

PROACT

G-Cloud 15

Managed Services for
Modern Workspace (AVD,
M365 and Entra ID)

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
29/01/2026	Colin Abram	V1	Document Upload



Managed Services for Modern Workspace (AVD, M365 and Entra ID)

Proact provide 24x7x365 monitoring and management services via our Service Operations. Proact's Service Operations includes support for a range of device hardware, platforms, software and systems. All monitoring and support activities are performed remotely via secure internet connectivity.

Service Operations for Workspace, provides the Customer with a 24/7 remote monitoring, support and management solution for a range of digital workspace environments, such as Microsoft 365, Azure Virtual Desktop, Citrix and Entra ID. This service includes:

- 24x7x365 Proact service desk and automated monitoring of devices
- Self-service support and self-service monitoring portals
- Fault co-ordination and resolution
- Event, incident and problem management.
- Incident response, action of pre-agreed changes, troubleshooting and resolution
- Proactive root cause analysis and prevention
- Security aligned operational controls
- Performance and capacity optimisation
- Change, patch and configuration management
- A named Service Delivery Manager to co-ordinate delivery and provide regular customer reports

Proact provide support for the following technology areas as part of the Monitoring and Management services:

- Storage systems and associated software
- Hypervisors
- Server Operating Systems
- Network appliances and devices (Firewalls, Switches, Routers, Load Balancers)
- Backup software and associated hardware platform
- Public Cloud
- Azure Virtual Desktop
- Workspace software
- M365, Intune, Entra ID and Active Directory

This document contains the following appendices detailing the service definitions for the Monitoring and Management services:

- [Appendix 1 – Service Operations for Modern Workspace](#)

Appendix 1 – Service Operations for Modern Workspace

1.1 - Service Overview

Service Operations for Workspace, provides the Customer with a 24/7 remote monitoring, support and management solution for a range of digital workspace environments, such as Microsoft 365, Azure Virtual Desktop, Citrix and Entra ID.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Respond to reasonable service requests for relevant information and advice.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on customer-managed systems.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Standing Charge
Proact shall: • Provide the Customer administrator with access to the Proact monitoring portal. • Provide an encrypted tunnel over the internet to secure service traffic. • Provide internet bandwidth for the transfer of service traffic. • Deploy remote monitoring applications to collect statistics/events/alerts for CIs. • Deploy remote management applications to manage CIs. • Create monitoring profiles to meet the Customer's threshold requirements. • Provide critical fault alert, vendor co-ordination, incident support and hardware break-fix. • Provide a service review report. • Provide a change advisory board to review normal, standard, and emergency change requests. • Subject to agreement, join the Customer's change advisory board, for relevant changes. • Implement agreed changes to CIs. • Provide a major incident report, where required.



- Provide incident trend analysis.
- Organise a quarterly service review meeting.
- Review the DR/redundancy test plan provided by the customer.
- Perform agreed DR/redundancy test actions for CIs during normal Proact business hours.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.
- Provide an external IPv4 public IP address for the creation of the encrypted tunnel, where required.
- Provide a network administrator to configure and troubleshoot service traffic, where required.
- Provide service accounts and passwords/keys with privileges to allow Proact to manage/monitor the CIs.
- Ensure CIs retain historic log data and make log data available to Proact for troubleshooting.
- Provide sufficient licenses for the CIs to achieve the level of functionality the Customer requires.
- For hardware CIs, provide a minimum of a break-fix vendor support contract.
- For compatible devices, configure 'dial home' diagnostics to report to Proact's service desk.
- Provide 'on demand' remote access to managed CIs, when required by Proact.
- Provide and manage servers/cloud instances to host the remote monitoring/management applications.
- Install CI software major version upgrades to introduce functionality or remain in vendor support.
- Inform Proact of planned maintenance or other operations that may impact the service.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Nominate named individuals to engage with Proact on the approval and timing of changes.
- Work with Proact to agree predefined actions for common types of incidents.
- Provide thirty days' notice of the intention to perform a DR/redundancy test for CIs.
- Provide Proact with a DR/redundancy test plan for all CIs seven working days prior to testing.

The following elements are out of scope of the service:

- DR/redundancy testing performed outside of local business hours.

1.2 - Proact Modern Workspace - Desktop Operations

Desktop Operations - User (Per User)

Proact shall:

- Provide a Virtual Desktop Management Plane (VDMP).
- Connect the VDMP to the Customer's Virtual Desktop Environment (VDE).
- Monitor/manage the configuration settings, hosts and policies of the Customer's VDE.
- Monitor/manage the CIs within the Customer's VDE.
- Monitor resource health status, availability, identity, and access management alerts.
- Create, deploy and update code to streamline and automate management of the VDE.
- Monitor/manage cloud service native key vaults, databases and log tools related to the VDE, where required.
- Monitor/manage cloud service native storage and automation tools related to the VDE, where required.
- Monitor/manage cloud service native networks and network security tools related to the VDE, where required.
- Perform user density and load balancing checks to optimise performance.
- Suspend user sessions and user profiles, upon request.
- Inform the Customer of maintenance activities impacting the VDE.
- Make cost recommendations related to modern workspace environment(s) during quarterly service reviews.
- Provide and manage a single master image for the Customer VDE.

