

NOC

Overview: A Guide to Uptime's NOC for MSP Outsourcing. Reclaim your time and focus on what matters most with seamless, reliable, and efficient NOC.

uptime

Contents

Page	Contents
01	Introduction
02	Proven Process
03	Service Comparison
05	Service Level Agreement (SLA)
06	Escalation Process
07	Skills & Certifications
08	Scope of Works
20	On-boarding
23	Uptime Partner Portal
25	Security & Compliance

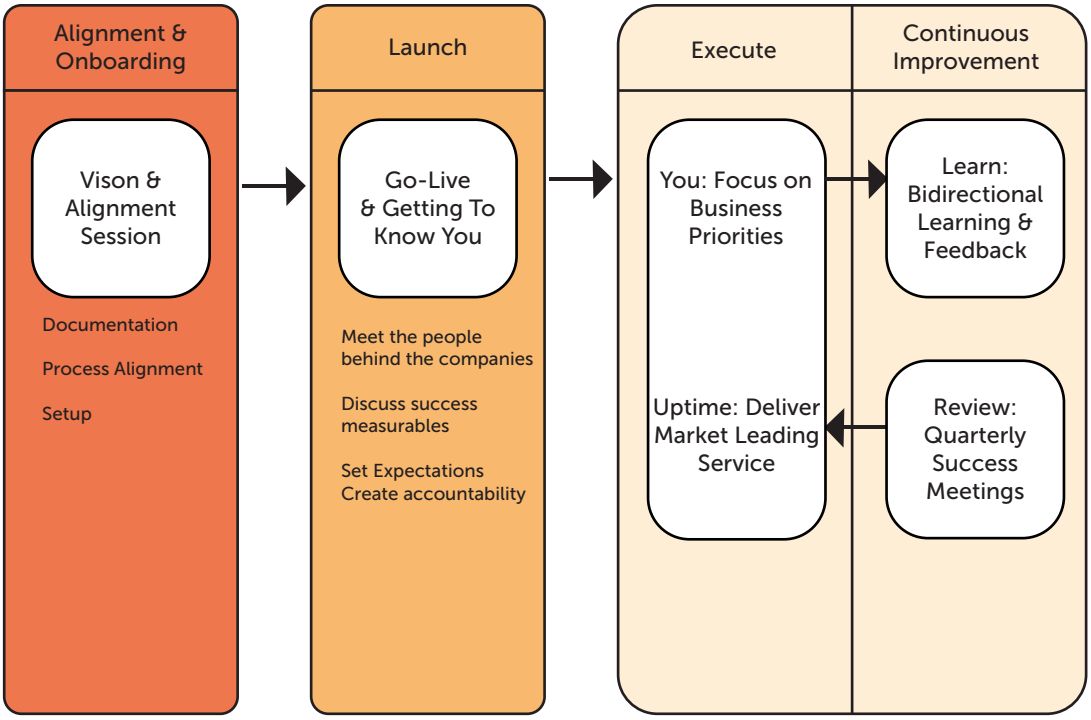
uptime

Introduction

This brochure explains our Network Operations Centre (NOC) services in more detail and is designed to answer some of the initial questions you may have.

If you have any further questions, one of our specialists will be happy to answer them.

Proven Process



Service Comparison

Workstation	Standard	Premium
Monitoring & Notification	✓	✓
Windows Patch Management	✓	✓
Automation (SaaS)	✓	✓
Patch Whitelisting Service (SaaS)	✓	✓
24/7 Coverage	✓	✓
Web Based Management Portal (SaaS)	✓	✓
Anti Virus Management (SaaS)	✓	✓
Remote Remediation		✓
Windows & 3rd-Party Patch Management		✓
Anti Virus/Anti Malware Updates		✓
Automated Disk Clean-up & Health Check Services		✓
Server	**Standard**	**Premium**
Monitoring & Notification Services	✓	✓
Automation	✓	✓
24/7 or In-hours or OOH Coverage	✓	✓

Service Comparison

Server	Standard	Premium
Remediation and RCA Services		✓
Patch Management		✓
Service Requests		✓
Vendor Management		✓

