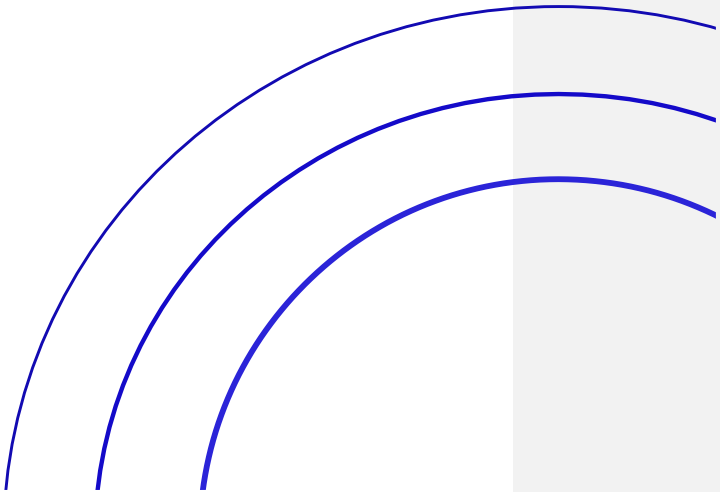
Calligo

CloudCore Service Description



Document Control

TITLE:	**CloudCore Service Description**	**DOCUMENT REF NO:**	QMS REC52
DESCRIPTION:	This document defines the services provided by Calligo's CloudCore service		
OWNER/ AUTHORITY:	VP, Cloud Operations	**VERSION NO:**	1.6
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	25/11/2022
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The VP Cloud Operations 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, Project Management Frameworks as well as the guidance and requirements of the CSSF.
Approved by the Chief Operating Officer, Calligo ("Entity") on 25 November 2022

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Initial Issue	Director, Product & Service Development	CEO	28/10/17
1.1	Verbiage Review	Director, Product & Service Development	CEO	10/11/17
1.2	Added RACI Matrix, Glossary of Terms and amendments	Director, Product & Service Development	CEO	16/01/18
1.3	Verbiage Review	Director, Product & Service Development	Chief Experience Officer	22/01/18
1.4	Group Review	Legal Counsel	CISO	19/03/18
1.5	Verbiage Review	Legal Counsel	Director, Product & Service Development	23/03/18
1.6	Re-design, change of ownership and verbiage review	VP, Cloud Operations	Chief Operating Officer	25/11/22
1.7	Remove Service Locations table and add link to external Service Locations document.	Director, Operations Management	Chief Operating Officer	10/01/23

1. Service Overview

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

CloudCore is a managed "Infrastructure as a Service", commonly referred to simply as (IaaS), a form of IT outsourcing delivering compute, network, and storage resources over the internet, or dedicated private circuit, to companies on a "fixed term contract" basis.

2. Service Inclusions

2.1. CO-CC-BVDC

This service provides IaaS base VDC.

2.2. CO-ITSM-MON

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

2.3. CO-ITSM-OSP

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

2.4. 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

2.5. CO-SW-LICENSE

This service provides Application, OS, and Appliance licensing.

3. Service Provisions

3.1. CO-CC-BVDC

3.1.1. Inclusions

CO-CC-BVDC	
Scope Item	**Description**
Configuration and Management of CloudCore infrastructure	Configuration and management of CloudCore infrastructure.
Monitoring of CloudCore infrastructure	This element of service is described in SI: CO-ITSM-MON
Patching of CloudCore infrastructure	This element of service is described in SI: CO-ITSM-OSP
VDC Internet Connectivity	Responsible for Virtual Datacentre internet connectivity
Specification of VDC	Specification of client virtual datacentre (e.g.: specification of CPU, RAM and Storage) Specification of the design for the client dedicated managed services context hosted on virtual datacentre.
Configuration of VDC	Configuration of client virtual datacentre (e.g.: configuration of CPU, RAM and Storage)
Firewalls	Configuration of client firewalling, routing, Network Address Translation, Virtual Private Network, and load balancing services
Specification of Calligo VM templates	Specification of Calligo Virtual Machines templates.

