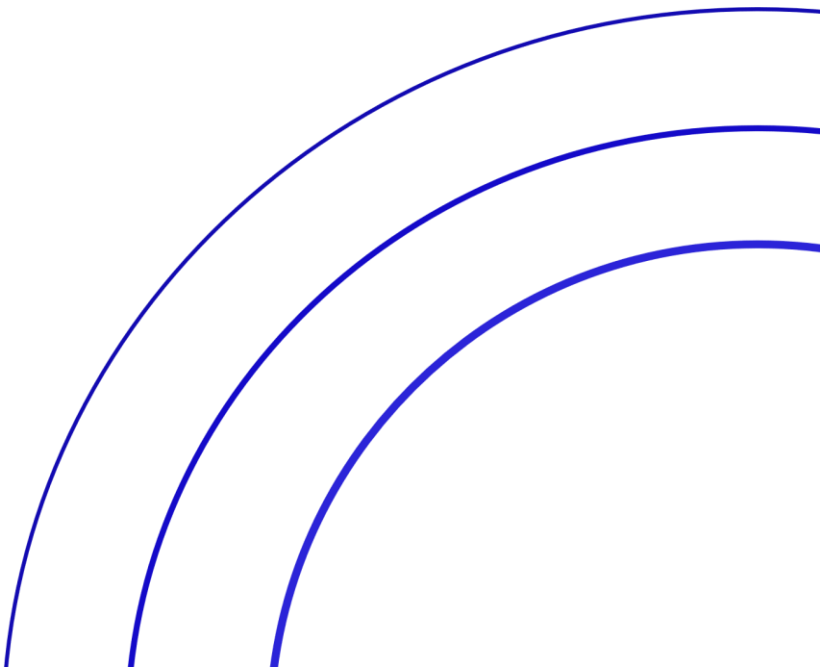
Service Description - Managed Workstation - Azure



Document Control

TITLE:	**Service Description - Managed Workstation - Azure**	**DOCUMENT REF NO:**	QMS REC153
DESCRIPTION:	This document defines the services provided by Calligo's Managed Workstation - Azure service		
OWNER/ AUTHORITY:	Chief Operating Officer (COO)	**VERSION NO:**	1.6
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	22/07/2024
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The Chief Operating Officer (COO), is the owner of this document and is responsible for ensuring that this service description is reviewed in line with the review requirements of Calligo's Information Security Management System and Project Management Frameworks.
Approved by the Chief Operating Officer, Calligo ("Entity") on 22 July 2024

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Initial Issue	Director, Operations Management	VP Cloud Operations	23/01/23
1.1	Updated supporting documentation links	Director, Operations Management	VP Cloud Operations	20/02/23
1.2	Updated Service Description Title	VP Cloud Operations	Chief Operating Officer	04/09/23
1.3	Updated optional offerings	Director, Operations Management	VP, Cloud Operations	26/09/23
1.4	Change of ownership	Cloud Operations Team	COO	30/04/24
1.5	Updated formatting and removed references to the CSSF	COO	COO	22/07/24
1.6	Added MDM SI as an optional element.	Director, Operations Management	COO	24/08/21

Contents

1. Service Overview

This document defines the services provided by Calligo's Managed Workstation - Azure service. The Managed Workstation - Azure service is one of a suite of services within the Calligo Operating Model.

2. Service Inclusions

2.1. CO-ITSM-AVDP

This service leverages Microsoft Azure to provide support for Azure Virtual Desktops (persistent).

2.2. CO-ITSM-IMG

This service leverages SCCM/MECM, Intune or AVD deliverables.

2.3. CO-ITSM-IPM

This service leverages Microsoft Intune to deliver Endpoint Configuration and Management.

2.4. CO-ITSM-OSP

This service leverages Datto RMM and PowerBI to deliver patching and reporting to Windows OS assets.

2.5. CO-ITSM-MON

This service leverages Datto RMM and PowerBI to deliver monitoring and reporting for the in-scope service assets.

2.6. CO-ITSM-SD

This service leverages an ITSM platform and trained Level 1 Service Desk Analysts to cover activities that provide a client facing Service Desk.

