Client service description

Uptime Service Plans

28 October 2019 | Document Version 9.05

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shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.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 out-dated 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.

top EMPLOYER GLOBAL 2019
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

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.

We will support you in improving availability and performance and enable you to offload some of your operational tasks while you remain in full management control.

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
- multi-vendor 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.

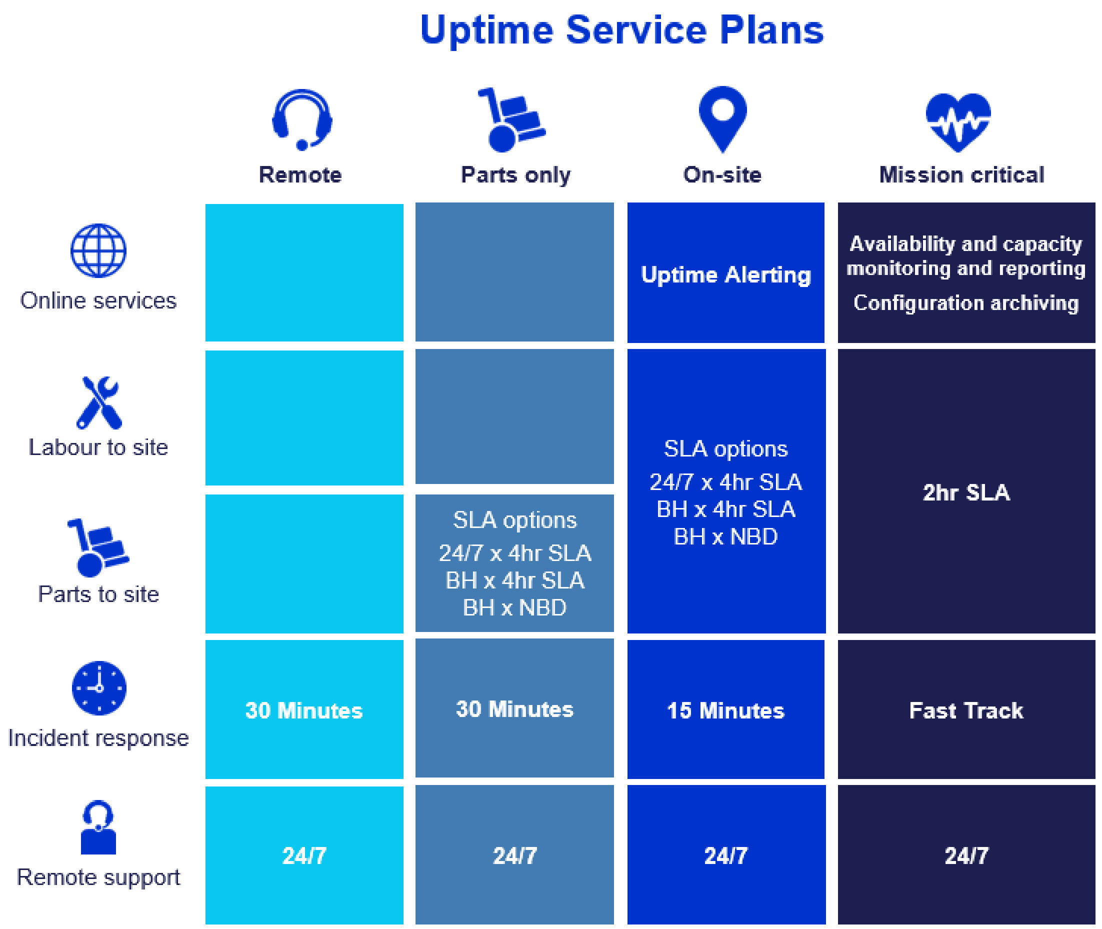
Uptime Service Plans

- 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 2 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.



Uptime Service Plans

	Remote	Parts only	On-site	Mission critical
Online services			Uptime Alerting	Availability and capacity monitoring and reporting Configuration archiving
Labour to site			SLA options 24/7 x 4hr SLA BH x 4hr SLA BH x NBD	2hr SLA
Parts to site		SLA options 24/7 x 4hr SLA BH x 4hr SLA BH x NBD		
Incident response	30 Minutes	30 Minutes	15 Minutes	Fast Track
Remote support	24/7	24/7	24/7	24/7

Figure 1 Uptime Service Plans

1. Mission Critical and on-site Plans can be applied to hardware and software
2. On-site parts and labour SLAs apply only when required to restore service
3. Where 2-hour response times are not available in remote geographies, response time will be 4 hours

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 24/7 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 pre-defined 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]

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.

[1] Please see Appendix F for a graphical representation of service levels in the incident process.

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).

1.6. 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.

Refer to Appendix B for a comprehensive list of supported tier one products and Appendix C for tier two products.

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:

- 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 the United Kingdom in English
- Global Delivery Center Prague supports 16 countries in Europe and seven European languages including: Czech, Dutch, English, French, German, Italian and Spanish

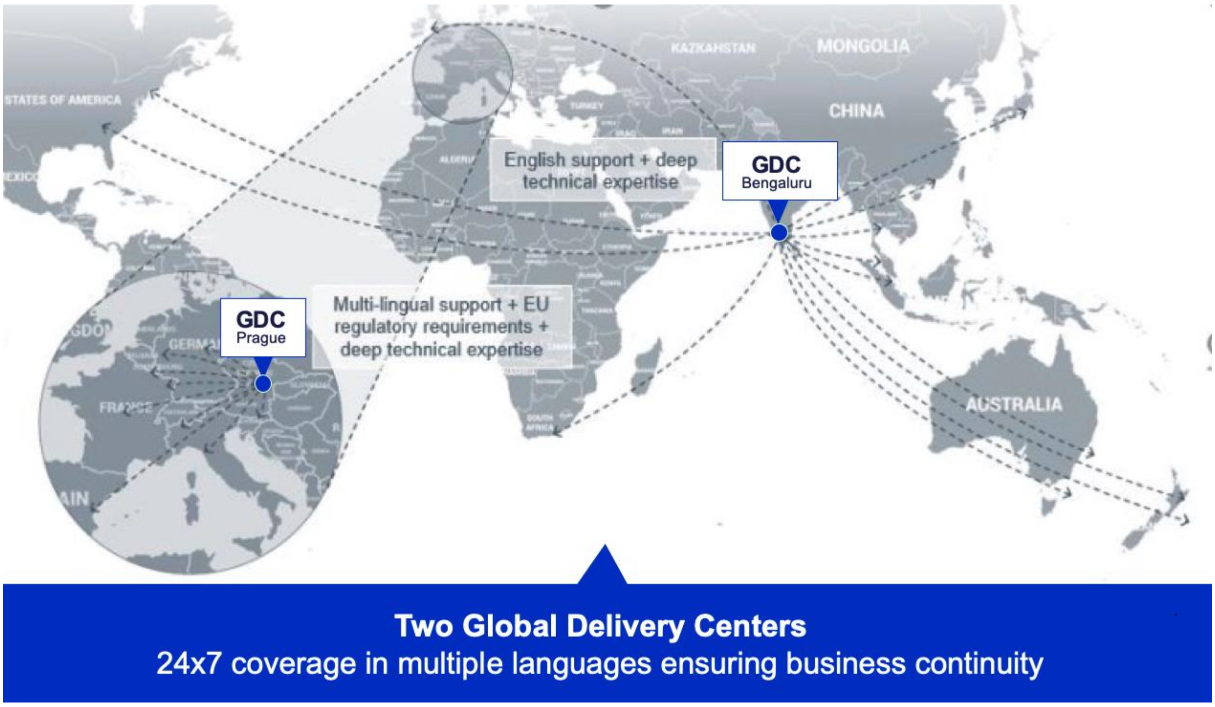

KAZAKHSTAN
MONGOLIA
STATES OF AMERICA
CHINA
MEXICO
English support + deep technical expertise
GDC
Bengaluru
GDC
Prague
Multi-lingual support + EU regulatory requirements + deep technical expertise
GERMANY
FRANCE
SPAIN
AUSTRALIA
Two Global Delivery Centers
24x7 coverage in multiple languages ensuring business continuity

Figure 2 Delivery model

Refer to Appendix D for a list of countries in which we have a direct presence and Appendix E for a list of countries where our reach is extended through our Preferred Partner Programme.

2. Uptime service features

2.1. Remote support

Only about 14% of the total service incidents turn out to be hardware failures (source: NTT 2016 Network Barometer). This implies that up to 86% of all incidents can be diagnosed and resolved remotely. Resolving incidents remotely is important to your organization because it not only reduces the resolution time significantly but also helps to keep prices low by avoiding unnecessary dispatches.

2.1.1 Description

When a service incident is opened for your organization, it is routed to an engineer skilled in the related technology who then connects to your IT environment and begins diagnosis. If the asset is software-only, then the engineer works continuously on a remote basis to resolve the incident.

If the asset is hardware, with or without an embedded software component, then the engineer first determines whether there is a hardware problem or not and completes this level of fault isolation in sufficient time to ensure that your contracted on-site service level commitment is met (if the same has been procured). If it is determined that the incident is not a hardware problem, then the engineer continues to work remotely to resolve the incident.

2.1.2 RACI model

In the summary of responsibilities table throughout this document, the responsible, accountable, consulted, and informed (RACI) model is used. The RACI model describes the participation by various roles in completing tasks or deliverables. RACI is an acronym for each of the four roles as follows:

2.1.3 Summary of responsibilities

Activity	NTT	Client
Provide remote diagnostic connectivity.	C	RA
Diagnose fault domain (hardware or software).	RA	C
Collect physical indicators (lights, etc.).	A	R
Update service incident and status.	RA	C

Table 2 Remote support summary of responsibilities

2.2. Incident response

When incidents are reported to us or detected by monitoring systems, we will respond and attempt to resolve the incident remotely. If the incident can't be resolved remotely, we will dispatch replacement parts, and/or an engineer to your site for resolution within the service level commitment.

2.2.1 Response commitment

Our commitment to assign a qualified engineer to your incident varies as per your service plan. Refer below figure for response time details of the four service plans.

Service plan	Remote	Parts only	On-site	Mission critical
Response	30 mins	30 mins	15 mins	Fast track

Figure 3 Service plan versus response time

With our Remote and Parts only service plans a qualified engineer is assigned and begins work within 30 minutes. The on-site service plan commitment is 15 minutes.

For the mission critical service plan, we also route (fast track) the call directly to senior engineers in order to improve mean-time-to-repair.2 This is applicable to clients who are connected to NTT.

Please see Appendix F for a graphical representation of service levels in the incident process.

2.2.2 Incident and service request workflow

The Global Delivery Center is responsible for the incident management process. The figure below gives an overview of the incident handling process.

To fast track a call **you are required to call** the NTT Support Center to help in achieving the 5 minutes response commitment

2 During service transition, we agree with your organization the prerequisites to fast track a service call under a mission critical service plan.

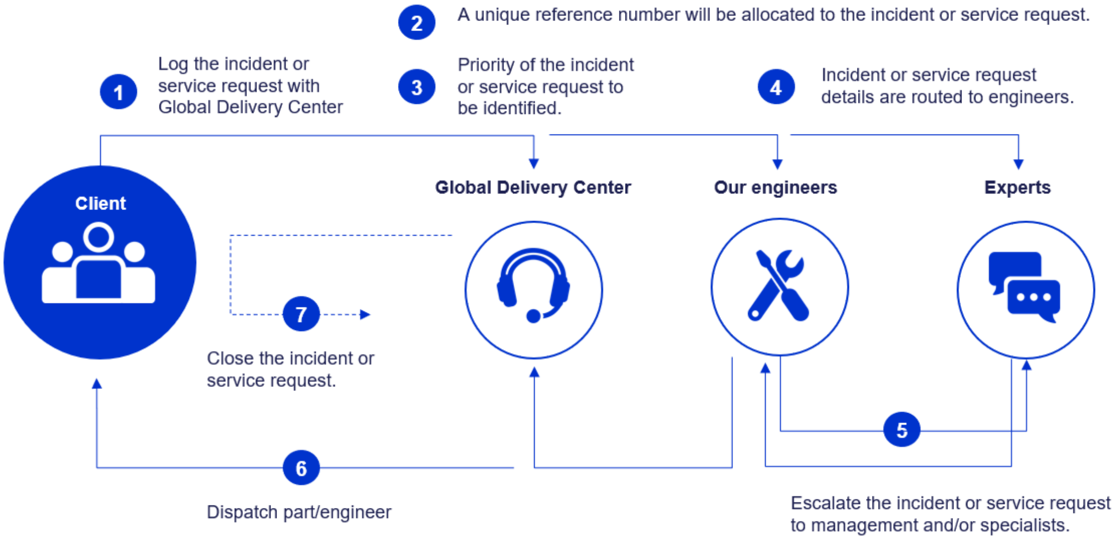

2 A unique reference number will be allocated to the incident or service request.
1 Log the incident or service request with Global Delivery Center
3 Priority of the incident or service request to be identified.
4 Incident or service request details are routed to engineers.
Client
Global Delivery Center
Our engineers
Experts
7 Close the incident or service request.
5
6 Dispatch part/engineer
Escalate the incident or service request to management and/or specialists.

