Multitone Electronics plc

Multitone i-Message, i-Message Cloud, Multitone IM-Lite & Multitone Apps

System Overview, Architecture, Operation & Security

Issue: 6.0 (November 2025)

Multitone Electronics PLC Basingstoke, RG23 7NL, 2025 reserve the copyright of this document, which is not to be copied, reproduced or disclosed to a third party without prior written consent

TABLE OF CONTENTS

1. INTRODUCTION 9
2. MULTONE i-MESSAGE - SYSTEM OVERVIEW 9
3. MULTITONE i-MESSAGE - ARCHITECTURE, SOFTWARE & PROTOCOLS 9
3.1 Multitone i-Message - System Architecture & NDB Clustering 10
3.1.1 System Architecture 10
3.1.2 MYSQL Network Database 11
3.2 Multitone i-Message - Cloud Services (Support Only) 12
3.2.1 Multi-tenancy - i-Message Cloud Services 12
3.2.2 Multitone i-Message Cloud Hybrid Support 14
3.2.3 Amazon Web Services 14
3.3 Multitone i-Message - Server Software 14
3.3.1 Multitone i-Message 14
3.3.2 Multitone IM-Lite A, B, C & D 15
3.3.3 Multitone IM-Lite product variants 16
3.3.4 Multitone i-Message & IM-Lite Accessory Devices 17
3.4 Multitone i-Message - Communications Processor (CCP) 18
3.4.2 Multitone i-Message - Communications Processor (CCP) - Alarm Agents 19
3.4.3 Multitone i-Message - Communications Processor (CCP) - External Modules 20
4. MULTITONE i-MESSAGE - TELEPHONE SUPPORT 20
4.1 SIP Interface 20
4.2 Analogue/SIP interface 21
5. MULTITONE i-MESSAGE - ON-PREMISES, CLOUD SECURITY & COMPLIANCE 21
5.1 Introduction 21
5.2 Application of NCSC principles to Multitone i-Message cloud services 21
5.2.1 Principle 1, Multitone i-Message - Data in Transit Protection 21
5.2.2 Principle 2, Multitone i-Message - Protection & Resilience 22
5.2.3 Principle 3, Multitone i-Message - Separation Between Users 23
5.2.4 Principle 4, Multitone i-Message - Governance Framework 23
5.2.5 Principle 5, Multitone i-Message - Operational Security 23
5.2.7 Principle 7, Multitone Electronics plc - Secure Development 24
5.2.8 Principle 8, Multitone Electronics plc & i-Message - Supply Chain Security 24
5.2.9 Principle 9, Multitone i-Message - Secure User Management 25
5.2.10 Principle 10, Multitone i-Message - Identity & Authentication 25
5.2.11 Principle 11, Multitone i-Message - External Interface Protection 26
5.2.12 Principle 12, Multitone i-Message - Secure Service Administration 26
5.2.13 Principle 13, Multitone i-Message - Audit Information for Users 26
5.2.14 Principle 14, Multitone i-Message - Secure Use of the Service 27
6. Multitone i-Message System Security 27
6.1 Multitone i-Message Hardware - Statement of Security Compliance 27
6.2 Multitone i-Message - Network Security 28
6.3 Multitone i-Message - System Security 29
6.3.1 Software Security & Update Management 29
6.3.2 Antivirus Software Policy 30
6.3.3 Server & Client Security 30
6.3.4 Server Virtualisation – Not Advised 30

6.3.5 Multitone SMART DMZ Secure Proxy Server Security 30
6.4 Multitone i-Message - Database Security & Back-up 31
6.5 Multitone i-Message - Paging & Transmitter Network Security 32
6.6 Multitone i-Message - On-premises System Resilience 33
6.6.1 Design Topology of the Multitone i-Message Platform 33
6.6.2 Server Start-up, Failover & Recovery 34
6.6.3 Network Outage Failover 35
6.6.4 Keep Alive 36
6.6.5 Multitone i-Message - Database Synchronisation & Clusters 36
6.6 Multitone i-Message - Statement on the Use of External Penetration Testing ... 36
6.6.1 What Penetration Testing Multitone do on the Servers / Application? 37
6.6.2 What is the Greenbone Test Environment? 37
6.6.3 Test Regime 38
6.6.4 Pass / Fail Criteria 39
6.6.5 Is this an Independent test or Standard? 40
6.6.6 How often is Testing Undertaken? 40
6.6.7 Will Multitone provide the Report Results of a Successful Certified Release? 40
6.7 Multitone i-Message - HTTPS Certificates & Self-signed Certificates 40
7. MULTIONE i-MESSAGE - CALL LOG, AUDIT & SYSTEM MONITORING 42
7.1 Call Log 42
7.2 SNMP System Monitoring 42
8. MULTITONE i-MESSAGE - SYSTEM HARDWARE 43
8.1 System Control Unit (SCU) 43
8.2 Multitone i-Message - Servers & Specification 45
8.2.1 IM-SV1- Dell R260 PowerEdge Server (Non RAID) 45
8.2.2 IM-SV1-RAID - Dell R260 PowerEdge Server (RAID 1) 46
8.2.3 IM-SV3 - Dell R360 PowerEdge Server 46
8.2.4 IM-SV1-UK i-Message Server Upgrade Kit 47
8.2.5 IM-SV3-UK i-Message Server Upgrade Kit 47
8.3 Multitone IM-Lite - Hardware Specification 47
9. MULTITONE I-MESSAGE - PERIPHERAL HARDWARE SUPPORT 49
9.1. Multitone i-Message - Digital Private Mobile Radio (DPMR) support 49
9.1.1 Kenwood Nexedge - system overview 49
9.1.2 Sepura Tetra interface - System Overview 51
9.1.3 Motorola Mototrbo (SMTP Gateway) - System Overview 52
9.2 Dual Bearer Interface (IM-DBID, IM-DBIR, IM-DBI2R) 53
9.2.1 Dual Bearer Interface - Transmitter Interface 55
9.2.2 Dual Bearer Interface - GPS synchronisation 55
9.2.3 Public Address (PA) Sound Systems 55
9.2.4 Dual Bearer Interface & Direct Line Contact (DLC) support 56
9.2.5 RS232 & RS485 support 56
9.2.6 Dual Bearer Interface - Product Operation 56
9.3 Multitone Integrator (IM-INT-D, IM-INT-R, IM-INT2-R) 56
9.3.1 Technical Specification 57
9.3.2 Product Features 58
9.4 Multitone i-Message - DLC Interface (IM-LITE-DLC) 59
9.4.1 Technical Specification 59
10. MULTITONE SMART APPS 60

10.1 Multitone Smartapp Options 60
10.2 Multitone Smartapps, Key Features 61
10.3 Multitone Smartapps, Device Security 63
11. MULTITONE APPS CONFIGURATION 65
11.1 Introduction 65
11.2 Access Control 65
11.3 Design topology of the Multitone smartapp platform 66
11.3.1 SMAP Data Internal Only 66
11.3.2 SMAP SIP Portion Internal Only 67
11.3.3 SMAP Data & SIP Internal Only 68
11.3.4 Multitone Apps - SIP Internal Trunk 69
11.3.5 Multitone Smartapps, Connecting from External / Internal 70
11.3.6 Multitone Smartapps. Data Internal & External Use 71
11.3.7 Multitone Smartapps, SIP Internal & External Use 72
11.3.8 Multitone Smartapps, Data Using AWS Cloud Proxy 73
11.4 Further Notes on Design Topology of Multitone Smartapps 75
11.4.1 SIP Application Layer Gateway (ALG) 75
11.4.2 Keep Alive 75
11.4.3 Network Address Translation (NAT) 75
11.4.4 Domain Name Server (DNS) 75
11.4.5 Multitone Smartapps SIP Internal & External Use 76
11.5 Firewall Requirements 76
11.5.1 Important Firewall Port Information 76
11.5.2 Cloud Notification Ports & IP Addresses 78
11.5.3 Cloud Proxy Ports & IP Addresses 78
11.6 Multitone i-Message & Smartapp Encryption 79
11.6.1 Encrypted from the First Packet 79
11.6.2 Note on AES Encryption 80
11.6.3 Sending Messages Between Devices 82
11.6.4 Not Stopping at TCP Security 82
11.6.5 Password Security 83
APPENDIX 84
1. Multitone i-Message Server Software - Port Allocations 84
2. Communication Processor - Port Allocations (Hardware) 84
3. Multitone i-Message Component Dimensions & Weights 86
4. Multitone i-Message Components Power Rating 87
5. Multitone i-Message Failover & Start-up Estimation 89
6. Multitone SMART Apps WiFi Usage (Typically up to 20 Apps) 90
7. Multitone Smart Apps - Product Variants, Software Versions, Operating Systems & Status 91
8. Multitone Appear - Product Variants, Software Versions, Operating Systems & Status 92
9. Multitone i-Message Software Matrix 93

CHANGE CONTROL

Date	Section	Change	Issue
12th Nov 2025	Up-issued to issue 6.0	Up-issued document to conform with revised branding.	Issue 6.0
12th Nov 2025	Section 8.2, sub sections 8.2.1., 8.2.2., and 8.2.3.	Revised and updated IM-SV1, IM-SV1-RAIDand IM-SV3technical specification with respect to Dell 260 non-Raid and RAID 1 options.	Issue 6.0
15th Jan 2025	Up issued to issue 5.9	General edit and corrections to text, no change in content	Issue 5.9
15th Jan 2025	6.7 Multitone i-Message – HTTPS certificates &self-signed certificates	Added new section providing details of HTTPS certification and self signed certificates	Issue 5.9
23rd Oct 2024	6.3.4 Server Virtualisation	Added further information as to minimum VM requirement for a virtual machine environment to operate.	Issue 5.8
23rd Oct 2024	6.6, Multitone i-Message - Statement on the Use of External Penetration Testing	Added new section 6.6, Multitone i-Message - Statement on the Use of External Penetration Testing, This includes sub-section 6.6.1 to 6.6.7.	Issue 5.8
21st March 2024	8.1 System Control Unit (SCU)	Added new CPU, touch screen and microphone specifications	Issue 5.7
21st March 2024	6.6.5 Multitone i-Message - Database Synchronisation & Clusters	Amended note with respect to IM-Lite-D clustering support	Issue 5.7
26th October 2023	8.2 Multitone i-Message - Servers & Specification 8.2.1 IM-SV1- Dell R250 PowerEdge Server 8.2.2 IM-SV1-RAID - Dell R250 PowerEdge Server 8.2.3 IM-SV3 - Dell R350 PowerEdge Server 8.2.4 IM-SV1-UK i-Message Server Upgrade Kit 8.2.5 IM-SV3-UK i-Message Server Upgrade Kit	Added specification for Dell R250 Server 32 GB RAM, 1 x SSD (IM-SV1) Dell R250 Server 32 GB RAM, 1 x SSD, RAID 1 (IM-SV1-RAID) Dell R350 Server 32 GB RAM, 3 x SSD, RAID 5 (IM-SV3)	Issue 5.6
4th October 2023	Revised section 6.3.1 Software Security & Update Management Added new section 6.6.2 Server Start-up, Failover & Recovery	Added Windows Server IoT 2022 Added Multitone i-Message server start-up, failover and recovery:	Issue 5.5
28th July 2023	Revised Section 11.3, Design Topology for Multitone SMART Apps sub-sections and added new sub-section11.3.8 Multitone Apps - Data using AWS Cloud Proxy.	Added new sub-section with respect to Multitone apps data using AWS cloud proxy.	Issue 5.4
28th July 2023	Revised Section 11.3, Design Topology for Multitone SMART Apps sub-sections: 11.3.1 SMAP Data Internal Only, 11.3.2 SMAP SIP Portion Internal Only 11.3.3 SMAP Data & SIP Internal Only 11.3.4 Multitone Apps - SIP Internal Trunk 11.3.5 Multitone Apps - Connecting from External/Internal 11.3.6 Multitone Apps - Data Internal & External Use	Replaced text and updated all text and drawings associated with these sections.	Issue 5.4

	11.3.7 Multitone Apps - SIP Internal & External Use		
2nd Feb 2023	New section 3.2.2, Multitone i-Message cloud/hybrid support	Added statement to describe Multitone i-Message cloud/hybrid support.	Issue 5.3
2nd Feb 2023	Section 10.1, Multitone app options	Added Multitone Appear crew and Multitone Messenger descriptions.	Issue 5.3
2nd Feb 2023	Section 10.2, Multitone Apps – device security	Added Multitone Messenger user on-boarding, non-invitation, hacker protection and session security.	Issue 5.3
2nd Feb 2023	11.6.1 Encrypted from the first packet	Added new diagram and refined Multitone Appear encryption description and added Multitone Messenger encryption	Issue 5.3
15th Nov 2022	Section 11.2 Access control	Updated table	Issue 5.2
15th Nov 2022	Section 8.2.1 IM-SV1- Dell R240 PowerEdge Server, Dual HDD, No RAID Section 8.2.2 M-SV1-HiSpec - Dell R240 PowerEdge Server,1 x SSD, No RAID 8.2.3 IM-SV3 - Dell R340 PowerEdge Server, HDD, RAID 5, 2 x PSU 8.2.4 IM-SV3-HiSpec - Dell R340 PowerEdge Server, SSD, RAID 5, 2 x PSU Section 8.2.5 IM-SV1-UGK i-Message Server Upgrade Kit Section 8.2.6 IM-SV3-UGK i-Message Server Upgrade Kit	Corrected technical specification for IM-SV1-HiSpec and IM-SV3-HiSpec, added IM-SV1-UGK and IM-SV3 upgrade kits replacing IM-SV-UGK.	Issue 5.2
4th Oct 2022	Section 8.2.2. IM-SV1-UGK and 8.2.4 IM-SV3-UGK	Corrected technical specifications	Issue 5.1
7th Sept 2022	Section 5	Updated content to include: NCSC principles and compliance, i-Message cloud services multi-tenancy and AWS support, updated server specification and revised style.	Issue 5.0
20th Jan 2021	Section 6, Multitone SMART Apps (Product Status & Availability)	Updated table to latest iOS and Android software	Issue 4.5.0
24th Nov 2021	Appendix 1, 4 - Multitone i-Message Components Power Rating	Revised server rating IM-SV1 and IM-Sv3 power and thermal data	Issue 4.4.9
24th Feb 2021	Appendix 7 (New),	Added i-Message Software Matrix	Issue 4.4.8
6th Jan 2021	1. Revised section 5.6.2 2. Corrected issue referencing in change control	Updated ISO 27001 from applying to accredited	Issue 4.4.7
23rd Nov 2020	Revised Section 3.2 Multitone i-Message Server Software	Revised issue number ActiveMQ (Version 5.15.11) Apache Web Server (Version 2.2.25) 7zip (Version 19.00 (x64) Java Runtime Version 8.0.0 MySQL Network Database (NDB) cluster database methodology 8.0.0 MCS Version 4.33 March 2020	Issue 4.4.6 (incorrect Issue 4.3.1)
23rd Nov 2020	Revised Section 6, Multitone Smart Apps Product Status and Availability	Updated table	Issue 4.4.6 (incorrect Issue 4.3.1)
4th Nov 2020	Correct Multitone i-Message Components Power Rating	IM-SV1 corrected from 150 to 250 Watts, IM-SV3 vale added, 350W max, IM-NS1 correct from 16W to 19W	Issue 4.4.5 (incorrect Issue 4.3)
7th Aug	Section 8.3 Multitone IM-Lite Hardware Specification	Revised CPU spec	Issue 4.4.4
6th Aug 2020	Revised Section3.3.3., Multitone i-Message Communication Processor - External Modules	Added Multitone Major Incident Management Module	Issue 4.4.4
6th Aug 2020	Added new subsection 3.1.2., Network Architecture	No new info added	Issue 4.4.4
6th Aug 2020	Added new sub-section 3.1.1, System Architecture	Added section on NDB clustering	Issue 4.4.4
6th Aug 2020	Added new sub-section 3.1.1,	Added section on NDB clustering	Issue 4.4.4

	System Architecture		
28th Jul 2020	Appendix 1, Section 4. Multitone i-Message Components Power Rating	Added thermal output rating BTU per hour	Issue 4.4.4
28th Jul 2020	Sections 3.2.1, 5.3.1,8.0	Revised and updated Windows Server support to include 2019	Issue 4.4.3
16th Apr 2020	Section 8.1 System Control unit	Revised and updated specification	Issue 4.4.2
5th Mar 2020	3.2 Multitone i-Message Server Software, Sub-section 3.2.1 Multitone i-Message	Added details and use of Multitone i-Message supports Microsoft Windows Server Embedded Standard 2016, 64Bit Multi-Language ESD OEI 16 Core Telco Licence.	Issue 4.2.1
5th Mar 2020	3.3.1 Multitone i-Message Communication Processor - messaging Protocols	Added two new protocols: Prism IPX Interface Protocol and SAGRN Protocol (Windows Only) New Zeeland	Issue 4.2.1
5th Mar 2020	3.3.3 Multitone i-Message Communication Processor - External Protocols	Added two new sections and modules - Section 3.3.3 Multitone i-Message Communications Processor - External Protocols. New protocols include RotaWatch (Beta only, not available for sale) and WorkFlow to support Multitone Asset Management System.	Issue 4.2.1
11th Nov 2019	Section 3.3.2 Communication Processor Alarm - Agents	Three new protocols added: - CEI XML Spacelabs Protocol - Austco Alarm Protocol - Modbus TCP Protocol	Issue 4.2
11th Nov 2019	Section 8.2.2 - IM-SV3- Dell R340 PowerEdge Server, Dual Disk, RAID	Revised spec for Dell R340 PowerEdge Server, Dual Disk, Non-RAID specification to include service rails	Issue 4.2
11th Nov 2019	Section 8.2.1 - IM-SV1- Dell R240 PowerEdge Server, Dual Disk, Non-RAID	Amended Dell R240 PowerEdge Server, Dual Disk, Non-RAID specification to include service rails.	Issue 4.2
19th Sept 2019	Section 5.5 Multitone i-Message Paging and Transmitter Network Security	Added additional information on Multitone Message devices supporting Raspberry Pi hardware	Issue 4.1
23rd Aug 2019	All sections reviewed and revised	All sections reviewed and revised All sections reviewed and revised, document up-issued to Issue 4.0.	Issue 4.0
11th Jun 2019	Updated Appendix II Multitone SMART Apps (Product Status & Availability)	Updated table	Issue 3.3.6
18th Mar 2019	General updates	General revision of English and tidy-up	Issue 3.3.5
15th Nov 2018	Appendix 2 - Multitone SMART Apps (Product Status & Availability)	Updated tables	Issue 3.3.4
15th Nov 2018	Section 14, i-Message Component Power Ratings	Updated table	Issue 3.3.4
15th Nov 2018	Section 13, i-Message Component Dimensions	Updated table	Issue 3.3.4
15th Nov 2018	Appendix 4, Multitone Integrator	Updated specification	Issue 3.3.4
15th Nov 2018	Section 3.1, Point 1	Updated Window Server operating system requirements	Issue 3.3.4
15th Nov 2018	Section 5.2, Sub-section 5.2.1 and 5.2.2	Update message and alarm agent protocol specification to include: MIP and TNPP (server)	Issue 3.3.4
9th Apr 2018	Section 13, i-Message Component Dimensions (mm) & Approximate Weights (kg)	Changed Length to Width	Issue 3.3.3
8th Mar 2018	Section 4, Multitone i-Message - Multiple Communications Bearer Support	Added new Section 4.2 ISDN Support, this explains how i-Message can use a second ISDN bearer as opposed to TCP/IP. Section 4.3 PSTN and ISDN Connection times	Issue 3.3.2
8th Mar 2018	Section 4,Multitone i-Message - Multiple Communications Bearer Support	Added new Section 4.3 PSTN and ISDN Connection times	Issue 3.3.2
5th Apr 2018	Added new Section 14, i-Message Component Power Ratings, re-issued document at Issue 3.3.2	Added matrix listing component parts, part numbers and power rating for that hardware	Issue 3.3.1

9th Apr 2018	New Appendix, Appendix 4	Multitone Integrator Overview and product description added	Issue 3.3.0
	Section 9 System Control Unit	As result of product replacement, new specification added	Issue 3.2.9

1. INTRODUCTION

The purpose of this document is to provide an overview of the Multitone i-Message system with regard to key features, system architecture, connectivity, operation and system security (anti-virus protection, network security and database encryption).

2. MULTONE i-MESSAGE - SYSTEM OVERVIEW

The Multitone i-Message supports the following functions:

- Time-critical voice and data messaging
- Point-to-point messaging with voice and data
- Point-to-multipoint messaging (broadcast) with voice and data
- Multiple mobile technologies supported:
  - Onsite Paging
  - Wide Area Paging (POCSAG)
  - SMART apps
  - Fixed line telephony
  - SMS messaging
  - Email
  - GPRS, 3G, 4G, 5G and WiFi
- Multi-site operation using TCP/IP and GD92 protocols - GD92 is a UK Home Office protocol supporting multiple communications bearers, protocol interfacing and automated routing.
- The system supports multiple levels of system and network redundancy and resilience and utilizes an upgradeable software and modular architecture.
- Enables centralised management of users, team and communications (fixed and mobile devices).
- Audit trail with file export and analysis tools.

3. MULTITONE i-MESSAGE - ARCHITECTURE, SOFTWARE & PROTOCOLS

The Multitone i-Message system supports almost an unlimited number of users, however, various protocols have limitations placed on them in terms of number of users supported and these are:

- SMART App messaging up to 20,000 plus users running on iOS and Android platforms

- Mk7 supports up to 40,000 users, using system number 0, 1, 2 and 3. A single user call is processed at 6 seconds per call, assuming 512 baud with time-stamp

- Mk6 supports up to 100,000 users. A single user call is processed at 6 Seconds per call, assuming 512 baud with time-stamp

- POCSAG supports up to 2,000,000 users. A single user call is processed at 6 seconds at 512 baud, 3 seconds at 1200 baud and 2 seconds at 2400 baud

- EIA Two-Tone supports up to 1,000 users

- SMS text messaging - For a single message to multiple users, this is currently, limited to 70 concurrent handsets, please note this will be extended to 26,000 concurrent handsets

***Note**: When selecting the required paging protocol a Multitone Dual Bearer Interface (DBI) will be required for encoding, for more information please see Appendix 1, or for Multitone IM-Lite the Universal Peripheral Audio (UPA) interface provides a direct link to the transmitter.*

3.1 Multitone i-Message - System Architecture & NDB Clustering

3.1.1 System Architecture

Multitone i-Message based systems use a cloud type architecture, which can support multiple Multitone i-Message operating together in server cluster. The Multitone i-Message cloud comprises a Master System, referred to as the Primary Master. Any additional systems linked to the Primary Master are Primary Solo systems. This ensures service continuity should one or more server services fail within the server cluster. This feature is ‘IP Takeover’ or ‘IP Failover’, with each server within the server clusters; a mirror image of the other.

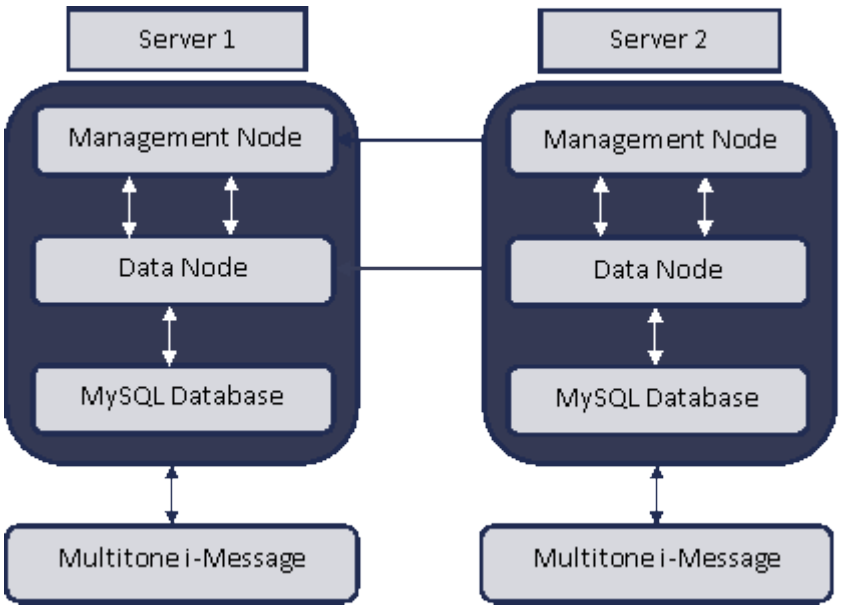
Each Multitone i-Message system links multiple servers (installed with Multitone i-Message software) together in clusters of up to 4-servers. Servers can be co-located in a single rack, or distributed across multiple locations, if they reside on the same IP subnet. Only different Multitone i-Message clusters can be distributed across different IP subnets to form the Multitone i-Message Cloud.