Network Devices	Essentials	Standard	Premium
Device Heartbeat Monitoring & Notification Services	✓	✓	✓
24/7 Coverage	✓	✓	✓
Monitoring & Notification Services		✓	✓
Automation		✓	✓
Only in Hours or OOH Coverage		✓	✓
Remote Remediation			✓
Vendor Management			✓
Service Request			✓

Service Level Agreement (SLA)

We offer a comprehensive SLA covering our NOC

NOC SLA

Priority Level	High	Medium	Low
First Response	30 Minutes	2 Hours	8 Hours
SLA Target	90%	90%	90%

- **Low Priority:** one device/user is affected. The issue relates to only a minor enhancement. There is no productivity loss.
- **Medium Priority:** one device/user is affected moderately and there is some productivity loss or multiple machines/users are affected with only minor loss of productivity.
- **High Priority:** incident affects multiple machines/users and several business-critical functions in one area.

Escalation Process

Our goal is to find a solution within the stated resolution time, or escalate back to you in a timely fashion.

NOC Escalation Process

We will escalate an incident to you in the following scenarios:

- The issue appears to be caused by a system, network or service that we cannot access;
- The issue appears to be caused by a system, network or service we do not support;
- The issue involves non-supported application(s), device(s) or third party vendor(s);
- The issue cannot be resolved by best endeavours within the escalation time frame below;

Incident Priority Level	Escalation Time Frame	Escalation Point	Escalation Type
High	Within 2 hours	Your technical contact	Phone Call + Email + Ticket
Medium	Within 4 hours	Your technical contact	Email + Ticket
Low	Within 16 hours	Your technical contact	Email + Ticket

Skills & Certifications

Our NOC is staffed by several tiers of engingeers ranging from NOC Analysts (Level 1) up to NOC Consultants with specific product and platform expertise. As part of their ongoing personal development, our engineers follow specific ongoing training paths to ensure their skills are kept current.

Each tier has a broad range of industry and platform certifications:

Level 1	› Microsoft Certified: Azure Fundamentals › Microsoft Certified: Security, Compliance, and Identity Fundamentals
Level 2	› Microsoft Certified: Azure Fundamentals › Microsoft Certified: Security, Compliance, and Identity Fundamentals › Microsoft Certified: Azure Administrator Associate › Microsoft Certified: Azure Network Engineer Associate › Microsoft Certified: Windows Server Hybrid Administrator Associate › Microsoft Certified: Information Security Administrator Associate › Microsoft Certified: Cloud and AI Security Engineer Associate › Microsoft Certified: Identity and Access Administrator Associate › Microsoft Certified: Azure Virtual Desktop Specialty › Microsoft 365 Certified: Endpoint Administrator Associate › CCNA › Linux related certifications (RHCA, RHCE) › AWS Certified Solutions Architect - AssociateMi
Level 3 / Consultant	› Microsoft Certified: Azure Administrator Associate › Microsoft Certified: Azure Network Engineer Associate › Microsoft Certified: Windows Server Hybrid Administrator Associate › Microsoft Certified: Information Security Administrator Associate › Microsoft Certified: Cloud and AI Security Engineer Associate › Microsoft Certified: Identity and Access Administrator Associate › Microsoft Certified: Azure Virtual Desktop Specialty › Microsoft 365 Certified: Endpoint Administrator Associate › Microsoft Certified: Microsoft Certified: Azure Solutions Architect Expert › Microsoft 365 Certified: Enterprise Administrator Expert › Microsoft Certified: Cybersecurity Architect Expert › CCNA, CCNP, CCIE › Linux related certifications (RHCA, RHCE) › Product related certifications (VMWare, Citrix, Fortinet, Veeam, AWS, CISSP, etc)

Scope of Works

Remote device monitoring, management and remediation designed to troubleshoot and fix issues with IT services and applications.

How does it work?

Directly supported Remote Monitoring and Management (RMM) software

If you're using RMM software that we directly support, we'll provide NOC services using your own instance of that software. The current list of directly supported RMM software is available on request.

In the above scenario, we may ask your team to assist us with configuration and related requests where required. Automation options will depend on your RMM software's capabilities.

Other RMM Software

If you're using RMM software that we don't support directly, we can still provide you with the full range of NOC services. In this scenario we'll deploy our own monitoring agents on a 'Software as a Service' (SaaS) basis to run alongisde yours. We can also install anti-virus and anti-malware software.