2.7. CO-SW-LICENCE

This service provides Application, OS, and Appliance licensing.

2.8. CO-ITSM-MDM (Optional)

This service delivers a solution designed to meet the needs of customers requiring enterprise mobile device management at scale.

3. Service Provisions

3.1. CO-ITSM-AVDP

3.1.1. Inclusions

CO-ITSM-AVDP	
Scope Item	**Description**

Alerting	Alert on the PaaS management environment for Critical alerts Alert of virtual desktop hosts availability Platform performance alerting and resolution Review AVD pool sizing based on alerting elements Performance alerting and resolution
Reporting	Storage reporting Trend reporting Publishing requests Application issues
Imaging	Requires SI: **CO-ITSM-IMG (AVD Components)**
Application packaging and Deployments	Requires SI: **CO-ITSM-APP**
Intune Platform Management	Requires SI: **CO-ITSM-IPM**
OS Patching	Requires SI: **CO-ITSM-OSP**
AVD Management	Windows Virtual Desktop Management for Multisession and Dedicated Power users. Creation and management of Host Pools Manage Application Groups Manage AVD Tenant elements
Monitoring	Requires SI: **CO-ITSM-MON**

3.1.2. Exclusions

CO-ITSM-AVDP	
Exclusion Item	**Description**
Additional Systems Management	Systems management and administration activities extending beyond the scope of this service are available at an additional cost as defined in the commercial agreement.
Self Service	Cloud Management Portal self-service features are only available on Enterprise Agreement Azure subscriptions, or Azure CSP subscriptions
Co-management	Remediation work required because of customer configuration changes that break the desired service functionality.
Non-supported Applications	Deployed applications are not supported except for the issue of WVD service availability and deployment issues. Application support remains with the existing customer application support teams.

3.2. CO-ITSM-IMG

3.2.1. Inclusions

CO-ITSM-IMG	
Scope Item	**Description**
Image Planning (All)	Plan quarterly build and release cycle. Collect pre-requisite components.
Image Management (SCCM/MECM)	Maintain lifecycle / support of image. • Pre-requisite components. • Operating System Updates. Scheduled image captures. • Application addition/deletions. • Adding software updates. • Maintenance of deployment task sequence. ○ Reliability improvements. ○ Task addition/deletions. • Testing ○ Verify capture / deployment changes. ○ Testing in virtualized test environment that properly mirrors production • Task sequence failures ○ Analysis of logs files / reports ○ Corrective action • Advisory services on image optimization • Long term image planning • Communication of documents • Troubleshooting for image deployment failures Offline image troubleshooting
Image Management (AVD)	Creation of Base VM. • Take Snapshot of initial disk of the Image VM Customize VM • Install the latest Windows updates. • Complete any necessary cleanup, such as cleaning up temporary files, defragmenting disks, and removing unnecessary user profiles. • Optimize drivers (defrag) • Remove user profiles • Generalize VM Capture VM Managed Image or Add to the Shared Image Gallery. Remove Base VM Add required Language Packs
Image Management (Intune)	Configure Autopilot if required. Create Profile • Configure Out of Box experience ○ User Driven ○ Self Deploying • Join AAD Create Device enrollment Enable Device cleanup rules if required.

CO-ITSM-IMG	
Scope Item	**Description**
	Enable and configure configuration Policies.

3.2.2. Exclusions

CO-ITSM-IMG	
Exclusion Item	**Description**
Imaging Testing (Production)	Initial testing is done as part of image management however final testing and signoff requires client testing on test and / or production endpoints.
Client test environment configuration	Testing environment configurations are the responsibility of the client unless a separate Professional Services engagement has been purchased.
Provisioning and configuration of a remote KVM.	KVM purchase and configuration is provided by the customer as each configuration can be very environment specific.
Feature Updates	Feature Updates are included in CO-ITSM-OSP.
OS Hardening	OS hardening is client function and environment specific. Although there are baselines available, there is much design and testing required. Enablement of this requires a separate Professional Services engagement.
Addition of new hardware models mid OS release	Additional hardware model support requirements introduced during a build cycle, result in the new models being deferred until the next cycle or causing the cycle to reset to the initial design phase.
Additional customer development outside standard configuration.	Adding new features such as TPM, Bit locker management; OSD front end; Dynamic application management

