NODE4

Empowering business to do more

Schedule Document

FortiClient Endpoint Service

Node4 Limited

01/06/2024

Schedule Document

FortiClient Endpoint Service

This schedule contains additional terms and conditions, service description and service levels applicable to the FortiClient Endpoint Service and should be viewed with associated Order Form, Node4's General Terms and Conditions and the Acceptable Use Policy.

1. Overview

FortiClient Endpoint Service provides the Client with FortiClient endpoint software along with additional Node4 management services to deliver an endpoint VPN and security capability.

2. Definitions

"Client Responsible Incident" means in the event that a Service Affecting or Non-Service Affecting Incident is identified as being attributable to Client Provided Equipment, Premises, Client power supplies, or the action of the Client, employees or agents of the Client, the Incident shall be deemed the responsibility of the Client. Any downtime shall not be included in service availability measurements and does not qualify for compensation.

"Compute Resource" means a pool of memory (RAM) and processor (vCPU) on shared virtualisation hardware on which the Client runs Virtual Machines.

"FortiClient" means the Fortinet FortiClient endpoint agent software product, which is an endpoint Virtual Private Network (VPN) and protection client.

"FortiClient EMS / EMS" means the Fortinet FortiClient Enterprise Management Server (EMS) software product, which is a software package that provides centralised management capabilities for FortiClient endpoint agent software.

"FortiGate" means the Fortinet FortiGate network firewall, which is a physical or virtual appliance providing network security capabilities.

"Hypervisor" means hardware and software used to create and run Virtual Machines allowing multiple operating systems to run concurrently on a single host computer.

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

"Installation Fees" means charges payable by the Client for the installation of Services as provided in the Order Form.

"IPsec" means the Internet Protocol Security suite that enables encryption of communications between two endpoints connected to an Internet Protocol network.

"License" means a perpetual or user based or other software license as required to be purchased under the terms of a software license agreement from a Third Party Software Vendor.

"Monthly Review Period" means the calendar monthly periods commencing on the 1st of each month during the Term, over which Service performance measurements are calculated, provided that the first Monthly Review Period will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client.

"Node4 Network" means the network wholly owned and managed by Node4.

"Non-Service Affecting Incident" means a Incident or condition which is not a Service Affecting Incident.

"Planned Outage" means proactive work required to maintain the service provided, Node4 may with reasonable notice require a temporary outage in service. Wherever possible Node4 will agree the outage with you in advance of the required work. Any planned downtime shall not be included in Incident or service reliability measurements.

"Service Affecting Incident" means any failure of Node4 service, which, in our reasonable opinion causes a loss of a Client's service. In all such cases the service shall be deemed unavailable and the length of downtime recorded by Node4 from when the Incident is registered by Node4 and a Service Ticket allocated.

"Service Availability" means the time for which a Node4 service is usable, expressed as a percentage of the total time in a given Monthly Review Period. The Node4 service shall be deemed available for the purposes of calculating Service Availability if it is not usable due to an event outside our reasonable control, a Client Responsible Incident, a Third Party Attributable Incident or is due to a Planned Outage.

"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 for information.

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

"SSL / TLS" means Transport Layer Security (TLS), often referred to interchangeably with the legacy term Secure Sockets Layer (SSL), which are cryptographic protocols designed to enable secure communications over a computer network.

"Third Party Attributable Incident" means in the event that a Service Affecting or Non-Service Affecting Incident is identified as being attributable to a third party this measurement period shall not be included in service availability measurements. Such Incidents do not qualify for rebates or compensation. Node4 will endeavour to resolve and rectify such Third-Party Attributable Incidents as soon as possible.

"Virtual Machine" means an operating system instances running on Compute Resource.

"Virtual Private Network (VPN)" means encapsulated communications between computers on a network, typically with encryption, designed to provide secure and private transfer of information over an untrusted or insecure network.

3. Specific terms

The following terms and conditions shall apply when Node4 provides the FortiClient Endpoint Service to the Client.

3.1 Disclaimer

FortiClient software will not detect and prevent or make the Client invulnerable to all possible threats and attacks.

3.2 Third parties

The Client commits to fully manage all their customers and suppliers directly. Node4 will not interface directly with any third parties working with the Client unless by prior arrangement. If the Client requires Node4 to provide their customers with a customer care or NOC service this is available on request and subject to Professional Service Fees.

Node4 shall not be liable in respect of any contract, agreement or relationship that Client may have with any third party. If a dispute arises between Client and a third party involving Node4's FortiClient Endpoint Service, Node4 shall provide the Client with reasonable information and assistance (to the extent that such is not adverse to Node4's interests to Client (at Client's expense)) in the resolution of such dispute.

