Caliber PUBLIC SAFETY

Protecting Tomorrow–Today.™

Online RMS

Version (11.8.3)

Product Change Notice

01 March 2022

REVISION HISTORY

Revised By	Revision Date	Version	Notes
T. Thompson	01 Mar 2022	1.0	Production release.

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.8.3 release of the Online RMS product and will assist with release preparation activities including:

- Internal staff training
- Customer release training
- Customer release notes
- Release announcement and promotion
- Online help and eLearning updates
- Updates to web site product information and product collateral

PRODUCT REQUIREMENTS

For best performance, we recommend a computer, laptop, or tablet purchased within the last 3 years; running an industry popular web browser that is actively supported by the browser manufacturer and connects to the internet using DSL, Cable, or 4G cellular. The browser must support TLS 1.2 or higher.

IMPORTANT NOTICE FOR ONLINE RMS AGENCIES

ONLINE RMS TO DESUPPORT INTERNET EXPLORER (IE) 11 – AUG 2021

Microsoft announced IE 11 will stop working optimally with Microsoft 365 services on Aug. 17, 2021. IE is no longer supporting new web standards that are used by modern applications. For this reason, Online RMS will no longer consider IE a modern web browser. Caliber recommends agencies plan to move from IE 11 to a modern web browser as soon as possible.

RELEASE MILESTONES

The following table contains the high-level release milestones for the Online RMS 11.8.3 release.

End Date	Milestone
24 Jan 2022	11.8.3 Sprint 1 Starts
22 Feb 2022	11.8.3 Code Lock
01 Mar 2022	11.8.3 Release Available

APPENDIX: 11.8.3 PRODUCT CHANGE NOTICE (PCN) – DETAILED JIRA LISTING

TABLE A: Release Enhancements and Product Software Issue Resolutions

This table contains enhancement, software issue, and interface JIRAs contained in the 11.8.3 release.
* - Denotes a software resolution was released prior to the 11.8.3 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-74544	N/A	Community Reporting - Multiple Images / Remaining Work	Enhancement	Community Reporting	Software Improvement - Community Report enhanced to allow multiple image files to be uploaded by citizens.
IA-74874	413618	NIBRS Reporting 10 unique offense when there are more the 10 offenses on an incident	Release Defects	State Submissions	Software Update - The Indiana NIBRS file generation process was adjusted to process up to 10 unique offenses when more than 10 offenses are being reported in an incident report.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-74905	N/A	OK SIBRS: XML reporting extra and incorrect property to association when there are two property offenses (not lesser), and one vehicle is associated to both offenses Part 2 Testing Issue	Release Defects	State Submissions	Software Update - The Oklahoma Incident Based Reporting (OK SIBRS) has been updated to correct two scenarios involving 290 offenses with vehicles also associated to 240 offenses.
IA-74957	N/A	Online RMS- Install script for release 11.8.3	DevTask	Admin	Install table script for release 11.8.3
IA-75028	414563 414566	RMS terminating User Session	Bug/Defect	Admin	Software Update - Resolved an issue with interment user sessions expiring due automatic InterDex inquires.
IA-75049	N/A	Online RMS- Jasper Ad hoc Person Image View Update	Enhancement	Ad Hoc Reporting	Software Update - The person image view for Jasper Ad Hoc reporting was updated to return the image thumbnail view.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-75076	410454	OK SIBRS Warning Institutional, Other, Runaway and Missing Roles are only valid for Incidents with 80s series offenses only applies to Offender with one of these Roles	Enhancement	State Submissions	Oklahoma SIBRS configuration update. Deactivated the Incident Warning for "Institutional, Other, Runaway and Missing Roles" for 80s series offense of Oklahoma Agencies. Testing verified that the submission logic is properly handling and only submitting valid roles for 80s series offenses. The validation warning is not needed and was causing confusion.
IA-75135	N/A	Incident Approval Notification clean up script	Bug/Defect	Notifications	Data Script to remove 'Approve Incident Report' notifications where the incident report had already been approved.

--END--

APPENDIX: SERVICE COMMITMENTS

Caliber Public Safety designs its processes and procedures related to its RMS system based on the service commitments that Caliber Public Safety makes to its business units, the laws and regulations that govern the system and the operational and compliance requirements that Caliber Public Safety has established.

Security, availability, confidentiality, and processing integrity commitments include, but are not limited to, the following:

Security Commitments

- Secure Socket Layer (SSL) FIPS140-2 compliant encryption is used to encrypt the transmission of data with Caliber hosted systems.
- Access to customer data is restricted to Caliber employees and/or subcontractors whose job function requires access.
- RMS Development, operations, and customer service personnel are required to maintain active CJIS certification.
- Systems are subject to vulnerability scanning.

Availability Commitments

- Caliber will maintain a highly available platform (99.9% uptime) that includes redundancy for critical system components except during planned downtime as communicated to users or unplanned downtime caused by circumstances beyond its reasonable control. In practice, Caliber routinely exceeds 99.99% uptime.
- User entity data is backed up daily and replicated to a secondary location.
- User entity data is maintained and stored within the United States.

Confidentiality Commitments

- Upon termination of services, Caliber will return confidential data to customers subject to the terms of the current RMS SaaS agreement.
- Caliber shall protect information designated as confidential from unauthorized access.
- Confidential data shall only be stored within Caliber's company information systems.

Processing Integrity Commitments

- The organization communicates requirements to user entities regarding the information, data, or other specifications necessary to complete processing in alignment with standard business operations.
- Data processing requests are only performed as authorized by the user entity.
- Data shall be stored and maintained in the system with no unauthorized alteration.