



e2e Managed Peripherals Service - Service Definition Document



OVERVIEW

A range of **cloud peripheral and cloud access device managed services**, purchased as a service on a month by month basis. These services are primarily designed to support e2e's other cloud services such as our Cloud IaaS and PaaS services, Managed Cloud VM services, Cloud Security Services and Cloud Connect and Mobility services, although it is possible for us to provide these services to customers in order to support their use of any other cloud services (IaaS, PaaS or SaaS).

TYPICAL USE CASES

- Organisations who want to transition to the cloud but do not have the skills, time or desire to provide and manage the end user devices and peripherals.
- Organisations who have fully embraced the cloud model and want a fully cloud-enabled working environment and services to facilitate seamless office based and remote working.
- Organisations who wish to turn their offices based IT services into cloud based office services – i.e. want to be able to remove all on prem office equipment and support and instead see the office as simply a set of desks with internet connections to their cloud services.
- Organisations who wish to reduce office based costs and fix office links to the cloud with simpler, cloud based services
- Organisations who want to move their desktop computing services to a cloud model but still require an office with printers and desktops
- Organisations wishing to add secure mobility services – who want to use secure, managed mobile devices to access cloud services.
- Organisations that require a secure end to end solution in order to comply with security standard such as ISO27001:2013 and Cyber Essentials Plus (CES+) or other security demands imposed by their customers. These services are all designed to assist organisations with such assessments and tests.
- Organisations that simply want an end to end, pay as you go cloud based IT service model that enables them to focus on their business and utilise the latest technology and cloud based services securely.
- Organisations who recognise that the end user devices are critical to the overall security of their business.

The service comes in three variations that align with the organisation's workload, availability, threat and data classification posture. Organisations can choose a profile that meets their security requirements. All e2e Managed Services are designed to handle OFFICIAL and OFFICIAL-SENSITIVE data.

The managed service support model can also be scaled up on demand (on a day by day basis if needed), providing outstanding value for money and return on investment.

- ✓ **Assured security** – highly experienced team capable of securely maintaining and configuring devices and working with expert design advice that follows the latest CESG guidelines
- ✓ **Service assurance** – expert service management and maintenance designed along ITIL guidelines to ensure a quality service

- ✓ **Secure management** – we manage your devices from a secure operations centre thereby reducing exposure to your device management interfaces
- ✓ **Enables your team to focus on cloud compute** – removes the pain of managing cloud access and peripheral component
- ✓ **Standards compliance** - having assured services and process in place helps with your Information Assurance and standard such as ISO27001.

Note: this is a support and management service that does not provide any actual equipment or hardware.

FEATURES

- Provides managed services for End User Devices (EUDs), desktops, laptops, tablets, printers, Wi-Fi access points, networking and mobile devices
- Includes Cloud Connect Mobile VPNs and MDM services
- Includes secure builds, anti-virus and standard applications designed to facilitate your use of or transition to cloud services
- Designed to handle OFFICIAL and OFFICIAL-SENSITIVE data

BENEFITS

- ✓ Allows you to focus on utilising your cloud services/applications
- ✓ Allows you to consume cloud services securely
- ✓ Receive the benefits of the cloud without the hassle
- ✓ Scale your service level up and down daily or monthly
- ✓ Easy to leave with short minimum term
- ✓ Have the freedom to choose the best cloud service
- ✓ Reduce office IT costs
- ✓ Enables you to focus on service consumption and not management
- ✓ Benefit from pay as you go, easy to join, easy to leave services

TYPES OF DEVICES MANAGED BY THE SERVICE

- Cloud based Wi-Fi access points (i.e. access points managed through cloud services)
- Supporting office networking that provides access to the internet
- Office based printers (that are used to print from cloud solutions such as print servers in an IaaS or PaaS service, cloud SaaS applications or cloud end user devices or virtual machines that require printing, scanning or other office bound print related services)
- Cloud end user devices; desktops, laptops, tablets and mobile phones used to connect to cloud services

MOBILE WORKFORCE MONITORING

With the expansion of mobile working and the consequent fluidity of working environments our service offers some unique protective monitoring and alerting features when this service is used in conjunction with the Cloud Connect Service and Protective Monitoring Service:

GEO ALERTING

It is possible to define acceptable location policies that control which countries your personnel can connect from when travelling. Once defined we monitor your mobile devices and alert should a breach occur.