4. Fees

Fees will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client.

Fees may comprise any or all of the following.

4.1 Installation and set-up fees

Any applicable Design, Configuration, and Installation Fees for the implementation of the FortiClient Endpoint Service shall be detailed on the Order Form.

4.2 Monthly fees

Monthly Fees are paid in advance. Monthly Fees for FortiClient Endpoint Service are associated with the total number of endpoints on which FortiClient software will be installed and the licensed feature level required by the Client. The total endpoint quantity and license tier will be detailed on the Order Form.

4.3 Professional service fees

Additional tasks undertaken at the request of the Client by Node4 personnel, will be charged at rates agreed between the parties in advance.

5. Client responsibilities

To deliver and support the FortiClient Endpoint Service we expect the Client to provide:

- Details of endpoint types and quantities in scope.
- Specification of requirements for FortiClient software on endpoints in scope.
- Liaison with Node4 engineering, provisioning, and project management teams to facilitate deployment.
- Liaison with Node4 Client Support teams to facilitate endpoint software support.
- Provide training and support to end users on how to use the FortiClient software and connect to remote access VPN where appropriate. Node4 typically support this training activity by preparing user guides and documentation and delivering "train the trainer" type sessions.
- Support of individual user and endpoint issues, where the FortiClient Endpoint Service infrastructure is available and operational.

Where the Client supplies user or multi-factor authentication systems for use, the Client will be expected to:

- Validate compatibility between FortiGate, FortiClient and the proposed multi-factor authentication system with their vendor.
- Appropriately configure the user or multi-factor authentication system for use and integration with FortiGate and FortiClient.
- Troubleshoot any issues with the user or multi-factor authentication system and liaise with the system vendor as required.

Where the Client does not take the FortiClient endpoint deployment service from Node4, the Client will be expected to:

- Configure software deployment or endpoint management systems to install the FortiClient software on endpoint devices in scope. Node4 will supply the FortiClient software package to the Client for supported systems.
- Ensure that software deployment or endpoint management systems are able and configured to regularly update or patch FortiClient software on endpoint devices in scope. Node4 will supply updated FortiClient software packages to the Client where requested and appropriate.
- Verify the installation or update/patch of the FortiClient software on endpoint devices in scope.

6. Service provision

Node4 FortiClient Endpoint Service is for the supply and usage of FortiClient software, associated licensing and Node4 professional and support services.

6.1 Supported Versions

Node4 will support versions of FortiClient software in line with the vendor product lifecycle policy. Where the vendor announces end of support for a product version, Node4 will also cease support of those versions.

6.2 Licensing

Client must license the total quantity of endpoints that FortiClient software will be deployed to, with the appropriate license tier to enable all the features they wish to utilise.

Node4 may not support all the features and capabilities of all license tiers. Features that Node4 will support are detailed in the Supported Features section of this document.

6.3 Firewall Support

Client must have a FortiGate firewall of an appropriate specification to support the quantity of FortiClient endpoints that will utilise the remote access features.

6.4 Installation

Node4 will deploy the FortiClient EMS centralised management software for the Client as agreed in a prior Statement of Works (SoW). Node4 will agree requirements with the Client and configure the FortiClient endpoint software package with the necessary features and functionality.

Node4 will validate the service configuration as part of the installation.

Inclusive within the service, Node4 will supply the produced software installation package to the Client for them to install to endpoint devices in scope, using the methods or tools of their choice. Node4 can discuss and advise on general best practices for this as required.

Optionally, and where specified on the Client Order Form, Node4 can deploy the FortiClient software installation package to Client endpoint devices using our supported list of tools. Node4 will advise on tools supported by this service as part of the pre-sales engagement, the output of which will be detailed in a Statement of Works (SoW). The Client must have or purchase appropriate licensing for the relevant tools for Node4 to deliver this option.

6.5 FortiClient EMS Centralised Management

FortiClient EMS software will typically be supplied where centralised management of FortiClient endpoint software is required. This may be deployed by Node4 on a Microsoft Windows based server hosted on Node4 infrastructure.

Alternatively, Clients may opt to host the FortiClient EMS software on their own infrastructure and Microsoft Windows based server. It will be specified on the Client Order Form if Node4 are providing FortiClient EMS as a hosted service.

6.6 Supported Features

Node4 will support the following features of the FortiClient endpoint software.

