REDCENTRIC

MANAGED WIRELESS LAN SERVICE
SERVICE DEFINITION

SD072 V5.0
Issue Date 31st May 2018

redcentric
business technology. managed.

1) SERVICE OVERVIEW

1.1) SERVICE OVERVIEW

The Redcentric Managed Wireless LAN Service (Managed WLAN Service) offers design, deployment, monitoring, support and management of wireless LAN infrastructure deployed on Customer sites. The service utilises products from one of the leading Wireless LAN manufacturers.

The service delivers enterprise features and uses centralised, cloud based systems for provisioning, monitoring and management. Engineers in Redcentric's Service Management Centre (SMC) manage Customer WLAN environments undertaking administration tasks and resolving issues as necessary.

The standard Service can be enhanced with additional optional functionality to offer enhanced Guest Internet Access for example. Charging for the Managed WLAN Service is based on a per access point, per month model.

2) SERVICE DESCRIPTION

2.1) COMPLEMENTARY SERVICES

Redcentric offers an extensive portfolio of services designed to meet the requirements of companies of all sizes. Specifically Redcentric's Managed Firewall Service, Managed LAN Switch Service, Internet Service and connectivity portfolio are designed to complement the Managed WLAN Service.

2.2) SERVICE DESIGN

The Managed WLAN Service can accommodate a wide range of coverage, performance and functionality requirements. Solution design is based on requirements of each individual customer site, and not a generic design.

2.2.1) Initial Design

A Radio Frequency (RF) coverage plan is produced using Customer provided location plans of the areas of the building(s) where WLAN coverage is required. The individual components required to deliver the Service including specific model(s) of Access Point (AP) and any centralised authentication infrastructure are derived from specific Customer requirements for each site.

The initial design is based on the following customer supplied information:

- Location floor plans
- Details of internal features (wall type)
- Anticipated user density
- Required services (E.g. Data, Voice, Guest Internet access etc.)
- Security requirements including WLAN encryption and authentication methods
- Radio coverage and system redundancy requirements
- Details of Internet access where Redcentric is not providing Wide Area Network connectivity

External factors such as interference and building construction can affect the wireless coverage.

Customers can select optional site surveys which generally results in a design more likely to meet any Radio Frequency (RF) coverage requirements, and without a site survey the design is less likely to provide optimum coverage.

2.2.2) Design Guidelines

Redcentric produces initial desktop designs based on industry best practice by applying the following design principles by default:

- For data only wireless, Redcentric will propose AP coverage overlap of 15% and no resilient AP visibility.
- For data only wireless where a level of resilience is required, Redcentric will propose AP coverage overlap of 15% per cell with visibility of 1 additional AP at -75dBm.
- For voice/video (e.g. real-time traffic), Redcentric will propose AP coverage overlap of 20% per cell with visibility of at least 2 AP's at -67dBm.

2.3) WIRELESS LOCAL AREA NETWORKS

The standard Managed WLAN Service is capable of supporting several Wireless LANs. Wireless LANs have many uses, two of the most common being 1) to extend the corporate wired LAN to support wireless end-user devices and 2) to provide visitors' Guest Internet access. A maximum of 8 Service Set Identifiers (SSID's) can be configured. However, good design dictates that there should be as few as possible. Each SSID generally maps to a local VLAN on the wired LAN.

2.3.1) Corporate Wireless LAN

Connection to the Corporate LAN will be provided using a dedicated SSID which can be broadcast from all or a sub-set of the access points on the managed wireless network. Authentication and authorisation of corporate users and/or devices will be achieved using either:

- The Customer's existing RADIUS server and an authentication credential store such as the corporate Active Directory or a compatible LDAP compliant server. If the customer requires a RADIUS server to be supplied as part of the solution this can be provided at additional cost.
- A Redcentric supplied authentication server – please see section 2.4.1 below

2.3.2) Guest Internet Access Wireless LAN

The basic Managed WLAN Service enables the Customer to provide a basic Guest Internet access capability to its visitors, via a dedicated SSID. There are two alternative options:

2.3.2.1) **Basic Guest services**

If so required by the Customer, the SSID may be configured as an 'open' SSID allowing a user to associate with this SSID with no requirement for a Pre-Shared Key.

