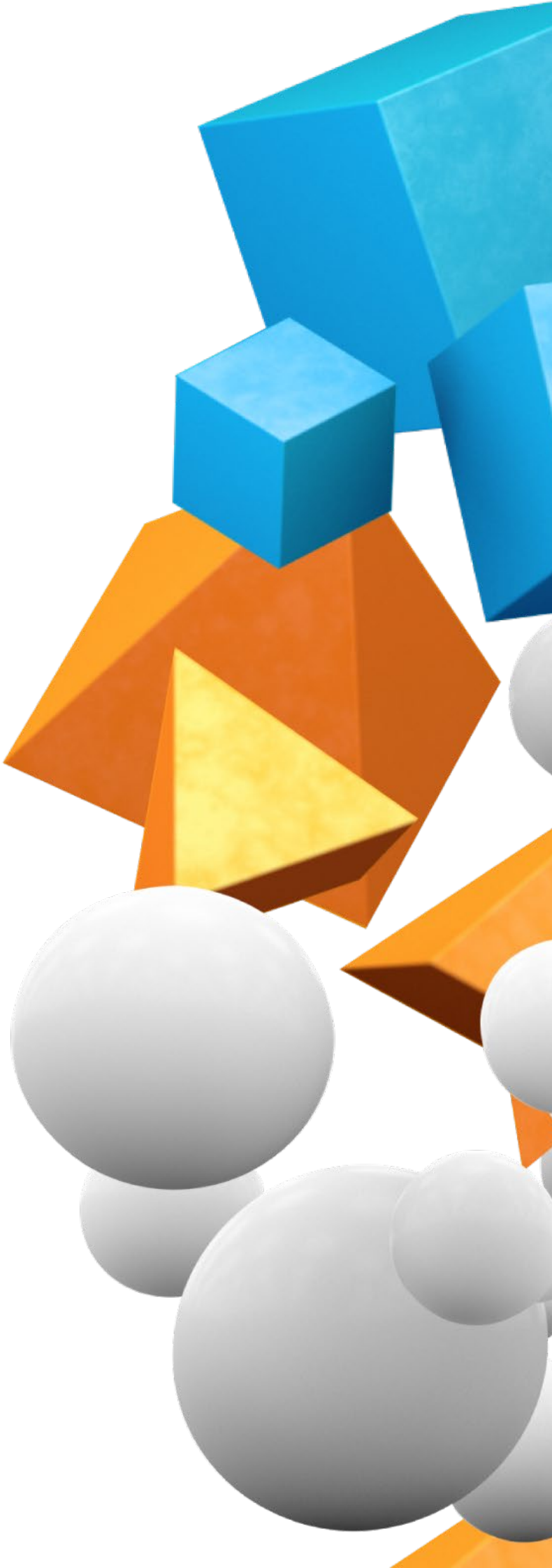
Service Description – CloudProtect 2FA for External Customers



TITLE	Service Description – CloudProtect 2FA for External Customers
DOCUMENT REFERENCE	QMS REC83
DESCRIPTION	Service description for the “CloudProtect 2FA for External Customers” service.
OWNER / AUTHORITY	Director of Product & Service Development
QMS / ISMS DOCUMENT CROSS REFERENCE	• QMS QP4 – Design & Development of Products & Services • QMS REC28 – Design Board Submission
VERSION NUMBER	1.0
VERSION DATE	01/08/2019

Contents

1. Introduction

The purpose of this document is to detail the CloudProtect Two-Factor Authentication (2FA) for External Customers service according to ITILv3 standards.

It sets out:

- the key features of the service;
- responsibilities; and
- how you can use the service.

As with all services, we are at times dependent on you, as the Client, to take certain steps to enable us to properly provide this service. We have described, by way of a RACI matrix, how our responsibilities will be apportioned and what we require from you.

This is intended to help you to identify what we do and, perhaps just as importantly, what we don't do in respect of each service. If you believe any area of responsibility (whether on our behalf or yours) needs to be amended or up-dated, please contact us at https://calligo.cloud/io.

This Service Description is subject to change from time as time, as our services develop to meet our client's needs. We will notify you in writing of such changes as they occur.

If a conflict exists between the terms of (a) our Master Services Agreement and/or standard terms and conditions and (b) this Service Description, the terms of the documents listed at (a) shall govern.

The Service Description form part of the service design and is used to document the key elements of the service.

2. Service Information

CloudProtect 2FA for External Customers provides unified access security, which includes secure access to your applications and data, regardless of where your users are and on any device. This reduces the risk of a data breach and ensures trusted access to sensitive data.