6.6.1 Remote Access (SSL + IPsec)

FortiClient remote access provides client dial-in connectivity to FortiGate firewalls for secure access to internal networks. This connection can be encrypted using IPsec or SSL/TLS. Node4 will configure and support this feature for Clients where required.

Where Node4 also manage the FortiGate firewall we will also support with the changes required to enable the client VPN services on these firewalls.

6.6.2 User Authentication

FortiGate firewalls support multiple authentication system integrations for use with FortiClient VPN, including LDAP, RADIUS and PKI certificate infrastructure. Where the Client specifies the user authentication system to be used, they should validate compatibility between FortiGate FortiClient and their chosen system with their vendor in advance. Node4 will configure and support this feature for Clients where required and in line with the Clients requirements.

6.6.3 Multi-Factor Authentication

FortiGate firewalls support several multi-factor authentication systems for use with FortiClient VPN. Where the Client specifies the multi-factor authentication system to be used, they should validate compatibility between FortiGate FortiClient and their chosen system with their vendor in advance. Node4 will configure and support this feature for Clients where required and in line with the Clients requirements.

6.6.4 SSO Mobility Agent

FortiClient SSO mobility agent reports username and IP address information to FortiAuthenticator appliances for transparent authentication. Node4 will configure and support this feature for Clients where required.

A separate FortiAuthenticator appliance is required to utilise this feature which is not included within the FortiClient Endpoint Service.

6.6.5 Logging & Reporting

FortiClient software can transmit endpoint and traffic log information to FortiAnalyzer appliances for storage and analytics. Node4 will configure and support this feature for Clients where required.

A separate FortiAnalyzer appliance is required to utilise this feature which is not included within the FortiClient Endpoint Service.

6.6.6 Web Filtering

FortiClient web filtering provides the capability to analyse user web traffic in real-time to monitor and optionally take action on website access ,where those web assets have been analysed and appropriately categorised. Node4 will configure and support this feature for Clients where required.

Clients will be required to define their internet/web access policy and specify the actions they wish to be implement for each defined web category. Node4 can discuss and advise on general best practices for this as required.

6.6.7 Application Firewall

FortiClient application firewall provides the capability to analyse user web application traffic in real-time to monitor and optionally take action on application usage, where those applications have been analysed and appropriately categorised. Node4 will configure and support this feature for Clients where required.

Clients will be required to define their application usage policy and specify the actions they wish to be implement for each defined application category. Node4 can discuss and advise on general best practices for this as required.

6.6.8 Software Inventory

FortiClient software inventory provides the ability to report on software usage for endpoints with FortiClient installed. It will also identify the versions of installed applications where possible. Node4 will configure and support this feature for Clients where required, except for the software patching functionality which Node4 will not support for unmanaged endpoints.

6.6.9 Vulnerability Scan

FortiClient vulnerability scanning will attempt to identify known vulnerabilities for software on endpoints with FortiClient installed. Node4 will configure and support this feature for Clients where required, except for the software patching and vulnerability remediation functionality or activities which Node4 will not support for unmanaged endpoints.

6.7 Service Exclusions

FortiClient Endpoint Service neither offers nor provides:

- Endpoint or user management services.
- Support of individual user and endpoint issues, where FortiClient Endpoint Service infrastructure is available and operational.
- Use of FortiClient EMS to deploy to endpoints that are not Microsoft Windows based and are not on the FortiClient EMS deployment feature supported Operating Systems list.
- Endpoint software patching or vulnerability management.
- FortiClient Anti-Virus features where other Anti-Virus solutions are installed on endpoints.
- Centralised authentication where an Identity Management platform is not ordered from Node4.
- Multi-factor authentication where a 2FA/MFA platform is not ordered from Node4.
- Storage or archival of logs where a FortiAnalyzer platform is not ordered from Node4. Log retention periods depend on FortiAnalyzer platform sizing.
- Log monitoring, analysis, or reporting.
- Security monitoring, analysis, or reporting.
- Security engineering or consulting.

Where any of the above services are provided by Node4, they are provided as additional services not subject to the terms and clauses in this document.

6.8 Maintenance Window

Where Node4 plans to perform essential works Node4 will endeavour to perform such works during low traffic periods and will endeavour to give the Client at least five (5) days prior notice. In the event of emergency works or a Service Affecting Incident, Node4 will aim to provide notice in advanced and as much advanced notice as possible.

This notice may be provided on N4Status (www.n4status.co.uk) rather than a direct notification. Clients can subscribe to status updates on the N4Status website to receive automated direct notifications.

7. Incident management

7.1 Incident handling

Incidents are handled as outlined in Incident Management Schedule Document.