On opening a web browser and attempting to access an Internet page the user will be re-directed to a 'captive portal' which will prompt the user to enter the pre-defined guest username and password. Once the user has input the correct details and accepted the applicable terms and conditions access to the Internet will then be permitted.

Redcentric will change the password on the Customer's behalf on a monthly basis (or less often if required) and inform the dedicated customer contact(s) of the new password.

2.3.2.3) **INDIVIDUAL END USER AUTHENTICATION**

As an alternative to using a generic guest user account, guest users can be authenticated against either a Customer provided authentication server using the RADIUS protocol, or a Redcentric provided authentication server – please see section 2.4.2 below.

Redcentric recommends the user authentication approach rather than a single shared user name and password for all users, since this will enable the customer to maintain greater oversight of the use of its service.

2.4) ADVANCED SERVICE OPTIONS

The following services are optionally available to enhance the Standard Managed WLAN Service. Redcentric will provide you with details of applicable additional costs when designing the Service.

2.4.1) Enhanced Corporate authentication Option

The enhanced corporate option provides the following features:

- Ability to apply relevant network permissions (E.g. VLAN assignment and/or firewall rules) based on the user's or workstation's group membership.
- Ability to apply Network Access Control (NAC) polices to devices. For example this could ensure that devices connecting to the corporate WLAN meet anti-virus and patch management policies.

2.4.2) Enhanced Guest Option

The enhanced guest option provides the following features:

- Guest sponsorship. As part of the Guest login process, a web portal prompts guests to provide the email address of their visiting sponsor. The sponsor can grant or reject access to the Guest.
- Use of text messages to associate a mobile phone number with a user. Naturally a Short Message Service (SMS) gateway is required to achieve this and SMS charges are applicable.
- Portal customisation. This allows customisation of the guest registration interfaces to provide full corporate branding. The Customer is required to provide Redcentric suitably formatted template(s).
- Guest portal access. This provides access to authorised users and allows them to review, configure, customise and monitor guest accounts (e.g. view guest activity and set the start date and/or end date of individual accounts)
- Multiple guest portals. Required when Customers have different Guest profiles, each to be treated differently.

2.4.3) On-Boarding of Non-Corporate Devices Option

This option allows Customers to implement on boarding policies for non-corporate devices and control the level of access these devices have within the corporate network.

This option presents a dedicated WLAN (SSID) where non-corporate devices can connect. Authentication requests are passed to the Customer's corporate directory infrastructure using the method described in the standard service corporate access section above. Assuming access is granted, a digital certificate is made available for the device to accept. If that device is subsequently lost or stolen the certificate can be revoked to prevent that device gaining access to the corporate network.

To have a previously authorised device's certificate revoked, the customer should contact the Redcentric helpdesk with full details of the device (make, model and MAC address) and Redcentric will carry out the revocation on the Customer's behalf.

2.4.4) Internet Access Policy Enforcement – Managed Firewall Option

Standard design dictates that users connected to the corporate WLAN access the Internet through the same gateway (i.e. firewalls) as corporate devices on the wired network – this does not form part of the Managed WLAN Service.

Where users connected to the Guest WLAN access the Internet via Redcentric's central infrastructure, a dedicated security gateway is required. For optimum functionality, Redcentric deploys next generation firewalls where the Customer does not wish to deploy their own Guest Internet firewall(s).

Redcentric's next generation firewalls support content filtering, anti-virus and intrusion detection functionality in addition to application-aware firewalling. Furthermore, models from one firewall manufacturer communicate with the wireless LAN infrastructure through Application Programming Interfaces (API) to provide unrivalled logging and reporting capability.

