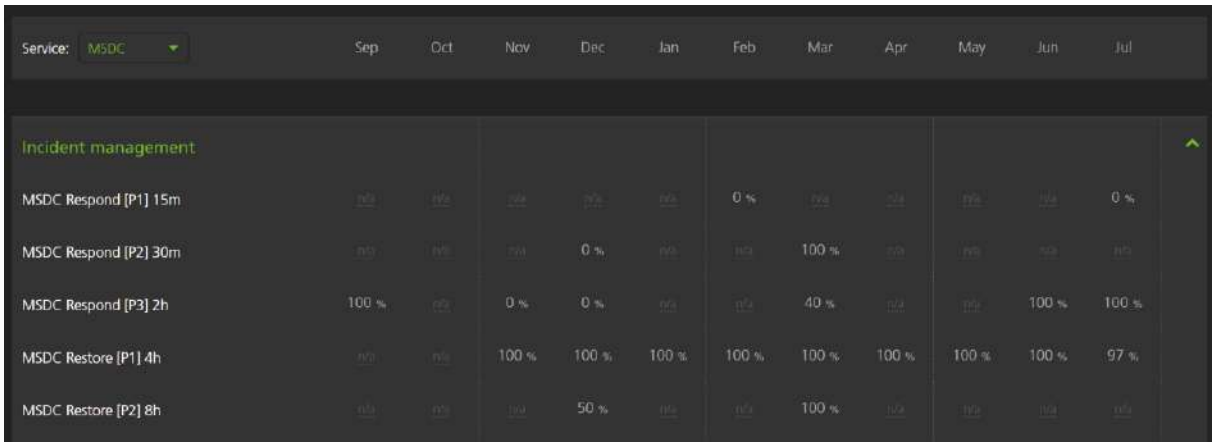

Figure 21 Service level dashboard – incident management

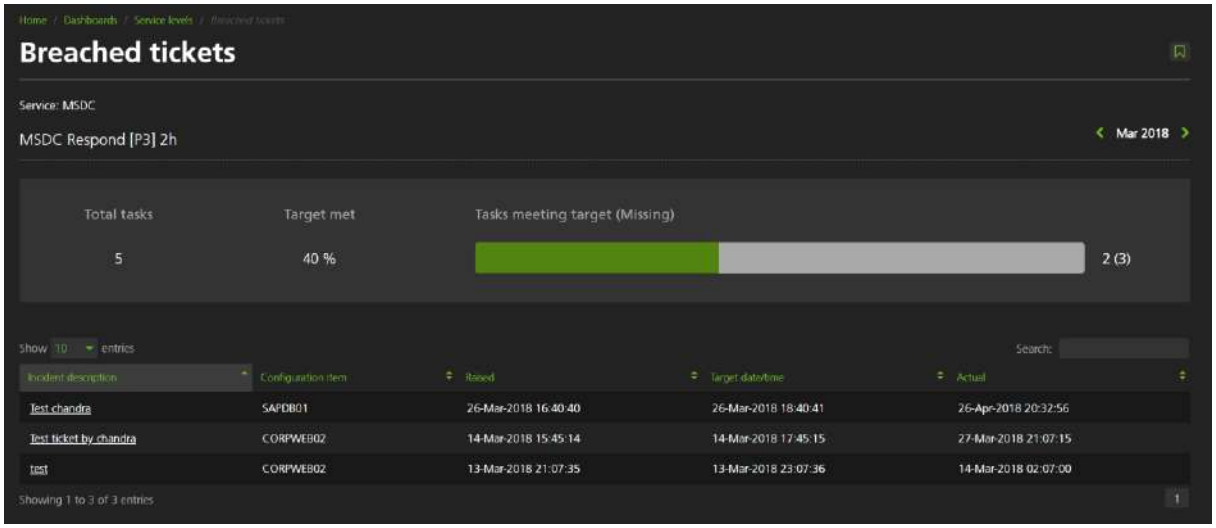

Figure 22 Service level dashboard – breached tickets

3.6. Live chat

You will be able to communicate with our support team via real -time live chat.

Once a chat session is finished the chat transcript will be sent to you via email and you will also be able to view it in Manage Centre.