3.3. CO-ITSM-MON

3.3.1. Inclusions

CO-ITSM-MON	
Scope Item	**Description**
Base OS Monitoring	Monitoring covers in-support Windows Server family operating systems
Resource Monitoring	The following items are currently within scope -CPU utilization -Memory (RAM) utilization -Disk utilization
Availability Monitoring	-RMM Agent heartbeat -URL availability
Remediation	-Remediation services to ensure all management functionality is operable

	-Remediation services to restore operability, or resolve service availability issues of monitored options
Service Monitoring	Monitoring of core OS and role services (defined as per service design)

3.3.2. Exclusions

CO-ITSM-MON	
Exclusion Item	**Description**
End-of-Life OS	Microsoft OS that has passed end of support date and no extended support agreement exists
End user OS	Non-Windows Server OSes (e.g., Windows 10)
Non-OS application	3rd party software installed to a monitored system Troubleshooting of issues at the application level for applications related to services not provided by Calligo.
Licensing	Application or Server licensing expiration or renewal periods
Customer Internet Connectivity	Monitoring of external IP addresses for connectivity
Procurement	As part of remediation activities, procurement of required hardware or software is out of scope and requires a separate service agreement
Specific Functionality	Monitoring can detect if a system or service is available, but cannot validate full functionality

3.4. CO-ITSM-IPM

3.4.1. Inclusions

CO-ITSM-IPM	
Scope Item	**Description**
Setup	The service item includes the following: Configuration of Intune settings and features that are in scope as per commercial agreement
Administration	The service item includes the following: • Administer Intune **platform.** • Administer Windows Store for Business • Administer Autopilot Monitoring of Intune service
Remediation	The service item includes the following: Remediation of issues with Intune service

3.4.2. Exclusions

CO-ITSM-IPM	
Exclusion Item	**Description**
Remediation of physical disk space issue	Customer is responsible for sufficient disk space in physical endpoints.
Remediation or recovery of systems where a failed	This element of Service Requires: **CO-ITSM-OSP**

installation is caused due to desktop OS issues	
Assets added/removed without notification, or where configuration changes have been to made assets without submission via Change Management Process	Calligo needs to be informed in the form of a change record to the scope or configuration changes that could impact agent's health.

3.5. CO-ITSM-OSP

3.5.1. Inclusions

CO-ITSM-OSP	
Scope Item	**Description**
Monthly patching of systems running Windows OS currently supported by Microsoft	For supported OS versions: Deprecated OS versions require a separate Microsoft Extended Support Contract and a separate deployment agreement. Applicable patches are automatically approved unless otherwise agreed via Patch Advisory reporting and additional approval workflows. Critical, Monthly and Security updates are included as part of regular patch deployments.
Configuration and maintenance of deployment rules, settings, and deployment options.	Administration of rules, products, update classifications, agent settings Zero-day patch deployment
Consolidation of Monthly updates into cumulative updates and deployment of the cumulative updates.	Previous months applicable patches are consolidated into a single deployment to cover all patches in all previous deployments. These deployments are active with the current months deployments and follow the same schedule.
Maintenance of groups for systems in scope	Checking health and heartbeat of assigned assets in specific groups and schedules.
Exclusion of patches from deployment scope for known issues with the patch or resulting from testing during the pilot deployment	Removal of patches from deployment scope for known issues with the patch or as a result of testing during the pilot deployment.

Standard Reporting	Standard Monthly and regularly scheduled reports are included in this service.