- Work with the Customer to deploy and update the master image, no more than once per calendar month.
- Deploy host pools based upon the master image.
- Report on host pool resources that breach Customer defined size thresholds.
- Assign host pools to required user groups.
- Perform master image optimisations or scaling policy changes to improve performance and scale.
- Deploy, update or remove Standard Applications, upon request.
- Work with the Customer to deploy, update or remove Non-Standard Applications, upon request.
- Review patch/security updates for the OS and Standard Applications monthly and provide update packages.
- Inform the Customer of scheduled application and update tasks, prior to deployment.
- Stage application and update tasks to customer-defined test, acceptance, and production user groups.
- Provide patch status reports as part of scheduled service review reports.

The Customer shall:

- Provide access to the Customer's public cloud tenant and network, where required.
- Provide the Virtual Desktop Environment (VDE) for Proact to manage.
- Maintain a valid subscription and provide credentials/access for the VDE to Proact's VDMP.
- Utilise the public cloud provider's native identity and access management tooling, where required.
- Limit access to the public cloud tenant through specific public IP address ranges, where required.
- Maintain overall responsibility for the security posture, policies and settings of the public cloud tenant and VDE.
- Provide access to native, and third-party, access keys stored within cloud key vaults, where required.
- Inform Proact of changes that may impact security of the public cloud tenant and VDE.
- Inform Proact of user sessions or user profiles to be suspended.
- Manage file & directory permissions within file shares.
- Monitor/manage end user devices and peripherals and ensure VDE compatibility.
- Manage and troubleshoot end user device hardware and network access to the VDE.
- Define the monthly schedule for updating the master image.
- Provide a valid VDE desktop operating system subscription.
- Define the usage and application requirements for the master image.
- Inform and work with Proact to deploy, update or remove Standard and Non-Standard Applications.
- Provide update packages and installation documentation for Non-standard Applications.
- Provide valid licenses/subscriptions for all Standard and Non-Standard Applications.
- Define: test, acceptance, and production user groups for staged application and update tasks.
- Notify Proact of changes to application and update tasks at least eight working hours prior to commencement.
- Validate the functionality of the CIs following application deployment/update and patch/security update tasks.
- Provide Proact with non-privileged accounts that mimic production users for testing, where required.

The following elements are out of scope of the service:

- Expansion of the VDE into additional public cloud tenants, regions or environments.
- Upgrades or enabling of new features within the public cloud tenant, VDE or VDMP.
- Creation of new base/master images.



Desktop Operations - Images (Per Image)

Proact shall:

- Validate the additional master image provided by the customer is compatible with the VDE.
- Add additional images, beyond the provided master image, to the VDE, upon request.
- Monitor and manage the additional images, in line with the VDE master image.

The Customer shall:

- Request additional images for the VDE.
- Provide pre-installed OS disk file to be used as the foundation of the new image.

The following elements are out of scope of the service:

- Creation of additional master images.

1.3 - Proact Modern Workspace – M365 Operations

M365 Operations - User (Per User)

Proact shall:

- Provide a Modern Workspace Management Plane (MWMP).
- Connect the MWMP to the Customer's Modern Workspace Environment (MWE).
- Monitor/manage the configuration settings and access policies of the Customer's MWE.
- Report on license usage within the platform and assign/remove licenses, upon request.
- Define a global configuration baseline for the Customer's MWE.
- Report configuration changes within the MWE that differ from the global configuration baseline.
- Create, modify or remove email policies and resources, upon request.
- Expand mailbox storage, upon request.
- Report on inactive users or mailboxes
- Monitor team collaboration environment.
- Create, modify or remove team collaboration templates, teams and policies, upon request.
- Report on inactive team collaboration environment resources.
- Monitor document management environment.
- Create, modify or remove document management sites, resources, and policies, upon request.
- Expand document management storage, upon request.
- Report on inactive document management environment resources.
- Monitor personal storage usage and access controls
- Create and set personal storage quotas, upon request.
- Work with the Customer to define personal storage access and sharing policies
- Manage personal storage access and sharing policies
- Manage the Customer's MWE endpoint security service.
- Configure endpoint security service alerts and integrate with the Customer's incident management system.
- Define a baseline security policy for customer endpoints and apply to the default endpoint group.
- Report on inactive endpoints devices.
- Remove inactive endpoints devices, upon request.
- Update endpoint security service exclusion lists, upon request.
- Work with customer to define the security update and AV definition compliance policy for endpoints.
- Report on the endpoints that do not achieve security update and AV definition compliance.
- Follow Proact's guidance on blocked files and safe browsing practices.