What we ask of you

To help things run smoothly there are a few things that we need you to do.

You need to let us know if a monitoring agent has been decommissioned or is no longer required. If a supported device is shown as unavailable and the monitoring agent is not able to accept maintenance tasks, we'll ask you to verify whether the agent has been decommissioned or has connectivity issues. In the case of decommissioning, we will remove the monitoring agent and let you know when this has been done.

You also need to ensure that we can access supported devices for scheduled maintenance and remediation where applicable. If we're running scheduled maintenance tasks for devices that are unavailable during the agreed maintenance window, we will reschedule the tasks to the next agreed maintenance cycle.

Scope of Works

Prerequisites

In any supported environment, certain requirements must be met before we can provide our NOC services. For example, all workstations must be running a supported operating system version. Our current list of prerequisites is available on request. If any of your customers' networks don't meet these prerequisites our projects team can help you to bring them up to the required level.

Coverage

We'll detail which devices we're supporting and when we are supporting them within your contract. You can add, decrease and make changes to your list of supported devices at any time in any given month.

NOC services are provided on the following basis:

- 24/7/365: 24 hours a day, 7 days a week, 365 days a year.
- In-hours: your normal business hours, Monday to Friday only, excluding public holidays.
- Out-of-hours: outside of your normal business hours, 7 days a week including public holidays.

Types of NOC Services

Monitoring & Notification

We use default notification profiles that have been defined for each server, product or role by our NOC team. These will be preselected during the on-boarding process and are not customisable. From time to time we will update the default monitoring templates and notification profiles to reflect new updates and product enhancements as they are released. We will only provide support for templates that you have preselected.

Where feasible, we can provide customised default notification profiles upon request, either during the on-boarding process or later on.

If you need to request a change to a default monitoring template, for example, an adjustment to the monitoring threshold, let us know and we'll review and confirm back to you.

Remote Remediation

Remediation work will only be carried out for monitored services via the default monitoring templates. You can request the scheduling of an issue remediation task outside of office hours to avoid disruption to your customers.

Scope of Works

Automation

Where the facility exists within either your own or our RMM software, remediation work may be automated to increase the efficiency of service delivery if we feel this would be advantageous.

Root Cause Analysis (RCA)

We carry out root cause analysis (RCA) for the unexpected shutdown and reboot of servers. RCA is delivered outside of our Service Level Agreement.

Preventative Maintenance

Maintenance activities are scheduled to avoid any unplanned downtime and include:

- Windows patch management: security and critical patches are deployed on a scheduled basis.
- Anti-virus/anti-malware updates: maintenance of definition updates for supported anti-virus and anti-malware products.
- Disk cleanup and temporary file deletion.
- Disk health check.
- Investigation of RMM generated warnings requiring preventative action for monitored services.
- Third-party application patch management for supported applications.

Triaging Service

We will triage received alerts. Failed alerts will be escalated back to your nominated technical contact for remediation.

Third-party Vendor Coordination and Management

We will make first contact with the relevant third-party vendor(s) on your behalf, provided that you have supplied us with their details during the on-boarding process. Once first contact has been made, we'll carry out any vendor recommended diagnostics in the first instance. If the issue persists and/or cannot be progressed further, we will escalate the incident back to you for further action, in line with the escalation process detailed in our Service Level Agreement.

Projects

A project is defined as an out-of-scope planned task, (or series of planned tasks) that has a defined start and end date, along with definitive milestones if applicable. Project work can be requested for both monitored and unmonitored devices and for supported technologies.
Projects are billed at our current project hourly rate.

Scope of Works

Service Requests

A Service Request is defined as a formal request made by the Partner for the Supplier to carry out a minor, pre-approved change to a supported device under premium support, where the request is not incident, or alert driven.

Service Requests are not part of the standard NOC monitoring, triage, remediation, or preventive maintenance services and are delivered on a best-efforts basis, subject to availability and suitability.

All Service Requests are billed monthly in arrears at the Supplier's standard hourly rate, charged in 5-minute increments.