Figure 4 Incident handling overview

The management process for incidents and requests is as follows:

1. Depending on the service procured, either your IT department places a call to our Global Delivery Centers, or our Global Delivery Centers detect a service-affecting failure through the deployed availability monitoring or Uptime alerting service features.
2. A unique reference number is assigned to the incident. This number is used for future tracking and follow-ups.
3. Your team is consulted to confirm the impact and urgency of the incident or service request. These values determine the initial priority of the incident.
4. If required, the details of the incident or service request are routed to NTT engineers to assist with further diagnosis.
5. If required, the service desk escalates the incident or service request to the relevant management and/or technical specialist for resolution. Escalation is managed in line with the contracted service level commitment.
6. The service desk is responsible for co-ordinating the management of the incident or service request and retains ownership of it through to resolution.
7. Incidents and service requests are closed automatically once agreement is reached that the request has been resolved and assuming that the client has provided no feedback to the contrary.

Throughout the process, NTT keeps the client updated on the status of the incident/service request.

Incidents and service requests can be logged 24 hours a day, seven days a week, regardless of the service level commitment procured. The Global Delivery Center remains the client's single point of contact for the duration of the incident or service request, regardless of whether NTT involves other parties to assist.

2.2.3 Escalation management

NTT considers the escalation management process to be critical to the effective delivery of Uptime. NTT has implemented strict escalation processes and clearly defined responsibilities for resolving escalations.

Technical escalation – Where required, NTT engineers call upon in- house and external (vendor/partner) specialists to assist in determining a course of action.

Service level escalation – A service level escalation is triggered when a service level is either at risk of breach or has already been breached and requires immediate action.

The Global Delivery Centers remain the client's first point of contact for all incident and service request related queries, even during the escalation period.

2.2.4 Access to vendor support

Certain types of failures require our engineers to escalate an incident to the vendor's support desk. NTT have agreements in place for all Uptime supported assets and are able to escalate these type of issues as and when required.

In some instances, access to these vendor support desks is extended directly to your organization. Based on NTT's contractual agreement with the vendor, we provide your team with the relevant vendor information required to access services and features offered to you through such contracts. Please note that the available services and features vary from vendor to vendor but typically include the following:

- **Access to vendor documentation** – Once registered, you'll have access to vendor document repositories and knowledge bases, where applicable. Methods of access to documentation and any required usernames or passwords var ies between the vendors.
- **Access to vendor advisory bulletins** – Certain vendors publish advisories (for known errors, workarounds, etc.) via advisory bulletins that you'll have access to, once registered with the vendor.
- **Access to vendor support tools** – Certain vendors provide diagnostics and other tools relating to their products. Once registered with the vendor, you'll have access to these tools. A limited number of vendors give the client access to a portal that allows the client to track the progress of incidents that NTT has escalated to them.
- **Access to software updates and upgrades** – If the vendor provides software subscription as part of their support packages this is provided to you as well.

Some vendors allow direct client access to the software updates and upgrades applicable to their equipment

2.2.5 Summary of responsibilities

Activity	NTT	Client
Provide the ability to log incidents and requests 24/7.	RA	C
Provide technical support and a suggested path to resolution.	RA	C
Set up and provide support through a secure connection.	RA	C
Provide you with progress updates.	RA	C
Set up an account with the vendor.	RA	C
Perform preliminary checks to validate the need for assistance before logging the incident.	C	RA
Provide the necessary information for our Global 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

Table 3 Incident response summary of responsibilities

2.3. Parts to site

Parts to site is a logistics service that provides you with replacements for faulty hardware.

2.3.1 Parts delivery

When the resolution of an incident requires a replacement part, NTT delivers the replacement part to your site in line with the service level commitment procured. NTT is responsible for any costs associated with the faulty part's return.

2.3.2 Return material authorization (RMA)

On conclusion of an incident, where replacement parts have been shipped to a location, NTT manages the faulty part return process with the applicable vendor.

2.3.3 Summary of responsibilities

Activity	NTT	Client
Deliver the replacement part to your site in line with the service level commitment.	RA	C
Collect the faulty part within a pre-arranged time frame.	RA	C
Administer the RMA process with the vendor.	RA	I
Activity	NTT	Client
Prepare any faulty part(s) for collection, within a pre-arranged time frame.	C	RA

Table 4 Parts to site summary of responsibilities

2.4. Labour to site

Labour to site provides for on-site engineering support in the resolution of an incident.

2.4.1 Engineer dispatched to client site

If an incident cannot be resolved remotely a certified engineer is sent to your site. The engineer remains on-site until the incident has been resolved or a workaround has been implemented.

NTT engineers sent to your site perform the following responsibilities:

- notify your designated contact that they've arrived to commence work
- execute on-site incident diagnostics and resolution
- replace, reconfigure, and restore the asset to pre-failure working condition
- keep your designated contacts posted with updated status throughout the resolution process
- provide regular updates to our Global Delivery Centers on the status of the incident and the resolution details
- provide governance of engineering actions while at your site

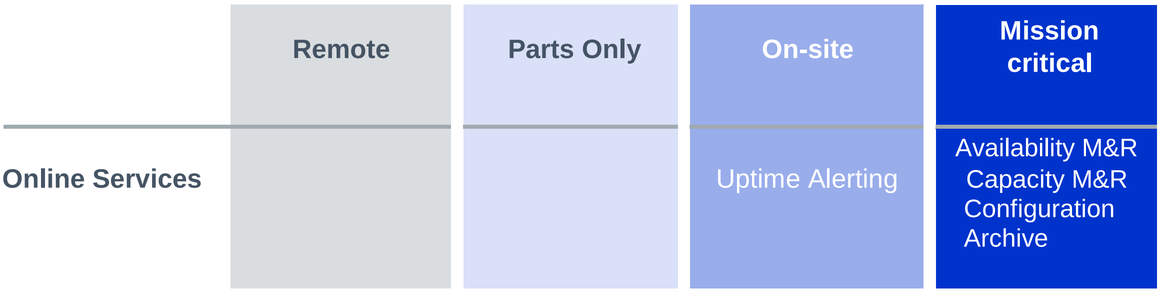
2.4.2 Summary of responsibilities

Activity	NTT	Client
Dispatch an engineer and resolve the incident in line with the contracted service level commitment	RA	C
Provide access to the site and the configuration item whenever needed to resolve an incident	C	RA
Provide updates to designated contacts within your organization	RA	C
Provide accurate information to the Global Delivery Centers or engineers	C	RA
Provide access to the relevant site and people as arranged	C	RA
Keeps an up-to-date copy of the configuration of covered assets and provides it to the engineer when requested	C	RA

Table 5 Labour to site summary of responsibilities

2.5. Online services

Included in the on-site and mission critical plans is a set of online services that are absolutely critical to achieving the highest levels of availability for your covered assets. These online services apply to the service plans as follows:



	Remote	Parts Only	On-site	Mission critical
Online Services			Uptime Alerting	Availability M&R Capacity M&R Configuration Archive

Figure 5 Online services per service plan

Please note that some service level commitments may be impacted before the deployment of the service plan relevant online services.

2.5.1 Uptime alerting

For our on-site service plan, this capability provides warnings of a failure or imminent failure of hardware components enabling us to proactively initiate incident resolution[3]. On an average, this accelerates incident response by 69% and repair time by 32% (source: NTT 2016 Network Barometer). It also saves time of your service desk team by eliminating the tasks normally required to identify the failure and submit a ticket. We use secure remote access to receive hardware failure alerts and intelligently translate that data with our remote management tools for your Cisco assets under contract.

Even if a monitoring solution is already in place in your environment, without this Uptime alerting feature, delays are still introduced through the need for your service desk to identify the events and execute the event management process, and after fault level isolation, place a call to NTT which being manual, is prone to error. The Uptime alerting feature eliminates these issues and ensures minimum response time.

Today most IT assets have the capability to send out Simple Network Management Protocol (SNMP) traps when they discover key failures within their hardware components. These traps automatically trigger the incident management process within our Global Delivery Centers. This means that service-affecting incidents are acted upon immediately to keep minimize downtime.

[3] Please note that while we are developing the ability to deliver this service on all supported vendors, today we only support this feature on Cisco.

2.5.1.1 Hardware failure alerting

The Cisco assets in your IT Infrastructure need to be Simple Network Management Protocol (SNMP) enabled to be able to send hardware failure alerts. This means that only service-affecting events trigger the incident management process.

The table below shows an overview of hardware component failures which are processed and actioned through Uptime alerting.

Component	What is measured
Chassis	chassis temperature critical chassis failure
Power supply	power supply temperature critical power supply failure power supply redundancy lost
Fan	fan failure fan redundancy lost
Central processing unit (CPU)	CPU temperature critical CPU failure
Memory	memory usage high memory failure

Table 6 Overview of hardware component failures

NTT’s systems analyse the hardware failure alert and based on the predetermined criteria, automatically log and manage an incident as per the standard Uptime incident management process.

2.5.1.2 Summary of responsibilities

Activity	NTT	Client
Establish virtual private network (VPN) connectivity between your infrastructure and NTT's remote infrastructure management (RIM) toolset	RA	C
SNMP enable assets to send alerts	C	RA
Configure NTT's Global Services Operating Architecture (GSOA) systems to collect events from your covered assets	RA	I
Tuning of events to trigger the incident management process	RA	C
Firewall and access control list configuration modifications to enable Uptime alerting	C	RA
Advise of scheduled outages	C	RA
Advise of any MACDs (Moves, Adds, Changes, Deletes)	C	RA
Action alerting events through the standard Uptime incident management process	RA	C

Table 7 Uptime alerting summary of responsibilities

2.5.2 Availability monitoring and reporting

Availability monitoring and reporting is included in the mission critical service plan and can be optionally added to any of the other service plans. For the on-site service plan, it is an upgrade to the included alerting service feature. Availability monitoring enhances NTT's ability to proactively manage service incidents across vendors and technologies based on immediate and accurate failure information.

Even if a monitoring solution is already in place in your enviro nment, without this availability monitoring feature, delays are still introduced through the need for your service desk to identify the events and execute the event management process and, after fault level isolation, place a call to NTT which being manual, is prone to error. Availability monitoring eliminates these issues and ensures minimum response time.

2.5.2.1 Availability monitoring

The entire goal of IT infrastructure is to be running and stable all the time, to provide services to your users. Availability monitoring helps us keep downtime to a minimum while reducing time to resolution when failures occur.

NTT proactively monitors the availability of your contracted assets under the mission critical service plan. Availability events (whether informational or exceptions such as a component failure) are recorded and managed, and if required (in the case of exceptions) logged and addressed as an incident (see incident response section 2.2). It is critical however, for any event that affects network IT service availability, that you be notified within 15 minutes of the ac tual detection of the failure by our monitoring systems – referred as initial notification. This notification is sent either via email or SMS.

