



Advanced Cloud-based Telephony Service for General Practice

Better Workplace catalogue

Service Description: NHSE-BW-RS0101-D

Effective Date: 17 Nov 2023

redcentric

AGILE • AVAILABLE • ASSURED

Contents

Service Overview	3
Service Description	4
Service Components	6
Service Capability & Limitations	18
System Provisioning	22
Service Provisioning	23
Service Support	27
Service Levels & Service Credits	29
Professional Services	30

Service Overview

Unity IP Voice Pro is Redcentric's Advanced Cloud-based Telephony Service for General Practice. Unity IP Voice Pro service is a hosted enterprise voice solution for organisations needing to update their existing telephony system while controlling equipment, training, and operational costs.

Unity IP Voice Pro delivers:

- A carrier-grade IP telephony system with an extensive and innovative range of enterprise level user features
- Optional Unified Communications features including instant messaging, presence, video calling and desktop sharing.
- Access to the service from desktop IP phones, desktop PCs, laptops and supported tablet PCs and smartphones
- A fully managed and hosted service with 24-hour technical support
- Call centre options with advanced call control and reporting
- Free calls between staff connected to Unity IP Voice Pro
- Low setup costs with additional users and features charged on a pay-as-you-use basis.
- Improved productivity for mobile staff by providing them with full access to all voice functionality regardless of where they are working even on external phones such as in a hotel.
- A powerful but easy to use provisioning interface for the system administrator - no need for specialised inhouse or contracted skills to manage the telephone system.
- Project managed migration from an existing PBX environment on a per-user basis to maximise existing investment and avoid the need for a large, simultaneous upgrade.
- Rapid recovery in the event of major IT or office facilities failure with the ability to transfer all telephony services quickly and seamlessly to a temporary office location.
- A future-proof and highly scalable communications platform which can be easily integrated with your desktop computing environment.

Find out more

Watch our two Redcentric Unity IP Voice Pro videos to see features and benefits:

Introduction and Benefits - <https://www.youtube.com/watch?v=WHhVImwi6Ds>

Capabilities, handsets and integration options - <https://www.youtube.com/watch?v=VtXRN-mZgCU>

Why not join us in one of our Unity IP Voice Pro sessions. There will be an opportunity for you to meet our experts and ask questions. You can register for one of the next events at <https://www.redcentricplc.com/lp/webinar-modernising-healthcare-telephony/>

Service Description

The Unity IP Voice Pro Switches

The Unity IP Voice Pro service is built on two centrally managed, software based, IP Voice Pro Switches hosted in Redcentric's highly secure and resilient data centre environments.

This completely replaces the need for any customer site PBX equipment and enables customers to deploy Unity IP Voice Pro service with minimal upfront capital investment or in-house skills.

The Unity IP Voice Pro Switch technology is based on SIP (Session Initiation Protocol) which provides a highly, scalable, cost effective and future proof platform for the provision of IP voice services.

Redcentric's Unity IP Voice Pro platform has been deployed in a highly available configuration across Redcentric Data Centre locations in Reading and Shoreditch. The core Unity IP Voice Pro Switches are maintained and supported by Redcentric 24 / 7 and access to the Unity IP Voice Pro Service is delivered across Redcentric's national IP Network (Managed IP-VPN) and via a range of connection technologies including SoGEA, EFM, leased lines and 10Mbps, 100Mbps and 1Gbps Ethernet as required.

Redcentric UK Network - Managed IP-VPN

Unity IP Voice Pro is provisioned on a dedicated, secure VPN across Redcentric's Managed IP-VPN MPLS network*. To assure call quality and IP Telephony performance, Redcentric have implemented Quality of Service (QoS) systems throughout the network.

A direct connection from the customer site to the nearest Managed IP-VPN point of presence (POP) is required to provide service. These connections are available in bandwidths from 1Mbps to 1Gbps.

*Unity IP Voice Pro may also be delivered across certain 3rd party Internet connections by using the "Unity Off-Net" service for Polycom phones or by using Unity UC software clients.

PSTN Connectivity

For external calls, Redcentric offers a low-cost PSTN breakout service directly from within its core network, which removes the need for PSTN lines to be installed at each office. This can be a very significant saving particularly when compared with the cost of installing ISDN30 lines. Redcentric's high speed PSTN interconnect enables IP callers to make and receive external calls, for example other providers' landline telephones, mobile telephones, and international destinations.

Emergency Calls

Calls to the emergency services can be made using Unity IP Voice Pro, subject to the Unity IP Voice Pro service being available. Please see Section A of the Schedule to the MSA for further information about emergency calls.

Site location information is held by Redcentric, which defines the physical location address associated with each telephone number. This address information may be provided to the emergency services if they are contacted to direct them to the source of the call. As such the accuracy of this information is critical. The Customer is responsible for notifying Redcentric of any change address where voice services are provisioned. Moving services to a new location without providing updated site location information is in breach of the General Condition 4 of the General conditions of Entitlement enforced by OFCOM.

Audio Codec Preference

Unity IP Voice Pro can be specified to prefer the G.711 audio codec.

All outbound calls made will attempt to negotiate in G.711. This includes calls to both other sites within the organisation using the Unity service and external calls to the PSTN. All inbound calls from the PSTN will also attempt to negotiate in G.711. Inbound calls from other sites within the organisation will attempt to negotiate based on the codec preference for the calling site.

The G.711 codec uses approximately 100kbps of bandwidth per concurrent call (dependent on the network technology).

Service Components

Office Connectivity

Unity IP Voice Pro is delivered as a service over a Redcentric connection. If a Managed IP-VPN connection is already installed, it's usually possible to supply voice over the existing connection without significant modification if there is sufficient bandwidth capacity (see below for more details). Managed IP-VPN connections are available for small and home offices as a SoGEA connection, through to PPC and Ethernet connections for larger offices.

Unity IP Voice Pro can also be delivered over certain 3rd party Internet connections using the Unity Off-Net service.

Unity IP Voice Pro across Managed IP VPN

Each customer is provisioned with a private voice network over Managed IP-VPN. This ensures business grade call quality between sites. Managed IP-VPN is Redcentric's dedicated 10Gbps national MPLS network and is specifically designed to carry high volumes of both voice and data traffic without causing degradation to the voice service.