2.5) WLAN INTERNET ACCESS AND COMMUNICATIONS DATA

2.5.1) The Customer Corporate Wireless LAN and Guest Internet Access Wireless LAN services (together "WLAN Services") will be provided to end users by the Customer, and not by Redcentric (Redcentric will provide such services to the Customer as subcontractor). The WLAN Services will be branded accordingly, and basic branding will be set up during implementation of the services. Bespoke branding will be provided if the Customer chooses the portal customisation services (see paragraph 2.4.2).

2.5.2) The Customer will be responsible for all user management in relation to the WLAN Services, including (1) (unless otherwise agreed in writing) user authentication and (2) maintaining and supplying to government agencies etc. any records relating to the use of the WLAN Services as required by law from time to time.

2.5.5) The WLAN Services are set up in such a way that each end user must accept the Customer's end user licence agreement (EULA) before being able to access the service. The WLAN Services are provided with a simple and generic EULA between the Customer and the end user. The generic EULA will not be suitable for the Customer's business, and the Customer must amend the EULA to suit its own requirements (as explained in, and subject to, the legal agreement between Redcentric and the Customer).

2.6) LICENSING

All subscription and licensing costs required to deliver the basic and, when chosen, optional functionality are included in the Charges for the Managed WLAN Service. The number of licences incorporated into the design for the basic Service and any optional features form part of the contract between Redcentric and the Customer for the provision of the Services. If additional licences are required for any reason (e.g. to resolve issues relating to higher than expected user or guest count), additional one-off and/or recurring Charges (at Redcentric's standard rates at the relevant time) may be applicable.

2.7) REDCENTRIC RESPONSIBILITIES

Redcentric is responsible for the following aspects:

- Solution design based on information and requirements provided by the customer
- Configuration of the centralised management, reporting, etc. components
- General upkeep of the platform including hardware and software upgrades
- Ongoing support of Customer-specific WLAN configuration including advice and implementation of minor changes
- Arranging replacement of faulty hardware

2.8) CUSTOMER RESPONSIBILITIES

The Customer is responsible for all other aspects including but not limited to:

- Providing Redcentric with the Customer's detailed coverage, functional and other requirements
- Providing Redcentric with the technical details required for the design. E.g. WLAN IP address ranges, SSID names, VLAN assignments, local DNS servers, DHCP scopes and options etc.
- Providing Redcentric with the Customer's branding template and Acceptable Use Policy (AUP) for Guest portal
- Providing Redcentric with suitable digital security certificate(s) as required – this is commonly a wild-card certificate
- Configuration of DNS to match the fully qualified domain name(s) of any required digital certificate(s)
- Install and connect access points unless Redcentric installation option is chosen
- Ensuring LAN is configured correctly and is fit for purpose, unless Redcentric Managed LAN switch option is chosen
- Ensuring suitable cabling is in place to connect access points to the wired LAN, unless Redcentric LAN cabling option is chosen
- Undertaking any design changes required after initial deployment
- Unless otherwise agreed with Redcentric, end user authentication, including supplying and maintaining an authentication platform being a RADIUS server and an authentication credential store such as the corporate Active Directory, or a compatible LDAP compliant server
- Meeting any compliance requirements associated with offering a public Internet service to guests

2.9) DEPLOYMENT

Deployment of the Redcentric Managed WLAN Service is simplified thanks to Redcentric's centralised provisioning platform. Access Points added to the Customer's appropriately configured local and wide area networks will connect to Redcentric's centralised provisioning platform and use a secure connection to pull down configuration details.

The Managed WLAN Service has been designed so that Customers can physically deploy / install APs using their own resource. Alternatively Redcentric can optionally arrange for engineering resource to complete this task at an additional cost.