3.5.2. Exclusions

CO-ITSM-OSP	
Exclusion Item	**Description**
The development of patch “work arounds” in the absence of an approved system vendor’s patch.	This is a chargeable addition to the service and is priced on effort required as each mitigation or “work around” is unique.
Ad-hoc and /or custom patch reporting	This is a chargeable addition to the service and is priced on effort required.
Manual Patching of systems	This is a chargeable addition to the service and is priced on effort required.
Removal of patches from systems once installed	This is a chargeable addition to the service and is priced on effort required as backouts can vary and be unique.
Remediation or recovery of non-compliant systems caused due to existing OS issue.	The required patches are identified, downloaded and the installation is attempted but fails due to OS issues. Any troubleshooting beyond included remediation steps is a chargeable addition to the service. If the server blue screens due to applied patches during or immediately after patch installation, any troubleshooting beyond included remediation steps is a chargeable addition to the service.
Performing manual vulnerability remediation steps.	Manual steps required before or after automated patching windows is a chargeable addition to the service and is priced on effort required. This falls into the same area as “Manual patching of systems” above.
Compliance on assets added/removed without notification, or where configuration changes have been made to assets without submission via Change Management Process	Calligo needs to be informed in the form of a change record to the scope or configuration changes that could impact agent's health and the patching process.

3.6. CO-ITSM-SD

3.6.1. Inclusions

CO-ITSM-SD	
Scope Item	**Description**
Access to the Calligo ITSM platform	24/7 access to the Calligo ITSM platform that provides capabilities for clients to raise new support tickets and to access open or historic support tickets.
Telephone Support	Access to the Calligo Service Desk via the issued telephone contact numbers during regional Business Hours only.
First Line Fix	Access to the Calligo L1 Service Desk Analysts for first line fix or resolution.

3.6.2. Exclusions

CO-ITSM-SD	
Exclusion Item	**Description**
24/7 Telephone Support	This is a chargeable addition.
Onsite support	All support delivered via the Service Desk offering is remote.

3.7. CO-SW-LICENSE

3.7.1. Inclusions

CO-SW-LICENCE	
Scope Item	**Description**
Client Agreement	Creation of a Customer Agreement, between the client and Application, or OS Vendor
Manage licenses	Management of products and service subscription licenses
Billing Support	Provide billing support from application or OS vendor
Manage Tenant Subscription	Managed subscription changes on behalf of the Client
Reporting	Provide license total / usage
Invoicing	Invoice creation and delivery

3.7.2. Exclusions

CO-SW-LICENCE	
Exclusion Item	**Description**
Installation of software	This element of service is described in SI: **CO-ITSM-SD**
Tracking of client licensing compliance	Client is responsible for maintaining licensing compliance on applications and OS

3.8. CO-ITSM-MDM (Optional)

3.8.1 Inclusions

CO-ITMS-MDM (Optional)	
Scope Item	**Description**
User configuration	Support for: Add / Remove users. Grant / Remove permissions.
Mobile Application Management (MAM)	Support for: Publishing mobile applications. Pushing mobile applications. Configure mobile applications. Secure mobile applications. Monitor mobile applications. Update mobile applications.
Intune Company Portal App	Support for: Configuration Branding Device Enrolment Enrolment issues
Configuration and maintenance of device configuration policies	Android Policies for Mobile Device Management iOS Policies for Mobile Device Management There are many device level Configuration Policies available within Intune. Please see link below for summary information for each category. Device features and settings in Microsoft Intune | Microsoft Learn Each are utilized to create a custom series of Device control and experience settings and can be reviewed / evaluated to suite client needs.
Administer Remote Wipe, Remote Lock and Device Cleanup.	By using the Retire or Wipe actions, devices may be removed from Intune that are no longer needed, being repurposed, or missing and user / application data to render it non recoverable. Device will continue to be issued Wipe commands even if the device loses power and will process the command when it is next powered on. Wipe commends are supported by the current platform.
Reporting	Reporting on device enrolment (type and count).

3.8.2 Exclusions

CO-ITMS-MDM (Optional)	
Exclusion Item	**Description**
Support for non-Microsoft MDM solutions	Application specific support for non-Microsoft applications will be the responsibility of the client and / or third-party vendors.
Costs for Mobile device hardware	Purchase costs and hardware update costs are the responsibility of the client.
Costs for certificates	Required SSL certificates will be at an additional charge as required.
Out of support devices.	Device hardware no longer supported. Out of support OS versions.

