Schedule document

N4MDM

PUBLIC
Node4 limited
03/08/2020

Schedule document

N4MDM

This Schedule contains additional terms, service description and service level agreement applicable to the N4 End Point Management Service and should be viewed with associated Order Form, Node4's General Terms and Conditions.

1. Service description

N4MDM provides a managed suite of security controls for mobile devices, monitored by Node4 SOC. The different service features of N4MDM are described below.

Information discovered by the service will be critical to the security integrity of the client. It is important that the information from the service is escalated to the appropriate areas within the client's organisation that mitigating actions can be taken by the clients IT department.

2. Definitions

"Fees" means fees as described in this schedule and where relevant set out in the Order Form, and shall be payable by the customer in accordance with Clause 6 of Node4's Standard Terms and Conditions;

"Exploit" A method to use a Vulnerability to gain unauthorised access to functions, data, or privileges with malicious intent. An exploit can include a script, virus, Trojan, or a worm. The exploit is mainly defined by the way it replicates and spreads. An attack is the use of an Exploit.

- A script refers to a document with steps to manually find and exploit vulnerabilities. A script is replicated by publishing it.
- A virus refers to malicious software attached to a medium (e.g., files, removable media, and documents). A virus replicates using this medium.
- A Trojan refers to malicious software embedded in applications. The Trojan will not replicate itself; it spreads with the application.
- A worm refers to a self-contained program (or set of programs) that spreads copies to other computers. A worm can spread through network connections and e-mails in a matter of hours.

"Incident" means an unplanned interruption to a service or a reduction in service quality

"Installation Fees" means fees payable by the customer for the installation of Firewall Services as provided in the Order Form;

"Service Desk" means the single point of entry for all Service Tickets and Service Requests which can be accessed over the phone, by email or via our portal. **"Service Request"** means a request for a change or for information which can be completed within 30 minutes by a support engineer

"Service Ticket" means the tickets which are raised in relation to Incident or Service Request

"SOC" means Security Operations Centre.

"Threat" A (suspected) use of an Exploit, or the (suspected) presence of a Vulnerability in the configuration, platform, of application code. A Threat can be an infection by a worm or virus, or it can be a targeted attack. Exploits can also combine into Blended Threats, exploiting multiple security weaknesses or defects

"Threat Signature" Code used to recognise a Threat by its pattern. A Threat Signature may contain algorithms to detect dynamically changed malicious behaviour, combat obfuscation, or impersonation.

"Vulnerability" A weakness or defect that can be exploited to gain access to data, functions, or privileges violating the intended authorisation. Vulnerabilities can range from defects in application or system software (e.g. bugs), in the user administration (e.g. non-protected user accounts), in the configuration (e.g. unintended network or file access), in the policy and rule set definition (e.g. unrestricted open ports or exposed IP-addresses), etc. The combination of all vulnerabilities of a given system or infrastructure is the exposure.

3. Specific terms

The following terms and conditions shall apply when Node4 provides N4MDM Services to the Customer.

3.1 Termination of service

Upon the termination or cessation of the service the customer is obligated to remove all N4MDM licences from devices and infrastructure within 1 month of the end of service date.

3.2 Customer indemnity

N4MDM involves the use of network scanning and testing technology that has inherent risks, including, but not limited to, the loss, disruption, or performance degradation of a customer's or a third party's business processes, telecommunications, computer products, utilities, or data (the "Scanning and Penetration Tests Risks"). The customer authorises Node4 to perform the network scanning and assumes all risk for adverse consequences resulting from or associated with such component of N4MDM.

Node4 shall take reasonable steps to mitigate these Scanning Risks; however, the customer understands that these Scanning Risks are inherent in the provision of certain computer security services and the use of certain computer security products and cannot be eliminated.

The customer shall indemnify and defend Node4 for all costs and expenses related to a third party's claim of loss, damages and liabilities (including legal expenses and the expenses of other professionals) incurred by Node4, resulting directly or indirectly from any claim attributable to or arising out of Node4's use of network scanning technology (each, a "Scanning Claim"), including, without limitation, the use by Node4 of network scanning technology to analyse assets that are not controlled directly by the customer, including, without limitation, servers hosted by third parties. This obligation of the customer in connection with a Scanning Claim shall not apply if Node4's gross negligence or wilful misconduct gave rise to such Scanning Claim.

3.3 Warranty

Node4 does not warrant that N4MDM will detect and prevent all possible threats and vulnerabilities or that such services will render the customer's network and systems invulnerable to all security breaches and vulnerabilities.

The customer hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Node4. Customers will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys' fees) and liability of any kind that may be incurred as a result of customer's breach of the foregoing warranty.

4. Fees

Installation and reoccurring Fees will commence when Ready For Service Notification is provided by Node4, this will follow the installation of the solution.