LOCATION REPUTATION CHECKING

It is possible to define in our system which types of environment are acceptable for use by your mobile work force. Our service monitors the environments your mobile devices are in (such as a coffee shop, hotel Wi-Fi, airport Wi-Fi, or other known compromised networks) and alerts if a potential policy breach has occurred. Our service determines and alerts on how private a mobile users internet link is. Many environments pose serious threats to privacy either by enabling an attacker to sweep up all communications on a compromised network, providing compromised network elements (such as DNS services) from which to attack, or by spying on a mobile device with cameras or close proximity individuals.

IDENTIFICATION OF COMPROMISED HOME NETWORKS

Home working is becoming a norm and although it offers great flexibility, organisations cannot rely on the security of the home environments. Although it is possible to encrypt mobile devices and communications, corporate assets are still vulnerable to attacks from a compromised home network. Many home routers are insecure and traffic and user behaviour will often reveal much insight to an attacker. This could lead to data loss, reputational damage, or corporate compromise. Our service can identify and alert when a home network is compromised.

CUSTOMER RESPONSIBILITIES

The customer is responsible for all hardware, equipment, devices, power, cabling and the purchase of the actual internet connections at the location. The service covers devices in offices, at home, and mobile; e2e manage the device and are responsible for the health and proper functioning of the device but not any location specific issues such as power or internet problems.

HOW DO WE DELIVER THE SERVICE?

All of these services are cloud managed – we manage everything over the Internet from our cloud based operations centre. We have different levels of service levels and security – to suit most security requirements; all our service delivery methods are suitable for OFFICIAL and OFFICIAL-SENSITIVE and all our builds are in line with the latest CESG guidelines. We are CES+ and ISO27001:2013 and IASME certified and operate our cloud services out of two UK based Tier 3 and Tier 4 datacentres.

There are a number of scenarios:

1. Customer uses e2e Cloud Connect service for secure laptop, desktops, printing etc.
 - In this scenario e2e cloud connect secures the end user devices and the Wi-Fi and switches are managed as part of the secure cloud connect service. Cloud connect is also used to provide secure printing and management of any onsite services
 - e2e use cloud connect to remotely manage EUDs, etc – all through secure IPsec VPNs in line with CESG architectural practice and guidelines
 - In this scenario all office based services and devices are effectively in the cloud – they are all securely connected to the internet and other cloud services by Cloud Connect; the user experience is the same no matter where or how they are connected
2. Customer does not use e2e Cloud Connect but instead uses another cloud access solution provided by their cloud supplier
 - In this scenario e2e will evaluate whether providing the service in this scenarios is repeatable, secure and supportable. Extra on boarding effort may be required in this scenario.

HOW DO I KNOW WHICH SERVICE IS APPROPRIATE?

There is a level of service appropriate for all organisations. If you do not currently know what the right level of service is we offer a simple process:

1. e2e provide a free, one day on site cloud workshop led by a CESG Senior IA Architect where we work with your organisation to establish your requirements and cover aspects such as your organisations risk profile and security assurance requirements, connectivity requirements as well as your platform and application requirements.
2. The workshop report includes expert advice from e2e and includes generating your heat map similar to the below and this gives us a score:

Heat Map Scoring Chart														
0-3	4	5	6	7	8	9	10	11	12	13	14	15		
Very Low	Low		Medium			High			Very High					

3. This score then maps to our recommended services:

Recommended Service				
Score	Basic	Enhanced	Premium	Custom
3	Basic			
4	Basic			
5	Basic			
6	Basic			
7		Enhanced		
8		Enhanced		
9		Enhanced		
10			Premium	
11			Premium	
12			Premium	
13				Custom
14				Custom
15				Custom

4. If you need more help we can provide follow up workshops with no commitment from you to purchase a cloud service. We will walk you through a risk based approach that starts with your business requirements and allows you to decide which service aligns best.