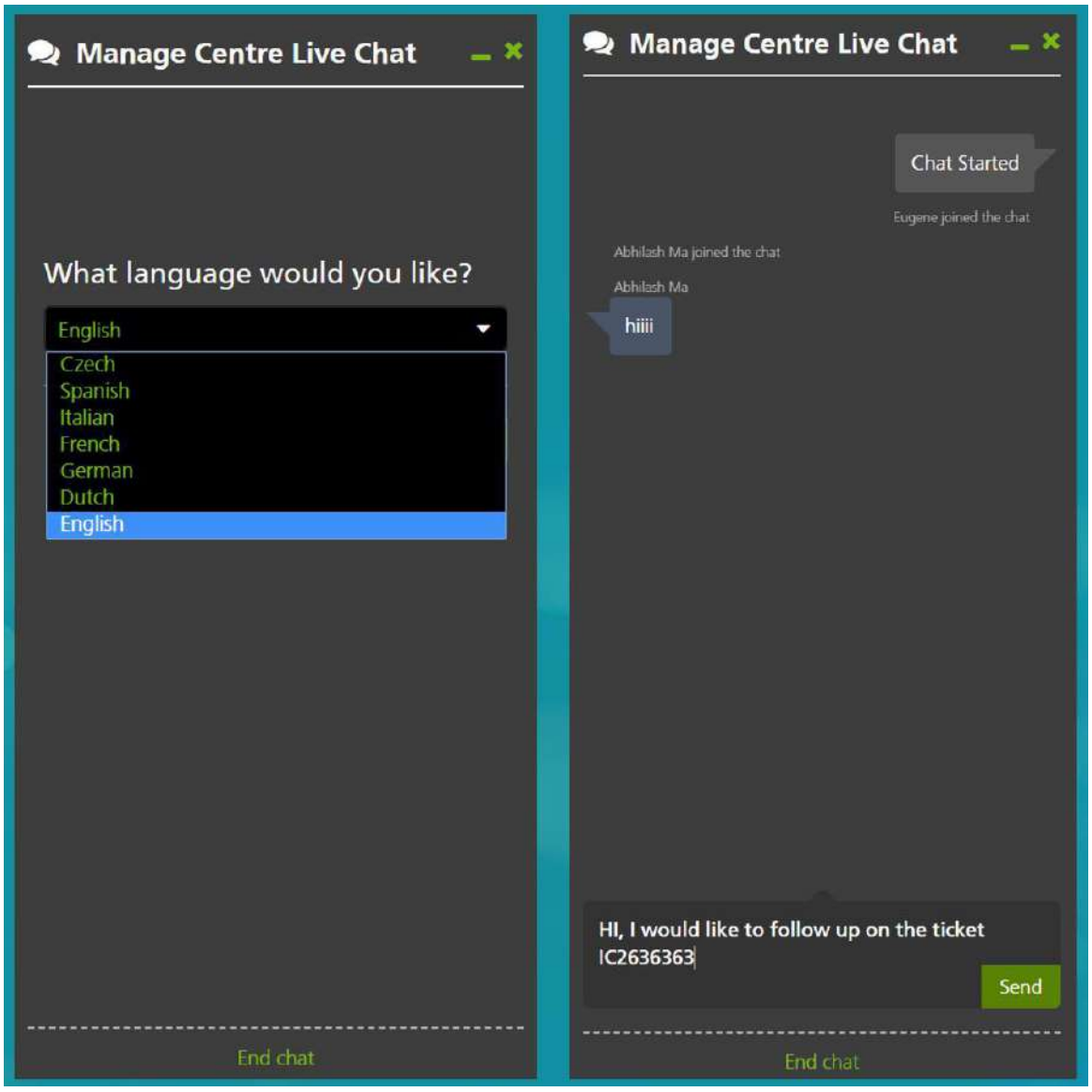

Figure 23 Manage Centre Live Chat

3.7. Availability and capacity reports

See availability reporting section 2.5.2.2 and capacity reporting section 2.5.3.2 for details on these reports.

4. Transition

NTT's service transition process follows our project management methodology Primer and uses Transition Implementation Methodology (TIM). Dependent on the actual Uptime service features procured, this takes the form of a formalized project where a project manager or transition manager is involved to manage the process. The methodology consists of the following standard phases:

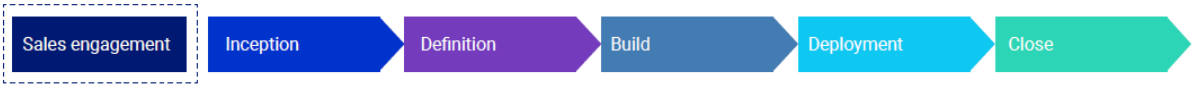

Figure 24 Transition Implementation Methodology phases

4.1. Sale engagement

During the sales engagement phase, we identify the client's business needs and objectives and propose an appropriate high-level service.