With the Managed IP-VPN connection, Redcentric provides a fully managed multi-service router for each customer site to shape traffic and to ensure that voice traffic is not negatively impacted by other traffic (such as Internet traffic) also using the Managed IP-VPN connection.

Unity IP Voice Pro across the Internet

Unity IP Voice Pro can be delivered across certain Internet connections using the Unity Off-Net service. Unity software clients also work via the Internet.

Unity IP Voice Pro Bandwidth Requirements

If all available voice channels to a site are in use, the Unity IP Voice Pro system will prevent an additional call being setup to protect the other active calls from call degradation.

An incoming call which is unable to complete because the circuit is congested will be treated as if the person they were calling was on the phone. This may include for example, diverting the call to voice mail, placing it in a queue, or diverting it to someone else.

A caller on hold does not consume a channel, it is only when the call is active (i.e., a two-way conversation) that a channel is needed.

Note: A call made between two phones on the same site does not consume a channel because once the call is established and the voice path is routed directly between the two phones and not over the Managed IP-VPN circuit.

Webex Softphone Package

The softphone package provides end users the ability to make, and answer calls on any device. The desktop, mobile, and tablet clients are all softphone capable.

The softphone client requires a suitable Internet connection. It registers and connects with Redcentric's voice platforms via the Internet and is therefore subject to the same limitations as the Unity off-net service. Please see limitations section for details.

Webex Softphone requirements

The Webex softphone is intended to work over wireless or wired Internet access. Please note that the quality of the experience when using the softphone is dependent on the availability of bandwidth and quality of the Internet connection available.

Please note that whilst the Unity service may work over mobile data networks, it is the customer's responsibility for ensuring that any such use of the service is permitted within the terms and conditions of their mobile provider. The customer is also responsible for any data charges incurred through such use of the service via mobile data networks.

Bandwidth requirements for the various Webex softphone features are as follows:

- HD voice call 100kbps (G.722)
- Standard voice call 100kbps (G.711)

Unity Reporting

Unity Reporting is fully integrated with the Redcentric hosted telephony service. Providing customers with meaningful insights into their ongoing business operations. A feature rich, fully customisable selection of real-time dashboards, wallboards, and historic reports, which are ideally suited to all customer environments.

The following table provides a summary of the different report styles available within the standard and Pro service offerings.

Reporting Area	Reports Included	
	GP Surgery User Professional	GP Surgery User Standard
ACD Agent List*	Y	-
ACD/DND Activity Log	Y	-
ACD N/A Code Usage	Y	-
Active Call/Contact List	Y	Y
Call/Contact Items by Day/Week/Month	Y	Y
Call/Contact Items By DDI/ID	Y	Y
Call/Contact Items by Half Hour Interval*	Y	Y
Call/Contact Items by Account Code	Y	-
Call/Contact Items by Telephone No/ID	Y	Y
Dashboard View	Y	Y
External Content (Via URL)	Y	Y
Extension List*	Y	Y
Historic Call/Contact List	Y	Y
Hunt Group List*	Y	-

Reporting Area	Reports Included	
	GP Surgery User Professional	GP Surgery User Standard
Trunk Interface List	Y	Y
Unreturned Lost Calls*	Y	Y
Wallboard*	Y	Y

The Unity Call Reporting service can only be used with Redcentric's Unity IP service. Customers can purchase additional supervisor / wallboard licenses if required.

Directory Enquiries

New telephone numbers provided as part of the Unity IP Voice Pro service are not as standard published into BT Directory Enquiries. Numbers ported to the Unity IP Voice Pro service from other providers are adopted as they currently exist.

Client Security

The Webex Collaborate client allows users to access and make use of features of the Unity service from their mobile device. It also provides remote access to corporate telephone directories and the ability to initiate business telephone calls. As such, it should be ensured that the use of the application does not contravene any corporate security or compliancy rules or guidelines. It should also be ensured that users using the application use the timed lock and security PIN code feature on their mobile devices to prevent unauthorised access to the Unity service in the event of loss or theft.

Customer Responsibility

- Under the OFCOM Condition 4 of the General conditions of Entitlement relating to site location information for emergency services:
 - Provision of accurate site location information for each telephone number provided as part of the Unity IP Voice Pro Service
 - Immediate notification of any changes of address associated where voice services are provisioned
 - Advising where users are nomadic and work from no fixed location
 - Notification where users change from working between a fixed location and being nomadic, or change from being nomadic, to working at a fixed location
- LAN Design, capacity, performance, and availability
- LAN port availability, cabling to desk, UTP patch cable supply
- LAN IP addressing, DHCP server availability and configuration
- Provision of required Quality of Service settings on LAN
- Provision of suitable computer hardware, software, equipment, and services necessary to connect to and to use the Unity IP Voice Pro service, and for ensuring that all equipment connected conforms to the specifications and routing protocols specified by Redcentric

- Configuration of any firewall or other Internet limiting device to provide Internet access on required ports to user PCs as specified to operate Unity IP Voice Pro software applications
- Local dial plans, definition of extension numbers and ranges, CLI preferences
- Local (company) dial plans and numbering
- Ensuring Customer administrators are authorised and trained in the use and configuration of Unity system
- Identification of any analogue telephone line requirements such as lift lines
- Office cabling*
- Provision, management, maintenance, and availability of any non-Redcentric network used for the delivery of the Unity IP Voice Pro service when using the Unity Off-Net service.
- Ongoing self-administration of system settings configurable within Group Admin configuration portal:
- access to the administration Interface by the Customer's system administrator enables control over certain functionality of the Unity IP Voice Pro Service and the management of accounts including:
 - Creation/configuration of authorised users (where required licences have been assigned by Redcentric)
 - Enabling/disabling licensed features Entering and maintaining dial plans, DDIs, extension numbers and CLI settings
 - Controlling voice mail settings
 - Integrating company-wide directories for click to dial features
 - Setup and configuration of licensed group services such as ACD/Call Centres and Auto Attendant/Name dialling
 - Ensuring the security and proper use of all user IDs and passwords (including those of the System Administrator) used in connection with the Services (including changing passwords on a regular basis) and must take all necessary steps to ensure that they are kept confidential, secure, used only for the proper purpose, and not disclosed to unauthorised third parties

Redcentric Responsibility

- Unity IP Voice Pro Core system operation, availability & Customer zone implementation
- Quality of Service across Managed IP-VPN VPN and across core network
- UK and international dialling dial plans
- Provision for the Customer's ability to make / receive calls to / from the PSTN.
- Supply of any software application required to use the Unity IP Voice Pro Service
- Redcentric reserves the right to access the administration Interface and the service configuration stored by the Customer at any time for technical and operational reasons and to amend, modify and update the Administration Interface as reasonably required from time to time.

