Managed Service Experience Insights Technical Service Description

Overview of Service

NTT's Managed Service Experience Insights is an extension of our Managed Campus Networking portfolio, providing Network Layer insights natively integrated into the NTT Managed Networks solutions service offering and the Managed Campus Networks (MCN) platform. SEI extends the MCN Managed Campus solution by enabling the creation of sophisticated synthetic monitoring tests that offer actionable visibility into how users experience accessing critical business applications, whether in the Cloud or on-premises, from multiple locations on the network. The Managed Service Experience Insights service supports the following:

- Continuous Path Quality Monitoring: Gain visibility into connection quality for proactive issue identification and swift
- Path Discovery: Visualizes the traffic paths between agents and internet destinations, allowing you to view the latency of each hop at regular intervals, during latency spikes, and in real time.
- Multiple Agent Formats: SPEKTRA Edge Appliance Agents, docker agents for network devices, and cloud environments enable comprehensive coverage of critical nodes in the network.
- Variety of Target Formats: Monitor managed targets in the client environment and public endpoints with various target formats, including ICMP, HTTP, UDP, and Speed Test Targets.
- Speed Testing: Assess connection throughput at regular intervals or in real time.
- Flexible and Robust Alerting: Implement proactive performance monitoring, rapidly identify issues, and expedite problem resolution with customizable alerts.

Service Experience Insights seamlessly becomes a part of the Managed Campus service offering, creating a comprehensive network monitoring solution by deploying up to five agents per site using the SPEKTRA Edge Appliance and lightweight Docker agents

The Client Insights service will be supported in accordance with the NTT processes described in the *MCN Statement of Work and Specific Terms documents..*

Client Responsibilities and Prerequisites

- An active Managed Services contract with NTT for the Campus Network environment
- The Client must be in possession of an active hardware service contract for the device(s) under management with the vendor, or a vendor approved third party such as NTT Uptime Support Services
- The Client must delegate authority to NTT engineers to contact the vendor (or authorized third party) directly for the purposes of the service.
- Client network infrastructure that supports hosting of container-based applications (only applicable for deploying docker containerized probing agents)
- Any licenses management, if required
- Any software or firmware operating on the device must be a version currently supported by the vendor.
- Simple Network Management Protocol (SNMP) must be enabled and configured for devices to be managed as part of the Service.

Scope of Service

Managed Service Experience Insights monitoring provides client with insight into the quality of services consumed by each campus network managed by NTT. Deep dive into each campus performance and gain a comprehensive view into how the enterprise is accessing the critical services that drives business.
For the purposes of the offering, the following definitions are provided:

- **Targets of interest** - these are SaaS, cloud or data center locations that end-users of the client routinely connect to, in order to perform their job function. Typically referred to as business-critical applications or services, and act as target locations for monitoring services.
- **Locations** - where users connect from and are typically branch or campus locations where users connect to the client's network. Campus Insights Agents are deployed onto network infrastructure in these locations.
- **Agents** - are lightweight probing software that can be configured to send synthetic traffic to internet endpoints and other agents to continuously measure the quality of network traffic to business-critical services.

The service comprises either hardware appliances or container-based agents which are deployed onto client network infrastructure already managed by NTT. A large number of out-of-the-box Insights into families of business-critical applications and services are supported. These include:

- Collaboration services
- Office applications
- SaaS based ERP and CRM services
- Campus to Campus services
- Public and Private Cloud hosted services

Throughout the onboarding process NTT will work with the client to identify which of the available Insight families should be used, or to capture any customer defined Insight requirements. NTT will work with the client to define which locations on the network need to connect to which specific targets of interest. i.e. **Probing Distributions** are policies to trigger synthetic monitoring traffic between agents and targets. Once implemented, monitoring analytics will be available via the NTT Services portal.
Service Experience Insights supports the following key use cases:

Sensitivity Label: General

- Continuous path monitoring, including ping loss, latency, jitter, and ping round trip time between edge locations and SaaS, Cloud or on-premise targets (for example to Microsoft Teams, or com)
- Speed test monitoring between edge locations and Cloud or on-premise targets (e.g., from a campus location to a data center).
- Internet path discovery and monitoring showing the route traffic takes from the edge location to targets.