4.2. Service inception

During the inception phase, we assign NTT resources and initiate a kick - off meeting with the client to:

- discuss high-level scope, schedule, and processes of the procured Uptime service features
- provide required templates to the client for completion
- provide any relevant technical documentation

4.3. Service definition

During the definition phase, NTT commences the contract administration tasks as outlined in section 5 and in addition may:

- provide and discuss a detailed schedule and process of the procured Uptime service features
- provide a detailed project statement of work (SOW) for any required activities during the subsequent phases

4.4. Service build

During the build phase, NTT sets up the procured Uptime service features inclusive of, but not limited to:

- remote connectivity for incident and service request diagnosis
- availability monitoring technical set-up as described in detail under section 2.5.2.1

- Manage Centre portal including asset tracking interface (if procured)

4.5. Service deployment

During the deployment phase, Operations Readiness Test (ORT) is conducted to verify accurate working of system. Upon successful completion of ORT, service handover to our operations teams is done. Specific client training is conducted, and the technical set-up of the procured Uptime service features is moved to the NTT service management systems.

4.6. Closure

The transition phase marks the end of the transition process as we move into the standard Uptime service delivery processes. The transition project is officially closed off.

4.7. Secure remote connection to the client's site

Experience has shown that the ability to connect remotely to assets and systems has greatly reduced the time taken to analyse and diagnose incidents. As part of Uptime, NTT connects to your IT environment through an encrypted VPN, typically over the internet.

A professional security team in our Global Delivery Centers handles the management of our security systems, thereby protecting both our network and the client's network from any security breaches. A document detailing the security controls in place is available for your review.

5. Contract lifecycle management

Contract lifecycle management is the aspect of Uptime concerned with the management of client's Uptime contract and information relating to the associated configuration items.

Contract lifecycle management comprises of two phases:

- **Service deployment** – The initial set-up and configuration of the contract items and their components in NTT's management systems.
- **Service maintenance** – Timely update and amendment of the contract components.

The following tasks are performed as part of contract lifecycle management:

- configuration item recording
- re-distribution of welcome and renewal packs
- contract billing
- contract renewal

5.1. Configuration item recording

NTT records the details of all configuration items under support (for example, serial number and physical location) to enable and assist in the provision of Uptime.

NTT provides the client with a list of all required configuration item information. Examples of the data requested are:

- manufacturer
- product code
- serial number
- physical location (address)

5.2. Distribution of welcome and renewal packs

NTT provides the client with a welcome pack once the initial Uptime contract has been signed. Renewal packs are provided whenever subsequent contract renewals are signed.

Both packs contain the following information:

- the master services agreement (if applicable) and service level commitments
- a list of the configuration items and their associated service levels supported by Uptime

- procedure and contact details associated with logging incidents and service requests with our Global Delivery Centers
- an escalation and communication matrix for incidents and service requests logged with our Global Delivery Centers
- the name and contact details of the NTT service level management contact (where service level management is procured)
- the Uptime client service description and relevant addenda
- a service unit matrix defining the number of service units utilized for MACD and Consultant on Call engagements (where MACDs and / or Consultant on Call is procured)
- other financial considerations related to the management of MACDs and service units

5.3. Contract billing

Contract billing covers the management of the invoicing process and ensures that charges associated with Uptime are processed accurately and on time. This includes credits, invoices, additions, and subtractions of configuration items under support.

Billing is provided in line with deliverables defined in the Uptime contract. This relates to payment for Uptime, time and material charges, project charges or penalties/rewards, where negotiated and applicable.

5.4. Contract renewal

Contract renewal includes, but is not limited to:

- maintaining the contract details in NTT's management system
- initiating the contract renewal process 90 days prior to the contract anniversary date
- conducting a contract renewal meeting with the client to reach an agreement on any changes to the contract configuration item details
- activating the renewed contract in our management system and making it available for viewing on the Services Portal

5.5. Changes to client/escalation contacts

NTT updates your escalation contact details in the NTT management system within two business days of receipt of a request.