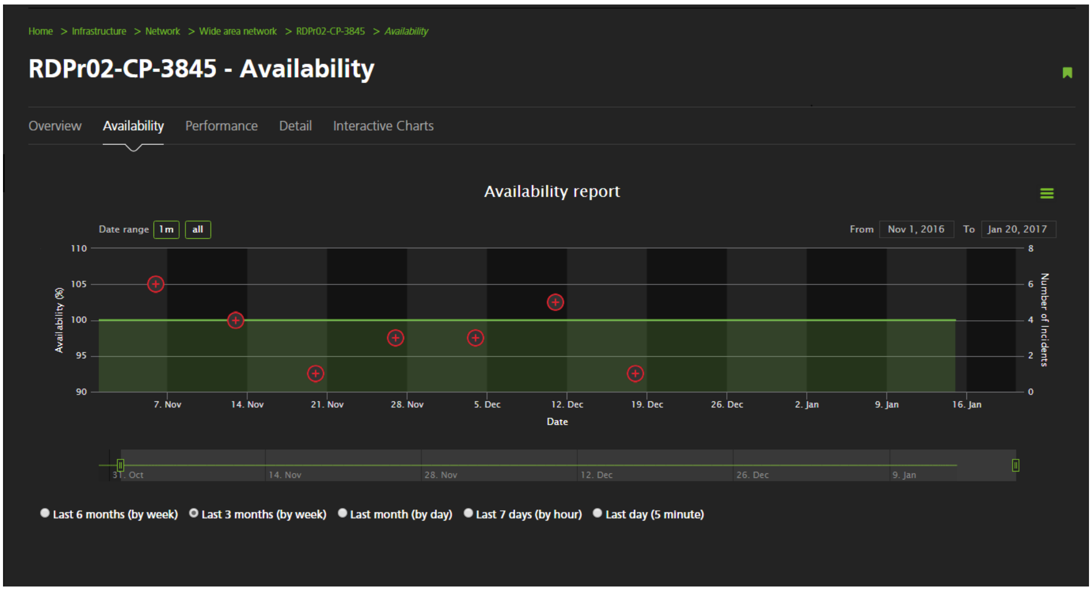
2.5.2.2 Availability reporting

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

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:



From Nov 1, 2016 To Jan 20, 2017

Figure 6 Real-time device availability

2.5.2.3 Summary of responsibilities

Activity	NTT	Client
Establish a connectivity between your infrastructure and NTT RIM toolset.	RA	C
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 Uptime alerting.	C	RA
Advise of scheduled outages.	I	RA
Advise of any MACDs.	CI	RA
Action detected events through underpinning standard Uptime incident management process.	RA	C

Table 8 Availability monitoring summary of responsibilities

2.5.3 Capacity monitoring and reporting

Capacity monitoring is a key mechanism to achieve future downtime avoidance. Capacity monitoring is included in the mission critical service plan and is an optional service that can be attached to the other service plans.

2.5.3.1 Capacity monitoring

Most organization size an environment to handle the average load it takes while also allowing capacity to briefly and occasionally spike above average levels. While you want to ensure sufficient capacity, you also need affordable capacity. You, like most organizations, want to get the most of out your investment. To do this, without impacting user experience, you need to keep an eye on key metrics that let you know how well you are utilizing your assets and be warned if you are impacting your users.

NTT proactively monitors capacity utilization of your covered assets by configuring a set of thresholds. NTT also helps assist your organization in determining the best threshold setting for each metric. Thresholds are set only to generate alert notifications after a baseline period of three months.

Capacity and performance related events (whether informational or service impacting) are recorded and, if service impacting, logged, and addressed as an incident (see incident response section 2.2).

2.5.3.2 Capacity reporting

In addition to the threshold alerting discussed in the previous section and on 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:

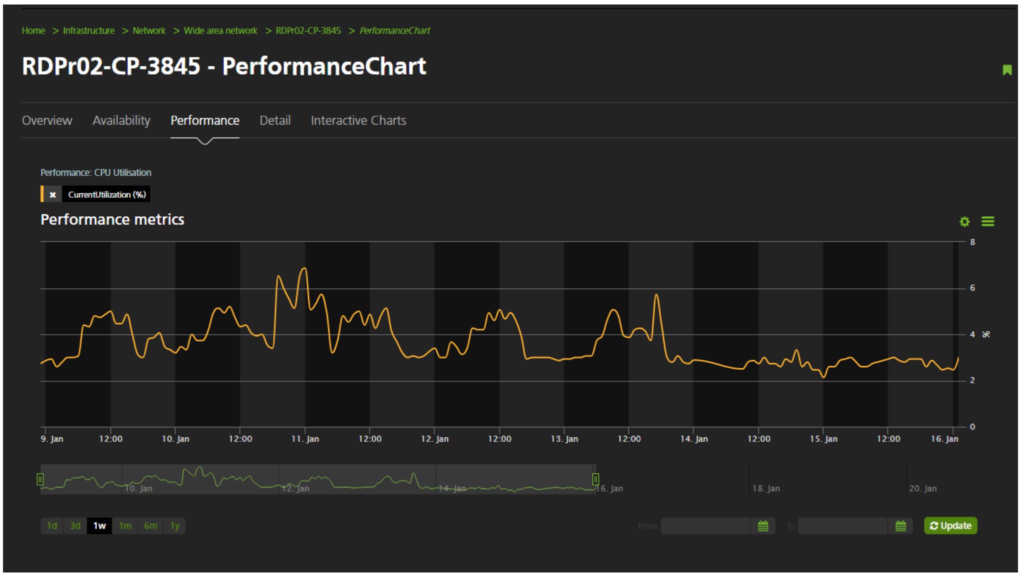
- **Interface bandwidth utilization** is a report that provides utilization information on a per interface basis allowing you to analyse things such as your telecommunications circuit bandwidth needs.
  - **configuration item**: configured name given to the asset
  - **type**: asset category such as 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.



Home > Infrastructure > Network > Wide area network > RDPr02-CP-3845 > *PerformanceChart*

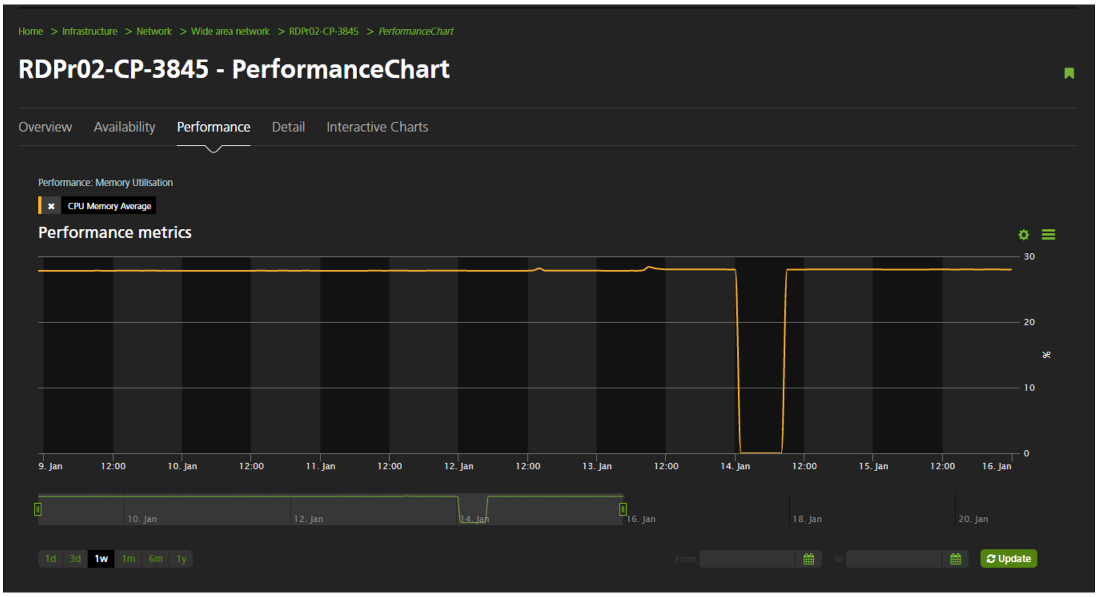
RDPr02-CP-3845 - PerformanceChart

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.



Home > Infrastructure > Network > Wide area network > RDPr02-CP-3845 > *PerformanceChart*

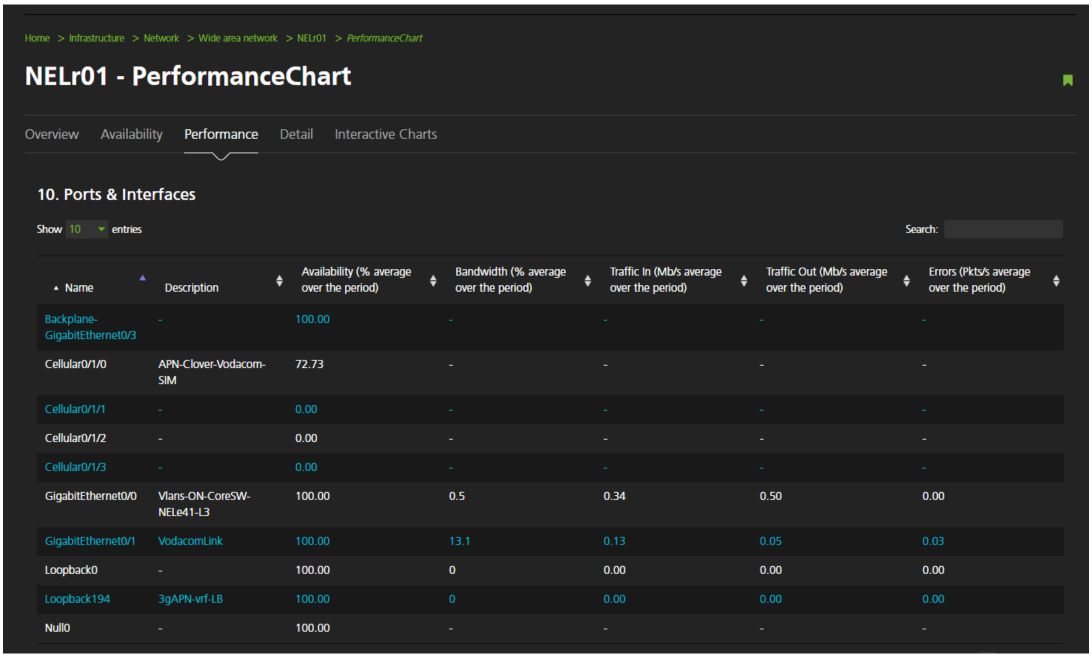
RDPr02-CP-3845 - PerformanceChart

Overview Availability Performance Detail Interactive Charts

Performance: Memory Utilisation

Performance metrics

Figure 8 Real-time memory utilization



Home > Infrastructure > Network > Wide area network > NELr01 > *PerformanceChart*

NELr01 - PerformanceChart

Overview Availability Performance Detail Interactive Charts

10. Ports & Interfaces

Show 10 entries Search:

Name	Description	Availability (% average over the period)	Bandwidth (% average over the period)	Traffic In (Mb/s average over the period)	Traffic Out (Mb/s average over the period)	Errors (Pkts/s average over the period)
Backplane-GigabitEthernet0/3	-	100.00	-	-	-	-
Cellular0/1/0	APN-Clover-Vodacom-SIM	72.73	-	-	-	-
Cellular0/1/1	-	0.00	-	-	-	-
Cellular0/1/2	-	0.00	-	-	-	-
Cellular0/1/3	-	0.00	-	-	-	-
GigabitEthernet0/0	Vlans-ON-CoreSW-NELe41-L3	100.00	0.5	0.34	0.50	0.00
GigabitEthernet0/1	VodacomLink	100.00	13.1	0.13	0.05	0.03
Loopback0	-	100.00	0	0.00	0.00	0.00
Loopback194	3gAPN-vrf-LB	100.00	0	0.00	0.00	0.00
Null0	-	100.00	-	-	-	-

Figure 9 Real-time interface bandwidth utilization

2.5.3.3 Summary of responsibilities

Activity	NTT	Client
Configure GSOA systems to monitor threshold metrics on your covered assets.	RA	I
Tuning of thresholds after the three-month baseline period to trigger the incident management process.	RA	C
Advise of scheduled outages.	I	RA
Advise of any MACDs.	CI	RA
Action threshold breaches through underpinning standard Uptime incident management process.	RA	C

Table 9 Capacity monitoring summary of responsibilities

2.5.4 Configuration archive

NTT's annual Network Barometer report puts the percentage of downtime caused by human error at almost 40% while some industry research houses have it at as much as 80%. Asset configuration is complex and error prone and impacts downtime.

When a failure is a hardware failure, the largest factor in a quick replacement is easy availability of the most recent configuration file. Without implementing automated systems and relying instead on manual backups, it often happens that the repair is effected and the configuration reloaded, but there is some small difference between the last running configuration and the backed-up configuration that ends up causing hours of research and extended downtime.

2.5.4.1 Automated archiving

To address both of these situations, NTT will configure our RIM systems to archive the configuration of each covered device able to be archived. Two situations will initiate the archiving process:

1. Receipt of a configuration change SNMP trap from the covered asset
2. On a monthly schedule

In both situations, the downloaded configuration will be compared with the most recently stored version. The following results occur:

- If the configuration has not changed, the downloaded one is discarded
- If the configuration has changed, the previous configuration file becomes "current minus 1" and the new configuration becomes the current configuration[4]

2.5.4.2 Summary of responsibilities

Item	NTT	Client
Modify firewall rules as required to allow archiving [5]	C	RA
Provide necessary device credentials to allow configuration download[6]	A	R
Configure NTT systems to collect archives per schedule	RA	I

Table 10 Configuration Archiving summary of responsibilities

[4] More than two configuration files are able to be stored upon client re quest and may attract and additional service fee.