4.1 Installation fees

Any applicable set-up Fees for the implementation of the support service as detailed on the Order Form.

4.2 Reoccurring fees

Service Fees paid either monthly or annually in advance based on the support provided and any other related service and are identified on the Order Form.

4.3 Additional professional services

A full range of Professional Services are available to the customer in addition to what is provided as part of the support contract. The Professional Service Fees include but are not limited to:

- Installation and configuration
- Remote services
- Management

The Professional Services are subject to the price list below. Specific rates for large or repeat orders can be agreed on a case by case basis in writing.

All incremental expenses incurred during these Professional Services will be passed directly to the customer. Provisioning costs such as cabling will be discussed and agreed with the customer in the Order Form.

Tasks undertaken by Node4 at the request of the customer or activities undertaken by the customer which require the remote support of Node4 personnel will be charged at the hourly rates shown below.

Time Support Required:	Per Hour

Mon – Fri 07.00 – 19.00	£80.00 Per Hour
All Other Times	£120.00 Per Hour

Time is charged by the hour. These rates are for a support / provisioning engineer and are subject to an annual review by Node4.

5. Service provision

5.1 Service features

N4MDM Standard

- Access Portal
- SSO
- MFA
- Conditional Access
- Email management
- Mobile App Management
- Mobile Device Management

N4MDM Advanced

- Advanced Desktop Management
- Per-App VPN Tunnelling
- App Wrapping
- Content Locker App
- Boxer App
- Secure Browser App
- Email Gateway
- Risk-based conditional access

N4MDM Enterprise

- Virtual Apps and Desktops

5.2 Implementation

Prior to commencement of N4MDM, Node4 will schedule a Deployment meeting to introduce the N4MDM service delivery team, identify the appropriate contacts for Customer, discuss the scope of the N4MDM service and its business impacts, and obtain a completed Request for Information Schedule (RFIS) from the customer.

Upon receipt of completed RFIS, Node4 shall create a proposed project plan with key milestones, Phase Checkpoint Reviews and time-scales. N4MDM will only be provisioned after the customer has approved the project plan. During the implementation of the N4MDM, the customer may propose changes to the project plan or the N4MDM service. Node4 will assess the customer's proposal and may require the customer to submit a new Service Order or Amendment to reflect the approved changes.

5.3 Centralised management

Node4 SOC will manage administration tasks and MACs for the Customer. Customer Service Requests for highly secure actions, such as password reset will only be processed once authorisation has been established by a call back to a known authorised contact number.

5.4 Management reports

The reports functionality allows you to access detailed information about the devices, users, and applications in your N4MDM solution. The exports of these reports are in CSV format.

5.5 Device enrolment

The enrolment process may differ slightly depending on the device platform. Node4 SOC will provide assistance via standard ticketing process. Device models are restricted to Apple (iOS/MacOSx), Android and Windows.

5.6 Profiles and policies

You can think of profiles as the settings and rules that, when combined with compliance policies, help you enforce corporate rules and procedures. They contain the settings, configurations, and restrictions that you want to enforce on devices. Each device type can have device specific profiles. Profiles and Policies must be provided by the Customer.

5.7 Applications (Apps)

Apps are classified as internal, public, purchased and web which are deployed to the devices in accordance with profiles and policies as defined by the Customer.

5.8 Self service portal

Customer access to the self-service portal will be restricted to the service / support roles. The Portal provides the tools necessary for most Level 1 service desk functions. The primary tool available in this role is the ability to see and respond to device info with remote actions. However, this role also contains report viewing and device searching abilities

5.9 Security service advisor

The services contain allocated time per month for a Security Service Advisor to consult with the customer. This time cannot be transferred or rolled over to earlier or later months.

5.10 Moves, adds and changes

Node4 will provide a Service Request service. This will cover configuration changes and addition or deletion of devices, users and policies. The service is available on an allocated number of Service Requests per month., . Service Requests cannot be combined or carried over to the next month. Non-standard changes requests will be charged at the appropriate Professional Services rates. The number of included monthly standard MAC tickets is identified on the order form.

5.11 Exclusions

Node4 does not provide onsite installation, architectural and policy design services under N4MDM service. N4MDM service also does not include policy and configuration reviews, initial setup or maintenance of configuration on Subordinate Devices or migrations from management stations located on the customer's premises to management stations hosted the SMC or from third-party owned management stations to management stations either located on the customer's premises or hosted in the SMC. All of these excluded services, however, can be conducted by Node4 under a separate agreement.

6. Asset management

6.1 General

If defined on the Order Form Node4 asset management service captures and updates key information about managed devices into a CMDB portal, assigns a unique asset number from the service tag and provides reporting via a Customer accessible online portal and as part of the existing scheduled service reviews.