The client is requested to advise NTT of changes to any of the nominated escalation contacts within 48 hours of the alteration via the Manage Centre portal.

Appendix A Network services optimization assessment

In order to provide your organization with the best-fit support service of NTT, we offer a Network Service Optimization Assessment. The Network Service Optimization Assessment is a rapid assessment service that helps you find ways to improve service performance while optimizing spend. The assessment identifies areas of operational concern, and indicates the gap between your operating environment today, and where you need it to be in the future. The assessment helps in the following ways:

- understanding key market trends and why they're important to you
- interpret key IT operations efficiency statistics about how your network/support functions are performing
- plot your current level of service management maturity against the four key processes:
  - incident management
  - problem management
  - change management
  - service asset and configuration management
- define the possible return on investment by:
  - reusing the headcount required to manage your network
  - improving the mean-time-to-repair, which reduces downtime and improves organizational perception of IT
  - improving your overall network availability and reliability
  - reducing the total cost of ownership of your network while improving service
- strengthen business and IT alignment

The Network Service Optimization Assessment is an additional service priced separately.

Appendix B Service option dependency map

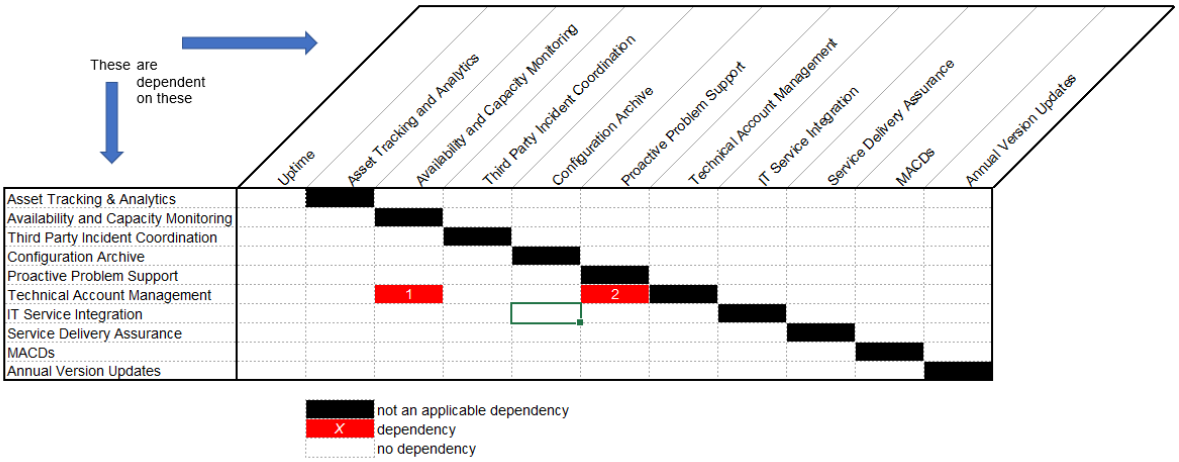

Figure 25 Service option dependency map

Appendix C Predefined list of standard MACDs

- Network Standard MACD's
- Collaboration Standard MACD's
- F5 MACD's
- Blue Coat MACD's
- Aruba MACD's
- Check Point MACD's
- Juniper Security MACD's
- NetApp MACD's
- Riverbed MACD's
- Meraki Wireless MACD's
- Avaya MACD's
- Palo Alto MACD's
- Cisco Wireless MACD
- WebEx

Network Standard MACD's

MACD Type	MACD Description. 1 SU=15 Min	Service Units
Administration	SNMP server ip address change	1
	SNMP community change.	1
	logging server ip change	1
	logging size change	1
	Interface or managed object description	1
	Welcome or Login Banner	1
	Clock time zone	1
	AAA	1
	Turn on or Off CDP	1
	Add/Delete/Modify DHCP ip helper	1
	Change interface speed and duplex	1
	Add or change VLAN on access switch port	1
Access List	Existing ACL add port single port (Moderate)	1
	Existing ACL add new line for Single Network or users/host or Port	1
Bandwidth Shaping and Queuing	Install license files (additive only) (define)	1
	Any single change to bandwidth shaping rules	2

	Bandwidth upgrade or downgrade that does not require any physical change to the terminating equipment	1
	Any single change to queuing or traffic prioritization	2
Routing	Addition or modification of a secondary TCP/IP subnet on a network device	1
	Add/Delete/Change - Static route	2
	Add/Delete/Change - IGRP	3
	Add/Delete/Change - BGP	3
	Enable new interface/sub-interface and assign IP address	1