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

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

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.

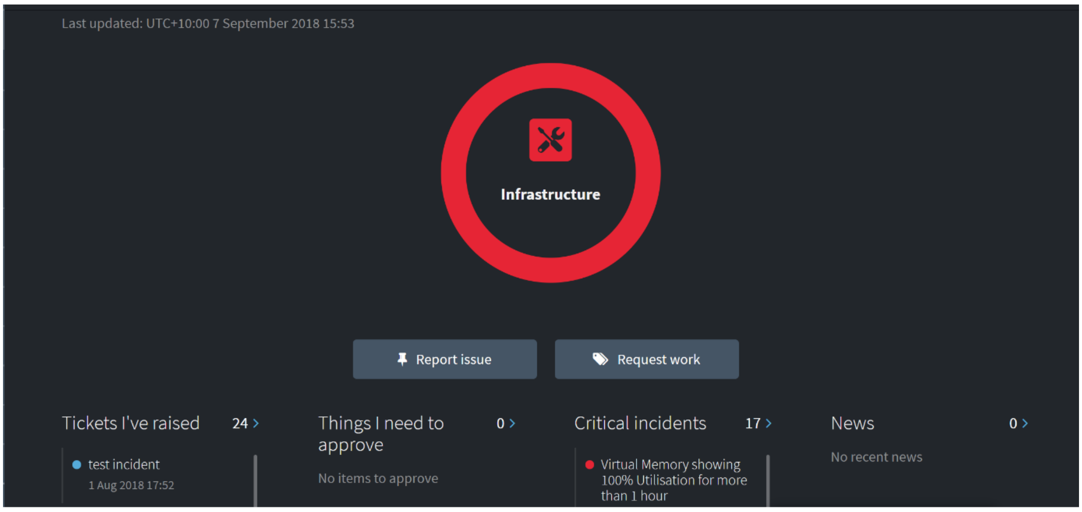
The Manage Centre portal, a web-based portal that enables clients to log incidents and service requests, query the status of incidents and service requests, and view contract information and other service reports.

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



Last updated: UTC+10:00 7 September 2018 15:53

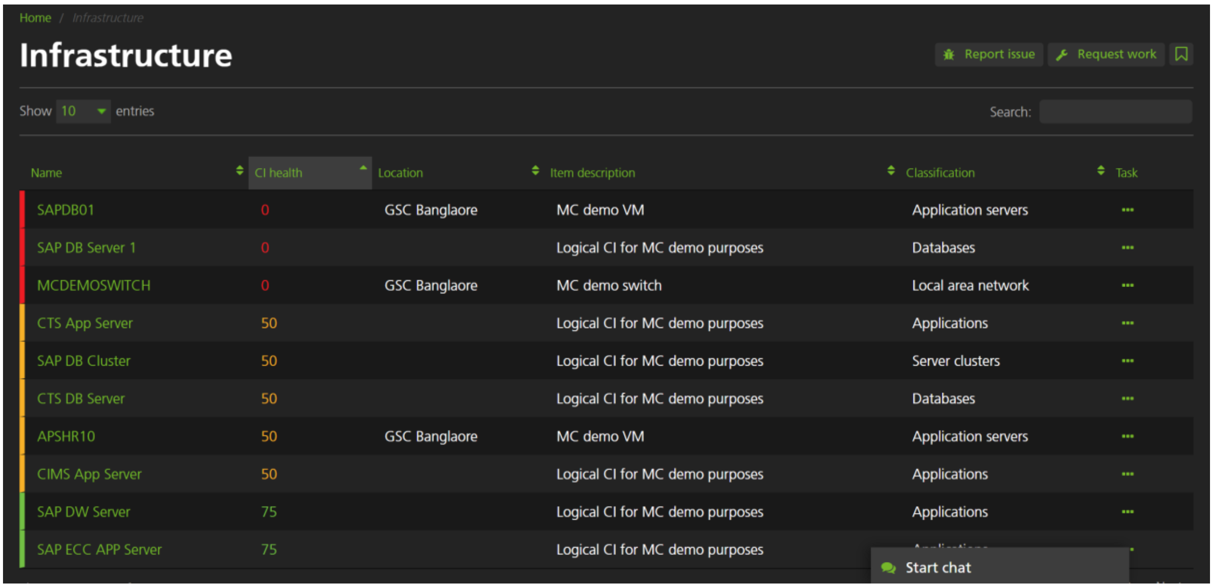
test incident
1 Aug 2018 17:52

No items to approve

Virtual Memory showing 100% Utilisation for more than 1 hour

No recent news

Figure 10 View infrastructure health

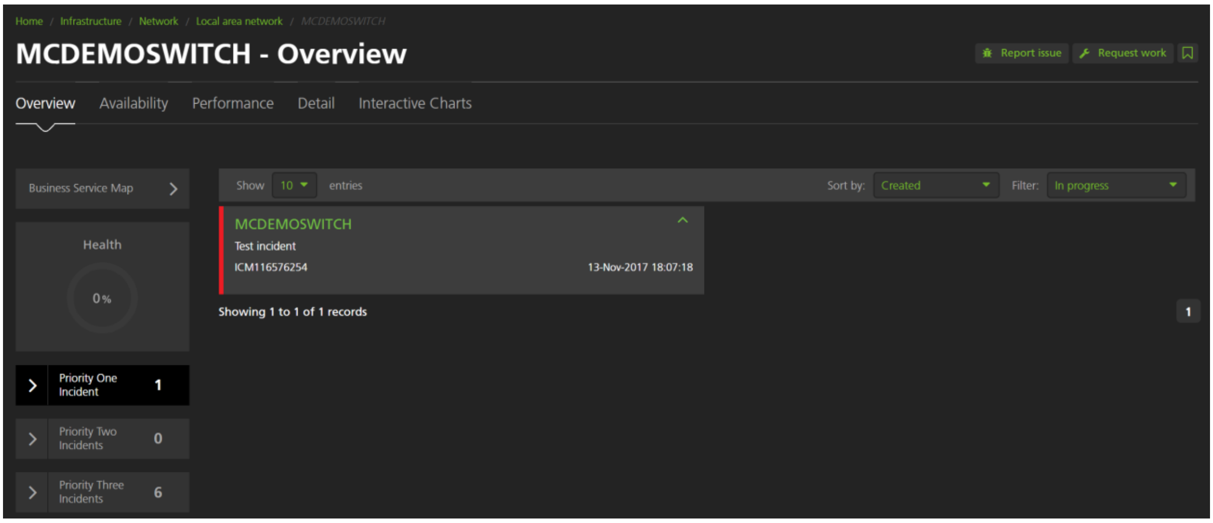


Infrastructure

Show 10 entries Search:

Name	CI health	Location	Item description	Classification	Task
SAPDB01	0	GSC Banglaore	MC demo VM	Application servers	•••
SAP DB Server 1	0		Logical CI for MC demo purposes	Databases	•••
MCDEMOSWITCH	0	GSC Banglaore	MC demo switch	Local area network	•••
CTS App Server	50		Logical CI for MC demo purposes	Applications	•••
SAP DB Cluster	50		Logical CI for MC demo purposes	Server clusters	•••
CTS DB Server	50		Logical CI for MC demo purposes	Databases	•••
APSHR10	50	GSC Banglaore	MC demo VM	Application servers	•••
CIMS App Server	50		Logical CI for MC demo purposes	Applications	•••
SAP DW Server	75		Logical CI for MC demo purposes	Applications	•••
SAP ECC APP Server	75		Logical CI for MC demo purposes	Applications	•••

Figure 11 View infrastructure health



MCDEMOSWITCH - Overview

Show 10 entries Sort by: Created Filter: In progress

MCDEMOSWITCH
Test incident
ICM116576254 13-Nov-2017 18:07:18

Showing 1 to 1 of 1 records

Figure 12 View infrastructure health - overview

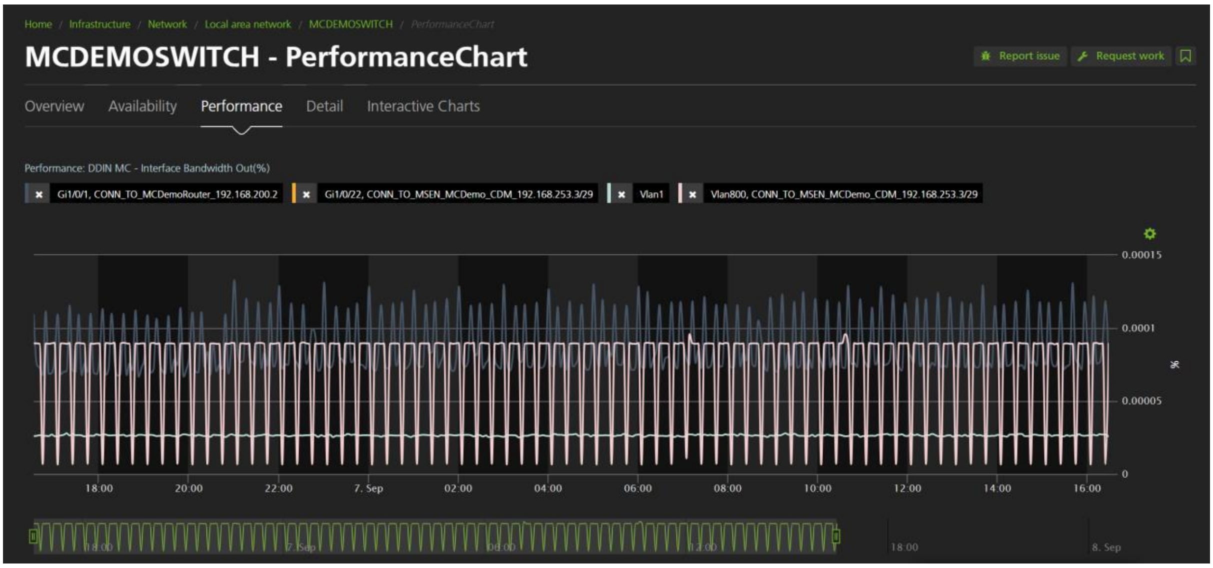

Home / Infrastructure / Network / Local area network / MCDEMOSWITCH / PerformanceChart
MCDEMOSWITCH - PerformanceChart
Report issue
Request work
Overview
Availability
Performance
Detail
Interactive Charts
Performance: DDIN MC - Interface Bandwidth Out(%)
Gi1/0/1, CONN_TO_MCDemoRouter_192.168.200.2
Gi1/0/22, CONN_TO_MSEN_MCDemo_CDM_192.168.253.3/29
Vlan1
Vlan800, CONN_TO_MSEN_MCDemo_CDM_192.168.253.3/29
0.00015
0.0001
0.00005
0
%
18:00
20:00
22:00
7. Sep
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
8. Sep