Service Requests require a minimum of 48 hours' notice to schedule and will be assessed by the Supplier's NOC team with respect to risk, feasibility, and in-house skillset. Where a Service Request is deemed to fall outside the scope of minor changes, or is considered project-based work, the request will be referred to the Partner and may be quoted separately. Each Service Request ticket is capped at four (4) hours of effort

Service Requests are not covered under the standard NOC Service Level Agreement (SLA).

Types of Device

We deliver NOC services for the following device classes, inclusive of virtualised environments.

› Workstations › Servers › Network Devices

If the monitoring and management of multiple VLANs on a network device is required, each VLAN will be treated as a separate network device.

Scope of NOC Services

We offer a number of clearly defined NOC packages that make it easy to map our services to your own.

Workstation Standard

Preventative maintenance services for monitored Microsoft Windows workstations. Package includes: Windows Patch Management, AV Management. The following standard monitors will be configured.

› Patch failures › Reboot required status › AV definition update
› AV threat detection

Root Cause Analysis (RCA) services and service requests are not included and the standard polling level for workstations is every 4 hours.

Scope of Works

Maintenance Activity	Schedule	Details
Windows Patch Management	Weekly	Microsoft critical and security patches will be approved automatically and installed during the agreed scheduled maintenance window. A workstation reboot will be initiated if required.
Anti-virus / Anti-malware	Daily	All definition and signature updates are performed on a daily or as needed basis.

Anything not listed here or within Supported Items and services is considered out of scope

Workstation Premium

Monitoring and notification, remote remediation and preventative maintenance services for monitored Microsoft Windows workstations.

Alerts received are analysed, prioritised and corrective action taken. Patching, anti-virus/anti-malware definition updates and other maintenance activities are carried out on a scheduled basis.

Root Cause Analysis (RCA) services and service requests are not included.

We will monitor and take corrective action based on the notifications received. We configure these standard monitors:

› CPU › Memory › Disk space › Anti-virus and anti-malware status

The standard polling level for workstations is every 4 hours.

Scope of Works

Preventative maintenance

We will perform maintenance activities on the scheduled basis below:

Microsoft Windows

› Windows patch management: security and critical patches are automatically deployed and applied using our predefined schedule.

› Supported third-party Windows application patches are scheduled and installed automatically.

› Anti-virus/anti-malware updates: definition updates for supported anti-virus and anti-malware products.

› Disk cleanup and temporary file deletion.

› Disk health check.

** In order to regulate alert frequency within acceptable parameters, we will configure an appropriate delay trigger for certain monitored services.*

Scope of Works

Maintenance Schedule

Maintenance Activity	Schedule	Details
Windows Patch Management	Weekly	Microsoft critical and security patches are approved automatically and installed during the agreed scheduled maintenance window. A workstation reboot is initiated if required.
Third-party Windows Application Patch Management	Weekly	Supported third-party application patches are approved and installed automatically during the agreed scheduled maintenance window. A workstation reboot is initiated if required.
Anti-virus/ Anti-malware**	Daily	All definition and signature updates are performed on a daily or as needed basis.
Disk cleanup***	Monthly	Temporary files are removed.
Disk Health Check	Monthly	Disk issues are identified and flagged as appropriate.

Service requests

Out-of-scope services for workstations, including Service Requests, may be carried out for monitored devices where the Partner has a valid Service Desk Services contract in place for the relevant Partner Customer(s). Such requests will be undertaken by the Supplier Service Desk. Examples of Service Requests include (but are not limited to);

› Email account configuration › Application installation and troubleshooting
› User password resets

Scope of Works

Scope of NOC Services

We provide the additional skill-set that operates in the background offering service continuity 24/7.

Server Standard

Monitoring and notification of failed alerts..

Alerts received are analysed, prioritised and failed alerts are triaged back to you for remediation.

Preventative maintenance, remediation, Add-On's, vendor management and Root Cause Analysis (RCA) services are not included. Anything not listed here is considered out of scope.

We will monitor the standard services below (and any additional services agreed during on-boarding) for failures and triage alerts based on severity. Standard monitoring includes:

- Critical Windows availability
- CPU, memory, paging/swap file and disk space
- Backup
- HTTP/HTTPS
- Anti-virus/anti-malware
- Heartbeat

Server Premium

Monitoring and analysis of alerts, preventative maintenance, remediation, Add-On's, vendor management and Root Cause Analysis (RCA).