LEVELS OF SERVICE

Baseline	
Service Hours	8am to 6pm Mon-Fri
Service Hours Response Time	4 hours
Emergency/out of hours 24/7 response time	8 hours
Change Windows	Inside Service Hours
Server Patching routine	Monthly, inside service hours
Enhanced	
Service Hours	8am to 6pm Mon-Fri
Service Hours Response Time	1 hour
Emergency/out of hours 24/7 response time	8 hours
Change Windows	Inside Service Hours plus 2 changes/month out of hours.
Server Patching routine	Monthly outside Service Hours – all emergency and non-monthly security patches charged in addition
Other benefits	Includes secure remote support/assistance
Premium	
Service Hours (change windows 24/7/365)	24/7
Service Hours Response Time	1 hour
Change Windows	24/7
Server Patching routine	Up to twice Monthly emergency and security patching included
Other benefits	Includes secure remote support/assistance Monthly service review included.

	<p>One day per month on site support Named technical account manager.</p>
--	--

SERVICE LIMITATIONS

e2e's service levels above include support for the device, its connectivity to a network (Wi-Fi or wired) and are based on ensuring the device is functioning. It does not include application support; it does include troubleshooting any fault that is down to an e2e build or e2e configuration issue. It does not include any hardware, hardware support or warranty – all hardware is the responsibility of the customer.

The service is designed to keep the devices running, secure and patched.

SCALE UP AND SCALE DOWN SERVICE OPTIONS

e2e offer an innovative solution that provides unique flexibility to their Service. Customers can scale up service levels and can also scale down. This allows them to utilise the appropriate level of service at all times thereby avoiding situations where customers are paying for premium support services when they require a more basic level.

SHORT TERM SERVICE SCALE UP OPTIONS

The service includes the BAU activities relating to managing the service but it is possible that the customer requires the reassurance of having e2e resource on hand to support their IT team during critical times.

The service adds scale up support to cover emergencies or other times of high service demand or heightened importance.

MEDIUM TERM SERVICE SCALE UP OPTIONS

It is possible to scale up from Baseline to Enhanced and from Enhanced to Premium or from Baseline to Premium.

There are no one off charges for scaling service levels up or down.

Customers are charged at the new level of service pricing for the period of time they operate at that level of service. There is a one month minimum term for a scale up of this type and the customer can scale down in the same manner.

CLOUD SERVICE SCALE DOWN OPTIONS

It is possible to scale down from Enhanced to Baseline and from Premium to Enhanced or from Premium to Baseline.

Customers are charged at the new level of service pricing for the period of time they operate at that level of service. There is a one month minimum term for a scale up of this type and the customer can scale down in the same manner.

OTHER SERVICES

Build - we work with you to incorporate any custom server/VM builds required for your applications. We then use these templates to deploy to your devices.

Custom Cloud design - we work with you to incorporate any customisations you wish to make. We can accommodate many different types of customer specific requests as long as they relate to configuration only (not bespoke development) and charge on a time and materials basis.

Ad hoc support – we come and spend the day with you and your team assisting with any support issues or working as one of your support team to assist in a support task. This would only be needed in exceptional circumstances but we understand that there may be critical events that requires as much de-risking as possible and having an e2e cloud support expert on site is one way to achieve this.

Data migration services - we assist you to move your data into or out of a cloud service. Can also be used to connect to and migrate data to other cloud systems such as hybrid or public cloud services for the purpose of data or machine migration or configuring ongoing hybrid cloud services.