Collaboration Standard MACD's

MACD type	MACD Description <1 SU= 15 Min>	Service Unit
		1
	Voice extension creation, modification or removal	1
	Voice pickup creation, modification or removal	1
	hunt group creation, modification or removal	1
	Voicemail account creation, modification or removal	1
	Password reset	1
	ARC Operator Console user account creation, modification or removal	2
	Permission or access level change	1
	Music on Hold Change	1
	Phone Background Image Change	1
	Exp Module Speed Dial Change	1
	Phone Idle Display change	1
	Phone Ringtone Change	1
Voice Endpoint	IP Phone (including CIPC/Jabber/Android and CSF based devices)	1
	Analog VG Endpoint	1

	FXS based device	1
	ATA 186/187/188	1
Routing	Addition or modification to a voice route for an IP telephony application	1
	Change Schedule on Unity CNX	2
	Change Schedule on ARC	2
	Change Unity CNX Call Handler	2

F5 MACD's

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
Load Balancing	Server Addition to Server farm	1
	Server Deletion from Server farm	1
	Server disabling from Server farm	1
	VIP change on Load Balancer	1
	Port add/delete/change on Server of Server farm	1
	VIP creation	3
	Change cipher suite on SSL profile	2
	Monitor configuration	2
	Create SSL profile	2
User Management	Add user account	2
Administration	HTTPD/tomcat service restart	1
	Restrict SSL/TLS version for GUI access	2
Access List	Layer 4 ACL creation	2
	Layer 7 ACL creation	2

	Layer 4+7 ACL creation	2
	ACL modification	2
	Change ACL/ACE order	1
DNS	WIP modification	2
	Member addition to existing pool	2
	Member deletion from existing pool	2
	Member disabling from WIP pool	2
VPN	Lease pool configuration for SSL VPN	2
Security	Profile (HTTP) modification	3
	Remote desktop resource item modification	2
	App tunnel modification	3
	Enable/Disable Attack Signature	2
	Disable policy on virtual server	1

Note: Client should have the valid certificate available for Certification Renewal.

Blue Coat MACD's

MACD Type	MACD Description <1 SU=15 Min>	Service Units
Administration	Modification SSL cipher suites for proxy GUI access	1
	Configure/Change Login password	1
	Creating Local Group/User accounts	2
	Configure Email alert for system issue	1
DNS	Configure/Modify DNS setting	1
Proxy	Rule addition in Virtual policy Manager (VPM)	2
	Rule Deletion in VPM	2
	Modify the VPM policy	1
	Downloading new BCWF database	1
	Create/Modify proxy services	2
	Providing Read/Write access	2
Bandwidth Shaping & Queuing	Enable/Disable traffic discovery	1
	Create top 10 category graph	1

Aruba MACD's

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
Administration	Managing AP Whitelists	1
	Whitelist DB Optimization	1
	Configure VLANs	1
	Assign an IP Address to a VLAN	1
	Enabling IPv6	1
	Configure Authentication Servers	1
	Configure Server Groups	1
User Management	Configure MAC-Based Authentication	1
	Configure Clients	1
	Configure 802.1X Authentication	1
	Enable 802.1X Supplicant Support on an AP	1
	Configure Stateful 802.1X Authentication	1
	Configure Captive Portal	1
Load Balancing	Cluster Load Balancing	1
Security	Configure Firewall Policies	2
Administration	Configure User Roles	2
	Assign User Roles	2

Profile Management	Configure the Virtual AP Profile	1
	Configure SSID Profiles	1
	Configure ARM Profile	2
	Detect Rogue APs	1
	Configure Client Blacklisting	1
Access Point Management	Naming and Grouping APs	1
	Enable DHCP to Provide APs with IP Addresses	1
	Configure Installed APs	2
	Configuring AP Image Preload	1
	2.4 GHz and 5 GHz Radio RF Management	2
	High-Throughput APs	1
	Managing AP Console Settings	1
	Configure Mesh Cluster Profiles	1
	Creating and Editing Mesh High-Throughput SSID Profiles	1
	Configure Mobility Domains	1
	Configure Split Tunnelling	1
	Configure Bridge	1
	Configure Uplink Bandwidth	1
	Provision 4G USB Modems on Remote Access Points	2