Alerts received are analysed, prioritised and corrective action taken. Windows patching, anti-virus/anti-malware definition updates and other maintenance activities are carried our on a scheduled basis.

Remediation, moves, adds and changes (MAC) requests, vendor management and Root Cause Analysis (RCA) services.

Scope of Works

Monitoring and Notification

We will monitor the following critical services and any additional services agreed during on-boarding for failures and triage alerts based on severity:

- Heartbeat
- HTTP/HTTPS.
- Backup*
- Critical Windows availability
- CPU, memory, paging/swap file and disk space.
- Anti-virus/anti-malware.

** The Uptime NOC team will monitor for backup job failure and take corrective action to remediate the issue. All media unavailable, tape cleaning or backup hardware issues will be escalated back to the client.*

Remote Remediation and Root Cause Analysis (RCA)

We will carry out remediation work on notifications received and root cause analysis (RCA) will be carried out for unexpected server shutdown or reboots.

We'll commence RCA once the server is back online and will carry out the following activities to determine the root cause:

- Analysis of the event logs.
- Analysis of the memory dump file.
- Review of hardware diagnostic logs.

We'll produce an RCA report and share this with you. This will give an overview of the incident, the corrective action(s) taken and list any recommendations to prevent future occurence.

Preventative Maintenance

We will perform maintenance activities on a scheduled basis as follows.

- Windows patch management: security and critical patches are automatically deployed and applied to our predefined schedule.
- Supported third-party application patches are scheduled and installed automatically.
- Anti-virus/anti-malware updates: definition updates for supported anti-virus and anti-malware products.
- Disk cleanup and temporary file deletion.

Scope of Works

Maintenance Schedule

Maintenance Activity	Schedule	Details
Windows Patch Management	Monthly	Microsoft critical and security patches are approved automatically and installed during the agreed scheduled maintenance window. A server reboot is initiated if required.
Third-party Application Patch Management	Monthly	Supported third-party application patches are approved and installed automatically during the agreed scheduled maintenance window. A server reboot is initiated if required.
Anti-virus / Anti-malware	Daily	All definition and signature updates are performed on a daily or as needed basis.
Disk Cleanup	Monthly	Temporary files are removed.

Sanity check process

The Uptime NOC team will carry out sanity checks after patch installation and upon rebooting to:

› Check the monitored Windows services for any failures and remediate issues.
› Check the server heartbeat and escalate back to the Client if the server is down within the standard SLA.

The services will be carried on an automated basis via the RMM.

Add-On

Partners have the option to purchase the warning Add-On which will enable us to investigate RMM generated warnings for monitored services and it will be remediated or escalated to Client as required. The standard SLA will not be applied for RMM warning notifications.

Service Requests

Any pre-approved Service Requests raised by the Partner for supported devices may be carried out in accordance to the Statement of Work. Examples of Service Requests include (but are not limited to);

› Manual installation of approved updates outside of the standard patching schedule
› Group Policy Object management › Security Certificate installation
› Microsoft Exchange Email Connector configuration
› Configuration of graceful shutdown procedures for supported servers

Scope of Works

Scope of NOC Services

Our white label 24/7 NOC lets you expand your service offering and accelerate your business growth.

Network Device Essentials

Connectivity alerts received will be analysed, prioritised and triaged back to you for remediation work.

Suitable for managed and unmanaged devices that support SNMP.

Preventative maintenance, remediation, moves, adds and changes (MAC), vendor management and root cause analysis services are NOT included.

Essentials service includes:

› 24/7 Device heartbeat Monitoring & Alerting (Routers/Switches, WAP's & Firewalls)

Network Device Standard

Monitoring and notification of critical alerts. Suitable for managed devices that support SNMP.

Suitable for managed and unmanaged devices.

Alerts received are analysed, prioritised and triaged back to you for remediation work.

Preventative maintenance, remediation, moves, adds and changes (MAC), vendor management and root cause analysis (RCA) services are not included.

We will monitor the following services and any agreed additional services (where the facility exists) for failures and triage alerts based on the severity. Standard monitoring includes:

- › Device heartbeat
- › Interface traffic utilisation
- › CPU, memory, utilisation
- › System temperature
- › Interface status
- › Fan status

Scope of Works

Network Device Premium

Monitoring and notification, remediation and preventive services.