Security - Voice Security Best Practices

The purpose of this section is to detail the potential security risks associated with the operation of any phone system and to provide information and requirements on how to minimise these risks when using the Webex Collaborate service.

Security and privacy must focus on controlling unauthorised access or excessive access to features within the voice platform. It is imperative that you ensure the correct level of security is implemented on your organisation's configuration to prevent fraudulent use of the Service. Fraudulent use can result in additional call costs to your organisation if the appropriate security measures are not implemented.

It's your organisation's responsibility to ensure adequate security practises/processes are followed and that the appropriate security measures are implemented. The security requirements in the following document are subject to constant review and improvement.

Background: How Phone Systems are attacked

Inherent within any voice system is the potential for abuse. The methods through which a service can be abused include the following:

- Unauthorised remote access to a telephony system to:
 - Make expensive calls at zero cost to themselves
 - Make calls to premium rate numbers to fraudulently generate revenue
 - Unlawfully intercept confidential information such as voicemail messages
- Deliberate and direct misuse by staff including:
 - Making expensive calls whilst at work to save on their own bill
 - Fraudulent use of call forwarding – when users misuse their call forwarding services to make long distance or premium rate calls by dialling their own number from outside the office
 - Calling premium rate numbers to generate revenue for themselves / another
- Inadvertent direct misuse by staff including:
 - Being coerced or tricked into dialling premium rate numbers
 - Being coerced or tricked into providing a service for fraudsters (such as through call forwarding)
- Deliberate remote misuse by staff including:
 - Dialling into the phone system from outside the office to make non-business or fraudulent calls
 - Accessing the system using a voice service web portal or software application to make non-business or fraudulent calls

Hackers are constantly looking for ways to access telephony systems via a user's account with a view to scanning the options for a means of making outbound calls. The Customer ends up bearing the costs of these calls, which are often made to expensive premium rate or international numbers. Details of how to hack into telephone systems are even posted on the Internet.

Ensuring that each user's password is hard to deduce is the primary method to combating the fraudsters.

If a hacker accesses a system, fraudulent abuse may take the form of:

- Accessing a user's account and establishing an onward call from the system.
- Accessing a user's account, setting the call forwarding to an external number (such as a premium rate dialling service) and then calling the user's number at a local rate.
- Interception of the user's confidential voicemails.

All these attacks are preventable with the adoption of a simple voice security policy. It is imperative that adequate security is implemented on your organisation's telephony configuration to prevent this.

It is important to note that the following configuration elements including the definable policies are included within your security policy.

1. Group Administrator and end-user Passwords
2. End-user voice-mail passcodes
3. Outgoing Calling Plan
4. Making outgoing calls through the voice-mail portal
5. Housekeeping (managing new and redundant user accounts)

Group Administrator and End-User Passwords

The Group Administrator (responsible for management of the Unity IP Voice Pro Service at Group level) and users require passwords to access the web admin portal. This portal provides the group admin with administrator privileges, allowing them access to manage the Unity IP Voice Pro Service and configure users and features. This portal also provides users with access to configure and manage their own individual features. The user passwords are also used by users to log in to the voice service software applications.

Unauthorised access to the portal at either group or user level would have significant security consequences and as such Redcentric require the following:

- Passwords must be at least 8 characters in length
- Passwords must contain at least:
 - One number
 - One uppercase character
 - One lowercase character
 - One non-alpha numeric character
- Password ageing is enabled by default at system level. *
- The limit for password retries lock-out is set to 3 or less to prevent multiple systematic retries.
- The e-mail address to which account lock-out notifications are sent is constantly monitored.

Note: Customers who do not wish to enable password ageing by default will be required to sign a customer waiver prior to Redcentric disabling this feature. The waiver can be accessed by calling the support desk.

Password Rules

The group administrator can manage password rules as follows:

The screenshot shows the 'Password Rules' configuration window. At the top, it says 'Configure the password rules to be used when creating or updating passwords.' Below this is a 'Cancel' button. The 'Rules apply to:' section has three radio buttons: 'Group Administrators Only' (selected), 'Group Administrators and Users', and 'Group Administrators and Users use external authentication'. There is also a checkbox for 'Allow users to be created on web portal'. The 'Password format:' section has several checkboxes: 'cannot contain the login ID', 'cannot contain the old password', 'cannot be the reverse of the old password', 'cannot be any of the last 3 passwords' (with a dropdown set to 3), 'must contain at least 1 number(s)', 'must contain at least 1 uppercase alpha character(s)', 'must contain at least 1 lowercase alpha character(s)', 'must contain at least 1 non-alphanumeric character(s)', and 'must be at least 8 characters' (with a dropdown set to 8). The 'Passwords expire:' section has two radio buttons: 'Never' (selected) and 'After 60 Days'. The 'Disable login:' section has two radio buttons: 'Never' and 'After 3 failed login attempts' (selected). There is a checkbox for 'When login is disabled, send e-mail to:' with a text field containing 'support@redcentricplc.com'.

End-User Voice-Mail Passcodes

The easiest way for hackers to access a telephone system is by selecting a user number then trying 'easy' passcodes to gain access to the menus. Because of this, Redcentric require the following voicemail passcode rules are followed:

- Passcodes cannot be the user's own extension or phone number
- Passcodes must not be repeating digits such as "1111" or "2222" etc.
- Passcodes must not use "1234" or use their extension number.
- Passcodes must be a minimum of 6 digits
- The limit for passcode retry lock-out is set to 3 or less to prevent multiple systematic retries.
- Ensure the e-mail address to which account lock-out notifications are sent is constantly monitored.