	Convert an Instant AP to Remote AP or Campus AP	2
	Enable Bandwidth Contract Support for Remote APs	1
Logging & Monitoring	Configure SNMP	1
	Enable Capacity Alerts	1
	Configure Logging	1
	Enable Guest Provisioning	1
	Setting System Clock	1
	Configure Guest VLANs	1
VPN	Configure VPN for L2TP/IPsec with IKEv2	2
	Configure Remote Access VPNs for XAuth	2
Routing	Configure Static IP Routes	1

Check Point MACD's

MACD type	MACD Description <1 SU= 15 Min>	Service Units
Administration	Interface addition	1
	Backup	1
	change interface IP	1
Routing	change static route	1
	Changes in dynamic route	1
	Add static route	1
	add dynamic route	1
Security	add nat rule	1
	Create an Object	1
	add basic policy (L3/L4)	1
	add IPS policy	1
	add Application /URL filtering layer policy	1
	add firewall zone	1
	change in nat rule	1
	delete policy	1
	delete nat rule	1
	Create HTTPS inspection	2

	Generate CSR	2
	Renew certificate	3
	Bind certificate	1
VPN	Changes in IPSEC VPN	3
	changes in Remote access VPN	3
DNS	Firewall DNS change	1

Juniper Security MACD's

MACD type	MACD Description <1 SU= 15 Min>	Service Units
Administration	configure a new cluster	2
	integrating firewall with external server (syslog/snmp)	2
	Configure a new Interface	1
	configuring new firewall authentication user	1
	integrating firewall with external authentication server	2
	change an ip on interface	1
Routing	configure routing	2
	edit in routing	1
Security	Create a Zone	1
	configure new policy based forwarding rule	1
	configure a new Security policy	2
	configure a nat rule	2
	change a zone	1
	edit the policy based forwarding	1
	edit the security policy	1
	edit the nat rule	1
	generate a new certificate	1

	renew a certificate	1
	new ssl inspection policy	2
	edit ssl inspection policy	1
VPN	changes in existing site to site vpn	2
	changes in remote access vpn	2
	configure new site to site vpn	2
	configure new remote access vpn	2

NetApp MACD's

MACD Type	MACD Description	Service Units
Administration	Assigning ownership for un-owned disks and array LUNs	1
	Removing ownership of a disk from one node and assigning it to the partner node	1
	Zeroing a disk	1
	Modifying a LIF	1
	Copy a volume	1
	Unlock a user account with password auth method	1
	Set the system time zone	1
	Storage system configuration back up	1
	Setting system date and time	1
	Synchronizing system time	1
	Relocating aggregate ownership within an HA pair	2
	Performing a manual takeover	1
	Performing a manual giveback	1
	Updating disk shelf firmware manually	1
	Updating disk firmware manually	1
	Nondisruptive Operations for NetApp ONTAP 9.0 upgrade	2

	Create a CIFS server on a Vserver	2
	Create a CIFS share	1
	Create export policy	1
	Create export policy rule	1
	Add one or more license keys	1
	Modify a password for a user	1
	Modify a CIFS server	1
	Delete a CIFS server	1
	Delete a CIFS share	1
	Delete export policy	1
	Delete export policy rule	1
	Delete a license from the storage system	1

Meraki Wireless MACD's

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
Administration	Configure VLANs	1
	Assign an IP Address to a VLAN	1
	Configure the Loopback IP Address	1
	Configure LACP / LAG	1
	Configure Authentication Servers	2
User Management	Configure MAC-Based Access Control	2
	Configure Clients	1
	Configure 802.1X Authentication	2
	Configure Captive Portal / Splash Page	2
Profile Management	Configure SSID Profiles	2
	Configure ARM Profile	2
	Detect Rogue APs	2
	Configure Client Blacklisting	2
Access Point Management	Naming / Tagging APs	2
	Enable DHCP to Provide APs with IP Addresses	2
	Configure Installed APs	2
	Configure AP Image Preload	2

	2.4 GHz and 5 GHz Radio RF Management	2
	Configure Mesh Profiles	2
	Creating and Editing Mesh High-Throughput Profiles	2
	Configure Bandwidth Limitation	2
Logging & Monitoring	Configure SNMP	1
	Configure Logging	1
	Setting System Clock	1