4. Roles and Responsibilities

The table below provides a responsibility matrix for the core Managed Workstation - Azure elements:

Service Activities – Core Elements	Calligo	Customer
CO-ITSM-AVDP		
Provide 24x7 availability and alerting	R, A	C, I
Review and Report on System availability and Health	R, A	C, I
Remediation of Discovered health issues	R, A	C, I
Review and Maintain Logs	R, A	C, I
Respond to system alerts and initial triage	R, A	C, I
Review deployed applications	I	R, A, C
Report Consumption	R, A	C, I
Provide applications installation deliverables	C. I	R, A
Publish New applications	R, A	R, C, I
Resolving application deployment issues	I	R, A, C
Perform Incident triage and escalation to appropriate resolver groups	R, A	C, I
Respond to system alerts and initial triage	R, A	C, I
Service operational readiness and adoption	R, A, C, I	R, C, I
Configure Pool Sizes	R, A	C, I
CO-ITSM-IMG		
Initial creation of image (required project if net-new)	R, A, C	I
Provide customer-initiated configuration Item change requests with clear requirements	C, I	R, A
Provide Calligo initiated configuration Item change requests with clear requirements	R, A	C, I
Validate customer proposed image changes based on provided requirements	R, A	C, I
Validate Calligo proposed image changes based on provided requirements	C, I	R, A
Provide a virtualized testing environment (with KVM access as appropriate) for image build, deployment and verification	C, I	R, A
Apply change requests to Image	R, A, C	I
Verify implemented image changes against requirements	R, A, C	I
Build and test offline image builds on a predefined schedule	R, A, C	I
End to End deployment process validation	R, A, C	I
Notify Calligo of changes to supported models of hardware for image	C, I	R, A
Create and maintain driver packages	R, A, C	I
Download device drivers/software from vendor publicly available website	R, A, C	I
Apply driver package to image	R, A, C	I
Build application packages for model specific software	R, A, C	I
Provide physical hardware models for driver package and model specific software testing	C, I	R, A
Provide and configure remote access solution (IP KVM, vPro) and maintain connectivity	C, I	R, A
Validate all devices have an installed device driver	R, A, C	I
Complete driver functionality unit testing (display, power management, function keys, audio, etc.)	I	R, A, C

Service Activities – Core Elements	Calligo	Customer
CO-ITSM-IPM	**Calligo**	**Customer**
License Assignment	R, A, C	-
Administer the Intune platform	R, A, C	-
Administer the Windows Store for Business	R, C, I	R, A, C, I
Manually join devices to Azure Active Directory	C, I	R, A
Manually deploy Intune Agent	C, I	R, A
Define the requirements for policy changes	C, I	R, A
Recommend and implement policy changes	R, A	C, I
Provide a test environment for policy change unit testing	I	R, A, C
Manage Autopilot policies	R, A, C	I
Request management of new devices	C, I	R, A
Provision Autopilot devices	R, A, C	I
Delegate access to the Azure Active Directory platform	C, I	R, A
Manage on-premise Active Directory Group membership	C, I	R, A
Set policies for Mobile Devices Management	C, I	R, A
CO-ITSM-OSP		
Business application verification, maintenance, and testing	C, I	R, A
Patch Deployment	R, A, C	
Defining standard recurring deployment schedules, exclusions, and targets	C, I	R, A
Compliance measurement for SLO/SLA purposes	R, A, C	I
Maintenance of SCEM collections for systems in scope	R, A, C	I
Add and remove systems to scope	R, A	C, I
Review released list of patches from Microsoft and provide customer notification prior to scheduled installation	R, A	C, I
Identify patches to be excluded and approve list of patches for deployment	C, I	R, A
Identify business areas that require patch reporting and provide contact information for recipients	C, I	R, A
Provide SMTP relay for subscription-based delivery of reports and alerts	C, I	R, A
Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I
Identify patches to be excluded and approve list of patches for deployment	C, I	R, A
Identify business areas that require patch reporting and provide contact information for recipients	C, I	R, A
Provide SMTP relay for subscription-based delivery of reports and alerts	C, I	R, A
Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I
CO-ITSM-MON		
Configuring standard monitoring	R, A	C, I
Requesting monitoring changes	R, C	R, A
Responding to alerts	R, A	C, I
Remediation	R	R, I
Raising support requests	R	R, A
Contacting Calligo Service Desk via telephone for P1 Support Requests	I	R, A