Suitable for managed devices only that support SNMP.

Alerts received will be analysed, prioritised and corrective action taken. Preventive maintenance (back-up of network device configuration only). Remediation, Add-On and vendor management are included.

Root Cause Analysis (RCA) services are not included.

We will monitor the following standard services and any agreed additional services (where the facility exists) for failures and triage alerts based on severity.

- Device heartbeat
- CPU, Memory, Utilisation
- Interface status
- Interface Traffic Utilisation
- System Temperature
- Fan Status

Remote remediation

Alerts received will be analysed, prioritised and remediated within the standard SLA.

Preventative maintenance

Where the facility exists, the Uptime NOC team will administer the automated back-up of the network device configuration for each supported network device on a monthly basis. Back-ups will be stored on a shared drive on the Client and/or Client Customer's specified local server. Where the automated back-up of a network device is not available, the Uptime NOC will not administer the back-up of that device.

Service Requests

Any pre-approved Service Requests raised by the Partner for supported devices may be carried out in accordance with the Statement of Work. Examples of Service Requests include (but are not limited to);

- Manual back-up or restoration of network device configuration files
- Firmware updates for supported network devices
- Minor configuration changes to supported network devices
- SNMP configuration updates for monitored network devices
- Interface enablement or disablement on supported network devices

On-boarding

On-boarding enables us to clearly identify each of your support requirements and gather the information required for us to deliver our services successfully against these.

Objectives

The main objectives of the on-boarding process are to:

› Analyse your requirements in detail

› Identify service delivery methods and document these

› Ensure a smooth handover to our support team

What is the role of the on-boarding team?

Our on-boarding team will work with you to gather all the information required by our NOC and/or Service Desk teams, so they can support both you and your clients fully and in line with expectations.

It is very important that you supply us with all the relevant information that we will need in order to begin service delivery. Our on-boarding team will guide you through the information that we require to ensure that we have everything in place before we commence work.

To ensure that we can deliver the best possible service, we will undertake a separate on-boarding process each time you add a new client, user or device. We will endeavour to on-board any new clients as quickly as possible; you can help us with this process by supplying all of the information required at the time of on-boarding.

On-boarding

On-boarding process

1 You
- Contact our sales team

2 Both
- Initial discussion
- Customer requirements
- Technical Q&A

3 Both
- Finalise commercials
- Book on-boarding call
- Agree live services to on-board

4 Us
- Send contract out with agreed on-boarding timeframe

5 You
- Sign contract
- Pay on-boarding fee to secure on-boarding slot in queue

6 You
- Provide access to platforms

7 Both
- On-boarding call
- Knowledge transfer
- Devices/users

8 Us
- System setup
- Site review

9 Both
- System test
- Go Live
- Ongoing reporting and review

On-boarding

What to expect during your on-boarding call

In the course of your initial on-boarding call, we will ask the following questions:

To help us to understand your business better, we will want to:

› Confirm our understanding of your organisation, its business model and geographic location(s);
› Ask you about your clients; how many do you have and what type;
› Confirm the RMM platform you are using and its status;
› Identify any PSA software in use (e.g. Autotask, Connectwise etc.).

To double-check the services and capability you require from us, we will;

› Confirm the specific service(s) you will be using;
› Ask about any specific issues and the reasons for using our service;
› Explain our NOC and/or Helpdesk and how they work;
› Explain the scope of the support we provide, covering services monitored and work requests for NOC and Helpdesk;
› Explain the technical implementation;
› Set out our escalation process and SLA.

We will run through a checklist of preliminary information to:

› Gather/confirm contact information (technical and account);
› Gather environment information and case escalation flow details;
› Collect serial numbers and asset numbers;
› Identify any recurring or frequent issues that we should be aware of.

The timescale to on-board your clients depends on a number of factors. You can help us to on-board as quickly as possible by supplying all on-boarding information as agreed and on time.

A simple on-boarding can be achieved in a matter of days or even hours. For more complex on-boarding requirements we recommend a phased approach over a number of weeks. Our primary concern is to ensure that on-boarding is done right first time. Whatever your on-boarding requirement we will work with you to ensure it goes smoothly.

