Software Release Note
Vocality Gateway Suite 8.3.1

Date of software release: 20th December 2024
Release Note date: 20th December 2024
Release Note version: 1.0
Release Identification: 8.3.1-16c5100ea

Purpose of Release

The key purpose of the release is to improved mobile connectivity loss recovery, the first release of the new RallyTac integration, and a fix for updating TX only talk groups.

Document History

Version	Date	Details
1.0	20th December 2024	Initial Draft

Hardware Affected

This release is targeted to all versions of Cubic's RoIP, M3X RoIP and M3-SE-MFGW.

Pre-Requisites

This release should only be installed on Cubic's RoIP products currently running release 4.17.2 and later.

For earlier releases, please use the Software Portal to upgrade to 4.17.2 first.

Upgrade Instructions

This software release will only upgrade from the 8.2.2 release, or later, due to an upgrade to the download image encryption.

Important Notes

Rallytac Engage Feature Usage

The new RallyTac Engage feature requires SWF/1E license. Please contact Cubic Vocality sales to purchase it.

Key Features and Enhancements

RallyTac Engage Integration

Modern secure communication systems are often complex to setup and scale; however, recent changes made to the Vocality RoIP software have simplified this process.

The Vocality RoIP now features embedded Rallypoint and Engage Bridge software modules from Rally Tactical Systems, which support secure voice communications between connected Rallypoint enabled devices, forming a mesh network in the process.

- The Vocality RoIP can be specified as a Rallypoint for other Rallypoint-enabled devices and third-party software platforms to connect to the RoIP, or the Vocality RoIP can be configured to use an external Rallypoint to create a secure connection with other nodes.
- Security is applied at a group/channel level, meaning only devices configured to access the group/channel can speak to and hear audio from the group/channel.
- Connecting two or more Rallypoint-enabled devices creates a secure mesh network (i.e. the connected devices act as a single network), which can be set up quickly and easily. Additional nodes can be added with minimal configuration.
- The connection topology is flexible and allows for both traditional structured designs as well as more complex configurations, which can also include network/mesh resiliance measures. Once connected, a device can communicate with all the nodes within the Rallypoint mesh network.

For more information on this feature, please use the following link :-

Cubic Rallypoint Info

Enhancements

- Added the ability to online upgrade to ENC4 software images. These have better encryption.
- Improved mobile connectivity monitoring to ensure automatic recovery from a loss of network connectivity.
- When updating a TX only talk group, audio was no longer sent, it was only recoverable by deleting the talk group and recreating. This has now been fixed.

DTECH Mission Solutions UK Limited, Unity, Building A, Watchmoor Park, Camberley GU15 3YL

Web: www.cubic.com/vocality | Email: Vocality.sales@cubic.com | Tel: +1 858-505-2445

DTECH Mission Solutions UK Limited, registered AFC House Honeycrock Lane, Salfords, Redhill, Surrey, United Kingdom, RH1 5LA, is a trading name of GATR Technologies INC, a Cubic Corporation Business.

- Removed Codec2 & G729a support from the Rallytac functionality, as no audio was present when using them. Will be re-instated in a later release.
- RTP talkgroup and Rallytac codec names were inconsistent. Now they match.

Restful API
- Added ability to create an Engage talkgroup.

Security fixes

Library	Version	CVE	Info
apache2-native	2.4.58	CVE-2024-40898	https://nvd.nist.gov/vuln/detail/CVE-2024-40898
apache2-native	2.4.58	CVE-2024-38477	https://nvd.nist.gov/vuln/detail/CVE-2024-38477
apache2-native	2.4.58	CVE-2024-38476	https://nvd.nist.gov/vuln/detail/CVE-2024-38476
apache2-native	2.4.58	CVE-2024-38474	https://nvd.nist.gov/vuln/detail/CVE-2024-38474
apache2-native	2.4.58	CVE-2024-27316	https://nvd.nist.gov/vuln/detail/CVE-2024-27316
apache2-native	2.4.58	CVE-2023-44487	https://nvd.nist.gov/vuln/detail/CVE-2023-44487
apache2-native	2.4.58	CVE-2017-1000118	https://nvd.nist.gov/vuln/detail/CVE-2017-1000118

Component Version Numbers
Changes highlighted.
- vocality_api-2.2.1
- vocality_database-1.3.0
- vocality_dispatch-1.6.0
- vocality_filesystem-1.1.1
- vocality_mcpttgateway-2.0.1
- vocality_modemupgrade-1.2.7
- vocality_multibearer-3.4.2
- vocality_nodemanager-4.17.3
- vocality_nodeui-4.19.1
- vocality_password-1.1.2
- vocality_picfirmware-1.1.0
- vocality_radiogateway-5.0.0
- vocality_registry-3.4.0
- vocality_registryclient-3.4.0
- vocality_release-8.3.1
- vocality_secure-4.2.3
- vocality_serial-3.2.1
- vocality_utils-2.2.3