Each Multitone i-Message system must include one server (installed with Multitone i-Message software) as a minimum requirement; this becomes the Primary Server, without which the Multitone i-Message system will not operate. In order to ensure service continuity supply of a second server is highly recommended though not essential, installed with the Multitone i-Message software, this will elect itself to the secondary server function.

3.1.2 MYSQL Network Database

Multitone i-Message 1.8.0 and above supports MySQL Network Database (NDB) cluster database methodology 8.4.3 (non-enterprise licence).

The current Multitone implementation of NDB clusters is that the data nodes operate in a local node group of up to 4 x Multitone i-Message servers/data-nodes. Note, implementation across multiple, geographically dispersed server cluster locations or node groups is yet to be undertaken. The schematic below illustrates the current architecture of Multitone i-Message with respect to operation between dual Multitone i-Message servers - please note up to 4 servers can be connected, for the purposes of this diagram, 2 server connections are displayed to demonstrate the concept:



The impact is to reduce server synchronisation time from approximately 8 down to 1 to 2 minutes. This would suggest that Multitone i-Message achieves “Five 9’s” availability. However, given the fact that the system is dependent on a range of third party infrastructure, such as the customer’s network, telephone system, Microsoft updates etc., a more accurate calculation is 99.9% availability.

3.1.3 Network Architecture

In terms of network connectivity, the Multitone i-Message server cluster links to the TCP/IP network via a standard network switch. This enables the Multitone i-Message system to interface to the following infrastructure:

- Telephone system
- Paging transmitters
- Off air call verification system

- Intelligent transmitter monitoring system
- Existing Access 3000 paging systems
- PC/Touch-screen HTML interface to the Multitone i-Message system

***Note**: Total estimated network load is 1 percent of a 100Mb network, with potential peak loads of up to 5 percent.*

3.2 Multitone i-Message - Cloud Services (Support Only)

3.2.1 Multi-tenancy - i-Message Cloud Services

Multi-tenancy allows the Multitone i-Message system to “separate” customers and department, i.e. users, teams and personal information within a single i-Message installation - essential for cloud operation. This enables Multitone i-Message to host securely multiple customers, for example Customer A, Customer B and Customer C etc. When Customer A and their nominated employees access the system they will only see details relating to Customer A. By adopting multi-tenancy enables:

1. Customers to create and manage users and associated devices

2. Customers to create and manage teams and groups and associated devices

3. Customer management of the call log functions

4. Customer to send user and team calls

However, the following caveats **MUST** be observed:

1. If integration with telephony, computer based systems or paging is required, the ability to supply on-site hardware to support necessary interfaces, e.g. Pagers, Transmitters, Integrators and Dual Bearer Interfaces etc., will be required.

2. It must be accepted that access to system, set-up and configuration of interfaces, live-boards, white-boards, blackboards, activity log and call logs is not a shared activity. Multitone will manage this element of the installation as part of system set-up with the customer as part of support process

3. Each instance and customer domain will support the following customer user and supervisory functions:

    - User, team and group messaging
    - User and team administration
    - Transfer management
    - User presence administration.
    - User device administration

- Access to map-boards and live-maps*
- Access to whiteboards, blackboards, live-board and majax incident management*

* Multitone will be required set-up and configure these applications on the customer's behalf

***Note**: The System Control Unit (SCU) will enable customer to access all the above features and functions. Access to the "engineering functions" is restricted, limited to Multitone authorised staff only.*

4. Alarm panel - visual access to alarm status and the ability to acknowledge alarm receipt, Multitone will be required set-up and configure these applications on the customer's behalf.

5. Calls and queries log - access to the call log and the ability to set-up and run queries with the ability will be required to export logs in HTML or CSV format. Please note that system log is no longer available to customers, this is provided as an engineering tool for Multitone.

6. User and team administration - the ability to create, edit and delete users, teams, canned speech messages (recordings) and alpha messages within a single customer domain.

7. User profiles - to allow client users to amend personal profiles within the scope of their access rights.

8. Customer database back-up - the ability to back-up the Multitone i-Message database to the cloud only, no data resides on the customer site. Please note it is the customer who owns and manages this data; therefore it the customers responsibility under GDPR to ensure record accuracy and removal - not Multitone. Multitone may only have access to this data at the customers written permission

9. Device tab - for many current Multitone i-Message users this facility is not used, but available if required.

10. Telephony - the ability for a customer to interface and configure local single and/or multi-site telephony services, e.g. PBX or cloud service provider, under their domain identity with Multitone i-Message operating in the cloud.

11. Device channels – the ability to organise and isolates multiple device channels, ensuring that only specific customers devices are called without interference.

3.2.2 Multitone i-Message Cloud Hybrid Support

By creating single customer instance within AWS it is possible to allow the customer to support a cloud/hybrid solution linking the cloud via VPN to on-premises equipment supporting Multitone i-Message 1.8.0 software. This ensures Five 9's or greater cloud delivery with the local servers, failing over should there be any failure in the delivery of cloud services.

3.2.3 Amazon Web Services

Multitone's i-Message as a cloud service is available via the Amazon Web Services (AWS); the rationale for AWS as our service provider is as follows:

- Global market presence - AWS has the largest global infrastructure footprint of any provider, with many major organisations deploying cloud services, e.g. Cerner, Pando, Alertive, Swissphone and SPOK Go.

- Highly secure - 24/7 monitoring, AES 256 encrypted network designed to meet the most stringent security requirements in the world.

- Low latency - single-digit millisecond latencies with low packet loss with high overall network quality, for speech applications, such as i-Message this is essential.

- High service availability - 100GbE fibre network backbone, delivering a global availability of 4 9's, by splitting the architecture up to 5 9's is achievable.

- Flexibility - enables companies to be extremely flexible with respect to rapid scalability, this ensures that you can add additional resources as and when they are required, for example, smoothing peak loads by deploying hundreds or even thousands of servers in minutes.

3.3 Multitone i-Message - Server Software

3.3.1 Multitone i-Message

Each Multitone i-Message server supports the following software:

- Windows Server 2012, 2012R2, 2106, 2019, 2022

- Multitone i-Message supports Microsoft Windows Server Embedded Standard 2016, 64Bit Multi-Language ESD OEI 16 Core Telco Licence.

***Note**: This is an embedded licence, supplied and pre-loaded as part of the Multitone i-Message system (the hardware). This licence does not require a Client Access Licence (CAL). The use and operation of licence enables Multitone Electronics plc as the Original Equipment Manufacturer (OEM) under the terms of the licence from Microsoft to supply this software to customers as part of the Multitone i-Message system and for the customer to use the system without let or hindrance.*

- ActiveMQ, Version 5.15.11 (1.8.0) 5.16.4 (1.8.1)
- Apache Web Server, Version 2.4.49 (1.8.0), 2.4.53 (1.8.1)
- 7zip (Version 19.00 (x64), 1.8.0 and 21.07 (x64) 1.8.1
- Java Runtime Version 8.0.0
- MySQL Network Database (NDB) cluster database methodology 8.0.27 (1.8.0) and 8.0.30 (1.8.1)
- MCS Version 4.33 March 2020 (1.8.0) and 4.37 (1.8.1)
- Asterisk PBX module - This operates under LINUX it runs as a virtual machine as a result the system will not operate in a virtualised environment.
- Multitone i-Message Communications Processor (CCP) - Developed by Multitone is an intrinsic part of the Multitone i-Message system with respect to communications protocol support.

Multitone i-Message software, configured as an image, designed to operate as a single cloud instance, on multiple server clusters or on a single server dependent upon application. This ensures no software or network contention with other applications.

3.3.2 Multitone IM-Lite A, B, C & D

Each Multitone IM-Lite system supports the following software, please note that IM-Lite does not support multiple server redundancy as it is contained system:

- Microsoft Windows 10 Professional (OEM Licence Key)
- ActiveMQ, Version 5.15.11 (1.8.0) 5.16.4 (1.8.1)
- Apache Web Server, Version 2.4.49 (1.8.0), 2.4.53 (1.8.1)
- 7zip (Version 19.00 (x64), 1.8.0 and 21.07 (x64) 1.8.1
- Java Runtime Version 8.0.0

- MySQL Network Database (NDB) cluster database methodology 8.4.30 (1.8.1)

- MySQL (Version 5.7.26 version) non enterprise licence, ODBC (Version 5.3.10), 1.6.3

- IM-Lite-B, C & D - Asterisk PBX module - This operates under LINUX it runs as a virtual machine as a result the system will not operate in a virtualised environment.

- Multitone i-Message Communications Processor (CCP) - Developed by Multitone is an intrinsic part of the Multitone i-Message system with respect to communications protocol support.

3.3.3 Multitone IM-Lite product variants

Multitone IM-Lite is available in four options:

- Multitone IM-Lite A
- Multitone IM-Lite-B
- Multitone IM-Lite-C
- Multitone IM-Lite-D

The following table provides an overview of key features with respect to users, licences, message agents, alarm agents, hardware requirements and power options:

	Multitone IM-Lite-A	**Multitone IM-Lite-B**	**Multitone IM-Lite-C**	**Multitone IM-Lite-D**
System users	500 users	50 users	500 users	300 users
Redundancy	Single CPU, no redundancy	Single CPU, no redundancy	Single CPU, no redundancy	Dual CPU with CPU failover & redundancy
Multitone Appear app support	20 licences – any combination of Multitone Appear or Appear Lite, additional licences may be ordered separately	20 licences - any combination of Multitone Appear or Appear Lite, additional licences may be ordered separately	20 licences - any combination of Multitone Appear or Appear Lite, additional licences may be ordered separately	20 licences - any combination of Multitone Appear or Appear Lite, additional licences may be ordered separately
Message Agents	Any combination up to 3, additional agents may be ordered separately	Any combination up to 3, additional agents may be ordered separately	Any combination up to 3, additional agents may be ordered separately	Any combination up to 3, additional agents may be ordered separately
Alarm Agents	Any combination up to 3, additional agents may be ordered separately.	Any combination up to 3, additional agents may be ordered separately.	Any combination up to 3, additional agents may be ordered separately.	Any combination up to 3, additional agents may be ordered separately.

Telephone Interface	N/A	10 concurrent extension Multitone Appear+ Conferencing not supported	250+ concurrent extensions	250+ concurrent extensions
Universal Peripheral Interface (UPI), 16 DLC's	Up to 3 (48 DLCs max)	Up to 3 (48 DLCs max)	Up to 3 (48 DLCs max)	Via Multitone Integrator
Universal Peripheral Audio Interface (UPA)Transmitter support (Transmitter Interface or 16 DLC's)	Up to 3 For speech and synchronisation, a single UPA will be required with an Audio Distribution Unit (ADU)	Up to 3 - For speech and synchronisation, a single UPA will be required with an Audio Distribution Unit (ADU)	Up to 3 - For speech and synchronisation, a single UPA will be required with an Audio Distribution Unit (ADU)	Via Multitone Integrator/Dual Bearer Interface
USB/RS232 Interface	Up to 3	Up to 3	Up to 3	Via Multitone Integrator
Ethernet Port (RJ45)	1 only	1 only	1 only	2 only
Multitone i-Message hardware expansion, e.g. to support additional transmitters, message and alarm agents	Yes via 8 port Network Switch	Yes via 8 port Network Switch	Yes via 8 port Network Switch	Yes via 8 port Network Switch
Mounting options	Desk, Wall & Rack options available	Desk, Wall & Rack options available	Desk, Wall & Rack options available	Desk, Wall & Rack options available
Multitone i-Message software	Yes	Yes	Yes	Yes
Power options	UK, EU & North America	UK, EU & North America	UK, EU & North America	Dual UK, EU & North America
Temperature range (subject to confirmation)	Operating 0°C to +50°C	Operating 0°C to +50°C	Operating 0°C to +50°C	Operating 0°C to +50°C

3.3.4 Multitone i-Message & IM-Lite Accessory Devices

The newer images are marked on the web Interface as "Multitone Device", the Multitone device combined Image covers the following products:

- IM-DBI
- IM-LITE-DLC
- IM-INT (Formerly IM-MINI)
- P1061M
- P1058
- EMS-DBI

For the current release, Multitone Device Image Version 3.00 supports the following system software:

- Raspbian Buster Linux 10
- Apache Web Server 2.4.38
- XRDP 0.9.9

3.4 Multitone i-Message - Communications Processor (CCP)

The Multitone i-Message Communications Processor supports a total of 64 Message Transfer Agents (MTA) and User Agents (UA), 2 x agents are reserved for the Router Agent and the Universal Datagram Protocol (UDP) agent, leaving a total of 62 agents available for messaging, system interfacing and information reporting. If additional interfaces are required, use of CCP's will extend the number of interfaces available. Agent support is as follows:

- 62 x Mk6/Mk7 encoders
- 62 x Call verification Units
- 62 x POCSAG encoders
- 1 x SMTP nominated email outgoing mail agents (only 1 can be specified)
- 62 x RS232 interfaces
- 62 x TCP/IP Interfaces
- 992 x Direct Closing Contacts (DLCs)
- 62 x Display Agents (Wallboard Displays)
- 1 x SMS Gateways (only 1 can be specified)
- 62 x Printer Interfaces
- 62 x Web Sockets
- 62 x Call Verification Units
- 124 x Directly connected transmitters (sharing same connection)
- Over 300 master and slave, synchronised transmitters
- 1 x LAN Peripheral Interface (LPI) supports up to 30 Multitone absence and charging racks (slave version only) giving a total of 240 pockets

***Note**: For RPR950, RPR750, RPR550 and RPR530 receivers, 1 x PSU supports up to 4 x A3RF or 4 A3RP (Intrinsically Safe) slave absence and charging racks. For MIT870 Management Information Terminal, 1 x PSU supports up to 9 x A3RR Slave Absence & Charging Racks, this supports both standard and intrinsically safe (IS) configurations.*

3.4.1. Multitone i-Message - Communications processor (CCP) - Messaging Protocols

Multitone i-Message supports the following message protocols:

- Email (SMTP) Interface
- SMS (PrimetexT) Interface
- Multitone Integrator & RS232 Serial GSM Modem (United Kingdom)
- Multitone Integrator & RS232 Serial GSM Modem (Europe)
- TAP RS232 Interface & Cable (Multitone Integrator Required)
- TAP & SMS Wide Area Dial out (PSTN Modem & Cable) UK
- TAP & SMS Wide Area Dial out (PSTN Modem & Cable) EU
- ESPA 4.4.4 RS232 Interface (Multitone Integrator Required)
- ESPA-X (Incoming Only)
- MEP RS232 Interface (Multitone Integrator Required)

- MSP (Scope) RS232 Interface & Cable (In) Multitone Integrator Required
- MSP (Scope) RS232 Interface & Cable (Out) Multitone Integrator Required
- SNPP output
- Kenwood Digital Interface (Data Only) - 25-way cable - LPI required
- EkoTek Interface & Cable - i-Message to EkoTek - LPI Required
- Access 3000 Interface & Cable - 2 x LPIs Required
- Access 3000 Absence Rack Interface & cable - LPI Required
- Direct Line Contacts (DLCs) Multitone Integrator or IM-Lite-DLC interface required
- TPL Systems 2-way Interface (GPRS, 3G, SigFox & POCSAG)
- Protocol Scripting Interface - Price on Application (POA)
- SMPP Interface (GSM, GPRS, 3G)
- Polycom UC Protocol (Spectralink WiFi Messaging)
- Command Processor Protocol (Station Text Command)
- Samsung TAPI Interface
- Sepura (SDS Protocol) Interface
- TNPP Protocol (Server)
- Multitone MIP Protocol (Data only)
- Scope CX5 Protocol (TCP/IP)
- Prism IPX Interface Protocol
- SAGRN Protocol (Windows Only) New Zeeland

3.4.2 Multitone i-Message - Communications Processor (CCP) - Alarm Agents

- Gent Interface (Multitone Integrator Required)
- Rauland Borg Interface (Multitone Integrator Required)
- Codem2/Nursecall Interface (Multitone Integrator Required)
- Static Systems 925 Interface (Multitone Integrator Required)
- Texecom Premier 48 Interface (Multitone Integrator Required)
- Minerva 16/80 Interface (Multitone Integrator Required)
- Morley-IAS ZX Interface (Multitone Integrator Required)
- Tyco MX/ZX Interface (Multitone Integrator Required)
- Chubb 380A Interface (Multitone Integrator Required)
- Guardsman Printer Interface (Multitone Integrator Required)
- Wipath PDR2000 Interface (Multitone Integrator Required)
- Controlmaster 600 Interface (Multitone Integrator Required)
- Clover Interface (Multitone Integrator Required)
- Satchwell BMS Interface(Multitone Integrator Required)
- Protec Interface (Multitone Integrator Required)
- Gent Binary Interface (Multitone Integrator Required)
- Ziton ZCP2 Interface (Multitone Integrator Required)
- Universal Printer Interface (Multitone Integrator Required)
- Static Systems Codemlon Interface (Multitone Integrator Required)
- OPC-DA (Swisslog) Gateway Protocol (Intel NUC PC Required)
- Scope ConneXions 2 Mk7 Alarm System Protocol (Intel NUC Required)

- Capture Protocol
- Static Systems IP Fusion
- Honeywell Notifier 10 3000
- CEI XML Spacelabs Protocol
- Austco Alarm Protocol
- Modbus TCP Protocol
- Alarm Agent Cable Installation Kit (1 per alarm agent)

3.4.3 Multitone i-Message - Communications Processor (CCP) - External Modules

- RotaWatch (External Module) - Beta Released Only
- WorkFlow (External Module)
- Multitone Major Incident Management (Majax) Module

4. MULTITONE i-MESSAGE - TELEPHONE SUPPORT

The Multitone i-Message system interfaces to your telephone system using either SIP or Analogue. The interface is voice prompted taking the user through a structured menu in order to send user or team calls. Voice prompts may be over-dialled in order to increase speed.

As the Multitone i-Message system supports an internal PBX capability it is possible to use this facility as a standby PBX, though this is limited to 255 simultaneous calls and features are limited to send, receive and transfer a call. Please note using the 3:1 ratio, 250 simultaneous calls means that it can support a system of approximately 750 telephone extensions.

The Multitone i-Message system includes supports a telephone truck detection feature - i-Message keeps polling trunks to ensure constant connection with the customers PBX reducing jitter on speech messages to less than 100ms, to ensure no delays and clipping.

4.1 SIP Interface

The Multitone i-Message system supports up to:

- 1,000+ SIP Interfaces
- Maximum off 1,000+ simultaneous conversations

- Maximum one-way voice message length is 30 Seconds on all devices (Pagers, Mobile Phones, Multitone SMART Apps, DECT and WiFi phones)

Where the PBX supports SIP, the Multitone i-Message system will interface to the SIP PBX using:

- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

- SIP Info (RFC 2976 The SIP Info Method)

4.2 Analogue/SIP interface

In order to interface to your telephone system the Multitone i-Message system supports SIP and Analogue telephone interfaces. This will provide either Trunk (preferred) or Extension level access. Dependent on physical location, the Multitone i-Message system can interface to the telephone either directly using the network hub (local connection) or via the customers IP network (non-local connection).

In terms of network security, the SIP/Analogue interface sits behind the Multitone i-Message system and therefore the customer's network. Consequently, you cannot use this interface to access the Multitone i-Message system, the customer PBX or IP network. Even if the IP addressed were penetrated, the result would be to prevent connectivity it would not damage operation of the PBX or the Multitone i-Message system.

5. MULTITONE i-MESSAGE - ON-PREMISES, CLOUD SECURITY & COMPLIANCE

5.1 Introduction

The purpose of this section is to outline how Multitone Electronics PLC adhere to the NCSC principles with respect to the provision of cloud services and has the necessary methods, processes and audit controls to ensure that the cyber security is constantly monitored, reviewed and revised with respect to cloud, on-premises equipment to mitigate cyber risk. Multitone i-Message is available as an on-premises or a cloud based solution provisioned via AWS. The first section of this document considers the NCSC principles in context of Multitone and Multitone i-Message as a service. Section two focuses on the security processes adopted with respect to the provision of Multitone i-Message as an on-premises solution.

5.2 Application of NCSC principles to Multitone i-Message cloud services

5.2.1 Principle 1, Multitone i-Message - Data in Transit Protection

1. Distributed Denial of Service (DDoS) - for Multitone apps, the server IP addresses/port numbers are not in the public domain, but are available to app users via the Multitone administrator. There is also the option to deploy i-Message DNS, hiding IP addresses and ports.

2. Man in the Middle (MITM) - the Multitone i-Message System Control Unit (SCU) user interface is browser base secured with an HTTPS certificate. Multitone smart apps support end-to-end encrypted sessions using AES 128/256.

3. Internet Protocol Spoofing - inherent in AWS design.

4. Port Scanning - inherent in AWS design.

5. Encryption at rest - data between the Multitone i-Message cloud service and Multitone apps (Appear, Appear Lite, Appear Crew and Appear WorkFlow) is encrypted to AES 128 and Multitone Messenger is encrypted to AES 256. For Multitone Appear, Lite and Crew and Workflow Access to the app service is user name and password protected. Multitone Messenger supports two-factor authentication and is a password-less application. Multitone apps do not interface with any external APIs as the system is unique to Multitone i-Message only.

5.2.2 Principle 2, Multitone i-Message - Protection & Resilience

1. Physical location of data - Multitone i-Message is deployed via the AWS data centre, located in UK regional zone only. The AWS data centre location is unknown and is not disclosed.

2. Data centre security - provided by AWS as part of our supply contract, please refer to document: Using AWS in the context of NCSC UK's Cloud Security Principles, October 2016.

3. Encryption at rest - Multitone i-Message cloud supports MySQL clustering database this is password protected with user logon using AES 256 encrypted passwords. For Multitone apps the device database is AES 256 encrypted.

4. Data sanitisation - system executable commands ensure that all user entered data is Multitone i-Message system compliant, any suspicious looking content is automatically excluded and ignored.

5. Physical resilience and availability - the service level agreement with AWS states a minimum service availability of: Five 9's (99.999%).

6. Data back-ups - Multitone i-Message backs-up data automatically as part of a regular schedule.

5.2.3 Principle 3, Multitone i-Message - Separation Between Users

1. User separation - databases are organised by segregation, this is achieved through configuration by allocating named Multitone customers with association to individual users (a user is an entity inside the Multitone i-Message with allocated devices (Pager, Apps, Email, SMS). Furthermore, individual users can be further segregated to a single department with least access limited to a single set of applications.

2. Health-check - monthly updates to operating system and quarterly updates to third party software, e.g. MySQL, Apache Web Server 2 etc.

5.2.4 Principle 4, Multitone i-Message - Governance Framework

1. Named security owner - Multitone i-Message cloud services, Dave Bond, Head of Research & Development (Multitone Board) and daily operational management: Ryan Monaghan, Head of UK Customer Services.

2. Multitone corporate Information Security Management System (ISMS) - ISO27001 certification, note this does not include Multitone i-Message.

3. Security certification - for HTTPS, security certificates are generated by Multitone Electronics PLC

5.2.5 Principle 5, Multitone i-Message - Operational Security

1. Configuration and change management - system upgrades, fixes and new features are undertaken under the Multitone ISO9001. This ensures that any new features, change request are documented, recorded, reviewed and signed-off at key delivery gates to enables annual audit and ongoing ISO9001 certification.

2. Vulnerability management - Microsoft security and other relevant bulletins are reviewed daily by the software SQA team. Server updates are reviewed monthly with critical updates addressed within 1 to 2 weeks from notification. Other patches, such as general bugs addressed generally within 4 to 8 weeks from notification and severity assessment. The Multitone change control system (Redmine) is used to log (with serial number) the required fix, allocate resources and track progress.

3. With respect to incident management and protective monitoring, Multitone have the following tools and processes in place:

    a. The Multitone i-Message system via system log and employment of the event action manager (EAM) can generate adequate audit events with respect to multiple login attempts, failed login attempts and any suspicious activity with alarms to enable fast and effective identification of suspicious activity.

b. Deploying alarm notifications, regular analysis enables Multitone to identify potential compromises or inappropriate use of your service.

c. The service provider takes prompt and appropriate action to address incidents usually within minutes of the event occurring, with any fix implemented within 24 hours.