The Insights are combined with available network metric information providing a holistic view of network health and user experience. Clients can select services to monitor from our library of common business services or add custom monitoring endpoints.

Service Experience Insights Components

This section provides details about the components present in Managed Service Experience Insights.

Agents

Agents are lightweight probing software deployed to hosts in the network and managed by the cloud-based Service Experience Insights (SEI) Controller.

The primary purpose of agents is to:

- Create probing data by sending synthetic probing traffic to targets and receiving replies.
- Capture information about the host device that may be impacting network performance.
- Upload the resulting data to the SEI Controller, where it is saved as time series metrics data.
- Perform real-time on-demand troubleshooting tests behind the NAT.
- Act on probing and management instructions downloaded from the SEI Controller.

Agent-to-agent probing is an optional configuration for Static and Cloud Agents. When configured, these agents reply to probing from other agents and are called “managed targets” that can be added to probing distributions.

There are two options available for SEI Agents, namely software agents and hardware agents.

Hardware-based Agents are NTT provided appliances that natively run the SEI Agent software and are connected to the client’s network infrastructure such as a switch. The appliance (SPEKTRA Edge Appliance) is a Linux based device operating with EdgeLQ OS. This device is suitable for environments in which the network infrastructure is not capable of docker containers. Hardware agents are typically used as static agents (dedicated network devices).

Software Agents are software-based images loaded onto the client’s docker container capable infrastructure (such as Cisco Catalyst 9K series switches) or on Virtual Machines hosted in the Cloud to perform the tasks required for the SEI offering. Software agents can be either static agents or cloud agents. The following table shows the Service Experience Insights software agents supported.

Agent Type	Hosting Environment	Supported Environments
Static Agent	Run as Docker Image on application-hosting network devices.	• Network devices capable of supporting Docker containerized agents. • Available in the public Docker Repository and can be activated using a token.
Cloud Agent	For data centers and cloud environments	• Deployed to VMs with Docker runtime hosted in public or private cloud environments. • Azure, GCP, AWS VM images available upon request

All agents send synthetic traffic to probe internal targets within the network and internet-based external targets. Static and cloud agents can also be configured as “managed targets” that respond to probing by other agents providing flexibility to deploy agents widely across the network providing continuous and on-demand insights about network traffic quality for business-critical services inside and outside the network.

Probing distributions define the probing targets, protocols, and intervals and agents receive these instructions automatically from the SEI Controller thereby sending probing traffic and receiving replies from targets at intervals defined in the probing distribution. The resulting probing and device data is stored in the agent’s local memory for up to one hour. Every 60 seconds, agents upload stored data to the SEI Controller and check for new or updated probing instructions. At the same time locally stored data is discarded after it has been uploaded to the SEI Controller. Should the agent be unable to communicate with the SEI Controller for more than one hour, probing continues but any buffered data older than one hour is overwritten with each new minute of data. When communication is restored, the agent reconnects to the SEI Controller, the last hour of test data is uploaded to the time series database and erased from local memory.

Additional Agent Deployment

After completing the initial onboarding of the Service Experience Insights agents, the Client may request installation of additional Campus Insights agents throughout the life of the Managed Campus Networking service contract. When requiring additional agents to be deployed, the following must be taken into consideration:

- A Service Request must be raised by an authorized client representative through the NTT Services Portal
- An NTT engineer will contact the client to authorize installation of the Managed Service Experience Insights agent on the network infrastructure device defined by the client or for a NTT representative to install a SPEKTRA Edge appliance at the requested location(s) in alignment with NTT’s standard change processes.
- Once authorized, the NTT engineer will deploy the Managed Service Experience Insights agent onto the client’s network infrastructure during a mutually agreed time (ie; a Scheduled Maintenance Window).
- Where an appliance is to be installed, the client must ensure that the required cabling, power and other required infrastructure is available prior to the SPEKTRA Edge Appliance being installed.

Sensitivity Label: General

- Once installed, a NTT engineer will configure the specific out-of-the-box or custom Insights derived from this agent, and validate that monitoring metrics and analytics are available via the NTT Services Portal
- This will also include authorization for additional service charges.

Agent Removal

The Client may request removal of Campus Insights agents from the network infrastructure, or to have a SPEKTRA Edge Appliance removed, by raising a Service Request with NTT.

- An NTT engineer will contact the client to agree a suitable time during which the Campus Insights agent will be removed from the network infrastructure device defined by the client and following NTT's standard change processes..
- If the Agent is a hardware appliance, the NTT engineer will contact the Client to arrange a suitable time to disconnect and remove the appliance.
- Charges may continue to apply, depending on the terms of the MCN at the time of subscribing to the offering.

Targets

Service Experience Insight supports Unmanaged Targets and Managed Targets. Probing protocol and available metrics vary by the type of target.
Probe public and private services and other installed agents

Target Type	Description	IP Type
Managed Targets	Managed Targets are devices with agents deployed by NTT. Enable target functionality on Static and Cloud Agents.	External & Internal IP
Unmanaged Targets	Unmanaged targets are services or devices which doesn't have agents deployed by NTT. Probe unmanaged public and private services using IP or URL.	Publicly accessible IP or URL

The following table shows the protocols supported by each type of target.

Target Type	ICMP	HTTP	UDP	Speed Test
Unmanaged Targets	✓	✓	--	✓
Managed Targets	✓	✓	✓	✓

The metrics supported by the above protocols are shown in the table below.

		ICMP	HTTP	UDP	Speed Test
Latency (ms)		✓	✓	✓	--
Jitter (ms)		✓	✓	✓	--
Loss (%)		✓	--	✓	--
HTTP Availability (%)		--	✓	--	--
HTTP Request Response Time (ms)		--	✓	--	--
Connection set up	DNS lookup (ms)	--	✓	--	--
	Initial connection (ms)	--	✓	--	--
	SSL (ms)	--	✓	--	--
Request Response	Request Send (ms)	--	✓	--	--
	Waiting TTFB (ms)	--	✓	--	--
	Content Download (ms)	--	✓	--	--
Hops Latency (ms)		✓	✓	✓	--
Probing Interval Default		30 seconds	60 seconds	30 seconds	1 hour
Probing Interval Custom		1 sec to 10 mins	30 sec to 10 mins	100 ms to 10 mins	1, 6, 12, 24 hrs
Probing Duration		N/A	N/A	N/A	3, 8, 10 sec

Service Experience Insights Options

The NTT Managed Service Experience Insights service is packaged on the basis of the number of campus locations and the number of Insights (Targets to monitor).
The following table shows the available options.

Package	Locations	Agents Per Site	Total Agents (Max)	Probing Sessions
Small (10 Insights)	15	5	75	750
	50	5	250	2500
	100	5	500	5000
Medium (20 Insights)	15	5	75	750
	50	5	250	2500
	100	5	500	5000
Large (30 Insights)	15	5	75	750
	50	5	250	2500
	100	5	500	5000
Custom Package*	Custom Insights & Locations			

**Custom Package is applicable if either the number of insights is greater than 30 or Locations greater than 100*

Supported Technologies

Managed Service Experience Insights static agents are deployable on any network infrastructure that supports Docker runtime container based third party applications but has only been extensively tested on Cisco Catalyst 9K series switches. Consult the NTT Deals Desk to confirm whether the intended infrastructure supports containerized Docker runtime environments.
Optionally, the SPEKTRA Edge Appliance can be provided by NTT where the infrastructure is not capable of supporting Docker containers or where the deployment of a hardware appliance is preferred.
The SPEKTRA Edge appliance is connected to a suitable network device such as a switch and the agent operating on the appliance is then configured accordingly.

Service Specific Operations

Monitors

The following monitoring metrics and analytics are available via the NTT Services Portal as part of the Campus Insights service.