- Inform the Customer of alerts related to blocked files, and recommendations regarding safe browsing practices.
- Manage the Customer's MWE endpoint administration service.
- Enrol and remove endpoint devices in the endpoint administration service, upon request.
- Work with customer to define endpoint access, security, compliance and conditional access policies.
- Report on inactive MWE endpoint administration service resources.
- Create, modify and remove endpoint resources, upon request.
- Deploy, update or remove Standard Applications, upon request.
- Work with the Customer to deploy, update or remove Non-Standard Applications, upon request.
- Review patch/security updates for the OS and Standard Applications monthly and provide update packages.
- Inform the Customer of scheduled application and update tasks, prior to deployment.
- Stage application and update tasks to customer-defined test, acceptance, and production user groups.
- Provide patch status reports as part of scheduled service review reports.

The Customer shall:

- Provide access to the Customer's public cloud tenant and network.
- Provide the Modern Workspace Environment (MWE) for Proact to manage.
- Maintain a valid subscription and provide credentials/access to allow Proact's MWMP to manage the MWE.
- Create, modify and remove users, groups and device entries within the Customer's MWE.
- Troubleshoot MWE connection issues on Customer's end-user devices.
- Provide licenses for the platform and inform Proact where licenses are to be added or removed.
- Provide five working days' notice of configuration changes that may breach the global configuration baseline.
- Create, modify and remove email accounts, shared mailboxes and distribution lists.
- Manage user and device-level mail settings.
- Define the criteria by which users or mailboxes are considered inactive.
- Request mailbox storage expansion, where required.
- Inform Proact of email resource to be removed from the environment.
- Request team collaboration storage expansion, where required.
- Define the criteria by which team collaboration environment resources are considered inactive.
- Inform Proact of team collaboration resources to be removed from the environment.
- Inform Proact of document management sites or resources to be created, modified or removed.
- Request document management storage expansion, where required.
- Define the criteria by which document management environment resources are considered inactive.
- Inform Proact of desired personal storage quotas.
- Work with Proact to define personal storage access and sharing policies.
- Respond to endpoint security service alerts and device notifications.
- Join new endpoints to the default endpoint group, to which the baseline security policy is applied.
- Follow Proact's guidance on blocked files and safe browsing practices.
- Manage and respond to any security incidents.
- Work with Proact to define the security update and AV definition compliance policy for endpoints.
- Remediate endpoints that do not achieve security update and AV definition compliance.
- Inform Proact of endpoint security service exclusion lists updates.
- Inform Proact which inactive endpoint devices that may be removed.
- Maintain overall responsibility for endpoint security and vulnerability resolution.
- Inform Proact of endpoint devices to be added, and inactive endpoint devices to be removed.
- Work with Proact to define endpoint access, security, compliance and conditional access policies.

- Remediate endpoints that do not meet access, security, compliance and conditional access policy requirements.
- Define the criteria by which endpoint devices are considered inactive.
- Remediate any endpoint device-specific issues.
- Inform and work with Proact to deploy, update or remove Standard and Non-Standard Applications.
- Provide update packages and installation documentation for Non-standard Applications.
- Provide valid licenses/subscriptions for all Standard and Non-Standard Applications.
- Define: test, acceptance, and production user groups for staged application and update tasks.
- Notify Proact of changes to application and update tasks at least eight working hours prior to commencement.
- Validate the functionality of the CIs following application deployment/update and patch/security update tasks.

The following elements are out of scope of the service:

- Defender advanced detection, endpoint detection and response and 24x7 vulnerability management.

1.4 - Proact Modern Workspace – Identity Services

Identity Services - User (Per User)

Proact shall:

- Provide an Identity Services Management Plane (ISMP).
- Connect the ISMP to the Customer's Identity Services Environment (ISE).
- Monitor/manage the configuration settings and policies of the Customer's ISE.
- Manage IAM functions including Single Sign-On (SSO) and Multi-Factor Authentication (MFA).
- Manage controls such as hybrid access, privileged identity management (PIM), and conditional access.
- Manage user authentication settings including password, password-less a certificate-based authentication.
- Configure application authentication including OAuth and SAML authentication.
- Add/remove third-party/line-of-business application access to identity services, where required.
- Inform the Customer of AD Connect synchronisation issues.
- Work with the Customer to remediate synchronisation errors within AD Connect.
- Perform OU filter adjustments, where required.
- Assist the Customer with updating AD Connect software, upon request.

The Customer shall:

- Provide the Identity Services Environment (ISE) for Proact to manage.
- Maintain a valid subscription and provide credentials/access to allow Proact's ISMP to manage the ISE.
- Maintain responsibility for internal policy, organisational decisions and user/group management.
- Inform Proact when third-party/line-of-business application access to identity services should be added/removed.
- Assist with AD Connect errors and resolve AD Connect errors related to the customers Active Directory.
- Define OUs and maintain users and groups for synchronisation.
- Update AD Connect software as requested by Proact or to remain in vendor support.

1.5 - Proact Modern Workspace - Desktop Services

Desktop Services - User (Per User)

Proact shall:

- Connect to the Customer's Virtual Desktop Management Plane (VDMP).
- Monitor/manage the configuration settings, hosts and policies of the Customer's VDE.
- Monitor/manage the CIs within the Customer's VDE.
- Monitor resource health status, availability, identity, and access management alerts.
- Create, deploy and update code to streamline and automate management of the VDE.
- Monitor/manage cloud service native key vaults, databases and log tools related to the VDE, where required.
- Monitor/manage cloud service native storage and automation tools related to the VDE, where required.
- Monitor/manage cloud service native networks and network security tools related to the VDE, where required.
- Perform user density and load balancing checks to optimise performance.
- Suspend user sessions and user profiles, upon request.
- Inform the Customer of maintenance activities impacting the VDE.
- Make cost recommendations related to modern workspace environment during quarterly service review.

The Customer shall:

- Provide a Virtual Desktop Management Plane (VDMP).
- Maintain a valid subscription and provide credentials/access for the VDE and VDMP.
- Provide access to the Customer's public cloud tenant and network, where required.
- Utilise the public cloud provider's native identity and access management tooling, where required.
- Limit access to the public cloud tenant through specific public IP address ranges, where required.
- Maintain overall responsibility for the security posture, policies and settings of the public cloud tenant and VDE.
- Provide access to native, and third-party, access keys stored within cloud key vaults, where required.
- Inform Proact of changes that may impact security of the public cloud tenant and VDE.
- Inform Proact of user sessions or user profiles to be suspended.
- Manage file & directory permissions within file shares.
- Monitor/manage end user devices and peripherals and ensure VDE compatibility.
- Manage and troubleshoot end user device hardware and network access to the VDE.

The following elements are out of scope of the service:

- Expansion of the VDE into additional public cloud tenants, regions or environments.
- Upgrades or enabling of new features within the public cloud tenant, VDE or VDMP.

Desktop Services - Images (Per Image)

Proact shall:

- Work with the Customer to deploy and update master images, no more than once per calendar month.
- Deploy host pools based upon the master images.
- Report on host pool resources which breach Customer-defined size thresholds.
- Assign host pools to required user groups.
- Perform master image optimisations or scaling policy changes to improve performance and scale.
- Deploy, update or remove Standard Applications, upon request.
- Work with the Customer to deploy, update or remove Non-Standard Applications, upon request.

- Review patch/security updates for the OS and Standard Applications monthly and provide update packages.
- Inform the Customer of scheduled application and update tasks, prior to deployment.
- Stage application and update tasks to customer defined test, acceptance, and production user groups.
- Provide patch status reports as part of scheduled service review reports.

The Customer shall:

- Define the monthly schedule for updating master images.
- Provide a valid VDE desktop operating system subscription.
- Define the usage and application requirements for master images.
- Inform and work with Proact to deploy, update or remove Standard and Non-Standard Applications.
- Provide update packages and installation documentation for Non-standard Applications.
- Provide valid licenses/subscriptions for all Standard and Non-Standard Applications.
- Define: test, acceptance, and production user groups for staged application and update tasks.
- Notify Proact of changes to application and update tasks at least eight working hours prior to commencement.
- Validate the functionality of the CIs following application deployment/update and patch/security update tasks.

The following elements are out of scope of the service:

- The creation of new master images, or the onboarding of new master images created by the Customer.



1.6 - Service Level Agreement

1.6.1 - Response Time Service Levels

Definition	Description
Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: • a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or • an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or • an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges for the directly affected service.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges for the directly affected service.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.

Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours of the change being agreed. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.



1.7 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
LogicMonitor

1.8 - Glossary

Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract. The CIs will be the relevant M365 Users, M365 Devices, Entra ID Users, Virtual Desktops Users and Master Images within the Customer's modern workspace environment managed by Proact, as set out in the Contract.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.
Standard Application	A software product that is part of the Microsoft 365 suite (including but not limited to Microsoft Outlook, Word, Excel, PowerPoint, Teams, OneDrive, SharePoint, and Edge), as well as the following third-party web browsers: Google Chrome and Mozilla Firefox.
Non-Standard Application	A software product the customer wishes to install within their master images not explicitly listed as a Standard Application.