5.2.6 Principle 6, Multitone Electronics plc - Personnel Security

1. Staff screening - Multitone does not adhere to BS7858:2012, to ensure personnel security the following checks are undertaken on all new Multitone UK employees: passports, driving licences, previous employment history and references, verification of education (certificates, diplomas and degrees). For non-UK nationals: passport, driving licence, UK status and eligibility, previous employment history and references and verification of education.

2. Multitone access & service management - for Multitone i-Message, three employees - Head of Customer Services, Consultant Technical Specialist (Fires) and Technical Support Engineering Manager. For AWS access is limited to two employees, Head of Customer Services and Tech Support Engineering Manager.

5.2.7 Principle 7, Multitone Electronics plc - Secure Development

IS09001-2015 certified - Multitone systems are designed for mission critical operation, i.e. healthcare, fire and rescue etc., software design is in accordance with the principles developed by Saltzer and Schroeder (1974) in respect of protection of information in computer systems. All development IPR is encrypted, password protected and not accessible via the internet. For reasons of flexibility Multitone does not include products or design services controls with respect to 27001, 27002 and 27017 and is not included within the scope of our ISMS.

5.2.8 Principle 8, Multitone Electronics plc & i-Message - Supply Chain Security

1. Security requirements for third-party providers supporting Multitone systems and devices with respect to intellectual property are established under mutual non-disclosure agreement between Multitone and the third party, this is policed under GDPR.

2. In support of data we process under the ISMS (ISO27001) we have not, and do not enter into Non-Disclosure Agreements as it is data under the GDPR; of which we are required by law to protect and preserve in any instance.

3. Multitone i-Message cloud services can interface to third customer gateways for alarm/messaging applications using an IP and/or an RS232 interface. In this situation input device will be required to identify a user or team identification number but not individual user details; this remains resident within the Multitone i-Message system database.

5.2.9 Principle 9, Multitone i-Message - Secure User Management

1. The number of system users and local system administrators will be identified to Multitone by the customer.

2. The number of local users and administrators with user name, passwords and access rights are configured and authenticated by Multitone only.

3. Rights are assigned on the basis of least privilege, i.e. only those users who require basic user and/or admin rights are granted access.

4. User and basic admin access can be limited to a dedicated device using a locked image ensures no email or web browser access.

5. The customer will not be given configuration and/or engineering rights, these remain with Multitone.

5.2.10 Principle 10, Multitone i-Message - Identity & Authentication

1. Active Directory - Optional and at user name and password access only, validates that the Multitone i-Message user name and password with Active Directory authentication data, if verified then access is granted to the Multitone i-Message system.

2. Access limits - Multitone i-Message is limited to a private community and is not publicly available.

3. TLS support - Multitone i-Message supports authentication over TLS using an X.509v3 client certificate that identifies an individual user.

4. Two-factor authentication - The Multitone Messenger app supports using two-factor authentication via email link or QR code, also incorporates password lock after three unsuccessful login attempts.

5. Admin authentication - using access rights mechanism, it is possible to differentiate separate user accounts and admin accounts if required. Note access to i-Message system configuration, engineering and AWS management is entirely blocked and limited to Multitone access only.

5.2.11 Principle 11, Multitone i-Message - External Interface Protection

1. Network connection - via internet or private network dependent upon application. For apps and web interfaces only an internet connection may be adopted supporting HTTPS. Where access to SIP and GD92 a VPN tunnel between AWS and the customer network is recommended, this ensures security and customer segregation.

2. External interface protection - i-Message cloud services sit behind a firewall with unnecessary ports and IP addresses blocked. For Multitone apps an additional proxy server is provided creating DMZ between Multitone i-Message cloud, the customer and external IP networks.

3. Geo-location lock - via firewall with the ability to block non-customer IP addresses. Also note use of the AWS UK activity zone will be deployed for UK customers only.

5.2.12 Principle 12, Multitone i-Message - Secure Service Administration

1. Dedicated system administration model - the single administrative model is adopted, permissions restricted with the account restricted to 3 employees.

2. Normal workstation for system admin - for customer user and local administrative access can be restricted to the employment of dedicated devices, these employ a locked-down image with the Multitone i-Message application only enabled. These devices are solely for messaging and local service management and not for general use, i.e., use of email, general browsing and other PC applications is removed and therefore, unavailable.

5.2.13 Principle 13, Multitone i-Message - Audit Information for Users

1. Audit log of users - this is provided via system log; this records all transactions on the system by time and date

2. Audit log retention - no time limit, system logs automatically backed-up for archiving as a matter of routine

3. Protective monitoring feed - customer incidence reporting through Multitone customer support desk, Multitone are monitoring the system 24/7

4. Security dashboard - no, however, Multitone i-Message does have the ability to facilitate alarming within the system for any suspicious activity.

5. Supplier audit logging - yes, please note that data is made available via negotiation to avoid GDPR infringement.

5.2.14 Principle 14, Multitone i-Message - Secure Use of the Service

1. Device access controls - user name and password protected, passwords, as stated, are encrypted.

2. Posture checking - no, but Multitone i-Message web interface currently supports Apache 2 server V2.4.49, the System Control Unit (Java) and smart apps will only operate on versions o latest maintained versions of iOS, Android, also all smart devices must be enterprise grade and support WiFi traversing if deploying on internal WiFi networks.

3. Bring Your Own Device (BYOD) controls - when the app is operational, all transactions between the Multitone i-Message system and the app are monitored and logged, therefore, an independent SMART device will have system transparency.

4. Malware protection – anti-virus malware protection applied to cloud servers, supervisor module will maintain service integrity to ensure service delivery.

6. Multitone i-Message System Security

6.1 Multitone i-Message Hardware - Statement of Security Compliance

The Multitone i-Message system, designed as an always available, resilient, critical messaging platform. Multitone certifies that the Multitone i-Message system uses a customised, hardened Windows Server Operating System with the latest operating system security patches and updates when commissioned at a customer site. Once installed into the ‘End User's’ environment it is the responsibility of the ‘End User’ to ensure that the operating system is updated as required, subject to the restrictions and conditions listed below, particularly where updates may cause an Operating System to reboot.

Implementation of Microsoft Windows updates must be under controlled conditions, where correct procedures is followed, will ensure minimal system downtime is experienced, thus preventing loss of service to a critical system during the update. If required the customers Change Advisory Board (CAB) process will require correct instigation with a description of works and potential impact on services highlighted to the Trust. If Microsoft Windows updates are applied, they must be undertaken manually, not set to automatic.

Any updates requiring a system re-start will require the presence of a Multitone Engineer to ensure that performance of all work is undertaken correctly, so there is a minimal risk to the system and associated components.

The Multitone i-Message system sits behind the customers firewall and generally does not have direct access to the internet. However, if a customer's network is compromised by a cyber event, such as "WannaCry", that is the only way by which the Multitone i-Message system is affected. Generally, the Multitone i-Message systems sits on its own V-LAN separated from the main/core network with only specific ports used for browser sessions etc., this adds a level of security by limiting the amount of network traffic allowed to access the Multitone i-Message servers and equipment.

It is the responsibility of the 'End User' to install and maintain the appropriate Anti-Virus and/or Anti-Malware protection, which is compliant with the "End User's" policy. Most Anti-Virus software operates with Multitone i-Message servers and applications this includes: Sophos and McAfee.

However, please inform Multitone and provide a copy of any specific anti-virus product, if an alternative installation is required, this will allow Multitone to test this software prior to installation, ensuring no detrimental effects. If the installation of anti-virus software requires a server re-start, it is necessary that a Multitone Engineer is present to ensure any loss of service is minimised and controlled. This would require the authorisation of the trust via normal CAB process in use, before any works can commence. If an update to anti-virus software requires the servers to be re-started, the above would re-apply.

If a Multitone Engineer were required on site for Trust specific security policy updates, this would be a chargeable visit and would need to be organised with Multitone to schedule a suitable date to have an Engineer in attendance.

With respect to Multitone i-Message peripheral network devices, the Multitone i-Message eco-system supports a range of peripheral devices, designed to sit behind the Multitone i-Message system and therefore in the customer's network. Whilst these devises are network enabled, with the exception of the System Control Units (SCU) they are not Microsoft Windows devices, using a hardened and embedded operating system and only communicate to the Multitone i-Message system at the application level via a proprietary protocol. They cannot be utilised as a gateway or point of entry back to the Multitone i-Message system. The SCU's can support anti-virus and windows updates though care is required when performing updates to the Windows Operating System.

6.2 Multitone i-Message - Network Security

The Multitone i-Message system operates behind the clients existing computer network infrastructure (Firewalls, NATs and External Routers etc.) it is not a public system that is freely available on the internet. The system relies on the customer's network security arrangements to ensure secure operation.

Multitone i-Message uses the GD92 UK Home Office protocols, running over TCP/IP, allows the system to operate using unique network ports, further enhancing overall network security. GD92 uses a clean, well-defined architecture with full protocol layer separation making it very bandwidth efficient and is about 25% more efficient than an IP network. Tested by Logicalis (Cyber Security Specialists) GD92 was more or less impossible to penetrate.

Multitone recommends that the paging element of the Multitone i-Message system to operate using its own network using the current transmitter cabling. This saves time, hardware costs and ensures system continuity as it is fully independent from any other communication network within the customer organisation.

It is possible to put the Multitone i-Message system behind a separate router; this would separate i-Message from the main network. However, it would make configuration and set-up more complicated and is not a complete guarantee from virus attack.

6.3 Multitone i-Message - System Security

Multitone i-Message software, configured as an image, operates on a single server or cluster environment; this ensures no software or network contention with other applications. The following security processes are enforced:

6.3.1 Software Security & Update Management

Multitone i-Message supports Windows Server 2012, 2012 R2, 2016, 2019, Win IoT using the Microsoft telco licence, Client Access Licence (CAL) and Windows Server IoT 2022

With respect to Microsoft bug fixes and software updates, Multitone regularly reviews all applicable updates, undertakes appropriate compatibility testing, making these available via the Multitone Server Update Notice to relevant agents and end users. This is an ISO 9000-controlled process managed by the Multitone Software Quality Assurance (SQA) Team.

With respect to patching, Multitone’s policy is one of controlled patching, this is undertaken by a qualified Multitone Engineer or by the customers IT department, whichever is easier. For any critical updates, installation is immediate and undertaken in a controlled manner and according to Multitone operational policies for the Multitone i-Message system.

Please note that updates to Multitone i-Message system dependent software, such as MySQL and Apache etc., is regularly updated and released as a Multitone i-Message software point release.

6.3.2 Antivirus Software Policy

There are no restrictions on what anti-virus software by the end user; customer preferred antivirus software is supportable. For any critical updates to the antivirus software that require a re-start we strongly recommend it is done in a controlled manner and according to Multitone operational policies for the Multitone i-Message system.

6.3.3 Server & Client Security

Client access to the software is via user name and password authentication, control of client features is via access rights determined by the system administrator.

6.3.4 Server Virtualisation – Not Advised

The Multitone i-Message platform supports a Linux based Asterisk PBX, this runs inside a virtual machine on the Windows machine to which the Multitone i-Message system is running, therefore, for this reason the system **designed not to operate in a virtualised environment**.

For non-speech applications virtualisation is supportable, you will require need similar server specification as to that required for an on-premises installation. For virtualisation we will require 2 x Windows based servers, 16GB RAM with high specification CPU (Minimum 2) and 500GB HDD.

If speech is required partial virtualisation can be supported, a separate server or servers are required to support the i-Message PBX; this avoids the problem of network jitter where speech paging is required. For this to operate Multitone will require 2 of PBX VM, Multitone will provide the image, the minimum specification is 4GB RAM, high specification CPU and 150GB HDD.

This architecture is that it allows the Multitone i-Message to run as a sub-system if there is any failure or faults in the clients IT systems, furthermore this architecture allows a message to be sent using non-TCP/IP routes, providing additional redundancy.

6.3.5 Multitone SMART DMZ Secure Proxy Server Security

The Multitone DMZ Secure Proxy Server provides additional layer of network security without breaching existing client security requirements with respect to external internet connections from applications such as Multitone SMART apps.

Multitone DMZ Secure Proxy Server acts as a two-way proxy between Multitone SMART Apps and the Multitone i-Message SMAP Server forwarding TCP/IP connections from one IP address and port to another and filters out all non-Multitone SMART Apps traffic. As a result, only packets encrypted with the Multitone i-Message SMAP Server headers are accepted. The Multitone SMART Apps DMZ Secure Proxy Server sits between Multitone SMART Apps and the actual Multitone i-Message SMAP Server on the network, allowing the real Multitone i-Message Appear Server to be hidden inside the network, protecting it from attack.

The Multitone DMZ Proxy Server can be set-up to form a chain of proxies, this enables use of multiple firewalls to transfer and forward traffic from the Multitone SMART application to the Multitone i-Message SMAP Appear Server. It is possible to apply restrictions on the number of active TCP/IP connections that you can proxy onto a given IP address and port. This allows you to restrict the amount of traffic passing through the proxy server guarding primary routers and servers from Distributed Denial of Service (DDoS) attack. Multitone SMART Apps DMZ Secure Proxy Server uses five distinct configuration parameters to achieve this objective:

- Listen address - The IP address to listen for incoming TCP/IP connections from an IP connection source, Multitone SMART Apps,

- Listen port - The port number to listen for incoming TCP/IP connections from an IP connection of any description,

- Connect address - The IP address to forward all Multitone SMART Apps Server packets to the Multitone SMART Apps Server and Multitone i-Message,

- Connect port - The port number to forward all Multitone SMART Apps Server packets to the Multitone i-Message system,

- Maximum proxy connections - The maximum number of proxy connections forwarded at any one time, i.e. the number of Multitone SMART Apps devices connected through the Multitone SMART Apps DMZ Secure Proxy Server at one time. The default is set at 1,000 concurrent connections.

6.4 Multitone i-Message - Database Security & Back-up

The Multitone i-Message system database is fully encrypted using Advanced Encryption Standard (AES 256) bit encryption (MySQL database).

Backup of the Multitone i-Message system, configuration and database is automatic or manual, undertaken at any point in time. Use of third party storage devices for a backup may be used. Each backup is logged with time and date stamp.

With regard to system, data integrity and performance the backup method adopted by Multitone i-Message will have no impact of system operation. Servers are clustered, therefore back-ups are taken from the non-operational server, as each server is mirrored; this ensures that it will have no impact on system performance. Each server cluster will support up to 4-servers, so even if one server were to fail in this process the impact on operation and performance would be negligible.

To ensure successful completion of an unattended backup, is a fully automated process; the Multitone i-Message system automatically sends notifications via email that a backup has taken place.

6.5 Multitone i-Message - Paging & Transmitter Network Security

The paging transmitters, off-air call verification system and intelligent transmitter interface all connect to the Multitone i-Message system via a network interface (LAN Peripheral Interface). The LAN Peripheral Interface or LPI allows interfacing to other devices, such as transmitters, RS232 inputs and closing contacts etc.

In terms of network security, the Dual Bearer Interface (DBI), Multitone Integrator and/or the LAN Peripheral Interface (LPI) sit behind the Multitone i-Message system, therefore the customer's network. You cannot use the LAN Peripheral Interface to access the Multitone i-Message system nor can paging calls be made through this hardware, calls must originate from the Multitone i-Message system.

Even if the IP address was changed, or the configuration of Dual Bearer Interface and/or LAN Peripheral Interface were penetrated and altered, the result would be to prevent a device or agent connected to this hardware from operating; it would not affect network security. As a final point, as the LAN Peripheral Interface uses unique ports, the network security risk is insignificant and the Multitone i-Message system will immediately detects if an LPI is out of order and raise this as a fault.

For Multitone i-Message physical interfaces supporting Raspberry Pi based hardware, please note the following security features:

1. Use of non-default passwords

2. Identified as a Multitone device, not a Raspberry PI/Linux box, please note that Version 3.0 will use different names

3. Fixed image - unused services within the device are switched off limiting vulnerability and required no external access, they should be ring fenced within the hospital network and therefore will pose no risk to the network, essentially a secure black box.

4. The Multitone i-Message system monitors all devices interfaces to the system, if a hacker were to access this device (which is located behind customer network security and firewalls), the device would stop operating and i-Message will detect and raise an alarm.

6.6 Multitone i-Message - On-premises System Resilience

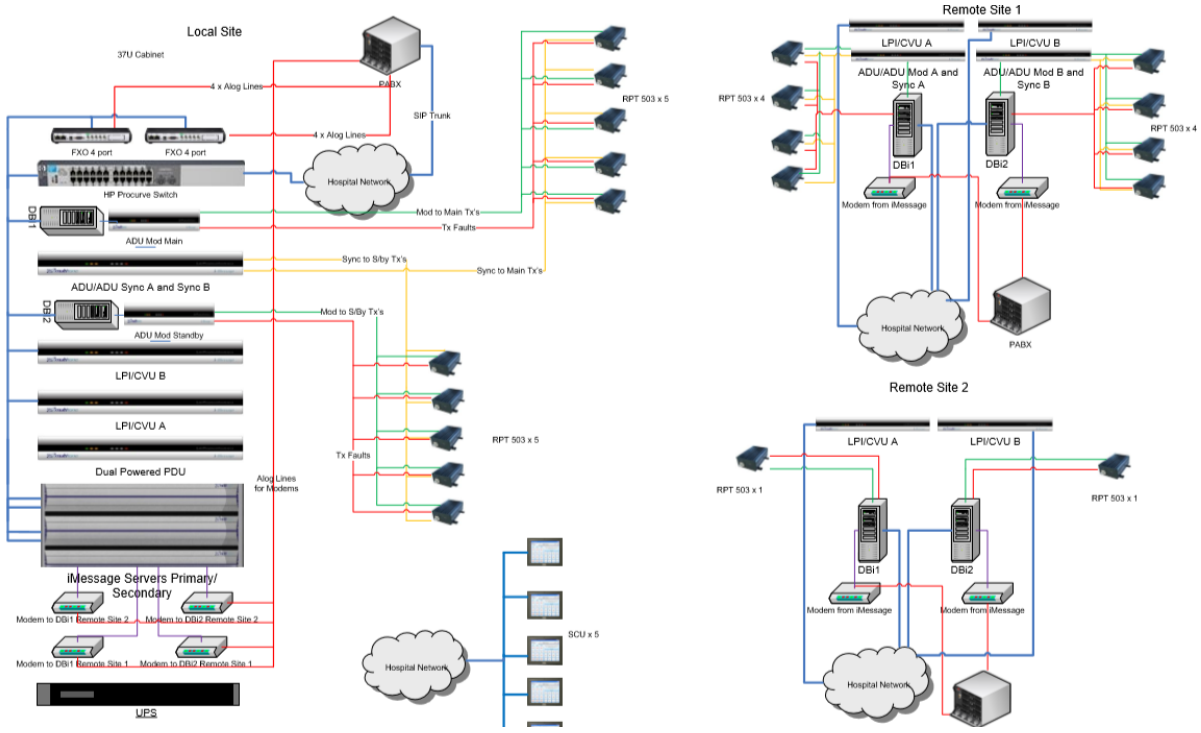
The section provides describes how the resilience of Multitone i-Message system operates with respect to a network environment and how the system overcomes a network outage by deploying numerous techniques utilised within the Multitone i-Message system.

6.6.1 Design Topology of the Multitone i-Message Platform

Wherever possible, the design of Multitone i-Message systems is to eliminate single points of failure, this means duplicating every aspect of the system topology including but not limited to the following items:

- Servers
- Network Switches
- Uplinks to Hospital Networks
- Transmitter networks
- Peripheral Equipment

In a perfect implementation, duplication of all Multitone i-Message hardware creates a fully resilient configuration. As per the schematic below the system is fully duplicated other than the network switch and the UPS. Adding an additional UPS and network switches would produce the most resilient system with no single point of failure.



6.6.2 Server Start-up, Failover & Recovery

The following table provides “estimates” for a variety of failure modes with respect to Multitone i-Message server start-up, failover and recovery:

1. How long does it take i-Message start-up, with windows already running?	Typically 45 seconds to 1 minute.		
2. How long does it take for an i-Message server failover from secondary to primary server?	Approximately 30 seconds, +/-10 seconds.		
3. How long does it take for Multitone i-Message to detect a network error so that a switchover takes place?	Estimate less than 60 seconds.		
4. What is the synchronisation time of secondary server database:	Zero (0) seconds, no impact on service.		
5. Multitone i-Message internal Private Branch Exchange (PBX) offline to recovery?	Typically up to 5 minutes +/- 1 minute 20 seconds, note i-Message makes various attempts in this time to attempt a fix and then restarts i-Message after 5 minutes).	5a. Does this affect other Multitone i-Message services during this period?	No, zero impact, it will not affect the rest of the system until it re-starts, which is approximately 30 seconds +/-10 seconds (See point 3).
		5b. Apart from the PBX problem, is the function of i-Message affected?	No phone access, no live speech, you can send text and canned messages plus voice from Multitone Appear and/or Multitone Messenger.
		5c. If the Multitone i-Message restarts after 5 minutes, this will result in a switch-over to the standby system?	Yes
6. On server changeover how long does it take to power up a server and then re-start Multitone i-Message:	This depends on the server; it is not possible to calculate accurate statistics. Typically, if the server is off the time to start and be ready for use is the server start-up time plus 1 minute for the i-Message application.		

6.6.3 Network Outage Failover

Multitone i-Message has built in methods for dealing with network outages. Firstly, it is worth pointing out that Multitone i-Message does not require a wider network to operate, the application is IP based, however, it only requires that the network ports on the server are ‘alive’ and connected to a switch that is powered on. As such, any network outage locally to the Multitone i-Message system servers should not affect running of the system at any point, assuming there are no ‘network storms’ within the V-LAN or SUBNET that the Multitone i-Message system resides.

To ensure that this does not occur, it is always wise to locate the Multitone i-Message system in its own subnet or V-LAN. By this the only way in which the Multitone i-Message servers would be compromised is not through a network outage but instead a power failure or switch failure. Both of these event types can be mitigated by ensuring the two (or more servers) used on a single site have resilient UPS power, or at the very least plugged into different spurs from a different supply.

Multitone i-Message can configured so that each server has its own switch that connects together by one or more CAT5/6 or fibre cable utilising RSTP within the supplied switches. For remote devices, such as System Control Units (SCU) or Dual Bearer Interfaces (DBI) we have the ability to reduce impact of any wider network outage. When using Telephony to place user and team calls there are also additional methods to bolster resilience.

For SCU’s these devices can only connect over IP only, so it is advised where they are connected across the core network that at least one unit is hardwired back to the local switch at the Multitone i-Message server location, this way at least one unit will stay-up in the event of a wider network fault. The design of the SCU’s is such that they are on a site local to the server. Therefore, there is no need for alternate bearers for this device.

For DBI’s, these devices run the transmitter network and often be situated remote from the sever site we have included an alternate bearer over PSTN to allow calls to continue across multiple sites where they have been cut off due to a wider area network issue. This back-up route kicks in automatically once the network fails, it then remains connected until the network has been restored and no traffic has been seen on the PSTN link for 3 minutes (this item is configurable). Multitone i-Message will use the IP bearers as a primary preference and PSTN as a secondary, so once the IP links have been re-established Multitone i-Message will no longer put calls through the PSTN link. When using DBI’s it is advantageous to implement multiple units per site along with multiple transmitter networks. This way Multitone i-Message can use the multiple units alternately and lock to a single unit in the event of a fault on another.

For telephony connections, it is always preferable to use SIP. SIP provides users with more functionality on the Multitone i-Message system such as using caller ID and SIP trunk monitoring. In the event of a network outage, which can compromise the SIP trunk, it is therefore advisable to implement analogue extensions or trunks interfacing with an FXO or FXS respectively. This allows for a fall back method for incoming telephony calls in the event of a wider network outage. The FXO and FXS units connect over IP on the local switch to the Multitone i-Message servers.

The Multitone i-Message system constantly monitors all peripherals and should one become unreachable over IP it will raise an alarm to this effect and establish a PSTN link to maintain service. The alarms warning that a device is unreachable over IP will continue until service restoration.

6.6.4 Keep Alive

The Multitone i-Message system runs a health check on all peripherals every minute and reports back the health state and any alarms can then be configured to go to Multitone engineers or onsite staff or both via email, pager, SMS (where available) and Multitone smart apps (where available). If a link fails in between this poll when Multitone i-Message attempts to send the message over IP it will immediately get a 'No Bearer' message and fall back to the secondary method and if configured tertiary and so on until it is able to successfully deliver the message.