Service Activities – Core Elements	Calligo	Customer
Correctly assigned the right category and priority to all incoming support requests	R, A	C, I
Providing full and detailed information when creating new support requests	I	R, A
Providing detailed and regular ticket updates	R, A	I
Responding to all ticket updates where additional information or testing is requested from Calligo Service Desk	I	R, A
Providing prompt confirmation of ticket closure agreements.	I	R, A
CO-SW-LICENCE		
Create a valid Customer Agreement between Application or OS vendor and Client	R, A	I
Accurate count of licenses required	A	R
Request changes to subscription being managed	I	R, A
Provide subscription billing invoices for managed subscriptions	A, R	I
Payment of subscription invoices from Calligo	I	R, A
CO-ITSM-MDM (Optional)		
Recommend parameters/settings for MDM configuration policies.	R, A	C, I
Provide MDM application list	C, I	R, A
Implementation of MDM configuration policies	R, A, C	I
Implementation of MDM application management policies	R, A, C	I
Define in scope end-user mobile devices for management	I	R, A, C
Remediate threats on end-user mobile devices	C, I	R, A
Remediate non-compliance with policies on end-user mobile devices	C, I	R, A
Generate tickets for incident management purposes	R, A, C	I
Service operational readiness and adoption	R, A, C, I	R, C, I
Respond and resolve customer-initiated service requests	R, A	C, I
Communicate and utilize device onboarding procedures for end-user mobile devices.	C, I	R, A
Manually install the Intune Company Portal application on end-user mobile devices using provided Procedures.	C, I	R, A
Sign into the Intune Company Portal on end-ser mobile devices to register devices in Azure Active Directory.	C, I	R, A
Manually setup exchange profile on end-user mobile devices using provided procedures.	C, I	R, A
Pilot and testing of policy changes.	C, I	R, A
Delegate access to the Office 365 portal.	C, I	R, A
Administer the Office 365 platform for devices.	R, C, A	I
Approve proposed configuration changes to O365 platform.	C, I	R, A

* Subject to having purchased Microsoft SPLA licensing from Calligo

R=Responsible, A=Accountable, C=Consulted, I=Informed

5. Reporting

The table below provides details on the additional Monthly Reporting and Analytics for Managed Workstation - Azure that are included in the core service:

Service Item	Reporting Item	Description	Frequency
CO-ITSM-AVDP	**Trend reporting**	Errors, Management Activities, Connections, Agent health Status	1 per month
CO-ITSM-AVDP	**Application issues**	Errors with installed applications	1 per week
CO-ITSM-IMG	**Task Sequence Deployment Report (MECM)**	The report includes compliance summary and a list of non-compliant systems.	1 per month.
CO-ITSM-IMG	**OS Versions**	List of all endpoints under scope and OS version details.	1 per month.
CO-ITSM-IMG	**Applications and versions**	List of installed applications and versions.	1 per month.
CO-ITSM-MON	**Monitoring Performance**	Average values of resource utilization for monitored systems during the previous period	Monthly
CO-ITSM-MON	**Monitoring Alerts**	Alerts raised during the previous period and current status (open or resolved)	Monthly
CO-ITSM-MON	**Device Monitor status**	List of configured monitors for each supported system	Monthly
CO-ITSM-OSP	**Asset lists (Deployment Collections)**	List of all assets currently in scope as well as their current collection memberships and deployment windows	1 Monthly. Sent a day after Patch Tuesday
CO-ITSM-OSP	**Patch Advisory**	The report lists all required patches that are scheduled for deployment.	1 Monthly. Sent a day after Patch Tuesday
CO-ITSM-OSP	**Pre-Patch Compliance Report**	The report includes compliance summary and a list of non-compliant systems.	1 per deployment. Sent prior to deployment.
CO-ITSM-OSP	**Asset Compliance State (Current Cycle)**	Current patch compliance state for the current month deployments.	1 Monthly after deployment completion
CO-ITSM-OSP	**Asset Compliance State (Cumulative Cycle)**	Current patch compliance state for the cumulative (OS in support Date through Current – 1) deployments.	1 Monthly after deployment completion
CO-SW-LICENSE	**License Consumption report**	Report of current license(s) purchase	1 Monthly