Uptime Partner Portal

Our Uptime Partner Portal integrates your support platforms onto one unique system, allowing you to manage your clients more effectively.

What is the Uptime Partner Portal?

The Uptime Partner Portal is an exciting next step as we continue to evolve and make enhancements to how we support your MSP business.

Autotask PSA and Datto RMM link seamlessly via API's, enabling you to easily enable support for your clients devices and manage all Uptime support tickets. The straightforward and clean design is organised by the clients, device types and devices. Tickets are automatically synchronised between your platforms and the Uptime Partner portal as and when support is needed.

Uptime Partner Portal Benefits

You will automatically benefit from the following Uptime Partner Portal benefits:

› Ability to sort, filter and add/remove clients and devices in a matter of minutes
› Significant reduction in time taken for consolidations
› Consolidations at the MSP's pace
› Ability to turn on support for client devices
› Full visibility of clients managed by Uptime
› Secure platform – built on Windows Azure
› Multifactor Authentication

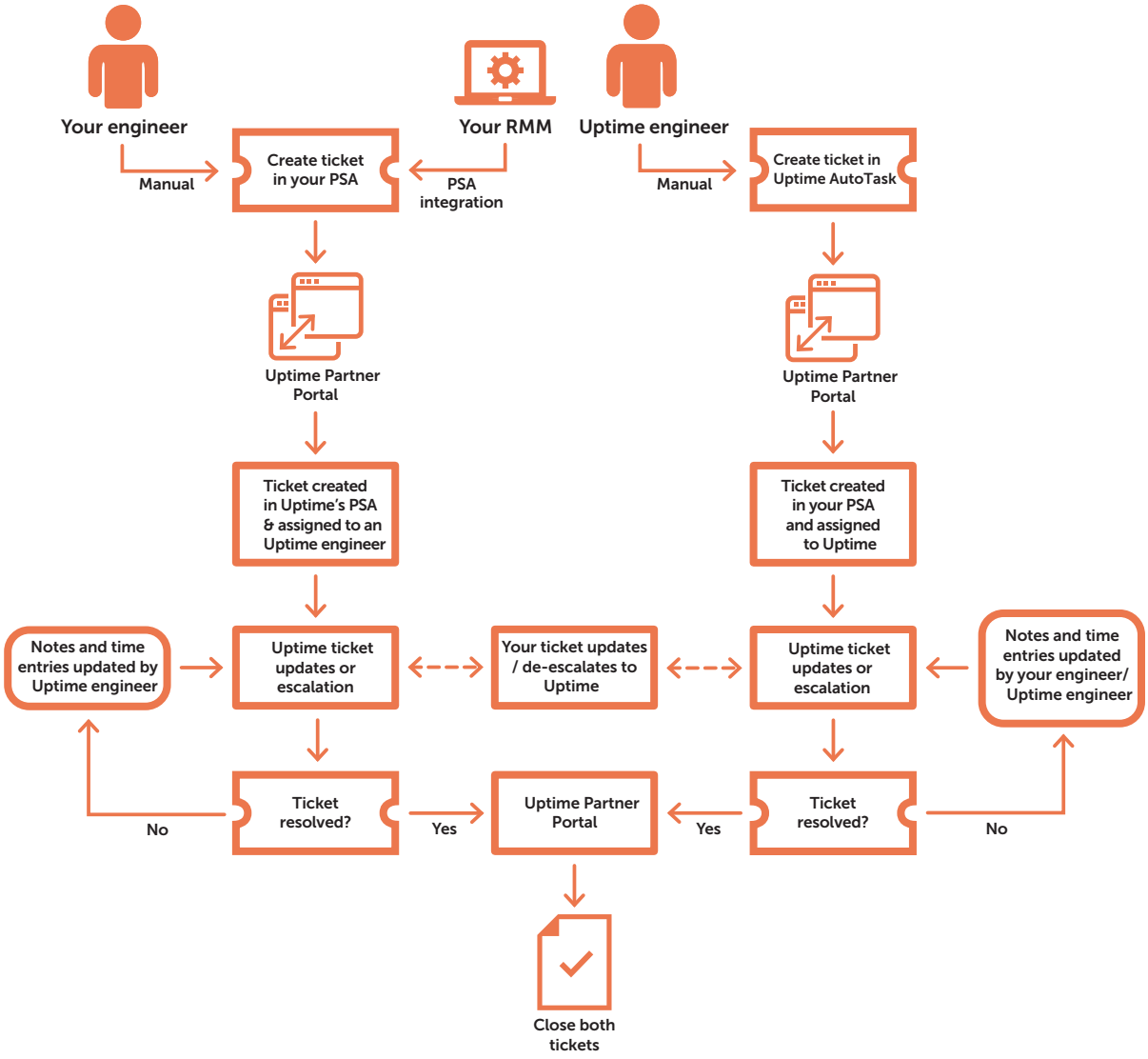
Additional features coming soon

› N-central RMM Integration
› Connectwise Manage PSA Integration
› Intelligent Reporting

Uptime Partner Portal

What is the Uptime Partner Portal?

The diagram below is an example of how Helpdesk and ticket integration works with our NOC. We appreciate that all MSP's are different and therefore Helpdesk integration varies for each partner. This will be discussed with you during on-boarding.



Security & Compliance

We are committed to ensuring that security is considered and maintained within all aspects of our operation. We have implemented the following security control mesaures within our NOC. Details of Helpdesk security measures are available seperately on request.

NOC Security Measures- Technical Delivery Centre (Colombo, Sri Lanka)

Human Resource

- Employment history verification
- ID document checks
- Professional qualifications verification
- Minimum of 2 verified references
- Criminal record checks
- NDAs and confidentiality agreements in place for every employee

Physical

- 24/7 onsite security
- Biometric access control system with dual authentication
- Night vision enabled CCTV system throughout suite

Infrastructure

- Access to information controlled by principal of least access
- Domain controlled environment utilising group policy, enabling access control and monitoring
- Multi-factor authentication to further control access to infrastructure resources and tools