6.6.5 Multitone i-Message - Database Synchronisation & Clusters

Multitone i-Message relies on a fully synchronised database to allow failover from one server to another to occur with no loss of call logs or data. Whilst two or more servers are online they also share the "message queue" meaning if one server were to suffer a power failure during a call the next server will pick-up the call and send it once it has taken over the cluster. In the unlikely event, that two server's loose connection both will assume the other has failed and run 'solo' until the restoration of the clustered. At that point, they will elect a new cluster master and slave topology and service will continue as expected.

Note: Section 6.4 applies to Multitone i-Message and IM-Lite D systems only, for Multitone IM-Lite systems; IM-Lite-A IM-Lite-B and IM-Lite-C do not support multiple servers and clustering capabilities, where this is required, a Multitone i-Message or IM-Lite-D system must be provided.

6.6 Multitone i-Message - Statement on the Use of External Penetration Testing

Multitone prioritises the security and integrity of our on=premises/cloud-based servers through a comprehensive, in-house approach, see below. Multitone does not use external penetration testers for the following reasons:

1. **Data security and confidentiality** - by keeping penetration testing internal, we maintain strict control over sensitive data, ensuring that it remains confidential and protected from potential exposure to third parties.

2. **Network familiarity** - **o**ur internal team possesses in-depth knowledge of our network architecture, applications, and security protocols. This expertise allows for more efficient and effective identification and remediation of vulnerabilities specific to our environment.

3. **Customised testing** - Internal testers can tailor their approaches to suit our unique infrastructure and operational requirements. This level of customisation ensures more relevant and thorough testing compared to generic external assessments.

4. **Rapid response and resolution** - with an in-house team, we can promptly address and mitigate any identified vulnerabilities, minimising potential risks and downtime. Our established processes ensure that issues are resolved swiftly and effectively.

5. **Cost efficiency** - utilising internal resources for penetration testing is more cost-effective, eliminating the need for external consultancy fees while leveraging our existing security team's capabilities.

6.6.1 What Penetration Testing Multitone do on the Servers / Application?

The Greenbone GSM One tool provides comprehensive port scanning capabilities for our cloud-hosted servers, operating within the same network to bypass external firewalls. This allows direct scanning of the server OS and applications to identify security vulnerabilities contained within. GSM One does not perform DDoS attacks or password attacks on our systems. It is designed solely to detect CVEs and other application-based security vulnerabilities. Issues identified during scheduled scans are addressed within two weeks, while zero-day.

6.6.2 What is the Greenbone Test Environment?

The Greenbone test environment is employed by Multitone to test Multitone i-Message vulnerability using Greenbone's security assessment tools, such as the Greenbone Vulnerability Manager (GVM) and OpenVAS. This environment typically includes various components like the scanner, manager, and user interfaces configured to scan and assess target systems for vulnerabilities. Components of the Greenbone test environment include:

1. Greenbone Vulnerability Manager (GVM) - manages scan tasks, schedules, and stores scan results.

2. OpenVAS (Open Vulnerability Assessment System) - performs the actual vulnerability scans.

3. Greenbone Security Assistant (GSA) - provides a web-based user interface for interacting with GVM.

4. Target Systems - virtual machines or isolated network segments designed for testing purposes.

5. Feeds (Greenbone Security Feed) - Databases of vulnerability tests used by OpenVAS for scanning.

6.6.3 Test Regime

The test regime involves systematic procedures to validate the functionality and reliability of the Greenbone tools, this typically includes:

1. Initial setup - installation and configuration of GVM, OpenVAS, and GSA.

2. Feed updates - ensuring the latest vulnerability feeds are downloaded and integrated.

3. Baseline scans - conducting initial scans on predefined targets to establish a baseline.

4. Test Scenarios:

    - Known vulnerabilities - scanning systems with known vulnerabilities to verify detection.

    - False Positives/Negatives - assessing the accuracy of scan results by checking for false positives and negatives.

    - Performance testing - measuring the performance of the tools under various loads and configurations.

    - Regression Testing - ensuring new updates do not introduce new issues.

6.6.4 Pass / Fail Criteria

The pass/fail criteria for the tests are determined by predefined benchmarks and objectives:

1. Detection Accuracy:
   - Pass: All known vulnerabilities are correctly identified; minimal false positives/negatives
   - Fail: Significant vulnerabilities are missed or high false positive/negative rate.

2. Performance Metrics:
   - Pass: Scans complete within acceptable time frames and resource usage is within limits
   - Fail: Scans are excessively slow or resource usage is unacceptable.

3. Stability and Reliability:
   - Pass: No crashes or significant errors during scans and management operations.
   - Fail: Frequent crashes or errors that impede normal operations.

4. Usability:
   - Pass: User interface is intuitive, and all major functions are easily accessible and operable
   - Fail: Interface issues that significantly hinder usability.

5. Compliance and Reporting:
   - Pass: Reports are comprehensive, accurate, and meet compliance standards
   - Fail: Reports are incomplete, inaccurate, or non-compliant.

Typical Workflow in a Greenbone test environment

1. Preparation:
   - Set up the Greenbone environment
   - Define test targets and scenarios
   - Update feeds.

2. Execution:
   - Conduct initial and subsequent scans
   - Monitor system performance and stability

3. Analysis:
   - Review scan results
   - Identify and document any issues or anomalies

4. Reporting:
   - Generate and review detailed reports
   - Compare results against pass/fail criteria

5. Iteration:
    - Address any detected issues
    - Repeat tests as necessary to verify fixes and improvements

6.6.5 Is this an Independent test or Standard?

Greenbone's testing environment includes a blend of independent internal testing processes and alignment with industry standards and best practices and Multitone have found no major issues with its performance.

6.6.6 How often is Testing Undertaken?

The test is run monthly on a schedule automatically and then reviewed by Multitone's staff and then our SQA team with Development work to add any required patches such as: Apache, openSSL, Java etc., as well as any Windows based patches and then test again.

6.6.7 Will Multitone provide the Report Results of a Successful Certified Release?

Multitone does not usually share the results of our vulnerability scans with external parties as they contain sensitive information etc.

6.7 Multitone i-Message - HTTPS Certificates & Self-signed Certificates

When using Multitone i-Message, or any application running with HTTPS and a self-signed certificate, the browser will display an error message upon accessing the website. This is normal. The error occurs because the certificate authority (CA) is not recognised nor can it be verified.

Understanding certificate authorities

All certificate authorities are registered in an online repository that browsers consult. If a website uses a Corticated Authority that is not listed, the browser flags it as an error. However, even in such cases, the transmitted data remains fully encrypted. For Multitone i-Message, Multitone ensures secure communication using **TLS 1.3** and **AES-256** encryption.

Certification authority certificates

The Multitone i-Message platform supports Certificate Authority certificates. As a result of restrictions imposed by certification authorities, Multitone has opted to use self-signed certificates. Nonetheless, if a customer requires an external certificate, this can be accommodated, the following conditions apply:

1. Fully Qualified Domain Name (FQDN) - A FQDN is required; standard IP addresses are not supported.

2. External Browser Port Accessibility - The browser port must be externally accessible to update the certificate, which must be renewed every 3 months.

Updating the Certificate

To update the certificate, the Multitone i-Message service must be stopped; this process should be planned alongside regular system maintenance. In addition customers providing their own certificates must supply:

- The certificate authority certificate
- The server.pem file
- The key.pem file

These files will be added to our configuration folder and referenced in the Apache configuration file. The customers will be responsible for updating their certificates upon expiry.

Important Notes

- Incorrect information in a genuine CA certificate will result in a warning.
- Despite warnings, all data remains fully encrypted at all times.

7. MULTIONE i-MESSAGE - CALL LOG, AUDIT & SYSTEM MONITORING

7.1 Call Log

The Multitone i-Message call log module operates as a separate ‘fat’ client on a separate PC; linked to the Multitone i-Message system for data input, but also operates independently of the system for analysis purposes, supporting the following facilities:

- Enables 100,000+ records storage, this should be regularly purged with data stored on a third party storage device, or retained in a flexible storage format, CD-ROM etc.
- Records can be extracted into HTML or Text (comma de-limited)
- Checks the Multitone i-Message internal call log to back-up only correct data
- Real time call logs
- Records include sender message, recipient messages, time-stamps with one-way voice (emergency calls, e.g. crash calls)
- Records all call verifications, e.g. call sent, automatic call acknowledgements and read receipts
- Instant operator and user call success or failure notification
- On logging of call failures will facilitate multiple re-sends
- User number, device number and RIC number used search
- Analysis tools – Time, sender, recipient, message or device type searches with pictorial histograms
- Export call log file

7.2 SNMP System Monitoring

Multitone i-Message supports the SNMP protocol; the system sends information to a SNMP trap location, whereby monitoring server/device poles the trap for system, fault and licence status information.

8. MULTITONE i-MESSAGE - SYSTEM HARDWARE

8.1 System Control Unit (SCU)

All interfaces to the Multitone i-Message system are web based; in order for the user interface to operate, java will be required on each PC/machine where speech access is required. All user interfaces are Username, Password and fully Access Right protected and will operate on a standard PC. The System Control Unit (SCU) provides an alternative PC/Web based touch-screen interface to the Multitone i-Message system. Specification is as follows:

Product	Intel NUC Kit with 13th Generation Intel Core Processors
Processor	Intel Core i3-1315U Processor (10M Cache, up to 4.50 GHz)
Operating Systems	Operating Systems Windows 10IoT Enterprise
CPU, max turbo frequency	4.50GHz
Max memory	64Gbyte
Memory type	DDR4-3200 1.2V SODIMMs
ECC memory supported	No
Internal drive form factor	M.2 SSD
M.2 Card Slot (storage)	22x80 NVMe (M); 22x42 SATA (8)
Graphic Output	2 x HDMI 2.1 TMDS Compatible, 2x DP 1.4a via Type C
Thunderbolt, C Ports	2 x Thunderbolt, C 4
USB configuration	Front: 2x USB 3.2 Rear: 2x USB 4 (type C), 1x USB 3.2, 1x USB 2.0
	Internal: 1x USB 3.2 on m.2 22x42 (pins), 2x USB 2.0 (headers)
Serial port (internal header)	No
Audio	Front panel: 3.5mm headphone/microphone jack
Integrated LAN	Intel Ethernet Controller i226-V
Wireless included	Intel Wi-Fi 6E AX211 (Gig+)
M.2 Card Slot (wireless)	22x30 (E)
Additional headers	Front panel (PWR, RST, 5V, 5Vsby, 3.3Vsby)
	Internal 2x2 power connector
PCI Express Revision	Gen 4 (m.2 22x80 slot); Gen 3 (otherwise)
PCI Express Configurations	PCIe x4 Gen 4: M.2 22x80 (key M) PCIe x1 Gen 3: M.2 22x42 (key B) PCIe x1: M.2 22x30 (key E)
DC Input Voltage Supported	12-20 DC
Chassis Dimensions	117 x 112 x 37 [mm] (L x W x H)

Board Form Facto	UCFF (4" x 4")

Display size	39.62cm / 15.6“ Diagonal
Panel type	TFT (LED Backlight)
Aspect ratio	16:09
Resolution (H x V)	1366 x 768
Panel brightness	220cd/m² (Typical)
Contrast (Typ.)	500:1 (Typical)
Contrast (Active)	40.000.000:1 (Active)
Viewing angle L/R; U/D	110° H / 85° V (CR >5) – 90° H / 65° V (CR >10)
Response time	12 m/sec (Type)
Pixel pitch	0.252 (H) x 0.252 (V) mm
Touch type	Projected Capacitive Type - 10 Point Touch
Display colours	262K Colours
Horizontal frequency	30 ~ 61 kHz
Vertical frequency	56 ~ 75 Hz
Max display frequency	1366 x 768 @ 60Hz
Inputs	Input 1: D-Sub (VGA), Input 2: HDMI, Input 3: USB (Touch function)
Built-in speakers	Yes 1W x 2; Earphone (Audio Out)
Power consumption	On: 10W; Stand-by: ≤0.5W; Off: ≤0.5W
AC power	External Power Supply
	Input: AC 100 ~ 240 Volt; 50 ~ 60 Hz
	Output: 12V – 3A
Product dimensions	37.2 x 36.8 x 248.6 mm (W x D x H).
Net/Gross weight	1.32Kg / 2.36 Kg
Bezel & colour	Plan Bezel Arm/ Base: Texture Rear Cover – Texture
VESA mounting	75 x 75 mm
Monitor stand	Smart Adjustable Stand (“book“ type)
Tilt/Kensington lock	15° ~ 50° / Yes
Display protection	Thickness 0.83 mm
Hardness/transmittance	≥7H Toughened hard panel surface / ≥90%
Controls	Menu Brightness (+) Volume (-) Input/Enter Power
Colour	Warm, Natural, Cool, User Mode
Preset mode	PC, Movie, Game Modes
On-screen display	15 OSD Languages

- 23in (H) x 4.5in (W) x 4.5in (D)

• 18” goose neck with sturdy base
• 10’ shielded cord with Plug–n-Play USB connector
• Illuminated on/off switch
• Unidirectional noise cancelling
• Colour: black

8.2 Multitone i-Message - Servers & Specification

Multitone i-Message supports two server options; both options support Windows Server 2012, 2012R2, 2016, 2019 and Win IoT using the Microsoft Telco licence, Client Access Licence (CAL). Server options are:

8.2.1 IM-SV1- Dell R260 PowerEdge Server (Non RAID)

Overview

Compact 1U server for embedded/server appliance applications, pre-installed with Windows Server IoT 2022 and Multitone i-Message 1.8.1 software or above.

Technical Specification

- **Processor**: Intel Xeon E-2456 3.3 GHz, 6C/12T, 18 MB Cache, Turbo, HT, DDR5
- **Memory**: 16 GB UDIMM, 5600 MT/s ECC
- **Storage**: 960 GB SSD SATA Read Intensive, Hot-plug, 2.5″ (no RAID)
- **Expansion**: PERC H755 Adapter, Low Profile
- **Networking**: Broadcom 5720 Dual Port 1 Gb On-Board LOM
- **Chassis & Form Factor**
  - 2.5″ chassis with hot-plug drives and cabled PSU (SAS/SATA)
  - Single non-redundant 450 W Platinum PSU
  - 1U/2U static rails for 2-post and 4-post racks
  - Dimensions: H 42.8 mm × W 482 mm × D 585-598.6 mm
- **Management & Security**
  - iDRAC9 Basic 16G
  - TPM 2.0
  - iDRAC Group Manager Disabled
  - Secured Component Verification
- **Power & Cooling**
  - Power-saving BIOS
  - No additional fans
  - No Energy Star
- **Software & OS**
  - Windows Server IoT 2022 (16 Core, ESD)
  - Multitone i-Message 1.8.1 or above pre-installed
- **Warranty & Support**
  - Basic Next Business Day 12 Months
  - ProSupport optional with 12-month initial + 24-month extension

8.2.2 IM-SV1-RAID - Dell R260 PowerEdge Server (RAID 1)

Overview
Same as above but configured for RAID 1, providing mirrored storage for high availability.

Technical Specification

- **Processor**: Intel Xeon E-2434 3.4 GHz, 4C/8T, 12 MB Cache, Turbo, HT, DDR5
- **Memory**: 16 GB UDIMM, 5600 MT/s ECC
- **Storage**: 2 × 960 GB SSD SATA Read Intensive in RAID 1
- **Expansion**: PERC H755 Adapter, Low Profile
- **Networking**: Broadcom 5720 Dual Port 1 Gb On-Board LOM
- **Chassis & Form Factor**
  - 2.5″ chassis with hot-plug drives and cabled PSU (SAS/SATA)
  - Single non-redundant 450 W Platinum PSU
  - 1U/2U static rails for 2-post and 4-post racks
- **Management & Security**
  - iDRAC9 Basic 16G
  - TPM 2.0
  - iDRAC Service Module not installed
  - iDRAC Group Manager Disabled
  - Secured Component Verification
- **Power & Cooling**
  - Power-saving BIOS
  - No additional fans
- **Software & OS**
  - Windows Server IoT 2022 (16 Core, ESD)
  - Multitone i-Message 1.8.1 or above
- **Warranty & Support**
  - Basic Next Business Day 12 Months
  - ProSupport optional with 12-month initial + 24-month extension

8.2.3 IM-SV3 - Dell R360 PowerEdge Server

Overview
Larger 2.5″ chassis server, supports up to 8 hot-plug drives. Pre-installed with **Windows Server IoT 2022** and Multitone i-Message.

Technical Specification

- **Processor**: Intel Xeon E-2456 3.3 GHz, 6C/12T, 18 MB Cache, Turbo, HT, DDR5
- **Memory**: 32 GB UDIMM, 5600 MT/s ECC
- **Storage**: 480 GB SSD SATA Read Intensive, Hot-plug, 2.5″
- **Expansion**: Front PERC H755 SAS controller
- **Networking**: Broadcom 5720 Dual Port 1 Gb On-Board LOM
- **Chassis & Form Factor**

- 2.5″ chassis with up to 8 hot-plug drives
- Dual redundant hot-plug PSU (1+1)
- Riser Confine 2, Butterfly Gen4 Riser (x8/x8)
- ReadyRails static rails for 2/4-post racks

- **Management & Security**
  - iDRAC9 Basic 16G
  - TPM 2.0
  - iDRAC Service Module not installed
  - iDRAC Group Manager Disabled
- **Power & Cooling**
  - Standard fans
  - Power-saving BIOS
- **Software & OS**
  - Windows Server IoT 2022 (16 Core, ESD)
  - Multitone i-Message 1.8.1 or above
- **Warranty & Support**
  - Basic Next Business Day 12 Months
  - Optional 30-month extension
  - OEM Enterprise Program support
- **Dimensions**
  - Height: 42.8 mm (1.69 inches)
  - Width: 482 mm (18.98 inches)
  - Depth: 585.3 mm (23.04 inches) without bezel
  - Depth: 598.94 mm (23.58 inches) with bezel

8.2.4 IM-SV1-UK i-Message Server Upgrade Kit

- 1 x Kingston Dell KTD-PE426E/16G 16GB DDR4 2666MT/s ECC Un-buffered Memory RAM DIMM
- 1 x Storage Capacity 960GB, 12Gb/s SAS SSD Drive 1.00 EA
- 1 x 3.5 inch Hard Drive Caddy Tray Compatible for Dell PowerEdge Servers with 2.5 inch HDD/SSD Adapter

8.2.5 IM-SV3-UK i-Message Server Upgrade Kit

- 1 x Kingston Dell KTD-PE426E/16G 16GB DDR4 2666MT/s ECC Un-buffered Memory RAM DIMM
- 3 x Storage Capacity 960GB, 6Gb/s SAS SSD Drive 1.00 EA
- 3 x 3.5 inch Hard Drive Caddy Tray Compatible for Dell PowerEdge Servers with 2.5 inch HDD/SSD Adapter

8.3 Multitone IM-Lite - Hardware Specification

- Multitone IM-Lite (IM-Lite-A, B, C & D)
  - Intel® Core™ i3 8109U Processor (3.6 GHz, Dual Core, 4 MB Cache, 28W TDP

- Two DDR4 2400 SO-DIMM sockets (up to 32 GB, 2400 MHz), 1.2V
- 4x USB 3.1 ports (2x back panel ports and 2x front ports including one charging port) and 2x additional USB 2.0 ports via internal header
- Power - 19V, 90W power brick

- Peripheral connectivity:
  - 1 x Integrated Intel 10/100/1000 Network Connection
  - 1 x Socket RJ45 x RJ45 Panel Mount (Telephone Interface Only)
  - Up to 3 PBA UPA Transmitter Interfaces
  - Up to 3 UPI Direct Line Interfaces (DLC) supporting up 48 closing contacts
  - Up to 3 RS232 interfaces

- Dimensions:
  - Desk mount option - 355mm (Width) x 202mm (Depth) x 64mm (Height)
  - Rack facia option (2U) - 483mm (Width) x 88mm (Depth) x 50mm (Height)

- Power supply options:
  - Mains input 120V/240V
  - DC Power 19V, 90W
  - Power Cord Options - Types B (North America), E (European Union), and G (United Kingdom)

- Temperature performance:
  - 0° C to +40°C (Operating)
  - -20° C to +60°C (Storage)

- Environmental compliance:
  - Europe RoHS (Directive 2011/65/EU)

9. MULTITONE I-MESSAGE - PERIPHERAL HARDWARE SUPPORT

This section provides an overview of Multitone i-Message peripheral hardware interfaces:

- Multitone i-Message Digital Private Mobile Radio (DPMR) Support
- Dual Bearer Interface
- Multitone Integrator
- Multitone IM-Lite-DLC Interface

9.1. Multitone i-Message - Digital Private Mobile Radio (DPMR) support

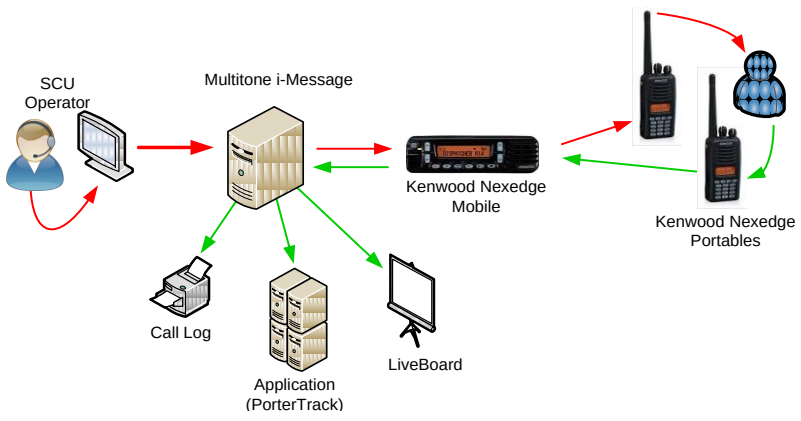
This section provides overview of the Digital Private Mobile Radio (DPMR) interfaces supported by the Multitone i-Message system, these include:

- Kenwood Nexedge supporting their Digital Mobile System (DMS) protocol
- Sepura Tetra interface supporting the Tetra SDS Protocol, and
- Motorola MotoTrbo supporting SMTP (Email) protocol

9.1.1 Kenwood Nexedge - system overview

Multitone i-Message interfaces to Kenwood Nexedge through their Digital Mobile System (DMS) protocol, providing a text messaging capability. This enables Multitone i-Message via the System Control Unit or Multitone SMART Apps to send text messages to a Kenwood Nexedge mobile and/or hand portable device. Please note that due to system configuration, you can only send text - speech support is not currently available.

The Kenwood Nexedge portable user can acknowledge a message. However, due to addressing issues the originating device (Multitone SMART Apps) cannot receive a reply. Nonetheless, from the schematic below it can be seen that Multitone i-Message will log these receipts and where configured the response is posted via LiveBoard. If the receipt relates to a third-party application, i.e. PorterTrack, Multitone i-Message pushes data back to the PorterTrack server.



To simplify the acknowledgement mechanism, Multitone recommends that Kenwood Nexedge portable devices is set-up with pre-configured response messages, such as: “Accept”, “Started” or “Completed” or text message relevant to the application in hand.

***Note**: PorterTrack is an application that allows the remote management of hospital porters with the ability for head porter to allocate jobs to porters whilst on the move.*

To interface the Kenwood Nexedge DPMR system to Multitone i-Message you will need to select the **Kenwood Digital Interface**, part number: **IM-L4-13**, from configurator, this includes a 25-way D-Type cable. A LAN Peripheral Interface (LPI) is also required this provides the physical interface between the two systems. For Kenwood Nexedge equipment, the following is required:

Digital & FM Mobile Radios:

- Kenwood NEXEDGE NX700/NX800 VHF/UHF Digital and FM Mobile Radios
- Kenwood NEXEDGE NX720/NX820 VHF/UHF Digital and FM Mobile Radios

Digital & analogue portable radio:

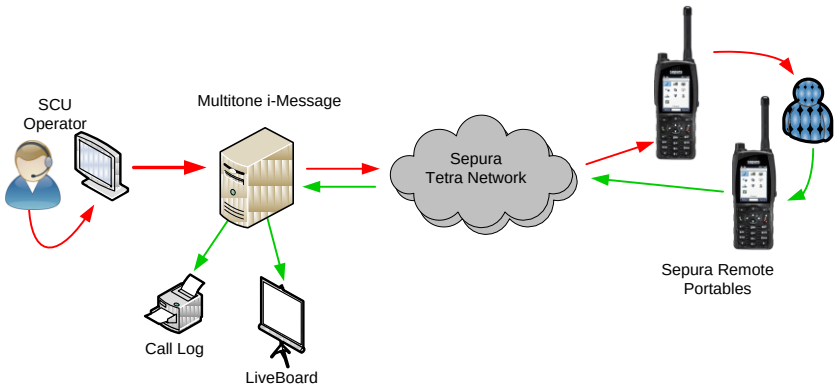
- NX-210 NEXEDGE VHF Digital/Analogue Hand Portable Radio
- NX-220E/320E NEXEDGE VHF/UHF Digital and FM Hand Portable Radios
- NX-200G/300G NEXEDGE VHF/UHF Digital and Analogue Hand Portable Radio

***Note**: Must support NX subscriber unit PC Serial Interface compatible software application, e.g. KENWOOD AVL and Dispatch Messaging software.*

9.1.2 Sepura Tetra interface - System Overview

The Tetra Short Data Services (SDS) protocol allows Multitone i-Message to interface to an external Tetra network. Tetra SDS is a bi-directional text messaging protocol (non-speech) and is similar to SMS, supporting message lengths of up to 160 characters.