Figure 13 View infrastructure health – performance chart

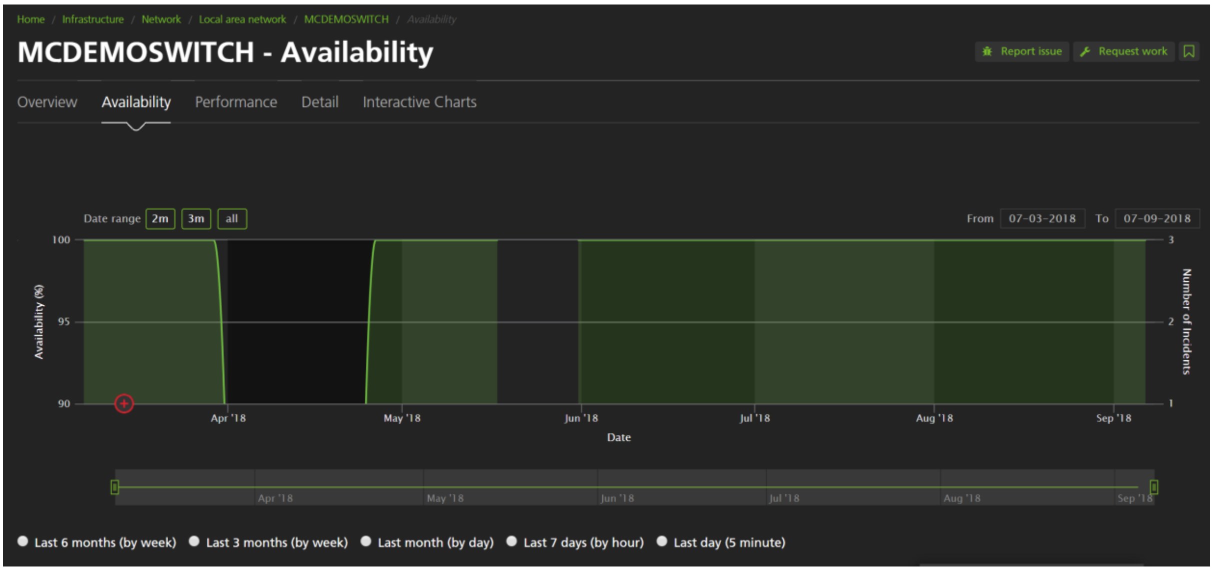
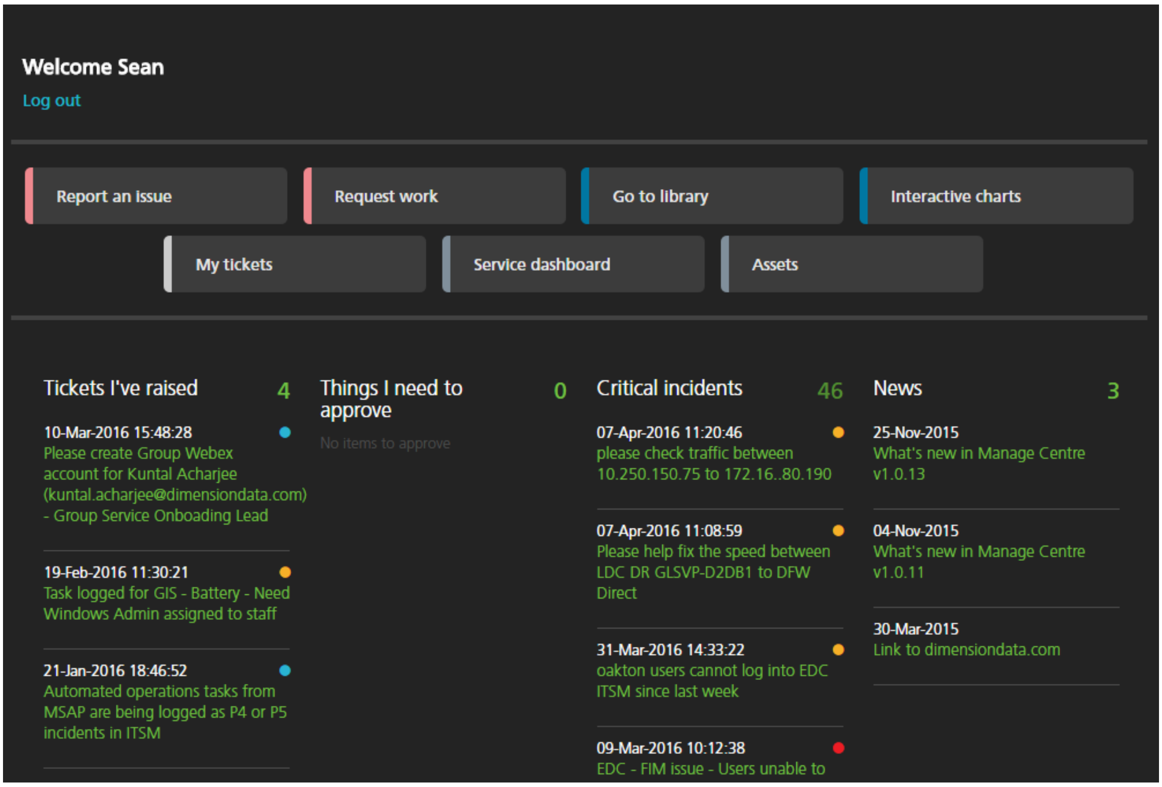


Figure 14 View infrastructure health – availability chart

3.2. Online incident and request logging

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

- log incidents and service requests [7]
  - 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)



Tickets I've raised 4

10-Mar-2016 15:48:28 ●
Please create Group Webex account for Kuntal Acharjee (kuntal.acharjee@dimensiondata.com) - Group Service Onboading Lead

19-Feb-2016 11:30:21 ●
Task logged for GIS - Battery - Need Windows Admin assigned to staff

21-Jan-2016 18:46:52 ●
Automated operations tasks from MSAP are being logged as P4 or P5 incidents in ITSM

Things I need to approve 0

No items to approve

Critical incidents 46

07-Apr-2016 11:20:46 ●
please check traffic between 10.250.150.75 to 172.16..80.190

07-Apr-2016 11:08:59 ●
Please help fix the speed between LDC DR GLSVP-D2DB1 to DFW Direct

31-Mar-2016 14:33:22 ●
oakton users cannot log into EDC ITSM since last week

09-Mar-2016 10:12:38 ●
EDC - FIM issue - Users unable to

News 3

25-Nov-2015
What's new in Manage Centre v1.0.13

04-Nov-2015
What's new in Manage Centre v1.0.11

30-Mar-2015
Link to dimensiondata.com

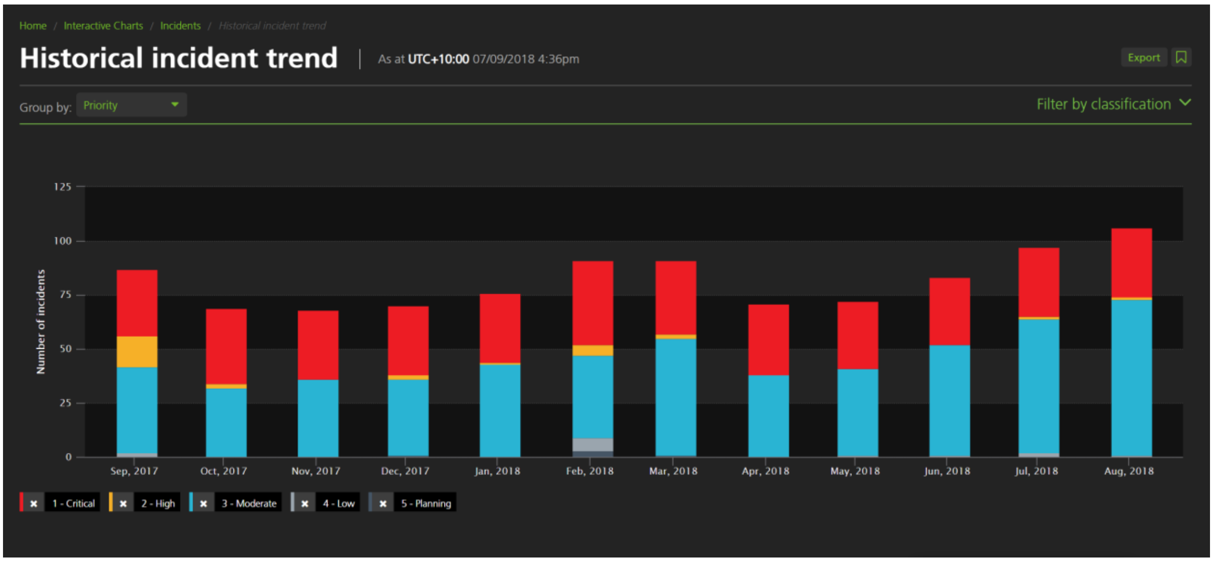
Figure 15 Incident and service request logging

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

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



Home / Interactive Charts / Incidents / *Historical incident trend*

Historical incident trend | As at **UTC+10:00** 07/09/2018 4:36pm

Group by: Priority

Figure 16 Historical incident trend report chart

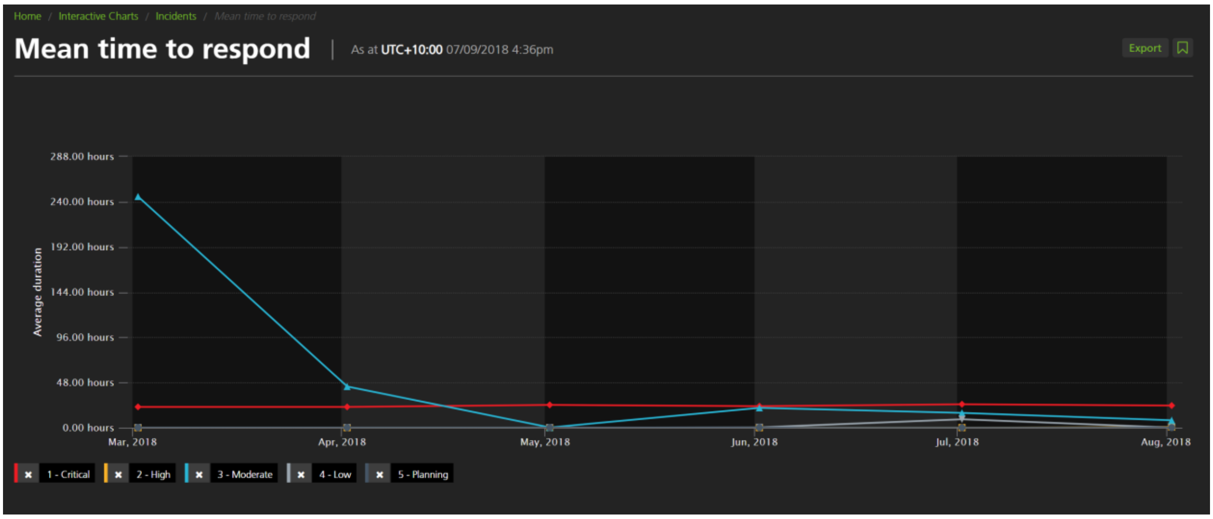
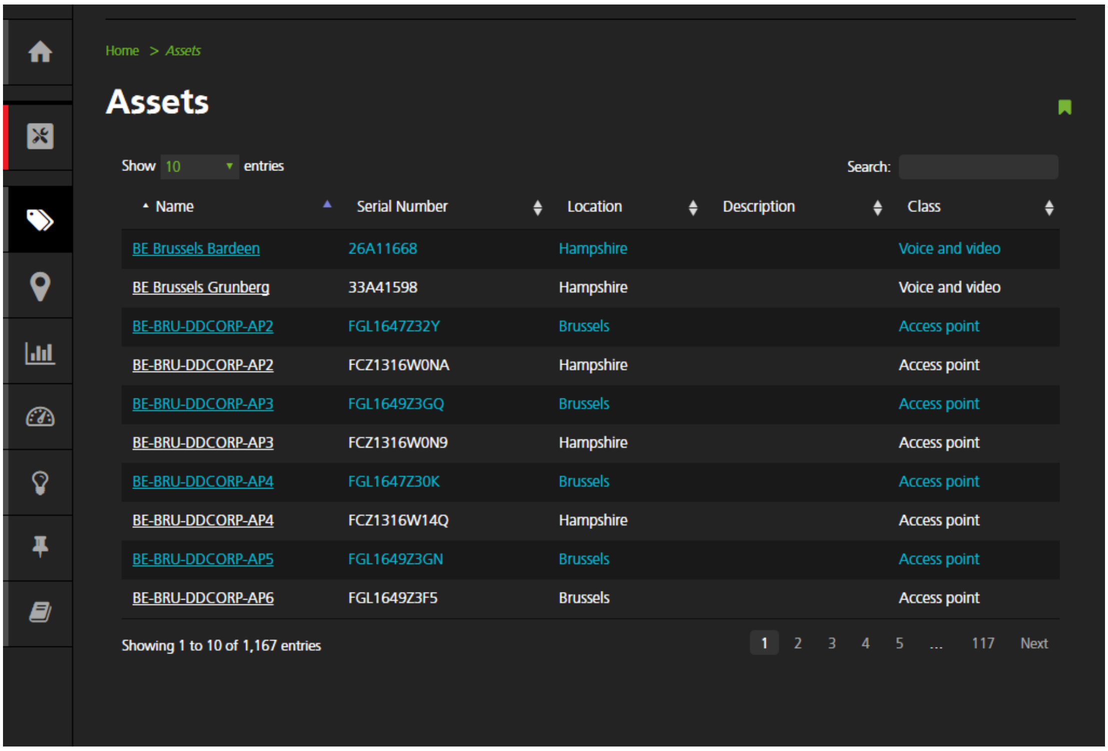


Figure 17 Mean time to respond report chart

3.4. Online access to asset reports

Manage Centre provides easy and convenient access to asset reports.