- Remote access sessions AES-256 encrypted
- All systems kept current with security patches, anti-virus and anti-malware software and definitions
- All operations performed as per ITIL best practice

Security & Compliance

Redundancy

› 24/7 backup generator and UPS facilities
› Redundant Internet connectivity based on wired and wireless technologies
› Cloud-based SaaS and IaaS environments are used for critical business systems e.g. VoIP telephony, call management and PSA functions
› Business continuity/disaster recovery plan with standby disaster recovery suite

Customer data

› Client and client customer data is stored on a hosted SSAE 16 Type 11 certified secure CRM and ticketing system
› Client and client customer credentials (if supplied) are stored within a secure database utility with options for cloud-based or local storage dependent on regulatory requirement
› All data stored within IT Glue is stored on EU servers to comply with GDPR regulation

Compliance and certifications

› ISO 27001: 2022 certification
› PCI DSS compliance
› HIPAA/HITECH regulated clients via Business Associate Agreement*
› GDPR compliance

* We can provide restricted NOC services for HIPAA/HITECH regulated clients. As a non-US based entity we do not hold passwords for regulated customers. Access control is implemented and maintained by way of customer-controlled granular security permissions that prevent access to any data that falls within regulatory scope.

About Uptime

Providing exceptional service to our partners' clients is our number one priority. Uptime has been providing specialist IT support since 2002, first as an MSP and now as a trusted partner to MSPs on an international basis.

We have built a reputation for helping our partners grow their managed services businesses by providing the highest quality Helpdesk, NOC, Staff Augmentation and project services at a fair price.

Operating from our headquarters in Crawley, we offer MSPs 24/7 support to complement and extend their own resources, enabling them to scale cost effectively and drive profitable growth.

For more information, please visit:

www.uptimeglobal.tech

Head office (UK/EMEA Sales)

Saxon House, Stephenson Way,
Three Bridges,
RH10 1TN

Telephone

+44 (0)203 7647688

Technical Operations (Sri Lanka)

77, Park Street,
Colombo 02,
Western

NOC & DT Operations (South Africa)

PO Box 3094 Houghton,
Houghton,
Gauteng, 2041

Helpdesk Operations (New Zealand)

Floor 38, 22 Albert Street,
Central Business District,
Auckland

Telephone

+64 99735483

Helpdesk Operations (USA)

8875 Hidden River Pkwy Suite 300,
Tampa, FL 33637,
United States

Telephone

+1 813 607 4883

uptime