Deployment, configuration, and support of Calligo templated VM's	Configuration & provision of client Virtual Machines resources (storage, memory, processor, network) Deployment & configuration of Virtual Machines from Calligo template. Installation of Virtual Machine Operating System For Virtual Machines provisioned from a Calligo template Management of client Virtual Machines deployed from a Calligo template
Application Support	Deployment, configuration, monitoring and management of applications related to services provided by Calligo.
IP Management	Management of internal private IP addresses Provisioning of Public IP addresses
Domain Management	Management of internal domains
Remote Access	Configuration, management, and maintenance of remote site access on Calligo sites.
Operating System Support	Troubleshooting of issues at the Operating System or application level for virtual machines deployed from a Calligo template.

3.1.2. Exclusions

CO-CC-BVDC	
Exclusion Item	**Description**
Specification of client networks	Specification of client internal networks in virtual datacentre
Specification of client VM's	Specification of client Virtual Machines size/resources (storage, memory, processor, network)
Specification of client customised VM's	Specification of client customized Virtual Machines / Virtual Machines templates.
Build and Implementation	Implementation of the design for the client dedicated managed services context hosted on virtual datacentre. Migration of client systems and data into client Virtual Datacentre
Internet Connectivity	Customer internet connectivity.
Customer owned Hardware, Software, and application specific licences	Customer owned hardware, software, and licenses.
Remote Site Access	Configuration, management, and maintenance of remote site access to CloudCore on client side
Backup Services	Add on as required (Additional Cost) – This element of service is described in SI: CO-CC-BAAS
Disaster Services	Add on as required (Additional Cost) – This element of service is described in SI: CO-CC-DRAAS
Deployment, configuration, and support of VM's not Calligo templated	Deployment & configuration of Virtual Machines not from Calligo template (client customized template, solutions deployed and/or maintained by/with third party vendors.). Installing Virtual Machine Operating System not provisioned from a Calligo template (client customized template, solutions deployed and/or maintained by/with third party vendors.). Manage Virtual Machines not created from Calligo templates (client customized template, solutions deployed and/or maintained by/with third party vendors.)
Security Services	Add on as required - This element of service is described in SI: CO-CC-SCC
IP Address Pricing	Add on as required (Additional Cost) – Public IP Addresses
DNS Domains	Add on as required (Additional Cost)
Licensing of Virtual Machines	Add on as required (Additional Cost) - This element of service is described in SI: CO-SW-LICENSE
Licensing of Microsoft client applications	Add on as required (Additional Cost) - This element of service is described in SI: CO-SW-LICENSE

3.2. CO-ITSM-MON

3.2.1. 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)

3.2.2. 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

3.3. CO-ITSM-OSP

3.3.1. 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.

3.3.2. 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.

3.4. CO-ITSM-SD

3.4.1. 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.

3.4.2. 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.

3.5. CO-SW-LICENSE

3.5.1 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

3.5.2 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

4. Roles and Responsibilities

The table below provides a responsibility matrix for the core CloudCore elements:

Service Activities – Core Elements	Calligo	Customer
CO-CC-BVDC		
Configuration and management of CloudCore infrastructure.	R, A	
Virtual Datacentre internet connectivity	R, A	I
Specification of client virtual datacentre (e.g.: specification of CPU, RAM and Storage)	R	A
Configuration of client virtual datacentre (e.g.: configuration of CPU, RAM and Storage)	R	A
Specification of client internal networks in virtual datacentre.	C	R, A
Configuration of client internal networks in virtual datacentre.	R	A
Specification of client firewalling, routing, Network Address Translation, Virtual Private Network and load balancing services provided from CloudCore service	C	R, A
Configuration of client firewalling, routing, Network Address Translation, Virtual Private Network, and load balancing services provided from CloudCore service	R	A
Specification of the design for the client dedicated managed services context hosted on virtual datacentre.	R, A	I
Specification of client Virtual Machines size/resources (storage, memory, processor, network)	C	R, A
Configuration & provision of client Virtual Machines resources (storage, memory, processor, network)	R	A
Specification of client customized Virtual Machines / Virtual Machines templates.	C	R, A
Specification of Calligo Virtual Machines templates.	R, A	
Deployment & configuration of Virtual Machines from Calligo template.	R, A	
Installation of Virtual Machine Operating System For Virtual Machines provisioned from a Calligo template	R, A	
Monitoring of client Virtual Machines deployed from a Calligo template up to the Operating System level.	R, A	I
Management of client Virtual Machines deployed from a Calligo template.	R, A	
Deployment, configuration, monitoring and management of applications related to services provided by Calligo.	R, A	I
Troubleshooting of issues at the application level for applications related to services provided by Calligo.	R, A	I
Licensing of non-Microsoft client Virtual Machine Operating System (including client customized template, solutions deployed and/or maintained by/with third party vendors.)	C	R, A
Licensing others client applications (non-Microsoft).	C	R, A
Customer internet connectivity.	I	R, A
Customer owned hardware, software, and application specific licenses.	I	R, A
Management of internal private IP addresses	R, A	
Management of internal domains	R, A	

