



Elevate[®]

Seamless Secure
Intelligent Networks

Service Description:

Enterprise Managed Services

Effortless.
From ground to cloud.



Version control

Date	Change/Update	User
06/02/2023	First version released	thom@elevate.uk
02/06/2023	Clarification of Co-Management	danny@elevate.uk
23/11/2023	Change in Co-Management section	danny@elevate.uk



Introduction

Description

This Service Description (SD) describes the Enterprise Managed Service offering that Elevate provides for the following products and services

- Enterprise Managed LAN, powered by Juniper Mist AI
- Enterprise Managed WiFi, powered by Juniper Mist AI
- Enterprise Managed Firewall, powered by Fortigate
- Connectivity-as-a-Service (of which managed services are made up of components Enterprise Managed LAN, Enterprise Managed WiFi and Managed Firewall)

This document refers to the above individually or collectively as “Enterprise Managed Services”

Overview

The Enterprise Managed Service includes the installation, configuration, management, monitoring and restoration of the services and equipment in accordance with the SLAs and policies set out below. This includes access to Elevate’s NOC and support from Elevate’s field engineers.

Support

Access to Support

End Users have access to the NOC team of Technical Support Engineers (TSEs) via email and phone. TSEs will respond in accordance with the Priority Level Guidelines below to help diagnose service problems, configure, troubleshoot, and provide work-around solutions where necessary, TSEs can also escalate any support request to senior management.

The NOC is integrated within the broader network and engineering teams which allows for problem escalation to subject matter experts based upon the technical problem.

Opening a Support Ticket

End Users can make service requests and open support tickets with the NOC as follows

- Email: support@elevate.uk
- Phone: 03301 222 970
(during business hours 08:30–17:30 option 1, then option 1. Outside of these hours, option 1)



Priority Level & Response Guidelines

Incident Level:		P1: Critical	P2: High	P3: Medium	P4: Low
Incident Description		Business critical function is down across one or more sites due to performance failures	Business critical function is impaired or degraded at one or more entire sites	Non-critical function is down or impaired and does not have significant current performance impact	Information requests. Non-urgent RMA requests.
Enterprise Managed Services	Examples	Complete site outage caused by Firewall or LAN due to device failure or WiFi due to failure of multiple APs	Partial outage or performance of Firewall, LAN or multiple APs degraded or experiencing random interruptions. Particular function of a device (e.g. SSL VPN, content filtering) not operating resulting in partial loss in services.	Performance is slightly degraded across Firewall, LAN or multiple WiFi APs. Device or function still working, but may be slow or inconsistent.	Information requests or standard questions on configuration or functionality. Standard change requests.
	Support Response	Within 1 hour	Within 4 business hours	Within 8 business hours	Within 12 business hours
	Support Update Frequency	Every 4 hours	Every business day	Every three business days	Every week
	Time to Fix SLA	Within 12 hours	Next business day	Next business day	N/A
	Customer Responsibility	Designated resources that are available 24x7x365 (priority lowered if no response within 1 hour) Ability to provide necessary diagnostic information.	Resources available Monday through Friday during local business hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information.	Resources available Monday through Friday during local business hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information.	Resources available Monday through Friday during local business hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information.

Business hours are: 08:30–17:30 UK, Monday to Friday, excluding UK bank holidays



Elevate Responsibilities

Once an End User initiates a support ticket with the NOC:

- A TSE will:
 - Begin troubleshooting, diagnostics, and problem replication as appropriate.
 - Provide the End User with periodic updates on problem status and escalate the problem as required according to escalation management guidelines, or at the End User's request.
- Hold appropriate spares to carry out our responsibilities
- Alert you if we believe our work will disturb unaffected parts of the network we manage
- Follow any health and safety procedures we have received a copy of, while our employees, agents or subcontractors are on site
- Carry out our responsibilities with due care and attention and in a way that keeps business disruption to a minimum
- Close the support ticket when the End User agrees that the problem has been resolved.

When a TSE updates a support ticket, the End User will receive an email with the update.

Resolution Process

As part of the resolution process, the TSE may take any of the following steps:

- Review configuration/debug information to identify resolution of issue
- Replicate the scenario/issue in a test environment (where possible)
- Troubleshoot live on the affected equipment
- Create and review packet captures to isolate the problem.
- Initiate our field engineer response
- Restore the service by either:
 - Repairing (and installing temporary Elevate equipment whilst the defective Equipment is being repaired if necessary – where this is done, we will replace temporary equipment free of charge)
 - Replacing the defective equipment with equivalent replacement equipment
 - Repairing or reconditioning equipment on the premises if we judge this to be appropriate

Escalations

If for any reason the End User is not satisfied with the progress of its support ticket, the End User can request the NOC to change the priority level of its request, or escalate the request by following the escalations process as defined in the Customer Escalation Guide.



End User Responsibilities

To provide the Enterprise Managed Services you must provide us with the correct environment, information, co-operation, assistance and access to facilitate as we reasonably require to enable us to provide the service. You'll be exclusively responsible and accountable for any charges, liabilities or losses incurred as a result of your failure to meet these requirements and associated general terms and conditions.

- **Environmental** – suitable and industry standard location with power protection free of surges and fluctuations and with suitable air conditioning and humidity control to keep equipment in good working order
- **Access Control** – suitable, controlled and where necessary restricted physical access to ensure equipment is appropriately protected against accidental or malicious physical damage, interference or disruption

Some repair work may be disruptive and so you must not unreasonably withhold permission to do such work, we will give you notice of the repair work and we will not start until you give us your permission to do so.

Proactive Support

All Enterprise Managed Services will be monitored by the vendor supported management platform – Juniper Mist Cloud Services for Enterprise Managed LAN and WiFi and FortiManager for Enterprise Managed Firewall.