Passcode Rules

A screenshot of the passcode rules screen in which the group administrator can manage passcode rules follows:

Passcode Rules
Configure the passcode rules to be used when creating or updating Portal passcodes.

Cancel

Passcode format: ☒ cannot be the user's own extension or phone number
☒ cannot be the user's own extension or phone number reversed
☒ cannot contain 3 or more repeated digits
☒ cannot contain more than 3 sequentially ascending digits or 3 sequentially descending digits
☒ cannot be repeating patterns
☒ cannot be any of the last 1 passcode(s)
☒ cannot be the reversed old passcode
☒ must be at least 4 characters, no more than 8 characters

Passcodes expire: ☐ Never ☒ After 30 Days

Disable login: ☐ Never ☒ After 3 failed login attempts

☒ When login is disabled, send e-mail to:
support@redcentricplc.com

Outgoing Calling Plan

The Outgoing Calling Plans (OCP) dictate what types of telephone numbers can be dialled by users. This includes originating (making) calls, and what service numbers that users can forward or transfer calls to. The OCPs are set and managed by the Group Administrator via the web admin portal. This feature can specify calling plans for the entire group, or individual departments. Redcentric strongly recommend that only the minimum number of call types are permitted. **Redcentric also recommends that calls to premium rate numbers and international destinations are barred.**

A screenshot of the Outgoing Call Plan screen for originating calls below:

Outgoing Calling Plan
Customize the Outgoing Calling Plan for the group and/or departments.

OK Apply Cancel

Originating Initiating Call Forwards/Transfers Being Forwarded/Transferred

Department	Group	Local	Freephone	National	International	Not Used	Directory Enquiries	Not Used	PNS (070)	PRS (0871)	PRS (09)	Casual	URL Dialing	Unknown
Group Default	Y	Y	Y	Y	N	Y	N	N	N	N	N	N	Y	Y

Select from drop-down list to permit call type; Users can be configured with their own custom settings in user-level Calling Plan

Legend

- Allow Y
- Block N
- Authorization code required A
- Transfer to 1st transfer number T1
- Transfer to 2nd transfer number T2
- Transfer to 3rd transfer number T3

Screenshot of the Outgoing Call Plan screen for initiating call forwards / transfers below:

Outgoing Calling Plan
Customize the Outgoing Calling Plan for the group and/or departments.

OK Apply Cancel

Originating Initiating Call Forwards/Transfers Being Forwarded/Transferred

Department	Group	Local	Freephone	National	International	Not Used	Directory Enquiries	Not Used	PNS (070)	PRS (0871)	PRS (09)	Casual	URL Dialing	Unknown
Group Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Check box to permit call type; Users can be configured with their own custom settings in user-level Calling Plan

Note: The Outgoing Calling Plan can be configured down to a specific user level. It is therefore important to ensure that Outgoing Calling Plans are carefully managed and maintained by the group administrator.

Default Outgoing Calling Plan

Redcentric will provision the IP Voice Pro Service with a default Outgoing Calling Plan. This is configured as below in the interests of security. Customers requiring the ability to call destinations prohibited by the default Outgoing Calling Plan will need their group administrator to enable the required destinations.

Call Type	Policy
Group Calls (calls within the Unity Group)	PERMITTED
Local Calls	PERMITTED
National Calls	PERMITTED
Freephone Calls	PERMITTED
International Calls	NOT PERMITTED
Directory Enquiries	NOT PERMITTED
PNS 070 (Personal Number)	NOT PERMITTED
Premium Rate (0871)	NOT PERMITTED
Premium Rate (09)	NOT PERMITTED

Table 12: Default Outgoing Call Plan

NOTE: *Currently there is no option to bar mobile calls which are permitted.*

Restricted International Destinations

In the interests of minimising the risk of fraudulent calls, Redcentric has barred access to the following high-risk international destinations.

Country Code	Destination	Country Code	Destination
00227	Niger	00594	French Guiana
00228	Togo	00595	Paraguay
00229	Benin	00596	Martinique
00231	Liberia	00597	Suriname
00232	Sierra Leone	00598	Uruguay
00233	Ghana	00599	Netherlands Antilles
00234	Nigeria	0060	Malaysia
00235	Chad	0062	Indonesia
00236	Central African Republic	0063	Philippines
00237	Cameroon	0065	Singapore
00239	Sao Tome and Principe	0066	Thailand
00240	Equatorial Guinea	00670	East-Timor
00241	Gabon	00672	Australian External Territories
00242	Congo	006721	Antarctic
00243	Republic of Congo	006723	Norfolk Island
00244	Angola	00673	Brunei Darussalm
00245	Guinea-Bissau	00674	Nauru
00246	Diego Garcia	00675	Papua New Guinea
00248	Seychelles	00676	Tonga
00249	Sudan	00677	Solomon Islands
00250	Rwanda	00678	Vanuatu
00251	Ethiopia	00679	Fiji
00252	Somalia	00680	Palau
00253	Djibouti	00681	Wallis and Futuna
00254	Kenya	00682	Cook Islands
00255	Tanzania	00683	Niue

Country Code	Destination	Country Code	Destination
00256	Uganda	00684	American Samoa
00257	Burundi	00685	Western Samoa
00258	Mozambique	00686	Kiribati Republic
00260	Zambia	00688	Tuvalu
00261	Madagascar	00689	Tahiti
00262	Reunion	00690	Tokelau
00263	Zimbabwe	00691	Micronesia
00264	Namibia	00692	Marshall Islands
00265	Malawi	0081	Japan
00266	Lesotho	0082	Korea Republic
00267	Botswana	0084	Vietnam
00268	Swaziland	00850	Korea
00269	Comoros and Mayotte	00853	Macao
0027	South Africa	00855	Cambodia
00290	St. Helena	00856	Laos
00291	Eritrea	00880	Bangladesh
00297	Aruba	00886	China-Taiwan
00298	Faroe	0092	Pakistan
00354	Iceland	0093	Afghanistan
00355	Albania	0094	Sri Lanka
00370	Lithuania	0095	Myanmar
00371	Latvia	00960	Maldives
00372	Estonia	00961	Lebanon
00375	Belarus	00962	Jordan
00377	Monaco	00963	Syrian Arab Republic
00380	Ukraine	00964	Iraq
00381	Serbia	00965	Kuwait
00382	Montenegro	00966	Saudi Arabia
00383	Kosovo	00967	Yemen
00385	Croatia	00968	Oman
00386	Slovenia	00970	Palestine