Name	Serial Number	Location	Description	Class
BE Brussels Bardeen	26A11668	Hampshire		Voice and video
BE Brussels Grunberg	33A41598	Hampshire		Voice and video
BE-BRU-DDCORP-AP2	FGL1647Z32Y	Brussels		Access point
BE-BRU-DDCORP-AP2	FCZ1316W0NA	Hampshire		Access point
BE-BRU-DDCORP-AP3	FGL1649Z3GQ	Brussels		Access point
BE-BRU-DDCORP-AP3	FCZ1316W0N9	Hampshire		Access point
BE-BRU-DDCORP-AP4	FGL1647Z30K	Brussels		Access point
BE-BRU-DDCORP-AP4	FCZ1316W14Q	Hampshire		Access point
BE-BRU-DDCORP-AP5	FGL1649Z3GN	Brussels		Access point
BE-BRU-DDCORP-AP6	FGL1649Z3F5	Brussels		Access point

Showing 1 to 10 of 1,167 entries

Figure 18 Asset reports

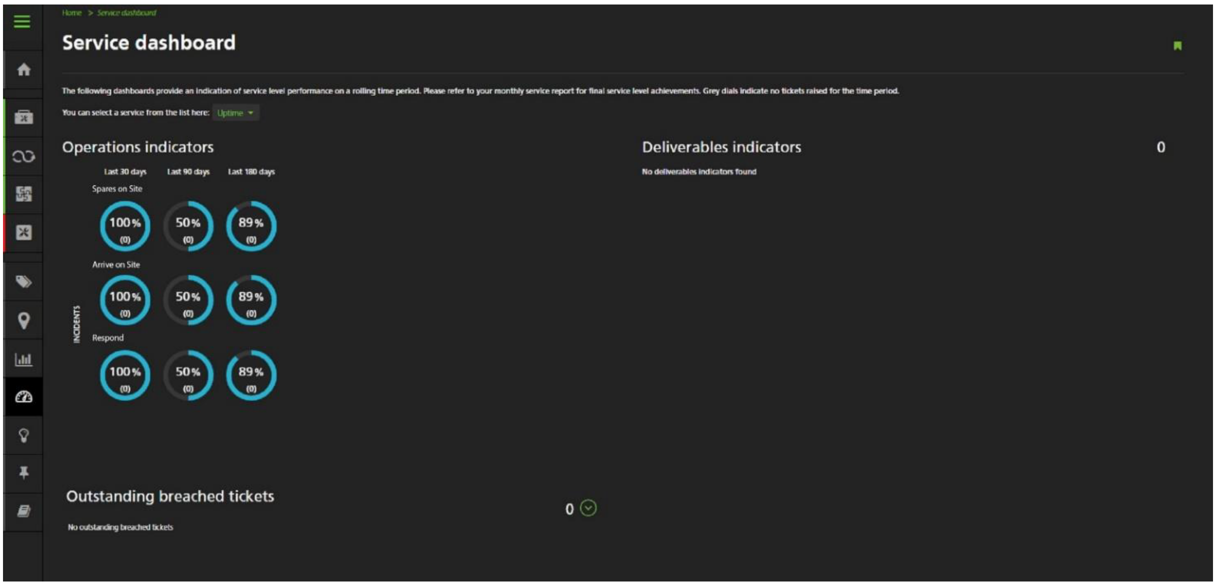
3.5. Service level dashboard

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.



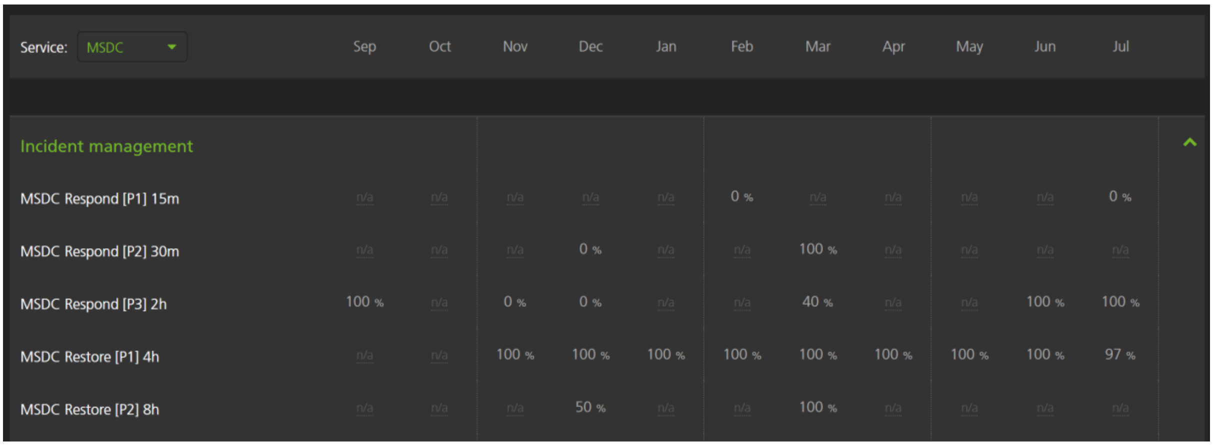
The following dashboards provide an indication of service level performance on a rolling time period. Please refer to your monthly service report for final service level achievements. Grey dials indicate no tickets raised for the time period.

You can select a service from the list here: Uptime

No deliverables indicators found

No outstanding breached tickets

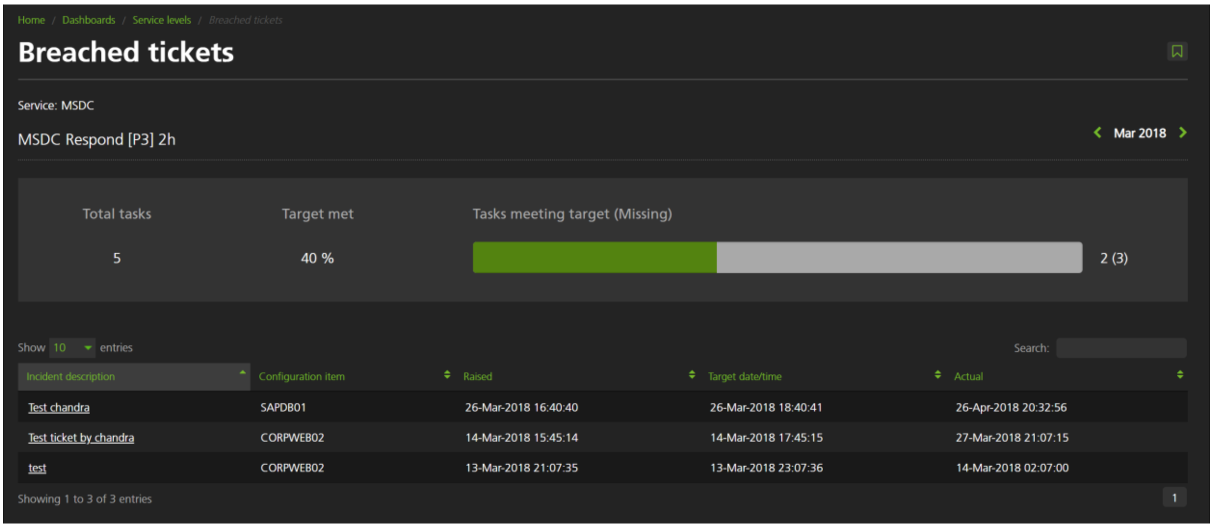
Figure 19 Service level dashboard



Service: MSDC

Incident management	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
MSDC Respond [P1] 15m	n/a	n/a	n/a	n/a	n/a	0 %	n/a	n/a	n/a	n/a	0 %
MSDC Respond [P2] 30m	n/a	n/a	n/a	0 %	n/a	n/a	100 %	n/a	n/a	n/a	n/a
MSDC Respond [P3] 2h	100 %	n/a	0 %	0 %	n/a	n/a	40 %	n/a	n/a	100 %	100 %
MSDC Restore [P1] 4h	n/a	n/a	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	97 %
MSDC Restore [P2] 8h	n/a	n/a	n/a	50 %	n/a	n/a	100 %	n/a	n/a	n/a	n/a

Figure 20 Service level dashboard – incident management



Home / Dashboards / Service levels / Breached tickets

Breached tickets

Service: MSDC

MSDC Respond [P3] 2h

Mar 2018

Total tasks	Target met	Tasks meeting target (Missing)
5	40 %	2 (3)

Show 10 entries

Search:

Incident description	Configuration item	Raised	Target date/time	Actual
Test chandra	SAPDB01	26-Mar-2018 16:40:40	26-Mar-2018 18:40:41	26-Apr-2018 20:32:56
Test ticket by chandra	CORPWEB02	14-Mar-2018 15:45:14	14-Mar-2018 17:45:15	27-Mar-2018 21:07:15
test	CORPWEB02	13-Mar-2018 21:07:35	13-Mar-2018 23:07:36	14-Mar-2018 02:07:00

Showing 1 to 3 of 3 entries

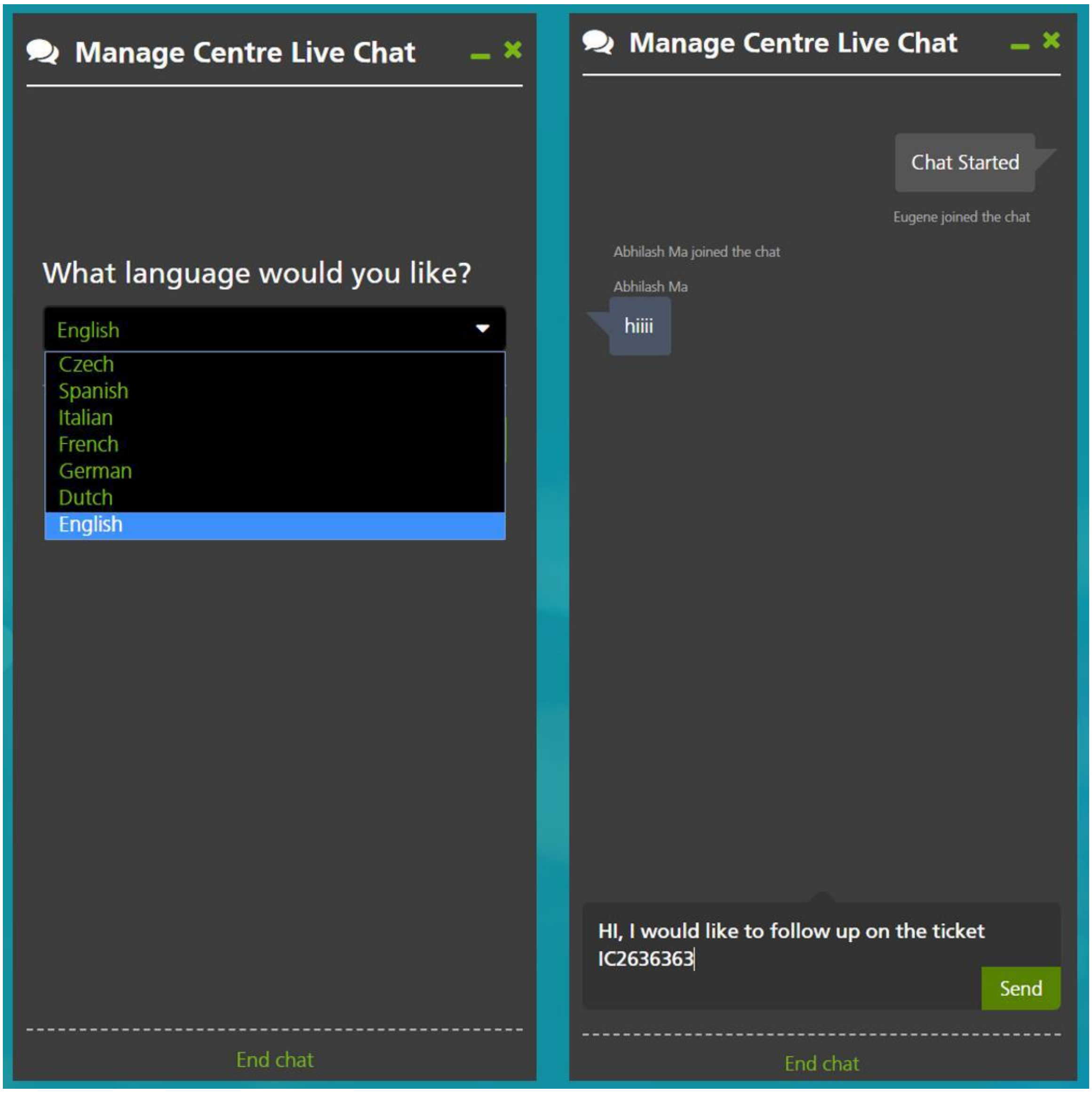
1

Figure 21 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.