Avaya MACD's

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
Administration	Coverage Path creation	2
Administration	Hunt Creation - PABX	2
Administration	International Privilege assignment	1
Administration	Send all calls feature alignment	1
Administration	Button Assignment (Pick-Up Group)	2
Administration	Station Name Change	1
Administration	Station License Count	1
Logging & Monitoring	System Health Checkup	4
Administration	Call Barging feature enablement	2
Administration	ACD feature request on station	1
Administration	Station Deletion	1
Administration	Call forwarding enablement	2
Administration	EC500 feature enablement	2

Administration	Announcement upload request	3
Administration	CM Back-up Request	3
Administration	Registration of IP phone Request	2
Administration	Agent Id creation/deletion - PABX	2
Administration	Skill alignment to agent request	2
Administration	Agent Name change request	1
Administration	Agent deletion Request	1
Administration	Agent id Password Reset request	1
Administration	Console permission on station/H.323/SIP (for announcement record)	2
Administration	Station Password Change	1
Administration	Call flow change	2
Administration	Voice Mail password Reset	1
Administration	Voice Mail Name change request	1
Administration	Voice Mail space request	2

Administration	Voice Mail reassignment request	2
Administration	Voice Mail Password unlock request	1
Logging & Monitoring	Voice Mail Health check request	3
Logging & Monitoring	Gateway Health check up	3
Voice Endpoint	Avaya one-x installation request	3
Administration	Avaya One-x configuration request	3
Voice Endpoint	SIP Station creation	3
Administration	SIP station password reset	2
Administration	SIP station Name change request	2
Voice Endpoint	H.323 Station creation	2
Administration	H.323 station password reset	1
Administration	H.323 station Name change request	1
Administration	Name change in IP office	2
Administration	Password change in IP office	2

Administration	Voice Mail Name change request	1
Logging & Monitoring	IP Office health checkup request	2
Voice Endpoint	New station creation in IP Office	2
Administration	New Voice Mail creation in IP Office	2
Logging & Monitoring	Health checkup of System Manager	2
Administration	ID Creation for SMGR login	3
Logging & Monitoring	Health checkup of Session Manager	3
Administration	Id Creation for SBC login	3
Logging & Monitoring	Health check-up of SBC	3
Logging & Monitoring	MPP status monitor	2
Logging & Monitoring	Port monitoring request (h.323/SIP)	3
Logging & Monitoring	Health check-up - AIC	4
Administration	Agent ID creation	3
Administration	Agent id deletion	2
Administration	Agent group assignment	2

Administration	CMS ID Creation	2
Administration	CMS Supervisor id Creation	2
Logging & Monitoring	CMS Skill report monitoring	2
Logging & Monitoring	CMS Agent report monitoring	2
Logging & Monitoring	CMS health check	3
Logging & Monitoring	BCMS health check UP	2
Administration	Skill alignment for particular group	2
Administration	Agent deletion	2
Logging & Monitoring	AACC health check up	4
Logging & Monitoring	AMS server health check up	2
Logging & Monitoring	Health Checkup Call center Elite	4
Logging & Monitoring	Health Check-up of ACM	4
Logging & Monitoring	AES Health Check UP	3
Administration	Station addition in AES	2
Logging & Monitoring	Services Monitoring in AES	2

Administration	Agent id creation	1
Logging & Monitoring	Health Checkup of ACR	3
Profile Management	Skill permission to supervisor	3
Logging & Monitoring	Gateway Health check up	3
Administration	ACR login ID creation	2
Administration	DECT addition	1
Administration	DECT Changes	1

The below Tasks should be considered as RFI.

Task Description
CM version request along with Patch
CM UP time request
Voice Mail up time request
Gateway Up time request
Gateway configuration details request
Avaya One-x not login
Voice Mail password request
IP Office Up time request

SMGR Back up request
SIP link Monitoring
Up time report verification
SBC back up Request
AAEP Back up request
AIC back up request
Agent id creation
CMS back up request (Admin\Maintenance)
CMS uptime report request
Agent addition
AACC Back-up Request
Agent Report in real time
AACC services status
Software version verification
Up time report verification
Disk space monitoring
AES back-up task
Gateway Up time request