Country Code	Destination	Country Code	Destination
00387	Bosnia and Hercegovina	00972	Israel
00389	Macedonia	00974	Qatar
00420	Czech Republic	00975	Bhutan
00421	Slovakia	00976	Mongolia
00500	Falkland Islands	00977	Nepal
00501	Belize	0098	Iran
00502	Guatemala	00992	Tajikistan
00503	El Salvador	00993	Turkmenistan
00504	Honduras	00994	Azerbaijan
00505	Nicaragua	00995	Georgia
00506	Costa Rica	00996	Kyrgyz Republic
00507	Panama	00998	Uzbekistan
00508	St. Pierre		

TABLE 13: RESTRICTED INTERNATIONAL DESTINATIONS

NOTE: The restricted international destinations are barred at system level. Even with international calls permitted by the group administrator on the Outgoing Calling Plan, these destinations will still be barred.

If the Customer needs to make calls to any of these high-risk international destinations, barring can be removed by submitting a request to Redcentric support.

NOTE: that this will remove barring to all high-risk international destinations as defined above. It is not possible to permit / bar individual high-risk international destinations.

Making Outgoing Calls Through the Voicemail Portal

This feature allows staff to make phone calls through the same portal that they use to pick up their voicemails. This can be beneficial to certain types of employees but also represents a security risk because it allows outgoing calls to be made by anyone that has been able to guess an employee's voice-mail passcode.

Because of this potential fraud risk, Redcentric do not enable this feature on any user accounts, and it is Redcentric's strong recommendation that this service remains disabled. Due to the significant scope for fraudulent use, Redcentric will request a written waiver of liability from the Customer before re-activating this service.

Authorisation Codes

The Authorisation Codes feature in Unity allows an administrator to enforce that a user enters a security code before they are permitted to make a call. This is primarily intended for public area phones but may also be used to prevent calls being made from any phone without first entering a security code.

Housekeeping

On new installations, new user accounts are normally created by the Redcentric service delivery team. Customers are also able to change passwords away from those initially set by Redcentric at any stage after deployment of the Voice Service. Customers may also configure new user accounts following installation after purchasing the user licences. Passwords and passcodes that are generated must always be secure (i.e., not 0000, 1234 etc.).

A redundant account with an easy to deduce password is the ideal vehicle for a hacker to fraudulently use the system and could remain undetected for a long time. The former employee could also continue to use the account (or pass on the details) at the organisation's expense. Redcentric recommends:

- Disable all visitor accounts when not required.
- Ensure that test or demo accounts are disabled when not in use or that they follow the strict password regime mentioned above.
- Remove all leaver accounts immediately or change the password.

NOTE: Redcentric will delete devices that have not connected/registered to the service for 90 days

Supplemental Security Recommendations

- Remove or de-activate all unnecessary system functionality.
- Review your bills regularly to spot any increases in call volumes or calls to suspicious destinations.
- Disable all surplus user accounts until you have a user for them.
- Only give individuals the appropriate and minimum level of system access they need to carry out a specific task i.e., Service Packs.
- Restrict access to your core communications equipment, such as your main computer room to avoid physical access to network switches. Hackers can intercept calls and reroute them, capture the data for later playback of the conversation or listen in on the call to capture the conversation in real time.
- Ensure that network switches are deployed within secure locations as opposed to network hubs to remove the threat of eavesdropping from within the network using PC based devices.
- Ensure that telephony devices are segmented from data devices by using the appropriate VLAN configurations
- Continually review these security recommendations at regular intervals.

Service Capability & Limitations

Unity IP Voice Pro requirements and prerequisites

Please see the latest version of the Unity requirements document for details of:

- Webex Network requirements and prerequisites
- Software / operating system requirements
- PC hardware requirements
- Firewall requirements

This document can be found at: <http://www.redcentricplc.com/downloads>

Call centre capacities

Capability	Capacity
Maximum number of agents in a queue	50
Maximum number of queues per Supervisor	15
Maximum number of agents per Supervisor	20
Maximum number of Supervisors per agent	1 or 2
Queue (ACD) Guard Timer	5 to 10 seconds
Maximum queue (ACD) size	525 (Call Centre Premium)

Call Centre limitations

Note: The following limitations apply to the Call Centre service

Features	Limitations
Wrap up state	<ul style="list-style-type: none">• Agents do not receive personal phone calls when in Wrap up state.• Agents do not receive phone calls when in Wrap up Agents can cause Wrap-up issues if they set their Do not Disturb status manually
Reports and statistics	<ul style="list-style-type: none">• Reporting statistics are stored for 12 months.
Call Forwarding	<ul style="list-style-type: none">• Call centre cannot be used in conjunction with Call Forwarding
IP Handsets	<ul style="list-style-type: none">• The application will not function correctly unless the agent or supervisor logged in is also registered device.

Music on Hold file format and specification

Features	Limitations
Group Music on Hold	<p>Required File Format and Specification</p> <p>The audio file format and specification must adhere to the following:</p> <ul style="list-style-type: none">• CCITT u-Law• 8.000 kHz• 8 bits mono• .WAV file type• Maximum recording duration 10 minutes• Maximum file size 4.6 MB
Music on Hold as part of Call Queue (ACD)	<p>Required File Format and Specification</p> <p>The audio file format and specification must adhere to the following:</p> <ul style="list-style-type: none">• CCITT u-Law• 8.000 kHz• 8 bits mono• .WAV file type• Maximum recording duration 5 minutes• Maximum file size 2.4 MB

Webex softphone – known limitations

- Call forward not reachable is not usable if mobile data is enabled as devices stay registered over the mobile data network (applicable to mobile versions of the client only)
- Under certain call scenarios, service tones (for example ringing tone) are US tones and not British tones.