Management of Public IP addresses	R, A	
Configuration, management, and maintenance of remote site access to CloudCore on client side	I	R, A
Configuration, management, and maintenance of remote site access on Calligo side.	R, A	I
Configuration, management, and maintenance of remote site access to CloudCore on client side	I	R, A
Troubleshooting of issues at the Operating System or application level for virtual machines deployed from a Calligo template.	R, A	I
Troubleshooting of issues at the infrastructure level	R, A	I
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
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
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
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
CO-ITSM-SD		
Raising support requests	R	R, A
Contacting Calligo Service Desk via telephone for P1 Support Requests	I	R, A
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

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

5. Reporting

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

Service Item	Reporting Item	Description	Frequency
CO-CC-BDVC	Availability	Uptime of the platform	Monthly
CO-CC-BVDC	Capacity	Capacity of the clients VDC	Monthly
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-CC-BVDC	All service requests or changes are logged via the Calligo ITSM system by clients.
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.

Commented [JC1]: Same, what is the required networking

Commented [SP2R1]: We have those details as part of acceptance docs

8. Access Requirements

Requirements Item

Access to hosted servers is either by virtual private network (VPN) or dedicated communication links depending on Client requirements.
Administrative access to all assets in scope as required for remediation actions
Service account for Datto RMM agent activities

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
CPU	1 Business Day	10% change in existing quota	10 Monthly
RAM	1 Business Day	10% change in existing quota	10 Monthly
Storage	1 Business Day	10% change in existing quota	10 Monthly
IP Addresses	1 Business Day	5 Total IPs with no previous requests in the current quarter	10 Monthly
Bandwidth	1 Business Day	10% change in existing quota	10 Monthly
Addition of a dedicated circuit	Vendor dependant		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

11. Standard SLO's

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

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 CloudCore service, Calligo can provide the following service items as optional add on services for CloudCore:

Service Item	Service Item Reference	Description

CloudCopy (BaaS)	CO-CC-BAAS	Calligo's Backup as a Service is a managed service that is designed to remove the overhead and complexity of managing and restoring data, irrespective of where the data resides. By establishing a secure connection to Calligo's hosted infrastructures, data can be safely and securely backed up and stored in encrypted format to protect the integrity of the data.
CloudShield (DRaaS)	CO-CC-DRAAS	Calligo's DR as a Services to designed to maintain business continuity and minimise data loss 24/7 without the need to invest in "always-on" hardware. Designed to replicate virtual, physical and cloud hosted servers to Calligo's hosted servers between Calligo datacentre regions, IT workloads are automatically replicated in real time providing continuous data protection (CDP) with the ability to perform point in time recovery. Calligo will manage the failover of protected critical systems as defined by the client in the event of a failure and restore services within agreed service levels to meet business continuity objectives.
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.
CloudWeb - SSL Certificates	CO-CW-SSLCERT	Calligo's SSL Service provides purchasing and provisioning of Certificates implemented in Client environments.
CloudProtect Server for CloudCore	CO-CP-SCC	This service adds Antivirus and Malware protection to the CloudCore environment.

14. Auxiliary Services

14.1. Service Onboarding & Transition

To launch CloudCore 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 CloudCore 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.

14.3. Superseded patch scenarios

This relates to the behavior which occurs when a newer update is released after the patch cycle has started:

- **Revisions -** When a metadata only revision to an update is made, the update identified in the deployment is still installed. There is no new update released by the vendor for this. Updates with material changes (binaries) are considered superseded updates and the supersede rule applies.

- **Supersede -** When the update source marks an included patch as superseded, the superseded update will not be installed. The newer update will need to be included at a future patch cycle.

- **Expiration -** At the time of installation, when a patch has been included for installation but is marked as expired by Windows Update, the install of that patch will not occur. The asset will report compliant since the patch no longer meets the requirements to install. Where a newer update becomes available it will need to be included on a future patch cycle.