Chat Started

Eugene joined the chat

Abhilash Ma joined the chat

Abhilash Ma

hiiii

HI, I would like to follow up on the ticket IC2636363

Figure 22 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:

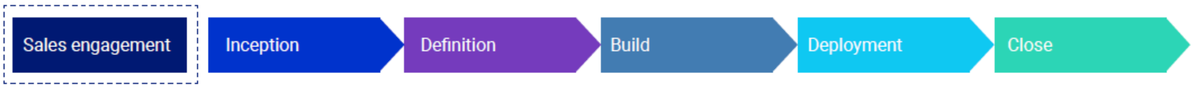


Figure 23 Transition Implementation Methodology phases

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 Tier one supported products

The following list is meant to be indicative as NTT are adding new products and technologies all the time. If you do not see something you are interested in on the list, please check with your NTT sales team.

Tier one supported products
Blue Coat
Blue Coat - Security and Policy Enforcement/Mobility
Blue Coat - Performance (WAN Optimization)
Blue Coat - Resolution (Secure Analytics)
Blue Coat - Security and Policy Enforcement/Mobility
Networking
Security
Check Point
Check Point - Endpoint Security
Check Point - Security Gateways
Check Point - Security Management
Security
Cisco
Cisco - Application Networking Services
Cisco - Collaboration Endpoints and Phones
Cisco - Conferencing
Cisco - Data Center Switching (Nexus)
Cisco - Email and Web security
Cisco - IPCC Enterprise (UCCE)
Cisco - Network Management
Cisco - Routers Fixed Configuration
Cisco - Routers Modular Configuration
Cisco - Servers - UCS Director
Cisco - Servers - UCS Manager

Tier one supported products
Cisco - Servers - Unified Computing
Cisco - Service Provider
Cisco - Switching Fixed Configuration
Cisco - Switching Modular Configuration
Cisco - Telepresence
Cisco - Unified Communications
Cisco - Video
Cisco - Wireless
Cisco Identity Management
Cisco Intrusion Prevention System
Cisco Network Security
Cisco Secure Access Control
Cisco Secure Mobility
Cisco Security Management
Communications
Contact Center
Data Center
Meraki
Networking
Security
F5
F5 - Security and Application Delivery
F5 - Viprion
F5 -LTM/GTM
Networking
Security
Juniper
Juniper - High End Routing (Service Providers)

Tier one supported products
Juniper - Network Infrastructure (Routing and Switching)
Networking
Security
Riverbed
Networking
Riverbed - Application Delivery (SteelApp (Stingray))
Riverbed - Performance Management (SteelCentral (Cascade/Opnet))
Riverbed - Storage Delivery (SteelFusion (Granite)/SteelStore (Whitewater))

Appendix C Tier two supported products

Tier two supported products
Aastra
Communications
Acme Packet
Communications
Adtech Global Solutions
Security
Aeroscout
Networking
Agito
Networking
Air Magnet
Networking
AirDefense
Security
Alcatel
Communications
Algosec
Security
Alvarion
Networking
APC
Data Center
Arista
Data Center
Aruba
Networking

Tier two supported products
Aspera
Data Center
Atea Systems
Communications
Audiocodes
Communications
Avaya
Avaya - Contact Center
Avaya - Unified Communications
Communications
Networking
Avepoint
Data Center
BMC
Data Center
Broadsoft
Communications
Calabrio
Contact Center
CipherTrust
Security
Citrix
Data Center
Clearswift
Security
Computer Associates
Networking
Crossbeam

Tier two supported products
Security
Dataflex
Communications
Dell
Data Center
Dell - SecureWorks (Verisign)
Dell - Servers
Dell - Storage
Security
Dialogic
Communications
eGain
Communications
eGlue
Communications
EMC
Data Center
EMC - Authentication
EMC - Backup and Recovery Solutions
EMC - Data Loss Prevention
EMC - Governance Risk and Compliance (GRC)
EMC - Identity and Access Management
EMC - Isilon NAS
EMC - Replication and Snapshot Solutions
EMC - SIEM
EMC - Storage Solutions
EMC - ViPR Management Software
EMC - Vmax

Tier two supported products
EMC - Vplex
EMC - Vspex
Security
EMC RSA
Security
Emerson / Liebert
Data Center
Envivio
Communications
Ericsson
Networking
Expand
FiberLink
Networking
FireEye
Security
Fortinet
Fortinet - Application Security
Fortinet - Management
Fortinet - Network Access
Fortinet - Network Security
Security
Frontrange
Networking
Genesys
Contact Center
GN Jabra
Communications

Tier two supported products
Hitachi Data Systems
Data Center
HP
Data Center
HP - Servers
HP - Storage
Networking
IBM
Data Center
Imperva
Security
Infoblox
Network Intelligence Platform
Infovista
Networking
IPCelerate
Communications
IPFX
Communications
ISS (Internet Security Systems)
Security
Jalasoft
Networking
Microsoft
End User Computing
McAfee
Firewall
Microsoft

Tier two supported products
Microsoft - Lync
NEC
Communications
Data Center
NetApp
Data Center
NetApp - FAS 3000 & 6000
NetApp - Network Security
NetApp - OnCommand System Manager
Netgear
Networking
Communications
Oracle (Acme Packet)
Communications
Oracle (MetaSolv)
Networking
Oracle (Sun)
Data Center
Palo Alto Networks
Security
Polycom
Communications
Polycom - Telepresence and Video
Polycom - Unified Communications
Polycom - Voice
Qualys
Security
Quantum

Tier two supported products
Data Center
Quest Software
Networking
Radware
Data Center
Senetas Security
Security
ServiceNow.com
Networking
Sonus
Communications
Sourcecode (K2)
End User Computing
SpeechCycle
Communications
SwordCiboodle
Communications
Symantec (MessageLabs)
Data Center
Symantec (Veritas)
Security
Trend Micro
Security
TSA CAABS
Communications
VCE
Data Center
VCE - Vblock

Tier two supported products
Verint Systems
Communications
VMware
Data Center
VMware (AirWatch)
Security
ZANTAZ EAS
Data Center

Table 11 Tier two supported products

Appendix D Direct presence countries

Direct presence countries	
Angola	Korea
Australia	Luxembourg
Austria	Malaysia
Belgium	Mexico
Botswana	Namibia
Brazil	Netherlands
Canada	New Zealand
Chile	Philippines
China, Beijing	Poland
China, Shanghai	Saudi Arabia
Czech Republic	Singapore
England	Slovakia
France	South Africa
Germany	Spain
Hong Kong	Switzerland
Hungary	Taiwan
India	Tanzania
Indonesia	Thailand
Ireland	Uganda
Isle of Man	United Arab Emirates
Italy	United States
Japan	Vietnam
Kenya	

Table 12 Direct presence countries

Appendix E Preferred Partner Programme countries

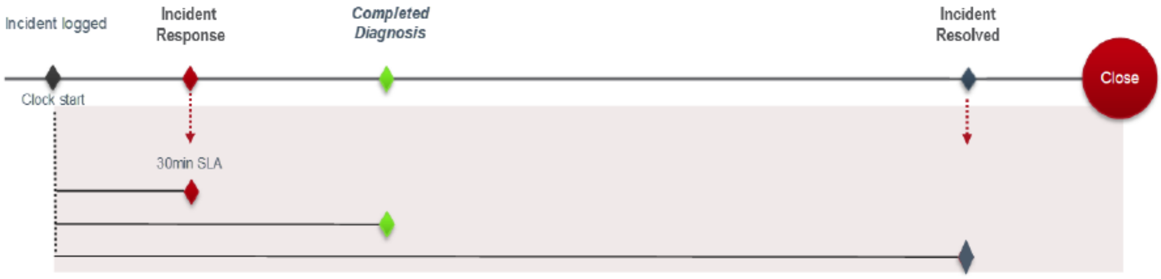
Preferred Partner Programme countries			
Albania	Dominica	Kuwait	Russia
Algeria	Dominican Republic	Latvia	Senegal
Anguilla	DRC	Lebanon	Serbia
Argentina	Ecuador	Lithuania	Seychelles
Armenia	Egypt	Macedonia	Sierra Leone
Aruba	El Salvador	Madagascar	Slovenia
Azerbaijan	Equatorial Guinea	Malawi	Sri Lanka
Bahamas	Estonia	Maldives	Sweden
Bahrain	Finland	Mali	St Lucia
Bangladesh	Gabon	Malta	Suriname
Barbados	Gambia	Mauritania	Tajikistan
Belarus	Georgia	Mauritius	Togo
Belize	Ghana	Moldova	Trinidad & Tobago
Bermuda	Gibraltar	Montenegro	Tunisia
Bolivia	Greece	Morocco	Turkey
Bosnia and Herzegovina	Grenada	Mozambique	Ukraine
Bulgaria	Guatemala	Nepal	Uruguay
Burkina Faso	Guernsey	Nicaragua	US Virgin Islands
Cambodia	Guinea Bissau	Niger	Uzbekistan
Cameroon	Guinea	Nigeria	Venezuela
Cayman Islands	Guyana	Norway	Zimbabwe
Central African Republic	Haiti	Oman	
Chad	Honduras	Pakistan	
Colombia	Iceland	Panama	
Congo	Iraq	Paraguay	
Costa Rica	Isle of Man	Peru	

Preferred Partner Programme countries			
Cote d'Ivoire/Ivory Coast	Israel	Portugal	
Croatia	Jamaica	Puerto Rico	
Curacao	Jersey	Qatar	
Cyprus	Jordan	Romania	

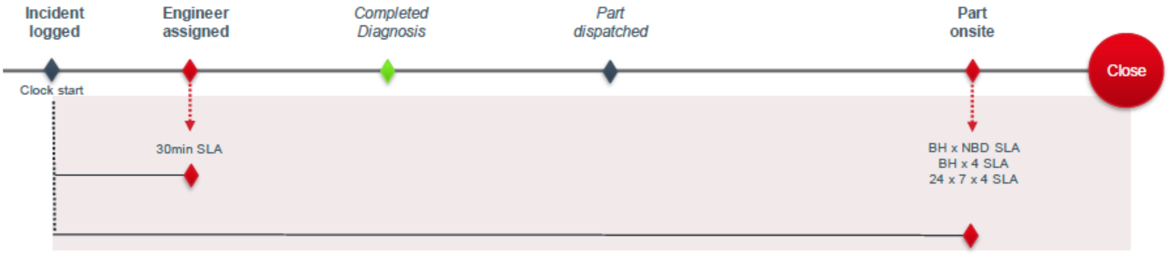
Table 13 Preferred Partner Programme countries

