Caliber PUBLIC SAFETY

Protecting Tomorrow–Today.™

Online RMS

Version (11.6.3)

Product Change Notice

13 July 2021

REVISION HISTORY

Revised By	Revision Date	Version	Notes
T. Thompson	13 July 2021	1.0	Production release.

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.6.3 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 11.6.3 release.

End Date	Milestone
01 June 2021	11.6.3 Sprint 1 Starts
06 July 2021	11.6.3 Code Lock
13 July 2021	11.6.3 Release Available

APPENDIX: 11.6.3 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 11.6.3 release.
* - Denotes a software resolution was released prior to the 11.6.3 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-73381	403673 405519 406027 406420 406539	User Receives Warning another RMS session is open when creating a Narrative. Research	Configuration	RMS Admin	Software modification to improve ending of session when user receives a warning of an open session when creating an incident report narrative.
IA-73391	405613	Evidence locations not being retained when a Checked-Out item is Checked back in	Bug/Defect	Evidence / Held Property	Software modification to default the property Location list of values with the previous checked in location, when performing a check in for evidence / held property.
IA-73411	N/A	Script to Add Bias to Incident Rules & Validations to Incident Offense Tab	Configuration	State Submissions	Software modification to support configuring Rules and Validations for Offense details page based on bias code entered.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-73439	N/A	MICR: Configuration for MICR requirements - 90Z-G	Configuration	State Submissions	State NIBRS Reporting - Configuration update to Michigan state MICR reporting.
IA-73454	N/A	Online RMS- Install script for release 11.6.3	DevTask	RMS Admin	Online RMS- Install script for release 11.6.3
IA-73541*	N/A	Online RMS- Jasper updates for Production (Bill)	DevTask	Ad Hoc Reporting	Database view modification to include Employee Rank/Title.
IA-73609*	406620	Evidence Recovered Time Issue	Bug/Defect	Evidence	Software modification to resolve an issue when checking in Evidence / Held Property by acting on Notification #20 - Evidence / Held Property Pending Check in.

--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.