Advice and consultancy – these days are typically used to support your organisation at times when you need expert cloud architects on site to support you. Examples of such events are when internal or external auditors have design/architecture questions, meetings with Accreditors/Assessors, preparing for penetration tests, preparing to roll out new applications to the cloud, cloud planning activities, presentations to the board/IT managers or any other such event that requires technical cloud architects present to support you.

Initial risk workshop and service alignment – we need to ensure we understand your business and its risks so we can jointly agree the right service level.

MORE INFORMATION AND CONTACT DETAILS

For more details on this service and to see the other services we offer visit

www.e2e-assure.com

Enquiries, and more information is available on request, email info@e2e-assure.com with any queries.

WHO ARE E2E?

e2e are a cloud security company with 20 years' experience of providing military grade cyber security. We provide repeatable cloud-based services to the public sector. Security depth, quality and service excellence set us apart from our competition.

OUR ORIGINS

e2e was founded by two industry experts, each holding 20 years' experience of delivering secure, end-to-end solutions. We have a history of designing secure networks for online payment systems; designing, developing and delivering cyber defence solutions; developing and starting up complete Managed Service solutions; and have built several worldwide Data Centres. Our clients over the years have covered most sectors from banking to the MoD.

OUR PEOPLE

e2e have brought together a highly experienced team of cloud experts, developers, security architects, CESG CLAS consultants, support specialists, security analysts and expert cyber security business development specialists. This core team has since been bolstered by the addition of a vibrant cloud support and cyber analyst team, recruited through channels such as the Cyber Security Challenge UK, SANS Cyber Academy and other government backed schemes to find cyber talent.

OUR WORK IN GOVERNMENT

We have earned an excellent reputation over the last three years as a trusted service provider to government and our cloud services are helping deliver key UK wide services. All our services are ISO27001:2013 accredited, CES and CES+, IASME certified, and we are the go-to organisation when a need for cost effective, cloud based services are required that must be secure to protect UK sovereign reputation. Our services to government cover central government, local government as well as other public sector organisations.

OUR AMBITIONS

e2e are a service company. We have a well-developed range of cloud-based services, all of which are designed to be repeatable, scalable, flexible and on-demand.

- We aim to be the best supplier: the easiest to deal with, the most reliable, and the best at delivering cloud service support and managed services. So far we have made a huge impression with our existing customers – e2e just does it better than the competition.

- We aim to be the most secure supplier, to deliver and maintain the most secure services. There is simply no other supplier on the market with our security credentials and no other supplier with the technology and team to deliver security-as-a-service at our level. We are miles ahead in this area and this is where we want to stay.

OUR METHODOLOGY

We focus on applying well established skillsets and a wealth of experience to ensure highly responsive delivery without sacrificing quality. We invest in our technology and our people so that our customers can benefit from our thirst for excellence. We understand how to integrate security seamlessly into our services, giving you secure cloud based services that 'just work'.

We have fully embraced the 'As a service' model: e2e is a cloud based business, with a cloud business model, operating model, service delivery model and we deliver all our services from our cloud based operations centre.

OUR QUALIFICATIONS

e2e is a UK based SME Company operating exclusively from within the UK using SC cleared staff. We operate out of two UK datacentres (Tier3 and Tier4). We are ISO27001:2013 accredited, CES and CES+, IASME certified, CLAS members, CESG CCP Senior level, UKCEB members, TechUK members, BCS and IoD members, Crown Commercial Suppliers, UK Cyber Security Forum members. We sponsor and recruit from the Cyber Security Challenge UK as well as the SANS Cyber Academy. We understand how to work with partners and ensure we are honest and straightforward to deal with. We embrace the cloud first approach and are heavily involved in UK Cyber in general; we want to help spread the UK cyber messages (CESG Cloud Security Principles, 10 steps, Get safe on line, etc.) and are active CiSP members with strong links within UK Cyber.