Palo Alto MACD's

MACD type	MACD Description <1 SU= 15 Min>	Service Units
Administration	Configure firewall interface	1
	New integration of External authentication server	2
	configure firewall into Cluster	2
	Integrate firewall with Panorama	2
	Install dynamic updates (URL/antivirus/threat)- does not require reboot	2
	Create new qos rule	2
	Changes in firewall interface	1
Routing	change in static route	2
	changes in dynamic routing	1
	configure static route	2
	configure dynamic routing	2
Security	create new nat rule	1
	create new zone	1
	create new ssl inspection profile	2
	generate new certificate	2
	create layer3/layer4 policy	2

	create inspection policy (till layer 7, including url filtering, antivirus)	2
	changes in nat Rule	1
	changes in ssl inspection	2
VPN	changes in site to site vpn	2
	create site to site VPN	2
	create remote access vpn	2
	changes in remote access vpn	2

Cisco Wireless MACDs

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
Administration	Managing AP Whitelists	1
	Configure VLANs	1
	Assign an IP Address to a VLAN	1
	Enable IPv6	1
	Configure LACP	1
	Configure Authentication Servers	2
	Configure Server Groups	2
	Installing AP license & Usage report	2
User Management	Configure MAC-Based Authentication	2
	Configure Clients	1
	Configure 802.1X Authentication	2
	Enabling 802.1X Supplicant Support on an AP	2
	Configure Captive Portal	2
Load Balancing	AP Load Balancing (Primary/Secondary/HA)	2
	User Load Balancing	2
Profile Management	Configure SSID Profiles	2
	Configure ARM Profile	2

	Detecting Rogue APs	2
	Configure Client Blacklisting	2
Access Point Management	Naming and Grouping APs	2
	Configure Installed APs	2
	Configure AP Image Preload	2
	2.4 GHz and 5 GHz Radio RF Management	2
	High-Throughput APs	2
	Configure Mesh Profiles	2
	Creating and Editing Mesh High-Throughput	2
	Configure Mobility Domains	2
	Configure FlexConnect	2
	Configure Bridge	2
	Configure Uplink Bandwidth	2
	Convert an Instant AP to Remote AP or Campus AP	2
Logging & Monitoring	Configure SNMP	1
	Configure Logging	1
	Guest Provisioning	1
	Setting System Clock	1
	Configure Guest VLANs	1

WebEx

WebEx Calling

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
User Management	Add user in Webex control Hub (if no SSO)	1
	Add Webex Calling feature to user (Assign Webex Calling Right + Assigne Extension and DID)	1
	Modify user in Webex control Hub (if no SSO)	1
	Modify Webex Calling feature to user (Change Extension and/or DID)	1
	Delete user in Webex control Hub (if no SSO)	1
	Delete Webex Calling feature to user	1
	Add MPP Phone	1
	Modify MPP Phone	1
	Delete MPP Phone	1
Administration	Add new Hunt Group	2
	Add new Call Queue	2
	Add new Auto Attendant	2
	Add Call Pickup Group	1
	Add Call Park Group	1

	Add Paging Group	1
	Modify Hunt Group	2
	Modify Call Queue	2
	Modify Auto Attendant	2
	Modify Call Pickup Group	1
	Modify Call Park Group	1
	Modify Paging Group	1
	Delete Hunt Group	2
	Delete Call Queue	2
	Delete Auto Attendant	2
	Delete Call Pickup Group	1
	Delete Call Park Group	1
	Delete Paging Group	1

WebEx Meeting

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
User Management	Add user in Webex control Hub (if no SSO) and assign Webex Meeting feature	1
	Modify Webex site for a user	1
	Delete user in Webex control Hub (if no SSO)	1
	Modify user in Webex control Hub (if no SSO)	1
	Modify user role (user->admin, or admin-> user)	1
	Add new Video Endpoints	1
	Delete Video endpoint	1
	Modify Video endpoint name or place	1
Administration	Add new Webex site URL	1
	Delete Webex site url	1
	Customize Default Meeting invite template	3
	Customize Webex site - branding (logo-banners)	3

	Modify/Force beta or stable firmware release for a Video endpoint	1

WebEx Teams

MACD Type	MACD Description <1 SU = 15 Min>	Service Units
User Management	Add user in Webex control Hub (if no SSO) and assign Webex Teams feature	1
	Add Hybrid Services feature to a user (Calendar, Call or Messaging Services)	1
	Modify user in Webex control Hub (if no SSO)	1

	Modify user role (user->admin, or admin-> user)	1
	Modify Hybrid Services features	1
	Delete user in Webex control Hub (if no SSO) or unassign Webex Teams feature	1