Appendix F Service level commitments per service plan

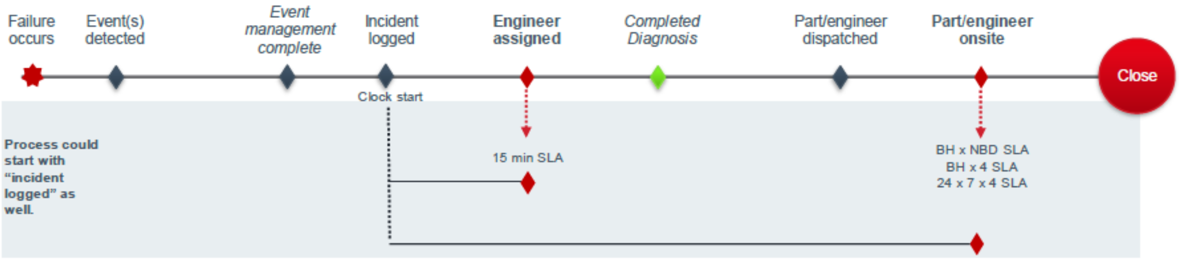
Appendix F.1 Remote



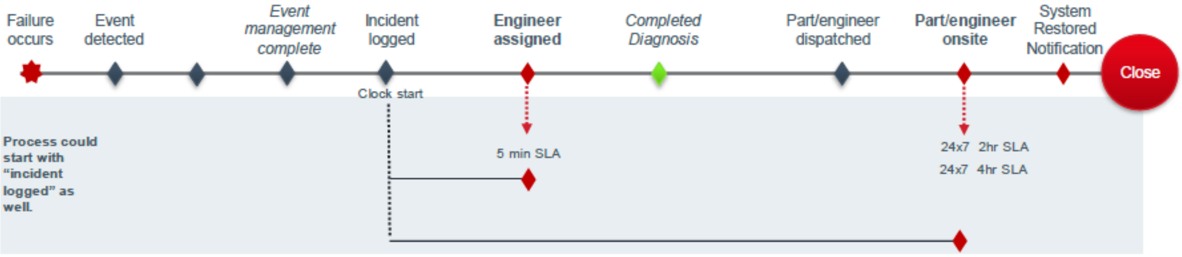
Appendix F.2 Parts Only



Appendix F.3 On-site



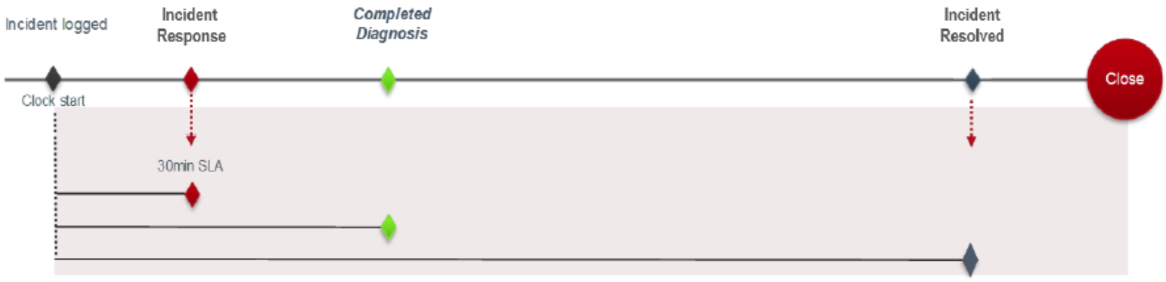
Appendix F.4 Mission critical



Appendix G European Service level commitments per service plan

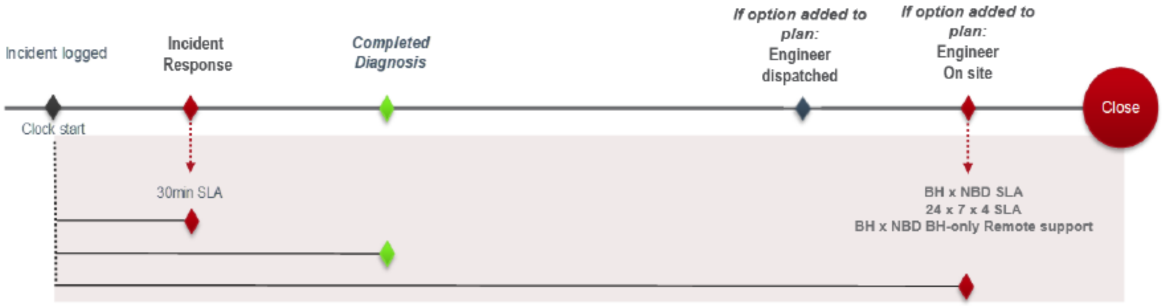
Appendix G.1 Remote

Appendix G.1.1 Remote



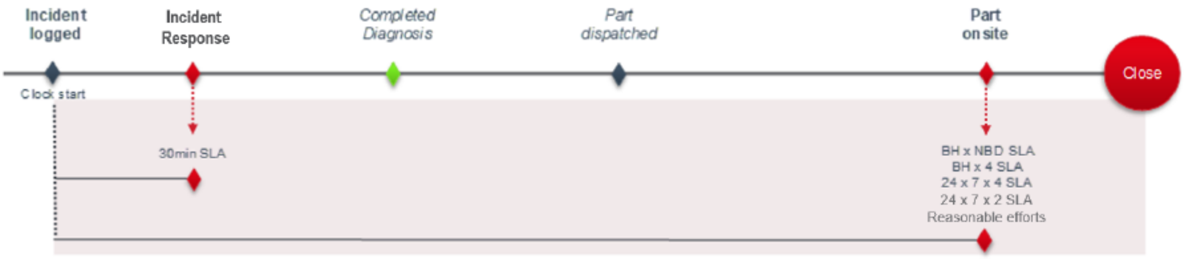
*In the case of BH-Only Remote SLA, the clock runs only during Business Hours.

Appendix G.1.2 Remote with labour to site (engineer only)


Incident logged
Incident Response
Completed Diagnosis
If option added to plan: Engineer dispatched
If option added to plan: Engineer On site
Close
Clock start
30min SLA
BH x NBD SLA
24 x 7 x 4 SLA
BH x NBD BH-only Remote support

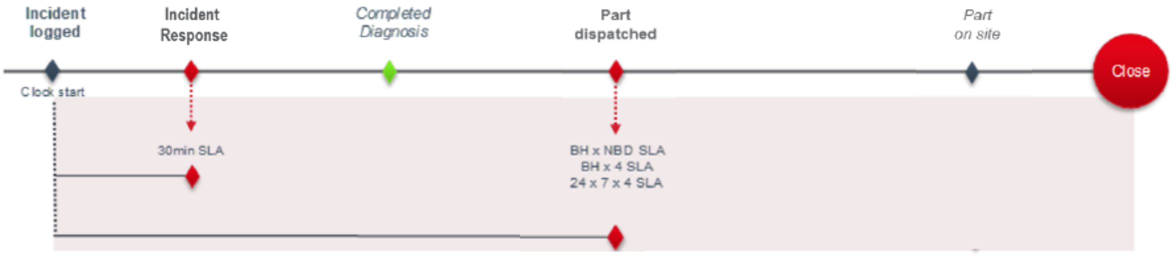
Appendix G.2 Parts only

Appendix G.2.1 Parts only



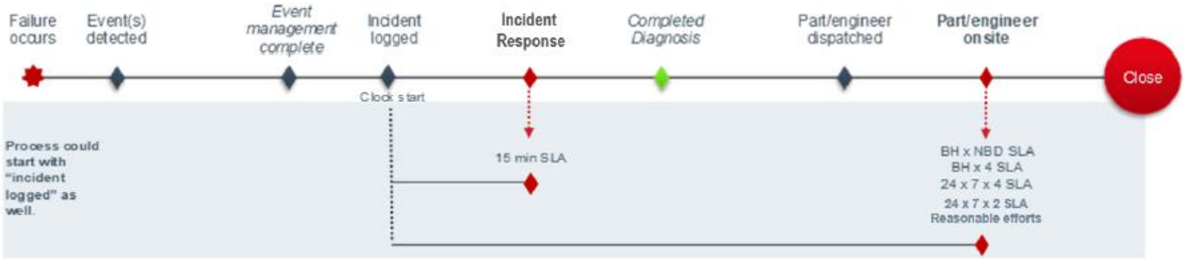
*In the case of Parts Only with BH-Only Remote SLA, the clock runs only during Business Hours. BH-only Remote options offered to Parts Only BHx4 and Parts Only BHxNBD SLAs.

Appendix G.2.2 Parts Only Ship



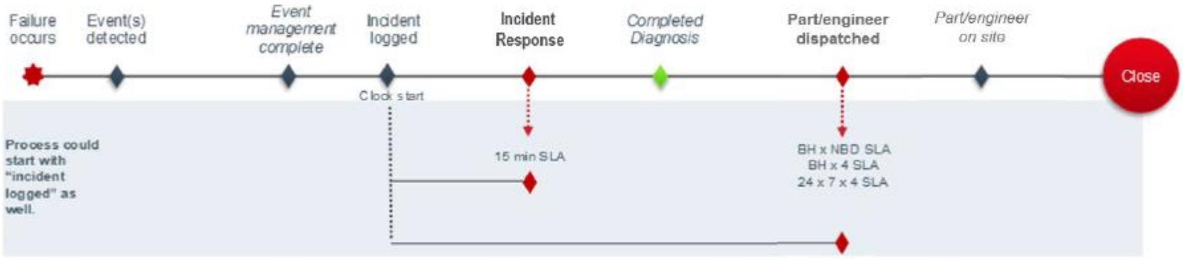
Appendix G.3 On-site

Appendix G.3.1 On-site

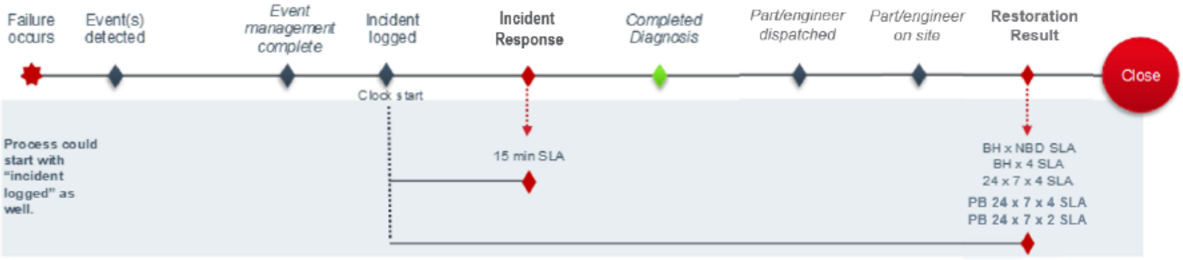


*In the case of on-site with BH-Only Remote SLA, the clock runs only during Business Hours. BH-only Remote options offered to on-site BHx4 and on-site BHxNBD SLAs.

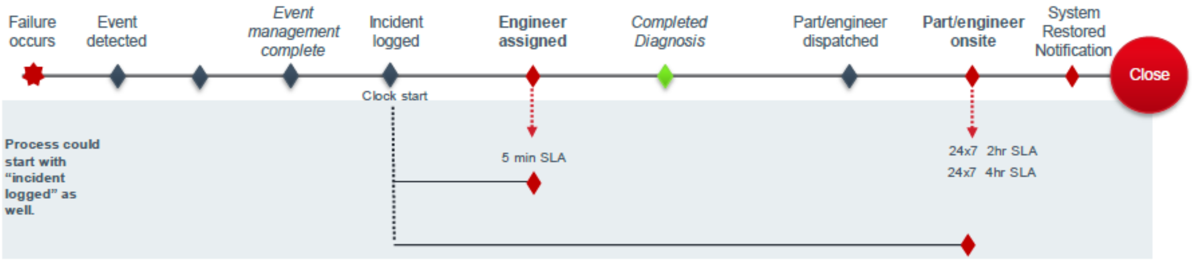
Appendix G.3.2 On-site Ship



Appendix G.3.3 On-site Result



Appendix G.4 Mission critical



Appendix H Uptime for NetApp

As a NetApp Support Services Certified (SSC) Partner, NTT provides first line and second line support Uptime services on NetApp environments, with specialist training, access to support tools, Technical Advisors, and backup support from NetApp via back-end software and hardware support contracts in place should escalation be required.

Appendix H.1 Uptime for NetApp

The Uptime for NetApp service comprises the same elements as the standard Uptime service, and includes the following AutoSupport enhancement unique to NetApp:

- **AutoSupport feature**: NetApp storage arrays include a feature called 'AutoSupport' which is a call home function, this enables the NetApp arrays to automatically send an email message to the support partner in the event of suspected issues. This service is discussed in more detail under the section below 'Uptime for NetApp AutoSupport'.

Appendix H.1.1 Uptime for NetApp AutoSupport

The Uptime for NetApp AutoSupport service means that the majority of incidents are not logged by the client directly. Clients may of course contact the service desk directly, or via Manage Centre as per the standard call logging method for Uptime, however on the whole NTT will know the client's NetApp devices are not optimally performing before the client does, and we will then contact the client to inform them of the issue.

The NetApp storage arrays include a feature called 'AutoSupport' which is a call home function. This means that the NetApp arrays automatically send an email AutoSupport notification message to NTT in the event of self -suspected issues. This means that a high percentage of Incidents for NetApp arrays will be opened proactively via the AutoSupport feature and NTT will then contact the client to inform them of the issue, most likely before they even know there is an issue.

NTT resolves the case either independently, or if escalation to NetApp is required, then with NetApp involvement – as appropriate per the Uptime Service Plan secured by the client for the estate in question.

Please note:

- AutoSupport feature is mandatory under Uptime for NetApp
- The **Next Business Day** (NBD) commitment for NetApp is only applicable until 15h00 of the current business day at the client location. I.e. only incidents logged before/at 15h00 at the client location can be guaranteed to be resolved or

responded to on-site before the end of the next business day. This constraint is the result of requirements imposed by NetApp and therefore is called out as an exception, as it affects NTT's ability to deliver the generically-defined NBD commitment.