2.10) LAN CABLING

Charging for the basic service does not include any structured cabling checks, cable work or patching between the Customer’s existing wired switch infrastructure and the location of each AP. Redcentric will undertake a general or detailed survey of existing structured cabling on request, and provide a report on its suitability. Redcentric can arrange for cabling to be upgraded, repaired, corrected, extended, tidied, re-patched, labelled and replaced as required to ensure a Customer’s entire LAN is fit for purpose. This work is chargeable and priced on application.

2.11) MANAGEMENT

Once deployed and commissioned, the Managed WLAN Service will be managed by Redcentric to ensure the wireless infrastructure is available and performs optimally. Management is provided by engineers in Redcentric’s SMC using a centralised management platform which connects to the WLAN infrastructure using secure tunnels.

2.12) DETECTION OF ROGUE ACCESS POINTS

The Managed WLAN Service APs monitor the RF space for other APs advertising the defined SSIDs in the surrounding area. If one of the defined SSIDs is being broadcast by another AP in the area, the managed AP reports details of the adjacent AP back to the centralised management server. If the adjacent AP is not on the list of APs being managed, the management server raises a rogue AP alert. A ticket will be raised and Redcentric staff will contact the customer. Rogue APs are a potentially serious security issue, and the customer should deal with the rogue AP as quickly as possible.

2.13) MONITORING / ALARMS

Under normal circumstances the Redcentric systems poll each access point every 5 minutes to confirm that it is available. This is in line with industry standard network management best practices. If an AP does not respond to several successive polls, an automatic alert is forwarded to the Redcentric network fault management system. This automatically raises an incident, which is placed in the technical support queue. Technical support engineers investigate these incidents 24 hours a day, 365 days a year.

Customers can become aware of problems in the short window before the polling procedures verify a problem and issue an alert. Redcentric provides additional means for Customers to raise faults, i.e. via telephone, email and the web portal.

Redcentric classifies problems according to severity. This allows the prioritisation of resource on issues that have the most impact on Customers’ businesses. Further details of the classifications can be found in Redcentric’s Customer Service Plan (CSP) which is available on request.

Redcentric is committed to continually improving and expanding its services, and in order to facilitate these improvements, it is necessary to carry out essential work from time to time. In accordance with Information Technology Infrastructure Library (ITIL) service management standards, these activities are carefully scheduled through the use of an internal change control process; this gives Customers maximum visibility of any given change and thereby ensures that planning and implementation is carried out to minimise the effect on Customers using Redcentric services.

Maintenance windows and procedures for communicating emergency outages are detailed in the CSP.

As well as availability polls, information regarding other aspects of the service is retrieved from the various platforms. Redcentric sets alarm thresholds for these parameters and support staff act accordingly when alarms are received.

2.14) HARDWARE SUPPORT

If Redcentric support desk staff determine that an AP has developed a fault, Redcentric will make arrangements to have it replaced 'next business day'. Customers can choose an expedited option which offers a target hardware replacement timeframe of 4 hours from the point that Redcentric determines a replacement is required. This timeframe is not practical for certain remote UK locations and Redcentric will notify the Customer of alternative target timeframes for these locations. Naturally, expedited hardware replacement will not improve repair times for faults caused by anything else. The expedited option is incorporated into the monthly Service Charge and is applicable regardless of the number of times it is called upon.

2.15) STANDARD REPORTS

Standard pre-defined reports provide Customers useful summary information on the following aspects of their service – a sample report is available:

- Access Point Uptime
- Bandwidth Usage
- SSID Usage
- Client Session Report
- Failed Authentications
- Rogues APs

Customers can use the monitoring / reporting portal to tailor these reports or produce other specific reports and access other useful information.