SIP ALG (Application Layer Gateway) Settings

SIP ALG can cause a mixture of problems by adjusting or terminating the Webex softphone packets in such a manner that they are corrupted and cause issues with the service, manifesting in a range of intermittent issues such as one-way audio, dropped calls, problems transferring calls, client dropping registration and making or receiving calls.

To ensure your users receive the best experience **SIP ALG should be disabled** on all CPE routers. **Users should speak to their respective service provider if they require details on how to achieve this.**

Webex Client – Deployment in a VDI Environment

Administrators can refer to the [Deployment Guide for Cisco Webex App for Virtual Desktop Infrastructure \(VDI\)](#) for more information about what features are supported, how to prepare your environment, and how to deploy the Webex App VDI solution.

Unity IP Voice Pro Off-Net Service (HSCN)

Unity Off-Net enables Unity IP Voice Pro to be delivered to supported Polycom IP phones across a non-Redcentric network connection.

Unity IP Voice Pro Off-Net (automated phone provisioning)

- Unity IP Voice Pro phones connect to the Customer's existing WAN connection via their LAN.
- The Customer must provide certain information in their DHCP scope to provide the phones with details of Redcentric's voice platform to facilitate automated provisioning.
- Redcentric do not provide any pre-configuration of the phones.
- Connection from the Customer site to Redcentric's SBCs, typically over the Internet

Technical Requirements – Unity IP Voice Pro Off-Net (automated phone provisioning):

- DHCP must be provided on the LAN to which the phones are connected.
- Where Redcentric do not pre-configure phones, additional information must be provided in the DHCP scope.
- The point of egress to the internet must be capable of running NAT or PAT
- Phones must be allowed:
 - Access to the internet for the purpose of resolving FQDNs via DNS
 - Access to the internet for the purpose of accessing Redcentric's HTTP and HTTPS servers for auto-configuration of the handsets.
 - Access to the internet for the purpose of reaching Redcentric's SBCs via the SIP and RTP protocols (ports are not relevant as there will be PAT in place).
 - Hold a TCP and/or UDP session open, always. The port will be re-initialised every 60 seconds via means of a re-registration with our SBCs.
 - Connect directly to the LAN via CAT5e cable.
 - There should only be wired LAN infrastructure between the handset and the Internet (no wireless links or repeaters)
- Phones must be able to resolve to:

Name / SRV Service Location	Addresses
dms.voicesys.co.uk	178.250.100.93 213.146.135.52
xsi.voicesys.co.uk	85.118.24.169 213.146.135.50

Name / SRV Service Location	Addresses
_sip._udp.edge.voicesys.co.uk	priority = 3 weight = 50 port = 5060 svr hostname = edge-acme1.voicesys.co.uk
_sip._udp.edge.voicesys.co.uk	priority = 4 weight = 50 port = 5060 svr hostname = edge-acme2.voicesys.co.uk
_sip._udp.edge.voicesys.co.uk	priority = 1 weight = 50 port = 5060 svr hostname = edge-oracle1.voicesys.co.uk
_sip._udp.edge.voicesys.co.uk	priority = 2 weight = 50 port = 5060 svr hostname = edge-oracle2.voicesys.co.uk
edge-oracle1.voicesys.co.uk	Signalling: 213.146.130.217 Media: 85.118.13.96/27 port: 5060
edge-oracle2.voicesys.co.uk	Address Signalling: 85.118.13.100 Media: 213.146.130.192/27 port: 5060
edge-acme1.voicesys.co.uk	Address Signalling: 213.146.130.196 Media: 178.250.96.64/27 port: 5060
edge-acme2.voicesys.co.uk	Address Signalling: 178.250.96.68 Media: 213.146.130.192/27 port: 5060

It is recommended / may be necessary for the Customer to disable any form of SIP Inspection on their firewall.

- Limitations – Unity **IP Voice Pro** Off-Net (automated phone provisioning)
- The maximum number of simultaneous calls that can be made is dependent on the symmetric bandwidth available on the Customer's Internet connection.
- Availability of the Unity IP Voice Pro service is dependent on the availability and correct operation of the Customer's Internet and related equipment.
- No call quality assurances can be made by Redcentric when the Unity IP Voice Pro Service is delivered across a non-Redcentric network, such as the Internet.

System Provisioning

Within the Unity IP Voice Pro core platform Redcentric will create a dedicated and secure Administration Zone for the Customer. This will allow an authorised administrator to log onto the Unity IP Voice Pro system to configure, manage and view all aspects of the service.

Subject to the Administrator having attended the recommended Unity IP Voice Pro- System Administrator training course, Redcentric will provide initial help in setting up and establishing the key System Administration parameters plus help with any problems / issues relating to the set up.

System maintenance

Note: Redcentric may perform remote handset security checks and firmware upgrades during the hours of 8pm – 3am Monday-Sunday. The checks/upgrades may force a reboot of the end user's handset. In the unlikely event of a user not being able to make a call the affected user should in the first instance power cycle the handset and if this does not clear the issue follow normal support process and raise a ticket with the Redcentric support desk.

Service Provisioning

Handsets

Redcentric's Unity IP Voice Pro service is compatible with the following vendors/devices:

- Polycom (V VX)
- Yealink DECT

Note: For a full list of supported device models please speak to your account team.

The phones may either be purchased or rented by the Customer and are either supplied with the installation of the Unity IP Voice Pro Service or may be sent to the Customer site for self-installation.

Note: When purchased, phones, cables and related accessories become the property of the Customer and as such the Customer is responsible for their on-going maintenance. They remain the ownership of the Customer at the end of the contract.

Unless otherwise stated, phones do not come with mains power supplies. If you are not intending on using 802.3af compliant Power over Ethernet, you will require power supplies which are available for an additional fee.