If an issue is detected, these systems will notify our NOC and the specified End User email addresses you provide.

Where a proactive alert relates to a loss of reachability of a device or site, our incident response can be triggered 24x7 by contacting our NOC to open a support ticket and confirm normal environmental conditions (including power supply) and when physical access can be provided.

Where a proactive alert relates to a degradation in service, this will be automatically assigned a P3 priority, which will be elevated as necessary and worked independently by the NOC in accordance with specified response times.

Co-Management

Where the service is deployed as "Co-Managed", you will be given limited read or write access to the management portals for the Enterprise Managed Services. Limited write access is provided on the basis that anyone making changes has sufficient training and experience to do so. Where write access is provided and a change you make causes a fault, your first action should be to revert the change. If an incident is triggered with us in relation to a configuration change you make, and where the change configuration and time hasn't been agreed with us, the ticket will be



prioritised as a maximum of a P2 and may result in a charge in accordance to clauses 6.3 and 8.9 of the Elevate General Terms and Conditions

Our SLAs, priorities, incident management, maintenance and change management otherwise remain the same.

Managed Workspace

In instances where Enterprise Managed Services are deployed within a multi-occupancy setting, such as a co-working space or serviced office, Elevate is proficient in offering additional comprehensive support. Our expertise extends to adeptly managing the diverse needs of multiple tenants and engaging directly with each end-user on a per-ticket basis, ensuring a seamless and efficient operational multi-user environment. Included with Managed Workspace is:

- Liaising with individual occupiers and end-users on setup
- Liaising with individual occupiers and end-users in support tickets
- Additional support for multiple WiFi SSIDs
- Additional support for individual tenant LAN networking
- Scope to add specific tenant requirements onto the current network (subject to network owner agreement)

Managed Workspace is subject to an additional charge and may be suggested as a solution during the initial scoping call of your requirements. The fee is determined based on the size (sq. ft.) of the installation location. To further understand the benefits of Managed Workspace, please engage with your designated Account Manager who will facilitate the process by providing a detailed and customised quotation, thereby enabling you to make informed decisions about optimising your workspace infrastructure.



Maintenance

To facilitate the secure and optimal performance of the Enterprise Managed Services, Elevate will facilitate regular and proactive maintenance, this will include both automated AI-driven optimisation, annual network review and proactive firmware upgrades in accordance with the table below.

Product	Maintenance Type	Description	Frequency
Enterprise Managed LAN & WiFi	WiFi Radio Resource Management (RRM)	Radio channel, channel width and power optimisation	Ongoing, AI-Driven
	Firmware Upgrade	Updated to Juniper MTAC recommended firmware release	Weekly
	Network Audit	Review of all firewall rules, feature usage and setup against latest best practice	Annual
Enterprise Managed Firewall	Firmware Patch	Update firmware patch (incremental software updates with fixes) in accordance with Fortigate recommendations	Every 6 months or within 30 days of applicable CVE
	Firmware Major Release	Update firmware major release in accordance with Fortigate recommendations	Every 2 years
	Network Audit	Review of all firewall rules, feature usage and setup against latest best practice	Annual

Maintenance is undertaken between 1am and 5am, Tuesday, Wednesday or Thursday unless otherwise agreed.



Changes

Network changes are requested by contacting our NOC and opening a support ticket, these will be automatically assigned a P4 priority and handled as shown below. Major changes are scoped, coordinated and implemented by our Customer Network Engineering (CNE) team.

Product		Minor		Major
Enterprise Managed Services	Service Affecting?	No	Yes	Any
	Example	Modify content filtering, additional user on existing VPN, switch port config change, additional SSID on existing network/vlan	Change to active firewall rules, SSID/Password changes on existing network/vlan	Add VPN, significant functionality change, build new network/vlan
	Undertaken	As agreed, during normal business hours	As agreed, either in hours or out of hours 17:30 – 22:00, Sunday–Thursday (excluding bank holidays).	As agreed, either in hours or out of hours 17:30 – 22:00, Sunday–Thursday (excluding bank holidays) or as otherwise agreed with account manager
	Completed	Within 2 business days	Within 2 business days	As agreed



SLA

Measurement

The SLA is measured from the time the incident is diagnosed, if there is any park time (incident passed back to End User for testing, awaiting further diagnostic information to be sent to us from the End User, lack of on-site access or waiting on the vendor if an incident has been escalated to them) then this pauses the SLA calculation.

Time to fix (TTF) SLA is measured from the time the incident is diagnosed to the time suitable replacement equipment is installed on-site and service restored.

Service Credits

Service credits will be issued based on a percentage of the monthly charge for affected equipment. The percentage paid will be equal to 25% of the monthly charge for each month where there is an SLA breach, not exceeding 100% in any billing cycle.

Exclusions

Elevate is not obligated to provide Enterprise Managed Services for any of the following:

- Third-party devices (hardware, software cabling, etc. not provided by Elevate) or problems associated with or arising directly or indirectly from such components;
- Problems with Enterprise Managed Services that have been modified without Elevate's written consent by any person;
- Elevate Equipment that has been damaged or altered by natural causes including but not limited to lightning strikes, thunderstorms, etc;
- Elevate Equipment that is physically damaged by the End User or damaged from any exposure to water (except for outdoor rated Products that are exposed to normal weather conditions);
- Problems with Wi-Fi Equipment that were not purchased directly from Elevate

Disclaimer

The service levels described in this SDD are targets or objectives that Elevate strives to achieve consistently in providing Support Services to End Users. A failure to meet any one or more of the service levels will not create any damage liability on the part of Elevate, or to withhold payment for Elevate Services on the part of End Users.