The protocol allows a remote Tetra device or hand portable to receive, acknowledge and respond to a message either from another remote Tetra device or in Multitone's case via Multitone i-Message. In the Tetra world, this is the Central Message Dispatch System. Multitone i-Message allows an SCU operator or Multitone SMART Apps user to send messages to a Tetra remote device; however, the acknowledgement can only be set back to Multitone i-Message, not the originating device. See diagram below:



On receipt of a call, Multitone i-Message will log these responses, in addition where configured use of a LiveBoard allows the display of available remote device Sepura users with current and previous message responses.

The Tetra SDS protocol can support a range of Messaging, GPS Location and Data applications. With respect to Multitone's implementation, this is limited to text messaging only, i.e. that is the ability to send or broadcast a message from Multitone i-Message to a remote Tetra device and receive a response.

The remote device can send “text” or “status” messages. A status messages are pre-formatted, sent as a numeric code, for example 01 = “Accept”, 02 = “Started”, 03 = “Completed”. The Tetra SDS protocol will automatically convert these status messages into text, enabling i-Message to forward the message back to the originating device, e.g. Multitone SMART Apps.

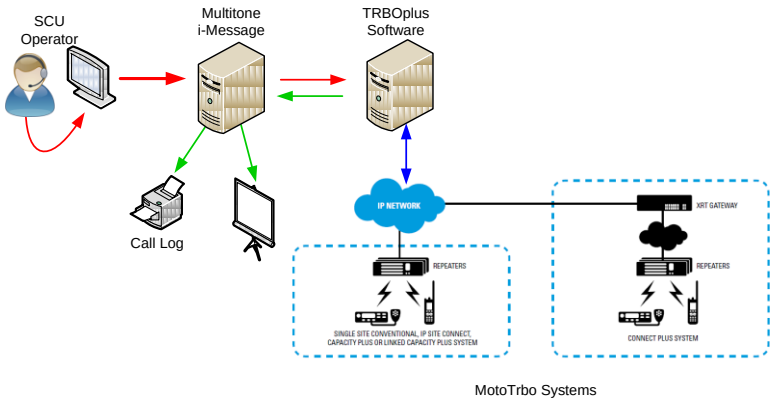
***Note**: The Tetra SDS Protocol has currently only been tested with Sepura Tetra systems. This is not to say that it will not work with other tetra systems, however, testing will be required to ensure that the protocol operates smoothly prior to sale.*

You can order the Tetra Sepura Messaging Agent using part number: **IM-L4-25**, as this is a TCP/IP interface no additional hardware other than standard cabling is required.

9.1.3 Motorola Mototrbo (SMTP Gateway) - System Overview

Using Neocom’ s TRBOnet Plus Control Room Solution software, supporting SMTP, provides an email gateway by which Multitone i-Message can send messages to Motorola MotoTrbo mobile end-point devices. As an authorised Motorola development partner, the Neocom application is a Motorola tested and approved solution, by adopting this gateway helps to negate the issue of having to implement Motorola’s complex messaging protocol into the Multitone i-Message system.

Referring the schematic below, it is now possible to send text or alarm messages from Multitone SMART Apps or the System Control Unit (SCU) via Multitone i-Message to Motorola MotoTrbo mobile and/or hand portable devices.



Please note the following operational conditions:

- Implementation is “receive only” automated message acknowledgement is not supported, however, hand portable users can respond to the email, by sending a reply, e.g. “message received”, this is used by Multitone i-Message as a “read receipt” and logs this information in the call log and if required directs it to the relevant live board.

- You cannot forward a message back to the originating device, e.g. Multitone SMART Apps, as you are sending an email response back to the Multitone i-Message system; Multitone i-Message cannot map this email address back to the originating user number.

- Finally, Motorola also support two further products **RDAC** (Repeater Diagnostics and Control) software and **Motorola Connect Plus**. These products also support an SMTP gateway, however, this is a single-way implementation, allowing "broadcast only" of an alarm messages via SMTP (email) to multiple MotoTrbo mobile radios and hand portables etc., there is no capability to text back message receipts.

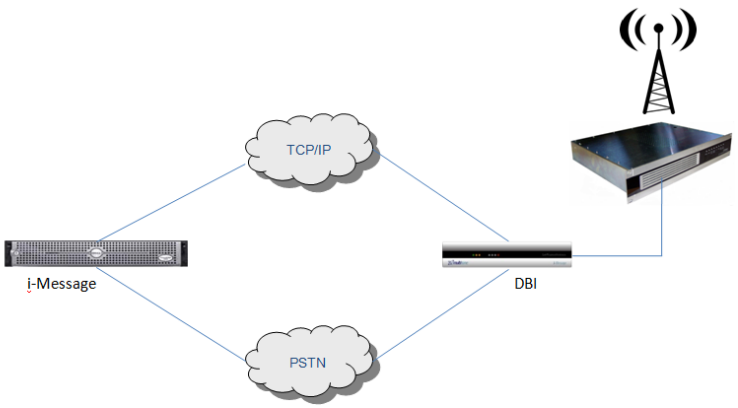
To support this option from Multitone i-Message configurator, please select the part number: **IM-L7-02** Email (SMPT) Gateway. This is a TCP/IP interface no additional hardware other than standard cabling is required.

9.2 Dual Bearer Interface (IM-DBID, IM-DBIR, IM-DBI2R)

The Dual Bearer Interface (DBI) is not a direct replacement for the LAN Peripheral Interface (LPI). The DBI supports a multi-bearer link to a remote transmitter or transmitters via a TCP/IP and/or a PSTN with the ability to support audio for speech applications, see diagram below. There are two versions of the Dual Bearer Interface:

- IM-DBI2R - 2 x Dual Bearer Interface (19" Rack/Tray Mount)
- IM-DBIR - 1 x Dual Bearer Interface (19" Rack/Tray Mount)
- IM-DBID - Dual Bearer Interface (Desk Mount)
- 2314-0044 - PSTN 56K V.92 Modem for Dual Bearer Interfaces (DBI)

In contrast, the LAN Peripheral interface only supports a single TCP/IP interface into a transmitter or transmitter network, therefore, provides only a single level of redundancy. Use of additional LPI's is can be deployed, however, they are reliant on the IP network, therefore, deemed a single point-of-failure.



The DBI runs on Linux, supporting the Multitone Communications Software (MCS) and includes a single USB peripheral with Audio interface (UPA); this enables use of this product for the following applications:

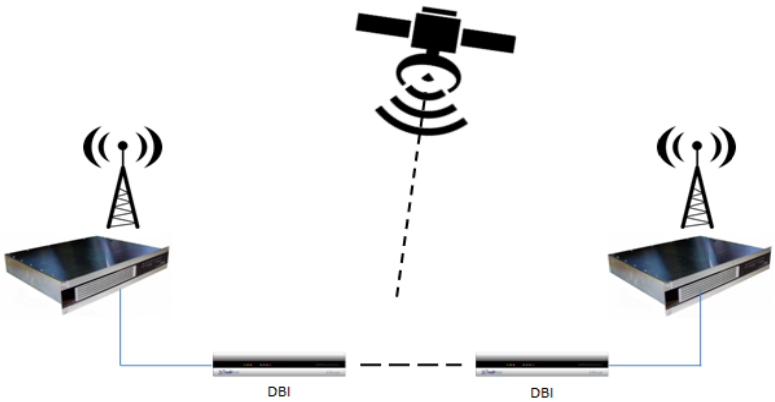
9.2.1 Dual Bearer Interface - Transmitter Interface

- Drives up to two local paging transmitters with alarms
- Supports: Multitone Mk7, Multitone Mk6 and POCSAG protocols
- Drives remote transmitters directly or via an Audio Distribution Unit (ADU), please note this uses a different connector and pin-out from the LAN Peripheral Interface (LPI)
- Drives remote transmitters via and Intelligent Transmitter Interface (ITI) with alarm monitoring, this can be directly or via an Audi Distribution Unit, please note this uses a different connector and pin-out from the LPI.
- Provide GPS synchronised speech paging using local or remote transmitters. Please note that the LPI could only do non-speech GPS synchronised paging using a local transmitter without off-air verification, and uses different connections

9.2.2 Dual Bearer Interface - GPS synchronisation

Provides a GPS simulator to synchronise multiple DBIs and/or UPA's for resilient paging applications, GPS synchronisation requires the following products:

- P1100-GP – High Stability Reference Unit (GPS)
- P1100-HS – High Stability Reference Unit (High Stability Oscillator)



9.2.3 Public Address (PA) Sound Systems

The Dual Bearer Interface can be configured to provides a controlled level audio output for use with a Sound Agent for Public Address applications

9.2.4 Dual Bearer Interface & Direct Line Contact (DLC) support

Supports up to 16 direct line closing contacts

***Note**: Engineers please note that the UPA is pin compatible with UPI and LPI, though there are some output level capability differences with rarely used channels (OP4 to OP7). If 16 channels of input and 16 channels of output are required, or if 16 high voltage outputs are required, the PIB2 is a more suitable interface.*

9.2.5 RS232 & RS485 support

- The Dual Bearer Interface does not support RS232 or RS485. If RS232 protocol support (TAP, ESPA 4.4.4. or MEP) is required, order the Multitone Integrator (IM-INT-D, IM-INT-R, IM-INT2-R).

- If RS485 is required for Absence & Charging, a LAN Peripheral Interface will be required.

9.2.6 Dual Bearer Interface - Product Operation

Typically, a DBI connects to the same network to which the Multitone i-Message server resides. The DBI then connects to only one transmitter at any given time via the UPA port using a 25-way D-type cable.

The internal 56k dial-up modem in each DBI typically connects to a telephone PBX or connected directly to the Multitone i-Message server providing there is another 56k dial-up modem connected to the Multitone i-Message server. If the Multitone i-Message system fails to send a call via the TCP/IP link, it will automatically switch and retry the call over the telephone line (the secondary bearer).

***Note**: When ordering a DBI and PSTN is required an additional 56k dial-up modem will be required, this interfaces to the Multitone i-Message system.*

9.3 Multitone Integrator (IM-INT-D, IM-INT-R, IM-INT2-R)

Multitone Integrator is a single point alarm and messaging server designed to integrate with wide range of alarm and messaging solutions, delivering urgent and time critical messages to a wide range of mobile devices supporting:

- SMS
- WiFi
- DECT
- Email
- Paging

Multitone Integrator captured, processed and sends key messages including alarms are to the right user or teams. Should no response to an alarm be received, the Multitone Integrator incorporates an automatic alarm escalation capability enabling it to send messages to other users or teams. Multitone Integrator provides a full range of messaging capabilities over a host of different interfaces and protocols. Three product options are now available:

- Single Multitone Integrator, Desk Mount (Part Number: IM-INT-D)
- Single Multitone Integrator, 19” Rack Mount (Part Number: IM-INT-R)
- Dual Multitone Integrators, 19” Rack Mount (Part Number: IM-INT2-R)

9.3.1 Technical Specification

Computer Processing Unit

Broadcom BCM2837B0, Core 4x Cortex-A53 running at 1.4GHz:

- 1GB RAM
- 2 x RS232 ports
- 1 x Universal Peripheral Interface with Audio (UPA)
- 1 x 10/100 Ethernet Port (RJ45)

Product Dimensions

Multitone Integrator (**IM-INT-D**)
Metric: 220mm (Length) x125mm (Depth) x 40mm (Height)
Imperial: 8.7” x 5.0” x 1.6”
Weight: 817 grams

Multitone Integrator (**IM-INT-R**)
Metric: 424mm (Length) x 125mm (Depth) x 40mm (Height)
Imperial: 16.7” x 5.0” x 1.6”
Weight: 1,643 grams

Multitone Integrator (**IM-INT2-R**)
Metric: 424mm (Length) x 125mm (Depth) x 40mm (Height)
Imperial: 16.7” x 5.0” x 1.6”
Weight: 1,824 grams

Power supply unit
5V, 2.5A (2500mA) micro USB power supply unit

Operating and storage temperature
Operating: 0˚ C to 70˚ C
Storage: -40˚ C to 85˚ C

Environment Compliance
EN55032 (class A), EN55024, EN60950

Protocol Support:

• SNPP output protocol • TAP RS232 protocol • MEP RS232 protocol • ESPA 4.4.4 RS232 protocol • MSP RS232 Scope protocol • TAP protocol (BT character set) • SMTP client (output) protocol • ProCad status protocol • Ekotek protocol (TAP) • SMPP protocol (GPRS, 3G, 4G) • Spectralink UC protocol • NEC DECT DMLS protocol • Spectralink XML-RPC protocol • PCR (Anoto) protocol • TAPI (Samsung) protocol • SDS Protocol (Tetra) • TNPP output protocol • RTX protocol • Halcyon (PhotonStar) protocol • MotoTurbo protocol • MSP (Scope RS232) paging protocol • Multitone Internet Protocol (MIP) • Prism IPX Protocol	• Codem2/Nursecall • Static Systems 925 • Premier 48 • Minerva 16/80 • Morley-IAS ZX • Tyco MX/ZX • Chubb 380A • Scope ConneXions II • Guardsman printer • Wipath PDR2000 • Controlmaster 600 • Clover • Satchwell BMS • Protec • Gent Binary • Gent Printer • Ziton ZCP2 • Universal Printer • Static Systems • Codemlon • UPI/LPI Protocol • Capture protocol • Static Systems IP Fusion • Honeywell Notifier ID3000 • OPC-DA Gateway Protocol • CEI-XML (Spacelabs) Protocol

9.3.2 Product Features

- Middleware platform with paging encoder: Yes
- RS232 2
- 25-Way (UPA/UPI) 1
- Ethernet RJ45f 10/100Mbps 1
- Multitone Mk6, Mk7 & POCSAG Yes
- Internal transmitter None
  (External connection required)

- Total recipients - Users: 999
- Total recipients - Teams: 999
- Basic administrator screen: Yes
- Simple messaging web based interface: Yes
- Escalation agent (pre-formatted messages) Yes (10 levels of escalation)
- Pre-formatted speech messages Yes (100)
- Protocol scripting Yes (1GB memory)
- 16 Configurable Closing Contacts: Yes
- Fully Qualified Domain Name Support (FQDN): Yes
- Input agents (any combination of below): 4 (In/Out)

9.4 Multitone i-Message - DLC Interface (IM-LITE-DLC)

The Multitone IM-Lite-DLC interface is a cost-effective system for supporting Direct Line Inputs (DLC), or closing contacts. Designed to operate with Multitone i-Message, Multitone IM-Lite and Multitone Integrator systems using a network switch, it is possible to stack interfaces, enabling multiple input support, for example for an 8-port switch, 300+ contacts are available. Two product options are:

- IM-Lite-DLC-48 - Supporting up to 48closing contacts (In/Out) with Desk/Wall or Rack mounting options
- IM-Lite-DLC-96 - Supporting up to 96-closing contacts (In/Out),) with Desk/Wall or Rack mounting options

9.4.1 Technical Specification

- Key dimensions:
  - Desk-mount option - 355mm (Width) x 202mm (Depth) x 64mm (Height)
  - Rack-mount option (2U) - 483mm (Width) x 88mm (Depth) x 50mm (Height)
  - Weight - 1.2kg

- Operates with the following Multitone integrated communications systems:
  - Multitone i-Message
  - Multitone IM-Lite
  - Multitone Integrator
- Full redundancy support

  With Multitone i-Message, using dual IM-Lite DLC interfaces it is possible to duplicate contacts, whereby each IM-Lite-DLC interface connects to a separate network switch, with each switch further connected to a separate Multitone i-Message server, therefore, if one server fails, the secondary server takes over operation of the IM-Lite-DLC interface.

***Note**: This configuration only operates with Multitone i-Message systems; this feature is not available on Multitone IM-Lite or the Multitone Integrator.*

- Desk, Rack or Wall mount options:
  - Desk/Wall mount (VESA mount)
  - Power options are UK, EU and NA

- Power supply options:
  - Mains input 120V/240V
  - DC Power 5V, 5A
  - Power Cord Options - United Kingdom, European Union and North America

- Temperature performance:
  - 0° C to +50°C (Operating)
  - -20° C to +70°C (Storage)

- Environmental compliance:
  - Europe RoHS (Directive 2011/65/EU)

10. MULTITONE SMART APPS

10.1 Multitone Smartapp Options

There are now two versions of the Multitone SMART app, these are:

- Multitone Appear:

  - Messaging, speech messaging, contacts, contact status

  - SIP Client - Voice over IP (VoIP) – may be set-up to be called as either a direct extension number (direct extension to extension calling) or with a hidden extension number, so that the SIP client may only be called as a User on the Multitone i-Message system.

  - Soft Buttons - customisable on-screen soft buttons for pre-formatted applications

- Multitone Appear Lite - this is a cut down version of Multitone SMART Apps, receive message only with call acknowledgement for simple fast messaging.

- Multitone Appear Crew - this is a cut down version of Multitone SMART Apps, receive message only with call acknowledgement with simple “canned” message response functionality.

- Multitone Messenger - Multitone Messenger is delivered via the Multitone i-Message system either on-premises, cloud or hybrid, supporting the following features:

  - One-to-one messaging
  - Chat messaging
  - User status indication and notification
  - Emergency messaging
  - Major Incident Management messaging
  - Secure, AES 256 bit encrypted, two-factor, non-password, session security
  - Full integrates with Multitone i-Message for time critical, emergency messaging

10.2 Multitone Smartapps, Key Features

Multitone SMART apps integrate with the Multitone i-Message system enabling real-time messaging from the Multitone i-Message system ‘to’ and ‘between’ SMART devices:

- Receive messages from the Multitone i-Message system or from any SMART running this application

- Processing speed - The Multitone i-Message Event Action Manager (EAM) enables Multitone i-Message to process Multitone SMART app messages at estimated speed of one call per 240 milliseconds. Likewise, a response received from the app is estimated all 1 response every 1.2 seconds, for 500 (all) devices this is approximately 10 minutes

- Multiple device messaging - send messages to other devices via Multitone i-Message, such as a pager, mobile phone, DECT or WiFi handset via the Multitone i-Message system

- Call acknowledgement - all messages sent are acknowledged with an automatic received receipt and a manual acknowledged read receipt with message and time stamp

- Instant presence notification - the ability to select and indicate personal status, e.g. Presence, Busy and Absence and so forth

- Team calling - the ability to initiate team calls using the Multitone SMART app to call other devices supported by the Multitone i-Message system, e.g. Pagers

- User and team directory - the ability to create a local directory of users and teams or to interrogate the Multitone i-Message database to search for a non-resident user/team and send a message

- On receipt of a message the SMART application is designed to automatically acknowledge a message, in addition the SMART device user may acknowledge a message with an appropriate response (data, speech or both)

- The app operates over both private WiFi and public mobile networks, such as GSM, GPRS, Edge, 3G and 4G etc.

  ***Note**: Crucially, the Multitone SMART app will operate on Home WiFi, 3rd Party WiFi and Hot Spot WiFi networks.*

- All transactions between the Multitone i-Message system and Multitone Appear, Appear Lite, Appear Crew and Appear WorkFlow is delivered using a secure monitored connection, which is encrypted at AES 128 with data stored, fully encrypted on the device. On Multitone Messenger encryption is AES 256.

- Contact access control - the ability to restrict access rights to specific user contacts, e.g. the CEO

- Bring Your Own Device (BYOD) support - when the app is operational, all transactions between the Multitone i-Message system and the app are monitored and logged, therefore, an independent SMART device will have system transparency

- Multitone Electronics Bring Your Own Device (BOYD) policy - adoption of BOYD is dependent on internal 3G/4G and site WiFi coverage. If 3G/4G coverage is poor, then the ability to use local WiFi will be required, in Multitone's experience low cost Android smart phones will not support WiFi base station hoping (port traversal), therefore, where messaging apps are supported, delayed messages receipt and response may result.

  Apple iOS devices are acceptable and will support full WiFi traversal; however, it is advised that iOS 14.8.1 should be the lowest operating system version supported to ensure apps are up to date and support the latest features.

  Android devices, must support Android 9, 10, 11 or 12 and **MUST** be of "enterprise grade", such as: top end Samsung Galaxy, Samsung X-Cover 4 or above, Spectralink Versity, Zebra Mobile Computers, Pixel 3A etc., these will support WiFi port traversal should there be insufficient internal 3G/4G coverage.

- Multi-media support with voice and media rich content and messaging:

  - Free format text messaging
  - Pre-stored messages for fast selection and message send
  - One-way speech (up to 30 seconds from Multitone i-Message only, no actual restriction on apps where speech is supported)
  - Images (photographs)
  - Video (up to 10 seconds per clip)

- FIHR attachments

- Battery life - the Multitone SMART Apps app can operate in variety of different modes; these are user selected or pre-set within the system. For Multitone Appear this include full app client/server operation to cloud only push notification, this provides the opportunity to vary battery usage dependent on circumstances such as being on-site within a good WiFi coverage to driving with poor mobile network and little WiFi coverage.

  Typically, for Android the impact of battery life reduces by between 5 and 6 percent in terms of average phone use in any 24-hour period. Likewise, for an Apple iOS device, battery life reduces by 9 to 10 percent in terms of average phone use in any 24-hour period.

  ***Note**: SMART device battery life is dependent on multiple variables, i.e. how many apps are open on the device or how busy the device is at any point-in-time, i.e. sending and receiving calls, internet and email activity etc.*

10.3 Multitone Smartapps, Device Security

From the viewpoint of system and device security, the Multitone i-Message designed to support the following parameters:

1. All data stored, transmitted and managed within the Multitone i-Message cloud and smart device is AES 256 encrypted

2. For Multitone Appear, Appear Lite and Appear crew the app is login and password protected with auto log-off challenged every 24 hours. This can be linked to Active Directory and utilise current logins and passwords.

3. Multitone Messenger password-less application - as a "password less" application Multitone Messenger relies on the Multitone i-Message system administrator inviting users to adopt the app - as with other apps a user is not required to authenticate with a password would normally be required. This not only removes the need for passwords and associated management; it eliminates this security venerability. Having received an invitation (email or text message) a user can verify their account via email link or QR code, a user is then sent a two step 5 digit verification code to access the application.

4. Multitone messenger – non-invited user and hacker protection - if a non invited user or hacker attempts to download the app and entered their email address, user name or phone number, they will be able to use the app, but this is limited to sending messages to themselves with no further access to the Multitone i-Message system. Non-invited users are effectively placed in limbo until the Multitone i-Message system administrator resolves the account either via admission, after verification of bona fides, or blocks that user from further system access.

5. Multitone Messenger - Session security - Session tokens are generated when the user logs in using the email link or QR code, these tokens use AES 256 bit encryption and are used for secure communication between the app and the Multitone i-Message server, this effectively hiding passwords, ports and IP addresses.

   The token is tied to a user's device session and is maintained by the app and server, not by the user. Tokens cannot be stolen, or used like a password by a malicious third party; effectively it makes one of the factors in a two factor authentication process, the second factor being the email or phone number of the user. On this basis, a user authenticates themselves using the session token (generated by the app and server and tied to the user's device) and their email or phone number. The tokens themselves are periodically (every 20 days) replaced, so the system provides enhanced security without user interaction.