7.2 Fault duration

All Incidents recorded by the Node4 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.

7.3 Hours of support

Node4 FortiClient Endpoint Service includes Gold level support, as detailed in the table below.

Support Hours	
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.

7.4 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.

7.5 Time to repair

Node4 aims to respond, update and resolve Incidents in relation to the Node4 FortiClient Endpoint Service within the following times:

Priority **(Number are in hours)**	**P1**	**P2**	**P3**	**P4**	**Service Request**
Response / Acknowledgement	0.5 Hours	1 Hour	2 Hours	4 Hours	12 Hours
Commencement	1 Hour	2 Hours	4 Hours	N/A	N/A
Frequency of Updates	1 Hour	2 Hours	12 hours if Resolve / Target to Fix exceeded		
Resolve / Target to Fix	4 Hours	8 Hours	12 Hours	36 Hours	60 Hours

Resolution times in the table above do not apply where there is a Client Responsible Incident, a Third Party Attributable Incidents or events outside Node4's reasonable control, any incidents including these aspects will be excluded from reporting provided.

All priority 1 & 2 Incidents should be raised via the Service Desk by a phone call. Should a priority 1 or 2 incident be raised via the portal or e-mail, the Client is required to follow this up with a corresponding phone call to enable work to commence immediately on the issue.

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 Service Request implemented outside normal business hours these will be dealt with as chargeable projects.

8. Service availability

Node4 will provide the Client with Service Credits, as set out below, for the failure to meet the below service availability objectives.

8.1 Service availability objective

Where Node4 host, deploy and support FortiClient EMS, the following service availability objective will apply:

Service	**Availability**
FortiClient EMS Virtual Machine (hosted on N4Cloud and managed by Node4)	99.95%

8.2 Service credits

Credits will only be provided for failure to meet the availability levels set out above.

The FortiClient EMS virtual machine is considered available if the Hypervisor host hosting the Client Virtual Machine is operating in a normal state and the Client Virtual Machine is powered on.

If a Hypervisor host fails, and the Virtual Machines are migrated to another host, then downtime shall be considered as the time between a) the time the Hypervisor host is detected as no longer functioning and b) the time the Virtual Machines start to power on on another host.

The following equation will be used to calculate the FortiClient EMS virtual machine component availability. References to hours are to the number of minutes in the applicable Monthly Review Period:

((Total minutes – Total Minutes Unavailable) / Total minutes) x 100

Node4 will provide the Client with service credits as set out below for the failure to meet the following targets:

Availability of the FortiClient EMS Virtual Machine	Service Credits as % of Monthly Rental Charge for FortiClient EMS Virtual Machine Component of the FortiClient Endpoint Service
<99.95%-99.85%	5%
<99.85%-99.7%	10%
<99.7%-99.5%	20%
<99.5%-99.0%	25%
<99%	50%

Where a Monthly Review Period incorporates part of a month, any Service credit will apply to a pro-rated Monthly Fee. Service credits will be calculated monthly, aggregated and credited to the Client on a quarterly basis. If a Service is cancelled during a Monthly Review Period, no Service credit will be payable in respect of that service for that Monthly Review Period. The Client must claim any Service credit due to a failure to meet the Service levels, in writing, within twenty one (21) business days of the date at which the Client could reasonably be expected to become aware of such failure. The Client shall not be entitled to any Service credits in respect of a claim unless and until Node4 has received notice of the claim in writing in accordance with the above. Should Node4 require additional information from the Client, the Client shall assist, and shall not be entitled to any Service credits until Node4 has received all the information it has reasonably requested.

8.3 Exclusions to payment of service credits

Service credits will not be payable by Node4 to the Client in relation to the Service Availability for Incidents or disruptions to the Service caused by any of the following:

- The Incident, action or negligence of the Client, its employees, agents or contractors;
- The Client failing to comply with Node4's Standard Terms and Conditions;
- An Incident in, or any other problem associated with, equipment connected on the Client's side of the Node4 Network Termination Point, except where such Incident or problem is directly caused by the action or negligence of Node4, its employees, agents or contractors;
- Any event described in Clause 12 (Force Majeure) of Node4's Standard Terms and Conditions (Schedule 1);
- A failure by the Client to give Node4 access to any equipment after being requested to do so by Node4;
- Planned Outage during any Maintenance;

Service credits are not applicable for more than one breach of any targets outlined in this document arising from the same occurrence.

The provision of Service credits shall be the sole and exclusive remedy for the failure to meet targets for the service. Node4 shall have no additional liability to the Client.