6.2 Asset entity definition and data

Assets which can be included are defined as either Online or Offline

Online Asset – an asset that can have an agent installed / respond to polling (smart phone and tablets) - Data is updated at point the agent is polled or checks in, most recent data is therefore at the point the devices was last seen online. The following online assets can be included

- Smart Phone
- Tablet

For online assets the following information will be captured

Online asset data fields
Date Purchased
Vendor Serial #
Warranty or Support Subscription
Warranty or Support Expiry
Asset Tag (Physical)
Client Acc #
Registered User / Stock Location
Previous Registered Users
Accountable Manager
Last Audited Date
Registered Location of Asset
Installed Operating System
Patch Status
Last Seen When?
Last Seen Where?
Repair History
Parent/Child Relationships
MAC Address
Device Name

Offline Asset – a 'dumb' asset that cannot have an agent installed (licence / projector / peripherals etc). Data is updated manually at point of change. The following offline assets can be included

- GSM/LTE Modem (USB)
- SIM Card

For offline assets the following information will be captured

Offline asset data Fields
Date Purchased
Vendor Serial #
Warranty or Support Subscription
Warranty or Support Expiry
Asset Tag (Physical)
Client Acc #
Registered User / Stock Location
Previous Registered Users

User Profiles Present
Accountable Manager
Last Audited Date
Registered Location of Asset
Installed Operating System
Repair History
Parent/Child Relationships
MAC Address
Device Name

6.3 Asset tags

If defined on the Order Form Node4 will provide tamper proof asset management stickers which include a barcode and unique identifier.

A service for applying the tags to devices is available on request at an additional cost.

6.4 Reporting

Reports will be included in any existing scheduled service reviews.

A portal is provided with read only access for the Customer with the ability to produce summary reports of the assets being managed. Access to the portal is optionally secured using Single Sign On (SSO) authentication, (SSO service available separately).

6.5 Online asset service dependencies

The asset management services are depended upon Node4 MDM for OS reporting, last seen location, remote wipe etc.

7. Incident management

This section refers to Incidents and management pertaining exclusively to the service portal for the N4MDM service and does not include any customer systems or customer infrastructure.

7.1 Incident handling

Incident are handled as outlined in the Incident Management Service Schedule Document.

7.2 Hours of support

The following table details the different Support Hours relating to the Support Level defined on the Order Form (if not defined Bronze support, is provided as standard on N4MDM Services).

Support Level	Support Hours
Bronze	Standard business hours support 9am to 5.30pm week days, excluding bank and national holidays
Silver	Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Silver Plus	Priority 1 and 2 - Support hours between 7am and 7pm 7-days a week, including bank and national holidays, excluding Christmas day, Boxing day and new year's day Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Gold	Priority 1 and 2 - Support hours 24/7 Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays

7.3 Incident priority

Each new Incident will be assigned a priority level by the Service Desk based on the following definitions. These levels allow us to prioritise resources and escalate where appropriate.

Priority	Description
1 - Critical	A major Incident resulting in total loss of service.
2 - High	A major Incident resulting in a severe service degradation or loss of service to a significant percentage of users.
3 - Medium	A minor Incident resulting in a limited or degraded service or a single end user unable to work.
4 - Low	General, single user with degraded service, non-service affecting support.
5 - Service Request	Request for a change to an existing service or system, a request for information or simple questionnaire to be completed.

7.4 Time to repair

Node4 aims to respond, update and resolve Incidents in relation to the N4MDM service within the following times

Priority	P1	P2	P3	P4	Change
Response / Acknowledgement	30 Mins	1 Hour	2 Hours	4 Hours	12 Hours
Commencement	1 Hour	2 Hours	4 Hours	N/A	N/A
Frequency of Updates	30 Mins	2 Hours	12 hours if Resolve / Target to Fix exceeded		
Resolve / Target to Fix	5 Hours	8 Hours	12 Hours	36 Hours	60 Hours

All category 1 & 2 Incidents should be raised via the Service Desk system then followed by a phone call.

* Acknowledgement refers to an automated service which generates a response and alerts engineers of a service failure; or where there is dialogue between the client and the engineer.

Service Requests outside of the support contract, or change request implemented outside normal business hours these will be dealt with as chargeable projects.

7.5 Incident duration

All Incidents recorded by the monitoring system will be reconciled against the corresponding Service Ticket raised by the Service Desk. The exact Incident duration will be calculated as the elapsed time between the Service Ticket being opened and the time when service is restored.

7.6 Maintenance window

Where Node4 plans to perform essential works on the portal, Node4 will endeavour to perform such works during low traffic periods and will endeavour to give the Customer at least five (5) days prior notice. In the event of an emergency or Service affecting Incident such notice may be less than 24 hours.

8. Service credits

Service credits are not available for N4MDM Services.