6. Multitone Appear WorkFlow and Multitone Messenger, data resident on the SMART device is sandboxed, automatic deletion occurs when the SMART device user logs out of the application

7. Contact access control - the ability to restrict access rights and user visibility to specific user contacts, e.g. the CEO or key department contacts is hidden

8. Accidental device loss - If a SMART device supporting the app is lost or stolen the login and details of the device can be revoked curtailing all future access

9. Call logging - all transactions between the Multitone i-Message and the app, or between apps using this application are logged, this includes: Time and date stamp, message content, sender, recipient, voice message content, call acknowledgement and message read receipts

10. Data transfer - regarding video handling, images and data files these are fully encrypted (Multitone Appear, Lite and Crew - AES 128, Multitone Messenger - AES 256), furthermore this information is not stored within the system; they are only available to sender and receiver of this information and the end-point devices involved. The data is sandboxed within the device and currently non-transferrable to other applications, i.e. a photograph of a tissue sample (bed sore) is not transferable to other applications such as the phone photo library for use with other applications.

11. Secure imaging data security - please note that images are encrypted using AES 128 for Multitone Appear and AES 256 for Multitone Messenger and held in a secure part of the SMART phone and not accessible via other applications on the device. Therefore, these images are not accessible to other non Multitone SMART Apps running on the phone and therefore, it is not possible to send these to non Multitone SMART Apps based contacts stored on your device. Likewise, forwarding of images is prevented once reviewed, this prohibits screen sharing or scraping.

11. MULTITONE APPS CONFIGURATION

11.1 Introduction

The purpose of this section is to provide guidelines to end users on how the LAN and WAN environment configuration in order to be able to run the Multitone SMART Apps service successfully at a customer site. Multitone SMART apps is designed to work both internally and externally of a customer's network. Failure to meet these requirements will result in quality and set-up/support issues.

11.2 Access Control

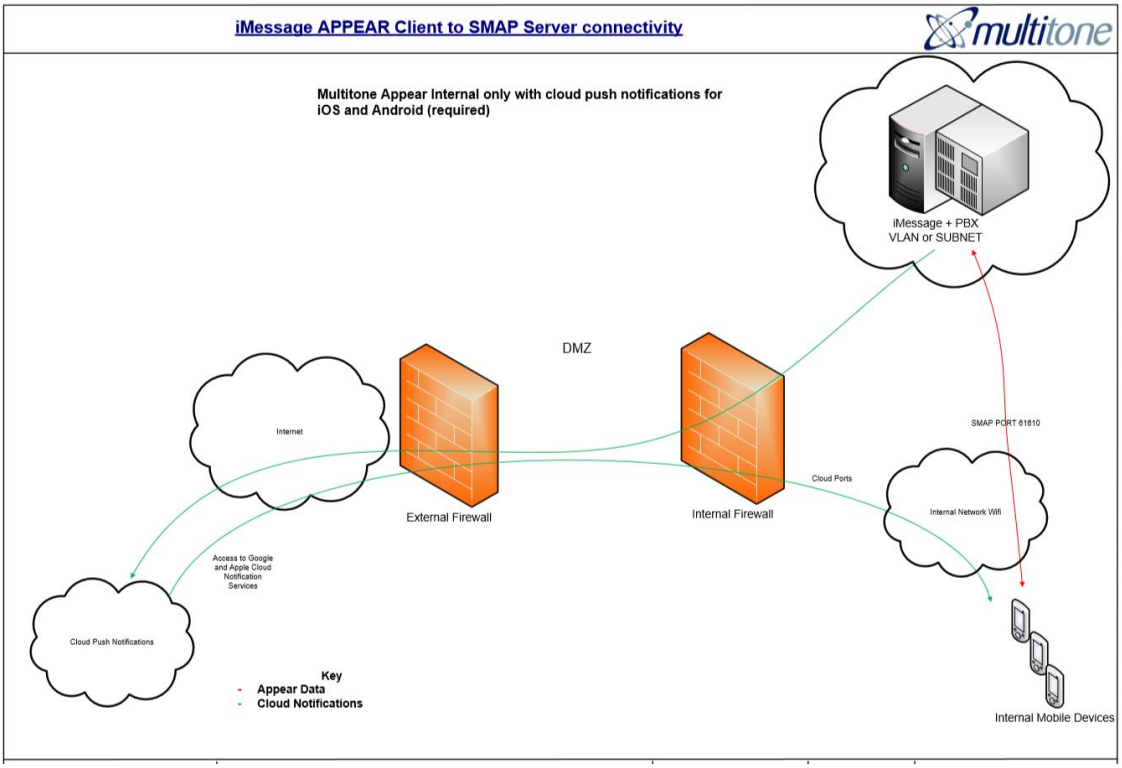
Network administrators must ensure that the following IP addresses and ports (both directions) are available and not blocked by firewalls. If these ports are not opened (i.e. a customer or network based firewall is blocking them), or IP addresses allowed, Multitone SMART Apps will not function correctly. These ports need to be available from each device using Multitone SMART Apps internally to the customer network both inbound and outbound as well as the Multitone i-Message solution server.

Ports	IP Address	Protocol	Usage	Flow Direction
61610 (configurable)	Multitone i-Message Solution IP	Proprietary AES 128 encrypted	Data & Messaging	Inbound from external
5060	i-Message PBX Solution IP	SIP (UDP/TCP)	VoIP Signalling	Inbound from external
10000 to 20000	i-Message PBX Solution IP	SIP RTP (UDP)	Voice & Data	Inbound from external
443, 2195, 2196, and 5223	https://api.push.apple.com	Apple Cloud (TCP)	Cloud Notifications	Outbound only for both Server and Clients
443, 5228, 5229, and 5230	https://fcm.googleapis.com/fcm/send https://www.googleapis.com/auth/firebase.messaging	Google Cloud (TCP)	Cloud Notifications	Outbound only for both Server and Clients

11.3 Design topology of the Multitone smartapp platform

11.3.1 SMAP Data Internal Only

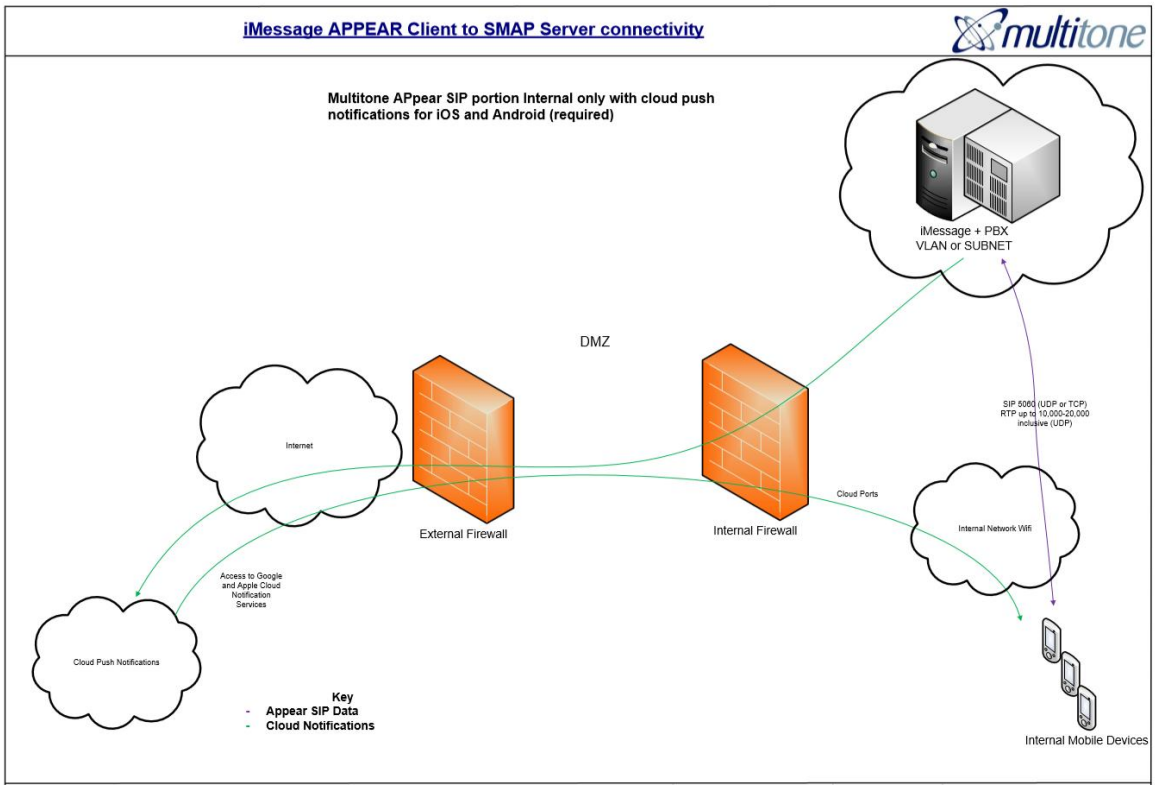
- For Multitone SMART Apps to function internally, the following IP addresses and ports need to be available and not blocked by firewalls:
  - Port 61610 (configurable): Multitone i-Message Solution IP, Protocol: Proprietary AES 128 encrypted, Usage: Data & Messaging, Flow Direction: Inbound from external.
  - Port 5060: i-Message PBX Solution IP, Protocol: SIP (UDP/TCP), Usage: VoIP Signalling, Flow Direction: Inbound from external
  - Ports 10000 to 20000: i-Message PBX Solution IP, Protocol: SIP RTP (UDP), Usage: Voice & Data, Flow Direction: Inbound from external.
- Internal devices connected to the WiFi network must have routing access to the Multitone i-Message server subnet. Firewall rules may be required to permit traffic from the WiFi network to the Multitone i-Message subnet.
- Multitone i-Message servers must have outbound access to both Google and Apple push notification servers. This allows message delivery and "wakes up" the SIP connection on devices running in the background.



11.3.2 SMAP SIP Portion Internal Only

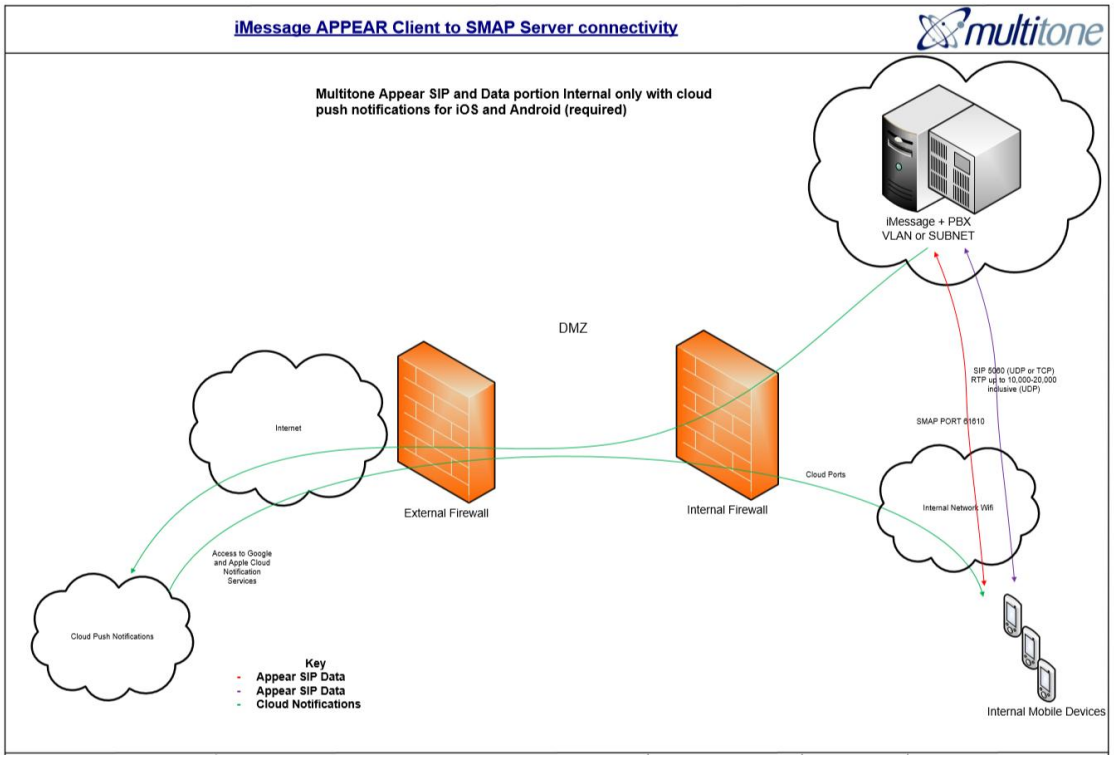
- This section illustrates the SIP portion of the app for VoIP and secure messaging within the internal network. Routing or allowing SIP data paths and RTP (real-time packets) between the WiFi network and the Multitone i-Message subnet/VLAN is essential.

- The cloud paths to Google and Apple push notification servers remain necessary for "waking up" devices before sending SIP calls, especially for iOS devices, which drop the link when the app goes into the background.



11.3.3 SMAP Data & SIP Internal Only

The above image illustrates the full requirement for devices to use both secure messaging and VoIP on the internal network only. After 1 minute of inactivity, the app allows the TCP link to drop, conserving battery usage on Android devices. Please note that the Multitone i-Message server must have access to the cloud push servers for this to operate correctly.

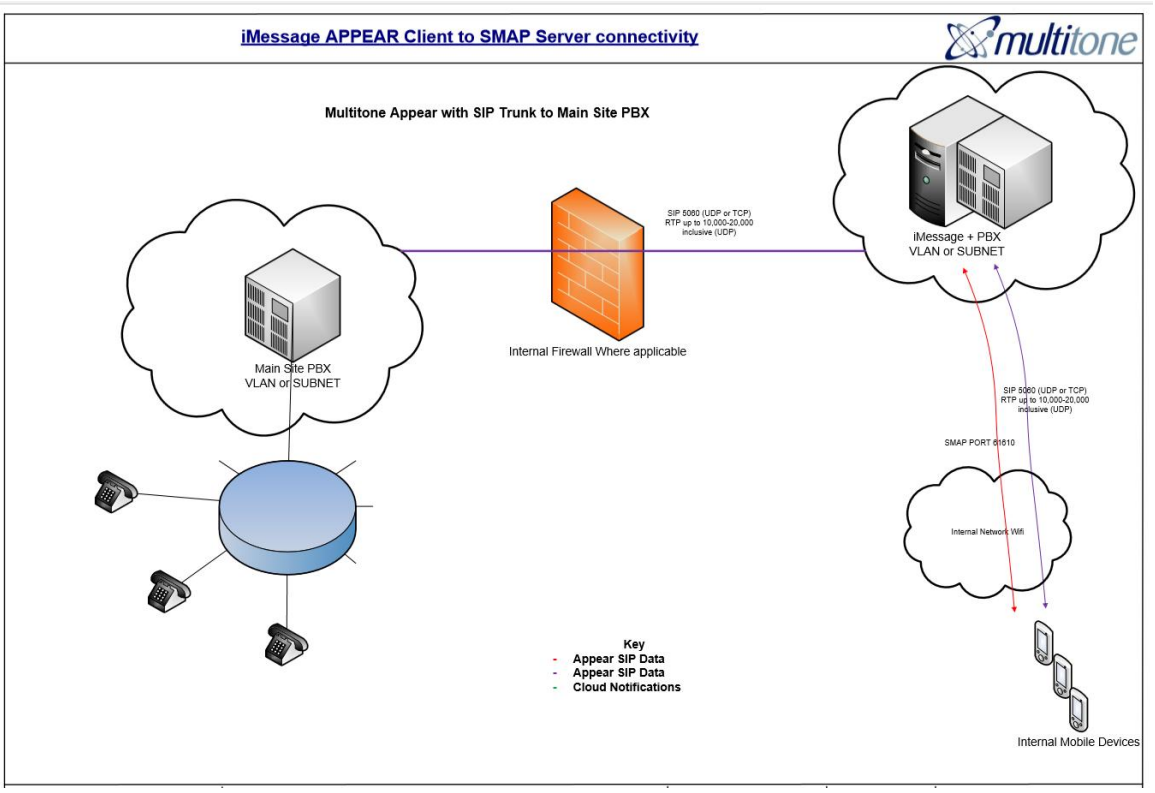


11.3.4 Multitone Apps - SIP Internal Trunk

- If required, a SIP trunk can be set up between the Main site PBX and the Multitone i-Message PBX, enabling desk phone users to call Multitone SMART Apps phone users and vice versa. This integration allows using a single device for all communication requirements.

- Running Multitone i-Message interconnected sites will have a pre-configured SIP trunk set up, enabling devices at any site to contact devices at any other site. For full resilience, multiple PBX systems on one or more sites can have SIP trunks to the main Multitone i-Message system and remote Multitone i-Message sites.

  ***Note**: This setup will require routing settings for primary and backup call handling.*



11.3.5 Multitone Smartapps, Connecting from External / Internal

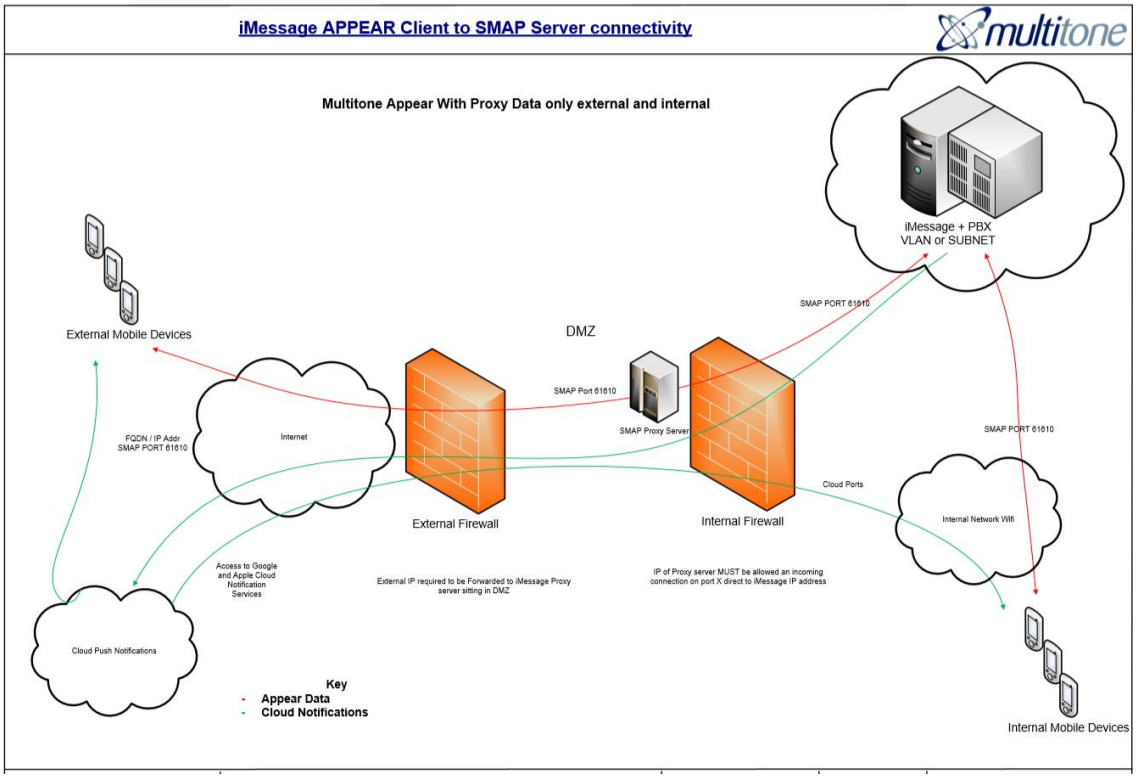
- For Multitone SMART Apps clients based externally to the core network, an external IP/FQDN must be provided for the clients to connect through the configured port. The port should be "Port Forwarded" to the internal floating Multitone i-Message IP address using the provided Multitone i-Message proxy in the middle, if supplied. The communication link is secure, utilizing Multitone's proprietary TCP protocol with AES 128 and AES 256 encryption.

- For internal clients within the core network, it is required that the subnets on which they reside can communicate back to the floating Multitone i-Message IP address. If a mixture of both internal and external devices is used, it is advisable to use an FQDN that can be resolved both internally and externally.

11.3.6 Multitone Smartapps. Data Internal & External Use

- To enable internal and external operation of Multitone SMART Apps, external devices must establish an incoming connection to the Multitone i-Message server inside the core network. Multitone's design supports encryption from the first packet to address security concerns (further detailed in the section below entitled "Encrypted from the first packet").

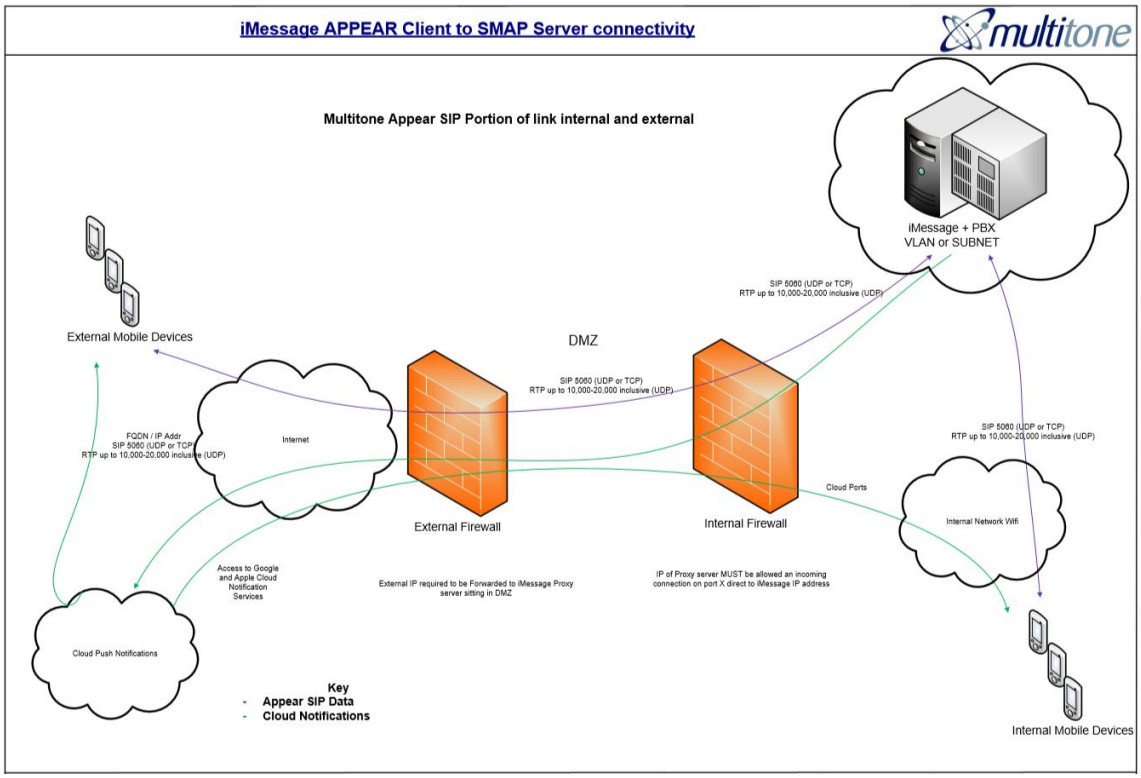
- For additional security, Multitone has developed the Multitone SMART Apps DMZ Proxy Server, which sits inside the DMZ of the network and inspects incoming packets. This server allows only identified Multitone SMART Apps packets to pass through to the smart app module within the Multitone i-Message server, serving as the first line of defence against potential attackers. Any incoming links without proper response appear as closed ports. Subsequently, the Multitone SMART Apps client goes through the full encrypted session setup process and user authentication upon any TCP disconnect/reconnect, restarting the process each time.



11.3.7 Multitone Smartapps, SIP Internal & External Use

- To enable SIP usage both internally and externally, the client device must have an incoming connection to the Multitone i-Message system. This requires allowing SIP ports (5060, configurable) and RTP ports (10,000 to 20,000) for live audio streams during calls.

- The Multitone i-Message PBX has a security feature that blocks an IP address for a pre-set period after a certain number of failed logon attempts. Configurable parameters include the number of failed attempts, the period they occur, and the duration of the ban. Multitone SMART Apps can use both secure and standard SIP with RTP and SRTP packets where required. TLS security with a unique certificate, generated within the PBX portion of the system, is used on each Multitone i-Message PBX server, unique to each site and i-Message installation.