2.1. Key Product Features

There are 3 editions available; Bronze, Silver and Gold. The Bronze edition includes:

- Integration with Client Applications
- One time passcodes via call, text or from mobile application
- Per user enablement, allow only those who need two factor authentication
- Restrict two factor authentication to specific IP addresses
- Enrol multiple phones per user if required

In addition to the above Silver offers:

- Risk Assessment via Phishing simulations
- Access Policies
- Enforces devices are secure and have up-to-date software
- Checks enabled security settings on mobile devices
- Checks Location and network data

In addition to all the features above Gold also offers:

- Identify corporate and personal devices for Clients using BYOD policy
- Limit access of applications to devices – corporate vs personal
- Secure on-premises applications

2.2. Locations of Service

The service is available globally.

2.3. Relation to other services

None.

2.4. Using the service

Client can perform the following with the service:

- Fully manage “CloudProtect 2 Factor Authentication (2FA) for External Customers” service (if required, fully managed otherwise)
- Add new users to the service
- Remove or amend Users from the service
- Setup/Configure authentication against access to their Application(s)
- Track and monitor access devices such as OS type and support

The Client’s use of the service is based on the following assumptions:

- That the Client will follow secure computing best practices
- Be responsible for the management of the service and any remedial work required to its own or third party applications and services, unless otherwise agreed with Calligo.

If the Client fails to meet those assumptions, Calligo will not be able to provide this service in the manner intended, if at all.

2.5. Requesting additional resource

Requests to make changes to Administrative access, and any service changes will require a service request ticket that will be actioned according to the Calligo Service Desk response times based upon priority of the request. The current Calligo Service Desk SLA’s are published at https://calligo.cloud/licences

2.6. Commercials

The latest prices per unit are available from our Account Management team and/or as contained in your Statement of Work (SOW).

2.7. Service Level

Service Availability target = 99.95% per calendar month. The service is available 24 hours 365 days a year.

If availability on a monthly basis falls below 99.8%, we will provide credits for the service affected as described below:

Monthly Uptime Percentage < 99.8%	Service Credit - 10% (of monthly charge)
Monthly Uptime Percentage < 99%	Service Credit - 25% (of monthly charge)

(For further information, please see our Service Level Agreement -https://calligo.cloud/licences).

2.8. Access to service

Clients can access the service via any of the supported devices provided the application has been installed or can receive text messages via any standard mobile/cell phone number. Details of the latest supported list can be found here https://calligo.cloud/compatibility in the Calligo compatibility matrix.

Administrative access if setup is available via the Vendor's website at https://admin.duosecurity.com/

2.9. Levels of Access

Clients using the service can have one or more of the following roles:

- Admin – Fully manage their subscribed service via the Vendor's portal.
- User – Can logon to the user's organization application(s) via a onetime passcode/sms/push notification for authentication.

2.10. Responsibilities

The service has split responsibilities to deliver all functionality and the following responsibilities are defined for each party:

2.10.1. RACI Definitions

- Responsible - Those who do the work to achieve the task. There is at least one role with a participation type of responsible
- Accountable - The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those responsible. In other words, an accountable must sign off (approve) work that responsible provides. There must be only one accountable specified for each task or deliverable
- Consulted - Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication
- Informed - Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication

Matrix

Item	Responsible	Accountable	Consulted	Informed
Creation of Client Account	Calligo	Calligo	Client	
Creation of Admin User for Organization	Calligo	Calligo	Client	
User management	Calligo	Client		
Setup/Configuration of Application Integration to MFA	Calligo	Client		
Configuration of policies for MFA access	Calligo	Client		
Maintaining a suitable client device to connect to the service	Client	Client	Calligo	
Ensure that the device is always available when accessing Client Applications	Client	Client		
Notify Calligo of any changes to Service requirements	Client	Client	Calligo	
Compliance with third party terms and conditions	Client	Client		

2.11. Documentation and Training

The end user documentation for this service is found on the Calligo Supportal as well as from Duo.com. The end user documentation for this service on the Calligo Supportal,

There is no formal training provided by Calligo for this service.

2.12. Standards and Policies

This service is compliant with the following compliance standards and policies up to the responsibility boundaries:

- ISO 9001
- ISO 27001

2.13. Backup and Restore

The two factor service is provided by a third party who provide their own back and resiliency. Clients have the ability to back up their own account from the client application on mobile devices.

2.14. Scheduled maintenance windows

The service does not require a maintenance window that affects the availability SLA.