Headsets

Redcentric's Unity IP Voice Pro service is compatible with the following headset vendors:

- Polycom
- Jabra
- JPL

Note: For a full list of supported device models please speak to your account team.

Redcentric offers a range of wired, wireless and USB headsets. Wired and wireless headsets may be used with supporting devices. USB headsets may be used with a compatible device and soft clients.

Note: that headsets become the property of the Customer and as such the Customer is responsible for their ongoing maintenance. They remain the ownership of the Customer at the end of the contract.

Headset Warranty

Headsets that develop a fault within the manufacturer's warranty period may be returned to Redcentric for a replacement.

This excludes headsets damaged through misuse, accidental damage, or through operation outside of the manufacturer's recommended operating conditions or if used in conjunction with a non-manufacturer approved device.

Consumables including cables, ear pads, and microphone tubes cords are not included in the hardware replacement policy. Headsets may be purchased only and are not available to rent.

Adapter for Analogue Phones (IADs)

Redcentric can provide converters that allow standard analogue phones to connect to the Unity IP Voice Pro service. These adapters can only be used with analogue phones.

Typical examples of where these adapters may be used include analogue wired phones within lifts.

2 port adapters are supplied with installation and initial configuration. **Note:** IADs become the property of the Customer and as such the Customer is responsible for their on-going maintenance. They remain the ownership of the Customer at the end of the contract.

Note: The use of analogue telephone adapters for fax machines, modems or other analogue data devices is not supported.

GP Surgery Service Packs (User Licences)

Unity IP Voice Pro users are provided functionality by assigning them with a service pack. This gives users a billing account and a phone number on the Unity system. There are two core service packs designed for the GP Surgery are defined below.

User Features

Features	Features Included		Theme
	GP Surgery User Professional	GP Surgery User Standard	
Auto-Attendant & Interactive Voice Response (IVR) capability Analysis			
Ability to use Hunt Groups	Y	Y	MUST DO
Auto Attendant	Y	Y	MUST DO
Auto Attendant to announce purpose of the call to Health or Care Professional	Y	Y	MAY DO
Call Queue	Y	Y	MUST DO
High priority Patient/Service User Call Queue prioritisation	Y	Y	MAY DO
Interactive Call Flow	Y	Y	MUST DO
Interactive Voice Response menu	Y	Y	MUST DO
Interact with solution using Dual Tone Multi-Frequency (DTMF) Tones	Y	Y	MUST DO
Line specific messages	Y	Y	MUST DO
Patient/Service User after call survey	Y	Y	MAY DO
Re-routing of unanswered routed calls	Y	Y	MUST DO
Skill based call allocation	Y	Y	MAY DO
Time condition call routing	Y	Y	MUST DO
Call Recording			
Add free text notes to Call Recordings	Y	Y	MAY DO
Attach inbound Call Recordings to the Patient/Service User's Electronic Patient Record (EPR)	Y	-	MAY DO
Attach outbound Call Recordings to the Patient/Service User's Electronic Patient Record (EPR)	Y	-	MAY DO

Features	Features Included		Theme
	GP Surgery User Professional	GP Surgery User Standard	
Automatic Call Recordings	Y	Y	MAY DO
Categorise Call Recordings	Y	Y	MAY DO
Configurable retention period of Call Recordings	Y	Y	MUST DO
Configure real-time call data dashboard	Y	Y	MUST DO
Export Call Recordings (Admin only)	Y	Y	MUST DO
In-queue position announcements	Y	Y	MUST DO
Manual record audio calls	Y	Y	MUST DO
Playback Call Recordings	Y	Y	MUST DO
Record audio call	Y	Y	MUST DO
Search for Call Recordings	Y	Y	MUST DO
View Call Events	Y	Y	MUST DO
Call Reporting & Forecasting			
Export report results	Y	Y	MUST DO
View call demand forecasting	Y	Y	MAY DO
View Call Event reports	Y	Y	MUST DO
View in-queue call backs conducted	Y	Y	MUST DO
View Interactive Call Flow reports	Y	Y	MAY DO
View Patient/Service User after call survey reports	Y	Y	MAY DO
View real-time call data dashboard	Y	Y	MUST DO
Clinical System Integration / Patient Callback			
Identify Patient/Service User from caller ID - (integration with the clinical system)	Y	-	MUST DO
In queue call back option	Y	-	MUST DO
Support calling Patient/Service Users from their Electronic Patient Records (EPR)	Y	-	MAY DO
Office Telephony			
3rd party conferencing	Y	Y	MUST DO
Call Forwarding	Y	Y	MUST DO
Call Hold	Y	Y	MUST DO
Calling Line Identifier	Y	Y	MUST DO

Features	Features Included		Theme
	GP Surgery User Professional	GP Surgery User Standard	
Call Monitoring	Y	Y	MUST DO
Call Switching between devices	Y	Y	MAY DO
Call Transfer	Y	Y	MUST DO
Call Waiting Indication	Y	Y	MUST DO
Conduct audio calls	Y	Y	MUST DO
Configure the blocking of outbound phone numbers	Y	Y	MUST DO
Health or Care Professional availability status	Y	Y	MAY DO
Manage Directory	Y	Y	MUST DO
Mute call	Y	Y	MUST DO
Play received voicemail	Y	Y	MUST DO
Search Directory	Y	Y	MUST DO
Share Directory	Y	Y	MAY DO

Service Support

Unity IP Voice Pro Service Desk

A dedicated Service Desk number 03330 102051 is available to GP Practices for service support relating to their Unity IP Voice Pro service.

Service Administration

The System Administrator has access to a web-based management tool which gives them control over the Unity IP Voice Pro service at a company-wide level.

End User Self Service

Viewed through a browser on the user's own PC, each individual Unity IP Voice Pro user has their own restricted access to the management web portal. In addition to this, each user can choose to install the Webex softphone which provides end users with easy and immediate control over all major features available to their licence type.

Example features include:

- Click to dial from corporate, group or personal directories.
 - Transfer a call to a colleague or make a 3-way call.
 - Enable / Disable Call waiting, 3-way calling, do not disturb.
 - Manage Voice mail options including delivery options and greeting messages.
 - Set call diversion options.
 - Quickly see call logs – missed calls, received calls, placed calls – and return any missed calls with a single click.
- Set remote working options, find me / follow me, redirect to alternative number e.g., mobile.