6. Data Residency

Calligo Data Residency

7. Service Requirements

Service Item	Requirements Item
CO-ITSM-AVDP	Provisioning - An Azure account with an active subscription
CO-ITSM-AVDP	Provisioning - No existing Azure AD DS domain deployed in your Azure tenant.
CO-ITSM-AVDP	Provisioning - Usernames you choose must not include any keywords that the username guideline list doesn't allow, and you must use a unique username that's not already in your Azure AD subscription.
CO-ITSM-AVDP	Provisioning - The username for AD Domain join UPN should be a unique one that doesn't already exist in Azure AD. The getting started feature doesn't support using existing Azure AD usernames when also deploying Azure AD DS.
CO-ITSM-IMG	The imaging technology is the latest released version of Microsoft System Centre Endpoint Manager, Microsoft Intune or Microsoft Deployment Toolkit.
CO-ITSM-IMG	Access to remote logs for testing results and troubleshooting is required for client systems.
CO-ITSM-IPM	Intune is licensed as a stand-alone Azure service, a part of Enterprise Mobility + Security (EMS) and included with Microsoft 365. For more information on how to get Intune, see Intune licensing. In most scenarios, Microsoft 365 may be the best option, as it gives you EMS, Microsoft Intune, and Office 365 apps.
CO-ITSM-MON	Datto RMM Agent must be installed to all monitored assets
CO-ITSM-MON	Network connectivity and necessary access rules are required for all monitored assets
CO-ITSM-OSP	Current in support or Extended support Windows OS assets.
CO-ITSM-OSP	Deployment of Datto RMM agent and relevant firewall / access configurations for each in scope asset
CO-ITSM-OSP	An agreed and defined re-occurring maintenance window for automated patch installation and remediation activities
CO-ITSM-OSP	Reboots are permitted within the agreed maintenance windows.
CO-ITSM-OSP	Outbound internet access for monitoring and patching.
CO-ITSM-SD	Client is provided information on support access methods
CO-ITSM-SD	All Priority 1 incidents are logged, and the client must follow up with a telephone call into support.

8. Access Requirements

Requirements Item
Administrative access to all assets in scope as required for remediation actions
Service account for Datto RMM agent activities
An account with the global administrator Azure AD role assigned on the Azure tenant and the owner role assigned on subscription you're going to use.

SCEM Administrator access in System Centre Endpoint Manager console. This access is required to be able to perform all aspects of Image management. Intune Service Administrator is required for Microsoft Intune based Image configuration.
Local Administrator access to all systems in scope for this service including SCEM infrastructure servers. Local administrator access is required for troubleshooting and remediation actions.
Client provides network KVM or System access with a minimum of two physical assets for testing.
All required licenses for supported OS
Administrator access in Intune Platform console. This access is required to be able to perform all aspects of systems management.

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Changes to settings and policies	24BHR	Review and testing of desired change and production impact unless for testing only.	1 monthly
Add / Remove Systems from scope	24BHR	Systems may be added or removed from scope. Must be done via Change Control Process.	1 monthly
Monitoring Report	48BHR	Provides data available from the platform	1 per week
Additional service monitoring	48BHR	Additional monitors may be added to existing systems	1 per week
Modify alert recipients	48BHR	Alert recipients may be adjusted to include client stakeholders	1 per week
Modify alert thresholds	48BHR	Client may request custom thresholds for an alert to be raised	1 per week
On demand tracking of compliance states	1BHR	Specific KB patch tracking submission	1 Monthly
Image update (All)	24BHR	New packages, updates or policy changes.	1 per month.
Drivers Update	48BHR	New model drivers to be supported.	1 per month.