2.16) MONITORING / REPORTING PORTAL

As part of the establishment process Redcentric will provide the Customer access to management portal(s) for the Managed WLAN Service that provides real-time and historical information including the following:

- Access Point inventory and status
- Access point client connection details – active and historical
- Access Point utilisation
- Security events – e.g. rogue AP detection
- Visual radio frequency overview, heat map and floor plan coverage (Note: this is dependent on the Customer supplying floor plans and details of access points they physically deployed)

2.17) CONFIGURATION SUPPORT & CHANGE REQUESTS

The validation and consequential implementation of change requests will be performed Monday to Friday between 8 am and 6 pm, with a target completion time of 48 hours for routine changes. Emergency changes are prioritised accordingly and performance targets are detailed in Redcentric's Customer Service Plan (CSP).

In accordance with the Redcentric change request procedure, all change requests must be submitted by a designated and authorised Customer technical contact. If the Redcentric engineer cannot validate the change requester against the authorised list, the engineer will place the change request on hold and attempt to contact one of the alternative authorised contacts. Redcentric must wait for the request to be ratified by a known authorised contact before proceeding with any change. It is therefore essential that Customers provide accurate and current contact information for their designated and authorised staff.

It is extremely easy to weaken network security by submitting a seemingly innocuous change request. Redcentric staff review change requests based only on the information they have available, and therefore Redcentric cannot take responsibility for weakness resulting from changes. If Redcentric support staff believe that a change request compromises the security of the Customer's network, Redcentric may ask the Customer to sign a disclaimer stating that they wish to go ahead regardless of the advice offered. In extreme cases, staff reserve the right to reject the change outright; for example if the weakness could affect other Redcentric Customers.

2.18) PERFORMANCE ASSURANCES

Due to the nature of wireless networks where environmental conditions change constantly and it is not possible to control user density, any issues relating to RF interference and bandwidth congestion are beyond Redcentric's control. (E.g. coverage, throughput, bandwidth availability etc.).

2.19) SERVICE CHARGES

The following table details one-off and recurring charges for standard, optional and ancillary charges.

Service	Charges
Desktop Survey & Design	Included in standard Service
Optional RF Site Survey	One-off
Optional Cabling Survey	One-off
Optional engineer AP deployment	One-off
Standard Wireless Service	Per Access Point per Month *
Enhanced Guest Service	Per User per Month
On-boarding of non-corporate devices	Per User per Month
Firewall security for Guest access	See Managed Firewall Service

Alternatively Customers can elect to pay an initial one-off charge which results in a lower monthly service charge.

3) IMPLEMENTATION AND ACCEPTANCE

3.1) ACCEPTANCE CRITERIA

The following Acceptance Criteria apply to the Managed WLAN Service:

- Confirm that a sample of devices can authenticate and connect to the Customer’s corporate WLAN
- Confirm that a sample of devices can authenticate and connect to the Guest WLAN(s)
- Confirm that Customer can access administration portal(s)

4) SERVICE LEVELS AND SERVICE CREDITS

4.1) SERVICE LEVELS

The Service Level applicable to the Managed Wireless LAN Service is as follows:

Service Level: Availability of the Service at each individual Access Point **Measurement Period: Month**	
Service Level	Not less than 99.5% Availability.

4.2) EXCLUSIONS FROM AVAILABILITY

In calculating Availability, in addition to the exclusions listed in clause 6.7 of the General Terms the following shall be excluded:

- Failure of connectivity to the Customer site which prevents Redcentric from measuring Availability
- Inability of the Customer's LAN to connect to Redcentric's remote platform due to a failure of WAN connectivity and/or any other cause that is not part of any Services being supplied by Redcentric
- Unavailability due to throughput (load) exceeding initial documented requirements
- Unavailability due to onsite power, cabling or local network issues
- Malicious attempts to disrupt service such as wireless jamming, Denial of Service etc.

4.3) FLOOR SERVICE LEVEL

The Floor Service Level applicable to the Managed WLAN Service in respect of Availability shall be 85% per Access Point in any given Month - i.e. each Access Point has its own Availability Service Level and its own Floor Service Level.