Moves, Adds and Changes

A key feature of Unity IP Voice Pro is it's easy to use and highly intuitive administration interface. Administration of traditional, PBX based systems require highly complex and time-consuming procedures often requiring specialist skills.

The Unity IP Voice Pro secure web portal provides the customer self-administration service management and enables end users to configure and manage their own services, significantly lowering the cost of customer service and operations.

The portal is a hierarchical, web browser based, management interface which allows both system administrator and individual users to configure the Unity IP Voice Pro Service to meet highly specific corporate practice and personal requirements.

It is expected that all the following adds, moves and changes will be undertaken by the Customer via the Unity web administration portal. Where the Customer requests that Redcentric undertake any of the following, this may incur an administration fee, per change.

Configuration and administration of the following Group Services and Features:

- Administrator passwords

- Hunt groups
- Call Queues (Call Centres)
- Auto-attendants (IVRs)
- Call pickup groups
- Incoming and outgoing call plans (in line with the Redcentric voice security policy unless otherwise agreed in writing)
- Password rules plans (in line with the Redcentric voice security policy)
- Voice portal pass-code rules (in line with the Redcentric voice security policy) Outgoing digit plan:
- Custom contact directories
- Common phone lists
- Departments
- Holiday schedules
- Time schedules
- Authorisation codes
- Music on hold
- Group / departmental CLI (telephone number) presentation options
- Group voicemail (where applicable)
- Feature access codes (FACS)
- Voice portal options

Configuration and administration of the following user services and features:

- User passwords and voice portal passcodes
- User voicemail
- User services and features
- User PC desktop applications

Management and administration of the following resources:

- Phones (devices)
- Numbers and their allocation (telephone numbers)
- User service pack allocation and availability
- Group service licence allocation and availability
- Recording of and uploading of voice prompts and announcements

Service Levels & Service Credits

The Service Levels and Service Credits applicable to the Redcentric Unity IP Voice Pro service are also set out in Schedule 12 of the NHS Contract for Advanced Telephony Services.

System Availability

Unity IP Voice Pro will be available 24/7, 365 days a year with an uptime of 99.99% and will be monitored and measured within the monthly system reporting.

No.	KPI Title	Severity Levels		Monthly Service Credit #
KPI1	Service Availability	Target Performance Level:	99.9%	NA
		Minor KPI Failure:	99.95% - 99.98%	10% of MS
		Serious KPI Failure:	99.75% - 99.94%	15% of MS
		Severe KPI Failure:	<99.75%	25% of MS
		KPI Service Threshold:	<98.0%	25% of MS
KPI2	Help Desk Response Times to dedicated Service Desk 03330 102051	Target Performance Level:	<=60 seconds	NA
		Minor KPI Failure:	61 – 90 seconds	NA
		Serious KPI Failure:	91 – 120 seconds	NA
		Severe KPI Failure:	121 – 150 seconds	NA
		KPI Service Threshold:	>= 151 seconds	NA
KPI3	Incident Management Response	Target Performance Level:	4 hours	NA
		Minor KPI Failure:	4 – 8 hours	NA
		Serious KPI Failure:	8 – 16 hours	NA
		Severe KPI Failure:	16 – 24 hours	NA
		KPI Service Threshold:	24+ hours	NA

MS means the total Charges payable in respect for the Service for the same Month.

Professional Services

Project Definition Workshop

The project definition workshop is a design session during which a Redcentric technical consultant will design the voice solution with the Customer.

Project definition workshops may be undertaken over the phone, over a web conference, at a Redcentric office or at the Customer site subject to requirements.

Voice Technical Consultancy

Typical examples of voice technical consultations may include:

- Post-installation workshops to change the solution design.
- Office moves.
- Disaster recovery planning

Voice Technical Consultancy may be delivered over the phone, over a web conference, at a Redcentric office or at the Customer site subject to requirements.

Voice Project Management

Project management of voice service implementation. May also include project management of Customer specific requests such as site relocations for example.

Administrator Training

This mandatory course is to familiarise system administrators with the steps required to carry out Customer managed adds, moves, and changes via the web administration portal.

The course objectives are:

- To be able to explain the roles of a group administrator and a user.
- To be able to set up Unity IP Voice Pro for a user using the self-service web administrator portal.
- To be able to manage group services.
- To be able to manage user services.

Unity IP Voice Pro Administration Training is delivered at the Customer site or remotely.

On-site Training

This optional consultancy service places a Redcentric voice training specialist onsite. Typical requirements for onsite training include:

- Floor-walker training – provides users with hands-on training, typically on or near to the day the new service goes live. It ensures staff are comfortable and proficient with the key operations and features of the Unity service and provides an on-hand resource to answer any user queries.
- Receptionist training – focused training on ensuring receptionists/call handlers is comfortable and proficient handling and fielding inbound calls using the provided services.

- CCGP / ARC training – for call centre deployments, provides hands-on training to agents and supervisors on the use of the Call Centre solution and applications.
- Train the trainer – a popular approach whereby the Redcentric trainer provides detailed end-user training to several Customer-designated 'power users'. These power users then provide onward training and assistance to end users.

Engineer Installation – During Business Hours

- Provides physical installation and testing of phones during business hours.
- Business hours are defined as Monday to Friday 0900 to 1730 excluding public holidays.
- Engineer Installation – Outside of Business Hours
- Provides physical installation and testing of phones outside of business hours.
- Out of business hours is defined as 0500 – 0900 and 1730 + and is subject to a minimum of four hours' work.

Failed Installation Appointment

A charge made where an installation appointment is cancelled with less than 24 hours' notice, where an engineer is unable to gain access to site or where an engineer is unable to carry out the installation due to a lack of site readiness.



Proactive

We think and
act quickly



Inspired

We create
excitement through
innovation

Trusted

We do what
we say we will

Collaborative

We work together
to deliver
a common goal

Transparent

We are open,
honest and fair





Head office

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522

E sayhello@redcentricplc.com

W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED

