Asset Tracking and Analytics Service Service Element

1 Definitions and Interpretations

1.1 In this document:

"Asset" means any Cisco discoverable device the client has in its IT environment and is discoverable via the Cisco discovery tool (i.e. it needs to be on a routable and discoverable network). Such device may be supported either by NTT or a third party, and may or may not have an underlying Cisco maintenance contract associated with it (as "Asset Tracking and Analytics Service Client Take-on Questionnaire" means the questionnaire that the client is required to complete in order to assist NTT in gathering the necessary information and resources to deliver on the Asset Tracking and Analytics (AT&A) service.

"Cisco Partner Support Service (PSS)" means NTT will be supported by Cisco as a service partner in the delivery of support services to NTT's end clients.

"Cisco SmartNet (SNT)" means the classic Cisco post-sales service which is sold as a product, and delivered from Cisco to the Client directly.

"End-of-X Data" means the vendor data in respect of an Asset or Configuration Item pertaining to the point at which the relevant Asset and/or Configuration Item will no longer be manufactured or supported by NTT, as determined by NTT based on any End-of-Life, end-of-service, end-of-sale, end-of-contract renewal, end-of-engineering, or end-of-software-maintenance announcements made by the manufacturer.

"NTT Management System" is a generic term used to describe the various systems used by NTT in connection with the supply of its Services. Generally, ITSM would qualify as the NTT management system further detailed in clause 5.1 hereunder.

"Service Portal" means the internet portal created and configured by NTT for access by the Client as part of the Services.

"Uptime Agreement" means the agreement dated on the date specified in the Agreement Details.

1.2 Any other terms used in this document not defined above shall have the meaning given to them in the Uptime Agreement.

2 Pre-requisites

The Client's obligations

2.1 The Client must complete the *Asset Tracking and Analytics Service Client Take-on Questionnaire* accurately that provides NTT with the necessary information to deliver the Service before Client Take-on can commence.

2.2 The Client must have an existing Uptime contract with NTT.

Transition

3 Project Manager

The Client's obligations

3.1 If NTT has appointed a Project Manager, the Client must assign a dedicated Project Manager to liaise and cooperate with the NTT Project Manager and to manage the Client Take-on.

4 Asset Tracking and Analytics Service Client Take-on Questionnaire

NTT's obligations

4.1 Using the completed Asset Tracking and Analytics Service Client Take-on Questionnaire, NTT must assess and validate the answers from the Asset Tracking and Analytics Service Client Take-on Questionnaire with the Client for completeness and accuracy.

5 Contract administration

NTT's obligations

5.1 NTT must set-up and configure the Client's contract information in the NTT Management System.

6 Service Portal set-up and instruction

NTT's obligations

6.1 NTT must:

(a) configure the Service Portal to enable the Client to access the Asset Tracking and Analytics Service home page;
(b) provide the Client with Service Portal login credentials requested;
(c) provide one Service Portal awareness training session, for up to five of the Client's employees, on the following topics:
    (i) reports produced by NTT as part the Service; and
    (i) the procedure for logging Incidents and Service Requests with the Service Desk; and
(d) delivery of the Service Portal awareness training session:
    (i) during Business Hours; and
    (ii) via a medium and for a duration agreed with the Client.

The Client's obligations

6.2 The Client must verify the accuracy of the information presented in the Service Portal and advise NTT of any errors and/or required changes.

7 Implementation of site-to-site connection

7.1 A dedicated connection between the Client network and NTT's network is required for the provision of the Services.

7.2 NTT's provision of the Service is subject to the availability and minimum bandwidth specification (as advised by NTT from time to time) of the connection.

NTT's obligations

7.3 NTT must:
(a) conduct a requirements-gathering exercise with the Client and determine the most suitable connection and implementation approach, and document the outcomes in a Connectivity Design document;
(b) review the standard precautions taken to ensure the security of the Network and discuss any specific security requirements relating to secure remote connections the Client may have based on its security policy;
(c) implement the connection as specified in the Connectivity Design document; and
(d) if required, implement any agreed Client security requirements at an Additional Charge.

The Client's obligations

7.4 The Client must:
(a) perform the required tasks to implement the connection; and
(b) ensure adequate firewall rules are in place to allow NTT access to the Assets and/or Configuration Items as outlined in the *Connectivity Design* document.

7.5 If on-premises NTT equipment is required for the site to site connection, the Client must:
(a) have access to the Internet at its site;
(b) allocate a public IP address;
(c) provide adequate rack space and power; and
(d) protect the on premises equipment from loss or damage and return it to NTT at the end of the Term.

7.6 If the Client's own on premises equipment is to be used, the Client must:
(a) provide NTT with the equipment specifications in order for NTT can assess and approve its suitability; and
(b) make configuration changes to the equipment as recommended by NTT.

8 Service delivery enablement and acceptance

NTT's obligations

8.1 NTT shall commence delivery of the Service Features once:
(a) connectivity has been provisioned;
(b) the Service Portal has been established;
(c) the Service Portal awareness training has been provided; and
(d) the Transition process has been completed.

Services

9 Automated discovery

Limitations

9.1 The automated discovery Service Feature is currently limited to Cisco Assets only.

9.2 At least one Asset must be on a Cisco PSS agreement to deploy the AT&A collector.

9.3 The duration taken to complete the Asset discovery is dependent on the size of the Client network (around one day per 1,000 Assets).

NTT's obligations

9.4 NTT will:

(a) perform an automated discovery of the Client's Assets using a discovery tool deployed in NTT's Global Service Operating Architecture;

(b) capture the Asset information from the discovery;

(c) following the automated discovery, enrich the Asset data using Cisco's and NTT's enrichment applications to provide additional Asset data including (but not limited to):

(i) End-of-X Data;

(ii) field notifications;

(iii) security alerts; and

(iv) NTT's service coverage.

9.5 NTT will:

(a) perform an Asset discovery on the Network;

(b) discover Assets by discovery protocols as specified in the Asset Tracking and Analytics Service Client Take-on Questionnaire; and

(c) perform the obligations set out in this clause 9.5 during Business Hours.

The Client's obligations

9.6 The Client must:

(a) provide information reasonably required for the Asset discovery ten Business Days prior to the scheduled commencement (this includes logging a request to update any of the information provided in the initial Asset Tracking and Analytics Service Client Take-on Questionnaire if there has been a change in the Client network, e.g. new network segments and respective security rule changes);

(b) complete the configuration of firewalls and other security measures to enable the Asset discovery on the Network five Business Days prior to the scheduled commencement;

(c) notify its operational and security teams, and implement appropriate change controls, so as not to cause "false positive" security alerts, prior to the scheduled Asset discovery;

(d) make a member of the Client's network team available to assist configuring firewalls, update access lists and generally supply any Client-specific data to make the discovery more successful;

(e) provide and/or update NTT with network authentication information to facilitate the Asset discovery;

(f) provide NTT with a management IP address that is included in ACLs and all firewall rules;

(g) allow NTT to poll the Client's IP address space as per the Asset Tracking and Analytics Service Client Take-on Questionnaire;

(h) if required, allow NTT to connect a PC to the Client network;

(i) ensure that a member of the Client's network team is available throughout the discovery and data collection phase to assist with any Client network issues at that time;

(j) ensure that a member of the Client's security team is available throughout the discovery and data collection phase to assist with any security or access issues which may arise;

(k) provide information to NTT that is accurate and complete;

(l) if required, ensure NTT's equipment left on the Client's premises to collect information will be safe and secure; and

(m) advise NTT in a timely manner of any delay to the scheduled dates.

The Client's authority

9.7 The Client hereby authorises NTT to:

(a) perform an Asset discovery, or Network scan on the Network in whole or in part at the agreed frequency;

(b) collect and collate the data produced by the Asset discovery; and

(c) provide the data to the relevant manufacturer, including those outside Australia, to enable NTT to obtain the end of sale and end of support dates, product notifications, security breach alerts and other information.

9.8 All information collected by NTT will be treated as the Client's confidential information.

10 Interactive Asset Data Reporting and Analytics

NTT's obligations

10.1 NTT must:

(a) provide the Client with access to an inventory of the discovered Assets and associated Asset data via NTT's Service Portal

(b) present the enriched Asset data in NTT's Service Portal;

(c) *present the following Asset Tracking and Analytics Service reports and Service Functionality via the Service Portal:*

(i) *summary dashboard* – a view of the high-level details of the Assets;

(ii) *vulnerable items report* – an overview of Assets that require immediate attention split into two categories;

A. "vulnerable", where (based on the Client specific configuration) a vulnerability is relevant; and

B. "vulnerable not verified", where not enough detail on the Client specific configuration is known but where an Asset model-specific vulnerability is known;

(iii) *outdated items report* - an overview of outdated or out of contract Assets;

(iv) *Assets becoming outdated soon* - an overview of Assets which will require the Client's attention to refresh equipment in the near future;

(v) *comparison report* – a comparison of the Asset summary view with a point in time in the past to allow the Client to view changes from discovery to discovery and to provide trend information; and

(vi) *advanced analysis* - the functionality to apply multiple filters and selection criteria depending on its specific needs and provides an export function into csv and/or excel format;

(d) make the Asset Tracking and Analytics Service reports available via the Service Portal within five Business Days, as a service level target (or multiples of 5 [Business Days] for every 1,000 Assets that are discovered) after the scheduled discovery; and

(e) if requested by the Client, update the NTT Management System with the data provided from the Asset Tracking and Analytics Service reports.

The Client's obligations

10.2 The Client must:

(a) review the information presented in the Asset Tracking and Analytics Service reports and, if required, request NTT make changes to Assets and associated information in the Asset list; and

(b) remain responsible for the Asset list information and approving all changes that NTT makes to Asset list.

11 Service Portal

NTT's obligations

11.1 NTT must:

(a) configure and maintain a Service Portal that provides the Client's IT management and technical support staff access to information relating to the Service, 24 hours a day, seven days a week;

(b) provide the following functionality in the Service Portal:

(i) conduct a post implementation review;

(ii) log Incidents and Service Requests;

(iii) query the status of Incidents, and Service Requests; and

(iv) view:

A. Predefined Service reports; and

B. Asset records.

The Client's obligations

11.2 The Client must:

(a) only allow authorised employees to have an account and access the Service Portal;

(b) ensure all users protect their user accounts and passwords with care;

(c) ensure responsible use of the Service Portal and will not attempt unauthorised access or unethical hacking; and

(d) notify NTT if accounts are to be deleted when employees leave their company.