2.15. Appendix A – Availability Table

Availability %	Downtime per month
90% ("one nine")	72 hours
95% ("one and a half nines")	36 hours
97%	21.6 hours
98%	14.4 hours
99% ("two nines")	7.20 hours
99.5% ("two and a half nines")	3.60 hours
99.8%	86.23 minutes
99.9% ("three nines")	43.8 minutes

2.16. Appendix B – Glossary

Access Control - A process that regulates who or what can view or use resources, either physical (like IT assets) or virtual (like connections to networks, files, and data).

Authentication - The process of verifying the credentials of a user, device, or action, as well as the origin and integrity of data.

Bring your own device (BYOD) – policy of allowing employees to bring their personal devices (laptops, tablets, and smart phones) to the workplace, and to use them to access the Organization's data and applications.

DNS (Domain Name Service) – A computing service used to translate an IP address to a name. Used both for public domains such as www.xyz.com and private internal domains.

GB – Gigabyte of capacity, 1 GB = 1024 Megabytes.

Gold Build – Template from which other virtual machines can be provisioned from. Contains all the required OS and software pre-installed.

High Availability – A configuration that provides for the loss of components within a site and maintain the service that is being delivered without the need to recover from backup or switch to another site.

Infrastructure as a Service (IaaS) – A service that provides computing resources such as memory, CPU, networking and disk to allow for virtual machines to be hosted in a resource consumption based model.

Input Output Operations Per Second (IOPS) – A unit of measurement for disk storage performance.

ITILv3 – Version 3 of the Information Technology Information Library which is a collection of best practice processes and documents to manage an information technology company.

Multiprotocol Label Switching (MPLS) – A network connection for high performance networking over the internet that can use quality of service to provide better reliability.

MB – Megabyte of capacity, 1 MB = 1024 Kilobytes.

Multi-tenant – Shared service or resources to provide a commodity of scale service where users pay for a subset of the service or resources as is required by the user.

Phishing - An attempt to deceive users and illegally acquire sensitive information by contacting them under the guise of a trusted source. Phishing typically employs emails or instant messages that appear to be legitimate, combined with imposter websites, to make bogus requests for personal details such as names, passwords, Social Security numbers, or financial credentials.

Platform – A grouping of technology and services that provide the overall service that is being delivered.

Platform as a Service (PaaS) – A service that provides tools to create computer applications without the need to run virtual machines that have operating systems (OS). The service is consumed on a resource consumption model.

Point-to-Point (P2P) – A private physical network connection between two locations not over the internet.

Protection Group – A group of virtual machines that are replicated together for consistency.

Public IP Address – A unique computerised address used in computer networks to define destinations for communication on the internet.

Recovery Time Objective (RTO) – The time in which a protected item can be made available for use after recovery.

Recovery Point Objective (RPO) – The point at which any protected item can be recovered to. This stipulates the potential amount of lost time or data.

Single sign-on – The use of a single credential to access multiple services or applications.

Software as a Service (SaaS) – A service that provides access to an application for use without access to any associated OS or infrastructure required to run that application. The service is consumed on a resource consumption model.

Solid State Disk (SSD) – A disk with no moving parts offering greater performance than traditional hard disk drives (HDD).

Storage Volumes – A logical partition of a storage system used to hold specific data.

TB – Terabyte of capacity, 1 TB = 1024 Gigabytes.

Multi Factor Authentication (MFA) – The use of a secondary authentication in addition to a username and password to gain access to a service or application.

User Persona – Settings and data specific to a user's configuration of an operating system or application. Allows for these settings to be transferred between virtual machines.

Virtual datacentre (vDC) – A logical representation of a physical datacentre's resources such as CPU, Memory and Disk.

Virtual Desktop – A virtual representation of a physical desktop comprised of memory, CPU, network and disk. The virtual desktop runs an operating system and applications.

Virtual Machine (VM) – A virtual representation of a physical server or desktop comprised of memory, CPU, network and disk. The virtual machine runs an operating system and applications.

Virtual private network (VPN) – An encrypted network connection over the internet between two end points.

2 Factor Authentication (2FA) – This is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are.

3. Document Control

DOCUMENT OWNER & APPROVAL
The is the owner of this document and is responsible for ensuring that this procedure or process is reviewed in line with the review requirements of Calligo's Integrated Management System.
Approved by Director of Product & Service Development, Calligo on 01 August 2019

CHANGE HISTORY RECORD				
VERSION	DESCRIPTION OF CHANGE	AUTHOR	APPROVAL	DATE OF ISSUE
0.1	Initial draft	Paresh Parmar		31/01/19
1.0	Initial release	Paresh Parmar	Mark Thomas	01/08/19