11.3.8 Multitone Smartapps, Data Using AWS Cloud Proxy

For certain implementations of Multitone SMART Apps, using an AWS Cloud Proxy can provide additional benefits. This approach involves utilizing two dedicated load-balanced Proxy servers hosted on Amazon Web Services (AWS). The setup ensures efficient handling of traffic from mobile devices, both internal and external, by directing it to the AWS Proxy using a dedicated Fully Qualified Domain Name (FQDN). From there, the AWS Proxy servers establish connections to the onsite Multitone i-Message system through the external WAN IP of the customer network. The key points of this configuration are as follows:

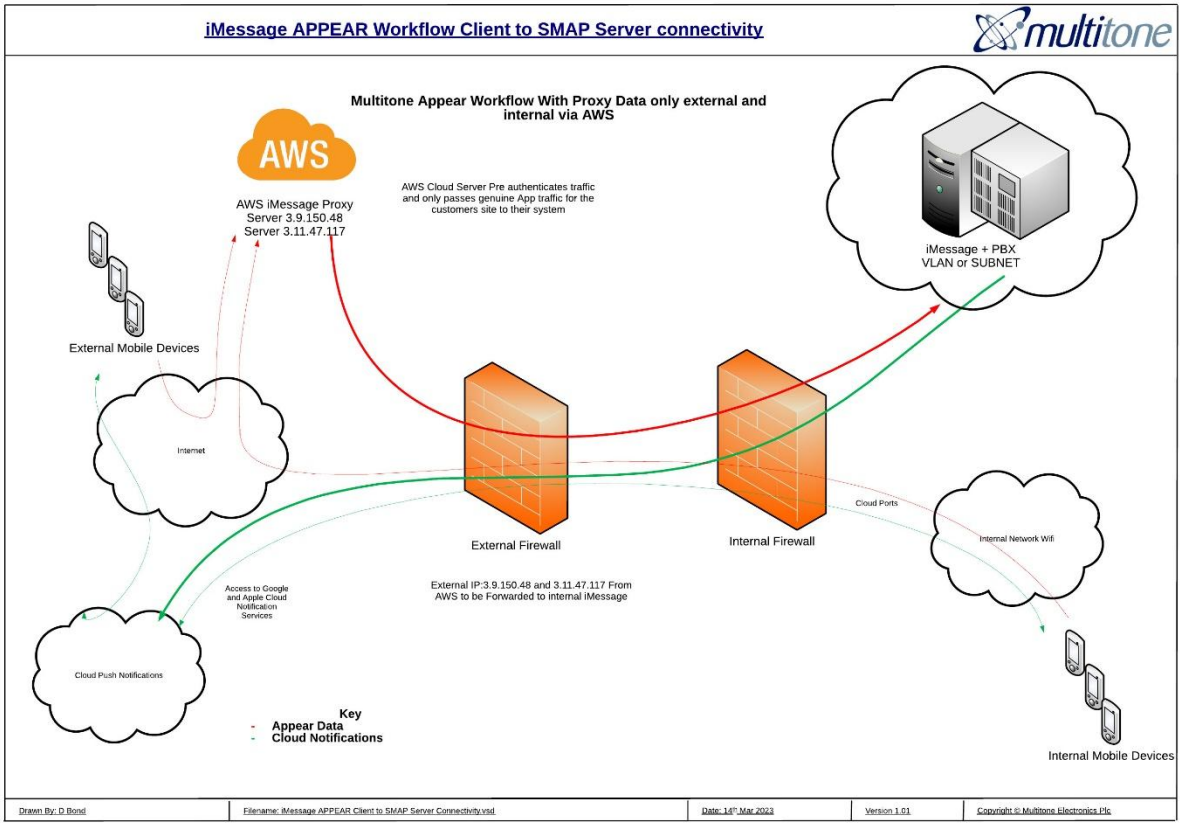
1. AWS Cloud Infrastructure: The implementation employs the AWS cloud infrastructure to host the dedicated load-balanced Proxy servers. AWS offers scalability, high availability, and reliability, ensuring seamless performance during peak loads.

2. Dedicated Load-Balanced Proxy Servers: Two Proxy servers are used, configured in a load-balanced setup. This redundancy ensures that the traffic is distributed evenly between the servers, enhancing performance and fault tolerance.

3. FQDN for AWS Proxy: A dedicated Fully Qualified Domain Name (FQDN) is assigned to the AWS Proxy servers, allowing all traffic from mobile devices, both internal and external, to be directed to these Proxy servers.

4. External WAN IP Connectivity: The AWS Proxy servers establish connections to the onsite Multitone i-Message system using the external WAN IP of the customer network. This ensures secure and efficient communication between the AWS cloud and the customer's premises.

By leveraging the AWS Cloud Proxy solution, Multitone SMART Apps can benefit from enhanced scalability, load balancing, and reliable connectivity for both internal and external users. This setup allows organizations to optimize their messaging and data delivery while ensuring robustness and seamless user experiences.


iMessage APPEAR Workflow Client to SMAP Server connectivity
multitone
Multitone Appear Workflow With Proxy Data only external and internal via AWS
AWS
AWS iMessage Proxy Server 3.9.150.48 Server 3.11.47.117
AWS Cloud Server Pre authenticates traffic and only passes genuine App traffic for the customers site to their system
iMessage + PBX VLAN or SUBNET
External Mobile Devices
Internet
External Firewall
Internal Firewall
Cloud Ports
Internal Network Wifi
Access to Google and Apple Cloud Notification Services
External IP:3.9.150.48 and 3.11.47.117 From AWS to be Forwarded to internal iMessage
Cloud Push Notifications
Key
- Appear Data
- Cloud Notifications
Internal Mobile Devices
Drawn By: D Bond
Filename: iMessage APPEAR Client to SMAP Server Connectivity.vsd
Date: 14th Mar 2023
Version 1.01
Copyright © Multitone Electronics Plc

11.4 Further Notes on Design Topology of Multitone Smartapps

11.4.1 SIP Application Layer Gateway (ALG)

SIP Application Layer Gateway (ALG) is common in many of today's routers and in most cases enabled by default on enterprise, business and home broadband routers. Its primary use is to prevent problems associated to the router's firewalls by inspecting VOIP traffic packets, and if necessary modifying them to allow connection to the required protocols or ports.

On many business and home class routers, Active SIP ALG will cause a mixture of problems by adjusting, or terminating SIP traffic packets in such a manner that they are corrupted and cause issues with the service. This can manifest in a range of intermittent issues such as; one-way audio, dropped calls, problems transferring calls, handset dropping registration and making or receiving internal calls. Please disable all SIP ALGs on all CPE routers. Where SIP ALG is activated Multitone will not accept any faults or issues if. For instructions on disabling this feature, please refer to the specific router guide.

11.4.2 Keep Alive

Handsets are pre-configured to send UDP keep-alive messages towards the Multitone i-Message platform every 60 seconds using the SIP port. These messages keep the firewall pinholes open which ensures the success of incoming calls. However, when using iOS or Android in "background" the devices will kill the link to save battery and in these situations, the Multitone i-Message system sends cloud "wakeups" when sending a message or call to unconnected devices.

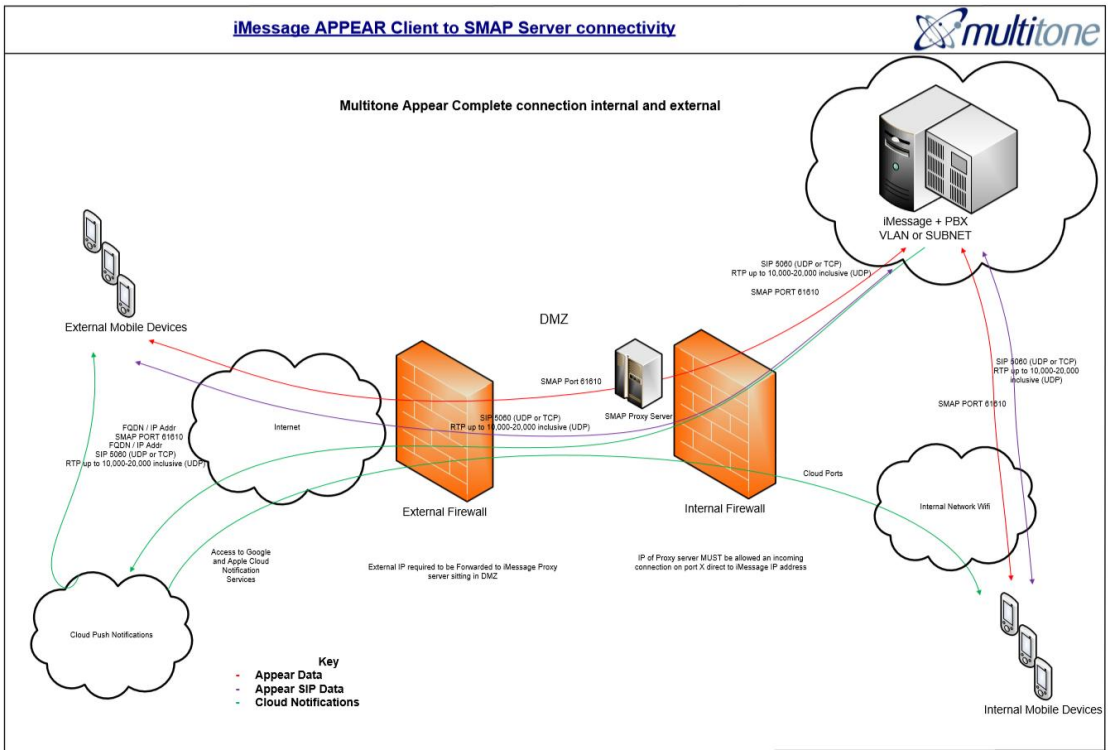
11.4.3 Network Address Translation (NAT)

For Multitone SMART Apps handsets to operate externally, away from the customer network, Multitone i-Message will be required to support an external IP address - this directs RTP traffic to the Multitone i-Message IP address. Internal units must have available routing to communicate with the Multitone i-Message solution.

11.4.4 Domain Name Server (DNS)

A DNS service must be available to the Multitone SMART Apps handsets if using the Fully Qualified Domain Name (FQDN) so that the domain names can be resolved to the associated IP addresses both internally and externally. Ideally, undertake configuration of the primary and secondary DNS as part of the initial deployment.

11.4.5 Multitone Smartapps SIP Internal & External Use



The picture above shows the full requirement for Multitone SMART Apps with Data and Voice for both internal and external users.

11.5 Firewall Requirements

11.5.1 Important Firewall Port Information

Apple and Google are changing the way applications can use the devices processing and network access resources in the operating system, driven by the aim to prolong battery life on mobile devices. As a result, it is no longer possible to create persistent network connections to third party servers from apps on these mobile operating systems. Going forward, any mobile applications that need to receive incoming notifications must use cloud-messaging systems from Apple and Google.

When sending a message or call to a user, who is logged into the Multitone SMART Apps Mobile Client on Android or iOS the Multitone i-Message server will send a notification to Apple or Google's servers. Apple or Google will forward the notification to the device and the app will wake up, alert for an incoming call/message and will set-up the TCP link for the duration of the event. Any Multitone SMART Apps Mobile Client operating behind firewalls must therefore allow access to Apple and Google push notification servers at the IP addresses and via the ports below.

These rules derive from Google and Apple who specify a wide range of IP addresses, their push notification servers scale to millions of requests, therefore new servers may be commissioned at new IP addresses in their ranges with no way to provide prior notice. For the Mobile client to receive push notifications from Apple or Google servers, when running on a phone behind a firewall, access to Apple and Google servers is fundamental to the provision of this service, the following ports are identified as:

- Apple TCP - 443, 2195, 2196 and 5223
- Google TCP - 443, 5228, 5229 and 5230

The connections to the cloud are outbound originated only, from the phone to the cloud-messaging server as well as from the Multitone i-Message server to the cloud-messaging server. The phone will keep the connection alive to Google or Apple and setup a new connection when required this forms part of the standard for cloud notifications.

Apple and Google may commission new servers, at new IP addresses at any time to manage the load across the systems. As a result, it is not possible to provide customers with a list of IP addresses to configure the firewall however the . Push Notification servers are identified using DNS requests but these are managed to Operating System processes so, again, it is not possible to state a list of hostnames that could be entered into a firewall that can allow traffic based on configured FQDNs.

Apple provides a straightforward solution, their servers will Multitone SMART Apps somewhere in their class a subnet: 17.0.0.0/8. Google however, only state that the IP addresses will Multitone SMART Apps in their ASN 15169. This contains hundreds of IP subnets, which would be impractical to input into a firewall. IP Engineering have summarised the subnets to a more manageable list but specifically added the FQDN for both Apple and Google cloud services. The iMessage servers MUST be able to resolve and communicate with these addresses to successfully send cloud push notifications:

11.5.2 Cloud Notification Ports & IP Addresses

IP Subnet	Ports	Function
8.0.0.0/10 23.224.0.0/11 35.128.0.0/9 64.0.0.0/4 104.0.0.0/5 128.0.0.0/3 162.216.0.0/13 185.0.0.0/8 172.96.0.0/12 172.192.0.0/10 173.192.0.0/10 192.104.160.0/23 192.158.28.0/22 192.178.0.0/15 199.192.0.0/11 207.223.160.0/2020 8.0.0.0/4 https://fcm.googleapis.com/fcm/send https://www.googleapis.com/auth/firebase.messaging	TCP: 443, 5228, 5229, 5230	Push Notifications for Multitone SMART Apps Mobile Client – Android Google operates these ranges and the servers behind them. Traffic will go outbound TO these IP addresses and ports from both the i-Message server AND the clients
17.0.0.0/8 https://api.push.apple.com	TCP: 443, 2195, 2196, 5223	Push Notifications for Multitone SMART Apps Mobile Client - iOS. Apple operates these ranges and the servers behind them. iOS based Multitone SMART Apps Mobile clients use Apple's Push Notification service to deliver notifications Traffic will go outbound TO these IP addresses and ports from both the i-Message server AND the clients

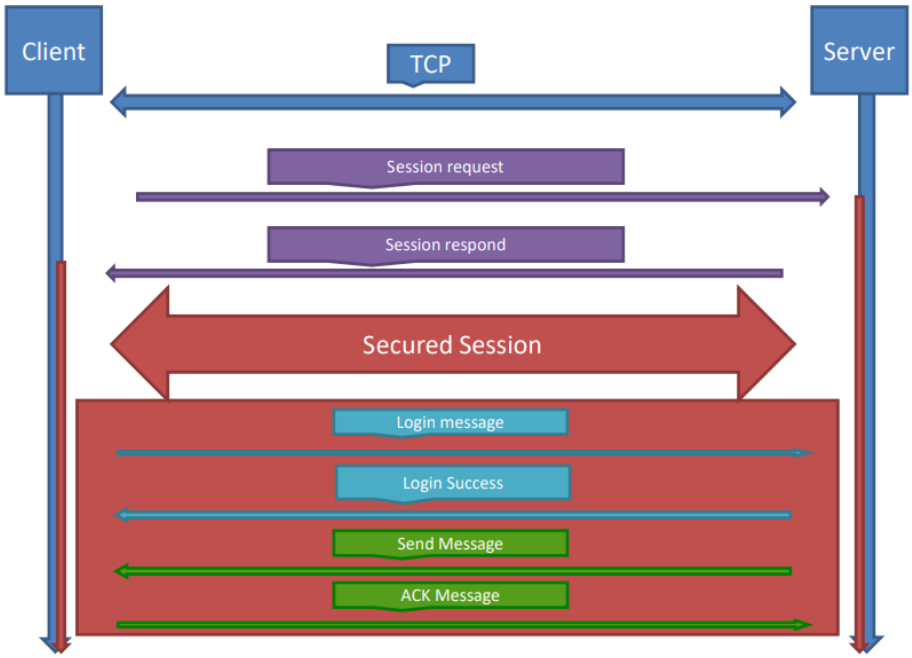
11.5.3 Cloud Proxy Ports & IP Addresses

When using the Cloud proxy Apps will be pointed to the FQDN appear.multitone-imessage.com on a provided and agreed port. Connections will be made from the app to the load balanced proxy servers in our AWS instance. These are then routed back to the local internal system on installed on site. A WAN IP will need to be provided by the customer IT department for Multitone to point these connections to. And a port forwarding rule set up to forward the incoming TCP traffic back to the iMessage IP address. The incoming connections will come specifically from one of two addresses 3.9.150.48 and 3.11.47.117 these are owned by Multitone and attached to our outbound connections on our AWS instance used for the Cloud Proxy services.

11.6 Multitone i-Message & Smartapp Encryption

11.6.1 Encrypted from the First Packet

To ensure absolute encryption, Multitone SMART Apps maintains an encrypted link from the first packet. The way in which it operates is as follows:



A standard 3-way handshake sets-up the TCP connection, this allows data flow to initiate, after which the Multitone SMART Apps app creates an ad-hoc “public” and “private key” pair and encrypts its own public key using the Multitone i-Message servers already known public key. It is worth noting that the Multitone i-Message public key is not actually publicised but it is hardcoded into the Multitone SMART Apps app and the Multitone i-Message system.

The Multitone i-Message server then decrypts this incoming packet using it own private key sending a response back that the client application decrypts using its own private key, once it has this information both side are able to create a “shared” key with AES 128 encryption (Multitone Appear) and AES 256 (Multitone Messenger). For Multitone Appear and Multitone Messenger this section makes up the RSA encrypted session request to establish the connection and relative response.

- Multitone Appear encryption:
  - Asymmetric RSA with ECB mode and PKCS1 padding
  - Key size:1KB symmetric: AES with CBC mode and PKCS5 padding
  - Key size 128 bit

- Multitone Messenger encryption:
  - Asymmetric RSA with ECB mode and OAEP padding
  - Key size: 3KB symmetric: AES and GCM and no padding
  - Key size 256 bit

From this point on all data passed between the client and server, encrypted at AES 128 bit (Appear) and AES 256 (Messenger) encryption. Each client will generate a new set of keys for the RSA and subsequent AES 128/AES 256 portions of the encryption each time it needs to negotiate the establishment of a new session. This occurs when you move from one network to another i.e. 3G/4G/5G to WiFi, or if you temporarily moved out of signal area.

This means these highly encrypted streams may only “live” for a few hours and a maximum time to live of 24-hours even though the time it would take to crack one is in the order of billions of years for the average attacker with a single super computer.

11.6.2 Note on AES Encryption

Any cryptographic algorithm requires multi-bit key to encrypt the data as shown in Figure 1:

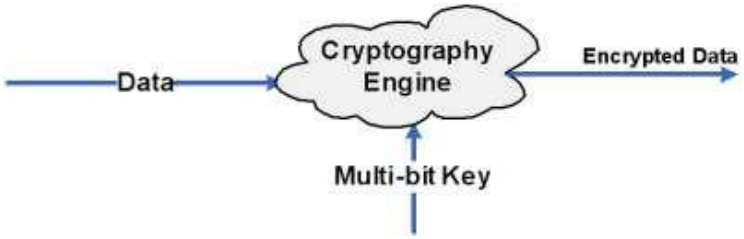


Figure 1: Multi-bit key to encrypt data using cryptographic algorithm

The key length used in the encryption determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. Brute-force attack involves systematically checking all possible key combinations until the identification of correct key. This is one way to attack when it is not possible to take advantage of other weaknesses in an encryption system. Here is an example of a brute force attack on a 4-bit key:

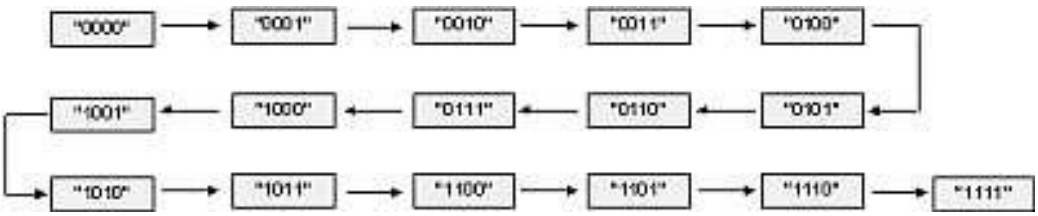


Figure 2: Brute force attack on 4-bit key

As shown, it will take a maximum 16 rounds to check every possible key combination starting with "0000." Given sufficient time, a brute force attack is capable of cracking any known algorithm. The following table just shows the possible number of key combinations with respect to key size:

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Figure 3: Key combinations versus key size

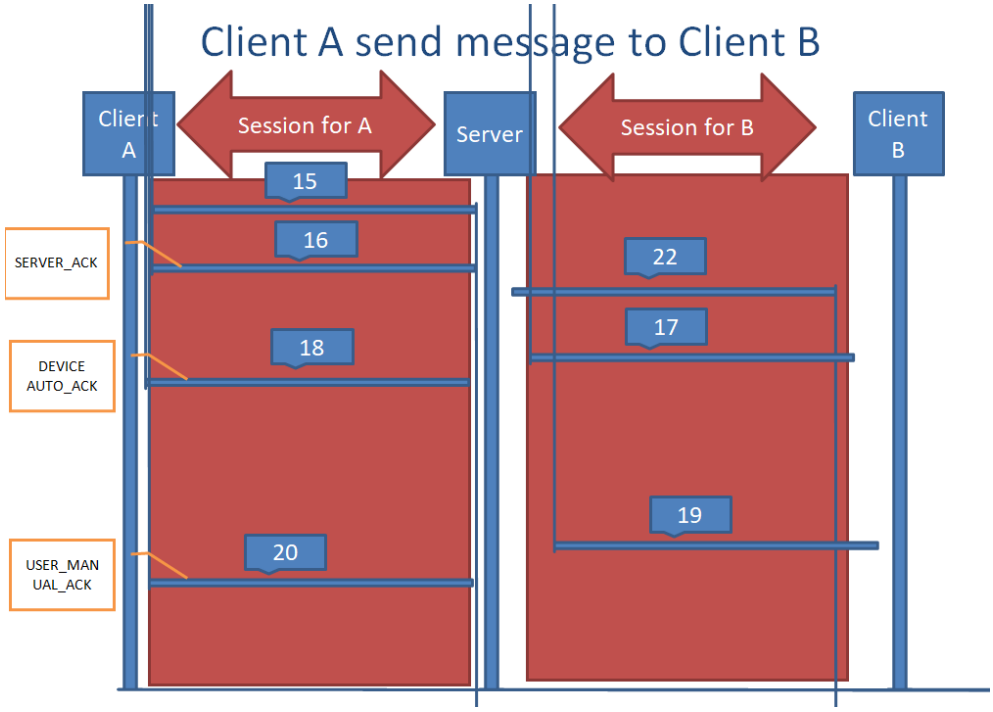
The increase in possible combinations is exponential as the key size increases. There is a physical argument that a 128-bit symmetric key is computationally secure against brute-force attack. Just consider the following:

- Faster supercomputer (as per Wikipedia): 10.51 Petaflops = 10.51×10^{15} Flops (Flops = Floating point operations per second)
- Number of Flops required per combination check: 1000 (very optimistic)
- Number of combination checks per second = $(10.51 \times 10^{15}) / 1000 = 10.51 \times 10^{12}$
- Number of seconds in one Year = 365 x 24 x 60 x 60 = 31536000
- Number of years to crack AES with 128-bit Key = $(3.4 \times 10^{38}) / [(10.51 \times 10^{12}) \times 31536000]$

  $= (0.323 \times 10^{26})/31{,}536{,}000$
  $= 1.02 \times 10^{18}$
  = 1 billion, billion years

11.6.3 Sending Messages Between Devices

When sending messages between devices, both devices have their own secure transmission path, so that data is secure within their respective AES 128 encrypted channels. Calls will always go to the server, not client-to-client:



11.6.4 Not Stopping at TCP Security

The information above shows how secure the TCP connection for the Multitone SMART Apps application is, this should alleviate any potential concerns at allowing it to operate on your network, however, some data is stored on the app such as messages for your inbox outbox etc., as well as attachments. These need to be secure too.

To ensure we have covered this off the Multitone SMART Apps application runs as a “sandboxed” entity with AES 256 encryption on the data stored within the app. Attachments and screen shots are blocked see note below. This means that should a user leave the organisation having had Multitone SMART Apps running on their personal device once their credentials have been removed from Multitone i-Message the app is no longer of any use to that person. They can no longer access any of the messages data or send/receive messages. Essentially, the app is on their device is now dead.

***Note**: iOS devices cannot have screen shots blocked under normal conditions, however, if managed by an MDM style solution this is then achievable. This is feature prevented on Android at all times, iOS is more restrictive to applications making administrator level decisions within the environment.*

11.6.5 Password Security

Users on Multitone i-Message will have their usernames and passwords created by the system administrator. However if you wish to use Active Directory for authentication the Multitone i-Message system can connect to your own AD server using LDAP/LDAPs and authenticate users. This ensures users only have one password for all their logins.