New Image release (All)	1QTR	Redesign specifications for all changes.	4 per year.
Offline Image Build (MECM)	24BHR		1 per Image.
Driver package (MECM)	24BHR	Supported Make / Model with revisions if available.	1 per supported Hardware Model.
Build and Capture Sequences (MECM)	1QTR		4 per year.
Add / Remove hardware from scope (All)	24BHR	Must be done via Change Control Process and Service Request tickets.	1 per month.

11. Standard SLO's

Service-Level-Agreement.pdf (calligo.io)

https://azure.microsoft.com/en-gb/global-infrastructure/geographies/#overview

Service Level Agreements – Home | Microsoft Azure

12. Related Documents

Supporting documents for this service:

Any clients onboarding to Calligo will require the following document as an introduction to service:

Calligo – Welcome to Support for Clients

13. Optional Services

In addition to the Managed Workstation - Azure service, Calligo can provide the following service items as optional add on services for Managed Workstation - Azure:

Service Item	Service Item Reference	Description
M365 Applications	CO-ITMS-M365APP	Calligo's M365 Application support provides real time monitoring of the M365 Tenant as well as User management and Mailbox provisioning. Technical support is provided for Word, Excel, PowerPoint, Teams, Outlook, OneDrive and SharePoint Online.
Application Currency	CO-ITMS-ACAAS	Calligo's Application Currency as a Service adds and additional layer of patch currency and security to installed third party applications.
M365 Anti-Virus	CO-ITMS-MAV	Calligo's M365 Anti-Virus provides endpoint level Antivirus and Malware protection.

Service Item	Service Item Reference	Description
Cloud Protect MFA	CO-CP-MFA	Multi Factor Authentication service
Service Delivery Manager	CO-ITSM-SDM	The Service Delivery Manager will be responsible for the business as usual and account management relationship. This will include service reviews, point of escalation, responsible for Information Technology Infrastructure Library (ITIL) practice adherence, interfacing with third-party suppliers also participating under the customer's Service Integration and Management model and ensuring that Calligo meets or exceeds Service Level Objective (SLO) targets.
Technical Account Manager	CO-ITSM-TAM	The Technical Account Manager will be responsible for the technical collaboration between the customer and Calligo support teams and will play a key role in technical service improvement, managing deployment of new services or configuration changes, ensuring optimal performance and uptime of the application stack, and interfacing with third-party suppliers as required under the customer's support model.

14. Auxiliary Services

14.1. Service Onboarding & Transition

To launch Managed Workstation - Azure service successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. Calligo will undertake several workshops to discuss and confirm each element of the service to ensure all parties are aware of roles and responsibilities in advance of service launch.

Service transition and onboarding covers areas such as ticket management setup, platform readiness with knowledge share, and finalising all ITIL practices. A test and acceptance criteria are captured and signed off, to allow for the Managed Workstation - Azure service to commence.

After service launch, Calligo uses a formal service transition framework as the basis to carry out acceptance into service procedures, for new services landing into managed services. We typically engage at the initial stages of a project to ensure service operation adoption and readiness is planned and carried out correctly. This materializes as follows:

- To review designs, build and test artefacts to ensure supportability.
- Attend change review boards to gain early sight of changes by way of knowledge acquisition.
- To witness and validate designs and builds are delivered as proposed and intended.
- Complete operational into service documentation, training, and runbook enablement, which is required as part of the service hand-over.

14.2. Change Request and Change Control Process:

All infrastructure changes introducing risk to the environment will require change control which includes, but not limited to, Microsoft Security Patching, Infrastructure Upgrades, Deployments, Configuration Item status change. This can be generated from maintenance or an event such as an upgrade required on the system released by Third Party vendors, requested by the customer, or from a monthly release of security patches.

Where possible Standard Changes will be used with minimal risk, repeatable implementation steps, and prior approval from the customer in the form of an email.

An Emergency, or unplanned, change process will be raised to resolve a Priority 1 or 2 incident or to implement an emergency Security Patch. This accelerates the time to implement and resolve.

All Requests for Change will be reviewed internally, assessed internally, and authorized or rejected through Calligo ITSM tool.