4.4) SERVICE CREDITS

The Service Credits applicable to the Managed WLAN Service shall be calculated as follows:

For each Access Point where availability is <99.5% in the relevant Month, a Service Credit may be claimed according to the table below. For the avoidance of doubt, for the purposes of paragraph 5.4 of the General Terms, the maximum value of Service Credits in any Month shall be a sum equal to half the Charges which would have been payable in respect of the aggregate of all Access Points in that Month had Redcentric provided the Managed WLAN Service in accordance with the applicable Service Levels.

In the following table:
"≥" means "greater than or equal to" and < means "less than"
"MS" means the average Charge payable for an Access Point in respect of the WLAN Service for the same Month

Service Availability	Service Credit
≥99.5%	None
≥99.5% but <99.0%	5% of MS
≥99.0% but <96.5%	15% of MS
<96.5%	20% of MS

5) DATA PROCESSING

5.1) DATA PROCESSING SCOPE

- The Managed Wireless LAN Service delivers the transport of Ethernet packets between devices.
- The Managed Wireless LAN Service does not involve any storage or backing up of data.

5.2) DATA STORAGE AND ENCRYPTION

- Redcentric configures equipment to encrypt Wireless LAN traffic according to Customer requirements.
- Redcentric's Managed Wireless LAN platform captures standard information about traffic over the platform, including the MAC addresses of connecting devices, username, at which site and access point the connection took place, and for how long. This traffic data does not enable Redcentric to identify any individual, and is retained in order to meet the Customer's needs in the management of the platform. As part of the standard configuration the majority of traffic data is retained for up to a year, and then deleted. Many of the data retention periods are configurable to meet the Customer's requirements and instructions (subject only to statutory data retention requirements), and these instructions can be dealt with as part of the initial implementation or subsequently.
- Redcentric does not capture, inspect, analyse, store or share the customer's traffic/data under normal circumstances.
- Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the customer's traffic in order to investigate and diagnose a very specific problem, e.g. to help resolve a problem relating to packet corruption. Such diagnosis would involve the examination of a small sample of packets.

5.3) DATA PROCESSING DECISIONS

- Redcentric does not make any data processing decisions in relation to the Managed Wireless LAN Switch Service. Any processing of data over Customer systems when using the Managed Wireless LAN Switch Service for transit is instigated, configured and managed by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Managed Wireless LAN Switch Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4) SUB-PROCESSORS

- With the exception of physical deployment, no 3rd parties are involved in delivering the Managed Wireless LAN Service, and there are no sub-processors appointed by Redcentric.

5.5) CUSTOMER ACCESS TO DATA

- The Customer controls its own platforms which use the Managed Wireless LAN Service to carry data, and the Customer therefore has full access to its own data.

5.6) SECURITY ARRANGEMENTS AND OPTIONS

- Managed Wireless LAN devises are located at Customer locations/sites. It is the Customer's responsibility to ensure physical security at such locations/sites meets its needs.

HARROGATE (HEAD OFFICE)

Central House
Beckwith Knowle
Harrogate
HG3 1UG

THEALE

2 Commerce Park
Brunel Road
Theale
Reading
RG7 4AB

CAMBRIDGE

Newton House
Cambridge Business Park
Cowley Road
Cambridge
CB4 0WZ

READING

3-5 Worton Drive
Reading
RG2 0TG

LONDON

Lifeline House
80 Clifton Street
London
EC2A 4HB

HYDE

Unit B
SK14 Industrial Park
Broadway
Hyde
SK14 4QF

INDIA

606-611, 6th Floor
Manjeera Trinity Corporate
JNTU – Hitech City Road
Kukatpally, Hyderabad – 72

0800 983 2522
sayhello@redcentricplc.com
www.redcentricplc.com

redcentric
business technology. managed.

bsi.

ISO 9001 Quality Management
FS 603185

ISO 22301 Business Continuity Management
BCMS 603194

ISO/IEC 27001 Information Security Management
IS 603187

ISO/IEC 20000-1 Information Technology Service Management
ITMS 668453