The Multitone i-Message database (although encrypted to AES 256 when exported) would **not** contain any passwords stored on the Active Director server but would contain the usernames. Operationally, with Active Directory enabled and a user attempts login with their username, Multitone i-Message will attempt to authenticate the user's credentials against the Active Directory. If this fails, it will attempt to authenticate locally, although we advise not to place passwords in Multitone i-Message if using Active Directory but it may be that some "generic" users such as switchboard operator may want a simple username and password for ease of use for sending cardiac paging messages through the system.

APPENDIX

MULTITONE i-MESSAGE TECHNICAL INFORMATION

1. Multitone i-Message Server Software, Port Allocations

IP usage	Network Adaptor Type	Ports Incoming (TCP and UDP)	Ports Outgoing (TCP and UDP)
Static IP 1	1Gbps	80, 443, 6000-6020, 60000-60009,22, 5060-5180 & 10000-20000RTP	ALL
Static IP 2	1Gbps	80, 443, 6000-6020, 60000-60009,22, 5060-5180 & 10000-20000RTP	ALL
iMessage Floating IP Address	Virtual	80, 443, 6000-6020, 60000-60009	ALL
Asterisk Floating IP Address	Virtual	22, 80, 5060-5180 & 10000-20000RTP	5060-5180 & 10000-20000RTP
DBI No 1	100Mbs	5999,6000-6020,22,80,3389	6001, 6012
FXO No.1	100Mbs	80	5060-5064 & 10000-20000RTP
SCU No 1 (Switchboard)	100Mbs		5060-5064 & 10000-20000RTP
Call Verifier 1	10Mbps	3001-3006, 80	3001-3006
SMS unit	100Mbps	80, 81, 443,	
LPI Unit	10Mbps half duplex	3001-3006, 80	3001-3006

Note: There are always exceptions and this although detailed may still be missing some ports based on system configuration and usage

2. Communication Processor, Port Allocations (Hardware)

Dual Bearer Interface, Multitone Integrator and LAN Peripheral interface port allocations and availability:

Dual Bearer Interface - Port Allocations			
Application	**Ethernet**	**Peripheral Port**	**Modem**
Audio Distribution Unit	Allocated	Available (CVU/DLC)	N/A
Call Verification Unit	Allocated	Allocated	N/A
Transmitter Interface (Speech)	Allocated	Allocated (Transmitter only)	Allocated (PSTN)
Intelligent Transmitter Interface (1 Transmitter Only)	Allocated	Allocated	N/A
Direct Line Contacts	Allocated	Allocated DLC's	N/A

Multitone Integrator - Port Allocations			
Application	**RS232 Ports**	**Peripheral Port**	**Ethernet**
Audio Distribution Unit	2 Ports Available	Available (CVU/DLC)	Allocated
Call Verification Unit	2 Ports Available	Allocated	Available
Transmitter Interface (Speech)	2 Ports Available	Allocated	Allocated
Intelligent Transmitter Interface (1 Transmitter Only)	2 Ports Available	Allocated	Allocated
SMS Modem Interface (IM-L4-04)	1 Port Allocated, 1 Available	Available (CVU/DLC/Tx)	Allocated
RS232 Interfaces	1 Port per RS232 Protocol	Available (CVU/Tx/DLC)	Allocated
Direct Line Contacts	3 Ports Available	Allocated	Allocated

LAN Peripheral Interface - Port Allocations				
Application		**RS232 Ports**	**Peripheral Port**	**RS485 Port (S-Bus)**
Audio Distribution Unit		3 Ports Available	Available (CVU/DLC)	Allocated
Call Verification Unit		3 Ports Available	Allocated	Available
Transmitter Interface (Speech)		3 Ports Available	Allocated	Allocated
Intelligent Transmitter Interface (1 Transmitter Only)		3 Ports Available	Available (CVU/DLC)	Allocated
SMS Modem Interface (IM-L4-04)		1 Port Allocated, 2 Available	Available (CVU/DLC/Tx)	Available
Kenwood		1 Port (Aux B) Allocated, 2 Available	Available (CVU/DLC)	Allocated
Access 3000 Interface	LPI1	2 Ports Allocated, 1 Available (Main)	Available (CVU/DLC)	Allocated
	LPI2	Allocated	Available (CVU/DLC)	Allocated
Absence & Charging		3 Ports Available	Available (CVU/DLC)	Allocated
EkoTek		1 Port Allocated, 2 Available	Available (CVU/Tx/DLC)	Available
RS232 Interfaces		1 Port per RS232 Protocol	Available (CVU/Tx/DLC)	Available
Direct Line Contacts		3 Ports Available	Allocated	Available

3. Multitone i-Message Component Dimensions & Weights

Product	Part No.	Width	Depth	Height	Weight (kg)
PC Server Hardware & Network Switch					
Server Hardware, Single Disk & PSU	IM-SV1	434mm	495mm	43mm (1U)	10.60kg
Server Hardware, RAID 1, Dual PSU	IM-SV3	440mm	700mm	43mm (1U)	
24 Port Network Switch	IM-NS1	440mm	240mm	44mm (1U)	3.15kg
Dual Bearer Interface (DBI)					
2 x Dual Bearer Interface (19" Rack/Tray Mount)	IM-DBI2R	440mm	135mm	43mm (1U)	1.60kg
1 x Dual Bearer Interface (19" Rack/Tray Mount)	IM-DBIR	440mm	135mm	43mm (1U)	0.75kg
Dual Bearer Interface (Desk Mount)	IM-DBID	220mm	135mm	43mm (1U)	0.80kg
External PSTN 56K V.92 Modem	2314-0044	68mm	26mm	20mm	
Multitone Integrator					
2 x Dual Bearer Interface (19" Rack/Tray Mount)	IM-INT-D	440mm	125mm	40mm (1U)	0.87kg
1 x Dual Bearer Interface (19" Rack/Tray Mount)	IM-INT-R	440mm	125mm	40mm (1U)	1.64kg
Dual Bearer Interface (Desk Mount)	IM-INT2-R	220mm	125mm	40mm (1U)	1.82kg
LAN Peripheral Interface (LPI)					
Dual LAN Peripheral Interface (Rack Mount)	IM-LPID-R	440mm	113mm	43mm (1U)	1.90kg
LAN Peripheral Interface (Desk Mount)	IM-LPIS-D	220mm	113mm	43mm (1U)	0.95kg
LAN Peripheral Interface (Rack Mount)	IM-LPIS-R	440mm	113mm	43mm (1U)	1.00kg
Call Verification Unit					
Call Verification Unit & LPI (Rack)	IM-CVU-LPI-R	440mm	113mm	43mm (1U)	1.95kg
Call Verification Unit & Dual Bearer Interface (Rack)	IM-CVU-DBI-R	440mm	113mm	43mm (1U)	1.75kg
Call Verification Unit Only (Desk Mount)	IM-CVU-D	220mm	113mm	43mm (1U)	0.90kg
Call Verification Unit Only (Rack Mount)	IM-CVU-R	440mm	113mm	43mm (1U)	1.00kg
Audio Distribution Unit (ADU) - Live VA: 12VA					
Dual Audio Distribution Unit (Rack)	IM-ADU2-R	440mm	113mm	43mm (1U)	1.85kg
Audio Distribution Unit & LPI (Rack)	IM-ADU-LPI-R	440mm	113mm	43mm (1U)	1.85kg
Audio Distribution Unit (Desk)	IM-ADU-D	220mm	113mm	43mm (1U)	1.85kg
Audio Distribution Unit (Rack)	IM-ADU-R	440mm	113mm	43mm (1U)	0.92kg
Intelligent Transmitter Interface (ITI) Live VA, 12 VA transmitting 53 VA					
Intelligent Transmitter Interface & LPI (Rack)	IM-ITI-LPI-R	440mm	113mm	43mm (1U)	1.85kg
Intelligent Transmitter Interface (Desk Mount)	IM-ITI-D	220mm	113mm	43mm (1U)	0.90kg
Intelligent Transmitter Interface (Rack Mount)	IM-ITI-R	440mm	113mm	43mm (1U)	1.00kg
Power Options					
6 x Socket 12V Power Distribution Unit (Rack Mount)	IM-PDU-R	420mm	113mm	43mm (1U)	1.66kg
PBX Analogue Interface Modules					
PBX Analogue Interface FXO 4 Port Extension Module	IM-PBX-TR	225mm	135mm	35mm	
PBX Analogue Interface FXS 4 Port Trunk/Extension Module (CISCO)	IM-CISCO-4EX	220mm	170mm	39mm	1.30kg
PBX Analogue Interface FXS 4 Port Trunk Module	IM-PBX-4EX	230mm	135mm	35mm	
PBX Analogue Interface FXS 8 Port Trunk Module	IM-PBX-8EX	230mm	135mm	35mm	-

4. Multitone i-Message Components Power Rating

Product	Part Number	Power Rating (figures quoted indicative for estimation only)	Thermal rating (Figures quoted indicative for estimation only)
PC Server Hardware & Network Switch			
Server Hardware, Single Disk, PSU, Windows 2012,R2, 2016, 2019 Server	**IM-SV1** **IM-SV1-UGK**	450W Single PSU	1725 BTU/hr per equipment item at 10°C to 35°C (50–95°F)
Server Hardware, RAID 1, Dual PSU, Windows 2012R2, 2016, 2019 Server	**IM-SV3** **IM-SV3-UGK**	550WDual PSU	1356 BTU/hr per equipment item at 10°C to 35°C (50°F to 95°F
24 Port Network Switch	**IM-NS1**	12W idle; 19W max 100 - 240V AC mains	Approx. 40 to 55 BTU/hr
Dual Bearer Interface (DBI)			
2 x Dual Bearer Interface (19" Rack/Tray)	**IM-DBI2R**	12VA @ 12V DC Nominal, 10W per unit	Approx. 34 BTU/hr x 2
Dual Bearer Interface (19" Rack/Tray)	**IM-DBIR**	12VA at 12V DC Nominal, 10W per unit, additional units added as multiples of 12VA	Approx. 34 BTU/hr
Dual Bearer Interface (Desk Mount)	**IM-DBID**	As above	Approx. 34 BTU/hr
External PSTN 56K V.92 Modem for DBI	**2314-0044**	USB port powered	Negligible
LAN Peripheral Interface (LPI)			
Dual LAN Peripheral Interface (Rack)	**IM-LPID-R**	2 x LPI at 12.5VA at 12V DC Nominal, 10W per unit	Approx. 34 BTU/hr x 2
LAN Peripheral Interface (Desk)	**IM-LPIS-D**	12.5VA at 12V DC Nominal, 10W per unit, additional units added as multiples of 12.5VA	Approx. 34 BTU/hr
LAN Peripheral Interface (Rack)	**IM-LPIS-R**	As above	As above
Call Verification Unit			
Call Verification Unit & LAN Peripheral Interface(Rack)	**IM-CVU-LPI-R**	CVU (6VA @ 12V, DC Nominal, 5W per unit) LPI (12.5VA at 12V DC Nominal, 10W per unit)	Approx. 51 BTU/hr
Call Verification Unit Only (Desk)	**IM-CVU-D**	6VA @ 12V DC Nominal, 5W per unit	Approx. 17 BTU/hr
Call Verification Unit Only (Rack)	**IM-CVU-R**	As above	As above
Audio Distribution Unit (ADU) - Live VA: 12VA			
Dual Audio Distribution Unit (Rack)	**IM-ADU2-R**	2 x ADU at 12VA @ 12V DC Nominal, 10W per unit	2 x Approx. 34 BTU/hr
Audio Distribution Unit & LAN Peripheral Interface (Rack)	**IM-ADU-LPI-R**	ADU (12VA @ 12V, DC Nominal, 10W per unit) LPI (12.5VA at 12V DC Nominal, 10W per unit)	Approx. 68 BTU/hr
Audio Distribution Unit (Desk)	**IM-ADU-D**	12VA @ 12V DC Nominal, 10W per unit, additional peripherals added as per their individual ratings	Approx. 34 BTU/hr
Audio Distribution Unit (Rack)	**IM-ADU-R**	As above	As above

Product	Part Number	Power Rating (figures quoted indicative for estimation only)	Thermal rating (Figures quoted indicative for estimation only)
Intelligent Transmitter Interface (ITI)			
Intelligent Transmitter Interface & LPI (Rack)	**IM-ITI-LPI-R**	ITI (12VA @ 12V DC Nominal, 10W per unit) LPI (12.5VA at 12V DC Nominal, 10W per unit)	Approx. 68 BTU/hr
Intelligent Transmitter Interface (Desk)	**IM-ITI-D**	12VA @ 12V DC Nominal, 10W per unit, additional peripherals added as per their individual ratings	Approx. 34 BTU/hr
Intelligent Transmitter Interface (Rack)	**IM-ITI-R**	As above	As above
Power Options			
6 Socket 12V Power Distribution Unit (Rack Mount)	**IM-PDU-R**	Output rating up to 12V 5A max, AC I/P 60W	Approx. 205 BTU/hr
PBX Analogue Interface Modules			
PBX Analogue Interface FXO 4 Port Extension Module	**IM-PBX-TR**	16VA @ 12V DC each, 14w per unit	Approx. 48 BTU/hr
PBX Analogue Interface FXS 4 Port Trunk/Ext. Module (CISCO)	**IM-CISCO-4EX**	0.3A Max at 230V	
PBX Analogue Interface FXS 4 Port Trunk Module	**IM-PBX-4EX**	16VA @ 12V DC each, 14w per unit	Approx. 48 BTU/hr
PBX Analogue Interface FXS 8 Port Trunk Module	**IM-PBX-8EX**	16VA @ 12V DC each, 14w per unit	Approx. 48 BTU/hr

5. Multitone i-Message Failover & Start-up Estimation

Failure mode	Estimated time
i-Message start-up, with windows already running:	Typically 45 seconds to 1 minute
i-Message server failover from secondary to primary server:	Approximately 30 seconds +/-10 seconds
Synchronisation of secondary server database:	Approximately 20 seconds +/- 5 seconds, (no impact on service)
Private Branch Exchange (PBX) offline: ***Note:*** *i-Message makes various attempts in this time to attempt a fix and then restarts iMessage after 5 minutes)*	Typically up to 5 minutes +/- 1 minute 20 seconds
Powering up a server and then starting i-Message:	This depends on the server therefore, it is not possible to calculate accurate statistics. Typically, if the server is off the time to start and be ready for use is the server start-up time plus 1 minute for the i-Message application.

6. Multitone SMART Apps WiFi Usage (Typically up to 20 Apps)

The WiFi will be at least 56Mbps to the device and the WiFi to the core network would easily be 1Gbps therefore this is not stretching the demand placed by SIP. It is only once you start using the incoming Broadband connection that bandwidth could be an issue.

To use A-law or U-law (standard for Multitone i-Message) you only actually use around 8Kbps for the audio stream each way so for 20 concurrent calls using A-Law would only use roughly 1 Mbps in total (500Kbps Up and Down). SIP really is not a high bandwidth event unless you use HD codecs for better quality voice:

<table>
<tr><th colspan="2">Incoming Bandwidth</th><th colspan="2">Outgoing Bandwidth</th></tr>
<tr><td colspan="2">Calls: 20</td><td colspan="2">Calls: 20</td></tr>
<tr><td colspan="2">RTP: 4.69 Kbps</td><td colspan="2">RTP: 4.69 Kbps</td></tr>
<tr><td colspan="2">UDP: 3.13 Kbps</td><td colspan="2">UDP: 3.13 Kbps</td></tr>
<tr><td colspan="2">IP: 7.81 Kbps</td><td colspan="2">IP: 7.81 Kbps</td></tr>
<tr><td colspan="2">Protocol: SIP</td><td colspan="2">Protocol: SIP</td></tr>
<tr><td colspan="2">Audio Codec: 8.00g.729a Kbps</td><td colspan="2">Audio Codec: 8.00g.729a Kbps</td></tr>
<tr><td colspan="2">* SIP overhead is disregarded</td><td colspan="2">* SIP overhead is disregarded</td></tr>
<tr><td>Incoming bandwidth:</td><td>472.5 Kbps
0.46 Mbps
59.06 Kbps
0.06 Mbps</td><td>Outgoing bandwidth:</td><td>472.5 Kbps
0.46 Mbps
59.06 Kbps
0.06 Mbps</td></tr>
<tr><td colspan="2">Total bandwidth (incoming and outgoing):</td><td colspan="2">945 Kbps
0.92 Mbps
118.13 Kbps</td></tr>
</table>

7. Multitone Smart Apps - Product Variants, Software Versions, Operating Systems & Status

Product	@ppear S/w Version	i-Message S/w Version	Key Features	Product Identity	Download Platform	Operating System	Status	Notes
@ppear Black Berry 7	1.3.22	1.5.2.0001	Status, Message, Contacts & Templates	Multitone @ppear	Side Loaded	Blackberry 7	Released s/w no longer supported	
@ppear Black Berry 10	0.9.15.69	1.5.3.0001	Status, Message, Contacts, Templates, Audio, Picture & Cloud Push Notification	Multitone @ppear	Side Loaded	Blackberry 10	Released s/w no longer supported	
@ppear Windows	1.0.0.5	1.6.0.0003	Status, Message, Contacts, Templates, Audio, Picture & Cloud Push Notification	Multitone @ppear	Side Loaded	Windows 8.1 Windows 10	Released s/w no longer supported	Do not use for emergency
@ppear Android	1.4.3.11	1.6.0.0003	Status, Message, Contacts, Templates, Audio, Picture & Cloud Push Notification	Multitone @ppear	Google Play	Android 5.1 (Lollipop) Android 6.0.1 (Marshmallow)	Released s/w no longer supported	Does not support i-Message 1.6.1.0002 or above
@ppear iOS	1.2.5	1.6.0.0003	Status, Message, Contacts, Templates, Audio, Picture & Cloud Push Notification	Multitone @ppear	Apple App Store	iOS 8 iOS 9 iOS 10	Released s/w no longer supported	Does not support i-Message 1.6.1.0002 or above

8. Multitone Appear - Product Variants, Software Versions, Operating Systems & Status

Multitone Appear, Multitone Appear Lite, Multitone Appear Crew, Multitone Appear Workflow, MallCall - Software Version Status (Issue 2.0)						
Product	Appear Software Version	Key Features	Download Platform	Operating System	i-Message Software Version	Status
Multitone Messenger (Android)	1.6.3	Status, Message, Chats, Contacts, Picture, Video, Cloud Push Notification, SIP Phone	Google Play	Android 5.0 & 5.1: Lollipop, Android 6.0: Marshmallow Android 7.0 & 7.1: Nougat Android 8.0 & 8.1:Oreo Android 10, 11, 12, & 13 Android 9.0 Pie	1.8.0.0293	Released 01/08/2023
Multitone Messenger (iOS)	1.3.6	Status, Message, Chats, Contacts, Picture, Video, Cloud Push Notification, SIP Phone	Apple App Store	iOS 14, 15, 16 & 17	1.8.0.0293	Released 01/08/2023
Appear (Android)	1.2.4.9	Status, Message, Contacts, Templates, Audio, Picture, Video, Cloud Push Notification, SIP Phone & Button Page	Google Play	Android 5.0 & 5.1: Lollipop, Android 6.0: Marshmallow Android 7.0 & 7.1: Nougat Android 8.0 & 8.1:Oreo Android 10, 11, 12, & 13 Android 9.0 Pie	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 10/04/2022
Appear (iOS)	1.3.6	Status, Message, Contacts, Templates, Audio, Picture, Video, Cloud Push Notification, SIP Phone & Button Page	Apple App Store	iOS 14, 15, 16 & 17	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 01/07/2022
Appear Lite(Android)	1.5.3.2	User & Team Messaging with Acknowledgement	Google Play	Android 5.0 & 5.1: Lollipop, Android 6.0: Marshmallow Android 7.0 & 7.1: Nougat Android 8.0 & 8.1:Oreo Android 10, 11, 12, & 13 Android 9.0 Pie	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 02/07/2022
Appear Lite (iOS)	1.0.6	User & Team Messaging with Acknowledgement	Apple App Store	iOS 14, 15, 16 & 17	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 14/07/2022
Appear Crew (Android)	1.0.0.35	Message, Crew Muster, Acknowledgement & Status Messaging	Google Play	Android 5.0 & 5.1: Lollipop, Android 6.0: Marshmallow Android 7.0 & 7.1: Nougat Android 8.0 & 8.1:Oreo Android 10, 11, 12, & 13 Android 9.0 Pie	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 26/07/2021
Appear Crew (iOS)	1.0.	Message, Crew Muster, Acknowledgement & Status Messaging	Apple App Store	iOS 14, 15, 16 & 17	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 26/05/2022
Mall Call - Control Room	1.7.0.4	Message, Contacts, Templates & News Feed	Side Loaded	Android x86 8.1	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 31/05/2019
Mall Call - Shop	1.2.9	Message & SMART Buttons	Side Loaded	Android 5.1. Lollipop	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 01/09/2021
Mall Call - Security	1.1.5	Message & Templates	Side Loaded	Android 4.4 Kit Kat	1.6.1.0002, 1.6.1.0003, 1.6.2.0001 RC 5 to RC 9, 1.6.3.0001 RC 1 to 7, 1.7.0.0001 RC 2, 1.8.0.0293	Released 03/09/2019

9. Multitone i-Message Software Matrix

Software Version	Date	Operating System	Primary Server Platforms	Key Features
1.3.1	June 2012 (Approx.)	Windows 2008 R2	Del R230 Del R330	Initial Release Multitone i-Message release, SCU, Alarms, Call Log, Queries, Users, Teams, Recordings, Alphas, Backup, Devices, Access 3000, Paging, DLC, Alarm Panels, Tasks
1.5.2	October 2014	Windows 2008 R2	Del R230 Del R330	- Multitone @ppear (Blackberry, Android, iOS) - Blackboard and Mopboard - SNMP - TAPI - OPC - Web Gateway
1.5.3	August 2015	Windows 2008 R2	Del R230 DelR330	- User details display - Team membership - Multi-line Alphas - GUI enhancements - Smart App Module Enhancements
1.6.0	October 2016	Windows 2008 R2 Windows 2012 R1 Windows 2012 R2	Del R230 DelR330	- Call Log Client (Admin Client) - Multitone Appear Enhancement - Event Action Manager (EAM) enhancements
1.6.1	November 2017	Windows 2008 R2 Windows 2012 R1 Windows 2012 R2	Del R230 DelR330	- Mall Call - SIP Client Interface with conference bridge - SCU revisions - Email to SMS - Multitone @ppear not supported on 1.6.1 and below
1.6.2	April 2018	Windows 2008 R2 Windows 2012 R1 Windows 2012 R2	Del R230 Del R330	- Multitone Appear - Multitone Appear Lite - SMAP user client - Image Upload Feature - Revised Team Management Features
1.6.3.1	October 2018	Windows 2008 R2 Windows 2012 R1 Windows 2012 R2	Del R230 Del R330	- DMZ Proxy Server - Meet Me - POCSAG Numeric 512 & 1200 Device - Beep code and pre-fixed messages sent via MIP or ESPA 4.4.4 - Live Voice prompt with live voice from telephone interface
1.7.0	August 2020	Windows 2016	Del R240 Del R340	- NDB Clustering 7.6.10 - Asset Tracking Support
1.7.1	Not for release superseded by 1.8.0	Windows 2016	Del R240, R340 AWS Cloud Services	- Major Incident Management (Majax) - Active Directory Users synchronisation (Beta release only) - Live Maps & Location Support (Indoor/Outdoor) - Super Proxy for smart apps
1.8.0	In testing	Windows 2016, 2019	Del R240, R340 AWS Cloud Services	- Major Incident Management (Majax) update with React - Multi-Tenancy (AWS Cloud Support) - Messenger (iOS, Android) - Cyber essentials - NDB Clustering 8.0.23 - Live Maps & Location Support(Indoor/Outdoor) update - Message Queuing Telemetry Transport (MQTT) message broker (IoT - BLE, LoRA, SigFox, WiFi) - New Enhanced Email introduced for in/out emails
1.8.1	In development	Windows 2016, 2019	Del R240, R340 AWS Cloud Services	- Roles - Workflow & Task Management - New WiFi pager system support

Software Version	Date	Operating System	Primary Server Platforms	Key Features
2.0	TBA Roadmap	TBA	TBA	- React/React Native UI/UX - React/React Native App running on iOS, Android - Restful API (Modular Architecture, Cloud Optimised)