Monitor	Description	Alerts	Performance Info	Resolution
Ping Loss	Number of ping packets lost, displayed as a percentage, between a Target of Interest and a client defined location.	✓	Between a Campus Insights agent and a SaaS or Cloud based Location of Interest.Between 2 Campus Insights agents	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.
Latency	Time taken to reach the target of interest from client defined location.	✓	Between a Campus Insights agent and a SaaS or Cloud based Location of Interest.Between 2 Campus Insights agents	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.
Jitter	Variation of time delay to the target of interest from client defined location.	✓	Between a Campus Insights agent and a SaaS or Cloud based Location of Interest.Between 2 Campus Insights agents	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.
Number of Hops	Number of hops a packet takes between a Target of Interest and a Client Defined Location and the latency between each hops.	✓	Between a Campus Insights agent and a SaaS or Cloud based Location of Interest.Between 2 Campus Insights agents	Used for Insights
Throughput (speed test)	Measures the speed, in Mbps, between a Client Defined Location and a Target of Interest	✓	Between 2 Campus Insights agents	Used for Insights

Sensitivity Label: General

Ongoing Management Activities

After initial onboarding, NTT will monitor and manage all Managed Service Experience Insights agents deployed onto network infrastructure managed by NTT under a Managed Campus Networking service contract.
Ongoing Management Activities include:

- Responding to Incidents where a Campus Insights agent is unresponsive.
- Performing Managed Service Experience Insights agent software updates when new software versions are available. These updates will follow the standard NTT Release and Deployment Management processes and be scheduled during a time mutually agreed by NTT and the Client.

Service Requests

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

Service Experience Insights Service Requests

Task	Description	Included
Target of Interest Management	Client can define a new Targets of Interest, modify an existing Target of Interest or remove an existing Target of Interest via a Service Request. As part of this Service Request, Client can define which Locations will be used to monitor the client experience between that location and the newly defined Target of Interest when defining new or modifying existing Targets of Interest.	✓
Agent Management	Client can request installation of new Service Experience Insights agents onto network infrastructure Managed by NTT or to uninstall a Service Experience Insights agent from network infrastructure Managed by NTT. Where the infrastructure is not currently Managed by NTT, client can request this infrastructure to be onboarded into NTT management.	✓
Probe Distribution Management	Client can define new probing policies, modification of probing policies or removal of probing policies, which defines the probing configuration on agents.	✓

Reporting & Analytics

The following pre-defined reports and analytics are available via the NTT Services Portal. For more detailed information on available reports and analytics, and their usage, please consult the NTT Campus Insights end user manual.

Report or Dashboard View	Description	Usage
Map Widget	The Map Widgets shows locations where Service Experience Insights agents are deployed around the globe.	The Map Widget is available via the Services Portal. Clients can drill down into locations of interest via the view. Also client can get a view of the services which needs attention due to degraded performance against configured threshold values.
Service Experience Insights	This dashboard widget provide a view of service experience of all deployed Service Experience Insights software agents with respect to packet loss, jitter and latency, to the targets of interest	The dashboard widget provides statistical and trend insights of packet loss, jitter and latency from deployed agents to the targets of interest. This can be used to further have a graphical view of these measurements over time.

Service Transition

Tasks Included in the Standard Transition

During client onboarding the following installation activities will occur:

- Client will define Locations and Targets of Interest in a template provided by NTT during the onboarding phase.
- Client will identify which network infrastructure under management by NTT will have Campus Insights agents deployed onto it.
- Once administrative privileges are granted to NTT, a scheduled maintenance window will be agreed with the client, during which time NTT will deploy Campus Insights agents onto the network infrastructure identified by the client.
- NTT will configure Managed Service Experience Insights based on the Locations and Targets of Interest defined by the client during onboarding.
- NTT will provide client defined users access to NTT Services Portal through which Managed Service Experience Insights analytics can be viewed.
- NTT will provide Managed Service Experience Insights software usage documentation.

Sensitivity Label: General

Tasks Excluded from the Standard Transition

The following tasks are not included in the standard transition:

- Physical installation and or connectivity of any infrastructure
- Cabling of any device
- Upgrading and or patching device firmware
- End user support

Sensitivity Label: General